On Classification and Some Properties of APN Functions

Bo Sun

Thesis for the Degree of Philosophiae Doctor (PhD)
University of Bergen, Norway
2018

UNIVERSITY OF BERGEN

On Classification and Some Properties of APN Functions

Bo Sun

Thesis for the Degree of Philosophiae Doctor (PhD)
at the University of Bergen

2018

Date of defence: 22.06.2018

Year: 2018

Title: On Classification and Some Properties of APN Functions

Name: Bo Sun

Print: Skipnes Kommunikasjon / University of Bergen

To my parents and my husband

Abstract

Boolean functions optimal with respect to different cryptographic properties (such as APN, AB, bent functions, etc.) are crucial to the design of secure cryptosystems. Investigating the properties and construction of these functions is therefore essential from both a theoretical and a practical point of view.

In this thesis, we focus on the investigation of Almost Perfect Nonlinear (APN) functions, which provide optimal resistance against differential attack. Following a general overview of the cryptography background and the role of Boolean functions in cryptography, we give a systematic overview of different classes of cryptographically optimal Boolean functions and their characterizations and properties, and describe original results about the construction of new APN functions in some detail.

In particular, we present an overview of our research concerning the existence of APN functions over $\mathbb{F}_{2^n}$ of algebraic degree n and a related construction involving changing the value of an existing APN function at a single point. We determine the Walsh spectra of the last three infinite quadratic APN families for which this had not been previously done. We give a table of representatives for all CCZ-inequivalent APN functions over the fields $\mathbb{F}_{2^n}$ for $6 \leqslant n \leqslant 11$ which arise from all known families of APN functions. This table significantly facilitates the process of checking whether a given APN function is equivalent to any of the known infinite classes. We also present the results of an experimental procedure for classifying all quadratic APN polynomials of a particular form over fields of dimension $6 \leqslant n \leqslant 11$.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisor Lilya Budaghyan for providing me the opportunity to obtain a Ph.D. degree and her continuous support, as well as for her patience, motivation, and immense knowledge. I am lucky and honored to be her student as she is one of the top researchers in our field and is a wonderful group leader. I never expected anyone could help me as much as she did. She not only shared her knowledge and dedication, her experience and wisdom with me, but also taught me to be an active person and to keep going no matter how tough life is. I am much indebted to her as my respected supervisor, yet she is much more to me than that: she is also my life mentor, role model, and best friend.

I would like to thank my co-supervisors, Chunlei Li and Nian Li. Our friendship began long before they became my co-supervisors. I sincerely appreciate their insightful comments and encouragement, their guidance, support and kind advice throughout my Ph.D. studies. I am flattered to be friends with these two wonderful people and a student of these two excellent young researchers.

My sincere thanks also go to Tor Helleseth who gave me the opportunity to join the team, to be supervised by Lilya and to collaborate with him on their work. Without his amazing support, it would not be possible for me to be part of this research. He is one of the most respected and highly reputed scientists worldwide; however, under his halo of academic excellence, he is also an incredibly humble, gentle, caring, positive and pleasant person. He will be my role model for life and work forever.

I thank my colleague, and one of my best friends Nikolay Stoyanov Kaleyski for his generosity and ongoing support during the writing of my thesis. His humility, kindness and talent for both writing and research inspire me a lot.

I'm grateful to Kjell Jørgen Hole, who spent time supervising me during part of my Ph.D. studies. I will also never forget how Per Øyvind Hervik Thorsheim helped me with an exciting project focused on user passwords and cheered me up in my time of uncertainty. I also thank Chunming Rong for suggesting an interesting topic of research to me and for supervising me at the beginning of my Ph.D. studies. I want to thank Khalid Mughal for introducing me to his field of research. I am fortunate to have met my schoolmate from my master's studies, Samson Hussien Gejibo, at our department in Bergen, and am grateful to him for his time assisting me with my Ph.D. studies and for cheering me up. I also want to say thank you to Christian Otterstad, who helped me out with many technical problems.

I would like to thank all my colleagues from the Selmer centre: Irene Villa, Andrea Tenti, Isaac Canales Martinez, Dong Yang, Diana Davidova, Matthew Parker, Igor Semaev, Alessandro Budroni, Dan Zhang, Navid Ghaedi Bardeh, Sachin Valera, Marco Calderini, Qian Guo and Wrya Kadir who built a friendly and warm research environment for me, and my friendship with them will last lifelong.

Tor Bastiansen, Ida Rosenlund, Liv Rebecca Arnedatter Aae and the other administrative personnel at our department always helped me out in time. Thanks to them, I never had to worry about bureaucracy. Special thanks go to Jan Arne Telle, who was helpful and just during the turning point of my Ph.D. studies. I am grateful to the COINS research school, and especially to Hanno Langweg and Urszula Nowostawska for giving me the opportunity to join many scientific activities funded by COINS.

I am not only lucky with my research, but also I had the most supportive family and friends.

My mother XiuLan Shi and my father GuoZhang Sun gave me the most peaceful and happy family I could ever imagine. I am especially grateful to my witty and sagacious father who has always cheered me up and knows me the best. I am very glad and proud to have fulfilled

one of the meanings of the name he gave to me by obtaining my Ph.D. degree. I will always bear in my heart the other virtues that he wished me in my name: having broad knowledge and a benevolent mind.

My husband XiaXi Li supported me a lot during my Ph.D. studies. He respected my decision to quit my stable job in Stockholm to pursue my Ph.D., he turned down many excellent career opportunities to accompany me here and he spent a lot of time taking care of our daughter.

My sincere thanks also go to my parents in law, Hong Zhang and GenLi Li. They respected and supported their son's decision to accompany me in Bergen. Especially my mother in law put aside her job to come here and take care of us so that I would have more time for my Ph.D. studies.

I am also infinitely grateful to my dear friends, Lu Li, Srimathi Varadharajan, Mithilesh Kumar, XinJiao Chen, Guang Yang, HongLei Cao who I know I can always trust and talk to about anything.

The above is by no means a complete list of all the people that I would like to thank.

The Ph.D. journey is indeed an adventure for me. During these years, I encountered many challenges in my life as well as in my research. Without all of the help and kindness that I got, my Ph.D. dream would have never come true.

7f716994ac4152ad194e116b61e1dae31c9db1c16dc13993 (DES-CBC)

Contents

List of Tables

Note: All tables are also available at https://boolean.w.uib.no/.

List of Figures

Summary

Typically there is only one nonlinear component in a symmetric block cipher, but it plays a vital role: this is the so-called "S-box", or "substitution box". Mathematically speaking, the S-box is nothing else than a vectorial Boolean function, mapping a sequence of input bits to a sequence of output bits.

Two of the most well-known and efficient attacks against such block ciphers are differential and linear attacks. The resistance of the cryptosystem to such attacks directly depends on specific properties of the underlying S-box, namely its differential uniformity and nonlinearity.

Different attacks exploit different properties of a vectorial Boolean function. Some of the most frequently used cryptographic attacks are differential attacks, linear attacks, and higher order differential attacks. The properties that these attacks exploit are differential uniformity, nonlinearity, and algebraic degree, respectively. Functions with low differential uniformity have better resistance to differential attacks. For vectorial Boolean functions from $\mathbb{F}_{2^n}$ to itself (which is the case that we consider most frequently), a differential uniformity of two is optimal, and the functions that achieve this value are called Almost Perfect Nonlinear (APN) functions. Similarly, a high nonlinearity indicates resistance against linear attacks. An upper bound on the nonlinearity of any vectorial Boolean function can be shown, and the functions achieving this optimal nonlinearity are called Almost Bent (AB).

The nonlinearity of a function can be expressed using the values of that function's so-called Walsh transform. Up to now, 11 infinite polynomial APN families have been found. The Walsh spectra (that is, the multisets of values of the Walsh transform) had previously been computed for 8 out of these 11 families. In our work we determined the Walsh spectra of the last three infinite families for which they

were not known [33]. The families in question are represented by the functions F_0, F_1 and F_2 defined as:

$$\begin{aligned} F_0(x) &= x^3 + a^{-1}\mathrm{tr}_n^1(a^3x^9) \\ F_1(x) &= x^3 + a^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18}) \\ F_2(x) &= x^3 + a^{-1}\mathrm{tr}_3^n(a^6x^{18} + a^{12}x^{36}) \end{aligned}$$

over $\mathbb{F}_{2^n}$ with $a \in \mathbb{F}_{2^n}^*$.

It turned out that these functions have Gold-like Walsh spectra. Over fields of odd dimensions, the Walsh spectrum of the functions from the Gold family is the same as that of the AB functions; the values in the spectrum are $0, \pm 2^{\frac{n+1}{2}}$. Over fields of even dimension, the values of the Walsh spectrum are $0, \pm 2^{n/2}$ and $\pm 2^{(n+2)/2}$. Combining this with the already known results in this direction, we conclude that all the known families of quadratic APN functions have Gold-like Walsh spectra.

Higher order differential attacks function by analyzing the propagation of a group of differences between a broad set of plaintext and ciphertext pairs. Vectorial Boolean functions with a high algebraic degree are optimal for preventing these attacks. However, the problem of finding an exact upper bound on the algebraic degree of APN functions in the general case remains open. We investigated this problem by considering a construction in which we change the value of a given APN function at one point [25]. We deduced several non-existence results which imply, in particular, that for most of the known APN functions F over $\mathbb{F}_{2^n}$ the function $x^{2^n-1} + F(x)$ is not APN. Thus, changing a value of one of these functions at a single point results in a function that is not APN. This, in turn, indicates that the algebraic degree of APN functions from many different classes cannot be equal to n. We conjecture that this is true for any APN function.

Nonlinearity and differential uniformity are invariant under affine, extended affine (EA) and Carlet-Charpin-Zinoviev (CCZ) equivalence. CCZ-equivalence is the most general among these three equivalence

relations, and vectorial Boolean functions are typically classified up to CCZ-equivalence. The classification of APN and AB functions is a hard open problem. So far, a complete classification of APN functions is only known for fields $\mathbb{F}_{2^n}$ of dimension $n \leqslant 5$ [13].

With our limited computing resources and with the vast amount of functions even over a field of relatively small dimension, an exhaustive search over all vectorial Boolean functions is impossible. Thus, characterizations and necessary conditions limiting the search space as well as specialized constructions are needed to find new APN functions.

One possibility is to examine all functions of a particular given form. In our work, we classified all quadratic APN functions with coefficients in $\mathbb{F}_2$ and a limited number of nonzero terms: trinomials, quadrinomials, pentanomials, and hexanomials over $\mathbb{F}_{2^n}$ for $6 \leqslant n \leqslant 11$. We found 5 new APN functions over $\mathbb{F}_{2^{11}}$ which are CCZ-inequivalent to all the known infinite APN families [90].

For classifying and finding new APN functions, it is necessary to test potential candidates for equivalence against the already known equivalence classes. Up to now, 17 infinite families of APN functions have been discovered. Among them there are 6 families of power functions and 11 families of polynomial functions. The polynomial families, in particular, are quite large and contain a very large number of functions even for small dimensions. The reason for this is that the definitions of these functions contain many parameters which results in a very large number of functions. Consider for instance the family defined by

$$F(x) = x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)},$$

where $q = 2^m$, $n = 2m$, $\gcd(i, m) = 1, \gcd(2^i + 1, q + 1) \neq 1, cb^q + b \neq 0, c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}, c^{q+1} = 1$. There are 45012 APN functions in this family for $n = 10$. Therefore, it is very difficult to check the equivalence of a given APN function to this family already over $\mathbb{F}_{2^{10}}$. Performing such a comparison is difficult not only for the

polynomial families, but also for the monomial ones. Nonetheless, conducting such equivalence tests is crucial when searching for new APN functions: for instance, a certain family was proved to be APN [56] but we showed that the functions in question are in fact affine equivalent to the Gold family [33].

This motivated us to simplify the comparison procedure by compiling a list of pairwise CCZ-inequivalent representatives from all the families. To explain our work in more detail, consider the aforementioned family over $\mathbb{F}_{2^{10}}$ as an example. First, we found the range of values of each parameter and we constructed the corresponding 45012 APN functions. Second, we tested all those 45012 APN functions against each other for equivalence; this produced two CCZ-inequivalent classes. Next, from each class, we chose one representative function with the "simplest" (based on certain criteria) coefficients. Finally, we checked for CCZ-equivalence between each of these two representatives and representatives of other families over $\mathbb{F}_{2^{10}}$ (themselves computed in a similar manner). In the end, both representatives turned out to be CCZ-inequivalent to other families, so we listed them in our table. We performed these computations for all dimensions n in the range $6 \leqslant n \leqslant 11$ [89].

This thesis is structured as follows. In Chapters 1 and 2, we present the general background behind cryptography as well as the basic notation and definitions along with some properties and equivalence relations of vectorial Boolean functions. Chapter 3 focuses on some more complicated notions and recent results on APN functions. It also contains a discussion of PN, plateaued, AB and crooked functions. Chapter 4 is dedicated to a summary of our original results. Section 4.1 concerns the work that we performed while investigating the upper bound on the algebraic degree of APN functions. We did this by changing the value of a given APN function over $\mathbb{F}_{2^n}$ at precisely one point of $\mathbb{F}_{2^n}$. A lot of non-existence results were found using this approach. Section 4.2 describes how we calculated the Walsh spectra of the three infinite polynomial families discussed above. These were

the last three infinite quadratic APN polynomial families whose Walsh spectra remained unknown; consequently, the Walsh spectra of all such families are now known. Section 4.3 demonstrates that the APN function found in [56] is affine equivalent to the Gold family. Section 4.4 describes the setup and results of an experimental procedure for classifying all quadratic APN polynomials with coefficients in $\mathbb{F}_2$ and a small number of nonzero terms over fields of small dimension. Finally, Section 4.5 provides a table of CCZ-inequivalent representatives from each of the known infinite APN families over fields of small dimensions. This allows any newly found APN function to be tested for equivalence against the known classes much more efficiently than by actually comparing it for equivalence against every single representative.

1 General Background of Cryptography

With the development of communication technology, information security has become critical. Cryptographic algorithms are the foundation and cornerstone of information security and have been applied in a multitude of important fields, such as payment and military defense systems.

Most contemporary data encryption principles and concepts are proposed by Claude Elwood Shannon. Cryptography became an independent subject thanks to Shannon's paper "Communication Theory of Secrecy Systems [85]", in which he systematically describes the entire cryptographic system and introduces many fundamental concepts allowing cryptography to be treated as a scientific discipline. In particular, he provides mathematical models for describing cryptographic algorithms and analyzing their properties. All cryptographic algorithms rely on the use of "keys", i.e., pieces of information known only to the legitimate communicating parties which allow them to encrypt and decrypt messages. Cryptosystems are divided into symmetric and asymmetric ones based on the characteristics and usage of the keys [88]: in symmetric cryptosystems, the same key is used for both encryption and decryption, while in asymmetric ones the key for encryption and the one for decryption may be different. Some of the most well-known asymmetric cryptosystems were invented several years before this formal classification: Ronald Linn Rivest, Adi Shamir, and Leonard Adleman invented the RSA cryptosystem (named after their initials) in 1977 [83] and Bailey Whitfield Diffie and Martin Edward Hellman designed the Diffie-Hellman key exchange in 1976 [47].

Symmetric cryptosystems, or ciphers, can be further subdivided into stream ciphers and block ciphers. The former encrypt the input stream one character at a time and are more lightweight and simpler to implement in hardware. The latter process entire blocks of data in a single operation, which makes it easier to design complicated

relationships between the input and the output since any given output character may depend on all input characters.

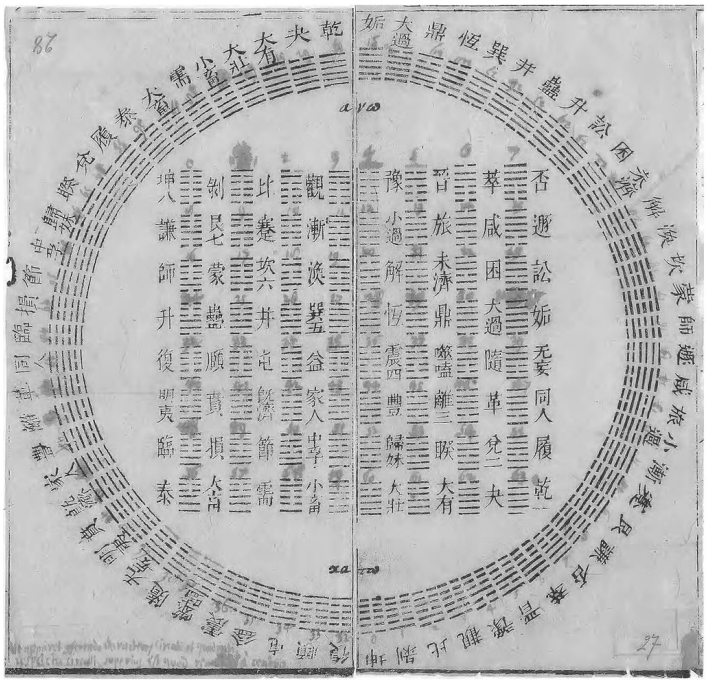


Fig. 1: *A Diagram of the "I Ching" Hexagrams Sent to Leibniz*

Shannon was also the first to demonstrate the practical application of Boolean algebra, which is the theoretical foundation behind modern computer technology, cryptography and various other branches of mathematics and engineering. In the following, we give a short overview of the history of Boolean algebra.

If we trace the origin of the binary number system, we will see that it has been known in many countries throughout history. Evidence of ancient binary-like systems has been discovered during archaeological excavations in Egypt (2400 BC - 1200 BC), China (900 BC - 801 BC) and India (200 BC - 101 BC). To give a concrete example, "I

Ching [54]" is an ancient Chinese book on divination containing a binary-like system. However, these number systems are not complete binary arithmetic systems as we know them today; for instance, the hexagrams from "I Ching" do not have operations defined on them. Gottfried Wilhelm Leibniz systematically introduced binary arithmetic based on the values 1 and 0. He also described "I Ching" in his paper [71] in relation to his work. Figure 1 presents a diagram of "I Ching", with the Arabic numerals added by Leibniz.

Leibniz also made many contributions to various branches of mathematics. Solving systems of linear equations using matrices and the invention of modern calculus are among his many achievements. He also introduced the principles of Boolean algebra without which the study of Boolean functions would have been impossible. Nearly one and a half centuries later, George Boole formally introduced what is now known as Boolean algebra [6] by publishing a series of articles between 1847 and 1854.

Fig. 2: *The Logical Machine of Marquand*

In 1880, Charles Sanders Peirce further studied Boolean algebra and showed that it is possible to describe it using a single binary operation [79]. In 1886, he discovered how logical operations could be implemented by electrical switching circuits [80].

Allan Marquand, a student of Peirce, built the world's first mechanical logical machine in 1881 and presented it publicly in 1885. A photograph of the device can be seen in Figure 2. The theory behind the machine was also published in 1885 [72].

A succinct overview of the most significant contributions of some of the pioneers in the field is given below under Table 1.

Table 1: *Some Pioneers and Their Achievements*

Year	**Name**	**Main Contribution**	**Ref.**
1703	Gottfried Wilhelm Leibniz (1646 - 1716)	introducing modern binary systems	[71]
1854	George Boole (1815 - 1864)	introducing Boolean algebra	[6]
1886	Charles Sanders Peirce (1839 - 1914)	further improving Boole's results and implementing Boolean operations via electric circuits	[78]
1885	Allan Marquand (1853 - 1924)	bulding the first mechanical logical machine	[72]
1940	Claude Elwood Shannon (1916 - 2001)	initiating the fundamental study of cryptography	[84]

2 Boolean Functions and Vectorial Boolean Functions

In this thesis, we study Boolean functions and vectorial Boolean functions as well as their cryptographic properties. A vectorial Boolean function is simply any function defined between two fields of characteristic two. In the particular case when the codomain of this function is the prime field $\mathbb{F}_2$, we call these functions simply Boolean functions. Despite their apparent simplicity, vectorial Boolean functions are fundamental to a wide variety of areas in mathematics and computer science. Boolean and vectorial Boolean functions play an essential role in cryptography since they are used as components of many different encryption algorithms. For instance, they appear under the name of "S-boxes", or "substitution boxes", in the design of block ciphers. According to Shannon's principles of confusion and diffusion [86], these functions should obfuscate the relation between the input and output of the cipher to make breaking it difficult. As a result, the underlying functions are one of the most important components of the cipher, which motivates the study of different classes of optimal Boolean functions (such as APN, AB, and bent functions) along with their construction and properties.

Different characteristics of a given function are used to measure its resistance against different types of cryptographic attacks; for instance, functions with high nonlinearity make ciphers stronger against the so-called linear attack. However, since different types of attacks exploit different characteristics of the function and since the values of these characteristics mutually restrict one another, it is in general impossible to find functions which are optimal with respect to all of these characteristics, and a compromise between the individual properties is necessary. This is one of the reasons that motivate researchers to examine many different classes of functions, such as Almost Perfect Nonlinear (APN) functions, crooked functions

and Almost Bent (AB) functions. All these families are described in this and the next chapter.

2.1 Notation and Basic Definitions

2.1.1 Notation

We use the following notation throughout the thesis to represent some fundamental concepts from field theory:

- $\mathbb{F}_{2^n}$ denotes the finite field with 2^n elements for any positive integer n;
- S^* denotes the set $S \setminus \{0\}$ for any set S; in particular, $\mathbb{F}_{2^n}^*$ is the multiplicative group of the finite field $\mathbb{F}_{2^n}$;
- for $m|n$, $\mathrm{tr}_n^m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is the trace function

$$\mathrm{tr}_n^m(x) = x + x^{2^m} + x^{2^{2m}} + ... + x^{2^{(n/m-1)m}}$$

  from the field with 2^n elements onto the field with 2^m elements;
- tr_n is the absolute trace function tr_n^1 from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$;
- $\mathbb{F}_2^n$ denotes the vector space corresponding to $\mathbb{F}_{2^n}$, i.e., the set of all n-dimensional vectors with elements from the prime field $\mathbb{F}_2$; any finite field can be regarded as a vector space in this manner;
- given a vector $u \in \mathbb{F}_2^n$, the i-th element of u is denoted by u_i for any integer $1 \leqslant i \leqslant n$;
- "$\cdot$" denotes the inner product in the vector space $\mathbb{F}_2^n$, which can be assumed to be defined as $a \cdot b = \mathrm{tr}_n(ab)$ if $\mathbb{F}_2^n$ is interpreted as a finite field.

Following the notation in the Magma programming language, we use the symbols "{∗ ∗}" to denote multisets, i.e., collections of elements in which the same element can occur several times. For example, two multisets A and B are equal if and only if A contains every element of B precisely the same number of times that B does.

2.1.2 Boolean Functions and Vectorial Boolean Functions

We begin the exposition of the thesis with some basic definitions and characteristics related to Boolean functions and vectorial Boolean functions.

Definition 1. An *n-dimensional Boolean function* is any mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

We will denote Boolean functions by the lowercase Latin letters f, g, h, etc. The following are some basic and frequently used properties of Boolean functions.

Definition 2. The *support* of a Boolean function f is the set $supp(f)$ of elements on which it evaluates to a non-zero value, i.e.,

$$supp(f) = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}.$$

The *Hamming weight*, or just *weight*, of a Boolean function f, denoted by $wt(f)$, is the size of its support. A Boolean function f is said to be *balanced* if $wt(f) = 2^{n-1}$, i.e., if f attains the values 0 and 1 the same number of times.

The *Hamming distance* $d(f, g)$ between two Boolean functions f and g is defined as the number of elements for which their values differ, i.e.,

$$d(f, g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|.$$

Note that the Hamming distance between f and g is also equal to the Hamming weight of the function $(f + g)$ defined as $(f + g)(x) = f(x) + g(x)$.

Definition 3. A *vectorial Boolean* (n, m)*-function* is any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$.

Vectorial Boolean functions will be denoted by the capital Latin letters F, G, H, etc.

Many of the notions and properties of Boolean functions can be naturally generalized to the case of vectorial Boolean functions.

Definition 4. For any positive integers n and m, an (n, m)-function F is said to be *balanced* if it attains every value from $\mathbb{F}_{2^m}$ the same number of times, i.e., if

$$|\{x \in \mathbb{F}_{2^n} : F(x) = v\}| = 2^{n-m}$$

for any $v \in \mathbb{F}_{2^m}$.

The Hamming distance can be generalized in a natural way as well:

Definition 5. The *Hamming distance* $d(F, G)$ between two (n, m)-functions F and G is defined as the number of field elements at which their values differ, i.e., as

$$d(F, G) = |\{x \in \mathbb{F}_{2^n} : F(x) \neq G(x)\}|.$$

The derivatives of a vectorial Boolean function F are vectorial Boolean functions closely related to F and are used almost ubiquitously i.a. in the study of APN functions.

Definition 6. Given an (n, m)-function F, its *derivative* in direction $a \in \mathbb{F}_{2^n}$ is the (n, m)-function $D_a F$ defined as

$$D_a F(x) = F(x) + F(a + x).$$

The derivatives are important for characterizing various properties of the function since they express the relationship between its input and output. More precisely, the derivative in direction a represents

the difference between the values $F(x)$ and $F(y)$ of the function for all pairs of inputs x and y whose difference $x + y$ is equal to a.

The image set of the derivative D_aF in direction a is denoted by H_a and is referred to as a *differential set* of F. Formally, we write

$$H_a = \{D_aF(x) : x \in \mathbb{F}_{2^n}\} \tag{1}$$

for any $a \in \mathbb{F}_{2^n}$.

The following values are important statistics of any given vectorial Boolean function.

Definition 7. For an (n, m)-function F and for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$ we define the number

$$\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : D_aF(x) = b\}|.$$

The *differential spectrum* of F is the multiset of the values $\Delta_F(a, b)$ for all a and b with $a \neq 0$, i.e., the multiset

$$\{* \ \Delta_F(a, b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m} \ *\}.$$

The *differential uniformity* Δ_F of the function F is then defined as the maximum value in its differential spectrum, i.e., as

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}} \Delta_F(a, b).$$

Another useful function related to Δ_F is denoted by γ_F and is defined as

$$\gamma_F(a, b) = \begin{cases} 1 & a \neq 0 \ \& \ \Delta_F(a, b) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

While $\Delta_F(a, b)$ represents the number of solutions x to the equation $D_aF(x) = b$, $\gamma_F(a, b)$ indicates whether this equation has solutions or not.

2.1.3 Representation of Boolean and Vectorial Boolean Functions

Boolean functions can be represented in many different ways. One of the most intuitive expressions of an n-dimensional Boolean function f is the *truth table (TT) representation* which consists of a list of the values $f(x)$ for all possible $x \in \mathbb{F}_2^n$. This can be conveniently done in a table, hence the name. For example, the TT representation of the Boolean function

$$f(x_1, x_2, x_3) = x_1 + x_3 + x_2x_3$$

with domain $\mathbb{F}_2^3$ is given below under Table 2. Recall that $\mathbb{F}_{2^n}$ can be interpreted as a vector space, in which case the argument x in $f(x)$ can be regarded as a vector $x = (x_1, x_2, \ldots, x_n)$.

Table 2: *Truth Table of* $f(x_1, x_2, x_3) = x_1 + x_3 + x_2x_3$ *on* $\mathbb{F}_2^3$

x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Another frequently used representation is the algebraic normal form (ANF).

Definition 8. Let f be an n-dimensional Boolean function. Then the polynomial

$$f(x) = \sum_{v \in \mathbb{F}_2^n} a_v \prod_{1 \leqslant i \leqslant n} x_i^{v_i}, a_v \in \mathbb{F}_2$$

is called the *algebraic normal form (ANF)* of the function f.

It can be shown that this representation always exists and is unique; see, e.g., [38].

While the above two representations usually suffice in the case of the relatively simple Boolean functions, a more extensive variety of representations exists and is commonly used when working with the more complicated vectorial Boolean functions.

A vectorial Boolean function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ can be represented simply as a vector of m Boolean functions of dimension n so that we have

$$F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$$

with $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ for all i. The Boolean functions f_i are called the *coordinate functions* of F; it is sometimes useful to study a given function or family of functions in terms of its coordinate functions.

A related notion is that of the *component functions* of an (n, m)-function F, which are the Boolean functions F_b for $b \in \mathbb{F}_{2^m}^*$ defined as

$$F_b(x) = \mathrm{tr}_m(bF(x)) = \sum_{i=1}^{m} b_i f_i, \tag{2}$$

where b_i is the i-th component of $b = (b_1, b_2, \ldots, b_m)$ regarded as an n-dimensional vector from $\mathbb{F}_2^m$.

Vectorial Boolean functions are frequently given in their ANF, which is a natural generalization of the ANF for Boolean functions.

Definition 9. Let F be a vectorial (n, m)-function. Then the polynomial

$$F(x) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}, a_u \in \mathbb{F}_2^m$$

is called the ANF of F.

Just as in the case of Boolean functions, the ANF of a vectorial function always exists and is unique.

An important characteristic of a function F is the degree of its ANF, called the algebraic degree of F and denoted by $d^\circ(F)$. For example, a function F with domain $\mathbb{F}_2^3$ and ANF

$$F(x_1, x_2, x_3) = x_1 + x_3 + x_2x_3$$

has algebraic degree two.

Definition 10. Let F be a vectorial Boolean function. Then we call the degree of its ANF the *algebraic degree* of F and we denote it by $d^\circ(F)$.

Some particular classes of functions are given specific names according to their algebraic degree (among other factors).

Definition 11. We say that a vectorial Boolean function F is:

- *affine* if $d^\circ(F) = 1$;
- *linear* if $d^\circ(F) = 1$ and $F(0) = 0$;
- *quadratic* if $d^\circ(F) = 2$;
- a *Dembowski-Ostrom polynomial (DO polynomial)* if F only consists of quadratic terms, i.e.,

$$F(x) = \sum_{0 \leqslant i < j < n} a_{ij} x^{2^i + 2^j}, \quad a_{ij} \in \mathbb{F}_{2^n}.$$

Another frequently used representation of (n, m)-functions when m is a divisor of n is the following:

Definition 12. Let F be an (n, m)-function with m dividing n. Then the polynomial

$$F(x) = \mathrm{tr}_n^m \left(\sum_{i=0}^{2^n - 1} c_i x^i \right), \quad c_i \in \mathbb{F}_{2^n}$$

is called the *univariate representation of* F.

In particular, for $n = m$, the univariate representation becomes

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

Table 3 presents the univariate representations of DO polynomials and linear, affine and quadratic functions in the case of $n = m$.

Table 3: *Univariate Representations of Some (n, n)-functions*

Name	Representation	d°
Linear	$F(x) = \sum_{0 \leqslant k < n} a_k x^{2^k}$, $a_k \in \mathbb{F}_{2^n}$	1
Affine	$F(x) = \sum_{0 \leqslant k < n} a_k x^{2^k} + c$, $a_k, c \in \mathbb{F}_{2^n}$	1
DO polynomial	$F(x) = \sum_{0 \leqslant i \leqslant j < n} a_{ij} x^{2^i+2^j}$, $a_{ij} \in \mathbb{F}_{2^n}$	2
Quadratic	$F(x) = \sum_{0 \leqslant i \leqslant j < n} a_{ij} x^{2^i+2^j} + \sum_{0 \leqslant k < n} a_k x^{2^k} + c$, $a_{ij}, a_k, c \in \mathbb{F}_{2^n}$	2

Note that the algebraic degree of $d^\circ(F)$ in this case, is equal to the maximum 2-weight $w_2(i)$ for any non-zero coefficient c_i, i.e.,

$$d^\circ(F) = \max_{\substack{0 \leqslant i \leqslant 2^n-1 \\ c_i \neq 0}} w_2(i)$$

where the 2-weight of a positive integer is defined as the number of ones in its binary representation, e.g., the number 11 can be written as $11 = 2^3 + 2^1 + 2^0$ so $w_2(11) = 3$.

Another representation in the case of an (n, n)-function with $n = 2k$ is the polynomial

$$F(x, y) = \sum_{0 \leqslant i,j \leqslant 2^k-1} a_{i,j} x^i y^j, (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$$

which is called the *bivariate representation* of F.

2.1.4 Walsh Transform

A frequently used transformation related to a given Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the *discrete Fourier transform* of f, defined as the integer-valued function

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_{2^n}} f(x)(-1)^{\mathrm{tr}_n(ax)}.$$

Although we do not employ the Fourier transform in our work directly, it does provide us with a natural definition of the Walsh transform in terms of the so-called sign function. The Walsh transform is a mapping related to a given Boolean function that is used in many important characterizations of optimal vectorial Boolean functions and their properties.

Given a Boolean function f, its *sign function* is the integer-valued function

$$f_\chi(x) = (-1)^{f(x)}.$$

Then the Walsh transform of f, which we denote by λ_f, can be defined as the Fourier transform of the sign function of f, i.e.,

$$\lambda_f(a) = \widehat{f_\chi(a)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{tr}_n(ax)}$$

for any $a \in \mathbb{F}_{2^n}$.

The Walsh transform can also be defined directly, i.e., without defining the Fourier transform and sign function.

Definition 13. Let F be a vectorial (n, m)-function. Then the *Walsh transform* of F is the integer-valued function $\lambda_F(a, b)$ defined as

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_m(bF(x))+\mathrm{tr}_n(ax)}$$

for any $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$.

Table 4 presents an overview of the different ways of representing the Walsh transform of both Boolean functions and vectorial Boolean functions. We distinguish between the cases when the function's domain and codomain are viewed as vector spaces and when they are viewed as finite fields, using the inner product or the trace function accordingly. Note that the properties of the Walsh transform do not depend on the choice of inner product and if we assume, as above, that the inner product is defined using the absolute trace function, then the two representations coincide.

Table 4: *Walsh Transform Representations over Both Vector Spaces and Finite Fields*

Conditions	**Walsh Transform (λ)**
$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$	$\lambda_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}$, $a \in \mathbb{F}_2^n, \quad b \in \mathbb{F}_2^m \setminus \{0\}$
$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$	$\lambda_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_m(bF(x)) + \mathrm{tr}_n(ax)}$, $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*$
$f : \mathbb{F}_2^n \to \mathbb{F}_2$	$\lambda_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + a \cdot x}$, $a \in \mathbb{F}_2^n$
$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$	$\lambda_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{tr}_n(ax)}$, $a \in \mathbb{F}_{2^n}$
n even, $f : \mathbb{F}_{2^{\frac{n}{2}}} \times \mathbb{F}_{2^{\frac{n}{2}}} \to \mathbb{F}_2$	$\lambda_f(a,a') = \sum_{x,y \in \mathbb{F}_{2^{n/2}}} (-1)^{f(x,y) + \mathrm{tr}_{n/2}(ax + a'y)}$, $a, a' \in \mathbb{F}_{2^{n/2}}$

The *Walsh coefficients* of an (n,m)-function F are the values of its Walsh transform $\lambda_F(a,b)$ for all possible values of a and b with $b \neq 0$.

An important characteristic of any given function F is its *Walsh spectrum*, which is the multiset Λ_F of all of its Walsh coefficients.

Using the multiset notation introduced earlier, we can write the Walsh spectrum of F as

$$\Lambda_F = \{* \ \lambda_F(a,b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^* \ *\}.$$

A closely related notion is that of the *extended Walsh spectrum*, which is simply the multiset of all the absolute values of the Walsh coefficients of F, i.e.,

$$\Lambda'_F = \{* \ |\lambda_F(a,b)| : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^* \ *\}.$$

The motivation for the definition of the extended Walsh spectrum is that it remains invariant under, e.g., CCZ-equivalence whereas the Walsh spectrum, in general, does not. An important practical application of invariant properties is that they often allow us to quickly disprove that two given functions belong to the same equivalence class.

Similarly to how the support of a Boolean function is defined as the set of all elements that it maps to non-zero values, we can define the *Walsh support* of an (n,m)-function F as the set of all pairs (a,b) for which the Walsh transform evaluates to a non-zero value, i.e., the set

$$\{(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^* : \lambda_F(a,b) \neq 0\}.$$

The Walsh support is used in the investigation of certain properties of vectorial Boolean functions; see, e.g., [42] where a property of the Walsh support of all highly nonlinear functions is derived.

A large number of useful characterizations can be obtained by investigating the Walsh coefficients and their power moments in particular. Here we present some properties of the Walsh transform which hold for any Boolean function and which are often used in the proofs of such characterizations. A simple identity which is true for any $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the following.

Proposition 1. (See, e.g., [77]) Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an n-dimensional Boolean function. Then

$$\sum_{a \in \mathbb{F}_{2^n}} \lambda_f^2(a) = 2^{2n}. \tag{3}$$

This identity is known as *Parseval's equality* or *Parseval's relation.*

Proof. From the definition of λ_F and the fact that the trace function is balanced over $\mathbb{F}_{2^n}$ we have

$$\begin{aligned} \sum_{a \in \mathbb{F}_{2^n}} \lambda_f^2(a) &= \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(y)} \sum_{a \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n^1(a(x+y))} \\ &= 2^n \sum_{x \in \mathbb{F}_{2^n}} (-1)^0 = 2^{2n} \end{aligned}$$

which is precisely Parseval's relation above. □

Applying (3) to the component functions of an (n, m)-function F, we get

$$\sum_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*} \lambda_F^2(a, b) = 2^{2n}(2^m - 1).$$

A similar result can be obtained for the first moment of the Walsh coefficients as follows.

Proposition 2. (See, e.g., [39]) Let f be an n-dimensional Boolean function. Then

$$\sum_{a \in \mathbb{F}_{2^n}} \lambda_f(a) = 2^n (-1)^{f(0)}.$$

Proof. Using the fact that the trace function is balanced over $\mathbb{F}_{2^n}$, we have

$$\sum_{a \in \mathbb{F}_{2^n}} \lambda_f(x) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} \sum_{a \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(ax)} = 2^n (-1)^{f(0)}$$

which is precisely what we needed to show. □

The definitions related to the Walsh transform of a vectorial Boolean function are summarised in Table 5 below.

Table 5: *Some Terms Related to the Walsh Transform of* (n, m)*-functions*

Term	Representation
Walsh Transform	$\lambda_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot F(x) + a \cdot x}$, $a \in \mathbb{F}_{2^n}, \quad b \in \mathbb{F}_{2^m}^*$
Walsh Coefficient	Specific value of Walsh Transform
Walsh Support	$\{(a,b) : \lambda_F(a,b) \neq 0, a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*\}$
Walsh Spectrum	$\Lambda_F = \{\lambda_F(a,b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*\}$,
Extended Walsh Spectrum	$\Lambda_F' = \{* \, \lvert\lambda_F(a,b)\rvert : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^* \, *\}$

2.2 Properties of Vectorial Boolean Functions and Cryptographic Attacks

Cryptography and cryptanalysis are interrelated and mutually reinforcing disciplines. Cryptography studies methods of encrypting sensitive data so that it cannot be read by an unauthorized listener while being broadcast over an insecure channel. In other words, cryptography is concerned with the design of secure ciphers and encryption algorithms. Encryption and decryption require the knowledge of a secret key (or keys) which should be known only to the legitimate communicating parties. Cryptanalysis then investigates whether and how it is possible to break these ciphers and algorithms so that the encrypted data and the secret keys can be recovered from their output without actually knowing the secret keys. Many encryption algorithms incorporate Boolean functions as part of their design; the security of the resulting cipher is then directly dependent on the properties of the underlying function. Thus, one of the primary purposes of the study of Boolean functions is to identify and construct functions that yield secure ciphers, i.e., ciphers that are not readily susceptible to cryptanalytic attacks. From this perspective, it is useful to examine different types of attacks in detail.

Here we recall the classification of ciphers which we have already discussed in the introduction. Encryption algorithms can be divided into symmetric and asymmetric algorithms. Symmetric algorithms use the same key for both encryption and decryption. Many well-known algorithms, such as DES (Data Encryption Standard), 3DES (Triple-DES) and AES (Advanced Encryption Standard) are all symmetric algorithms. Asymmetric algorithms, on the other hand, use different keys for encryption and decryption. Examples of asymmetric encryption algorithms are RSA (Rivest-Shamir-Adleman) and the ElGamal encryption scheme.

The main advantage of symmetric encryption is that it is much faster than asymmetric encryption. However, a significant drawback is that it needs secure key distribution mechanisms. Optimally, every pair of different users from a given group will have their secret key, which however makes the number of keys required extremely large even for a moderately sized group. Furthermore, symmetric encryption doesn't provide authentication and non-repudiation (more precisely, since both parties possess the same key, it cannot be deduced which party has encrypted a given message; in the case of asymmetric encryption this is possible since the keys are distinct).

Recall that symmetric ciphers can be classified into block ciphers and stream ciphers. For the purposes of this dissertation, we focus on the cryptanalysis of block ciphers. Block ciphers have many different modes of operation which specify how precisely the input is partitioned into blocks and consequently enciphered. The most common modes of operation are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) mode.

Figure 3 illustrates the encryption of a short plaintext message using a simple block cipher in CBC mode. In the diagram, F_k is a vectorial Boolean function depending on the key k, which is used for encrypting the plaintext blocks. The original text "Keep Calm and Finish PhD" is first converted to hexadecimal numbers and then

partitioned into blocks of four bytes. Then each of these blocks is encrypted using the function F_k, which depends on the key k as well as the current block of plaintext and the previously computed ciphertext block (this last detail is particular to CBC mode). Note that when enciphering the first plaintext block, no previously calculated ciphertext blocks are available, so we use a so-called Initialization Vector (IV) instead. After all the plaintext blocks are encrypted, the resulting ciphertext blocks are concatenated and converted from hexadecimal numbers back to text, yielding the encoded message.

In [86], Shannon proposed confusion and diffusion as two essential properties for secure cryptosystems. Confusion involves making the relation between the key and the ciphertext as complicated as possible. Diffusion means that a small change in the input can result in a significant difference in the output.

In 1949, Shannon published the landmark paper "Communication Theory of Secrecy Systems [85]" which ushered in a new era of using information theory to study cryptography and made him the founder and pioneer of modern cryptography. It was praised as having "transformed cryptography from an art to science" by the "Boston Globe" newspaper. In this paper, Shannon gives five criteria that secure cryptosystems should meet; however, he points out that even if one of them is not met, the security of the system can still be guaranteed. These criteria are the following:

(i) a large amount of plaintext demands complex encryption operations. However this is not mandatory for a small amount of plaintext;

(ii) a large key size is needed;

(iii) complex enciphering processes;

(iv) error propagation;

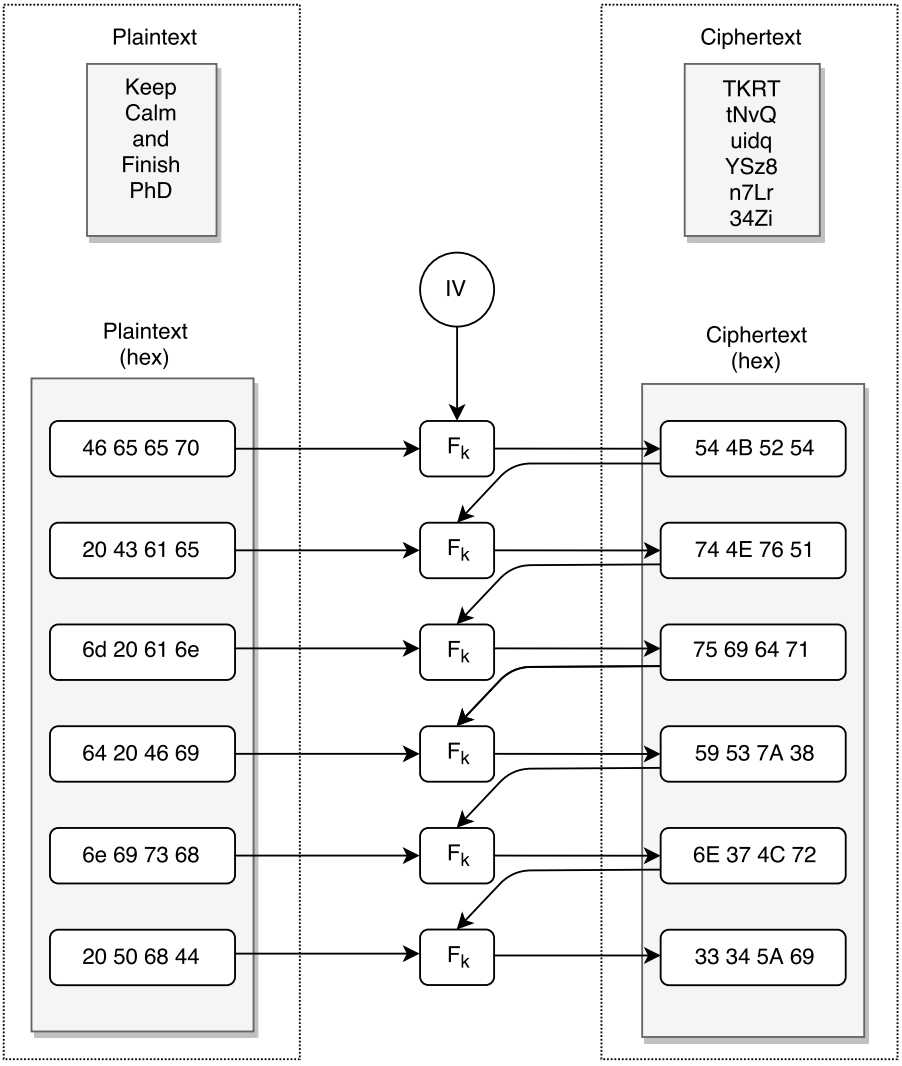


Fig. 3: *Encryption with a Symmetric Block Cipher in CBC Mode*

(v) the message is mixed with some nonsensical data, and then everything is enciphered together so that decryption becomes more difficult.

In order to obtain a complicated enciphering process, Shannon proposes a process called "product encipherment" that uses two operations referred to as substitution and transposition. Substitution replaces the input with other content (providing confusion), and transposition "shuffles" the text (providing diffusion). These two operations are applied alternatingly to encrypt the plaintext, which produces stronger ciphers than those relying on substitution or transposition alone.

The Data Encryption Standard (DES) can be regarded as a typical example of product encipherment. DES is based on an earlier design by Horst Feistel at IBM from the 1970s. Seven years later, it was selected as an official Federal Information Processing Standard (FIPS) in the United States by NIST (National Institute of Standards and Technology). Although DES is no longer considered secure for many applications, it is still interesting to study its design and limitations.

DES functions by running the input data multiple times through so-called Feistel units (forming together a Feistel structure, or Feistel network, which is in fact not exclusive to DES but forms the basis of many different block ciphers). An interesting property of the structure is its symmetry, which ultimately makes encryption and decryption identical (except for the key schedule, which must be reversed for decryption), thereby significantly simplifying the implementation of DES in both hardware and software.

DES operates on blocks of 64 bits, with the key also being 64 bits long; however, eight of the key bits are merely parity check bits so that the effective key size is 56 bits. Within each Feistel unit, the input is split into a left and a right half of 32 bits each; the right half is then copied to the left half of the output, while the left half of the input is XOR-ed with the output of a function depending on the right half of the input and the current key. At the heart of this function are eight

vectorial Boolean functions (called S-boxes, or substitution boxes), each of which replaces part of the input with a different sequence of bits. This is an example of a substitution operation and provides confusion. The other operations in DES provide diffusion. The entire network consists of sixteen such units so that the operation of the Feistel unit is repeated for sixteen rounds.

The differential attack introduced by Biham and Shamir [3] is one of the most efficient cryptanalytical tools that can be used against block ciphers. The differential attack is based on the study of how differences in the input can produce some particular difference in the output with a probability significantly larger or smaller than the uniform one.

Thus, to resist differential attacks, each S-box in the cipher should have the following property: if we run through all pairs of inputs with a fixed non-zero difference between them, the differences between the outputs should be as uniformly distributed as possible.

For a given vectorial Boolean function (or S-box) F, its resistance against differential attacks can be measured by its differential uniformity, which should be as low as possible. Among (n, n)-functions, Almost Perfect Nonlinear (APN) functions provide the best possible resistance against differential attacks [76] (note that despite their name, APN functions are in fact optimal objects). Note that Perfect Nonlinear (PN) functions would theoretically provide even lower differential uniformity, but they exist only under certain special conditions.

Another powerful attack against block ciphers is the linear cryptanalysis introduced by Matsui [73] which is based on finding affine approximations to the action of the cipher. Almost bent (AB) functions are S-boxes providing optimal resistance to this attack [44]. Moreover, every AB function is APN and therefore is optimal against differential attacks as well. However, AB functions exist only over binary fields of odd dimensions while APN functions exist for even dimensions too.

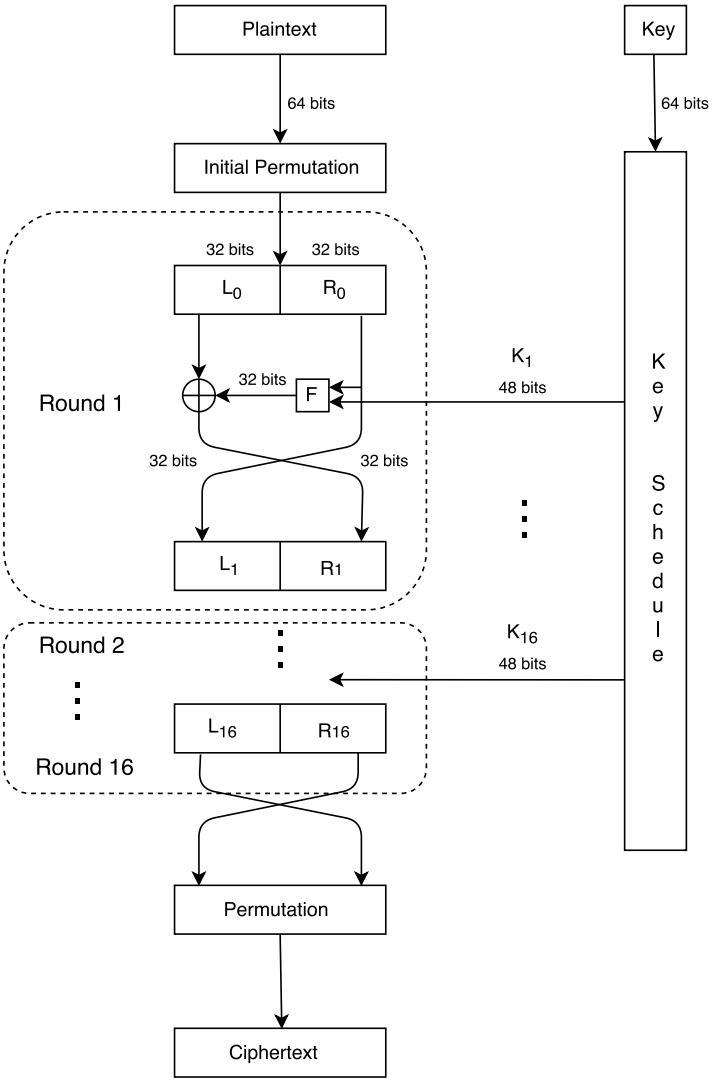


Fig. 4: *Encryption with DES*

More generally, the resistance of a function against linear cryptanalysis is measured by its nonlinearity, which should be as high as possible. The nonlinearity of a function is defined as its distance to the set of all affine functions. As in the case of PN and APN functions above, the functions with the highest possible nonlinearity (called *bent*) exist only under certain conditions, with the slightly weaker AB functions being optimal in the majority of cases.

In the following subsections, we examine some of the most important cryptographic properties of vectorial Boolean functions in more detail.

2.2.1 Nonlinearity

The notion of nonlinearity was introduced as a measurement of the resistance of a function to linear attacks [73]. Higher nonlinearity corresponding to more secure functions [44].

Definition 14. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an n-dimensional Boolean function. Then the *nonlinearity* of f, denoted $\mathcal{NL}(f)$, is the minimum Hamming distance between f and any affine function $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

In the case of a vectorial Boolean function F, the minimum nonlinearity from among all its component functions is taken.

Definition 15. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be an (n, m)-function. Then its *nonlinearity* is defined as

$$\mathcal{NL}(F) = \min_{b \in \mathbb{F}_{2^n}^*} \mathcal{NL}(F_b). \tag{4}$$

As Table 6 shows, if $n = m$ is odd, the highest nonlinearity is achieved by the AB functions and its value is $2^{n-1} - 2^{\frac{n-1}{2}}$. When n is even, the best-known nonlinearity among the monomial infinite families listed in Table 12 is achieved by the Gold and Kasami families.

A very useful observation allows us to express the nonlinearity of a Boolean function in terms of its Walsh coefficients. Since the

nonlinearity of a vectorial Boolean function is expressed via the nonlinearity of its component functions, the result can be easily generalized to the case of vectorial Boolean functions as well.

Proposition 3. [38] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an n-dimensional Boolean function. Then

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\lambda_f(a)|.$$

2.2.2 Differential Uniformity

The differential uniformity of a vectorial Boolean function measures its resistance to differential attacks. Although it may seem that differential uniformity and nonlinearity are two independent properties, they are in fact closely related [4, 44].

Recall that $\Delta_F(a, b)$ is the number of solutions x to the equation $D_a F(x) = b$. The relation between the differential uniformity and the Walsh transform is the following:

Proposition 4. [44, Lemma 3] Let F be an (n, n)-function. Then

$$\sum_{a,b \in \mathbb{F}_{2^n}} \Delta_F(a, b)^2 = \frac{1}{2^{2n}} \sum_{a,b \in \mathbb{F}_2^n} \lambda_F(a, b)^4 \tag{5}$$

or, equivalently,

$$\sum_{\substack{(a,b) \neq (0,0) \\ a,b \in \mathbb{F}_{2^n}}} \Delta_F(a, b)^2 = \frac{1}{2^{2n}} \sum_{\substack{(a,b) \neq (0,0) \\ a,b \in \mathbb{F}_{2^n}}} \lambda_F(a, b)^4, \tag{6}$$

since $\Delta_F(0, 0) = 2^n$, $\lambda_F(0, 0) = 2^n$ and $\lambda_F(a, 0) = 0$ for $a \neq 0$.

2.2.3 Algebraic Degree

The notion of the derivative of a vectorial Boolean function can be generalized to that of a *k-th order derivative* (for a natural number

$k \geqslant 1$) as follows. The first-order derivative of F is simply any derivative of F. Given a $(k-1)$-th order derivative D of F for any $k \geqslant 2$, the derivatives of D itself are the k-th order derivatives of F. The k-th order derivatives for $k \geqslant 2$ are collectively referred to as higher order derivatives. Higher order differential attacks are a generalization of the differential attacks exploiting higher order derivatives instead of (first-order) derivatives [70].

Functions with higher algebraic degrees are preferable in order to resist such as higher order differential attacks. This leads to the problem of finding upper bounds on the algebraic degree of various optimal classes of vectorial Boolean functions, such as APN and AB functions (see Chapter 3) and constructing functions which meet these upper bounds. On the other hand, finding lower and upper bounds on the algebraic degree of, e.g., APN or AB functions also facilitates their construction since candidate functions whose degree lies outside the established bounds can be safely ignored.

2.3 Equivalence Relations

As the dimension of the underlying field increases, the number of Boolean functions (and especially vectorial Boolean functions) defined over it increases astronomically, which makes their study and classification difficult. To make the situation manageable, different equivalence relations are introduced which allow the space of all (vectorial) Boolean functions of a given dimension to be partitioned into equivalence classes. Then we can restrict our attention to only a single representative function from each class. Consequently, when searching for new optimal functions (for some given characteristic), we are in fact looking for functions inequivalent to any of the already known representatives. Any newly constructed function must be checked for equivalence against all the known classes to ascertain that it is truly new and not merely a representative of one of the known equivalence classes.

Two natural equivalence relations are linear equivalence and affine equivalence, which merely involve composing a given function with linear (or affine) permutations from the left and the right.

Definition 16. Let F and F' be (n, m)-functions. We say that they are *linear equivalent* (*affine equivalent*) if there exists a linear (affine) permutation A_1 of $\mathbb{F}_{2^m}$ and a linear (affine) permutation A_2 of $\mathbb{F}_{2^n}$ such that

$$F' = A_1 \circ F \circ A_2.$$

Extended affine equivalence is essentially affine equivalence extended by the addition of an affine function.

Definition 17. Let F and F' be (n, m)-functions. We say that F and F' are *Extended Affine equivalent* (EA-equivalent) if

$$F' = A_1 \circ F \circ A_2 + A,$$

where $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m},\ A_1 : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m},\ A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine functions, and A_1, A_2 are permutations.

Although the two definitions above seem very similar, the two equivalence relations often behave quite differently. For instance, many properties that are invariant under affine equivalence are not invariant under EA-equivalence.

CCZ-equivalence is the most general equivalence relation that we work with and is defined in terms of the graphs of the corresponding functions. The *graph* of an (n, m)-function F is defined as the set $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$.

Definition 18. Let F and F' be two (n, m)-functions. We say that they are *CCZ-equivalent* if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ the image of the graph G_F of F via $\mathcal{L}$ is the graph $G_{F'}$ of F', i.e.,

$$\mathcal{L}(G_F) = G_{F'}.$$

When working with CCZ-equivalence, it is usually easier to consider the affine permutation $\mathcal{L}$ as a pair $\mathcal{L} = (L_1, L_2)$ where $L_1 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ and $L_2 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. If we also define $F_1 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $F_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ as

$$F_1(x) = L_1(x, F(x))$$

$$F_2(x) = L_2(x, F(x))$$

then we have

$$\mathcal{L}(G_F) = \{(F_1(x), F_2(x)) : x \in \mathbb{F}_{2^n}\}.$$

The function F is then CCZ-equivalent to $F' = F_2 \circ F_1^{-1}$.

Just as linear and affine equivalence are special cases of EA-equivalence, EA-equivalence is a special case of CCZ-equivalence [43]. Until 2006, however, it was believed that the CCZ-equivalence of two functions F and F' could be described in terms of EA-equivalence and the inverse of F when F is a permutation. Later it was established that CCZ-equivalence is, in fact, strictly more general than EA-equivalence [17, 29]. Using the representation of $\mathcal{L}$ as the pair $\mathcal{L} = (L_1, L_2)$, we can see more accurately how EA-equivalence is a specific case of CCZ-equivalence. This is shown in the following proposition, and we can also see under what conditions the two equivalences coincide.

Proposition 5. [29, Proposition 3] Let F and F' be two (n, m)-functions. Then F' is EA-equivalent to F or to the inverse of F (if it exists) if and only if there exists a linear permutation $\mathcal{L} = (L_1, L_2)$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that $\mathcal{L}(G_F) = G_{F'}$ and the function L_1 depends only on one variable, i.e., $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.

The relations between the different types of equivalence defined above are illustrated in Figure 5.

Another equivalence relation worth mentioning in the case of power functions is cyclotomic equivalence. Any exponent d with

$0 \leqslant d < 2^n - 1$ of a monomial $F(x) = x^d$ over $\mathbb{F}_{2^n}$ induces an equivalence class (d) of exponents defined as

$$(d) = \begin{cases} \{2^i d, \quad 2^i/d \quad : 0 \leqslant i < n\} & \text{if } x^d \text{ is a permutation} \\ \{2^i d \quad : 0 \leqslant i < n\} & \text{otherwise,} \end{cases}$$

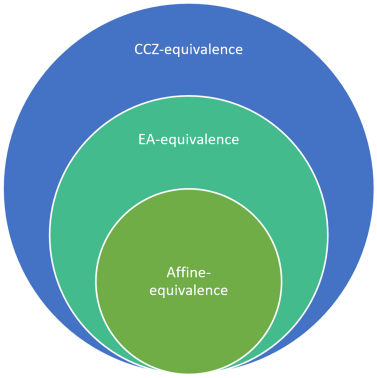


Fig. 5: *Relations Between Affine, EA- and CCZ-equivalence*

i.e., (d) is the union of the 2-cyclotomic cosets of d and $\frac{1}{d}$ modulo $2^n - 1$ if x^d is a permutation, and it is the 2-cyclotomic coset of d modulo $2^n - 1$ otherwise. If d and d' belong to the same equivalence class then we call the monomials x^d and $x^{d'}$ *cyclotomic equivalent.*

As the dimension of the field increases, it gets harder to tell if two given functions are equivalent or not; for this reason, properties which are invariant under different types of equivalence are useful since they allow us to quickly disprove the equivalence of two functions in a lot of cases.

The following properties are invariant under affine equivalence and EA-equivalence:

- nonlinearity;
- differential uniformity;

- algebraic degree;
- extended Walsh spectrum;
- differential spectrum;
- minimum degree (if the minimum degree of F is greater than 1);
- plateauedness (possibly with different amplitudes), and the set of amplitudes in the case that the function is plateaued (see Section 3.3 for the definition of plateaued functions);
- generalized crookedness (see Subsection 3.4.3 for the definition of generalized crooked functions).

The following properties are invariant under CCZ-equivalence:

- nonlinearity [43];
- differential spectrum (hence also differential uniformity);
- extended Walsh spectrum [14];
- the property of being plateaued with single amplitude, and the amplitude itself.

Note that if a function is plateaued with different amplitudes, then the property of being plateaued is not preserved under CCZ-equivalence in general.

The classes of bent, or PN functions (see Section 3.2) and APN and AB functions (see Section 3.4) are defined in terms of their differential uniformity (in the case of PN and APN functions) and nonlinearity (in the case of bent and AB functions). Therefore the property of being bent, PN, APN or AB remains invariant under CCZ-equivalence.

Many other properties, however, such as algebraic degree, minimum degree and the property of being a permutation are not invariant under CCZ-equivalence. In the case of algebraic degree, it is known that every permutation is CCZ-equivalent to its inverse. However, there is no clear relation between the algebraic degree of F and that of F^{-1}. For instance, the functions x^3 and x^{21} are inverses of one another over $\mathbb{F}_{2^5}$ of algebraic degrees 2 and 3, respectively.

Since proving that two functions are CCZ-equivalent is generally harder than proving that they are EA-equivalent, knowing conditions under which the two equivalence relations coincide can be very useful. This happens in the case of:

- Boolean functions [20, 31];
- bent functions [30, 31];
- quadratic APN functions (conjectured by Edel, proved by Yoshiara [95]).

The formal definitions of bent, or PN, and APN functions are given in Sections 3.2 and 3.4 of the next chapter.

In addition, for $n \geqslant 3$, two monomial APN functions are CCZ-equivalent if and only if they are EA-equivalent or one of them is EA-equivalent to the inverse of the other [46, 95, 96].

In general, EA-equivalence and CCZ-equivalence are different for functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ with $m \geqslant 2$ [21, 32, 81].

Budaghyan and Carlet [21] attempted to obtain an equivalence relation more general than CCZ-equivalence using the indicator function of the graph G_F of a function F. This lead to the following alternative characterization of CCZ-equivalence. Recall that the graph G_F of a function F over $\mathbb{F}_{2^n}$ is defined as the set of pairs $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$. Its indicator function is then defined as

$$1_{G_F}(x, y) = \begin{cases} 1 & F(x) = y \\ 0 & F(x) \neq y. \end{cases}$$

Theorem 1. [21, Theorem 1] Let n and m be positive integers and F and F' be two (n, m)-functions. Then F and F' are CCZ-equivalent if and only if the indicators 1_{G_F} and $1_{G_{F'}}$ of their graphs are CCZ-equivalent.

3 APN Functions and Their Subclasses

3.1 Background and Basic Definitions

Recall that nonlinearity measures the resistance of a given function to linear attacks, so that it should preferably be as high as possible. The so-called universal bound can be obtained from Parseval's relation (3) and bounds the nonlinearity of any given vectorial Boolean function from above.

Proposition 6. [18, 44, 87] Let F be any (n, m)-function. Then

$$\mathcal{NL}(F) \leqslant 2^{n-1} - 2^{n/2-1}.$$

This inequality is known as the *universal bound*.

Proof. From Proposition 3 we know that the nonlinearity of the component function F_b satisfies

$$\mathcal{NL}(F_b) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} |\lambda_F(a, b)|.$$

From Parseval's relation (Proposition 1) we have, for any $b \neq 0$,

$$\sum_{a \in \mathbb{F}_{2^n}} \lambda_F^2(a, b) = 2^{2n}$$

which implies

$$\max_{a \in \mathbb{F}_{2^n}} \lambda_F^2(a, b) \geqslant 2^n$$

since we add 2^n Walsh coefficients together. Therefore

$$\max_{a \in \mathbb{F}_{2^n}} |\lambda_F(a, b)| \geqslant 2^{n/2}$$

and hence

$$\mathcal{NL}(F_b) \leqslant 2^{n-1} - 2^{n/2-1}.$$

Since this holds for any component function F_b of F, the bound also applies to the nonlinearity of F itself. □

Functions that achieve this bound with equality are called *bent*; note that the definition is the same for both Boolean and vectorial Boolean functions (although, of course, two different notions of nonlinearity are used). Vectorial bent functions exist only for n even and $m \leqslant n/2$ [76].

Another upper bound on the nonlinearity of an arbitrary vectorial Boolean function is the Sidelnikov-Chabaud-Vaudenay (SCV) bound [44, 87] which is strictly better than the universal bound for $m \geqslant n$. The actual bound is

$$2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - \frac{2(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

As shown in [44], this bound is tight if and only if $m = n$.

The algebraic degree of a Boolean bent function can be bounded from above as follows:

Proposition 7. [39] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function. Then

$$d^\circ(f) \leqslant \frac{n}{2}.$$

3.2 Perfect Nonlinear (PN) Functions

Similarly to how bent functions are defined as optimal with respect to their nonlinearity, the class of Perfect Nonlinear (PN) functions is defined as optimal with respect to their differential uniformity.

More precisely, we say that an (n, m)-function F is *Perfect Nonlinear (PN)* if its differential uniformity is $\Delta_F = 2^{n-m}$. In fact, a function F is bent if and only if it is PN (see, e.g., [16]); thus, these two classes coincide.

However, bent (PN) functions exist only under certain conditions. For instance, in the frequently studied case of $n = m$, bent (PN) functions do not exist since the differential uniformity of any vectorial Boolean function is even. In such cases, the conditions imposed on

the nonlinearity and differential uniformity have to be weakened, and the resulting classes that satisfy these weaker conditions may not necessarily coincide, which is the reason that we keep the notions of PN and bent functions separate.

The following proposition characterizes the class of PN, or bent, functions.

Proposition 8. [39] Let F be an (n, m)-function. Then the following conditions are equivalent:

(i) F is bent;

(ii) F is PN;

(iii) the component function F_c is bent for any nonzero $c \in \mathbb{F}_{2^m}^*$;

(iv) $\lambda_F(a, b) = \pm 2^{\frac{n}{2}}$ for any $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^m}^*$.

Table 6: *Known Optimal Values and Classes for Differential Uniformity and Nonlinearity of (n, m)-functions*

Conditions	Δ_F	**Class**	$\mathcal{NL}(F)$	**Class**
$m \leqslant n/2$	2^{n-m}	PN (bent)	$2^{n-1} - 2^{\frac{n}{2}-1}$	bent (PN)
$n/2 < m < n$	$> 2^{n-m}$	-	$\leqslant 2^{n-1} - \frac{1}{2}\big(3 \cdot 2^n - 2 - \frac{2(2^n-1)(2^{n-1}-1)}{(2^m-1)}\big)^{1/2}$	-
$m = n, n$ *is odd*	2	APN	$2^{n-1} - 2^{\frac{n-1}{2}}$	AB
$m = n, n$ *is even*			$2^{n-1} - 2^{\frac{n}{2}}$ (Conjectured)	maximum nonlinear

More generally, Table 6 gives an overview of the optimal values of the nonlinearity and differential uniformity of vectorial Boolean functions (or the known upper or lower bounds, indicated by inequality signs, in the cases when the exact optimal values are unknown). The classes of functions attaining these optimal values are given as well. In the case of differential uniformity, PN functions (which exist only for $m \leqslant \frac{n}{2}$) attain the optimal value of $\Delta_F = 2^{n-m}$; in all other cases,

the value of Δ_F is strictly higher. In the case of nonlinearity, the bound given for $n/2 < m < n$ from [44] is tight only if $n = m$ and n is odd (this is the class of AB functions). In the case of $m = n$ and n even, the given value is only conjectured to be optimal. All known (n, n)-functions for n even have nonlinearity at most $2^{n-1} - 2^{n/2}$.

Recall that a low differential uniformity Δ_F of a vectorial Boolean function F indicates a high resistance to differential attacks so that we are interested in the construction and properties of functions with as low a value of Δ_F as possible. When considering (n, m)-functions, a particular case of interest is when n and m are equal, i.e., when the domain and codomain of F have the same dimension. Perfect nonlinear functions, which are optimal with respect to differential uniformity, do not exist in this, among other, cases which motivates the definition of the class of Almost Perfect Nonlinear (APN) functions as the class of functions having optimal differential uniformity $\Delta_F = 2$.

3.3 Plateaued Functions

Plateaued functions were first introduced [99] as a class of functions whose Walsh spectrum consists of no more than three values. The class of plateaued functions includes all bent functions (so that the notion of a plateaued function can be understood as a generalization of that of a bent function) as well as all AB functions; the relationship between the class of plateaued functions and that of APN functions is more complicated and is studied, e.g., in [41] (APN and AB functions are defined in Section 3.4 and Subsection 3.4.2 of this chapter). As with the other subclasses of the class of APN functions, the definition of plateuaed functions provides additional structure allowing us to derive more properties and characterizations than in the general case.

Definition 19. An n-dimensional Boolean function f is called *plateaued* if all of the values of its Walsh transform are in the set $\{0, \pm\lambda\}$ for some positive integer λ. The integer λ is called the *amplitude* of f.

The notion of a plateaued function can be naturally generalized to the case of a vectorial function F by requiring that all component functions of F are plateaued. Depending on whether all of the component functions have the same amplitude or not, we obtain two distinct notions.

Definition 20. [39] An (n, m)-function F is called *plateaued* if all of its component functions F_b for $b \neq 0$ are plateaued, with possibly different amplitudes.

Definition 21. [41] An (n, m)-function F is called *plateaued with single amplitude* if all of its component functions are plateaued with the same amplitude.

3.4 APN Functions

APN, or Almost Perfect Nonlinear, functions are defined to be the class of optimal vectorial Boolean (n, n)-functions with respect to differential uniformity.

Definition 22. An (n, n)-function F is called *Almost Perfect Nonlinear (APN)* if its differential uniformity Δ_F is equal to two, i.e., for every $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$ we have

$$|\{x \in \mathbb{F}_{2^n} : D_a F(x) = b\}| \leqslant 2.$$

Each of the following conditions is a necessary and sufficient condition for a function to be APN:

- For any nonzero $a \in \mathbb{F}_{2^n}$, the set

  $$H_a = \{F(x + a) + F(x) : x \in \mathbb{F}_{2^n}\}$$

  contains 2^{n-1} elements;

- For every $(a, b) \neq (0, 0)$, the system

$$\begin{cases} x + y & = & a \\ F(x) + F(y) & = & b \end{cases}$$

  admits 0 or 2 solutions;

- The function $\gamma_F : \mathbb{F}_{2^n}^2 \to \mathbb{F}_2$ has weight $2^{2n-1} - 2^{n-1}$ [43];

- F is not an affine function on any 2-dimensional affine subspace of $\mathbb{F}_2^n$ [61].

The properties of Boolean functions and vectorial Boolean functions have also been investigated from the point of view of coding theory. Although we do not make use of this perspective in our work, we briefly mention some interesting results in this direction. See, e.g, [92] for a general introduction to coding theory, where the notions of a linear code and its parity-check matrix (among other code-theoretic primitives) are defined.

Given a vectorial Boolean function F, the linear code C_F defined by the parity-check matrix.

$$\begin{bmatrix} 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(0) & F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{bmatrix} \tag{7}$$

as well as its extended code $\widetilde{C}_F$ given by the parity-check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(0) & F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{bmatrix}$$

are often useful for investigating the properties of F. A function F is APN if and only if the extended code $\widetilde{C}_F$ has parameters $[2^n, 2^n - 1 - 2n, 6]$ [14]. In the case when $F(0) = 0$, we can use a simpler characterization: F is APN if and only if the code C_F has minimum distance 5 [43].

A number of useful properties and characterizations of APN functions may be obtained by studying the power moments of their Walsh transform.

Tables 7 and 8 summarize the values of the different power moments of the Walsh transform. Although it is straightforward to obtain Table 8 from Table 7, we give both here for the reader's convenience. Note that the first two properties hold for any vectorial Boolean function, while the last two properties apply to APN functions only.

The formal statements of the entries in the table are given in Propositions 1, 2, 9 and 10.

Proposition 9. [44, Lemma 3] Let F be an (n, n)-function. Then F is APN if and only if

$$\sum_{a,b \in \mathbb{F}_{2^n}} {\lambda^4}_F(a, b) = 2^{3n+1}(3 \cdot 2^{n-1} - 1).$$

Proposition 10. [39, Equation 14] Let F be an APN function over $\mathbb{F}_{2^n}$ satisfying $F(0) = 0$. Then

$$\sum_{a,b \in \mathbb{F}_{2^n}} {\lambda^3}_F(a, b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1).$$

In the case of plateaued functions this condition is both necessary and sufficient for F to be APN.

APN functions can also be characterized in terms of the second power moment of their derivatives. Sometimes this leads to simpler expressions than the characterization given above. Note that only Walsh coefficients of the form $\lambda_{D_a F}(0, b)$ are considered in this case, i.e., they are only considered in terms of their second argument.

Proposition 11. [1] An (n, n)-function F is APN if and only if

$$\sum_{b \in \mathbb{F}_{2^n}} \lambda^2_{D_a F}(0, b) = 2^{2n+1}$$

for every derivative direction $a \in \mathbb{F}^*_{2^n}$.

Table 7: *Properties of the Power Moments of the Walsh Transform*

No.	Properties	Valid for
1	$\sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F(a,b) = 2^{2n}$	Any function
2	$\sum_{a,b\in\mathbb{F}_{2^n}} {\lambda^2}_F(a,b) = 2^{3n}$	Any function
3	$\sum_{a,b\in\mathbb{F}_{2^n}} {\lambda^3}_F(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1)$	Necessary condition for being APN, $F(0)=0$
4	$\sum_{a,b\in\mathbb{F}_{2^n}} {\lambda^4}_F(a,b) = 2^{3n+1}(3\cdot 2^{n-1}-1)$	Necessary and sufficient condition for being APN

Table 8: *Properties of APN's Walsh Transform*

No.	Properties	Valid for
1	$\sum_{a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^n}^*} \lambda_F(a,b) = 2^n(2^n-1)$	Any function
2	$\sum_{a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^n}^*} {\lambda^2}_F(a,b) = 2^{2n}(2^n-1)$	Any function
3	$\sum_{a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^n}^*} {\lambda^3}_F(a,b) = 2^{2n+1}(2^n-1)$	Necessary condition for being APN, $F(0)=0$
4	$\sum_{a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^n}^*} {\lambda^4}_F(a,b) = 2^{3n+1}(2^n-1)$	Necessary and sufficient condition for being APN

3.4.1 Properties of APN Functions

3.4.1.1 Walsh Transform of APN Functions

Recall that the power moments of the Walsh transform are very useful characteristics; see, e.g., Table 7 or Proposition 11. Besides the values that the Walsh transform can take, their frequencies are of interest as well. Here we show how the frequencies of the Walsh transform can be computed.

When n is even, the functions from the Gold family as well as the Gold-like functions (that is, those functions whose Walsh spectrum is the same as that of the Gold functions) are APN with a Walsh spectrum consisting of the five values $0, 2^{\frac{n}{2}}, -2^{\frac{n}{2}}, 2^{\frac{n+2}{2}}, -2^{\frac{n+2}{2}}$. Suppose the frequencies of these values are x_0, x_1, x_2,x_3 and x_4, respectively. Then by simple mechanical computations using the properties from Tables 7 and 8 we can obtain the following equations:

$$\begin{cases} x_0 + x_1 + x_2 + x_3 + x_4 = 2^{2n} - 1; \\ \sum\limits_{a,b \in \mathbb{F}_{2^n}} \lambda_F(a,b) = 2^{2n} = 2^n + 2^{\frac{n}{2}} x_1 - 2^{\frac{n}{2}} x_2 + \\ \qquad\qquad 2^{\frac{n+2}{2}} x_3 - 2^{\frac{n+2}{2}} x_4; \\ \sum\limits_{a,b \in \mathbb{F}_{2^n}} {\lambda^2}_F(a,b) = 2^{3n} = 2^{2n} + 2^n x_1 + 2^n x_2 + \\ \qquad\qquad 2^{n+2} x_3 + 2^{n+2} x_4; \\ \sum\limits_{a,b \in \mathbb{F}_{2^n}} {\lambda^3}_F(a,b) = 3 \cdot 2^{3n} - 2 \cdot 2^{2n} = 2^{3n} + 2^{\frac{3n}{2}} x_1 - \\ \qquad\qquad 2^{\frac{3n}{2}} x_2 + 2^{\frac{3(n+2)}{2}} x_3 - 2^{\frac{3(n+2)}{2}} x_4; \\ \sum\limits_{a,b \in \mathbb{F}_{2^n}} {\lambda^4}_F(a,b) = 3 \cdot 2^{4n} - 2 \cdot 2^{3n} = 2^{4n} + 2^{2n} x_1 + \\ \qquad\qquad 2^{2n} x_2 + 2^{2n+4} x_3 + 2^{2n+4} x_4. \end{cases}$$

By solving the above system of equations, we can obtain the values of x_0, x_1, x_2, x_3 and x_4. Table 9 lists the Walsh spectra of different functions and their corresponding frequencies.

Note that when $a = b = 0$, the corresponding Walsh coefficient is $\lambda_F(0,0) = 2^n$, so the frequency is 1. Thus this specific case is generally overlooked when describing Walsh spectra.

Table 9: *Some Functions' Walsh Spectra and Their Frequencies (under the Assumption $F(0) = 0$)*

Condition	Functions	Walsh Spectra	Frequencies	Ref.
$m \leqslant n/2$	bent	$2^{\frac{n}{2}}$	$2^{n-1} + 2^{\frac{n}{2}-1}$	[36]
		$-2^{\frac{n}{2}}$	$2^{n-1} - 2^{\frac{n}{2}-1}$	
$m = n$, n is odd	AB	0	$2^n - 2^{n-1}$	[36] [55]
		$2^{\frac{n+1}{2}}$	$2^{n-3} + 2^{\frac{n-3}{2}}$	
		$-2^{\frac{n+1}{2}}$	$2^{n-3} + 2^{\frac{n-3}{2}}$	
	Inverse ($n \neq 3$)	Any value divisible by 4 in $[-2^{\frac{n}{2}+1} + 1, 2^{\frac{n}{2}+1} + 1]$	unknown	[39]
	Dobbertin	Divisible by $2^{\frac{n}{5}}$, NOT divisible by $2^{\frac{2n}{5}+1}$	unknown	[35]
$m = n$, n is even	Gold	0	$(2^n - 1)(2^{n-2} + 1)$	[65]
		$2^{\frac{n}{2}}$	$\frac{1}{3}(2^n - 1)(2^n + 2^{\frac{n}{2}})$	
		$-2^{\frac{n}{2}}$	$\frac{1}{3}(2^n - 1)(2^n - 2^{\frac{n}{2}})$	
		$2^{\frac{n+2}{2}}$	$\frac{1}{12}(2^n - 1)(2^{n-1} + 2^{\frac{n}{2}})$	
		$-2^{\frac{n+2}{2}}$	$\frac{1}{12}(2^n - 1)(2^{n-1} - 2^{\frac{n}{2}})$	
	Dobbertin	Same as n is odd	unknown	[35]

3.4.1.2 Nonlinearity

The nonlinearity of a vectorial Boolean function is a critical indicator of its cryptographic strength as it measures the function's resistance to linear attacks, with higher values of the nonlinearity corresponding to more secure functions. This makes upper and lower bounds on its value for different classes of functions (including APN functions) important from a practical as well as purely theoretical point of view.

We know that an APN function cannot have nonlinearity 0 [39]. In [40], Carlet gives the following additional results:

Proposition 12. [40] Let F be an APN function over $\mathbb{F}_{2^n}$ for $n > 2$. For every two real numbers a and b such that $a \leqslant b$, let $N_{a,b}$ be the number of ordered pairs $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^*$ such that $\lambda_F(u, v) \in [2^n + a, 2^n + b]$. Then the nonlinearity of F is lower bounded by

$$2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{1}{2}(b + a + \sqrt{\Delta_{a,b}})},$$

where $\Delta_{a,b} = (N_{a,b}+1)(b-a)^2 + ab2^{n+2}(2^n-1) + 2^{4n+2} - 2^{3n+2}$.

Corollary 1. [40, Theorem 5.8] Let F be an APN function and let b be a positive number. If $\lambda_F^2(u,v)$ is not in the range $[2^n - \frac{2^{2n}}{b}; 2^n + b]$ for any $u \in \mathbb{F}_{2^n}$ and $v \in \mathbb{F}_{2^n}^*$, then the nonlinearity of F is lower bounded by $2^{n-1} - \frac{1}{2}\sqrt{2^n + b}$.

Recently, Carlet improved these results in the case of APN monomials as follows:

Theorem 2. [42] Let F be any APN power function over $\mathbb{F}_{2^n}$. Then, if n is odd, we have $\mathcal{NL}(F) \geqslant 2^{n-1} - 2^{\frac{3n-3}{4}}$ and if n is even, we have $\mathcal{NL}(F) \geqslant 2^{n-1} - 2^{\frac{3n-2}{4}}$.

Recall that the universal bound (Proposition 6) states that any (n,n)-function F has nonlinearity

$$NL(F) \leqslant 2^{n-1} - 2^{\frac{n-1}{2}}.$$

This bound is achieved when n is odd by the AB functions. The exact upper bound on the nonlinearity over $\mathbb{F}_{2^n}$ for n even is still an open problem.

3.4.1.3 Algebraic Degree

An exact upper bound on the algebraic degree of APN functions is not yet known. In the case of fields $\mathbb{F}_{2^n}$ of odd dimension, the highest known algebraic degree among the known APN functions is $n-1$ and is attained by the inverse APN functions [75]. In the case of fields $\mathbb{F}_{2^n}$ of even dimension, the currently known APN functions of highest algebraic degree are the Dobbertin functions for dimensions n divisible by 5 with exponent given as

$$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$$

which have algebraic degree $n/5 + 3$ [50], along with the Kasami functions with exponent

$$2^{2i} - 2^i + 1$$

which have algebraic degree $i + 1$ for $i \leqslant (n-1)/2$, $\gcd(n, i) = 1$ [66]; refer to Table 12 for the precise definitions of the Dobbertin and Kasami functions and the conditions on i and n under which these functions are APN.

We denote by $dh_{APN}(n)$ the highest algebraic degree among the known APN functions over $\mathbb{F}_{2^n}$. The currently established values of $dh_{APN}(n)$ are given in Table 10.

An overview of some of the known infinite APN families (including all known monomial APN families) along with their respective algebraic degrees can be found in Table 11.

3.4.2 AB Functions

Similarly to how APN functions are defined as a sort of "weaker" analog of PN functions, AB functions are defined as a "weakening" of bent functions i.a. in the case when $n = m$.

AB functions have nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$. They form a strict subclass of the class of APN functions, i.e., every AB function is APN, but the converse is not true in general.

Table 10: *Highest Algebraic Degree of the Known APN Functions on* $\mathbb{F}_{2^n}$

Conditions	$dh_{APN}(n)$	**Functions**
$n = 4$	3	Budaghyan-Carlet-Pott [29, Theorem 2]
$n = 6$	4	Budaghyan-Carlet-Pott [29, Theorem 3]
$\gcd(n, 2) = 1$	$n - 1$	Inverse
$\gcd(n, 4) = 4$ and $n \geqslant 8$	$\frac{n}{2}$	Kasami
$n = 10$	5	Dobbertin
$\gcd(n, 4) = 2$ and $n \geqslant 12$	$\frac{n}{2} - 1$	Kasami

Table 11: *Algebraic Degree and Nonlinearity of Some APN Functions on* $\mathbb{F}_{2^n}$

Functions	d°	$\mathcal{NL}$
Known infinite families of APN polynomials	2	Gold-like
$x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{tr_n}(x^{2^i+1})$, $n \geqslant 4$, n even [29, Theorem 2]	3	Gold-like
$[x + \mathrm{tr}_n^3(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{tr}_n(x)\mathrm{tr}_n^3(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1}$, $6\vert n$ $gcd(i,n) = 1$ [29, Theorem 3]	4	Gold-like
$x^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + x^{2^i}\mathrm{tr}_n^m(x) + x\mathrm{tr}_n^m(x)^{2^i}$ $+[\mathrm{tr}_n^m(x)^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + \mathrm{tr}_n^m(x)]^{\frac{1}{2^i+1}}(x^{2^i} + \mathrm{tr}_n^m(x)^{2^i} + 1)$ $+[\mathrm{tr}_n^m(x)^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + \mathrm{tr}_n^m(x)]^{\frac{2^i}{2^i+1}}(x + \mathrm{tr}_n^m(x))$, $m \neq n$, n odd, $m\vert n$, $gcd(i,n) = 1$ [29, Theorem 4]	$m+2$	Gold-like

It should be noted that under certain conditions the classes of APN and AB functions do coincide. In particular, for n odd, an APN function F is AB if and only if one of the following conditions is satisfied:

(i) all Walsh coefficients of F are divisible by $2^{\frac{n+1}{2}}$;

(ii) for any $c \in \mathbb{F}_{2^n}^*$, the Boolean function $c \cdot F$ is plateaued.

In particular, every quadratic APN function is AB when n is odd [43].

While the problem of an upper bound on the algebraic degree is is still open for APN functions, it is already wholly settled for AB functions. The algebraic degree of any AB function over $\mathbb{F}_{2^n}$ is upper bounded by $\frac{n+1}{2}$ [43] and the inverses of the Gold power functions attain this algebraic degree [43, 75]. Refer to Table 12 for the definition of the Gold functions. Note that any APN power function over a field of odd dimension is a permutation and hence has an inverse.

Each of the following is a necessary and sufficient condition for a function to be AB:

- For every $(a, b) \neq (0, 0)$, the system

$$\begin{cases} x + y + z & = & a \\ F(x) + F(y) + F(z) & = & b \end{cases}$$

  admits $3 \cdot 2^n - 2$ solutions if $b = F(a)$ and $2^n - 2$ otherwise [93];

- The function $\gamma_F : \mathbb{F}_{2^n}^2 \to \mathbb{F}_2$ is bent.

It is worth mentioning that the AB functions can be characterized in terms of the dual code of the linear code C_F defined in (7). Since the actual characterization is significantly more technical than in the case of APN functions, we do not present it here, but instead refer the reader to [43] for details.

3.4.3 Crooked Functions

Recall that an APN function F is defined as having differential uniformity Δ_F equal to two; equivalently, we can say that F is APN if and only if all of its derivatives $D_a F$ for $a \neq 0$ are 2-to-1 functions, which then implies that the image set of every such derivative must have precisely 2^{n-1} elements. However, the definition does not say anything about the structure and properties of those image sets, which naturally leads to the investigation of classes of functions whose differential sets have some given properties. Two such classes are the crooked functions and generalized crooked functions.

In order to define them, we first need the notion of an affine hyperplane, which we now recall. Consider the finite field $\mathbb{F}_{2^n}$. We say that the set

$$H(a, b) = \{x \in \mathbb{F}_{2^n} : \mathrm{tr}_n(ax) = b\}$$

is an *affine hyperplane* for any $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$. If in addition $b = 0$, then for any $a \in \mathbb{F}_{2^n}$ the set $H(a, 0)$ is called a *hyperplane*. Since

clearly $H(a,0) \cup H(a,1) = \mathbb{F}_{2^n}$, the sets $H(a,1)$ are simply referred to as complements of hyperplanes. Note that every affine hyperplane contains precisely 2^{n-1} elements due to the trace function being balanced.

We now proceed to the definitions of the crooked and generalized crooked functions.

Definition 23. An (n,n)-function F is called *crooked* if it satisfies all of the following conditions:

(i) $F(0) = 0$;

(ii) for any three distinct elements $x, y, z \in \mathbb{F}_{2^n}$ we have

$$F(x) + F(y) + F(z) + F(x+y+z) \neq 0;$$

(iii) for any $a \neq 0$ and any $x, y, z \in \mathbb{F}_{2^n}$ we have

$$F(x) + F(y) + F(z) + F(a+x) + F(a+y) + F(a+z) \neq 0.$$

Crooked functions have the following properties:

(i) Crookedness is invariant under affine equivalence, but is not invariant under EA- or CCZ-equivalence;

(ii) If F is a crooked function, then it is a bijection;

(iii) F is crooked if and only if the image sets H_a of its derivatives are all distinct and every complement of a hyperplane appears among them exactly once;

(iv) Any crooked function is AB.

The upper bound on the algebraic degree of crooked functions is $\frac{n-1}{2}$. This is strictly better than the upper bound for AB functions.

One natural way to extend the class of crooked functions is to allow the differential sets to be arbitrary affine hyperplanes (instead of only complements of hyperplanes). This leads to the notion of generalized crooked functions.

Definition 24. A function F is called *generalized crooked* if for any $a \in \mathbb{F}_{2^n}^*$, the set $H_a = \{D_aF(x) : x \in \mathbb{F}_{2^n}\}$ is an affine hyperplane.

The Gold functions x^{2^i+1} are the only power generalized crooked functions [68].

Generalized crooked functions have the following properties:

- Every quadratic APN function is generalized crooked. It is conjectured that every generalized crooked function is quadratic [67];
- A function F is *generalized crooked* if and only if the function $\gamma_F(a, b)$ is affine with respect to b [24];
- Every crooked function is generalized crooked, but the converse is not true in general.

It can be easily seen from the definitions that the crooked and generalized crooked functions form subclasses of the class of APN functions since any derivative of such a function must necessarily be a 2-to-1 mapping.

3.4.4 Known APN Functions

In general, the construction of APN functions that are inequivalent to the known ones is a difficult problem. In particular, once a potentially new APN function is constructed, it needs to be compared for equivalence against all the known classes. For this reason, it is useful to have a systematic overview of these known classes. In the following, we categorize the known APN functions into infinite families, an APN permutation of dimension six, and some sporadic APN functions.

See also Section 4.5 and Table 24 in which we list CCZ-inequivalent representatives from all known APN polynomial families over $\mathbb{F}_{2^n}$ for $6 \leqslant n \leqslant 11$. This is part of our original work and greatly facilitates the comparison procedure in practice.

It is worth mentioning that the majority of the known APN functions are either monomials or plateaued. Furthermore, all of the known infinite APN families are CCZ-equivalent to quadratic APN functions or to APN monomials, which makes the study of these classes particularly attractive. However, there exist APN functions that are CCZ-inequivalent to both monomials and quadratic functions: for instance, the function given by the polynomial

$$x^3 + w^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \mathrm{tr}_2(x^{21}) + \mathrm{tr}_3(w^{18}x^9) + \\ w^{14}\mathrm{tr}_6(w^{52}x^3 + w^6x^5 + w^{19}x^7 + w^{28}x^{11} + w^2x^{13})$$

over $\mathbb{F}_{2^6}$ (proved in [53] and originally constructed in [13]) is the only known example. Here w is a primitive root of $x^6 + x^4 + x^3 + x + 1$.

For dimensions $n \leqslant 5$, APN functions have been completely classified up to CCZ-equivalence [13]; in fact, all such APN functions are CCZ-equivalent to APN power functions. For dimensions, $n \geqslant 6$, the classification of APN functions is still an open problem. So far, there are only 17 known infinite families of APN functions, as well as some sporadic APN functions that have not been generalized into infinite families yet. Among the 17 infinite families, six are monomial APN families, and the others are polynomial APN families. It has been conjectured that classification of monomial APN functions is already complete up to CCZ-equivalence [49].

3.4.4.1 Infinite Families of APN Functions

Six infinite monomial APN and eleven polynomial APN families have been found so far. All the infinite polynomial families are quadratic and they have Gold-like Walsh spectra (that is, they have the same Walsh spectra as the Gold family of monomial functions). However, not all quadratic APN functions have Gold-like Walsh spectra; for example, some sporadic quadratic APN functions can have a 7-valued Walsh spectrum. The function defined in (8) below is one such example.

Monomials Table 12 summarizes the known infinite families of power APN functions. In the case of the Gold and Kasami families, the conditions given in the table can be restricted to $\gcd(i,n) = 1, 1 \leqslant i \leqslant \frac{n-1}{2}$ without loss of generality. This is because the functions that are obtained for $\gcd(i,n) = 1, i > \frac{n-1}{2}$ are EA-equivalent to the ones for $\gcd(i,n) = 1, i \leqslant \frac{n-1}{2}$.

The next-to-last column of Table 12 gives the conditions under which the respective families are AB; note that some of the families (Inverse and Dobbertin) can never be AB.

Yoshiara [96] found that two APN monomials x^d and x^e are CCZ-equivalent if and only if they are cyclotomic equivalent. Previously Budaghyan, Carlet and Leander [23] studied the relations between infinite families of APN monomials up to CCZ-equivalence. They found that any two Gold functions x^{2^i+1} and x^{2^j+1} with $1 \leqslant i, j < n/2$, $i \neq j$ are CCZ-inequivalent to one another and showed that no Gold function can be CCZ-equivalent to a Kasami or Welch function. Furthermore, they showed that the Inverse and Dobbertin functions are CCZ-inequivalent to one another and to all the other known power APN functions.

Table 12: *Known APN Monomials* x^d *over* $\mathbb{F}_{2^n}$

Family	d	Conditions	d°	AB	Ref.
Gold	2^i+1	$\gcd(i,n)=1$	2	n odd	[55, 75]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$0<i<\frac{n}{2}: i+1$ $\frac{n}{2}<i<n: n-i+1$	n odd	[64, 66]
Welch	2^t+3	$n=2t+1$	3	always	[50]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	$\frac{n+3}{4}$ $\frac{n+1}{2}$	always	[49]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	never	[2, 75]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$\frac{n}{5}+3$	never	[48]

The multiplicative inverse function x^{-1} which is studied in [75], is APN when n is odd and its differential uniformity is 4 when n is even. Partly because of its low differential uniformity, it is used as part of the S-box in AES [45].

Recall that according to Yoshiara's results mentioned above, checking whether a power APN function x^d is CCZ-equivalent to one of the known power functions is reduced to testing cyclotomic equivalence for x^d and $x^{d^{-1}}$. Table 26 lists all APN functions from the infinite monomial families and their inverses for odd dimensions $3 \leqslant n \leqslant 129$. A more detailed description is given in Section 4.6.

Polynomials While the history of the infinite monomial APN families goes back all the way to papers from the late 1960s and early 1970s, e.g., [55, 66], the first infinite polynomial APN family was only constructed in 2006 [22, 29].

So far, 11 infinite APN polynomial families are known and all of them contain functions that are CCZ-inequivalent to power functions. These are described in Table 13. It is worth mentioning that the first two APN functions inequivalent to APN monomials to be discovered were two binomials of the form

$$x^3 + ux^{36}$$

over $\mathbb{F}_{2^{10}}$ and

$$x^3 + ux^{528}$$

over $\mathbb{F}_{2^{12}}$ from [52] (with the element u in both cases satisfying some particular conditions; see Theorems 2 and 3 in [52] for details). These early examples inspired Budaghyan and her colleagues [22, 29] who made a breakthrough by finding the first two infinite APN polynomial families that are listed as No. 1 and No. 2 in Table 13. These also provided the first family of AB polynomials, which demonstrated the existence of AB polynomials CCZ-inequivalent to power functions.

Following the work in [22, 29], researchers proceeded to further study this direction. Meanwhile, Dillon independently discovered

several new APN functions over $\mathbb{F}_{2^6}$ [14]. Motivated by Dillon's work, Budaghyan and Carlet found families No. 3 and No. 4 later.

It is worth mentioning the functions with 7-valued Walsh spectra among the above results. The function

$$x^3 + w^{11}x^5 + w^{13}x^9 + x^{17} + w^{11}x^{33} + x^{48} \tag{8}$$

(where w is a primitive element of $\mathbb{F}_{2^n}$ defined by the polynomial $x^6 + x^4 + x^3 + x + 1$), due to Dillon [14], is quadratic and its Walsh spectrum consists of the seven values

$$\{-32, -16, -8, 0, 8, 16, 32\}$$

which can also be written as

$$\{-2^{n-1}, -2^{\frac{n+2}{2}}, -2^{\frac{n}{2}}, 0, 2^{\frac{n}{2}}, 2^{\frac{n+2}{2}}, 2^{n-1}\}.$$

In other words, it has two more values (32 and -32) than the Walsh spectrum of a Gold function for even n.

Budaghyan and Carlet introduced family No.4 in [19]. The property of this class of functions being APN is in fact a corollary of the following more general result.

Theorem 3. [19, Theorem 2] Let m and i be positive integers, $q = 2^m$, $n = 2m$, $gcd(i, m) = k$, and c,$s \in \mathbb{F}_{2^n}$ be such that $s \notin \mathbb{F}_q$. If the equation

$$x^{2^i+1} + cx^{2^i} + c^q x + 1 = 0$$

has no solution x with $x^{q+1} = 1$ and, in particular, if the polynomial $x^{2^i+1} + cx^{2^i} + c^q x + 1$ is irreducible over $\mathbb{F}_{2^n}$, then all the nonzero derivatives of the function

$$F(x) = x(x^{2^i} + x^q + cx^{2^i q}) + x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q} \tag{9}$$

are 2^k-to-1 mappings over $\mathbb{F}_{2^n}$.

When $k = 1$, functions of the form (9) are APN and are called Budaghyan-Carlet APN hexanomials. Bluher [5] was the first one to prove the existence of an APN hexanomial of this form. Bracken, Tan, and Tan [11] studied the specific case when k is even with $3 \nmid k$ and explicitly gave some examples of c and s in that form. This result indirectly proved the existence of Budaghyan-Carlet APN hexanomials for $m \equiv 2 \pmod 6$ or $m \equiv 4 \pmod 6$. The precise result is as follows.

Theorem 4. [11, Theorem 3.4] Let i and k be integers and $n = 2k$ such that $gcd(i, n) = 1$ and $3 \nmid k$. Denote $q = 2^k$ and $Q = q^2$. Let $s \in \mathbb{F}_Q \setminus F_q$ and let ω be a generator of $\mathbb{F}_{2^4}$ in $\mathbb{F}_Q$. Furthermore, let β and γ be elements of $\mathbb{F}_Q$ such that $\gamma^{2^i+1} + \omega\beta^{2^i+1} + 1 = 0$ with $\gamma^{q-1} \neq \beta^{q-1}$. Then the function

$$F(x) = x(x^{2^i} + x^q + cx^{2^i q}) + x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q},$$

where $c = \omega\beta^{q+2^i} + \gamma^{q+2^i}$, is APN over $\mathbb{F}_{2^n}$.

Qu, Tan and Li [82] also presented more explicit conditions on the coefficients c and s when m is even. As shown in [82], for every non-cube $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, the two equations

$$x^{2^i+1} = (1 + s^{-1})^{1-2^m} \tag{10}$$

and

$$y^{2^i+1} = (1 + s)^{1-2^m} \tag{11}$$

have exactly one solution x and y, respectively, such that $x^{2^i+1} = y^{2^i+1} = 1$. In the following we denote these unique solutions by s_1 and s_2.

Theorem 5. [82, Theorem 1] Let $n = 2m$ for m even and let i be a positive integer with $gcd(n, i) = 1$. For each non-cube $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, the polynomial G defined by

$$G(x) = x^{2^i+1} + cx^{2^i} + c^{2^m}x + 1$$

has no zeros over $\mathbb{F}_{2^n}$, where

$$c = \frac{ss_1 + s_2}{s+1}$$

and s_1 and s_2 are the unique solutions to equations (10) and (11) satisfying ${s_1}^{2^i+1} = {s_2}^{2^i+1} = 1$.

Göloğlu [57] attempted to find all possible values for the coefficient c for each pair (i, m) without assuming the condition $\gcd(i, m) = 1$. His results, however, are not very explicit and are much more complicated.

The construction of family No.5 is inspired by the fact that the function $F(x) + tr_n(G(x))$ is differentially 4-uniform for any APN function F and any function G; furthermore, family No. 5 is the only APN polynomial CCZ-inequivalent to monomials for every dimension and for every choice of parameters.

Families Nos. 5, 6, 7 are all of the form $L_1(x^3) + L_2(x^9)$, with L_1 and L_2 being linear functions over $\mathbb{F}_{2^n}$. For n even, if $L_1(x) + L_2(x^3)$ is a permutation then $L_1(x^3) + L_2(x^9)$ is APN [28]. In addition, for $n = 8$, the function $x^9 + \mathrm{tr}_n(x^3)$ is APN and CCZ-inequivalent to monomials and to $x^3 + \mathrm{tr}_n(x^9)$ [27].

Families Nos. 8, 9 and 10 were constructed by Carl Bracken and his colleagues [10].

It is worth noting that family No. 11 from Table 13 was originally given as

$$\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{k+s}+2^k} + \beta x^{2^k+1} + \sum_{i=1}^{k-1} \gamma_i x^{2^{k+i}+2^i}$$

under the conditions $n = 2k$, $\gcd(s, k) = 1$, s,k odd, $\beta \notin \mathbb{F}_{2^k}$, $\gamma_i \in \mathbb{F}_{2^k}$, α not a cube. However, Lilya Budaghyan, Marco Calderini and Irene Villa proved that this family is EA-equivalent to family No.3 from the same table (personal communication).

Table 13: *Known Classes of Quadratic APN Polynomials CCZ-inequivalent to APN Monomials over* $\mathbb{F}_{2^n}$

No.	Functions*	Conditions
1-2 [26]	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $p \in \{3, 4\}$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, $i = sk \bmod p$, $m = p - i$, $n \geqslant 12$
3 [19]	$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $cb^q + b \neq 0$, $\gcd(i, m) = 1$, $\gcd(2^i + 1, q + 1) \neq 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $c^{q+1} = 1$
4 [19]	$x(x^{2^i} + x^q + cx^{2^iq}) + x^{2^i}(c^qx^q + sx^{2^iq}) + x^{(2^i+1)q}$	$q = 2^m, n = 2m$, $\gcd(i, m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \backslash \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ is irreducible over $\mathbb{F}_{2^n}$
5 [27, 28]	$x^3 + a^{-1}\mathrm{tr}_n(a^3x^9)$	$a \neq 0$
6 [28]	$x^3 + a^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$
7 [28]	$x^3 + a^{-1}\mathrm{tr}_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$
8-10 [10]	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}, x^{2^s+2^{k+s}}$	$n = 3k$, $3\|(k + s)$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, $v, w \in \mathbb{F}_{2^k}, vw \neq 1$
11 [100]	$(x + x^{2^m})^{2^k+1} + u^{(2^n-1)/(2^m-1)}(ux + u^{2^m}x^{2^m})^{(2^k+1)2^i} + u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$m \geqslant 2$, $2\|m$, $n = 2m$, $\gcd(k, m) = 1$, i is even

* : u is primitive in $\mathbb{F}_{2^n}^*$

As can be seen from Table 13, all known infinite polynomial families of APN functions consist of quadratic functions. Furthermore, in the case when n is odd, they are all AB functions. However, their CCZ-equivalence classes may include functions whose algebraic degree

is higher than two (recall that CCZ-equivalence does not preserve algebraic degree in general).

Table 11 presents two particular examples of non-quadratic APN polynomials which are CCZ-equivalent but EA-inequivalent to the Gold functions.

3.4.4.2 APN Permutations

Trying to find APN permutations is a topic that is appealing from both a cryptographic and a purely mathematical point of view. For substitution-based ciphers such as AES, the S-boxes, i.e., the underlying vectorial Boolean functions, must be permutations.

Although searching for such functions is a difficult problem in general, the assumption that the functions are permutations provides additional insight into their structure from which useful properties and characterizations may be derived. For instance:

- over fields of even dimension, APN permutations cannot be quadratic [34];
- APN monomials are permutations over $\mathbb{F}_{2^n}^*$ if n is odd and are three-to-one if n is even [49];
- if F is a permutation over $\mathbb{F}_{2^n}$, then $d^\circ(F^{-1})$ equals $n-1$ if and only if $d^\circ(F) = n-1$ [7].

When n is odd, all APN functions from the known infinite monomial families are permutations. However, when n is even, it is extremely challenging to find APN permutations. For many years, researchers believed that such permutations do not exist. In 1994, Nyberg first proposed this problem publicly [76].

A number of non-existence results have been obtained in this direction. For instance, that any permutation F over a field of even dimension n satisfying one of the following conditions is not APN:

- $n = 2, 4$ [34, 62];

- F has a quadratic (or partially bent) component [34];
- F is a monomial [50];
- F is quadratic [76];
- all coefficients of F lie in $\mathbb{F}_{2^{n/2}}$ [62];
- All component functions of F are plateaued [1].

So far only one APN permutation over a field of even dimension has been found. The result, from 2009, is due to Browning, Dillon, Kibler and McQuistan [14, 15] and disproves Hou's conjecture [62] on the non-existence of APN permutations over fields of even dimension. The APN permutation in question is defined over $\mathbb{F}_{2^6}$ and is obtained via CCZ-equivalence from the Kim function [15] which is defined s,

$$k(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}^*$. It is worth noting that the Kim function itself is a quadratic APN function but is not a permutation.

The APN permutation over $\mathbb{F}_{2^6}$ can then be written as

$$\begin{aligned}
&w^{59}x^{60} + w^{34}x^{58} + w^{8}x^{57} + w^{23}x^{56} + w^{21}x^{54} + w^{39}x^{53} + \\
&w^{48}x^{52} + w^{48}x^{51} + w^{56}x^{50} + w^{24}x^{49} + w^{44}x^{48} + w^{26}x^{46} + \\
&w^{2}x^{45} + w^{13}x^{44} + w^{54}x^{43} + w^{45}x^{42} + w^{32}x^{41} + w^{41}x^{40} + \\
&w^{48}x^{39} + w^{45}x^{38} + w^{32}x^{37} + w^{14}x^{36} + w^{57}x^{35} + w^{50}x^{34} + \\
&x^{33} + w^{5}x^{32} + w^{31}x^{30} + w^{45}x^{29} + w^{51}x^{28} + w^{32}x^{27} + \\
&w^{30}x^{26} + w^{8}x^{25} + w^{33}x^{24} + w^{39}x^{23} + w^{36}x^{22} + w^{4}x^{21} + \\
&w^{38}x^{20} + w^{52}x^{19} + w^{17}x^{18} + w^{15}x^{17} + w^{31}x^{16} + w^{42}x^{15} + \\
&w^{5}x^{14} + w^{25}x^{13} + w^{9}x^{12} + w^{3}x^{11} + wx^{10} + w^{30}x^{9} + \\
&w^{22}x^{8} + w^{23}x^{7} + w^{54}x^{6} + w^{46}x^{5} + w^{60}x^{4} + w^{29}x^{3} + \\
&w^{20}x^{2} + w^{61}x,
\end{aligned}$$

where $w = u^{-2}$. For more properties of APN permutations, we refer the reader to [34] and [40].

3.4.4.3 Exceptional APN and Other APN Functions

An APN monomial of the form x^d is said to be *exceptional* if it is APN over $\mathbb{F}_{2^n}$ for infinitely many values of n; the exponent d is then called an *exceptional APN exponent*. The Gold and Kasami families of monomials were conjectured to be the only exceptional APN exponents [63], and this was later shown to be true [59]. The precise statement of the result is as follows.

Theorem 6. [59] The only exponents d such that x^d is APN for infinitely many fields $\mathbb{F}_{2^n}$ are $d = 2^i + 1$ and $d = 2^{2i} - 2^i + 1$.

Many sporadic APN functions are not CCZ-equivalent to the known infinite APN families but are not classified into new families either. In particular, there is an extensive list of quadratic APN functions over $\mathbb{F}_{2^n}$ for $n = 6, 7, 8, 9$, which have yet to be classified into infinite families [14, 53, 94, 98].

In 2008, Browning et al. [14] and Edel and Pott [53] found many new APN functions over $\mathbb{F}_{2^n}, 6 \leqslant n \leqslant 8$, one of which is not quadratic.

Yu, Wang and Li [97, 98] discovered 470 CCZ-inequivalent APN functions over $\mathbb{F}_{2^7}$ and 8157 over $\mathbb{F}_{2^8}$. Recently, Kai-Uwe Schmidt found among them many APN functions with a 7-valued Walsh spectrum; this result was verified by Alexander Pott and Razi Arshad (Alexander Pott, personal communication).

Table 14 presents some classes of non-quadratic APN functions constructed from quadratic functions via CCZ-equivalence [29]. For odd dimensions n the functions presented in the table are AB. In addition, the first function from Table 14 is an AB function that is EA-inequivalent to any permutation when $n = 5$; this disproves the conjecture that such AB functions do not exist [43].

Table 14: *Some APN Functions CCZ-equivalent to* $F(x) = x^3 + \mathrm{tr}_n(x^9)$ *but EA-inequivalent to* F *over* $\mathbb{F}_{2^n}$

No.	Function	Conditions	d°
1	$x^3 + \mathrm{tr}_n(x^9) + (x^2 + x)\mathrm{tr}_n(x^3 + x^9)$	$n \geqslant 5$ odd $\gcd(i, n) = 1$	3
2	$x^3 + \mathrm{tr}_n(x^9) + (x^2 + x + 1)\mathrm{tr}_n(x^3)$	$n \geqslant 4$ even $\gcd(i, n) = 1$	3
3	$\Big(x + \mathrm{tr}_n^3(x^6 + x^{12}) + \mathrm{tr}_n(x)\mathrm{tr}_n^3(x^3 + x^{12})\Big)^3 +$ $\mathrm{tr}_n\Big(\big(x + \mathrm{tr}_n^3(x^6 + x^{12}) + \mathrm{tr}_n(x)\mathrm{tr}_n^3(x^3 + x^{12})\big)^9\Big)$	$6 \mid n$ $\gcd(i, n) = 1$	4
4	$\Big(x^{\frac{1}{3}} + \mathrm{tr}_n^3(x + x^4)\Big)^{-1} + \mathrm{tr}_n\left(\left(\Big(x^{\frac{1}{3}} + \mathrm{tr}_n^3(x + x^4)\Big)^{-1}\right)^9\right)$	$3 \mid n$ n odd	4

4 Summary of Original Work

In this section, we present an overview of our original research results. Each of the following subsections describes one particular topic of research. We always reference the articles in which these results first appeared so that the reader may easily locate the relevant content in the context of the original publications.

Section 4.1 discusses a method of constructing one vectorial Boolean function from another in which the values of the original function are changed at precisely one point of the underlying field. Despite its apparent simplicity, this construction has interesting theoretical implications as it directly concerns the problem of the existence of an APN function over $\mathbb{F}_{2^n}$ of algebraic degree n. All results are published in [25].

In Section 4.2 we compute the exact Walsh spectra of the last three quadratic infinite polynomial families of APN functions for which they were not previously known. The results here are given in [33].

In Section 4.3 we show that an APN function constructed in [56] is affine equivalent to the Gold functions.

In Section 4.4 we describe the setup and results of an experimental procedure intended to find candidates for new APN functions among all polynomials of a particular form for fields of relatively low dimension. These results were presented at the 2nd International Workshop on Boolean Functions and their Applications [90].

Section 4.5 describes the motivation for and process of constructing a table of CCZ-inequivalent representatives from among the known infinite polynomial APN families for dimensions $6 \leqslant n \leqslant 11$. The table can be found in [89].

Finally, Section 4.6 describes how Table 26 was generated, which lists the inverses of all APN power functions belonging to infinite families for all odd dimensions n in the range $3 \leqslant n \leqslant 129$.

4.1 Existence of APN Functions of Algebraic Degree n over $\mathbb{F}_{2^n}$

An old open problem already mentioned in Chapter 3 is that of the maximum algebraic degree of an APN function F over $\mathbb{F}_{2^n}$. In [25], we conjecture that it can never be equal to n for $n \geqslant 3$. We investigate this problem using a construction that involves changing the value of a given function at one particular point. The construction is motivated by the fact that any function of algebraic degree n can be obtained by changing one point in some function of algebraic degree strictly less than n. In the following, we derive some non-existence results that support our conjecture.

Suppose that F is a given (n, n)-function and $u, v \in \mathbb{F}_{2^n}$ are two field elements. Define the function G as

$$G(x) = F(x) + u(x + v)^{2^n - 1} + u.$$

We can think of G as being constructed from F by changing its value at v to u since we have

$$G(x) = \begin{cases} F(x) & x \neq v \\ F(x) + u & x = v. \end{cases}$$

Under EA-equivalence we can assume that G is of the form

$$G(x) = F(x) + u(x + v)^{2^n - 1}$$

since adding a constant to a function produces an EA-equivalent function. Similarly, given F, u and v as above, we can construct a function F' EA-equivalent to F with $F'(0) = 0$ and $F'(1) = 1$ and a function G' EA-equivalent to G and of the form

$$G'(x) = F'(x) + x^{2^n - 1}. \tag{12}$$

Since EA-equivalence preserves APN-ness, this allows us to assume without loss of generality that $u = 1$ and $v = 0$ and that F satisfies $F(0) = 0$ and $F(1) = 1$.

One situation where this simplification cannot be used is when investigating the functions G obtained from a power function F. The reason for this is that the function F' constructed from F as described above does not necessarily have to be a power function. In this case, it is necessary to analyze one of the more general forms

$$G(x) = x^d + u(x+v)^{2^n-1} \tag{13}$$

or

$$G(x) = u(x+v)^d + x^{2^n-1}. \tag{14}$$

4.1.1 Characterizations

One natural characterization of the APN-ness of G is in terms of the derivatives of F. This is expressed in the following proposition which can be obtained in a straightforward manner from the definitions of G and of the class of APN functions.

Proposition 13. [25, Proposition 2] Let F be a function over $\mathbb{F}_{2^n}$ and let G be as defined in (12). Then G is APN if and only if the following two conditions are satisfied:

(i) for any $a \in \mathbb{F}_{2^n}^*$, the function $D_aF(x)$ is 2-to-1 on $\mathbb{F}_{2^n} \setminus \{0, a\}$;

(ii) for any $a \in \mathbb{F}_{2^n}^*$, the equation $D_aF(x) = D_aF(0) + 1$ has no solution.

Proof. Recall that by definition G is APN if and only if its derivatives D_aG for $a \in \mathbb{F}_{2^n}^*$ are 2-to-1. Note that the derivatives of F and of G in direction a coincide in all points except 0 and a. Since the first condition above demands that any D_aF (and therefore any D_aG) is 2-to-1 on $\mathbb{F}_{2^n} \setminus \{0, a\}$, then if G is not APN, D_aG has to be 2^k-to-1 for some $k \geqslant 2$ so that we must have

$$D_aG(0) = D_aG(a) = D_aG(x)$$

for $x \notin \{0, a\}$. From the definition of G, this becomes

$$D_a F(0) + 1 = D_a F(x)$$

which corresponds precisely to the second condition from the proposition unless $x \in \{0, a\}$; however, it is easy to see that $x \in \{0, a\}$ cannot possibly be a solution to the above equality either. □

If we assume, in addition, that F is APN, the above characterization takes the following simpler form.

Corollary 2. [25, Corollary 1] Let F be an APN function over $\mathbb{F}_{2^n}$ and G be defined by (12). Then G is APN if and only if $D_a F(x) = D_a F(0) + 1$ has no solution for any $a \in \mathbb{F}_{2^n}^*$.

Proof. This follows immediately from the fact that all derivatives $D_a F$ of an APN function F are 2-to-1 for $a \in \mathbb{F}_{2^n}^*$ by definition. □

Some facts, including some non-existence results for G, can be derived immediately.

Proposition 14. [25, Propositon 3] Let F be a function over $\mathbb{F}_{2^n}$ and G be defined by (12). Then

(i) G is not a permutation if $\deg(F) \neq n$;

(ii) $\Delta_G \leqslant \Delta_F + 2$; in particular, $\Delta_G \leqslant 4$ when F is APN;

(iii) $\lambda_G(a, b) \in \{ \lambda_F(a, b), 2 - \lambda_F(a, b) \}$ for any $a, b \in \mathbb{F}_{2^n}$, $b \neq 0$, and $\mathcal{NL}(F) - 1 \leqslant \mathcal{NL}(G) \leqslant \mathcal{NL}(F) + 1$;

(iv) for $n \geqslant 3$, if F is plateaued or $\deg(F) \neq n$, then G is not plateaued; in particular, if F is AB then G is not AB and $\mathcal{NL}(G) = 2^{n-1} - 2^{\frac{n-1}{2}} - 1$.

Proof. The first assertion follows simply from the fact that any permutation is balanced. The second assertion is obvious once we consider the fact that changing the value of F at a single point changes the value of D_aF (for any $a \in \mathbb{F}_{2^n}^*$) at precisely two points. The third statement can be seen by expressing $\lambda_G(a,b)$ as

$$\lambda_G(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(bx^{2^n-1}+bF(x)+ax)} = \\ 1 - (-1)^{\mathrm{tr}_n(b)} + (-1)^{\mathrm{tr}_n(b)} \lambda_F(a,b).$$

Finally, the fourth assertion is due to the fact that the algebraic degree of a plateaued function F over $\mathbb{F}_{2^n}$ with amplitude 2^l can be no greater than $(n-l+1)$. □

A characterization in terms of the Walsh coefficients of F is also possible.

Theorem 7. [25, Theorem 1] Let F be any function over $\mathbb{F}_{2^n}$ with $F(0) = 0$, and G be defined by (12). Then G is APN if and only if

$$\sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} \lambda_F^4(a,b) - 8 \sum_{\substack{a,b \in \mathbb{F}_{2^n} \\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b) \\ = \left(2^{3n+1} - 2^{2n+3}\right)(2^n - 1) - 2^{3n+2}. \tag{15}$$

Proof. We first express the fourth power moment of $\lambda_G(a,b)$ in terms of that of $\lambda_F(a,b)$. Note that we have

$$(-1)^{\mathrm{tr}_n(b)} \lambda_F(a,b) = \lambda_{F+1}(a,b).$$

Let us also denote

$$\epsilon_b = 1 - (-1)^{\mathrm{tr}_n(b)} = \begin{cases} 0 & \text{if } \mathrm{tr}_n(b) = 0 \\ 2 & \text{otherwise.} \end{cases} \tag{16}$$

Since

$$\begin{aligned}\lambda_G(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(bx^{2^n-1}+bF(x)+ax)} \\ &= 1-(-1)^{\mathrm{tr}_n(b)}+(-1)^{\mathrm{tr}_n(b)}\lambda_F(a,b) \qquad (17)\end{aligned}$$

holds for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, we can obtain from the above

$$\begin{aligned}\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \lambda_G^4(a,b) &= \sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \left(1-(-1)^{\mathrm{tr}_n(b)}+\lambda_{F+1}(a,b)\right)^4 \\ &= \sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \Big(\epsilon_b^4+4\epsilon_b^3\lambda_{F+1}(a,b) \\ &+ \quad 6\,\epsilon_b^2\,\lambda_{F+1}^2(a,b)+4\,\epsilon_b\,\lambda_{F+1}^3(a,b)+\lambda_{F+1}^4(a,b)\Big).\end{aligned}$$

We have

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \epsilon_b^4 = \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} 2^4 = 2^{2n+3}.$$

By the inverse Walsh transform formula, viz.

$$\sum_{a\in\mathbb{F}_{2^n}} \lambda_f(a) = 2^n(-1)^{f(0)}$$

and Parseval's identity (3), we get

$$\sum_{a\in\mathbb{F}_{2^n}} \lambda_{F+1}(a,b) = 2^n(-1)^{\mathrm{tr}_n(b)}$$

and

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} 6\epsilon_b^2\lambda_{F+1}^2(a,b) = 3\cdot 2^{3n+2}.$$

Using that $\epsilon_b^3 = 4\epsilon_b$, we have in addition:

$$\begin{aligned}
&\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} 4\epsilon_b^3\lambda_{F+1}(a,b)\\
=\ &\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} 2^4(1-(-1)^{\mathrm{tr}_n(b)})\lambda_{F+1}(a,b)\\
=\ &\sum_{b\in\mathbb{F}_{2^n}^*} 2^{n+4}((-1)^{\mathrm{tr}_n(b)}-1) = -2^{2n+4}.
\end{aligned}$$

We arrive then at:

$$\begin{aligned}
\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \lambda_G^4(a,b) \quad = \quad &\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} (\lambda_{F+1}^4(a,b) + 4\epsilon_b\lambda_{F+1}^3(a,b))\\
&+2^{2n+3}(3\cdot 2^{n-1}-1).
\end{aligned}$$

Again by the fact that $\lambda_{F+1}(a,b) = (-1)^{\mathrm{tr}_n(b)}\lambda_F(a,b)$, we have $\lambda_{F+1}^4(a,b) = \lambda_F^4(a,b)$ and

$$4\epsilon_b\lambda_{F+1}^3(a,b) = \begin{cases} 0 & \text{if} \quad \mathrm{tr}_n(b)=0\\ -8\lambda_F(a,b)^3 & \text{if} \quad \mathrm{tr}_n(b)=1. \end{cases}$$

Thus, the above equality can be written as

$$\begin{aligned}
\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \lambda_G^4(a,b) = \sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \lambda_F^4(a,b) - 8\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b)\\
+\ 2^{2n+3}(3\cdot 2^{n-1}-1)
\end{aligned}$$

which completes the proof. □

If F is assumed to be APN itself, the necessary condition from Proposition 9 and the characterization from Proposition 10 can be applied to the above theorem to obtain a simpler expression.

Corollary 3. [25, Corollary 2] Let F be an APN function over $\mathbb{F}_{2^n}$ with $F(0) = 0$ and let G be defined by (12). Then:

(i) G is APN if and only if

$$\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b) = 2^{2n}(3\cdot 2^{n-1}-1);$$

(ii) If G is APN, then

$$\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=0}} \lambda_F^3(a,b) = 2^{2n}(3\cdot 2^{n-1}-1).$$

Applying Proposition 9 leads to the following necessary conditions on the APN-ness of F and G.

Proposition 15. [25, Proposition 4] Let F be any function over $\mathbb{F}_{2^n}$ with $F(0) = 0$, and G be defined by (12). Then the following holds

(i) If G is APN then

$$\sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F^3(a,b) = 2 \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b). \tag{18}$$

(ii) If F is APN then

$$\sum_{a,b\in\mathbb{F}_{2^n}} \lambda_G^3(a,b) = 2 \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=0}} \lambda_F^3(a,b). \tag{19}$$

Proof. Defining ϵ_b by (16) we get

$$\sum_{a,b\in\mathbb{F}_{2^n}} \lambda_G^3(a,b) = \sum_{a,b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{tr}_n(b)}+\lambda_{F+1}(a,b)\right)^3$$

$$= \sum_{a,b\in\mathbb{F}_{2^n}} \Big(\epsilon_b^3 + \lambda_{F+1}^3(a,b) + 3\ \epsilon_b^2\lambda_{F+1}(a,b)$$

$$+3\ \epsilon_b\lambda_{F+1}^2(a,b)\Big) = 2^3\cdot 2^{2n-1} + \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=0}} \lambda_F^3(a,b)$$

$$- \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b) + 6\cdot 2^{2n}\cdot 2^{n-1} - 12 \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F(a,b)$$

$$= \sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F^3(a,b) - 2 \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b) \tag{20}$$

$$+3\cdot 2^{3n} - 2^{2n+1}$$

$$= - \sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F^3(a,b) + 2 \sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=0}} \lambda_F^3(a,b) \tag{21}$$

$$+3\cdot 2^{3n} - 2^{2n+1}.$$

If G is APN then using (20) and Proposition 10 we get (18). If F is APN then using (21) and Proposition 10 we get (19). □

Applying Theorem 7 leads to the following condition.

Corollary 4. [25, Corollary 3] Let F be any function over $\mathbb{F}_{2^n}$ with $F(0) = 0$ and G be defined by (12). If G is APN then

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \lambda_F^4(a,b) - 4 \sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F^3(a,b)$$

$$= \big(2^{3n+1} - 2^{2n+3}\big)(2^n - 1) - 2^{3n+2}. \tag{22}$$

If we define the values

$$M_0 = |\{(x,y,z)\in\mathbb{F}_{2^n}^3 : F(x) + F(y) + F(z) + F(x+y+z) = 0\}|, \tag{23}$$

and

$$N_i = |\{(x, y) \in \mathbb{F}_{2^n}^2 : F(x) + F(y) + F(x + y) = i\}| \tag{24}$$

for $i \in \{0, 1\}$, the characterization of the APN-ness of G given above can be expressed as follows.

Theorem 8. [25, Theorem 2] Let F be any function over $\mathbb{F}_{2^n}$ with $F(0) = 0$, and G be defined by (12). Then G is APN if and only if

$$M_0 - 4(N_0 - N_1) = (3 \cdot 2^n - 2)(2^n - 4), \tag{25}$$

where M_0, N_0, N_1 are defined by (23) and (24) respectively.

Proof. Proceeding from the definition, we can easily obtain

$$\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F^4(a, b) \\
= &\sum_{\substack{a,b,x,y,z,\\ w\in\mathbb{F}_{2^n}}} (-1)^{\mathrm{tr}_n(b(F(x)+F(y)+F(z)+F(w))+a(x+y+z+w))} \\
= &\ 2^n \sum_{b,x,y,z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(b(F(x)+F(y)+F(z)+F(x+y+z)))} \\
= &\ 2^{2n} M_0,
\end{aligned} \tag{26}$$

as well as

$$\begin{aligned}
&\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a, b) \\
&= \sum_{\substack{a,b,x,y,z\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} (-1)^{\mathrm{tr}_n(b(F(x)+F(y)+F(z))+a(x+y+z))} \\
&= 2^n \sum_{\substack{b,x,y\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} (-1)^{\mathrm{tr}_n(b(F(x)+F(y)+F(x+y)))} \\
&= 2^{2n-1}(N_0 - N_1).
\end{aligned} \tag{27}$$

Indeed, for any fixed $(x, y) \in \mathbb{F}_{2^n}^2$ we have

$$\sum_{\mathrm{tr}_n(b)=1} (-1)^{\mathrm{tr}_n(b(F(x)+F(y)+F(x+y)))} = 0$$

if $F(x) + F(y) + F(x + y) \notin \{0, 1\}$ due to the two-tuple-balance property of the trace function (i.e., $(\mathrm{tr}_n(x), \mathrm{tr}_n(\delta x))$ for $\delta \neq 0, 1$ takes each pair $(0, 0), (0, 1), (1, 0), (1, 1)$ exactly 2^{n-2} times when x runs through $\mathbb{F}_{2^n}$).

The result then follows from Theorem 7. □

Note that the values N_0 and M_0 used above are known when F is APN (see, e.g., [41]). More precisely, we have

$$M_0 = 2^n(3 \cdot 2^n - 2)$$

and

$$N_0 = 3 \cdot 2^n - 2.$$

Substituting these values into Theorem 8, we can obtain the following corollary, which is essentially a restatement of Corollary 2.

Corollary 5. [25, Corollary 4] Let F be APN with $F(0) = 0$ and G be defined by (12). Then G is APN if and only if the value N_1 as defined in (24) is zero, i.e.,

$$|\{(x, y) \in \mathbb{F}_{2^n}^2 : F(x) + F(y) + F(x + y) = 1\}| = 0.$$

4.1.2 Application to Specific Cases

The characterizations obtained in the previous subsection can now be applied to particular classes of vectorial Boolean functions to show that an APN function cannot be obtained from any of their representatives by changing the value of a single point. Since the majority of the known APN functions are either monomials or plateaued functions (or are equivalent to them), we concentrate on those two

cases. The obtained non-existence results are then generalized to the related equivalence classes using the observations from Subsection 4.1.3 below.

An interesting result is that $G(x) = F(x) + x^{2^n-1}$ cannot be APN if F is a monomial or a plateaued function over fields of non-trivial dimension.

Proposition 16. [25, Proposition 5] Let $n \geqslant 3$, $1 \leqslant d \leqslant 2^n - 2$, and $F(x) = x^d$ be a power function over $\mathbb{F}_{2^n}$. Then the function G defined by (12) is not APN.

Proof. Recall that by Proposition 13, a necessary condition for G to be APN is for the equation

$$D_a F(x) + D_a F(0) = 1$$

to have no solution for any $a \in \mathbb{F}_{2^n}^*$. In the particular case of $F(x) = x^d$, this means that

$$x^d + (x+a)^d + a^d = 1$$

has no solution $x \in \mathbb{F}$ for any $a \in \mathbb{F}_{2^n}^*$. In particular, if we take $a = 1$, then

$$\left(\frac{1}{x} + 1\right)^d = 1$$

has no solution $x \in \mathbb{F}_{2^n}^*$, so that $\gcd(d, 2^n - 1) = 1$.

If we denote $y = x/a$ and divide both sides by a^d, the necessary condition for G to be APN becomes that the equation

$$y^d + (y+1)^d = \frac{1}{a^d} + 1$$

has no solution $y \in \mathbb{F}_{2^n}$ for any $a \in \mathbb{F}_{2^n}^*$. But the expression $\frac{1}{a^d}$ ranges over all elements in $\mathbb{F}_{2^n}^*$ as a ranges over $\mathbb{F}_{2^n}^*$, so that the right-hand side of the equation ranges over $\mathbb{F}_{2^n} \setminus \{1\}$. Then $y^d + (y+1)^d$

must necessarily be the constant function 1 in order for the equation to have no solutions. Then a^d must be the constant function a, which contradicts $F(x) = x^d$ being APN. □

As discussed above, in the case of power functions we have to assume the function G to be in one of the more general forms (13) or (14). The following lemma demonstrates, however, that it is sufficient to consider only $v \in \{0, 1\}$.

Lemma 1. [25, Lemma 5] Let $u, v \in \mathbb{F}_{2^n}^*$ and let d satisfy $1 \leqslant d \leqslant 2^n - 2$. Then there exists some $w \in \mathbb{F}_{2^n}^*$ such that $u(x+v)^{2^n-1} + x^d$ is EA-equivalent to $w(x+1)^{2^n-1} + x^d$.

Proof. We have $u(x+v)^{2^n-1} + x^d = u(x/v+1)^{2^n-1} + v^d(x/v)^d$ and denoting $y = x/v$ we obtain the EA-equivalent function $w(y+1)^{2^n-1} + y^d$ where $w = u/v^d$. □

The general case thus becomes

$$F(x) = u(x+v)^d \tag{28}$$

for some $1 \leqslant d \leqslant 2^n - 2$ and $u \in \mathbb{F}_{2^n}^*$, $v \in \mathbb{F}_2$, $G(x) = F(x) + x^{2^n-1}$. According to the second condition in Proposition 13, if G is APN, then the equation $D_aF(x) + D_aF(0) = 1$, that is,

$$u(x+v)^d + u(x+v+a)^d = uv^d + u(v+a)^d + 1$$

has no solution for any $a \in \mathbb{F}_{2^n}^*$. Denoting $y = (x+v)/a$ we can rewrite the latter equation as

$$y^d + (y+1)^d = \left(\frac{v}{a}\right)^d + \left(\frac{v}{a}+1\right)^d + \frac{1}{ua^d}.$$

In the particular case of $\gcd(d, 2^n - 1) = 1$ and $v = 0$, the right hand side of this equation ranges over $\mathbb{F}_{2^n} \setminus \{1\}$ when a ranges over $\mathbb{F}_{2^n}^*$. If it has no solution for any $a \neq 0$ then $ux^d + u(x+1)^d$ cannot be 2-to-1 on $\mathbb{F}_{2^n} \setminus \{0, 1\}$. Hence G cannot be APN according to the first condition of Proposition 13.

We state this as a corollary below.

Corollary 6. [25, Corollary 5] Let $n \geqslant 3$ and $F(x) = ux^d$ be a function over $\mathbb{F}_{2^n}$ with $u \in \mathbb{F}_{2^n}^*$, $1 \leqslant d \leqslant 2^n - 2$ and $\gcd(d, 2^n - 1) = 1$. Then the function $G(x) = F(x) + x^{2^n-1}$ is not APN.

Another particular case for which we can obtain a direct theoretical result is that of the inverse function. The proof utilizes the following technical Lemma 2 whose proof we skip here for the sake of simplicity.

Lemma 2. [58, Lemma 2] Let $\overline{\mathbb{F}}_{2^n}$ denote the algebraic closure of $\mathbb{F}_{2^n}$. Let $f(z), g(z)$ be polynomials with coefficients in $\mathbb{F}_{2^n}$, where $\deg f < r = \deg g$ and $g(z)$ is a polynomial with t distinct zeros in $\overline{\mathbb{F}}_{2^n}$. If $\frac{f(z)}{g(z)} \neq h(z)^2 + h(z)$ for any rational function $h(z) \in \overline{\mathbb{F}}_{2^n}[z]$, then

$$\Big| \sum_{a \in L} (-1)^{\mathrm{tr}_n\left(\frac{f(z)}{g(z)}\right)} \Big| \leqslant (t + r - 2)\sqrt{2^n} + 1,$$

where L consists of all elements of $\mathbb{F}_{2^n}$ except the zeros of $g(z)$.

Proposition 17. [25, Proposition 6] Let $n \geqslant 3$ and $F(x) = u(x + v)^{2^n-2}$ be a function over $\mathbb{F}_{2^n}$ with $u \in \mathbb{F}_{2^n}^*$, $v \in \mathbb{F}_{2^n}$. Then the function G defined by (12) is not APN.

Proof. The equation $D_aF(x) = D_aF(0) + 1$, $a \in \mathbb{F}_{2^n}^*$, can be written as

$$u(x + v)^d + u(x + a + v)^d = uv^d + u(a + v)^d + 1$$

for $d = 2^n - 2$. If we find a solution for $D_aF(x) = D_aF(0) + 1$ for some $a \in \mathbb{F}_{2^n}^*$ then the function G is not APN by Proposition 2. According to Lemma 1 we can restrict to the cases $v \in \mathbb{F}_2$, and due to Corollary 6 further restrict to $v = 1$. Besides, we can consider only $n \geqslant 4$ since $n = 3$ is easy to check with a computer.

By a simple calculation of $D_aF(x) = D_aF(0) + 1$ we can obtain that for $x \notin \{1, a + 1\}$

$$x^2 + ax + a + 1 + \frac{a}{1 + (a + 1)^d + u^d} = 0. \tag{29}$$

However, it is also easy to check that $x = 1$ and $x = a + 1$ cannot be solutions of (29). Further note that (29) has solutions in $\mathbb{F}_{2^n}$ if and only if

$$\mathrm{tr}_n\Big(\frac{a+1}{a^2} + \frac{1}{a(1+(a+1)^d+u^d)}\Big) = 0$$

, i.e.,

$$\mathrm{tr}_n\Big(\frac{1}{a(1+(a+1)^d+u^d)}\Big) = 0, \tag{30}$$

where $a \notin \{0, 1, (u+1)^d\}$. For simplicity, define

$$\phi(a) = \frac{1}{a(1+(a+1)^d+u^d)} = \frac{u(a+1)}{(u+1)a^2+a}.$$

In what follows, we prove that there exists at least one $a \in \mathbb{F}_{2^n}^* \setminus \{1, (u+1)^d\}$ such that $\mathrm{tr}_n(\phi(a)) = 0$. First, we show that $\phi(a) \neq h(a)^2 + h(a)$ for any rational function $h(a) \in \overline{\mathbb{F}}_{2^n}[a]$, where $\overline{\mathbb{F}}_{2^n}$ denotes the algebraic closure of $\mathbb{F}_{2^n}$. Assume that

$$\phi(a) = \frac{\nu(a)^2}{\mu(a)^2} + \frac{\nu(a)}{\mu(a)}$$

for some $\mu(a), \nu(a) \in \overline{\mathbb{F}}_{2^n}[a]$ with $\gcd(\mu(a), \nu(a)) = 1$, then one gets

$$u(a+1)\mu(a)^2 = ((u+1)a^2+a)(\nu(a)^2 + \mu(a)\nu(a))$$

which implies that $a|\mu(a)$ and then $a^2|\mu(a)^2$. However,

$$a^2 \nmid ((u+1)a^2+a)(\nu(a)^2 + \mu(a)\nu(a))$$

since $\gcd(\mu(a), \nu(a)) = 1$ and $a|\mu(a)$. This leads to a contradiction. Therefore, $\phi(a) \neq h(a)^2 + h(a)$ for any rational function $h(a) \in \overline{\mathbb{F}}_{2^n}[a]$. By Lemma 2, we have

$$\Big|\sum_{a \in \mathbb{F}_{2^n}^* \setminus \{1,(u+1)^d\}} (-1)^{\mathrm{tr}_n(\phi(a))}\Big| \leqslant (2+2-2)\sqrt{2^n} + 1.$$

Thus, if $\mathrm{tr}_n(\phi(a)) = 1$ for any $a \in \mathbb{F}_{2^n}^* \setminus \{1, (u+1)^d\}$, then we have $2^n - 3 \leqslant (2+2-2)\sqrt{2^n} + 1$, which leads to $2^n \leqslant (1+\sqrt{5})^2 < 16$. This shows that there exists at least one $a \in \mathbb{F}_{2^n}^* \setminus \{1, (u+1)^d\}$ such that $\mathrm{tr}_n(\phi(a)) = 0$ if $n \geqslant 4$. □

Theoretical non-existence results can be obtained in the case of F plateaued as well. The following lemma is useful when working with plateaued functions.

Lemma 3. [58, Lemma 3] Let f be a plateaued Boolean function over $\mathbb{F}_{2^n}$ with amplitude 2^l. Then the distribution of its Walsh transform values is given by

Walsh Transform Value	Frequency
0	$2^n - 2^{2n-2l}$
2^l	$2^{2n-2l-1} + (-1)^{f(0)}\, 2^{n-l-1}$
-2^l	$2^{2n-2l-1} - (-1)^{f(0)}\, 2^{n-l-1}$

and we have $\sum_{a\in\mathbb{F}_{2^n}} \lambda_f^3(a) = (-1)^{f(0)}\, 2^{n+2l}$ and $\sum_{a\in\mathbb{F}_{2^n}} \lambda_f^4(a) = 2^{2n+2l}$.

Proof. Let us denote by N_+ (resp. N_-) the number of occurrences of 2^l (resp. -2^l), we have according to the Parseval identity that $2^{2l}(N_+ + N_-) = 2^{2n}$, and according to the inverse Walsh transform formula $\sum_{a\in\mathbb{F}_{2^n}} \lambda_f(a) = 2^n(-1)^{f(0)}$, that $2^l(N_+ - N_-) = 2^n(-1)^{f(0)}$. This directly gives the table above. The two other relations can be deduced either from this table, or from (again) the inverse Walsh transform formula and the Parseval identity, since we have $\sum_{a\in\mathbb{F}_{2^n}} \lambda_f^3(a) = 2^{2l} \sum_{a\in\mathbb{F}_{2^n}} \lambda_f(a)$ and $\sum_{a\in\mathbb{F}_{2^n}} \lambda_f^4(a) = 2^{2l} \sum_{a\in\mathbb{F}_{2^n}} \lambda_f^2(a)$. □

Theorem 9. [25, Theorem 3] Let F be a plateaued function over $\mathbb{F}_{2^n}$ with $n \geqslant 3$ and G be defined by (12). Then G is not APN.

Proof. Let n be odd and 2^{λ_b} be the amplitude of the component function F_b for $b \in \mathbb{F}_{2^n}^*$. We have $\lambda_b \geqslant \frac{n+1}{2}$. According to Lemma 3 , we have $\sum_{a\in\mathbb{F}_{2^n}} \lambda_F^3(a,b) = (-1)^{\mathrm{tr}_n(bF(0))}\, 2^{n+2\lambda_b}$ and $\sum_{a\in\mathbb{F}_{2^n}} \lambda_F^4(a,b) = 2^{2n+2\lambda_b}$. Hence, $\sum_{a\in\mathbb{F}_{2^n}} \lambda_F^3(a,b)$ is divisible by 2^{2n+1} and $\sum_{a\in\mathbb{F}_{2^n}} \lambda_F^4(a,b)$ is divisible by 2^{3n+1}, and therefore by 2^{2n+4} since $n \geqslant 3$. Then relation (15) cannot be satisfied since the term on the left hand side is divisible by 2^{2n+4} and the term on the right hand side is not.

Let now n be even. This case is more technical. Without loss of generality, we can assume that $F(0) = 0$. Suppose that G is APN. Then, by Proposition 13, for any $a \neq 0$ the image of $\mathbb{F}_{2^n} \setminus \{0, a\}$ by D_aF has $2^{n-1} - 1$ elements, and,

$$\sum_{b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = (2^{n-1} - 1) \cdot 2^2 + (4^2 - 2^2)$$

if $D_aF(x) = D_aF(0)$ has 4 solutions and

$$\sum_{b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = (2^{n-1} - 1) \cdot 2^2 + 2^2$$

otherwise. That is,

$$\sum_{b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = 2^{n+1} + 8t_a,$$

where $t_a = 1$ if $D_aF(x) = D_aF(0)$ has 4 solutions and $t_a = 0$ otherwise. Indeed, we know that D_aF is 2-to-1 on $\mathbb{F}_{2^n} \setminus \{0, a\}$; we deduce that $D_aF(\mathbb{F}_{2^n} \setminus \{0, a\})$ has size $2^{n-1} - 1$ and includes the element $D_aF(0)$ in the first case and does not include it in the second case.

Because $\Delta_F(0, b) = 0$ for any $b \neq 0$ then

$$\begin{aligned} \sum_{(a,b)\neq(0,0)} \Delta_F(a,b)^2 &= (2^n - 1)2^{n+1} + 8 \sum_{a\in\mathbb{F}_{2^n}^*} t_a \\ &= (2^n - 1)2^{n+1} + 8T, \end{aligned} \tag{31}$$

where $0 \leqslant T \leqslant 2^n - 1$.

Recall the equality

$$\sum_{(a,b)\neq(0,0)} \Delta_F(a,b)^2 = \frac{1}{2^{2n}} \sum_{(a,b)\neq(0,0)} \lambda_F(a,b)^4.$$

from Proposition 4.

Let 2^{λ_b} be again the amplitude of F_b for $b \in \mathbb{F}_{2^n}^*$. Then $\lambda_b = \frac{n+s_b}{2}$ for $0 \leqslant s_b \leqslant n$ and by Lemma 3

$$\frac{1}{2^{2n}} \sum_{(a,b)\neq(0,0)} \lambda_F(a,b)^4 = 2^n \sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b}. \tag{32}$$

The values s_b are even for all $b \neq 0$, and $2^{s_b} - 1$ and $2^n - 1$ are divisible by 3. Hence using (31)-(32) we get

$$\sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b} = 2(2^n - 1) + T' \tag{33}$$

where $T' = T/2^{n-3}$, $0 \leqslant T' \leqslant 7$. Then

$$\sum_{b\in\mathbb{F}_{2^n}^*} (2^{s_b} - 1) = 2^n - 1 + T'$$

and T' is divisible by 3. Hence $T' \in \{0, 3, 6\}$.

Using (32) and (33) we get

$$\begin{aligned} \sum_{\substack{a\in\mathbb{F}_{2^n} \\ b\in\mathbb{F}_{2^n}^*}} \lambda_F(a,b)^4 &= 2^{3n} \sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b} = 2^{3n}\left(2^{n+1} + v\right) \\ &= 2^{4n+1} + 2^{3n} v, \end{aligned} \tag{34}$$

where $v = -2$ if $T' = 0$ and $v = 1$ if $T' = 3$ and $v = 4$ if $T' = 6$.

Since G is APN then (15) holds by Theorem 7 and using (34):

$$\begin{aligned}
\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{tr}_n(b)=1}} \lambda_F^3(a,b) &= \frac{1}{8}\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*}\lambda_F^4(a,b)\\
&\quad -(2^{3n-2}-2^{2n})(2^n-1)+2^{3n-1}\\
&= 2^{2n}(7\cdot 2^{n-2}+2^{n-3}v-1)\\
&= \begin{cases} 2^{2n}(3\cdot 2^{n-1}-1) & \text{if } v=-2\\ 2^{2n}(15\cdot 2^{n-3}-1) & \text{if } v=1\\ 2^{2n}(9\cdot 2^{n-2}-1) & \text{if } v=4. \end{cases} \qquad (35)
\end{aligned}$$

By Lemma 3 and using (33), we get:

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} \lambda_F^3(a,b) = 2^{2n}\sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b} = 2^{2n}(2^{n+1}+v). \qquad (36)$$

Besides,

$$\begin{aligned}
\sum_{\substack{a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^n}^*\\ \mathrm{tr}_n(b)=0}} \lambda_F^3(a,b) &= 2^{2n}\sum_{\substack{b\in\mathbb{F}_{2^n}^*\\ \mathrm{tr}_n(b)=0}} 2^{s_b}\\
&\geqslant 2^{2n}(2^{n-1}-1). \qquad (37)
\end{aligned}$$

Hence by (35)-(37):

$$\begin{aligned}
2^{2n}(2^{n+1}+v) = \sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*}\lambda_F^3(a,b) &\geqslant 2^{2n}(2^{n-1}-1)\\
&+\begin{cases} 2^{2n}(3\cdot 2^{n-1}-1) & \text{if } v=-2\\ 2^{2n}(15\cdot 2^{n-3}-1) & \text{if } v=1\\ 2^{2n}(9\cdot 2^{n-2}-1) & \text{if } v=4. \end{cases}
\end{aligned}$$

Clearly, this inequality does not hold when $n\geqslant 4$ and $v\in\{1,4\}$. When $v=-2$ this corresponds to the case of F an APN function

and the last inequality becomes an equality. That is, we get that F_b is bent for all $b \in \mathbb{F}_{2^n}^*$ satisfying $\mathrm{tr}_n(b) = 0$. However, this is impossible if $n > 2$, since otherwise we would have an $(n, n-1)$-vectorial bent function. Indeed, take a basis $(b_1, .., b_{n-1})$ of the hyperplane of equation $\mathrm{tr}_n(b) = 0$ and define the vectorial $(n, n-1)$-function whose coordinates are $f_i(x) = \mathrm{tr}_n(b_i F(x))$ for $i = 1, .., n-1$. Then all its component functions are bent and, by definition, the function is then bent. This contradicts the fact recalled above that (n, m)-vectorial bent functions exist only for $2m \leqslant n$ [74]. □

From the theorem we can immediately deduce the following non-existence results:

Corollary 7. [25, Corollary 6,7] Let F be a function over $\mathbb{F}_{2^n}$ and let G be defined as in (12). Then G is not APN if F is:

- quadratic;
- AB (almost bent).

4.1.3 Generalization to Equivalence Classes

In the previous subsection, we described how the obtained characterizations could be applied to some specific classes of functions, viz. monomials and plateaued functions. We now present some results concerning the relationship between the EA- and CCZ-equivalence classes of F and G. Briefly stated, the following observations show that the possibility of obtaining an APN function using this construction does not depend on the choice of the representative from its equivalence class.

Proposition 18. [25, Proposition 7] Let F be a function over $\mathbb{F}_{2^n}$ and $G(x) = x^{2^n-1} + F(x)$. If a function G' is EA-equivalent to G then there exist some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, and a function F' EA-equivalent to F such that $G'(x) = u(x+v)^{2^n-1} + F'(x)$.

Proof. For EA-equivalent functions G and G' there exist affine permutations A_1, A_2 and an affine function A such that $G'(x) = A_1 \circ G \circ A_2(x) + A(x)$. Without loss of generality we can assume A_1 to be linear. Note that

$$A_1 \circ G \circ A_2(x) = A_1 \circ F \circ A_2(x) + A_1((A_2(x))^{2^n-1})$$

and denoting $F'(x) = A_1 \circ F \circ A_2(x) + A(x)$ we get

$$\begin{aligned} G'(x) &= F'(x) + A_1((A_2(x))^{2^n-1}) \\ &= F'(x) + A_1(1)(x + A_2^{-1}(0))^{2^n-1} \end{aligned}$$

since $A_1((A_2(x))^{2^n-1})$ takes value $A_1(1)$ if $x \neq A_2^{-1}(0)$ (that is, $A_2(x) \neq 0$) and 0 otherwise, and we can rewrite it as $A_1(1)(x + A_2^{-1}(0))^{2^n-1})$ (which takes the same values). Hence $G'(x) = F'(x) + u(x+v)^{2^n-1}$ for $u = A_1(1) \neq 0$ and $v = A_2^{-1}(0)$ and the function F' is EA-equivalent to F. □

Proposition 19. [25, Proposition 8] If F and F' are EA-equivalent functions over $\mathbb{F}_{2^n}$ then the function $G'(x) = x^{2^n-1} + F'(x)$ is EA-equivalent to $u(x+v)^{2^n-1} + F(x)$ for some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$.

Proof. For EA-equivalent functions F and F' there exist affine permutations A_1, A_2 and affine A such that $F'(x) = A_1 \circ F \circ A_2(x) + A(x)$. Without loss of generality we can assume $A_1(0) = 0$. Then $G'(x) = x^{2^n-1} + A_1 \circ F \circ A_2(x) + A(x)$ and it is EA-equivalent to $A_1^{-1}((A_2^{-1}(x))^{2^n-1}) + F(x) = A_1^{-1}(1)(x + A_2(0))^{2^n-1} + F(x) = u(x+v)^{2^n-1} + F(x)$ with $u = A_1^{-1}(1) \neq 0$ and $v = A_2(0)$. □

The latter proposition leads to an important non-existence result.

Corollary 8. [25, Corollary 8] Let F and F' be EA-equivalent functions over $\mathbb{F}_{2^n}$. If for any $v \in \mathbb{F}_{2^n}$ and any nonzero $u \in \mathbb{F}_{2^n}$ the function $x^{2^n-1} + uF(x+v)$ is not APN then for any $v' \in \mathbb{F}_{2^n}$ and any nonzero $u' \in \mathbb{F}_{2^n}$ the function $x^{2^n-1} + u'F'(x+v')$ is not APN either.

The following proposition is an analog to Proposition 18 for the case of CCZ-equivalence.

Proposition 20. [25, Proposition 9] Let F be a function over $\mathbb{F}_{2^n}$ and G be defined by (12). If a function G' is CCZ-equivalent to G then there exist some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, and a function F' CCZ-equivalent to F such that $G'(x) = u(x+v)^{2^n-1} + F'(x)$.

Proof. Since G and G' are CCZ-equivalent then for some affine permutation

$$\begin{aligned}\mathcal{L}(x,y) &= \big(L_1(x,y), L_2(x,y)\big)\\ &= \big(A_1(x) + A_2(y) + a, A_3(x) + A_4(y) + b\big),\end{aligned}$$

where A_1, A_2, A_3, A_4 are linear and $a, b \in \mathbb{F}_{2^n}$, we have $G'(x) = G_2 \circ G_1^{-1}(x)$ with

$$G_1(x) = L_1(x, G(x)) = A_1(x) + A_2 \circ G(x) + a$$

a permutation and

$$G_2(x) = L_2(x, G(x)) = A_3(x) + A_4 \circ G(x) + b.$$

Note that $G_1(x) = A_1(x) + A_2 \circ F(x) + A_2(x^{2^n-1}) + a$ and since it is a permutation then $A_2(0) = A_2(1) = 0$ and $G_1(x) = A_1(x) + A_2 \circ F(x) + a$. Take $F_1(x) = G_1(x)$ and $F_2(x) = A_3(x) + A_4 \circ F(x) + b$. Then, obviously, $F'(x) = F_2 \circ F_1^{-1}(x)$ is CCZ-equivalent to F and

$$\begin{aligned}G'(x) &= F'(x) + A_4((F_1^{-1}(x))^{2^n-1})\\ &= F'(x) + A_4(1)(x + F_1(0))\\ &= F'(x) + u(x+v)^{2^n-1}\end{aligned}$$

with $u = A_4(1)$ and $v = F_1(0)$. Note that $u \neq 0$ since otherwise the system

$$\begin{aligned}A_1(x) + A_2(y) + a &= a\\ A_3(x) + A_4(y) + b &= b\end{aligned}$$

would have two solutions $(0,0)$ and $(0,1)$ and $\mathcal{L}$ would not be a permutation. $\square$

In order to give an analog to Proposition 19 for CCZ-equivalence, we need to make an additional assumption on the affine permutation $\mathcal{L}$ from the definition of CCZ-equivalence.

Proposition 21. [25, Proposition 10] Let F and F' be two CCZ-equivalent functions over $\mathbb{F}_{2^n}$, that is, $\mathcal{L}(G_F) = G_{F'}$ for some affine permutation $\mathcal{L}(x,y) = (L_1(x,y), L_2(x,y))$ of $\mathbb{F}_{2^n}^2$. If $L_1(0,y)$ is not a permutation of $\mathbb{F}_{2^n}$ then there exist some $u, v, w \in \mathbb{F}_{2^n}$, $u, w \neq 0$, such that functions $wx^{2^n-1} + F(x)$ and $u(x+v)^{2^n-1} + F'(x)$ are CCZ-equivalent.

Proof. When the affine function $L_1(0,y)$ is not a permutation of $\mathbb{F}_{2^n}$ there exists $w \in \mathbb{F}_{2^n}^*$ such that $L_1(0,0) = L_1(0,w)$. Clearly a linear function $\mathcal{L}^\circ(x,y) = (x, wy)$ is a permutation of $\mathbb{F}_{2^n}^2$ and

$$\mathcal{L} \circ \mathcal{L}^\circ(x,y) = (L_1(x,wy), L_2(x,wy))$$

maps the graph of the function $w^{-1}F(x)$ to the graph of the function $F'(x)$. Moreover, $\mathcal{L} \circ \mathcal{L}^\circ$ maps the graph of $G(x) = x^{2^n-1} + w^{-1}F(x)$ to the graph of $G'(x) = u(x+v)^{2^n-1} + F'(x)$ for $u = L_2(0,w) + L_2(0,0)$ and $v = L_1(0, F(0))$. Indeed, note that $u \neq 0$ since otherwise $\mathcal{L}$ would not be a permutation and we have

$$\begin{aligned}
G_1(x) &= L_1(x, wG(x)) = L_1\big(x, F(x) + wx^{2^n-1}\big) \\
&= L_1(x, F(x)) + \big(L_1(0,w) + L_1(0,0)\big)x^{2^n-1} \\
&= F_1(x), \\
G_2(x) &= L_2(x, wG(x)) = L_2\big(x, F(x) + wx^{2^n-1}\big) \\
&= L_2(x, F(x)) + ux^{2^n-1} = F_2(x) + ux^{2^n-1}, \\
G'(x) &= G_2 \circ G_1^{-1}(x) = F_2 \circ F_1^{-1}(x) + u\big(F_1^{-1}(x)\big)^{2^n-1} \\
&= F'(x) + u(x+v)^{2^n-1}.
\end{aligned}$$

Hence, G and G' are CCZ-equivalent, and, therefore, $wx^{2^n-1} + F(x)$ and G' are CCZ-equivalent. □

The condition of $L_1(0, y)$ not being a permutation is indeed necessary as the following counterexample shows. If we take $F(x) = x^3$ and $F'(x) = F^{-1}(x) = x^{21}$ over $\mathbb{F}_{2^5}$, then F and F' are CCZ-equivalent via $\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y)) = (y, x)$ where $L_1(0, y) = y$ is a permutation. Then for any $u, u' \in \mathbb{F}_{2^5}^*$ and for any $v, v' \in \mathbb{F}_{2^5}$, the functions $G(x) = u(x + v)^{2^n-1} + F(x)$ and $G'(x) = u'(x + v')^{2^n-1} + F'(x)$ are CCZ-inequivalent as can be verified using a computer.

Under the assumption that the dimension n is even and one of the CCZ-equivalent functions is plateaued, Proposition 21 leads to the following nonexistence result.

Corollary 9. [25, Corollary 9] Let F and F' be CCZ-equivalent APN functions over $\mathbb{F}_{2^n}$ where F is plateaued and n is even. Then for an affine permutation $\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y))$ of $\mathbb{F}_{2^n}^2$ satisfying $\mathcal{L}(G_F) = G_{F'}$ there exists $w \in \mathbb{F}_{2^n}^*$ such that $L_1(0, w) = L_1(0, 0)$. Moreover, the function $u(x + v)^{2^n-1} + F'(x)$ is not APN for $u = L_2(0, w) + L_2(0, 0)$ and $v = L_1(0, F(0))$.

Proof. If $L_1(0, w) \neq L_1(0, 0)$ for any $w \in \mathbb{F}_{2^n}^*$ then $L_1(0, y)$ is a permutation of $\mathbb{F}_{2^n}$ and $F_1(x) = L_1(x, F(x))$ is a plateaued APN permutation which leads to a contradiction since all plateaued APN functions have bent components when n is even [39]. Hence, there exists $w \in \mathbb{F}_{2^n}^*$ such that $L_1(0, w) = L_1(0, 0)$. Since $w^{-1}F(x)$ is plateaued APN then $G(x) = wx^{2^n-1} + F(x)$ is not APN by Theorem 9. It follows from the proof of Proposition 21 that for $u = L_2(0, w) + L_2(0, 0)$ and $v = L_1(0, F(0))$ the function $G'(x) = u(x + v)^{2^n-1} + F'(x)$ is CCZ-equivalent to G, and, therefore, it is not APN. □

4.1.4 Conclusion and Future Work

Below we present a systematic overview of the results obtained by applying the above characterizations and observations to particular classes of functions. In all cases, F is a vectorial Boolean function over $\mathbb{F}_{2^n}$ and G is defined as $G(x) = F(x) + x^{2^n-1}$.

In the case when n is odd, G is never APN if F is CCZ-equivalent to:

(i) Gold, Kasami, Niho, Welch or Niho functions (see Table 1);

(ii) any of the functions in Tables 2-4;

(iii) any of the presently known sporadic examples of APN functions.

When n is even, G is never APN if F is EA-equivalent to:

(i) Gold, Kasami or inverse functions (see Table 1);

(ii) any of the functions in Table 4;

(iii) any of the presently known sporadic examples of APN functions including those in Table 5.

Finally, for any dimension n, G is not APN in the following cases:

(i) F is a Dobbertin function (or a sum of a Dobbertin function with an affine function);

(ii) n is odd and $F(x) = uF'(x)$ with any $u \in \mathbb{F}_{2^n}^*$ and F' a Dobbertin function (or a sum of a Dobbertin function with an affine function);

(iii) F is EA-equivalent to a Dobbertin function with $n \leqslant 15$;

(iv) $F(x) = uF'(x)$ with any $u \in \mathbb{F}_{2^n}^*$ satisfying $\mathrm{tr}_n(u^{-1}) = 0$ and F' either the second function in Table 2 or the second function in Table 3;

(v) $F(x) = uF'(x)$ with any $u \in \mathbb{F}_{2^n}^*$ satisfying $\mathrm{tr}_n^3(u^{-1} + u^{-2}) = 0$ and F' either the third function in Table 2 or the third function in Table 3;

(vi) F is EA-equivalent to any of the functions in Tables 2 and 3 with $n \leqslant 12$ even.

The question of whether an APN function can be obtained by changing the value of one point in a monomial remains open. We have only shown that this is impossible in the simplified case of $G(x) = x^d + x^{2^n-1}$ and under some specific conditions (when F is the inverse function, and when $v = 0$ with $\gcd(2^n - 1, d) = 1$ from the general form (28)).

The more general question of the existence of an APN function F of algebraic degree n remains open as well; we have shown that a large number of classes of functions cannot produce such an APN function using the described construction, but a conclusive nonexistence result for the general case has yet to be found.

4.2 Walsh Spectra of Quadratic APN Functions

Table 13 lists all the known infinite polynomial families of quadratic APN functions. As discussed in Chapter 3, the Walsh spectrum is a very important characteristic of any given function, in part because many characterizations depend on the Walsh coefficients of the function. The Walsh spectra of all the families in Table 13 except Nos. 5, 6 and 7 are already known [8, 12, 35, 37, 55, 60, 91]. We compute the Walsh spectra of the remaining three families from the table, viz. the functions

$$F_0(x) = x^3 + a^{-1}\mathrm{tr}_n(a^3x^9) \tag{38}$$

$$F_1(x) = x^3 + a^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18}) \tag{39}$$

$$F_2(x) = x^3 + a^{-1}\mathrm{tr}_n^3(a^6x^{18} + a^{12}x^{36}) \tag{40}$$

for any positive integer n and any nonzero element $a \in \mathbb{F}_{2^n}^*$.

4.2.1 Walsh Spectra of F_1 and F_2

According to the definition, for any $b, c \in \mathbb{F}_{2^n}$, one gets

$$\begin{aligned} g_i(x) &= \mathrm{tr}_n(bF_i(x) + cx) \\ &= \mathrm{tr}_n(bx^3 + ba^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18})^i + cx) \\ &= \mathrm{tr}_n(bx^3 + cx) + \mathrm{tr}_n(ba^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18})^i) \\ &= \mathrm{tr}_n(bx^3 + cx) + \mathrm{tr}_3\mathrm{tr}_n^3(ba^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18})^i) \\ &= \mathrm{tr}_n(bx^3 + cx) + \mathrm{tr}_3\mathrm{tr}_n^3(\mathrm{tr}_n^3(ba^{-1})(a^3x^9 + a^6x^{18})^i) \\ &= \mathrm{tr}_n(bx^3 + cx + \mathrm{tr}_n^3(ba^{-1})(a^3x^9 + a^6x^{18})^i) \end{aligned}$$

for $i \in \{1, 2\}$. For simplicity, denote $\mathrm{tr}_n^3(ba^{-1}) = \delta^2$. By a direct calculation, one obtains

$$\begin{aligned} & g_i(x) + g_i(x+u) + g_i(u) \\ =& \mathrm{tr}_n(bx^2u + bxu^2 + \delta^2(a^3x^8u + a^3xu^8 + a^6x^2u^{16} + a^6x^{16}u^2)^i) \\ =& \mathrm{tr}_n\big(x((bu)^{2^{-1}} + bu^2 + (\delta^{2/i}a^3u)^{2^{-3}}\big) \\ & + \mathrm{tr}_n\big(\delta^{2/i}a^3u^8 + \delta^{1/i}a^3u^8 + (\delta^{1/i}a^3u)^{2^{-3}})\big) \\ =& \mathrm{tr}_n\big(x((\delta^{2/i} + \delta^{1/i})a^3u^8 + bu^2 + (bu)^{2^{-1}}\big) \\ & + \mathrm{tr}_n\big(((\delta^{2/i} + \delta^{1/i})a^3u)^{2^{-3}})\big), \end{aligned}$$

which implies

$$\begin{aligned} |\lambda_{F_i}(b,c)|^2 &= \sum_{x\in\mathbb{F}_{2^n}}\sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_i(x)+g_i(x+u)} \\ &= \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_i(u)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(xL^i_{a,b,\delta}(u))}, \end{aligned}$$

where $L^i_{a,b,\delta}(u)$ is defined as

$$\begin{aligned} L^i_{a,b,\delta}(u) = (\delta^{2/i} + \delta^{1/i})a^3u^8 + bu^2 + (bu)^{2^{-1}} + \\ ((\delta^{2/i} + \delta^{1/i})a^3u)^{2^{-3}}. \end{aligned} \tag{41}$$

Note that $g_i(u) + g_i(u+v) + g_i(v) = \mathrm{tr}_n(vL^i_{a,b,\delta}(u))$. This means that for any u satisfying $L^i_{a,b,\delta}(u) = 0$ and any $v \in \mathbb{F}_{2^n}$ we have

$$g_i(u+v) = g_i(u) + g_i(v)$$

which implies

$$|\lambda_{F_i}(b,c)|^2 \in \{0, 2^n|\{x \in \mathbb{F}_{2^n} : L^i_{a,b,\delta}(u) = 0\}|\}. \tag{42}$$

In what follows, we discuss the number of solutions $u \in \mathbb{F}_{2^n}$ to $L^i_{a,b,\delta}(u) = 0$ by adopting Dobbertin's method [51], which also was used by Bracken et al. in [9] to determine the Walsh spectrum of $F_0(x)$ for the case of $a = 1$.

For simplicity, define $\theta_i = (\delta^{2/i} + \delta^{1/i})a^3$ for $i = 1, 2$. Then $L^i_{a,b,\delta}(u) = 0$ can be written as $\theta_i u^8 + bu^2 + (bu)^{2^{-1}} + (\theta_i u)^{2^{-3}} = 0$ and it can be readily verified that

$$uL^i_{a,b,\delta}(u) \quad = \quad \phi_i(u) + \phi_i(u)^{2^{-1}},$$

where $\phi_i(u)$ is given as

$$\phi_i(u) = bu^3 + \theta_i u^9 + \theta_i^{\frac{1}{2}} u^{\frac{9}{2}} + \theta_i^{\frac{1}{4}} u^{\frac{9}{4}}. \tag{43}$$

Then, if $L^i_{a,b,\delta}(u) = 0$, we must have $\phi_i(u) \in \mathbb{F}_2$.

Proposition 22. Let $a, b \in \mathbb{F}_{2^n}$ with $ab \neq 0$ and $\delta^2 = \mathrm{tr}_n^3(ba^{-1})$. If $\delta^{2/i} + \delta^{1/i} \neq 0$, then $L^i_{a,b,\delta}(u) = 0$ if and only if $\phi_i(u) = 0$ for $i = 1, 2$.

Proof. If $\phi_i(u) = 0$, we have $L^i_{a,b,\delta}(u) = 0$; and if $L^i_{a,b,\delta}(u) = 0$, we have $\phi_i(u) \in \mathbb{F}_2$. Thus, to complete the proof, we need to show that $L^i_{a,b,\delta}(u) = 0$ implies that $\phi_i(u) = 0$ for $i = 1, 2$. Suppose that $\phi_i(u) = 1$, one then gets $b = \theta_i u^6 + \theta_i^{1/2} u^{3/2} + \theta_i^{1/4} u^{-3/4} + u^{-3}$ which together with $\theta_i = (\delta^{2/i} + \delta^{1/i})a^3$ leads to

$$\begin{aligned} \frac{b}{a} = {} & (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})a^2u^6 + (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})^{\frac{1}{2}} a^{\frac{1}{2}} u^{\frac{3}{2}} + \\ & (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})^{\frac{1}{4}} a^{-\frac{1}{4}} u^{-\frac{3}{4}} + a^{-1}u^{-3}. \end{aligned} \tag{44}$$

For convenience, define $\mathrm{tr}_n^3(a^2u^6) = t$ and $\mathrm{tr}_n^3(a^{-1}u^{-3}) = r$. Notice that $\delta^{\frac{1}{2}} = \delta^4$ and $\delta^{\frac{1}{4}} = \delta^2$ since $\delta \in \mathbb{F}_{2^3}$. Then by $\mathrm{tr}_n^3(ba^{-1}) = \delta^2$ and (44) one has that

$$\delta^2 = \mathrm{tr}_n^3(\frac{b}{a}) = (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})t + (\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}})t^{\frac{1}{4}} + (\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})r^{\frac{1}{4}} + r. \tag{45}$$

We can rewrite (45) in the form

$$(\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})r^2 + r + (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})t + (\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}})t^2 + \delta^2 = 0.$$

Note that $\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}} \neq 0$ due to $\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}} \neq 0$. Then the above equation has a solution $r \in \mathbb{F}_{2^3}$ if and only if

$$\mathrm{tr}_3((\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})((\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})t + (\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}})t^2 + \delta^2)) = 0. \tag{46}$$

It is easy to verify that for $i = 1, 2$ we have

$$(\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})^2(\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})^2 = (\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})(\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}}),$$

which implies that (46) holds if and only if

$$\mathrm{tr}_3((\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})\delta^2) = 0.$$

Observe that $(\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})\delta^2 = (\delta^4 + \delta^2)\delta^2 = \delta^6 + \delta^4$ if $i = 1$, and it equals $(\delta^2 + \delta)\delta^2 = \delta^4 + \delta^3$ if $i = 2$. Thus, no matter which case we arrive at $\mathrm{tr}_3(\delta^3 + \delta) = 0$. By $\mathrm{tr}_3(\delta^3) = \mathrm{tr}_3(\delta)$ and $\delta^7 = 1$ we have $\delta^3 + \delta^6 + \delta^5 = \delta + \delta^2 + \delta^4$ which leads to $\delta = 0, 1$, a contradiction with $\delta^{2/i} + \delta^{1/i} \neq 0$. Therefore, if $\delta^{2/i} + \delta^{1/i} \neq 0$, then there is no solution $r \in \mathbb{F}_{2^3}$ to (45) and $L^i_{a,b,\delta}(u) = 0$ if and only if $\phi_i(u) = 0$. This completes the proof. □

Proposition 23. Let $a, b \in \mathbb{F}_{2^n}$ with $ab \neq 0$ and $\delta^2 = \mathrm{tr}_n^3(ba^{-1})$. Then $L^i_{a,b,\delta}(u) = 0$ defined by (41) has at most four roots in $\mathbb{F}_{2^n}$ for any $i \in \{1, 2\}$.

Proof. If $\theta_i = 0$, i.e., $\delta^{2/i} + \delta^{1/i} = 0$, then (41) is reduced to $bu^2 + (bu)^{2^{-1}} = 0$ which has at most four roots in $\mathbb{F}_{2^n}$ for any nonzero b. Next we consider the case $\theta_i \neq 0$. By Proposition 22, for this case we have $L^i_{a,b,\delta}(u) = 0$ if and only if $\phi_i(u) = 0$. Thus, to complete the proof, it suffices to show that $\phi_i(u) = 0$ has at most four roots in $\mathbb{F}_{2^n}$ for any $i \in \{1, 2\}$. If $\phi_i(u) = 0$ has no nonzero solution for some θ_i and b, then the desired result follows. Now let v be any fixed nonzero solution of $\phi_i(u) = 0$. Then for any u satisfying $\phi_i(u) = 0$ we have

$$u(u+v)\phi_i(v) + v(u+v)\phi_i(u) + uv\phi_i(u+v) = 0.$$

A direct calculation based on (43) gives

$$\begin{aligned} \theta_i^{\frac{1}{2}}(u^2v^{\frac{9}{2}} + v^2u^{\frac{9}{2}} + u^5v^{\frac{3}{2}} + v^5u^{\frac{3}{2}}) = \\ \theta_i^{\frac{1}{4}}(u^2v^{\frac{9}{4}} + v^2u^{\frac{9}{4}} + u^3v^{\frac{5}{4}} + v^3u^{\frac{5}{4}}), \end{aligned} \tag{47}$$

which can be written as

$$\theta_i^{\frac{1}{4}}(u^4v + uv^4)(u^{\frac{1}{2}}v + uv^{\frac{1}{2}}) = (u^2v + uv^2)(u^{\frac{1}{4}}v + uv^{\frac{1}{4}}) \tag{48}$$

since $\theta_i \neq 0$. Then, let $u = vz$, one obtains that

$$\theta_i^{\frac{1}{4}}v^{\frac{9}{4}}(z^4 + z)(z^{\frac{1}{2}} + z) = (z^2 + z)(z^{\frac{1}{4}} + z). \tag{49}$$

Note that v is a fixed nonzero element which means that z is uniquely determined by u. Thus, one can conclude that the number of solutions $z \in \mathbb{F}_{2^n}$ to (49) is no less than the number of solutions $u \in \mathbb{F}_{2^n}$ to $\phi_i(u) = 0$. Let $w = z^2 + z$ and rewrite (49) as

$$w\Omega_i(w) := \theta_i^{\frac{1}{4}}v^{\frac{9}{4}}(w^2 + w)w^{\frac{1}{2}} + w(w^{\frac{1}{2}} + w^{\frac{1}{4}}) = 0. \tag{50}$$

Observe that (48) holds for any u satisfying $\phi_i(u) = 0$ and the solution set of $\phi_i(u) = 0$ is an $\mathbb{F}_2$-linear space due to Proposition 22.

Then, one can conclude that the solution sets of both (49) and (50) are $\mathbb{F}_2$-linear spaces. Assume that w_1, w_2 and $w_1 + w_2$ are solutions of (50), then we have

$$0 = \Omega_i(w_1) + \Omega_i(w_2) + \Omega_i(w_1 + w_2) = \theta_i^{\frac{1}{4}} v^{\frac{9}{4}} (w_1^{\frac{1}{2}} w_2 + w_2^{\frac{1}{2}} w_1)$$

since (50) holds if and only if $\Omega_i(w) = 0$, which leads to $w_1 w_2^2 + w_2^2 w_1 = w_1 w_2 (w_1 + w_2) = 0$, i.e., $w_1 = 0$, $w_2 = 0$ or $w_1 = w_2$. This means that (50) has at most two distinct solutions in $\mathbb{F}_{2^n}$ and then (49) has at most four solutions in z since $w = z^2 + z$. This completes the proof. □

Theorem 10. The Walsh spectra of the functions F_1 and F_2 defined by (39) and (40), respectively, are $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ otherwise.

Proof. The Walsh transform of F_i, $i = 1, 2$, takes values from the set

$$\{0, \pm 2^{(n+1)/2}\}$$

if n is odd and takes values from the set

$$\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$$

if n is even. This follows from (42) and Proposition 23.

The Walsh transform takes all three values for n odd and all five values for n even since quadratic functions are plateaued and there exists no bent function from $\mathbb{F}_{2^n}$ to itself, while in the case of n even quadratic APN functions have some bent components. □

4.2.2 Walsh Spectrum of F_0

Bracken et al. in [9] had determined the Walsh spectrum of the APN function F_0 for the case of $a = 1$. In this section, we determine its

Walsh spectrum for any nonzero element $a \in \mathbb{F}_{2^n}$ by using the same techniques. By the definition, for any $b, c \in \mathbb{F}_{2^n}$, one gets

$$\begin{aligned} \mathrm{tr}_n(bF_0(x) + cx) &= \mathrm{tr}_n(bx^3 + ba^{-1}\mathrm{tr}_n(a^3x^9) + cx) \\ &= \mathrm{tr}_n(bx^3 + cx + \mathrm{tr}_n(ba^{-1})a^3x^9). \end{aligned}$$

For simplicity, let $\mathrm{tr}_n(ba^{-1}) = \delta$ and $g_0(x) = \mathrm{tr}_n(bF_0(x) + cx)$. Then, by a direct calculation, one obtains that

$$\begin{aligned} & g_0(x) + g_0(x+u) + g_0(u) \\ = \; & \mathrm{tr}_n(bx^2u + bxu^2 + \delta a^3x^8u + \delta a^3xu^8) \\ = \; & \mathrm{tr}_n\big(x((bu)^{2^{-1}} + bu^2 + (\delta a^3u)^{2^{-3}} + \delta a^3u^8)\big), \end{aligned} \tag{51}$$

which implies that

$$\begin{aligned} |\lambda_{F_0}(b,c)|^2 &= \sum_{x\in\mathbb{F}_{2^n}} \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_0(x)+g_0(x+u)} \\ &= \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_0(u)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}^n(xL^0_{a,b,\delta}(u))}, \end{aligned}$$

where $L^0_{a,b,\delta}(u)$ is defined as

$$L^0_{a,b,\delta}(u) = (bu)^{2^{-1}} + bu^2 + (\delta a^3u)^{2^{-3}} + \delta a^3u^8. \tag{52}$$

Note that $g_0(u) + g_0(u+v) + g_0(v) = \mathrm{tr}_n(vL^0_{a,b,\delta}(u))$ due to (51) and (52). This means that for any u satisfying $L^0_{a,b,\delta}(u) = 0$ and any $v \in \mathbb{F}_{2^n}$ we have

$$g_0(u+v) = g_0(u) + g_0(v)$$

which implies that

$$|\lambda_{F_0}(b,c)|^2 = 0, \text{ or } 2^n|\{x \in \mathbb{F}_{2^n} : L^0_{a,b,\delta}(u) = 0\}|. \tag{53}$$

Next we aim to determine the number of solutions to $L^0_{a,b,\delta}(u) = 0$ in order to determine the possible values of the Walsh spectrum of

$F_0(x)$. First, if $\delta = \mathrm{tr}_n(ba^{-1}) = 0$, then $L^0_{a,b,\delta}(u) = 0$ is reduced to $L^0_{a,b,0}(u) = (bu)^{2^{-1}} + bu^2 = 0$ which has at most 4 roots in $\mathbb{F}_{2^n}$. Now we assume that $\delta = \mathrm{tr}_n(ba^{-1}) = 1$, then $L^0_{a,b,\delta}(u) = 0$ is reduced to $L^0_{a,b,1}(u) = (bu)^{2^{-1}} + bu^2 + (a^3u)^{2^{-3}} + a^3u^8 = 0$, and it is straightforward to verify that

$$uL^0_{a,b,1}(u) = \phi_0(u) + \phi_0(u)^{2^{-1}}, \tag{54}$$

where $\phi_0(u)$ is defined by

$$\phi_0(u) = bu^3 + a^3u^9 + a^{\frac{3}{2}}u^{\frac{9}{2}} + a^{\frac{3}{4}}u^{\frac{9}{4}}.$$

Proposition 24. Let $a, b \in \mathbb{F}_{2^n}$ with $\delta = \mathrm{tr}_n(ba^{-1}) = 1$. Then $L^0_{a,b,1}(u) = 0$ if and only if $\phi_0(u) = 0$.

Proof. According to (54), we have $L^0_{a,b,1}(u) = 0$ if $\phi_0(u) = 0$; and $\phi_0(u) \in \mathbb{F}_2$ if $L^0_{a,b,1}(u) = 0$. Thus, to complete the proof, we need to show that $L^0_{a,b,1}(u) = 0$ implies that $\phi_0(u) = 0$. Suppose that $\phi_0(u) = 1$, one then gets $b = a^3u^6 + a^{3/2}u^{3/2} + a^{3/4}u^{-3/4} + u^{-3}$ which leads to

$$ba^{-1} = a^2u^6 + a^{\frac{1}{2}}u^{\frac{3}{2}} + a^{-\frac{1}{4}}u^{-\frac{3}{4}} + a^{-1}u^{-3}.$$

This contradicts the condition that $\mathrm{tr}_n(ba^{-1}) = 1$ and thus completes the proof. □

Proposition 25. Let $a, b \in \mathbb{F}_{2^n}$ with $ab \neq 0$ and $\delta = \mathrm{tr}_n(ba^{-1})$. Then $L^0_{a,b,\delta}(u) = 0$ defined by (52) has at most four roots in $\mathbb{F}_{2^n}$.

Proof. This can be proved in the same way as in Proposition 23. □

Theorem 11. The Walsh spectrum of the function F_0 defined by (38) is $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ otherwise.

Proof. The Walsh transform of F_0 takes values from $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and takes values from $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ if n is even. This follows from (53) and Proposition 25. The Walsh transform takes all three values for n odd and all 5 values for n even by the same reasons as in Theorem 1. □

4.3 Equivalence of Göloğlu's APN Trinomial to Gold Functions

In [56] the function

$$G(x) = x^{2^k+1} + \left(\mathrm{tr}_n^m(x)\right)^{2^k+1}$$

or, equivalently,

$$G(x) = x^{2^m(2^k+1)} + x^{2^k+2^m} + x^{2^{m+k}+1}$$

over $\mathbb{F}_{2^n}$ is shown to be APN, where $n = 2m = 4t$ for some natural t and $\gcd(k, n) = 1$. In [33] we show that this function is, in fact, affine equivalent to the Gold functions.

Although technical, the proof is straightforward and consists of constructing the affine permutations A_1 and A_2 from the Definition 16. These are defined to be

$$A_1(x) = \gamma^{2^k} x^{2^{m+k}} + \gamma x^{2^k}$$

and

$$A_2(x) = \gamma x^{2^m} + \gamma^{2^k} x,$$

where γ is a primitive element of $\mathbb{F}_{2^2}$.

Both A_1 and A_2 are evidently affine (even linear) functions. The fact that they are also permutations can be seen by observing that, e.g., $A_1(x) = 0$ can occur only for $x = 0$, which in turn is shown by contradiction. More precisely, if we assume that $A_1(x) = A_1(x)^{2^m}$ for some nonzero $x \neq 0$, we can obtain the equations

$$\begin{aligned}\gamma^{2^k} x^{2^{m+k}} &= \gamma x^{2^k}, \\ \gamma^{2^{m+k}} x^{2^k} &= \gamma^{2^m} x^{2^{m+k}}.\end{aligned}$$

Multiplying both sides of the above two equations by one another yields

$$\gamma^{2^k+2^{m+k}} = \gamma^{2^m+1}. \tag{55}$$

Due to γ being a primitive element of $\mathbb{F}_{2^2}$ and $\gcd(k, n) = 1$ with $n = 4t$, we have $\gamma^{2^k} = \gamma^2$, and therefore also

$$\gamma^{2^k+2^{m+k}} = \gamma^4 = \gamma$$

and

$$\gamma^{2^m+1} = \gamma^2$$

so that (55) becomes

$$\gamma = \gamma^2$$

which then contradicts γ being primitive over $\mathbb{F}_{2^2}$.

The remainder of the proof consists of applying A_1 and A_2 to the function

$$G'(x) = G(x)^{2^m} = x^{2^k+1} + x^{2^k+2^m} + x^{2^{m+k}+1}$$

which is clearly affine-equivalent to G. In particular, we show that for

$$L_2'(x) = L_2(x^{2^m})$$

we have

$$L_1(x)^{2^{m-k}+1} = L_2 \circ G'(x) = L_2'(x) \circ G(x)$$

which then implies that G is affine-equivalent to $x^{2^{m-k}+1}$.

4.4 Classification of Quadratic APN Polynomials in Few Terms in Small Dimensions

As discussed in Chapter 3, APN functions have been completely classified up to CCZ-equivalence for all finite fields of dimension $n \leqslant 5$ [13], as well as for $n = 6$ in the case of quadratic APN functions. The classification of APN functions over fields of dimension $n \geqslant 6$ in the general case remains an open problem, and since the number of functions (as well as their complexity) exponentially increases with the dimension of the field, searching for new APN functions is a challenging problem.

We utilize an experimental approach to search for new APN functions over $\mathbb{F}_{2^n}$ with $n \in \{6, 7, 8, 9, 10, 11\}$. Our method is based on constructing polynomials of a given form, testing whether they are APN or not, and then comparing the ones that are APN against all known representatives of the infinite monomial APN families. Provided the new function is not equivalent to any monomial family, we compare it against the switching classes from [53] for $6 \leqslant n \leqslant 8$ or against the CCZ-inequivalent representatives from Table 24 for $9 \leqslant n \leqslant 11$, thereby either classifying the found functions into one of those families, or concluding that a candidate for a new APN function (inequivalent to any of the known classes) is found.

4.4.1 Experimental Procedure

In our experiments, we examine all quadratic trinomials, quadrinomials, pentanomials, and hexanomials with all coefficients equal to one, i.e., we examine all

- quadratic trinomials of the form
$$F(x) = x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)},$$
- quadratic quadrinomials of the form
$$F(x) = x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)} + x^{2^{j_4}(2^{i_4}+1)},$$

- quadratic pentanomials of the form

$$\begin{aligned} F(x) &= x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)} + \\ &\quad x^{2^{j_4}(2^{i_4}+1)} + x^{2^{j_5}(2^{i_5}+1)}, \text{ and} \end{aligned}$$

- quadratic hexanomials of the form

$$\begin{aligned} F(x) &= x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)} \\ &\quad x^{2^{j_4}(2^{i_4}+1)} + x^{2^{j_5}(2^{i_5}+1)} + x^{2^{j_6}(2^{i_6}+1)}. \end{aligned}$$

In order to make the search more efficient, we impose some restrictions on the numbers i_k and j_k which prevent redundant computations. For instance, in the case of quadratic trinomials, the following restrictions are used:

- if n is even, then $i_1 \leqslant i_2, i_3 \leqslant \frac{n}{2}$;
- if n is odd, then $i_1 \leqslant i_2, i_3 \leqslant \frac{n-1}{2}$;
- $0 \leqslant j_2, j_3 \leqslant n-1$;
- $2^{i_1+1} < 2^{j_2}(2^{i_2}+1) < 2^{j_3}(2^{i_3}+1) \mod (2^n-1)$.

Similar conditions are used in the remaining three cases as well.

All such trinomials, etc. are tested for being APN over $\mathbb{F}_{2^n}$ with $6 \leqslant n \leqslant 11$. The following general procedure is used for the search:

- a polynomial F is constructed as discussed above;
- if F is not APN, we ignore it and continue the search;
- otherwise, we check whether F is CCZ-equivalent to one of the families of power APN functions; if so, we ignore it;
- otherwise, we test F for CCZ-equivalence against the known polynomial APN classes from [53] (for $6 \leqslant n \leqslant 8$) or against the representatives from Table 24 (for $n \geqslant 9$); thus we either classify F into one of the families, or have a candidate for a new APN function.

4.4.2 Experimental Results

There are 8438413 polynomials in total satisfying the above conditions. They include 7962 trinomials, 93710 quadrinomials, 909011 pentanomials and 7427730 hexanomials. Among them, there are 437 APN functions which are CCZ-inequivalent to infinite power families. We classified them in Tables 15, 16, 17 and 18 and chose a representative from each class in Tables 19, 20, 21, 22.

Table 15: *Classification of Quadratic APN Trinomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n	Family NO.	Functions	CCZ equivalent to
6	-	-	-
7	7.1	$x^{20}+x^6+x^3$ $x^{65}+x^{10}+x^3$	Tbl. 7: 8.1
	7.2	$x^{34}+x^{18}+x^5$	Tbl. 7: 2.1
8	8.1	$x^{72}+x^6+x^3$ $x^{132}+x^{24}+x^3$ $x^{144}+x^{96}+x^3$ $x^{129}+x^{36}+x^3$ $x^{66}+x^9+x^3$ $x^{132}+x^{36}+x^3$ $x^{144}+x^{72}+x^3$	Tbl. 9: 1.3
	8.2	$x^{144}+x^6+x^3$ $x^{36}+x^{24}+x^3$ $x^{132}+x^{96}+x^3$ $x^{12}+x^9+x^3$ $x^{129}+x^{72}+x^3$ $x^{192}+x^{66}+x^3$ $x^{72}+x^{36}+x^3$ $x^{144}+x^{132}+x^3$	Tbl. 9: 1.4
9	–	–	–
10	–	–	–
11	–	–	–

Furthermore, we found 5 new CCZ-inequivalent APN functions which are CCZ-inequivalent to known infinite families of APN functions. They are listed in Table 23.

Table 16: *Classification of Quadratic APN Quadrinomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n	Family NO.	Functions	CCZ equivalent to
6	-	-	-
7	7.1	$x^{72}+x^{40}+x^{12}+x^3$ $x^{96}+x^{18}+x^{10}+x^3$	Tbl. 7: 12.1
	7.2	$x^{33}+x^{17}+x^{12}+x^3$ $x^{96}+x^{40}+x^{36}+x^3$	Tbl. 7: 10.1
	7.3	$x^{34}+x^{33}+x^{10}+x^3$ $x^{34}+x^{33}+x^{17}+x^3$	Tbl. 7: 2.2
	7.4	$x^{66}+x^{34}+x^{20}+x^3$	Tbl. 7: 11.1
	7.5	$x^{68}+x^{18}+x^5+x^3$	Tbl. 7: 8.1
	7.6	$x^{66}+x^{18}+x^9+x^3$	Tbl. 7: 9.1
8	–	–	–
9	–	–	–
10	–	–	–
11	–	–	–

Table 17: *Classification of Quadratic APN Pentanomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n	Family NO.	Functions	CCZ equivalent to
6	-	-	-
7	7.1	$x^{68}+x^{40}+x^{24}+x^6+x^3$ $x^{65}+x^{34}+x^{20}+x^{12}+x^3$ $x^{80}+x^{66}+x^{36}+x^6+x^3$ $x^{96}+x^{72}+x^{48}+x^5+x^3$ $x^{66}+x^{36}+x^{24}+x^5+x^3$ $x^{80}+x^{68}+x^{48}+x^{40}+x^3$ $x^{34}+x^{33}+x^{10}+x^5+x^3$ $x^{65}+x^{40}+x^{33}+x^{18}+x^3$ $x^{40}+x^{34}+x^{20}+x^{17}+x^3$ $x^{68}+x^{36}+x^{33}+x^{18}+x^3$	Tbl. 7: 13.1
	7.2	$x^{40}+x^{36}+x^{12}+x^6+x^3$ $x^{36}+x^{33}+x^{20}+x^{12}+x^3$ $x^{65}+x^{20}+x^{18}+x^6+x^3$ $x^{36}+x^{18}+x^{12}+x^{10}+x^3$ $x^{96}+x^{40}+x^9+x^5+x^3$ $x^{96}+x^{65}+x^{10}+x^9+x^3$ $x^{80}+x^{66}+x^{10}+x^9+x^3$ $x^{96}+x^{68}+x^{66}+x^9+x^3$	Tbl. 7: 1.2
	7.3	$x^{96}+x^{34}+x^{20}+x^{12}+x^3$ $x^{96}+x^{72}+x^{24}+x^5+x^3$ $x^{68}+x^{66}+x^{17}+x^{10}+x^3$ $x^{40}+x^{34}+x^{18}+x^{10}+x^3$ $x^{80}+x^{48}+x^{12}+x^9+x^3$	Tbl. 7: 12.1
	7.4	$x^{80}+x^{72}+x^{66}+x^{24}+x^3$ $x^{68}+x^{66}+x^{17}+x^6+x^3$ $x^{80}+x^{68}+x^{34}+x^{24}+x^3$ $x^{72}+x^{48}+x^{36}+x^{10}+x^3$ $x^{72}+x^{65}+x^{34}+x^{33}+x^3$ $x^{48}+x^{40}+x^{10}+x^9+x^3$ $x^{80}+x^{68}+x^{18}+x^{10}+x^5$ $x^{66}+x^{40}+x^{34}+x^9+x^5$ $x^{80}+x^{40}+x^{36}+x^{17}+x^5$	Tbl. 7: 2.1

Table 17: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
7	7.5	$x^{80}+x^{68}+x^{66}+x^{65}+x^3$ $x^{33}+x^9+x^6+x^5+x^3$ $x^{68}+x^{33}+x^{20}+x^{10}+x^3$	Tbl. 7: 11.1
	7.6	$x^{66}+x^{48}+x^{36}+x^{12}+x^3$ $x^{40}+x^{36}+x^{34}+x^{24}+x^3$ $x^{68}+x^{20}+x^6+x^5+x^3$ $x^{96}+x^{34}+x^{24}+x^{20}+x^3$ $x^{66}+x^{65}+x^{34}+x^{10}+x^3$ $x^{68}+x^{48}+x^{36}+x^5+x^3$ $x^{96}+x^{80}+x^{12}+x^9+x^3$	Tbl. 7: 10.1
	7.7	$x^{24}+x^{10}+x^9+x^6+x^3$ $x^{68}+x^{65}+x^{12}+x^5+x^3$ $x^{96}+x^{48}+x^{33}+x^{17}+x^3$ $x^{34}+x^{33}+x^{18}+x^9+x^3$	Tbl. 7: 2.2
	7.8	$x^{72}+x^{40}+x^{34}+x^6+x^3$ $x^{80}+x^{66}+x^{40}+x^{20}+x^3$ $x^{65}+x^{36}+x^{20}+x^{17}+x^3$	Tbl. 7: 14.1
	7.9	$x^{80}+x^{40}+x^{24}+x^{20}+x^3$ $x^{66}+x^{48}+x^{10}+x^5+x^3$ $x^{80}+x^{40}+x^{17}+x^5+x^3$ $x^{40}+x^{33}+x^{17}+x^5+x^3$	Tbl. 7: 8.1
	7.10	$x^{68}+x^{33}+x^{24}+x^{20}+x^3$ $x^{72}+x^{66}+x^{48}+x^{20}+x^3$ $x^{72}+x^{66}+x^{18}+x^{10}+x^3$ $x^{66}+x^{34}+x^{20}+x^{17}+x^3$ $x^{68}+x^{40}+x^{33}+x^{10}+x^5$ $x^{80}+x^{72}+x^{33}+x^{20}+x^5$ $x^{80}+x^{66}+x^{34}+x^{20}+x^5$ $x^{40}+x^{33}+x^{20}+x^{18}+x^5$ $x^{72}+x^{36}+x^{20}+x^{17}+x^5$ $x^{36}+x^{33}+x^{18}+x^9+x^5$ $x^{72}+x^{40}+x^{17}+x^9+x^5$ $x^{80}+x^{18}+x^{17}+x^9+x^5$	Tbl. 7: 10.2

Table 17: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
8	8.1	$x^{36}+x^{33}+x^{12}+x^6+x^3$ $x^{72}+x^{33}+x^{12}+x^6+x^3$ $x^{132}+x^{72}+x^{24}+x^6+x^3$ $x^{66}+x^{36}+x^{24}+x^{12}+x^3$ $x^{144}+x^{12}+x^9+x^6+x^3$ $x^{144}+x^{129}+x^{18}+x^6+x^3$ $x^{144}+x^{129}+x^{36}+x^6+x^3$ $x^{132}+x^{129}+x^{72}+x^6+x^3$ $x^{132}+x^{96}+x^{18}+x^{12}+x^3$ $x^{132}+x^{96}+x^{66}+x^{12}+x^3$ $x^{144}+x^{96}+x^{36}+x^{24}+x^3$ $x^{132}+x^{96}+x^{72}+x^{24}+x^3$ $x^{192}+x^{144}+x^9+x^6+x^3$ $x^{129}+x^{66}+x^{36}+x^{12}+x^3$ $x^{192}+x^{66}+x^{36}+x^{24}+x^3$ $x^{192}+x^{144}+x^{33}+x^{24}+x^3$ $x^{192}+x^{132}+x^{33}+x^{24}+x^3$ $x^{36}+x^{33}+x^9+x^6+x^3$ $x^{144}+x^{66}+x^{36}+x^{12}+x^3$ $x^{144}+x^{66}+x^{33}+x^{24}+x^3$ $x^{144}+x^{96}+x^{12}+x^9+x^3$ $x^{132}+x^{129}+x^{96}+x^{72}+x^3$ $x^{192}+x^{144}+x^{96}+x^9+x^3$ $x^{96}+x^{36}+x^{24}+x^{18}+x^3$ $x^{144}+x^{132}+x^{129}+x^{18}+x^3$ $x^{192}+x^{129}+x^{72}+x^9+x^3$ $x^{192}+x^{129}+x^{72}+x^{18}+x^3$ $x^{192}+x^{129}+x^{66}+x^{36}+x^3$ $x^{192}+x^{144}+x^{36}+x^9+x^3$ $x^{96}+x^{72}+x^{36}+x^{18}+x^3$ $x^{66}+x^{33}+x^{18}+x^9+x^3$	Tbl. 9: 1.4

Table 17: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
8	8.2	$x^{72}+x^{66}+x^{12}+x^6+x^3$ $x^{144}+x^{66}+x^{48}+x^{12}+x^3$ $x^{48}+x^{24}+x^{18}+x^6+x^3$ $x^{192}+x^{96}+x^{66}+x^6+x^3$ $x^{144}+x^{96}+x^{33}+x^{24}+x^3$ $x^{129}+x^{36}+x^{33}+x^6+x^3$ $x^{96}+x^{36}+x^{18}+x^{12}+x^3$ $x^{192}+x^{144}+x^{36}+x^{12}+x^3$ $x^{132}+x^{36}+x^{33}+x^6+x^3$ $x^{144}+x^{132}+x^{18}+x^{12}+x^3$ $x^{144}+x^{72}+x^{33}+x^{12}+x^3$ $x^{144}+x^{72}+x^{33}+x^{24}+x^3$ $x^{144}+x^{72}+x^{66}+x^{48}+x^3$ $x^{144}+x^{132}+x^{66}+x^{48}+x^3$ $x^{129}+x^{24}+x^{12}+x^9+x^3$ $x^{129}+x^{96}+x^{48}+x^{33}+x^3$ $x^{192}+x^{132}+x^{24}+x^9+x^3$ $x^{192}+x^{144}+x^{129}+x^{18}+x^3$ $x^{72}+x^{66}+x^{48}+x^9+x^3$ $x^{132}+x^{66}+x^{48}+x^9+x^3$ $x^{144}+x^{72}+x^{48}+x^{36}+x^3$ $x^{144}+x^{132}+x^{48}+x^{36}+x^3$ $x^{192}+x^{48}+x^{36}+x^9+x^3$ $x^{72}+x^{48}+x^{36}+x^9+x^3$ $x^{132}+x^{48}+x^{36}+x^9+x^3$ $x^{144}+x^{129}+x^{66}+x^{18}+x^3$ $x^{96}+x^{36}+x^{18}+x^9+x^3$ $x^{192}+x^{72}+x^{36}+x^{18}+x^3$ $x^{192}+x^{132}+x^{36}+x^{33}+x^3$	Tbl. 9: 1.3
	8.3	$x^{130}+x^{66}+x^{40}+x^{12}+x^3$ $x^{192}+x^{160}+x^{144}+x^{10}+x^3$	Tbl. 9: 6.1
	8.4	$x^{66}+x^{40}+x^{18}+x^5+x^3$	Tbl. 9: 5.1
9	-	-	-
10	-	-	-

Table 17: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
11	11.1	$x^{12}+x^{10}+x^9+x^5+x^3$ $x^{1536}+x^{1026}+x^{514}+x^{513}+x^3$	New
	11.2	$x^{258}+x^{257}+x^{18}+x^{17}+x^3$	New
	11.3	$x^{96}+x^{66}+x^{34}+x^{33}+x^3$ $x^{192}+x^{130}+x^{129}+x^{65}+x^3$	New
	11.4	$x^{80}+x^{68}+x^{65}+x^{17}+x^5$	New
	11.5	$x^{260}+x^{257}+x^{36}+x^{33}+x^5$	New

Table 18: *Classification of Quadratic APN Hexanomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n	Family NO.	Functions	CCZ equivalent to
6	-	-	-
7	7.1	$x^{68}+x^{48}+x^{40}+x^{24}+x^6+x^3$ $x^{65}+x^{34}+x^{24}+x^{20}+x^{12}+x^3$ $x^{80}+x^{48}+x^{36}+x^{33}+x^6+x^3$ $x^{66}+x^{65}+x^{48}+x^{36}+x^{24}+x^3$ $x^{80}+x^{66}+x^{65}+x^{17}+x^6+x^3$ $x^{66}+x^{36}+x^{12}+x^9+x^6+x^3$ $x^{68}+x^{65}+x^{33}+x^{18}+x^6+x^3$ $x^{72}+x^{40}+x^{36}+x^{17}+x^{12}+x^3$ $x^{34}+x^{33}+x^{12}+x^6+x^5+x^3$ $x^{96}+x^{72}+x^{48}+x^6+x^5+x^3$ $x^{48}+x^{34}+x^{24}+x^{10}+x^5+x^3$ $x^{96}+x^{72}+x^{65}+x^{40}+x^{33}+x^3$ $x^{40}+x^{36}+x^{34}+x^{10}+x^5+x^3$ $x^{80}+x^{65}+x^{40}+x^{24}+x^{18}+x^3$ $x^{72}+x^{68}+x^{66}+x^{48}+x^{34}+x^3$ $x^{68}+x^{36}+x^{24}+x^{20}+x^{18}+x^3$ $x^{72}+x^{33}+x^{20}+x^{10}+x^9+x^3$ $x^{96}+x^{36}+x^{18}+x^{10}+x^9+x^3$ $x^{80}+x^{72}+x^{34}+x^{20}+x^{18}+x^3$ $x^{96}+x^{80}+x^{65}+x^{34}+x^9+x^3$ $x^{72}+x^{68}+x^{40}+x^{34}+x^{10}+x^5$ $x^{72}+x^{68}+x^{66}+x^{34}+x^{20}+x^5$ $x^{68}+x^{40}+x^{36}+x^{18}+x^{10}+x^5$ $x^{72}+x^{40}+x^{18}+x^{17}+x^{10}+x^5$ $x^{40}+x^{36}+x^{34}+x^{17}+x^{10}+x^5$ $x^{80}+x^{72}+x^{68}+x^{34}+x^{33}+x^5$ $x^{72}+x^{40}+x^{36}+x^{10}+x^9+x^5$ $x^{68}+x^{40}+x^{17}+x^{10}+x^9+x^5$ $x^{72}+x^{66}+x^{36}+x^{20}+x^9+x^5$ $x^{68}+x^{66}+x^{36}+x^{20}+x^{18}+x^5$ $x^{68}+x^{66}+x^{36}+x^{20}+x^{18}+x^5$ $x^{40}+x^{34}+x^{18}+x^{10}+x^9+x^5$ $x^{80}+x^{72}+x^{36}+x^{33}+x^9+x^5$	Tbl. 7: 14.2

Table 18: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
7	7.1	$x^{80}+x^{68}+x^{36}+x^{33}+x^{18}+x^5$ $x^{66}+x^{36}+x^{34}+x^{20}+x^{17}+x^5$ $x^{80}+x^{36}+x^{34}+x^{33}+x^{17}+x^5$ $x^{68}+x^{66}+x^{20}+x^{17}+x^9+x^5$ $x^{72}+x^{66}+x^{20}+x^{18}+x^{17}+x^5$ $x^{66}+x^{34}+x^{20}+x^{18}+x^9+x^5$ $x^{80}+x^{34}+x^{33}+x^{18}+x^9+x^5$ $x^{80}+x^{68}+x^{33}+x^{17}+x^9+x^5$ $x^{80}+x^{72}+x^{33}+x^{18}+x^{17}+x^5$	Tbl. 7: 14.2
	7.2	$x^{96}+x^{72}+x^{66}+x^{48}+x^{24}+x^3$ $x^{66}+x^{40}+x^{34}+x^{24}+x^6+x^3$ $x^{68}+x^{65}+x^{24}+x^{20}+x^6+x^3$ $x^{96}+x^{72}+x^{33}+x^{20}+x^{12}+x^3$ $x^{72}+x^{48}+x^{36}+x^{33}+x^{24}+x^3$ $x^{48}+x^{40}+x^{12}+x^9+x^6+x^3$ $x^{68}+x^{48}+x^{20}+x^9+x^6+x^3$ $x^{65}+x^{33}+x^{20}+x^{17}+x^{12}+x^3$ $x^{68}+x^{66}+x^{18}+x^{17}+x^{12}+x^3$ $x^{96}+x^{65}+x^{34}+x^{12}+x^{10}+x^3$ $x^{80}+x^{48}+x^{34}+x^{12}+x^5+x^3$ $x^{68}+x^{65}+x^{34}+x^{24}+x^{10}+x^3$ $x^{48}+x^{36}+x^{34}+x^6+x^5+x^3$ $x^{72}+x^{68}+x^{40}+x^{33}+x^5+x^3$ $x^{96}+x^{40}+x^{24}+x^{18}+x^5+x^3$ $x^{80}+x^{66}+x^{48}+x^{17}+x^5+x^3$ $x^{96}+x^{48}+x^{40}+x^{36}+x^5+x^3$ $x^{40}+x^{24}+x^{20}+x^9+x^5+x^3$ $x^{48}+x^{40}+x^{34}+x^{24}+x^{18}+x^3$ $x^{66}+x^{65}+x^{24}+x^{18}+x^{17}+x^3$ $x^{68}+x^{40}+x^{33}+x^{18}+x^{17}+x^3$ $x^{96}+x^{80}+x^{68}+x^{36}+x^{17}+x^3$	Tbl. 7: 14.1
	7.3	$x^{80}+x^{66}+x^{34}+x^{24}+x^6+x^3$ $x^{33}+x^{24}+x^{20}+x^{18}+x^{12}+x^3$ $x^{65}+x^{40}+x^{33}+x^{17}+x^{12}+x^3$	Tbl. 7: 12.1

Table 18: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
7	7.3	$x^{72}+x^{33}+x^{18}+x^9+x^6+x^3$ $x^{68}+x^{66}+x^{40}+x^{12}+x^5+x^3$ $x^{96}+x^{68}+x^{40}+x^6+x^5+x^3$ $x^{66}+x^{65}+x^{48}+x^{34}+x^{20}+x^3$ $x^{72}+x^{68}+x^{24}+x^{17}+x^5+x^3$ $x^{96}+x^{48}+x^{40}+x^{36}+x^{10}+x^3$ $x^{96}+x^{80}+x^{33}+x^{17}+x^{10}+x^3$ $x^{72}+x^{66}+x^{36}+x^9+x^5+x^3$ $x^{80}+x^{72}+x^{48}+x^{18}+x^9+x^3$ $x^{80}+x^{68}+x^{65}+x^{36}+x^9+x^3$	Tbl. 7: 14.2
	7.4	$x^{80}+x^{72}+x^{68}+x^{48}+x^{12}+x^3$ $x^{24}+x^{17}+x^{12}+x^{10}+x^6+x^3$ $x^{72}+x^{68}+x^{48}+x^{40}+x^{12}+x^3$ $x^{96}+x^{66}+x^{65}+x^{36}+x^6+x^3$ $x^{96}+x^{68}+x^{66}+x^{36}+x^{24}+x^3$ $x^{72}+x^{65}+x^{12}+x^6+x^5+x^3$ $x^{80}+x^{40}+x^{18}+x^6+x^5+x^3$ $x^{96}+x^{68}+x^{36}+x^{24}+x^5+x^3$ $x^{96}+x^{18}+x^{17}+x^{12}+x^{10}+x^3$ $x^{68}+x^{40}+x^{34}+x^{17}+x^{10}+x^3$ $x^{96}+x^{65}+x^{48}+x^{33}+x^{18}+x^3$ $x^{66}+x^{65}+x^{40}+x^{20}+x^9+x^3$ $x^{80}+x^{68}+x^{34}+x^{20}+x^9+x^3$	Tbl. 7: 2.1
	7.5	$x^{68}+x^{24}+x^{12}+x^{10}+x^6+x^3$ $x^{80}+x^{68}+x^{66}+x^{20}+x^{12}+x^3$ $x^{96}+x^{66}+x^{65}+x^{17}+x^6+x^3$ $x^{80}+x^{66}+x^{20}+x^{17}+x^{12}+x^3$ $x^{65}+x^{34}+x^{12}+x^6+x^5+x^3$ $x^{96}+x^{72}+x^{65}+x^{48}+x^{33}+x^3$ $x^{96}+x^{80}+x^{36}+x^{20}+x^5+x^3$ $x^{96}+x^{80}+x^{20}+x^{17}+x^5+x^3$ $x^{40}+x^{34}+x^{18}+x^{17}+x^5+x^3$ $x^{72}+x^{66}+x^{20}+x^{17}+x^9+x^3$	Tbl. 7: 1.2
	7.6	$x^{68}+x^{66}+x^{65}+x^{40}+x^{12}+x^3$	Tbl. 7: 11.1

Table 18: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
7	7.6	$x^{96}+x^{80}+x^{68}+x^{33}+x^6+x^3$ $x^{72}+x^{68}+x^{34}+x^{20}+x^6+x^3$ $x^{96}+x^{68}+x^{40}+x^{34}+x^{12}+x^3$ $x^{68}+x^{36}+x^{20}+x^9+x^6+x^3$ $x^{68}+x^{34}+x^{20}+x^9+x^6+x^3$ $x^{96}+x^{80}+x^{72}+x^{34}+x^{12}+x^3$ $x^{80}+x^{24}+x^9+x^6+x^5+x^3$ $x^{66}+x^{24}+x^{18}+x^{12}+x^5+x^3$ $x^{48}+x^{40}+x^{18}+x^{10}+x^5+x^3$ $x^{96}+x^{80}+x^{48}+x^{17}+x^{10}+x^3$ $x^{96}+x^{72}+x^{24}+x^{17}+x^{10}+x^3$ $x^{68}+x^{65}+x^{34}+x^{18}+x^{10}+x^3$ $x^{68}+x^{65}+x^{34}+x^{17}+x^{10}+x^3$ $x^{65}+x^{36}+x^{34}+x^{17}+x^{10}+x^3$ $x^{80}+x^{66}+x^{40}+x^{24}+x^{17}+x^3$ $x^{66}+x^{48}+x^{34}+x^{12}+x^9+x^3$ $x^{48}+x^{33}+x^{18}+x^{12}+x^9+x^3$ $x^{80}+x^{65}+x^{48}+x^{40}+x^{34}+x^3$ $x^{96}+x^{72}+x^{24}+x^{20}+x^{18}+x^3$	Tbl. 7: 11.1
	7.7	$x^{68}+x^{65}+x^{33}+x^{10}+x^6+x^3$ $x^{66}+x^{20}+x^{12}+x^9+x^6+x^3$ $x^{96}+x^{66}+x^{34}+x^{33}+x^{10}+x^3$ $x^{96}+x^{66}+x^{34}+x^{33}+x^{20}+x^3$ $x^{96}+x^{80}+x^{65}+x^{34}+x^5+x^3$ $x^{40}+x^{12}+x^{10}+x^9+x^5+x^3$ $x^{80}+x^{12}+x^{10}+x^9+x^5+x^3$ $x^{34}+x^{33}+x^{18}+x^{10}+x^9+x^3$	Tbl. 7: 2.2
	7.8	$x^{68}+x^{65}+x^{33}+x^{20}+x^6+x^3$ $x^{66}+x^{40}+x^{12}+x^9+x^6+x^3$ $x^{34}+x^{24}+x^{10}+x^9+x^6+x^3$ $x^{96}+x^{80}+x^{66}+x^{36}+x^{24}+x^3$ $x^{68}+x^{48}+x^{40}+x^{12}+x^{10}+x^3$ $x^{68}+x^{65}+x^{17}+x^{12}+x^5+x^3$ $x^{96}+x^{66}+x^{17}+x^{12}+x^{10}+x^3$	Tbl. 7: 9.1

Table 18: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
7	7.8	$x^{36}+x^{34}+x^9+x^6+x^5+x^3$ $x^{80}+x^{68}+x^{12}+x^{10}+x^5+x^3$ $x^{80}+x^{40}+x^{34}+x^{10}+x^5+x^3$ $x^{96}+x^{80}+x^{65}+x^{34}+x^{10}+x^3$ $x^{68}+x^{48}+x^{34}+x^9+x^5+x^3$ $x^{72}+x^{40}+x^{36}+x^{24}+x^{18}+x^3$ $x^{96}+x^{66}+x^{33}+x^{20}+x^{17}+x^3$ $x^{96}+x^{48}+x^{36}+x^{33}+x^{17}+x^3$ $x^{68}+x^{66}+x^{65}+x^{18}+x^{17}+x^3$	Tbl. 7: 9.1
	7.9	$x^{66}+x^{65}+x^{18}+x^{10}+x^6+x^3$ $x^{48}+x^{40}+x^{33}+x^{18}+x^{12}+x^3$ $x^{36}+x^{20}+x^{12}+x^6+x^5+x^3$ $x^{96}+x^{68}+x^{40}+x^{12}+x^{10}+x^3$ $x^{80}+x^{20}+x^{17}+x^6+x^5+x^3$ $x^{72}+x^{66}+x^{65}+x^{40}+x^{10}+x^3$ $x^{72}+x^{68}+x^{34}+x^{20}+x^5+x^3$ $x^{96}+x^{66}+x^{24}+x^{17}+x^{10}+x^3$ $x^{96}+x^{65}+x^{33}+x^9+x^5+x^3$ $x^{34}+x^{33}+x^{20}+x^{17}+x^{10}+x^3$ $x^{68}+x^{18}+x^{17}+x^{10}+x^9+x^3$	Tbl. 7: 13.1
	7.10	$x^{36}+x^{33}+x^{24}+x^9+x^6+x^3$ $x^{80}+x^{68}+x^{65}+x^{18}+x^{12}+x^3$ $x^{96}+x^{40}+x^{33}+x^{17}+x^{12}+x^3$ $x^{68}+x^{33}+x^{17}+x^9+x^6+x^3$ $x^{68}+x^{48}+x^{33}+x^{12}+x^5+x^3$ $x^{96}+x^{40}+x^{36}+x^{24}+x^{10}+x^3$ $x^{72}+x^{33}+x^{24}+x^{20}+x^{10}+x^3$ $x^{40}+x^{36}+x^{17}+x^{10}+x^5+x^3$ $x^{80}+x^{72}+x^{68}+x^{65}+x^{34}+x^3$ $x^{96}+x^{68}+x^{48}+x^{20}+x^{17}+x^3$ $x^{66}+x^{48}+x^{33}+x^{20}+x^9+x^3$ $x^{68}+x^{66}+x^{40}+x^{34}+x^9+x^3$	Tbl. 7: 10.1
	7.11	$x^{68}+x^{48}+x^{20}+x^{18}+x^{12}+x^3$ $x^{72}+x^{68}+x^{66}+x^{34}+x^{12}+x^3$	Tbl. 7: 10.2

Table 18: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
7	7.11	$x^{96}+x^{68}+x^{17}+x^{12}+x^5+x^3$ $x^{40}+x^{36}+x^{20}+x^{10}+x^5+x^3$ $x^{80}+x^{66}+x^{34}+x^{20}+x^{10}+x^3$ $x^{72}+x^{36}+x^{34}+x^9+x^5+x^3$ $x^{96}+x^{36}+x^{33}+x^{24}+x^{17}+x^3$ $x^{80}+x^{68}+x^{66}+x^{36}+x^{18}+x^3$ $x^{96}+x^{80}+x^{72}+x^{18}+x^{17}+x^3$	Tbl. 7: 10.2
	7.12	$x^{96}+x^{66}+x^{36}+x^{18}+x^{12}+x^3$ $x^{96}+x^{40}+x^{36}+x^{34}+x^{24}+x^3$ $x^{68}+x^{48}+x^{36}+x^{12}+x^5+x^3$ $x^{72}+x^{48}+x^{17}+x^{12}+x^{10}+x^3$ $x^{48}+x^{18}+x^9+x^6+x^5+x^3$ $x^{80}+x^{68}+x^{20}+x^{10}+x^5+x^3$ $x^{80}+x^{72}+x^{68}+x^{33}+x^{20}+x^3$ $x^{72}+x^{68}+x^{40}+x^{18}+x^5+x^3$ $x^{68}+x^{66}+x^{65}+x^{24}+x^9+x^3$ $x^{72}+x^{48}+x^{40}+x^{24}+x^{17}+x^3$ $x^{96}+x^{33}+x^{17}+x^{12}+x^9+x^3$ $x^{96}+x^{80}+x^{68}+x^{24}+x^9+x^3$ $x^{36}+x^{34}+x^{20}+x^{10}+x^9+x^3$ $x^{72}+x^{34}+x^{33}+x^{20}+x^{17}+x^3$	Tbl. 7: 8.1
8	8.1	$x^{136}+x^{72}+x^{33}+x^{12}+x^6+x^3$ $x^{160}+x^{80}+x^{34}+x^{24}+x^{12}+x^3$ $x^{192}+x^{136}+x^{40}+x^{20}+x^6+x^3$ $x^{144}+x^{136}+x^{130}+x^{40}+x^6+x^3$ $x^{136}+x^{132}+x^{96}+x^{18}+x^{12}+x^3$ $x^{144}+x^{129}+x^{68}+x^{36}+x^6+x^3$ $x^{144}+x^{96}+x^{68}+x^{36}+x^{24}+x^3$ $x^{192}+x^{132}+x^{34}+x^{33}+x^{24}+x^3$ $x^{160}+x^{136}+x^{36}+x^{24}+x^{10}+x^3$ $x^{129}+x^{96}+x^{68}+x^{20}+x^{10}+x^3$ $x^{129}+x^{72}+x^{68}+x^{65}+x^{20}+x^3$ $x^{144}+x^{132}+x^{80}+x^{68}+x^5+x^3$ $x^{80}+x^{72}+x^{36}+x^{17}+x^5+x^3$	Tbl. 9: 1.4

Table 18: *(continued)*

n	Family NO.	Functions	CCZ equivalent to
8	8.1	$x^{68}+x^{34}+x^{17}+x^{12}+x^9+x^3$ $x^{192}+x^{129}+x^{72}+x^{34}+x^{18}+x^3$ $x^{132}+x^{96}+x^{65}+x^{20}+x^{17}+x^3$ $x^{192}+x^{136}+x^{68}+x^{66}+x^{17}+x^3$	Tbl. 9: 5.1
	8.2	$x^{72}+x^{40}+x^{34}+x^{20}+x^{12}+x^3$ $x^{192}+x^{136}+x^{18}+x^{10}+x^5+x^3$ $x^{160}+x^{136}+x^{132}+x^{33}+x^5+x^3$ $x^{132}+x^{80}+x^{68}+x^{40}+x^{10}+x^5$ $x^{160}+x^{144}+x^{136}+x^{65}+x^{10}+x^5$ $x^{130}+x^{66}+x^{40}+x^{34}+x^{20}+x^5$ $x^{160}+x^{130}+x^{80}+x^{72}+x^{68}+x^5$	Tbl. 9: 6.1
	8.3	$x^{160}+x^{132}+x^{80}+x^{68}+x^6+x^3$ $x^{129}+x^{80}+x^{66}+x^{40}+x^{34}+x^3$ $x^{72}+x^{66}+x^{34}+x^{18}+x^{10}+x^5$ $x^{130}+x^{36}+x^{33}+x^{17}+x^9+x^5$ $x^{160}+x^{136}+x^{68}+x^{17}+x^9+x^5$ $x^{136}+x^{72}+x^{68}+x^{40}+x^{34}+x^5$	Tbl. 9: 4.1
9	-	-	-
10	-	-	-
11	-	-	-

Table 19: *Representatives for Quadratic APN Trinomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n		Functions	Families from Tables 13	Relation to [53]
6	–	–	–	–
7	7.1	$x^{20}+x^6+x^3$	–	Tbl. 7 : 8.1
	7.2	$x^{34}+x^{18}+x^5$	–	7 : 2.1
8	8.1	$x^{72}+x^6+x^3$	$N°5$	Tbl. 9 : 1.3
	8.2	$x^{72}+x^{36}+x^3$	–	9 : 1.4
9	–	–	–	–
10	–	–	–	–
11	–	–	–	–

Table 20: *Representatives for Quadratic APN Quadrinomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n		Functions	Families from Tables 13	Relation to [53]
6	–	–	–	–
7	7.1	$x^{72}+x^{40}+x^{12}+x^3$	–	Tbl. 7 : 12.1
	7.2	$x^{33}+x^{17}+x^{12}+x^3$	–	7 : 10.1
	7.3	$x^{34}+x^{33}+x^{10}+x^3$	–	7 : 2.2
	7.4	$x^{66}+x^{34}+x^{20}+x^3$	–	7 : 11.1
	7.5	$x^{68}+x^{18}+x^5+x^3$	–	7 : 8.1
	7.6	$x^{66}+x^{18}+x^9+x^3$	–	7 : 9.1
8	–	–	–	–
9	–	–	–	–
10	–	–	–	–
11	–	–	–	–

Table 21: *Representatives for Quadratic APN Pentanomials (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n		Functions	Families from Tables 13	Relation to [53]
6	–	–	–	–
7	7.1	$x^{68}+x^{40}+x^{24}+x^6+x^3$	–	Tbl. 7 : 13.1
	7.2	$x^{65}+x^{20}+x^{18}+x^6+x^3$	$N°5$	7 : 1.2
	7.3	$x^{40}+x^{34}+x^{18}+x^{10}+x^3$	–	7 : 12.1
	7.4	$x^{48}+x^{40}+x^{10}+x^9+x^3$	–	7 : 2.1
	7.5	$x^{33}+x^9+x^6+x^5+x^3$	–	7 : 11.1
	7.6	$x^{40}+x^{36}+x^{34}+x^{24}+x^3$	–	7 : 10.1
	7.7	$x^{24}+x^{10}+x^9+x^6+x^3$	–	7 : 2.2
	7.8	$x^{65}+x^{36}+x^{20}+x^{17}+x^3$	–	7 : 14.1
	7.9	$x^{40}+x^{33}+x^{17}+x^5+x^3$	–	7 : 8.1
	7.10	$x^{36}+x^{33}+x^{18}+x^9+x^5$	–	7 : 10.2
8	8.1	$x^{36}+x^{33}+x^9+x^6+x^3$	–	Tbl. 9 : 1.4
	8.2	$x^{72}+x^{66}+x^{12}+x^6+x^3$	$N°5$	9 : 1.3
	8.3	$x^{130}+x^{66}+x^{40}+x^{12}+x^3$	–	9 : 6.1
	8.4	$x^{66}+x^{40}+x^{18}+x^5+x^3$	–	9 : 5.1
9	–	–	–	–
10	–	–	–	–
11	11.1	$x^{12}+x^{10}+x^9+x^5+x^3$	–	–
	11.2	$x^{258}+x^{257}+x^{18}+x^{17}+x^3$	–	–
	11.3	$x^{96}+x^{66}+x^{34}+x^{33}+x^3$	–	–
	11.4	$x^{80}+x^{68}+x^{65}+x^{17}+x^5$	–	–
	11.5	$x^{260}+x^{257}+x^{36}+x^{33}+x^5$	–	–

Table 22: *Representatives for Quadratic APN Hexanomial (CCZ-inequivalent to infinite monomial families) in Small Dimensions with Coefficients Equal to* 1

n		Functions	Families from Table 13	Relation to [53]
6	–	–	–	–
7	7.1	$x^{34}+x^{33}+x^{12}+x^6+x^5+x^3$	–	Tbl. 7 : 14.2
	7.2	$x^{40}+x^{24}+x^{20}+x^9+x^5+x^3$	–	7 : 14.1
	7.3	$x^{33}+x^{24}+x^{20}+x^{18}+x^{12}+x^3$	–	7 : 12.1
	7.4	$x^{24}+x^{17}+x^{12}+x^{10}+x^6+x^3$	–	7 : 2.1
	7.5	$x^{40}+x^{34}+x^{18}+x^{17}+x^5+x^3$	$N°5$	7 : 1.2
	7.6	$x^{48}+x^{40}+x^{18}+x^{10}+x^5+x^3$	–	7 : 11.1
	7.7	$x^{40}+x^{12}+x^{10}+x^9+x^5+x^3$	–	7 : 2.2
	7.8	$x^{34}+x^{24}+x^{10}+x^9+x^6+x^3$	–	7 : 9.1
	7.9	$x^{34}+x^{33}+x^{20}+x^{17}+x^{10}+x^3$	–	7 : 13.1
	7.10	$x^{36}+x^{33}+x^{24}+x^9+x^6+x^3$	–	7 : 10.1
	7.11	$x^{40}+x^{36}+x^{20}+x^{10}+x^5+x^3$	–	7 : 10.2
	7.12	$x^{36}+x^{34}+x^{20}+x^{10}+x^9+x^3$	–	7 : 8.1
8	8.1	$x^{68}+x^{34}+x^{17}+x^{12}+x^9+x^3$	–	Tbl. 9 : 5.1
	8.2	$x^{72}+x^{40}+x^{34}+x^{20}+x^{12}+x^3$	$N°5$	9 : 6.1
	8.3	$x^{72}+x^{66}+x^{34}+x^{18}+x^{10}+x^5$	–	9 : 4.1
9	–	–	–	–
10	–	–	–	–
11	–	–	–	–

Table 23: *New APN Polynomials (up to CCZ-equivalence) over* $\mathbb{F}_{2^{11}}$

Classes No.	Polynomials
1	$x^{12}+x^{10}+x^9+x^5+x^3$ $x^{1536}+x^{1026}+x^{514}+x^{513}+x^3$
2	$x^{258}+x^{257}+x^{18}+x^{17}+x^3$
3	$x^{96}+x^{66}+x^{34}+x^{33}+x^3$ $x^{192}+x^{130}+x^{129}+x^{65}+x^3$
4	$x^{80}+x^{68}+x^{65}+x^{17}+x^5$ $x^{640}+x^{516}+x^{132}+x^{129}+x^5$
5	$x^{260}+x^{257}+x^{36}+x^{33}+x^5$

4.5 On the Equivalence of the Known Families of APN Functions in Small Dimensions

When searching for new APN functions, we are in fact looking for functions that are CCZ-inequivalent to the known ones. Even in the case when we want to compare a potentially new function against the known infinite families, this can be a difficult process requiring a lot of computation. For this reason, reducing the complexity of this comparison procedure is crucial when searching for new functions.

Note that comparing a given function F against only one representative of some particular infinite family is not enough, as the individual functions from the family do not necessarily have to belong to the same CCZ-equivalence class. Thus, any candidate F must be compared to all members of the family, which can be a considerable number of functions even for fields of moderately large dimension. For example, there are 45012 functions in family No. 3 from Table 13 over $\mathbb{F}_{2^{10}}$. In fact, all of the functions from family No. 3 for $n = 10$ fall into two distinct CCZ-equivalence classes; however, all of these 45012 functions have to be compared against one another for equivalence to come to this conclusion which is a very demanding computational task by itself.

For this reason, we compared all members of the known infinite APN families against one another and selected the "simplest" representative from each equivalence class. When selecting such a "simplest" representative, we prefer polynomial expressions consisting of fewer terms, and coefficients corresponding to smaller powers of the primitive element. In particular, we always select a power function as a representative if one is available.

In the following Table 24 we present our computational results. We only consider fields $\mathbb{F}_{2^n}$ of dimension $n \geqslant 6$ because all APN functions for $n \leqslant 5$ are CCZ-equivalent to power functions [34]. For each dimension between 6 and 11, we list a single representative from

each CCZ-equivalence class along with the family to which it belongs and it's switching class as described in [53] for dimensions $6 \leqslant n \leqslant 8$.

A more detailed overview of the computational results for the infinite polynomial APN families is presented in Table 25. The procedure that we use to generate the results in the table is the following: for every dimension $6 \leqslant n \leqslant 11$, we examine every family from Table 13 beginning with family No. 1 and ending with family No. 11. For every family, we compare all of its member functions against one another for CCZ-equivalence and partition the family into CCZ-equivalence classes, selecting a representative from each. We then compare these representatives to the ones from the previously examined families to determine whether the representatives from the newly processed family belong to one of the already encountered equivalence classes or not.

For every family and every dimension, we label the corresponding cell with "New" if we have encountered the corresponding CCZ-equivalence class for the first time, and we label it with the number of a family from Table 13 if it is CCZ-equivalent to the functions from that family. If the cell corresponding to a given family and dimension contains a dash, then functions from this family do not exist for the given dimension. Note also that some cells may include more than one representative since some of the families are not contained within a single CCZ-equivalence class.

For example, for dimension $n = 6$ we begin by observing that all the functions from family No. 1 are CCZ-equivalent to the Gold functions. Functions from family No. 2 do not exist in this case, so we proceed to Family No. 3. All of its functions fall into one CCZ-equivalence class which, however, does not coincide with that of the Gold functions; we, therefore, label this as a new CCZ-equivalence class and proceed to family No. 4.

Table 24: *CCZ-inequivalent APN Functions over* $\mathbb{F}_{2^n}$ *from the Known APN Classes for* $6 \leqslant n \leqslant 11$

n		Functions*	Families from Tables 12,13	Relation to [53]
6	6.1	x^3	Gold	Tbl. 5: 1.1
	6.2	$x^6 + x^9 + a^7x^{48}$	3	5: 1.2
	6.3	$ax^3 + a^4x^{24} + x^{17}$	8-10	5: 2.3
7	7.1	x^3	Gold	Tbl. 7 : 1.1
	7.2	x^5	Gold	7 : 3.1
	7.3	x^9	Gold	7 : 4.1
	7.4	x^{13}	Kasami	7 : 5.1
	7.5	x^{57}	Kasami	7 : 6.1
	7.6	x^{63}	Inverse	7 : 7.1
	7.7	$x^3 + \mathrm{tr}_7(x^9)$	5	7 : 1.2
8	8.1	x^3	Gold	Tbl. 9 : 1.1
	8.2	x^9	Gold	9 : 1.2
	8.3	x^{57}	Kasami	9 : 7.1
	8.4	$x^3 + x^{17} + a^{48}x^{18} + a^3x^{33} + ax^{34} + x^{48}$	4	9 : 2.1
	8.5	$x^3 + \mathrm{tr}_8(x^9)$	5	9 : 1.3
	8.6	$x^3 + a^{-1}\mathrm{tr}_8(a^3x^9)$	5	9 : 1.5
	8.7	$(x + x^{16})^3 + a^{17}(ax + a^{16}x^{16})^{12} + a(x + x^{16})(ax + a^{16}x^{16})$	11	None
9	9.1	x^3	Gold	
	9.2	x^5	Gold	
	9.3	x^{17}	Gold	
	9.4	x^{13}	Kasami	
	9.5	x^{241}	Kasami	
	9.6	x^{19}	Welch	
	9.7	x^{255}	Inverse	
	9.8	$x^3 + \mathrm{tr}_9(x^9)$	5	
	9.9	$x^3 + \mathrm{tr}_9^3(x^9 + x^{18})$	6	
	9.10	$x^3 + \mathrm{tr}_9^3(x^{18} + x^{36})$	7	

10	10.1	x^3	Gold	
	10.2	x^9	Gold	
	10.3	x^{57}	Kasami	
	10.4	x^{339}	Dobbertin	
	10.5	$x^6 + x^{33} + a^{31}x^{192}$	3	
	10.6	$x^{72} + x^{33} + a^{31}x^{258}$	3	
	10.7	$x^3 + \mathrm{tr}_{10}(x^9)$	5	
	10.8	$x^3 + a^{-1}\mathrm{tr}_{10}(a^3x^9)$	5	
11	11.1	x^3	Gold	
	11.2	x^5	Gold	
	11.3	x^9	Gold	
	11.4	x^{17}	Gold	
	11.5	x^{33}	Gold	
	11.6	x^{13}	Kasami	
	11.7	x^{57}	Kasami	
	11.8	x^{241}	Kasami	
	11.9	x^{993}	Kasami	
	11.10	x^{35}	Welch	
	11.11	x^{287}	Niho	
	11.12	x^{1023}	Inverse	
	11.13	$x^3 + \mathrm{tr}_{11}(x^9)$	5	

* : a is primitive in $\mathbb{F}_{2^n}^*$

We see that all of its functions are CCZ-equivalent to the ones from family No. 3. Family No. 5 is equivalent to the Gold functions, etc. Ultimately, we only find three distinct CCZ-equivalence classes for $n = 6$ (corresponding to families Nos. 1, 3 and 8).

Table 25: *CCZ-equivalence of Families of APN Polynomials over* $\mathbb{F}_{2^n}$ *from Table 13 for* $6 \leqslant n \leqslant 11$

	Functions*	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$	$n=11$
1	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$, $p=3$	Gold	–	–	–	–	–
2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$, $p=4$	–	–	–	–	–	–
3	$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	New	–	–	–	New I ($i=1$, $c=u^{31}$, $b=1$) New II ($i=3$, $c=u^{31}$, $b=1$)	–
4	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$N^\circ 3$	–	New	–	$N^\circ 3$: Case I ($i=1$, $c=u^3$, $s=u$) $N^\circ 3$: Case II ($i=3$, $c=u^3$, $s=w$)	–
5	$x^3+a^{-1}\mathrm{tr}_n(a^3x^9)$	Gold ($a=1$) $N^\circ 3$ ($a=u$)	New	New I ($a=1$) New II ($a=u$)	New	New I ($a=1$) New II ($a=u$)	New
6	$x^3+a^{-1}\mathrm{tr}_n^3(a^3x^9+a^6x^{18})$	Gold ($a=1$) $N^\circ 3$ ($a=u$)	–	–	New	–	–
7	$x^3+a^{-1}\mathrm{tr}_n^3(a^6x^{18}+a^{12}x^{36})$	Gold ($a=1$) $N^\circ 3$ ($a=u$)	–	–	New	–	–
8	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$, $v=0, w\neq 0$	New	–	–	–	–	–
9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$, $v\neq 0, w=0$	$N^\circ 8$	–	–	–	–	–
10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$, $v\neq 0, w\neq 0$	$N^\circ 8$	–	–	–	–	–
11	$(x+x^{2^m})^{2^k+1}+$ $u^{(2^n-1)/(2^m-1)}(ux+$ $u^{2^m}x^{2^m})^{(2^k+1)2^i}+$ $u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	–	–	New ($i=2$) $N^\circ 4$ ($i=0$)	–	–	–

u : primitive in $\mathbb{F}_{2^n}^*$

* : for the conditions for each family, please reference Table 13

– : doesn't exist

New : CCZ-inequivalent to other infinite families

4.6 Other Results

Table 26 gives the inverses of monomial APN functions from the infinite families for fields of odd dimensions n in the range $3 \leqslant n \leqslant 129$. The table allows to quickly and conveniently determine the inverse of an APN power permutation. The exponent of the inverses is given via the smallest representative of its cyclotomic coset, and in the case that this inverse belongs to an infinite monomial family itself, this is indicated in the table. We note that the problem of computing the inverse of APN exponents is theoretically treated in [69] where explicit formulas for the inverses of the Welch and Dobbertin exponents are derived. The same problem for the remaining monomial families appears to be more difficult, with only partial theoretical results on the inverses of the Gold and Kasami exponents being available at the time of writing. Table 26 hopefully fills this gap for most reasonable values of n.

In order to generate the table, for every dimension n we consider every infinite APN monomial family of functions. Furthermore, we consider all exponents e such that x^e is APN over $\mathbb{F}_{2^n}$, and we compute the exponent i such that x^i is the compositional inverse of x^e. We then list i as the product of the smallest number from its cyclotomic coset and a power of two.

The actual data for the table was computed using the Magma programming language, and the results were aggregated using a simple Python script.

5 Conclusion

We presented a systematic overview of several different classes of cryptographically optimal functions, their constructions and properties. We also gave a summary of original results concerning the construction and properties of APN functions. Some of them in particular focus on the problem of the maximum algebraic degree of an APN function. We compiled a table of CCZ-inequivalent representatives from the known infinite APN classes for the fields $\mathbb{F}_{2^n}$ with $n \in \{6, 7, 8, 9, 10, 11\}$ which greatly simplifies the process of checking whether a given APN function over one of these fields is CCZ-equivalent to one of these known classes. An experimental procedure for classifying the quadratic polynomial APN functions of a particular type over the fields $\mathbb{F}_{2^n}$ with $n \in \{6, 7, 8, 9, 10, 11\}$ was described and a brief summary of the experimental results was given. In addition, a number of tables and other reference materials were presented throughout the thesis.

6 Future Work

One of the most important problems addressed by our research is the existence of an APN function of algebraic degree n. We investigated this problem by means of a construction involving changing the value of a given function in one point. An interesting question that remains open is whether this construction can be generalized by changing the value of a given function at multiple points, and whether results in this direction can be used to provide additional insight into the maximum algebraic degree of an APN function or the distance between two APN functions over a given finite field.

The experimental procedure for classifying quadratic APN polynomials can be extended by running it over fields of dimension greater than 11 (although this would, of course, be much more computationally intensive) as well as generalized to polynomials of a different form. The same is true for the table of CCZ-inequivalent representatives.

Table 26: *APN Power Permutations and Its Inverses for odd n and* $3 \leqslant n \leqslant 129$

n	F	F's Family	F^{-1}	F^{-1}'s Family
3	x^3	Gold ($i = 1$), Welch, Niho, Inverse	$x^{3 \cdot 2^2}$	Gold
5	x^3	Gold ($i = 1$)	$x^{13 \cdot 2^2}$	Kasami ($i = 2$)
	x^5	Gold ($i = 2$), Niho	$x^{7 \cdot 2^3}$	Welch
	x^{15}	Inverse, Dobbertin	$x^{15 \cdot 2^2}$	
7	x^3	Gold ($i = 1$)	$x^{43 \cdot 2^6}$	
	x^5	Gold ($i = 2$)	$x^{27 \cdot 2^4}$	
	x^9	Gold ($i = 3$)	$x^{15 \cdot 2^4}$	
	x^{13}	Kasami ($i = 2$)	$x^{11 \cdot 2^3}$	Welch
	x^{57}	Kasami ($i = 3$)	$x^{39 \cdot 2}$	Niho
	x^{63}	Inverse	$x^{63 \cdot 2^2}$	
9	x^3	Gold ($i = 1$)	$x^{171 \cdot 2^8}$	
	x^5	Gold ($i = 2$)	$x^{103 \cdot 2^7}$	
	x^{17}	Gold ($i = 4$)	$x^{31 \cdot 2^5}$	
	x^{13}	Kasami ($i = 2$)	$x^{59 \cdot 2}$	
	x^{241}	Kasami ($i = 4$)	$x^{87 \cdot 2^5}$	
	x^{19}	Welch, Niho	$x^{27 \cdot 2^8}$	
	x^{255}	Inverse	$x^{255 \cdot 2^2}$	
11	x^3	Gold ($i = 1$)	$x^{683 \cdot 2^{10}}$	
	x^5	Gold ($i = 2$)	$x^{411 \cdot 2^8}$	
	x^9	Gold ($i = 3$)	$x^{231 \cdot 2^6}$	
	x^{17}	Gold ($i = 4$)	$x^{365 \cdot 2^5}$	
	x^{33}	Gold ($i = 5$)	$x^{63 \cdot 2^6}$	
	x^{13}	Kasami ($i = 2$)	x^{315}	
	x^{57}	Kasami ($i = 3$)	$x^{413 \cdot 2}$	
	x^{241}	Kasami ($i = 4$)	$x^{43 \cdot 2^4}$	
	x^{993}	Kasami ($i = 5$)	$x^{151 \cdot 2^2}$	
	x^{35}	Welch	x^{117}	
	x^{287}	Niho	$x^{107 \cdot 2^9}$	
	x^{1023}	Inverse	$x^{1023 \cdot 2^2}$	
13	x^3	Gold ($i = 1$)	$x^{2731 \cdot 2^{12}}$	
	x^5	Gold ($i = 2$)	$x^{1639 \cdot 2^{11}}$	
	x^9	Gold ($i = 3$)	$x^{911 \cdot 2^{10}}$	
	x^{17}	Gold ($i = 4$)	$x^{1453 \cdot 2^6}$	
	x^{33}	Gold ($i = 5$)	$x^{1243 \cdot 2^7}$	

Table 26: *(continued)*

n	F	F's Family	F^{-1}
13	x^{65}	Gold ($i = 6$)	$x^{127 \cdot 2^7}$
	x^{13}	Kasami ($i = 2$)	$x^{635 \cdot 2^7}$
	x^{57}	Kasami ($i = 3$)	$x^{723 \cdot 2^5}$
	x^{241}	Kasami ($i = 4$)	$x^{171 \cdot 2^5}$
	x^{993}	Kasami ($i = 5$)	$x^{1691 \cdot 2^{10}}$
	x^{4033}	Kasami ($i = 6$)	$x^{1245 \cdot 2^{12}}$
	x^{67}	Welch	$x^{367 \cdot 2^9}$
	x^{71}	Niho	$x^{347 \cdot 2^7}$
	x^{4095}	Inverse	$x^{4095 \cdot 2^2}$
15	x^{3}	Gold ($i = 1$)	$x^{10923 \cdot 2^{14}}$
	x^{5}	Gold ($i = 2$)	$x^{6555 \cdot 2^{12}}$
	x^{17}	Gold ($i = 4$)	$x^{1935 \cdot 2^8}$
	x^{129}	Gold ($i = 7$)	$x^{255 \cdot 2^8}$
	x^{13}	Kasami ($i = 2$)	$x^{2523 \cdot 2^{10}}$
	x^{241}	Kasami ($i = 4$)	$x^{3671 \cdot 2^{14}}$
	x^{16257}	Kasami ($i = 7$)	$x^{4791 \cdot 2^8}$
	x^{131}	Welch	$x^{4815 \cdot 2^2}$
	x^{2175}	Niho	$x^{1371 \cdot 2^8}$
	x^{16383}	Inverse	$x^{16383 \cdot 2^2}$
	x^{4679}	Dobbertin	$x^{5851 \cdot 2}$
17	x^{3}	Gold ($i = 1$)	$x^{43691 \cdot 2^{16}}$
	x^{5}	Gold ($i = 2$)	$x^{26215 \cdot 2^{15}}$
	x^{9}	Gold ($i = 3$)	$x^{14567 \cdot 2^{12}}$
	x^{17}	Gold ($i = 4$)	$x^{7711 \cdot 2^{13}}$
	x^{33}	Gold ($i = 5$)	$x^{19867 \cdot 2^9}$
	x^{65}	Gold ($i = 6$)	$x^{22197 \cdot 2^7}$
	x^{129}	Gold ($i = 7$)	$x^{19309 \cdot 2^8}$
	x^{257}	Gold ($i = 8$)	$x^{511 \cdot 2^9}$
	x^{13}	Kasami ($i = 2$)	$x^{10083 \cdot 2^{14}}$
	x^{57}	Kasami ($i = 3$)	x^{4599}
	x^{241}	Kasami ($i = 4$)	$x^{20123 \cdot 2^{13}}$
	x^{993}	Kasami ($i = 5$)	$x^{26267 \cdot 2^{16}}$
	x^{4033}	Kasami ($i = 6$)	$x^{683 \cdot 2^6}$
	x^{16257}	Kasami ($i = 7$)	$x^{23373 \cdot 2^{12}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
17	x^{65281}	Kasami ($i = 8$)	$x^{9399 \cdot 2^2}$
	x^{259}	Welch	$x^{7591 \cdot 2^{15}}$
	x^{271}	Niho	$x^{1451 \cdot 2^{14}}$
	x^{65535}	Inverse	$x^{65535 \cdot 2^2}$
19	x^3	Gold ($i = 1$)	$x^{174763 \cdot 2^{18}}$
	x^5	Gold ($i = 2$)	$x^{104859 \cdot 2^{16}}$
	x^9	Gold ($i = 3$)	$x^{58255 \cdot 2^{16}}$
	x^{17}	Gold ($i = 4$)	$x^{92525 \cdot 2^{13}}$
	x^{33}	Gold ($i = 5$)	$x^{15903 \cdot 2^{10}}$
	x^{65}	Gold ($i = 6$)	$x^{88757 \cdot 2^8}$
	x^{129}	Gold ($i = 7$)	$x^{52851 \cdot 2^8}$
	x^{257}	Gold ($i = 8$)	$x^{75483 \cdot 2^{10}}$
	x^{513}	Gold ($i = 9$)	$x^{1023 \cdot 2^{10}}$
	x^{13}	Kasami ($i = 2$)	$x^{40331 \cdot 2^{15}}$
	x^{57}	Kasami ($i = 3$)	$x^{9207 \cdot 2^{10}}$
	x^{241}	Kasami ($i = 4$)	$x^{77229 \cdot 2}$
	x^{993}	Kasami ($i = 5$)	$x^{38551 \cdot 2^6}$
	x^{4033}	Kasami ($i = 6$)	$x^{2731 \cdot 2^7}$
	x^{16257}	Kasami ($i = 7$)	$x^{104909 \cdot 2^{18}}$
	x^{65281}	Kasami ($i = 8$)	$x^{79453 \cdot 2^{18}}$
	x^{261633}	Kasami ($i = 9$)	$x^{75485 \cdot 2^{18}}$
	x^{515}	Welch	$x^{31563 \cdot 2^8}$
	x^{16895}	Niho	$x^{5803 \cdot 2^{15}}$
	x^{262143}	Inverse	$x^{262143 \cdot 2^2}$
21	x^3	Gold ($i = 1$)	$x^{699051 \cdot 2^{20}}$
	x^5	Gold ($i = 2$)	$x^{419431 \cdot 2^{19}}$
	x^{17}	Gold ($i = 4$)	$x^{370093 \cdot 2^{14}}$
	x^{33}	Gold ($i = 5$)	$x^{63551 \cdot 2^{16}}$
	x^{257}	Gold ($i = 8$)	$x^{204007 \cdot 2^{11}}$
	x^{1025}	Gold ($i = 10$)	$x^{2047 \cdot 2^{11}}$
	x^{13}	Kasami ($i = 2$)	$x^{161339 \cdot 2^{13}}$
	x^{241}	Kasami ($i = 4$)	$x^{339373 \cdot 2^{19}}$
	x^{993}	Kasami ($i = 5$)	$x^{225977 \cdot 2^{19}}$
	x^{65281}	Kasami ($i = 8$)	$x^{233131 \cdot 2^{19}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
21	$x^{1047553}$	Kasami ($i = 10$)	$x^{300471 \cdot 2^{11}}$
	x^{1027}	Welch	$x^{169615 \cdot 2^4}$
	x^{1055}	Niho	$x^{21867 \cdot 2^{11}}$
	$x^{1048575}$	Inverse	$x^{1048575 \cdot 2^2}$
23	x^3	Gold ($i = 1$)	$x^{2796203 \cdot 2^{22}}$
	x^5	Gold ($i = 2$)	$x^{1677723 \cdot 2^{20}}$
	x^9	Gold ($i = 3$)	$x^{932071 \cdot 2^{18}}$
	x^{17}	Gold ($i = 4$)	$x^{493455 \cdot 2^{16}}$
	x^{33}	Gold ($i = 5$)	$x^{1271003 \cdot 2^{17}}$
	x^{65}	Gold ($i = 6$)	$x^{129087 \cdot 2^{12}}$
	x^{129}	Gold ($i = 7$)	$x^{845427 \cdot 2^{10}}$
	x^{257}	Gold ($i = 8$)	$x^{1403605 \cdot 2^9}$
	x^{513}	Gold ($i = 9$)	$x^{1357229 \cdot 2^{11}}$
	x^{1025}	Gold ($i = 10$)	$x^{1203053 \cdot 2^{11}}$
	x^{2049}	Gold ($i = 11$)	$x^{4095 \cdot 2^{12}}$
	x^{13}	Kasami ($i = 2$)	$x^{645435 \cdot 2^{12}}$
	x^{57}	Kasami ($i = 3$)	$x^{735843 \cdot 2^{19}}$
	x^{241}	Kasami ($i = 4$)	x^{69615}
	x^{993}	Kasami ($i = 5$)	$x^{363253 \cdot 2^{16}}$
	x^{4033}	Kasami ($i = 6$)	$x^{1271005 \cdot 2^4}$
	x^{16257}	Kasami ($i = 7$)	$x^{1677773 \cdot 2}$
	x^{65281}	Kasami ($i = 8$)	$x^{10923 \cdot 2^8}$
	x^{261633}	Kasami ($i = 9$)	$x^{1484205 \cdot 2^{16}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{1268077 \cdot 2^{11}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{599479 \cdot 2^2}$
	x^{2051}	Welch	$x^{494893 \cdot 2^{11}}$
	x^{133119}	Niho	$x^{87403 \cdot 2^{12}}$
	$x^{4194303}$	Inverse	$x^{4194303 \cdot 2^2}$
25	x^3	Gold ($i = 1$)	$x^{11184811 \cdot 2^{24}}$
	x^5	Gold ($i = 2$)	$x^{6710887 \cdot 2^{23}}$
	x^9	Gold ($i = 3$)	$x^{3728271 \cdot 2^{22}}$
	x^{17}	Gold ($i = 4$)	$x^{1973791 \cdot 2^{21}}$
	x^{65}	Gold ($i = 6$)	$x^{516223 \cdot 2^{19}}$
	x^{129}	Gold ($i = 7$)	$x^{4942189 \cdot 2^{12}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
25	x^{257}	Gold ($i = 8$)	$x^{5614293 \cdot 2^{10}}$
	x^{513}	Gold ($i = 9$)	$x^{5036467 \cdot 2^{11}}$
	x^{2049}	Gold ($i = 11$)	$x^{4798171 \cdot 2^{13}}$
	x^{4097}	Gold ($i = 12$)	$x^{8191 \cdot 2^{13}}$
	x^{13}	Kasami ($i = 2$)	$x^{2581115 \cdot 2^{19}}$
	x^{57}	Kasami ($i = 3$)	$x^{2943443 \cdot 2^{13}}$
	x^{241}	Kasami ($i = 4$)	$x^{139247 \cdot 2^{13}}$
	x^{4033}	Kasami ($i = 6$)	$x^{2471063 \cdot 2^{8}}$
	x^{16257}	Kasami ($i = 7$)	$x^{5921613 \cdot 2^{24}}$
	x^{65281}	Kasami ($i = 8$)	$x^{43691 \cdot 2^{9}}$
	x^{261633}	Kasami ($i = 9$)	$x^{6711707 \cdot 2^{22}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{1436437 \cdot 2^{20}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{4798173 \cdot 2^{24}}$
	x^{4099}	Welch	$x^{1727247 \cdot 2^{16}}$
	x^{4159}	Niho	$x^{88747 \cdot 2^{20}}$
	$x^{16777215}$	Inverse	$x^{16777215 \cdot 2^{2}}$
	$x^{1082399}$	Dobbertin	$x^{5682605 \cdot 2^{1}}$
27	x^{3}	Gold ($i = 1$)	$x^{44739243 \cdot 2^{26}}$
	x^{5}	Gold ($i = 2$)	$x^{26843547 \cdot 2^{24}}$
	x^{17}	Gold ($i = 4$)	$x^{23685485 \cdot 2^{21}}$
	x^{33}	Gold ($i = 5$)	$x^{20336027 \cdot 2^{19}}$
	x^{129}	Gold ($i = 7$)	$x^{1040511 \cdot 2^{14}}$
	x^{257}	Gold ($i = 8$)	$x^{13056231 \cdot 2^{14}}$
	x^{1025}	Gold ($i = 10$)	$x^{7463879 \cdot 2^{11}}$
	x^{2049}	Gold ($i = 11$)	$x^{21681845 \cdot 2^{12}}$
	x^{8193}	Gold ($i = 13$)	$x^{16383 \cdot 2^{14}}$
	x^{13}	Kasami ($i = 2$)	$x^{10324443 \cdot 2^{22}}$
	x^{241}	Kasami ($i = 4$)	$x^{19492269 \cdot 2^{13}}$
	x^{993}	Kasami ($i = 5$)	$x^{9664217 \cdot 2^{1}}$
	x^{16257}	Kasami ($i = 7$)	$x^{14456249 \cdot 2^{23}}$
	x^{65281}	Kasami ($i = 8$)	$x^{14913195 \cdot 2^{1}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{14914903 \cdot 2^{23}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{22729909 \cdot 2^{18}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{19180983 \cdot 2^{14}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
27	x^{8195}	Welch	$x^{7648527 \cdot 2^{19}}$
	$x^{1056767}$	Niho	$x^{354987 \cdot 2^{21}}$
	$x^{67108863}$	Inverse	$x^{67108863 \cdot 2^2}$
29	x^3	Gold ($i = 1$)	$x^{178956971 \cdot 2^{28}}$
	x^5	Gold ($i = 2$)	$x^{107374183 \cdot 2^{27}}$
	x^9	Gold ($i = 3$)	$x^{59652327 \cdot 2^{24}}$
	x^{17}	Gold ($i = 4$)	$x^{94741933 \cdot 2^{22}}$
	x^{33}	Gold ($i = 5$)	$x^{16268831 \cdot 2^{20}}$
	x^{65}	Gold ($i = 6$)	$x^{90855093 \cdot 2^{19}}$
	x^{129}	Gold ($i = 7$)	$x^{4161791 \cdot 2^{22}}$
	x^{257}	Gold ($i = 8$)	$x^{77292763 \cdot 2^{15}}$
	x^{513}	Gold ($i = 9$)	$x^{80583091 \cdot 2^{13}}$
	x^{1025}	Gold ($i = 10$)	$x^{89566037 \cdot 2^{11}}$
	x^{2049}	Gold ($i = 11$)	$x^{29607823 \cdot 2^{15}}$
	x^{4097}	Gold ($i = 12$)	$x^{52022899 \cdot 2^{13}}$
	x^{8193}	Gold ($i = 13$)	$x^{76733293 \cdot 2^{14}}$
	x^{16385}	Gold ($i = 14$)	$x^{32767 \cdot 2^{15}}$
	x^{13}	Kasami ($i = 2$)	$x^{41297763 \cdot 2^{26}}$
	x^{57}	Kasami ($i = 3$)	$x^{47094227 \cdot 2^{15}}$
	x^{241}	Kasami ($i = 4$)	$x^{77968813 \cdot 2^{18}}$
	x^{993}	Kasami ($i = 5$)	$x^{1081311 \cdot 2^0}$
	x^{4033}	Kasami ($i = 6$)	$x^{86727349 \cdot 2^1}$
	x^{16257}	Kasami ($i = 7$)	$x^{77309147 \cdot 2^{22}}$
	x^{65281}	Kasami ($i = 8$)	$x^{81344093 \cdot 2^4}$
	x^{261633}	Kasami ($i = 9$)	$x^{107375003 \cdot 2^{28}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{174763 \cdot 2^{10}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{31642323 \cdot 2^9}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{20825211 \cdot 2^{20}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{11032043 \cdot 2^4}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{38350263 \cdot 2^2}$
	x^{16387}	Welch	$x^{23686927 \cdot 2^{17}}$
	x^{16511}	Niho	$x^{1398187 \cdot 2^{15}}$
	$x^{268435455}$	Inverse	$x^{268435455 \cdot 2^2}$
31	x^3	Gold ($i = 1$)	$x^{715827883 \cdot 2^{30}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
31	x^{5}	Gold ($i = 2$)	$x^{429496731 \cdot 2^{28}}$
	x^{9}	Gold ($i = 3$)	$x^{238609295 \cdot 2^{28}}$
	x^{17}	Gold ($i = 4$)	$x^{126322575 \cdot 2^{24}}$
	x^{33}	Gold ($i = 5$)	$x^{65075263 \cdot 2^{26}}$
	x^{65}	Gold ($i = 6$)	$x^{363420341 \cdot 2^{20}}$
	x^{129}	Gold ($i = 7$)	$x^{316296045 \cdot 2^{22}}$
	x^{257}	Gold ($i = 8$)	$x^{8356095 \cdot 2^{16}}$
	x^{513}	Gold ($i = 9$)	$x^{347448749 \cdot 2^{15}}$
	x^{1025}	Gold ($i = 10$)	$x^{358263637 \cdot 2^{12}}$
	x^{2049}	Gold ($i = 11$)	$x^{214853427 \cdot 2^{12}}$
	x^{4097}	Gold ($i = 12$)	$x^{321310107 \cdot 2^{16}}$
	x^{8193}	Gold ($i = 13$)	$x^{207854823 \cdot 2^{16}}$
	x^{16385}	Gold ($i = 14$)	$x^{306820827 \cdot 2^{16}}$
	x^{32769}	Gold ($i = 15$)	$x^{65535 \cdot 2^{16}}$
	x^{13}	Kasami ($i = 2$)	$x^{165191051 \cdot 2^{27}}$
	x^{57}	Kasami ($i = 3$)	$x^{188375763 \cdot 2^{23}}$
	x^{241}	Kasami ($i = 4$)	$x^{187125403 \cdot 2^{15}}$
	x^{993}	Kasami ($i = 5$)	$x^{2162655 \cdot 2^{16}}$
	x^{4033}	Kasami ($i = 6$)	$x^{355162805 \cdot 2^{27}}$
	x^{16257}	Kasami ($i = 7$)	$x^{45044779 \cdot 2^{11}}$
	x^{65281}	Kasami ($i = 8$)	$x^{153986231 \cdot 2^{9}}$
	x^{261633}	Kasami ($i = 9$)	$x^{378971565 \cdot 2^{28}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{699051 \cdot 2^{11}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{429497549 \cdot 2^{30}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{196242589 \cdot 2^{6}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{75203835 \cdot 2^{29}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{323851981 \cdot 2^{13}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{306820829 \cdot 2^{30}}$
	x^{32771}	Welch	$x^{127062735 \cdot 2^{10}}$
	$x^{8421375}$	Niho	$x^{5592491 \cdot 2^{16}}$
	$x^{1073741823}$	Inverse	$x^{1073741823 \cdot 2^{2}}$
33	x^{3}	Gold ($i = 1$)	$x^{2863311531 \cdot 2^{32}}$
	x^{5}	Gold ($i = 2$)	$x^{1717986919 \cdot 2^{31}}$
	x^{17}	Gold ($i = 4$)	$x^{505290271 \cdot 2^{29}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
33	x^{33}	Gold ($i = 5$)	$x^{1301505243 \cdot 2^{27}}$
	x^{129}	Gold ($i = 7$)	$x^{865652339 \cdot 2^{22}}$
	x^{257}	Gold ($i = 8$)	$x^{33423871 \cdot 2^{25}}$
	x^{1025}	Gold ($i = 10$)	$x^{477684679 \cdot 2^{14}}$
	x^{8193}	Gold ($i = 13$)	$x^{1420647093 \cdot 2^{15}}$
	x^{16385}	Gold ($i = 14$)	$x^{1385608621 \cdot 2^{16}}$
	x^{65537}	Gold ($i = 16$)	$x^{131071 \cdot 2^{17}}$
	x^{13}	Kasami ($i = 2$)	$x^{660764219 \cdot 2^{25}}$
	x^{241}	Kasami ($i = 4$)	$x^{891072087 \cdot 2^{20}}$
	x^{993}	Kasami ($i = 5$)	$x^{614184665 \cdot 2^{19}}$
	x^{16257}	Kasami ($i = 7$)	$x^{723357351 \cdot 2^{26}}$
	x^{65281}	Kasami ($i = 8$)	$x^{920956361 \cdot 2^{28}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{954438999 \cdot 2^{32}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{1453939381 \cdot 2^{22}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{1389794741 \cdot 2^{30}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{1227189687 \cdot 2^{17}}$
	x^{65539}	Welch	$x^{497395471 \cdot 2^{23}}$
	x^{65791}	Niho	$x^{5614251 \cdot 2^{26}}$
	$x^{4294967295}$	Inverse	$x^{4294967295 \cdot 2^2}$
35	x^{3}	Gold ($i = 1$)	$x^{11453246123 \cdot 2^{34}}$
	x^{5}	Gold ($i = 2$)	$x^{6871947675 \cdot 2^{32}}$
	x^{9}	Gold ($i = 3$)	$x^{3817748711 \cdot 2^{30}}$
	x^{17}	Gold ($i = 4$)	$x^{6063483245 \cdot 2^{29}}$
	x^{65}	Gold ($i = 6$)	$x^{528611391 \cdot 2^{24}}$
	x^{257}	Gold ($i = 8$)	$x^{4946732763 \cdot 2^{26}}$
	x^{513}	Gold ($i = 9$)	$x^{66978303 \cdot 2^{18}}$
	x^{2049}	Gold ($i = 11$)	$x^{3437651763 \cdot 2^{14}}$
	x^{4097}	Gold ($i = 12$)	$x^{5728021845 \cdot 2^{13}}$
	x^{8193}	Gold ($i = 13$)	$x^{1010704143 \cdot 2^{14}}$
	x^{65537}	Gold ($i = 16$)	$x^{4908833645 \cdot 2^{17}}$
	x^{131073}	Gold ($i = 17$)	$x^{262143 \cdot 2^{18}}$
	x^{13}	Kasami ($i = 2$)	$x^{2643056955 \cdot 2^{24}}$
	x^{57}	Kasami ($i = 3$)	$x^{602804727 \cdot 2^{18}}$
	x^{241}	Kasami ($i = 4$)	$x^{712857643 \cdot 2^{28}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
35	x^{4033}	Kasami ($i = 6$)	$x^{17039295 \cdot 2^0}$
	x^{65281}	Kasami ($i = 8$)	$x^{5148092109 \cdot 2^{34}}$
	x^{261633}	Kasami ($i = 9$)	$x^{4946732765 \cdot 2^7}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{6871948493 \cdot 2^1}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{2796203 \cdot 2^{12}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{2023134871 \cdot 2^{10}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{5179333453 \cdot 2^{30}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{2454285751 \cdot 2^2}$
	x^{131075}	Welch	$x^{2021346123 \cdot 2^{16}}$
	$x^{67239935}$	Niho	$x^{22457003 \cdot 2^{27}}$
	$x^{17179869183}$	Inverse	$x^{17179869183 \cdot 2^2}$
	$x^{270549119}$	Dobbertin	$x^{5749168821 \cdot 2^1}$
37	x^3	Gold ($i = 1$)	$x^{45812984491 \cdot 2^{36}}$
	x^5	Gold ($i = 2$)	$x^{27487790695 \cdot 2^{35}}$
	x^9	Gold ($i = 3$)	$x^{15270994831 \cdot 2^{34}}$
	x^{17}	Gold ($i = 4$)	$x^{24253932973 \cdot 2^{30}}$
	x^{33}	Gold ($i = 5$)	$x^{20824083867 \cdot 2^{29}}$
	x^{65}	Gold ($i = 6$)	$x^{2114445439 \cdot 2^{31}}$
	x^{129}	Gold ($i = 7$)	$x^{13850437235 \cdot 2^{24}}$
	x^{257}	Gold ($i = 8$)	$x^{13369548007 \cdot 2^{27}}$
	x^{513}	Gold ($i = 9$)	$x^{267912191 \cdot 2^{28}}$
	x^{1025}	Gold ($i = 10$)	$x^{19710757741 \cdot 2^{18}}$
	x^{2049}	Gold ($i = 11$)	$x^{7579600783 \cdot 2^{19}}$
	x^{4097}	Gold ($i = 12$)	$x^{22912085333 \cdot 2^{14}}$
	x^{8193}	Gold ($i = 13$)	$x^{20616682291 \cdot 2^{15}}$
	x^{16385}	Gold ($i = 14$)	$x^{4034674207 \cdot 2^{19}}$
	x^{32769}	Gold ($i = 15$)	$x^{22728239829 \cdot 2^{16}}$
	x^{65537}	Gold ($i = 16$)	$x^{22168655541 \cdot 2^{17}}$
	x^{131073}	Gold ($i = 17$)	$x^{19634435803 \cdot 2^{19}}$
	x^{262145}	Gold ($i = 18$)	$x^{524287 \cdot 2^{19}}$
	x^{13}	Kasami ($i = 2$)	$x^{10572227195 \cdot 2^{31}}$
	x^{57}	Kasami ($i = 3$)	$x^{2411209719 \cdot 2^{28}}$
	x^{241}	Kasami ($i = 4$)	$x^{2851430571 \cdot 2^{29}}$
	x^{993}	Kasami ($i = 5$)	$x^{5952076405 \cdot 2^8}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
37	x^{4033}	Kasami ($i = 6$)	$x^{34078655 \cdot 2^{19}}$
	x^{16257}	Kasami ($i = 7$)	$x^{11066502243 \cdot 2^{8}}$
	x^{65281}	Kasami ($i = 8$)	$x^{14175280307 \cdot 2^{27}}$
	x^{261633}	Kasami ($i = 9$)	$x^{9855378615 \cdot 2^{11}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{20242979181 \cdot 2^{32}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{8100434643 \cdot 2^{13}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{11184811 \cdot 2^{13}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{27487803803 \cdot 2^{34}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{12510719133 \cdot 2^{8}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{22996667093 \cdot 2^{24}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{22235731637 \cdot 2^{17}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{20710209117 \cdot 2^{36}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{19634435805 \cdot 2^{36}}$
	x^{262147}	Welch	$x^{8096487055 \cdot 2^{12}}$
	x^{262655}	Niho	$x^{89478827 \cdot 2^{19}}$
	$x^{68719476735}$	Inverse	$x^{68719476735 \cdot 2^{2}}$
39	x^{3}	Gold ($i = 1$)	$x^{183251937963 \cdot 2^{38}}$
	x^{5}	Gold ($i = 2$)	$x^{109951162779 \cdot 2^{36}}$
	x^{17}	Gold ($i = 4$)	$x^{32338577295 \cdot 2^{32}}$
	x^{33}	Gold ($i = 5$)	$x^{16659267103 \cdot 2^{30}}$
	x^{129}	Gold ($i = 7$)	$x^{80971786605 \cdot 2^{26}}$
	x^{257}	Gold ($i = 8$)	$x^{91982490325 \cdot 2^{25}}$
	x^{1025}	Gold ($i = 10$)	$x^{536347647 \cdot 2^{20}}$
	x^{2049}	Gold ($i = 11$)	$x^{88808773301 \cdot 2^{18}}$
	x^{16385}	Gold ($i = 14$)	$x^{53448948167 \cdot 2^{17}}$
	x^{65537}	Gold ($i = 16$)	$x^{82249046451 \cdot 2^{18}}$
	x^{131073}	Gold ($i = 17$)	$x^{53204340339 \cdot 2^{18}}$
	x^{524289}	Gold ($i = 19$)	$x^{1048575 \cdot 2^{20}}$
	x^{13}	Kasami ($i = 2$)	$x^{42288908763 \cdot 2^{34}}$
	x^{241}	Kasami ($i = 4$)	$x^{57028611671 \cdot 2^{23}}$
	x^{993}	Kasami ($i = 5$)	$x^{57024017081 \cdot 2^{22}}$
	x^{16257}	Kasami ($i = 7$)	$x^{78691134829 \cdot 2^{37}}$
	x^{65281}	Kasami ($i = 8$)	$x^{90912959189 \cdot 2^{1}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{58940812745 \cdot 2^{32}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
39	$x^{4192257}$	Kasami ($i = 11$)	$x^{93035615413 \cdot 2^{36}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{61083986603 \cdot 2^{37}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{39651134939 \cdot 2^{29}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{46293814983 \cdot 2^{34}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{78536994231 \cdot 2^{20}}$
	x^{524291}	Welch	$x^{32338947373 \cdot 2^{19}}$
	$x^{537395199}$	Niho	$x^{357914283 \cdot 2^{20}}$
	$x^{274877906943}$	Inverse	$x^{274877906943 \cdot 2^{2}}$
41	x^{3}	Gold ($i = 1$)	$x^{733007751851 \cdot 2^{40}}$
	x^{5}	Gold ($i = 2$)	$x^{439804651111 \cdot 2^{39}}$
	x^{9}	Gold ($i = 3$)	$x^{244335917287 \cdot 2^{36}}$
	x^{17}	Gold ($i = 4$)	$x^{129354309151 \cdot 2^{37}}$
	x^{33}	Gold ($i = 5$)	$x^{66637068351 \cdot 2^{36}}$
	x^{65}	Gold ($i = 6$)	$x^{372142397109 \cdot 2^{31}}$
	x^{129}	Gold ($i = 7$)	$x^{17046691967 \cdot 2^{28}}$
	x^{257}	Gold ($i = 8$)	$x^{367929961173 \cdot 2^{26}}$
	x^{513}	Gold ($i = 9$)	$x^{355787388333 \cdot 2^{29}}$
	x^{1025}	Gold ($i = 10$)	$x^{2145388543 \cdot 2^{31}}$
	x^{2049}	Gold ($i = 11$)	$x^{314452813531 \cdot 2^{21}}$
	x^{4097}	Gold ($i = 12$)	$x^{329021541787 \cdot 2^{21}}$
	x^{8193}	Gold ($i = 13$)	$x^{329866910515 \cdot 2^{17}}$
	x^{16385}	Gold ($i = 14$)	$x^{366526248277 \cdot 2^{15}}$
	x^{32769}	Gold ($i = 15$)	$x^{323387747629 \cdot 2^{16}}$
	x^{65537}	Gold ($i = 16$)	$x^{219476190835 \cdot 2^{19}}$
	x^{131073}	Gold ($i = 17$)	$x^{121214460871 \cdot 2^{18}}$
	x^{262145}	Gold ($i = 18$)	$x^{212809784551 \cdot 2^{21}}$
	x^{524289}	Gold ($i = 19$)	$x^{314148576109 \cdot 2^{20}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{2097151 \cdot 2^{21}}$
	x^{13}	Kasami ($i = 2$)	$x^{169155635043 \cdot 2^{38}}$
	x^{57}	Kasami ($i = 3$)	$x^{192896776803 \cdot 2^{37}}$
	x^{241}	Kasami ($i = 4$)	$x^{191616143003 \cdot 2^{20}}$
	x^{993}	Kasami ($i = 5$)	$x^{161660319895 \cdot 2^{32}}$
	x^{4033}	Kasami ($i = 6$)	$x^{354962594485 \cdot 2^{19}}$
	x^{16257}	Kasami ($i = 7$)	$x^{270532479 \cdot 2^{0}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
41	x^{65281}	Kasami ($i = 8$)	$x^{365790866133 \cdot 2^{35}}$
	x^{261633}	Kasami ($i = 9$)	$x^{22954032981 \cdot 2^{28}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{314453862107 \cdot 2^{31}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{94121618197 \cdot 2^{3}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{200952409245 \cdot 2^{11}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{439804664219 \cdot 2^{40}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{44739243 \cdot 2^{14}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{388062989133 \cdot 2^{36}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{85237621371 \cdot 2^{28}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{19309544439 \cdot 2^{28}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{226800278835 \cdot 2^{34}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{331361737069 \cdot 2^{20}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{157073239479 \cdot 2^{2}}$
	$x^{1048579}$	Welch	$x^{113185066767 \cdot 2^{24}}$
	$x^{1049599}$	Niho	$x^{358263467 \cdot 2^{32}}$
	$x^{1099511627775}$	Inverse	$x^{1099511627775 \cdot 2^{2}}$
43	x^{3}	Gold ($i = 1$)	$x^{2932031007403 \cdot 2^{42}}$
	x^{5}	Gold ($i = 2$)	$x^{1759218604443 \cdot 2^{40}}$
	x^{9}	Gold ($i = 3$)	$x^{977343669135 \cdot 2^{40}}$
	x^{17}	Gold ($i = 4$)	$x^{1552251709805 \cdot 2^{37}}$
	x^{33}	Gold ($i = 5$)	$x^{1332741367003 \cdot 2^{37}}$
	x^{65}	Gold ($i = 6$)	$x^{1488569588405 \cdot 2^{32}}$
	x^{129}	Gold ($i = 7$)	$x^{68186767615 \cdot 2^{36}}$
	x^{257}	Gold ($i = 8$)	$x^{855651072231 \cdot 2^{30}}$
	x^{513}	Gold ($i = 9$)	$x^{1320271272371 \cdot 2^{29}}$
	x^{1025}	Gold ($i = 10$)	$x^{1261488462701 \cdot 2^{31}}$
	x^{2049}	Gold ($i = 11$)	$x^{4292872191 \cdot 2^{22}}$
	x^{4097}	Gold ($i = 12$)	$x^{852342918771 \cdot 2^{20}}$
	x^{8193}	Gold ($i = 13$)	$x^{258740199183 \cdot 2^{18}}$
	x^{16385}	Gold ($i = 14$)	$x^{1466104984917 \cdot 2^{16}}$
	x^{32769}	Gold ($i = 15$)	$x^{879636149043 \cdot 2^{16}}$
	x^{65537}	Gold ($i = 16$)	$x^{133276171295 \cdot 2^{17}}$
	x^{131073}	Gold ($i = 17$)	$x^{1463163398869 \cdot 2^{19}}$
	x^{262145}	Gold ($i = 18$)	$x^{484826138511 \cdot 2^{22}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
43	x^{524289}	Gold ($i = 19$)	$x^{1418729010605 \cdot 2^{21}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{1256587114203 \cdot 2^{22}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{4194303 \cdot 2^{22}}$
	x^{13}	Kasami ($i = 2$)	$x^{676622540171 \cdot 2^{39}}$
	x^{57}	Kasami ($i = 3$)	$x^{771587107283 \cdot 2^{31}}$
	x^{241}	Kasami ($i = 4$)	$x^{1277440896429 \cdot 2^{25}}$
	x^{993}	Kasami ($i = 5$)	$x^{1319856925899 \cdot 2^{17}}$
	x^{4033}	Kasami ($i = 6$)	$x^{1419850373813 \cdot 2^{26}}$
	x^{16257}	Kasami ($i = 7$)	$x^{541065087 \cdot 2^{22}}$
	x^{65281}	Kasami ($i = 8$)	$x^{780021615715 \cdot 2^{10}}$
	x^{261633}	Kasami ($i = 9$)	$x^{666112421021 \cdot 2^{42}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{1325913496365 \cdot 2^{31}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{628598842807 \cdot 2^{12}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{340933854331 \cdot 2^{41}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{517922526871 \cdot 2^{14}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{178956971 \cdot 2^{15}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{1759218617549 \cdot 2^{42}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{800165422301 \cdot 2^{9}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{1471736556245 \cdot 2^{28}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{72978810871 \cdot 2^{40}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{91799339349 \cdot 2^{34}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{361512692501 \cdot 2^{38}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1256587114205 \cdot 2^{42}}$
	$x^{2097155}$	Welch	$x^{501247971087 \cdot 2^{27}}$
	$x^{4297064447}$	Niho	$x^{1433053867 \cdot 2^{33}}$
	$x^{4398046511103}$	Inverse	$x^{4398046511103 \cdot 2^{2}}$
45	x^{3}	Gold ($i = 1$)	$x^{11728124029611 \cdot 2^{44}}$
	x^{5}	Gold ($i = 2$)	$x^{7036874417767 \cdot 2^{43}}$
	x^{17}	Gold ($i = 4$)	$x^{6209006839213 \cdot 2^{38}}$
	x^{129}	Gold ($i = 7$)	$x^{5182194338669 \cdot 2^{36}}$
	x^{257}	Gold ($i = 8$)	$x^{5065454347483 \cdot 2^{31}}$
	x^{2049}	Gold ($i = 11$)	$x^{17171484671 \cdot 2^{34}}$
	x^{8193}	Gold ($i = 13$)	$x^{5818970364597 \cdot 2^{21}}$
	x^{16385}	Gold ($i = 14$)	$x^{3420732668359 \cdot 2^{20}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
45	x^{65537}	Gold ($i = 16$)	$x^{1954717168071 \cdot 2^{17}}$
	x^{131073}	Gold ($i = 17$)	$x^{532840314943 \cdot 2^{23}}$
	x^{524289}	Gold ($i = 19$)	$x^{5263807925659 \cdot 2^{23}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{8388607 \cdot 2^{23}}$
	x^{13}	Kasami ($i = 2$)	$x^{2706490160699 \cdot 2^{37}}$
	x^{241}	Kasami ($i = 4$)	$x^{5109763616173 \cdot 2^{22}}$
	x^{16257}	Kasami ($i = 7$)	$x^{5027575590253 \cdot 2^{22}}$
	x^{65281}	Kasami ($i = 8$)	$x^{2513477416649 \cdot 2^{1}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{3770061385289 \cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{5954278611637 \cdot 2^{40}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{3909374683819 \cdot 2^{1}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{3909374793047 \cdot 2^{41}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{3789086741177 \cdot 2^{37}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{2533412196059 \cdot 2^{44}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{5026342464951 \cdot 2^{23}}$
	$x^{4194307}$	Welch	$x^{1552252079887 \cdot 2^{25}}$
	$x^{4196351}$	Niho	$x^{5726624427 \cdot 2^{23}}$
	$x^{17592186044415}$	Inverse	$x^{17592186044415 \cdot 2^{2}}$
	$x^{68853957119}$	Dobbertin	$x^{5869799844565 \cdot 2^{1}}$
47	x^{3}	Gold ($i = 1$)	$x^{46912496118443 \cdot 2^{46}}$
	x^{5}	Gold ($i = 2$)	$x^{28147497671067 \cdot 2^{44}}$
	x^{9}	Gold ($i = 3$)	$x^{15637498706151 \cdot 2^{42}}$
	x^{17}	Gold ($i = 4$)	$x^{8278675785615 \cdot 2^{40}}$
	x^{33}	Gold ($i = 5$)	$x^{21323861872027 \cdot 2^{39}}$
	x^{65}	Gold ($i = 6$)	$x^{2165192128575 \cdot 2^{36}}$
	x^{129}	Gold ($i = 7$)	$x^{14182847663731 \cdot 2^{36}}$
	x^{257}	Gold ($i = 8$)	$x^{547616686335 \cdot 2^{32}}$
	x^{513}	Gold ($i = 9$)	$x^{21124340357555 \cdot 2^{31}}$
	x^{1025}	Gold ($i = 10$)	$x^{7826377401287 \cdot 2^{31}}$
	x^{2049}	Gold ($i = 11$)	$x^{20124980033243 \cdot 2^{35}}$
	x^{4097}	Gold ($i = 12$)	$x^{34351353855 \cdot 2^{24}}$
	x^{8193}	Gold ($i = 13$)	$x^{13621973425383 \cdot 2^{24}}$
	x^{16385}	Gold ($i = 14$)	$x^{4131506372127 \cdot 2^{24}}$
	x^{32769}	Gold ($i = 15$)	$x^{14074178335539 \cdot 2^{18}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
	x^{65537}	Gold ($i = 16$)	$x^{23456605984085 \cdot 2^{17}}$
	x^{131073}	Gold ($i = 17$)	$x^{22766374202669 \cdot 2^{19}}$
	x^{262145}	Gold ($i = 18$)	$x^{20694684100973 \cdot 2^{23}}$
	x^{524289}	Gold ($i = 19$)	$x^{23410479901525 \cdot 2^{20}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{23271587011253 \cdot 2^{22}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{22699629532853 \cdot 2^{22}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{20105374653293 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{16777215 \cdot 2^{24}}$
	x^{13}	Kasami ($i = 2$)	$x^{10825960642875 \cdot 2^{36}}$
	x^{57}	Kasami ($i = 3$)	$x^{12345393715667 \cdot 2^{33}}$
	x^{241}	Kasami ($i = 4$)	$x^{583973015535 \cdot 2^{24}}$
	x^{993}	Kasami ($i = 5$)	$x^{21117710003403 \cdot 2^{19}}$
	x^{4033}	Kasami ($i = 6$)	$x^{10364253419671 \cdot 2^{37}}$
	x^{16257}	Kasami ($i = 7$)	$x^{11332064480355 \cdot 2^{34}}$
	x^{65281}	Kasami ($i = 8$)	$x^{4311744255 \cdot 2^{0}}$
	x^{261633}	Kasami ($i = 9$)	$x^{5402392617669 \cdot 2^{3}}$
47	$x^{1047553}$	Kasami ($i = 10$)	$x^{8019716498131 \cdot 2^{2}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{21207255168603 \cdot 2^{38}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{20124980033245 \cdot 2^{10}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{4928550175995 \cdot 2^{6}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{12810976390301 \cdot 2^{13}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{28147497684173 \cdot 2^{1}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{715827883 \cdot 2^{16}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{24836028343725 \cdot 2^{40}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{20728777484717 \cdot 2^{41}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{23479199247189 \cdot 2^{30}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{23275881454293 \cdot 2^{42}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{732314304171 \cdot 2^{6}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{2891866428907 \cdot 2^{4}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{10052678938039 \cdot 2^{2}}$
	$x^{8388611}$	Welch	$x^{8278865269455 \cdot 2^{18}}$
	$x^{34368126975}$	Niho	$x^{22906493611 \cdot 2^{24}}$
	$x^{70368744177663}$	Inverse	$x^{70368744177663 \cdot 2^{2}}$
49	x^{3}	Gold ($i = 1$)	$x^{187649984473771 \cdot 2^{48}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
49	x^{5}	Gold ($i = 2$)	$x^{112589990684263 \cdot 2^{47}}$
	x^{9}	Gold ($i = 3$)	$x^{62549994824591 \cdot 2^{46}}$
	x^{17}	Gold ($i = 4$)	$x^{33114703142431 \cdot 2^{45}}$
	x^{33}	Gold ($i = 5$)	$x^{17059089497631 \cdot 2^{40}}$
	x^{65}	Gold ($i = 6$)	$x^{8660768514175 \cdot 2^{43}}$
	x^{257}	Gold ($i = 8$)	$x^{2190466744831 \cdot 2^{41}}$
	x^{513}	Gold ($i = 9$)	$x^{91081571411373 \cdot 2^{33}}$
	x^{1025}	Gold ($i = 10$)	$x^{93916528814933 \cdot 2^{31}}$
	x^{2049}	Gold ($i = 11$)	$x^{90940182812341 \cdot 2^{34}}$
	x^{4097}	Gold ($i = 12$)	$x^{137405407231 \cdot 2^{37}}$
	x^{8193}	Gold ($i = 13$)	$x^{80460685400941 \cdot 2^{24}}$
	x^{32769}	Gold ($i = 15$)	$x^{82787263147309 \cdot 2^{20}}$
	x^{65537}	Gold ($i = 16$)	$x^{93826423903573 \cdot 2^{18}}$
	x^{131073}	Gold ($i = 17$)	$x^{84442707768115 \cdot 2^{19}}$
	x^{262145}	Gold ($i = 18$)	$x^{81030691384475 \cdot 2^{20}}$
	x^{524289}	Gold ($i = 19$)	$x^{54727442643175 \cdot 2^{25}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{56185097971507 \cdot 2^{21}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{54479097024115 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{80421441091291 \cdot 2^{25}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{33554431 \cdot 2^{25}}$
	x^{13}	Kasami ($i = 2$)	$x^{43303842570875 \cdot 2^{43}}$
	x^{57}	Kasami ($i = 3$)	$x^{49381574861523 \cdot 2^{41}}$
	x^{241}	Kasami ($i = 4$)	$x^{2335891922927 \cdot 2^{37}}$
	x^{993}	Kasami ($i = 5$)	$x^{41385041893015 \cdot 2^{36}}$
	x^{4033}	Kasami ($i = 6$)	$x^{50111339799769 \cdot 2^{22}}$
	x^{65281}	Kasami ($i = 8$)	$x^{8623488767 \cdot 2^{25}}$
	x^{261633}	Kasami ($i = 9$)	$x^{81719652169125 \cdot 2^{1}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{93641919605589 \cdot 2^{1}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{2933417902763 \cdot 2^{17}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{40230342698423 \cdot 2^{14}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{11567935018475 \cdot 2^{14}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{99344109488973 \cdot 2^{48}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{2863311531 \cdot 2^{17}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{112589990893979 \cdot 2^{46}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
49	$x^{68719214593}$	Kasami ($i = 18$)	$x^{51210587027037 \cdot 2^9}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{10956611979515 \cdot 2^9}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{43134770015075 \cdot 2^{39}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{58054630034739 \cdot 2^{40}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{84828207552205 \cdot 2^{22}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{80421441091293 \cdot 2^{48}}$
	$x^{16777219}$	Welch	$x^{32597285998351 \cdot 2^{31}}$
	$x^{16781311}$	Niho	$x^{22912084651 \cdot 2^{38}}$
	$x^{281474976710655}$	Inverse	$x^{281474976710655 \cdot 2^2}$
51	x^3	Gold ($i = 1$)	$x^{750599937895083 \cdot 2^{50}}$
	x^5	Gold ($i = 2$)	$x^{450359962737051 \cdot 2^{48}}$
	x^{17}	Gold ($i = 4$)	$x^{397376437709165 \cdot 2^{45}}$
	x^{33}	Gold ($i = 5$)	$x^{68236357990463 \cdot 2^{46}}$
	x^{129}	Gold ($i = 7$)	$x^{226925562619507 \cdot 2^{38}}$
	x^{257}	Gold ($i = 8$)	$x^{324189078234843 \cdot 2^{42}}$
	x^{1025}	Gold ($i = 10$)	$x^{375666115259221 \cdot 2^{32}}$
	x^{2049}	Gold ($i = 11$)	$x^{124184177133455 \cdot 2^{37}}$
	x^{8193}	Gold ($i = 13$)	$x^{274844360703 \cdot 2^{26}}$
	x^{16385}	Gold ($i = 14$)	$x^{363228984292781 \cdot 2^{25}}$
	x^{65537}	Gold ($i = 16$)	$x^{125101898527175 \cdot 2^{20}}$
	x^{524289}	Gold ($i = 19$)	$x^{17321570070591 \cdot 2^{20}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{337715103898035 \cdot 2^{24}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{372345121630933 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{217916145638631 \cdot 2^{26}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{67108863 \cdot 2^{26}}$
	x^{13}	Kasami ($i = 2$)	$x^{173215370283483 \cdot 2^{46}}$
	x^{241}	Kasami ($i = 4$)	$x^{327024869207469 \cdot 2^{37}}$
	x^{993}	Kasami ($i = 5$)	$x^{233570373431993 \cdot 2^{28}}$
	x^{16257}	Kasami ($i = 7$)	$x^{171894172913319 \cdot 2^{23}}$
	x^{65281}	Kasami ($i = 8$)	$x^{160845307688649 \cdot 2^{28}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{375116896316245 \cdot 2^{43}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{234684711933255 \cdot 2^{40}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{241283903483465 \cdot 2^{41}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{364326285645237 \cdot 2^6}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
51	$x^{4294901761}$	Kasami ($i = 16$)	$x^{250199979414871 \cdot 2^{50}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{242501526656441 \cdot 2^{41}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{162410546366939 \cdot 2^{37}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{372413839010517 \cdot 2^{23}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{189604902972103 \cdot 2^{43}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{321685716430263 \cdot 2^{26}}$
	$x^{33554435}$	Welch	$x^{132458859940683 \cdot 2^{24}}$
	$x^{274911461375}$	Niho	$x^{91648338603 \cdot 2^{39}}$
	$x^{1125899906842623}$	Inverse	$x^{1125899906842623 \cdot 2^2}$
53	x^3	Gold ($i = 1$)	$x^{3002399751580331 \cdot 2^{52}}$
	x^5	Gold ($i = 2$)	$x^{1801439850948199 \cdot 2^{51}}$
	x^9	Gold ($i = 3$)	$x^{1000799917193447 \cdot 2^{48}}$
	x^{17}	Gold ($i = 4$)	$x^{1589505750836653 \cdot 2^{46}}$
	x^{33}	Gold ($i = 5$)	$x^{1364727159809243 \cdot 2^{47}}$
	x^{65}	Gold ($i = 6$)	$x^{1524295258494645 \cdot 2^{43}}$
	x^{129}	Gold ($i = 7$)	$x^{1326641750698349 \cdot 2^{40}}$
	x^{257}	Gold ($i = 8$)	$x^{876186697932007 \cdot 2^{43}}$
	x^{513}	Gold ($i = 9$)	$x^{17557893284351 \cdot 2^{36}}$
	x^{1025}	Gold ($i = 10$)	$x^{500888153678791 \cdot 2^{34}}$
	x^{2049}	Gold ($i = 11$)	$x^{901159515481907 \cdot 2^{34}}$
	x^{4097}	Gold ($i = 12$)	$x^{872799146724979 \cdot 2^{37}}$
	x^{8193}	Gold ($i = 13$)	$x^{1099377426431 \cdot 2^{40}}$
	x^{16385}	Gold ($i = 14$)	$x^{1286899814184667 \cdot 2^{27}}$
	x^{32769}	Gold ($i = 15$)	$x^{1489517921266389 \cdot 2^{24}}$
	x^{65537}	Gold ($i = 16$)	$x^{136474798390303 \cdot 2^{22}}$
	x^{131073}	Gold ($i = 17$)	$x^{1351083324191539 \cdot 2^{21}}$
	x^{262145}	Gold ($i = 18$)	$x^{1501205602456917 \cdot 2^{19}}$
	x^{524289}	Gold ($i = 19$)	$x^{496720610299663 \cdot 2^{23}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{69277756416127 \cdot 2^{27}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{1500467584215893 \cdot 2^{23}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{264400271187727 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{1347534017321395 \cdot 2^{25}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{1452774211892653 \cdot 2^{26}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{1286742904068973 \cdot 2^{26}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
53	$x^{67108865}$	Gold ($i = 26$)	$x^{134217727 \cdot 2^{27}}$
	x^{13}	Kasami ($i = 2$)	$x^{692861481133923 \cdot 2^{50}}$
	x^{57}	Kasami ($i = 3$)	$x^{158021039559159 \cdot 2^{36}}$
	x^{241}	Kasami ($i = 4$)	$x^{1308099476829613 \cdot 2^{42}}$
	x^{993}	Kasami ($i = 5$)	$x^{390039846882037 \cdot 2^{46}}$
	x^{4033}	Kasami ($i = 6$)	$x^{46900863959723 \cdot 2^{42}}$
	x^{16257}	Kasami ($i = 7$)	$x^{188931226294315 \cdot 2^{43}}$
	x^{65281}	Kasami ($i = 8$)	$x^{798741999750243 \cdot 2^{39}}$
	x^{261633}	Kasami ($i = 9$)	$x^{68853693951 \cdot 2^{0}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{780220444764563 \cdot 2^{50}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{346938537894459 \cdot 2^{45}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{928874348792627 \cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{1286899881293531 \cdot 2^{40}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{1349541325280973 \cdot 2^{46}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{1507041121487573 \cdot 2^{48}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{819369392432349 \cdot 2^{14}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{1801439851157915 \cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{11453246123 \cdot 2^{18}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{529839292601043 \cdot 2^{17}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{628411381167255 \cdot 2^{15}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1502665533729621 \cdot 2^{34}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{18689483349999 \cdot 2^{36}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{682373991820445 \cdot 2^{22}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{1457176544982197 \cdot 2^{21}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{1357250144131917 \cdot 2^{48}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{643371384925623 \cdot 2^{2}}$
	$x^{67108867}$	Welch	$x^{529838282020495 \cdot 2^{20}}$
	$x^{67117055}$	Niho	$x^{366503881387 \cdot 2^{27}}$
	$x^{4503599627370495}$	Inverse	$x^{4503599627370495 \cdot 2^{2}}$
55	x^{3}	Gold ($i = 1$)	$x^{12009599006321323 \cdot 2^{54}}$
	x^{5}	Gold ($i = 2$)	$x^{7205759403792795 \cdot 2^{52}}$
	x^{9}	Gold ($i = 3$)	$x^{4003199668773775 \cdot 2^{52}}$
	x^{17}	Gold ($i = 4$)	$x^{2119341001115535 \cdot 2^{48}}$
	x^{65}	Gold ($i = 6$)	$x^{6097181033978549 \cdot 2^{44}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
55	x^{129}	Gold ($i = 7$)	$x^{2792930001470 71 \cdot 2^{42}}$
	x^{257}	Gold ($i = 8$)	$x^{6028164481772245 \cdot 2^{41}}$
	x^{513}	Gold ($i = 9$)	$x^{70231573136383 \cdot 2^{46}}$
	x^{4097}	Gold ($i = 12$)	$x^{5390688936447387 \cdot 2^{40}}$
	x^{8193}	Gold ($i = 13$)	$x^{5149483865398125 \cdot 2^{40}}$
	x^{16385}	Gold ($i = 14$)	$x^{2198889054207 \cdot 2^{28}}$
	x^{65537}	Gold ($i = 16$)	$x^{3595897909601907 \cdot 2^{26}}$
	x^{131073}	Gold ($i = 17$)	$x^{5828191795391789 \cdot 2^{23}}$
	x^{262145}	Gold ($i = 18$)	$x^{6004822409696597 \cdot 2^{20}}$
	x^{524289}	Gold ($i = 19$)	$x^{3602886573896499 \cdot 2^{20}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{5185930018907355 \cdot 2^{28}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{1057596915858975 \cdot 2^{28}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{1985840287966151 \cdot 2^{25}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{5146971156100827 \cdot 2^{28}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{268435455 \cdot 2^{28}}$
	x^{13}	Kasami ($i = 2$)	$x^{2771445924535691 \cdot 2^{51}}$
	x^{57}	Kasami ($i = 3$)	$x^{632084158227447 \cdot 2^{46}}$
	x^{241}	Kasami ($i = 4$)	$x^{3139438744391323 \cdot 2^{39}}$
	x^{4033}	Kasami ($i = 6$)	$x^{187603455838891 \cdot 2^{43}}$
	x^{16257}	Kasami ($i = 7$)	$x^{3206844392482521 \cdot 2^{24}}$
	x^{65281}	Kasami ($i = 8$)	$x^{5957795741805269 \cdot 2^{25}}$
	x^{261633}	Kasami ($i = 9$)	$x^{137707388415 \cdot 2^{28}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{5403883185032403 \cdot 2^{52}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{5305612404709965 \cdot 2^{47}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{2573642555272631 \cdot 2^{15}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{1396465004896891 \cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{6358023004333485 \cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{45812984491 \cdot 2^{19}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{7205759404002509 \cdot 2^{54}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1542088855751413 \cdot 2^{40}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{72563338526703 \cdot 2^{51}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{2053116142412499 \cdot 2^{26}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{5428996928747101 \cdot 2^{54}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{5146971156100829 \cdot 2^{54}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
55	$x^{134217731}$	Welch	$x^{2119341095857453 \cdot 2^{27}}$
	$x^{2199157473279}$	Niho	$x^{1466015509163 \cdot 2^{28}}$
	$x^{18014398509481983}$	Inverse	$x^{18014398509481983 \cdot 2^{2}}$
	$x^{17600780175359}$	Dobbertin	$x^{6006266234841941 \cdot 2^{1}}$
57	x^{3}	Gold ($i = 1$)	$x^{48038396025285291 \cdot 2^{56}}$
	x^{5}	Gold ($i = 2$)	$x^{28823037615171175 \cdot 2^{55}}$
	x^{17}	Gold ($i = 4$)	$x^{8477364004462111 \cdot 2^{53}}$
	x^{33}	Gold ($i = 5$)	$x^{2183563455694786 7 \cdot 2^{49}}$
	x^{129}	Gold ($i = 7$)	$x^{1117172000588031 \cdot 2^{50}}$
	x^{257}	Gold ($i = 8$)	$x^{24112657927088853 \cdot 2^{42}}$
	x^{1025}	Gold ($i = 10$)	$x^{20668226972830573 \cdot 2^{38}}$
	x^{2049}	Gold ($i = 11$)	$x^{14418552247707443 \cdot 2^{36}}$
	x^{8193}	Gold ($i = 13$)	$x^{13948900786543847 \cdot 2^{42}}$
	x^{16385}	Gold ($i = 14$)	$x^{8795556184063 \cdot 2^{43}}$
	x^{65537}	Gold ($i = 16$)	$x^{21561094024518067 \cdot 2^{27}}$
	x^{131073}	Gold ($i = 17$)	$x^{2182513929877567 \cdot 2^{29}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{14011200749597127 \cdot 2^{23}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{23312492809004461 \cdot 2^{28}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{24007472753323349 \cdot 2^{24}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{7943357093627791 \cdot 2^{29}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{23244386281903797 \cdot 2^{27}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{536870911 \cdot 2^{29}}$
	x^{13}	Kasami ($i = 2$)	$x^{11085783698142779 \cdot 2^{49}}$
	x^{241}	Kasami ($i = 4$)	$x^{14949708306624087 \cdot 2^{44}}$
	x^{993}	Kasami ($i = 5$)	$x^{10304308513044185 \cdot 2^{31}}$
	x^{16257}	Kasami ($i = 7$)	$x^{15380442351703481 \cdot 2^{32}}$
	x^{65281}	Kasami ($i = 8$)	$x^{23831182967155413 \cdot 2^{34}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{20588512916761453 \cdot 2^{55}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{10999144301491755 \cdot 2^{55}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{12134714326624711 \cdot 2^{41}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{15441070109979209 \cdot 2^{46}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{10394272824315355 \cdot 2^{56}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{15520097177916089 \cdot 2^{55}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{16012798675561131 \cdot 2^{55}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
57	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{21069746282997173 \cdot 2^{10}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{24025064937270613 \cdot 2^{36}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{15019821295179207 \cdot 2^{50}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{23314789352264885 \cdot 2^{48}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{20587884240924087 \cdot 2^{29}}$
	$x^{268435459}$	Welch	$x^{7417693515747087 \cdot 2^{32}}$
	$x^{268451839}$	Niho	$x^{1466104982187 \cdot 2^{44}}$
	$x^{72057594037927935}$	Inverse	$x^{72057594037927935 \cdot 2^2}$
59	x^3	Gold ($i = 1$)	$x^{192153584101141163 \cdot 2^{58}}$
	x^5	Gold ($i = 2$)	$x^{115292150460684699 \cdot 2^{56}}$
	x^9	Gold ($i = 3$)	$x^{64051194700380391 \cdot 2^{54}}$
	x^{17}	Gold ($i = 4$)	$x^{101728368053545325 \cdot 2^{53}}$
	x^{33}	Gold ($i = 5$)	$x^{17468507645558303 \cdot 2^{50}}$
	x^{65}	Gold ($i = 6$)	$x^{8868626958514239 \cdot 2^{48}}$
	x^{129}	Gold ($i = 7$)	$x^{84905072044690285 \cdot 2^{50}}$
	x^{257}	Gold ($i = 8$)	$x^{56075948667648231 \cdot 2^{46}}$
	x^{513}	Gold ($i = 9$)	$x^{93267529125115309 \cdot 2^{47}}$
	x^{1025}	Gold ($i = 10$)	$x^{562400733955071 \cdot 2^{40}}$
	x^{2049}	Gold ($i = 11$)	$x^{31791149346162575 \cdot 2^{41}}$
	x^{4097}	Gold ($i = 12$)	$x^{96100242573405525 \cdot 2^{37}}$
	x^{8193}	Gold ($i = 13$)	$x^{95338010420009653 \cdot 2^{41}}$
	x^{16385}	Gold ($i = 14$)	$x^{82361588107556571 \cdot 2^{44}}$
	x^{32769}	Gold ($i = 15$)	$x^{17591649206271 \cdot 2^{30}}$
	x^{65537}	Gold ($i = 16$)	$x^{92982080543839925 \cdot 2^{28}}$
	x^{131073}	Gold ($i = 17$)	$x^{95889876499933909 \cdot 2^{27}}$
	x^{262145}	Gold ($i = 18$)	$x^{82975427975670939 \cdot 2^{25}}$
	x^{524289}	Gold ($i = 19$)	$x^{57646185181557555 \cdot 2^{22}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{96076883676714325 \cdot 2^{21}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{16954736093630223 \cdot 2^{22}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{2234344533901439 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{32021691793728455 \cdot 2^{27}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{86455040815504179 \cdot 2^{26}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{57533267058681459 \cdot 2^{28}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{86242160334523803 \cdot 2^{30}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
59	$x^{134217729}$	Gold ($i = 27$)	$x^{557865266332176 51 \cdot 2^{28}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{82351537270479725 \cdot 2^{29}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{1073741823 \cdot 2^{30}}$
	x^{13}	Kasami ($i = 2$)	$x^{443431347925711 95 \cdot 2^{48}}$
	x^{57}	Kasami ($i = 3$)	$x^{50566732658195043 \cdot 2^{55}}$
	x^{241}	Kasami ($i = 4$)	$x^{11959766645299243 \cdot 2^{52}}$
	x^{993}	Kasami ($i = 5$)	$x^{580524423806943 \cdot 2^{30}}$
	x^{4033}	Kasami ($i = 6$)	$x^{51314011921949913 \cdot 2^{27}}$
	x^{16257}	Kasami ($i = 7$)	$x^{84641189379919149 \cdot 2^{29}}$
	x^{65281}	Kasami ($i = 8$)	$x^{50413051805539507 \cdot 2^{25}}$
	x^{261633}	Kasami ($i = 9$)	$x^{83679822162081189 \cdot 2^{33}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{1100585368575 \cdot 2^{0}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{49931888879947163 \cdot 2^{55}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{96029891013291349 \cdot 2^{1}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{1501385991386453 \cdot 2^{40}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{23692096872770293 \cdot 2^{43}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{82361588107556573 \cdot 2^{13}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{93122747233359541 \cdot 2^{50}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{96450631725066965 \cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{52439641115670109 \cdot 2^{14}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{115292150460894413 \cdot 2^{1}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{183251937963 \cdot 2^{20}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{33909585372157591 \cdot 2^{18}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{40218260207936695 \cdot 2^{16}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{5061610896368631 \cdot 2^{40}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{22163453211271877 \cdot 2^{14}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{44168907146980451 \cdot 2^{1}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{86470927036370131 \cdot 2^{23}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{20178919776699515 \cdot 2^{50}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{86863950036261229 \cdot 2^{29}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{41175768098368951 \cdot 2^{2}}$
	$x^{536870915}$	Welch	$x^{32849785523212047 \cdot 2^{35}}$
	$x^{17592722915327}$	Niho	$x^{5864419928747 \cdot 2^{45}}$
	$x^{288230376151711743}$	Inverse	$x^{288230376151711743 \cdot 2^{2}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
61	x^{3}	Gold ($i = 1$)	$x^{768614336404564651 \cdot 2^{60}}$
	x^{5}	Gold ($i = 2$)	$x^{461168601842738791 \cdot 2^{59}}$
	x^{9}	Gold ($i = 3$)	$x^{256204778801521551 \cdot 2^{58}}$
	x^{17}	Gold ($i = 4$)	$x^{406913472214181293 \cdot 2^{54}}$
	x^{33}	Gold ($i = 5$)	$x^{69874030582233151 \cdot 2^{56}}$
	x^{65}	Gold ($i = 6$)	$x^{35474507834056831 \cdot 2^{55}}$
	x^{129}	Gold ($i = 7$)	$x^{2323717761223102 59 \cdot 2^{50}}$
	x^{257}	Gold ($i = 8$)	$x^{331969616112477403 \cdot 2^{47}}$
	x^{513}	Gold ($i = 9$)	$x^{346101192416090547 \cdot 2^{47}}$
	x^{1025}	Gold ($i = 10$)	$x^{2249602935818239 \cdot 2^{51}}$
	x^{2049}	Gold ($i = 11$)	$x^{372490988799284917 \cdot 2^{40}}$
	x^{4097}	Gold ($i = 12$)	$x^{384400970293620053 \cdot 2^{38}}$
	x^{8193}	Gold ($i = 13$)	$x^{67827189701025551 \cdot 2^{40}}$
	x^{16385}	Gold ($i = 14$)	$x^{371946479911613869 \cdot 2^{44}}$
	x^{32769}	Gold ($i = 15$)	$x^{70366596759551 \cdot 2^{46}}$
	x^{65537}	Gold ($i = 16$)	$x^{329426249222118253 \cdot 2^{30}}$
	x^{131073}	Gold ($i = 17$)	$x^{127102574455284679 \cdot 2^{28}}$
	x^{262145}	Gold ($i = 18$)	$x^{339061704309303661 \cdot 2^{30}}$
	x^{524289}	Gold ($i = 19$)	$x^{127160476236222223 \cdot 2^{27}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{384307534706333013 \cdot 2^{22}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{345876506357740339 \cdot 2^{23}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{345003027040988315 \cdot 2^{26}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{8937104323084543 \cdot 2^{31}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{23055167169271603 \cdot 2^{27}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{224163544907528647 \cdot 2^{28}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{383555107986713301 \cdot 2^{28}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{381281131836562101 \cdot 2^{29}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{223146098774220007 \cdot 2^{31}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{329406145400518363 \cdot 2^{31}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{2147483647 \cdot 2^{31}}$
	x^{13}	Kasami ($i = 2$)	$x^{177372539170284155 \cdot 2^{55}}$
	x^{57}	Kasami ($i = 3$)	$x^{202266930632780243 \cdot 2^{49}}$
	x^{241}	Kasami ($i = 4$)	$x^{47839066581196971 \cdot 2^{53}}$
	x^{993}	Kasami ($i = 5$)	$x^{2322097693065183 \cdot 2^{46}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
61	x^{4033}	Kasami ($i = 6$)	$x^{169807928027886743 \cdot 2^{44}}$
	x^{16257}	Kasami ($i = 7$)	$x^{228782971880788787 \cdot 2^{29}}$
	x^{65281}	Kasami ($i = 8$)	$x^{345411969594533581 \cdot 2^{36}}$
	x^{261633}	Kasami ($i = 9$)	$x^{88511698988786373 \cdot 2^{37}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{2201170738175 \cdot 2^{31}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{371919247047874229 \cdot 2^{57}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{384260267165003093 \cdot 2^{51}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{200886773813505181 \cdot 2^{60}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{373002011208496309 \cdot 2^{58}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{164713124611042743 \cdot 2^{17}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{347579167140109133 \cdot 2^{8}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{20246426423411703 \cdot 2^{58}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{339620288178891181 \cdot 2^{1}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{135638858905866963 \cdot 2^{21}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{733007751851 \cdot 2^{21}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{461168601846094235 \cdot 2^{58}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{209623157939793053 \cdot 2^{16}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{206363872030435049 \cdot 2^{11}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{176680015969462115 \cdot 2^{47}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{202227427792341603 \cdot 2^{49}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{383559505999670101 \cdot 2^{54}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{6005526784644437 \cdot 2^{48}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{80715413850916091 \cdot 2^{59}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{94760686673324821 \cdot 2^{56}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{329406145400518365 \cdot 2^{60}}$
	$x^{1073741827}$	Welch	$x^{101728368148287247 \cdot 2^{33}}$
	$x^{1073774591}$	Niho	$x^{23456248081067 \cdot 2^{31}}$
	$x^{1152921504606846975}$	Inverse	$x^{1152921504606846975 \cdot 2^{2}}$
63	x^{3}	Gold ($i = 1$)	$x^{3074457345618258603 \cdot 2^{62}}$
	x^{5}	Gold ($i = 2$)	$x^{1844674407370955163 \cdot 2^{60}}$
	x^{17}	Gold ($i = 4$)	$x^{542551296285575055 \cdot 2^{56}}$
	x^{33}	Gold ($i = 5$)	$x^{1397480611644663003 \cdot 2^{57}}$
	x^{257}	Gold ($i = 8$)	$x^{35888607147294975 \cdot 2^{48}}$
	x^{1025}	Gold ($i = 10$)	$x^{1322766526261123949 \cdot 2^{51}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
63	x^{2049}	Gold ($i = 11$)	$x^{1318910691458492123 \cdot 2^{43}}$
	x^{8193}	Gold ($i = 13$)	$x^{1383562093652450099 \cdot 2^{41}}$
	x^{65537}	Gold ($i = 16$)	$x^{1407353409372 15 \cdot 2^{32}}$
	x^{131073}	Gold ($i = 17$)	$x^{892620709738172019 \cdot 2^{30}}$
	x^{524289}	Gold ($i = 19$)	$x^{70949150992625727 \cdot 2^{26}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{896716847973298631 \cdot 2^{26}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{512409679771234759 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{1489293337488233141 \cdot 2^{24}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{1537041068643233109 \cdot 2^{27}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{1356245785945664813 \cdot 2^{27}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{1487640655539123629 \cdot 2^{31}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{4294967295 \cdot 2^{32}}$
	x^{13}	Kasami ($i = 2$)	$x^{709490156681136603 \cdot 2^{58}}$
	x^{241}	Kasami ($i = 4$)	$x^{956781331623939671 \cdot 2^{47}}$
	x^{993}	Kasami ($i = 5$)	$x^{659475744830502617 \cdot 2^{49}}$
	x^{65281}	Kasami ($i = 8$)	$x^{984348171455213001 \cdot 2^{34}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{1317629607940942701 \cdot 2^{31}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{658813545545053769 \cdot 2^{1}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{665163263472667067 \cdot 2^{56}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{988228485427982921 \cdot 2^{50}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{776681316259434183 \cdot 2^{7}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{993286219361850809 \cdot 2^{59}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{1024819115206552235 \cdot 2^{1}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{1024819115213542743 \cdot 2^{59}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{1560878344764576949 \cdot 2^{54}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{1537603949877177685 \cdot 2^{40}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{1320358825891032493 \cdot 2^{42}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{1492144392337003957 \cdot 2^{60}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{1317624578534239671 \cdot 2^{32}}$
	$x^{2147483651}$	Welch	$x^{542551344793440975 \cdot 2^{26}}$
	$x^{140739635838975}$	Niho	$x^{93824992258731 \cdot 2^{32}}$
	$x^{4611686018427387903}$	Inverse	$x^{4611686018427387903 \cdot 2^{2}}$
65	x^{3}	Gold ($i = 1$)	$x^{12297829382473034411 \cdot 2^{64}}$
	x^{5}	Gold ($i = 2$)	$x^{7378697629483820647 \cdot 2^{63}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
65	x^{9}	Gold ($i = 3$)	$x^{4099276460824344807 \cdot 2^{60}}$
	x^{17}	Gold ($i = 4$)	$x^{2170205185142300191 \cdot 2^{61}}$
	x^{65}	Gold ($i = 6$)	$x^{6243513378794002101 \cdot 2^{55}}$
	x^{129}	Gold ($i = 7$)	$x^{3717948417956963955 \cdot 2^{52}}$
	x^{257}	Gold ($i = 8$)	$x^{143554428589179391 \cdot 2^{57}}$
	x^{513}	Gold ($i = 9$)	$x^{5537619078657448371 \cdot 2^{49}}$
	x^{2049}	Gold ($i = 11$)	$x^{18005606709331967 \cdot 2^{44}}$
	x^{4097}	Gold ($i = 12$)	$x^{5520065470922116507 \cdot 2^{45}}$
	x^{16385}	Gold ($i = 14$)	$x^{1083049606280658463 \cdot 2^{47}}$
	x^{65537}	Gold ($i = 16$)	$x^{562941363617791 \cdot 2^{49}}$
	x^{131073}	Gold ($i = 17$)	$x^{5270578727582545627 \cdot 2^{33}}$
	x^{262145}	Gold ($i = 18$)	$x^{2033508212027934607 \cdot 2^{33}}$
	x^{524289}	Gold ($i = 19$)	$x^{3586617681061034215 \cdot 2^{33}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{5534024101722272563 \cdot 2^{25}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{6148916157252719957 \cdot 2^{23}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{5425513092210306349 \cdot 2^{24}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{5290926603308321133 \cdot 2^{25}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{5587193033927547 19 \cdot 2^{28}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{6136881658933455701 \cdot 2^{29}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{6100498074754706133 \cdot 2^{30}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{5270498316591225709 \cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{8589934591 \cdot 2^{33}}$
	x^{13}	Kasami ($i = 2$)	$x^{28379606267245464 03 \cdot 2^{62}}$
	x^{57}	Kasami ($i = 3$)	$x^{32362708901244830 27 \cdot 2^{51}}$
	x^{241}	Kasami ($i = 4$)	$x^{3214785274256445083 \cdot 2^{44}}$
	x^{4033}	Kasami ($i = 6$)	$x^{5955284102149790389 \cdot 2^{37}}$
	x^{16257}	Kasami ($i = 7$)	$x^{3660527550089450291 \cdot 2^{31}}$
	x^{65281}	Kasami ($i = 8$)	$x^{2645462202142565559 \cdot 2^{50}}$
	x^{261633}	Kasami ($i = 9$)	$x^{2793595967207959709 \cdot 2^{37}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{17600775976959 \cdot 2^{0}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{1453634298555742837 \cdot 2^{44}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{2136293663498081943 \cdot 2^{1}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{5270578731877512923 \cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{5559354423922964061 \cdot 2^{13}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
65	$x^{68719214593}$	Kasami ($i = 18$)	$x^{306095314058627063 \cdot 2^8}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{718052522689235195 \cdot 2^{17}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{7378697629487176091 \cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{2932031007403 \cdot 2^{22}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{651061555544269089 3 \cdot 2^{60}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{5433924611392887149 \cdot 2^{53}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{18577069294288863 \cdot 2^{44}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{6136952027543415637 \cdot 2^{29}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{48035486901463723 \cdot 2^8}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{758085373009843691 \cdot 2^4}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{2635249154000645559 \cdot 2^2}$
	$x^{4294967299}$	Welch	$x^{2136295729148137231 \cdot 2^{39}}$
	$x^{4295032831}$	Niho	$x^{93826423892651 \cdot 2^{50}}$
	$x^{18446744073709551615}$	Inverse	$x^{1844674407370955161 5 \cdot 2^2}$
	$x^{4504149450301439}$	Dobbertin	$x^{6149290037024042325 \cdot 2^1}$
67	x^3	Gold ($i = 1$)	$x^{49191317529892137643 \cdot 2^{66}}$
	x^5	Gold ($i = 2$)	$x^{29514790517935282587 \cdot 2^{64}}$
	x^9	Gold ($i = 3$)	$x^{16397105843297379215 \cdot 2^{64}}$
	x^{17}	Gold ($i = 4$)	$x^{260424622217076022 85 \cdot 2^{61}}$
	x^{33}	Gold ($i = 5$)	$x^{223596897863146080 27 \cdot 2^{59}}$
	x^{65}	Gold ($i = 6$)	$x^{249740535151760083 73 \cdot 2^{56}}$
	x^{129}	Gold ($i = 7$)	$x^{217356984434407120 45 \cdot 2^{54}}$
	x^{257}	Gold ($i = 8$)	$x^{212460554311985497 23 \cdot 2^{58}}$
	x^{513}	Gold ($i = 9$)	$x^{238764874560295172 29 \cdot 2^{51}}$
	x^{1025}	Gold ($i = 10$)	$x^{8206551509864932295 \cdot 2^{51}}$
	x^{2049}	Gold ($i = 11$)	$x^{72022426837323775 \cdot 2^{56}}$
	x^{4097}	Gold ($i = 12$)	$x^{14299941219941797491 \cdot 2^{44}}$
	x^{8193}	Gold ($i = 13$)	$x^{22136993498439195443 \cdot 2^{43}}$
	x^{16385}	Gold ($i = 14$)	$x^{14347592705239824839 \cdot 2^{45}}$
	x^{32769}	Gold ($i = 15$)	$x^{24404261621760092885 \cdot 2^{46}}$
	x^{65537}	Gold ($i = 16$)	$x^{21083279950213471085 \cdot 2^{49}}$
	x^{131073}	Gold ($i = 17$)	$x^{1125891317039103 \cdot 2^{34}}$
	x^{262145}	Gold ($i = 18$)	$x^{14281422889040452839 \cdot 2^{34}}$
	x^{524289}	Gold ($i = 19$)	$x^{24547667372953480021 \cdot 2^{30}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
67	$x^{1048577}$	Gold ($i = 20$)	$x^{1135046761120784511 \cdot 2^{34}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{4340412439953608463 \cdot 2^{26}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{24595664629008782677 \cdot 2^{24}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{14757397018187084595 \cdot 2^{24}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{4332189904428104735 \cdot 2^{29}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{287108865734934783 \cdot 2^{26}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{8138252895016945551 \cdot 2^{34}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{24592656548468798805 \cdot 2^{28}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{2234876672140769343 \cdot 2^{34}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{14728515953898710835 \cdot 2^{30}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{22077992941747231155 \cdot 2^{32}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{23802250453157861045 \cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{21081993236913698523 \cdot 2^{34}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{17179869183 \cdot 2^{34}}$
	x^{13}	Kasami ($i = 2$)	$x^{1135184250689818561 1 \cdot 2^{63}}$
	x^{57}	Kasami ($i = 3$)	$x^{12945083560497930963 \cdot 2^{59}}$
	x^{241}	Kasami ($i = 4$)	$x^{21431901828376243629 \cdot 2^{49}}$
	x^{993}	Kasami ($i = 5$)	$x^{6390412851315833461 \cdot 2^{38}}$
	x^{4033}	Kasami ($i = 6$)	$x^{23821136408607414965 \cdot 2^{32}}$
	x^{16257}	Kasami ($i = 7$)	$x^{21668144481243450669 \cdot 2^{33}}$
	x^{65281}	Kasami ($i = 8$)	$x^{13136322030899639885 \cdot 2^{28}}$
	x^{261633}	Kasami ($i = 9$)	$x^{1540419111998889813 \cdot 2^{14}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{12782004767605189011 \cdot 2^{34}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{35201551955967 \cdot 2^{34}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{11900544100324183139 \cdot 2^{13}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{11174453729448024251 \cdot 2^{62}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{2583962199428368635 \cdot 2^{65}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{192159402348784299 \cdot 2^{23}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{3032464877624514027 \cdot 2^{20}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{10541077033743117751 \cdot 2^{18}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{15220308792661613875 \cdot 2^{6}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{24619654529661840213 \cdot 2^{60}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{10295892069044302999 \cdot 2^{22}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{8680853855272343191 \cdot 2^{22}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
67	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{11728124029611 \cdot 2^{23}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{2951479051793863 8029 \cdot 2^{66}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{13415830930878262429 \cdot 2^{18}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{13207147620076173033 \cdot 2^{12}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{648219425136216055 \cdot 2^{12}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{24597160148062614869 \cdot 2^{42}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{73182935603347423 \cdot 2^{62}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{5684240996268728955 \cdot 2^{61}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{221365441279702335 55 \cdot 2^{25}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{23874310245145269941 \cdot 2^{32}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{22237171005948532429 \cdot 2^{31}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{21081993236913698525 \cdot 2^{66}}$
	$x^{8589934595}$	Welch	$x^{8680820752696167243 \cdot 2^{32}}$
	$x^{1125908496777215}$	Niho	$x^{375305695570603 \cdot 2^{51}}$
	$x^{73786976294838206463}$	Inverse	$x^{73786976294838206463 \cdot 2^2}$
69	x^3	Gold ($i = 1$)	$x^{19676527011956855 0571 \cdot 2^{68}}$
	x^5	Gold ($i = 2$)	$x^{11805916207174113 0343 \cdot 2^{67}}$
	x^{17}	Gold ($i = 4$)	$x^{10416984888683040 9133 \cdot 2^{62}}$
	x^{33}	Gold ($i = 5$)	$x^{17887751829051686431 \cdot 2^{60}}$
	x^{129}	Gold ($i = 7$)	$x^{4575936514408571007 \cdot 2^{56}}$
	x^{257}	Gold ($i = 8$)	$x^{57421771435671756007 \cdot 2^{59}}$
	x^{1025}	Gold ($i = 10$)	$x^{98478618118379187029 \cdot 2^{51}}$
	x^{2049}	Gold ($i = 11$)	$x^{84410284253343463131 \cdot 2^{57}}$
	x^{8193}	Gold ($i = 13$)	$x^{17363760563462479631 \cdot 2^{44}}$
	x^{16385}	Gold ($i = 14$)	$x^{98388639492805932373 \cdot 2^{43}}$
	x^{65537}	Gold ($i = 16$)	$x^{95213650476858529461 \cdot 2^{49}}$
	x^{131073}	Gold ($i = 17$)	$x^{4503565267894271 \cdot 2^{52}}$
	x^{524289}	Gold ($i = 19$)	$x^{88312042551161310619 \cdot 2^{35}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{88529988196213037491 \cdot 2^{33}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{32794219505344344519 \cdot 2^{26}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{97625845626986779317 \cdot 2^{27}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{1148426683959607807 \cdot 2^{35}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{59022375496395944755 \cdot 2^{29}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{86799725934704028013 \cdot 2^{34}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
69	$x^{2147483649}$	Gold ($i = 31$)	$x^{3253598968585138272 7\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{5712540107339161969 9\cdot 2^{33}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{34359738367\cdot 2^{35}}$
	x^{13}	Kasami ($i = 2$)	$x^{45407370027592742459\cdot 2^{61}}$
	x^{241}	Kasami ($i = 4$)	$x^{85727607313505004973\cdot 2^{46}}$
	x^{993}	Kasami ($i = 5$)	$x^{61229071970741875385\cdot 2^{52}}$
	x^{16257}	Kasami ($i = 7$)	$x^{62998291872569136569\cdot 2^{38}}$
	x^{65281}	Kasami ($i = 8$)	$x^{49127267316353642951\cdot 2^{34}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{98190387742496172885\cdot 2^{31}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{42163996511779534409\cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{61224436315675471415\cdot 2^{68}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{98370626193875187029\cdot 2^{1}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{95497377255530353333\cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{63246060104552518217\cdot 2^{55}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{42503603626023472859\cdot 2^{11}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{42574941487893350875\cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{65588423373196973399\cdot 2^{68}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{99896214061761256117\cdot 2^{58}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{63287075186799848905\cdot 2^{55}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{45052635779177281083\cdot 2^{50}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{84493962090025545133\cdot 2^{63}}$
	$x^{461168601627990425 7}$	Kasami ($i = 31$)	$x^{61521172752142521799\cdot 2^{59}}$
	$x^{184467440694145843 21}$	Kasami ($i = 32$)	$x^{49703242443389112007\cdot 2^{64}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{84327972923112123831\cdot 2^{35}}$
	$x^{17179869187}$	Welch	$x^{34723283738402657935\cdot 2^{28}}$
	$x^{17180000255}$	Niho	$x^{1501199875877547\cdot 2^{35}}$
	$x^{295147905179352825855}$	Inverse	$x^{29514790517935282585 5\cdot 2^{2}}$
71	x^{3}	Gold ($i = 1$)	$x^{78706108047827420228 3\cdot 2^{70}}$
	x^{5}	Gold ($i = 2$)	$x^{47223664828696452137 1\cdot 2^{68}}$
	x^{9}	Gold ($i = 3$)	$x^{26235369349275806743 1\cdot 2^{66}}$
	x^{17}	Gold ($i = 4$)	$x^{13889313184910721217 5\cdot 2^{64}}$
	x^{33}	Gold ($i = 5$)	$x^{71551007316206745663\cdot 2^{66}}$
	x^{65}	Gold ($i = 6$)	$x^{36325896022074193983\cdot 2^{60}}$
	x^{129}	Gold ($i = 7$)	$x^{18303746057634283775\cdot 2^{64}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
71	x^{257}	Gold ($i = 8$)	$x^{3950617874774216813 65\cdot 2^{57}}$
	x^{513}	Gold ($i = 9$)	$x^{460269637706593126 3\cdot 2^{54}}$
	x^{1025}	Gold ($i = 10$)	$x^{3939144724735167476 05\cdot 2^{52}}$
	x^{2049}	Gold ($i = 11$)	$x^{3814307725304667071 25\cdot 2^{56}}$
	x^{4097}	Gold ($i = 12$)	$x^{576320049166422015\cdot 2^{48}}$
	x^{8193}	Gold ($i = 13$)	$x^{3905044906803594103 57\cdot 2^{47}}$
	x^{16385}	Gold ($i = 14$)	$x^{3935545579712237213 01\cdot 2^{44}}$
	x^{32769}	Gold ($i = 15$)	$x^{3472349488990939661 25\cdot 2^{46}}$
	x^{65537}	Gold ($i = 16$)	$x^{3532569644974355808 51\cdot 2^{50}}$
	x^{131073}	Gold ($i = 17$)	$x^{3373170385652808230 03\cdot 2^{53}}$
	x^{262145}	Gold ($i = 18$)	$x^{9007164895264767\cdot 2^{36}}$
	x^{524289}	Gold ($i = 19$)	$x^{3808371689000779585 73\cdot 2^{35}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{2356573811612108982 27\cdot 2^{32}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{3398651097191082487 95\cdot 2^{36}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{3532830996899639082 51\cdot 2^{31}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{2361183522909807706 11\cdot 2^{26}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{3935305636953879565 65\cdot 2^{25}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{3819561136198798001 09\cdot 2^{27}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{2287968258568023425 15\cdot 2^{27}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{3386192323111715009 09\cdot 2^{35}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{3541738837753395679 23\cdot 2^{32}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{1311608341920696857 03\cdot 2^{30}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{2295434612192957708 55\cdot 2^{36}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{6931066321525893505 5\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{1301439582239512185 75\cdot 2^{36}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{2285016040452896596 23\cdot 2^{36}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{3373118917120826315 33\cdot 2^{35}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{68719476735\cdot 2^{36}}$
	x^{13}	Kasami ($i = 2$)	$x^{1816294801103709699 15\cdot 2^{60}}$
	x^{57}	Kasami ($i = 3$)	$x^{4142426739359338136 7\cdot 2^{54}}$
	x^{241}	Kasami ($i = 4$)	$x^{9797440835829174255\cdot 2^{48}}$
	x^{993}	Kasami ($i = 5$)	$x^{1735814467520060929 51\cdot 2^{62}}$
	x^{4033}	Kasami ($i = 6$)	$x^{585465718192209855\cdot 2^{36}}$
	x^{16257}	Kasami ($i = 7$)	$x^{2101637540971112793 21\cdot 2^{32}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
71	x^{65281}	Kasami ($i = 8$)	$x^{3074410249873009323 \cdot 2^{56}}$
	x^{261633}	Kasami ($i = 9$)	$x^{16931411095908660959 1 \cdot 2^{55}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{392761550969983642453 \cdot 2^{42}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{3808362973797230404 37 \cdot 2^{34}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{281543696183295 \cdot 2^{0}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{381135895287311456917 \cdot 2^{1}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{393518531373228012885 \cdot 2^{59}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{343197472997092567405 \cdot 2^{54}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{354175698849336446163 \cdot 2^{66}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{353773175944390744653 \cdot 2^{61}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{337317038565280823005 \cdot 2^{16}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{24642193120863895893 \cdot 2^{5}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{180920336215357844323 \cdot 2^{1}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1010623177270496816 53 \cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{2146541137303480843 81 \cdot 2^{21}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{472236648286967876813 \cdot 2^{1}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{46912496118443 \cdot 2^{24}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{4166793955475742816 45 \cdot 2^{64}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{915187302884377734 35 \cdot 2^{62}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{48375462630274323499 \cdot 2^{21}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{908175111628400473 01 \cdot 2^{3}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{204532359794883619283 \cdot 2^{49}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{2070807453908530166 75 \cdot 2^{2}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{2057091822846514576 93 \cdot 2^{30}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{1345529865257942268 99 \cdot 2^{30}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{2434900420456911741 95 \cdot 2^{64}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{3557947354927043940 61 \cdot 2^{66}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{1686559458216815773 99 \cdot 2^{2}}$
	$x^{34359738371}$	Welch	$x^{138893131873361145133 \cdot 2^{35}}$
	$x^{9007233614479359}$	Niho	$x^{6004799503248043 \cdot 2^{36}}$
	$x^{1180591620717411303423}$	Inverse	$x^{1180591620717411303423 \cdot 2^{2}}$
73	x^{3}	Gold ($i = 1$)	$x^{3148244321913096809131 \cdot 2^{72}}$
	x^{5}	Gold ($i = 2$)	$x^{1888946593147858085479 \cdot 2^{71}}$
	x^{9}	Gold ($i = 3$)	$x^{1049414773971032269711 \cdot 2^{70}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
73	x^{17}	Gold ($i = 4$)	$x^{5555725273964288486 71\cdot 2^{69}}$
	x^{33}	Gold ($i = 5$)	$x^{1431020146324134913243\cdot 2^{67}}$
	x^{65}	Gold ($i = 6$)	$x^{145303584088296775807\cdot 2^{67}}$
	x^{129}	Gold ($i = 7$)	$x^{13910847003802055668 29\cdot 2^{64}}$
	x^{257}	Gold ($i = 8$)	$x^{158024714990968672533 3\cdot 2^{58}}$
	x^{513}	Gold ($i = 9$)	$x^{184107855082637240 31\cdot 2^{64}}$
	x^{1025}	Gold ($i = 10$)	$x^{5252192966313556633 03\cdot 2^{54}}$
	x^{2049}	Gold ($i = 11$)	$x^{5208661908875255335 83\cdot 2^{59}}$
	x^{4097}	Gold ($i = 12$)	$x^{2305280196665679871\cdot 2^{61}}$
	x^{8193}	Gold ($i = 13$)	$x^{9141551619469373022 47\cdot 2^{50}}$
	x^{16385}	Gold ($i = 14$)	$x^{9182459331353487753 67\cdot 2^{48}}$
	x^{32769}	Gold ($i = 15$)	$x^{9445021187319617585 15\cdot 2^{46}}$
	x^{65537}	Gold ($i = 16$)	$x^{9426430616125348839 55\cdot 2^{51}}$
	x^{131073}	Gold ($i = 17$)	$x^{9140436067718210392 19\cdot 2^{52}}$
	x^{262145}	Gold ($i = 18$)	$x^{36028659580534783\cdot 2^{55}}$
	x^{524289}	Gold ($i = 19$)	$x^{1349257860456555928429\cdot 2^{36}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{1561729767800207923893\cdot 2^{35}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{1573354297586228046677\cdot 2^{33}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{36607500843174838399\cdot 2^{30}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{1388931351605775510829\cdot 2^{28}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{1574122254781543437653\cdot 2^{26}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{1416709958934644077363\cdot 2^{27}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{1431020167648006953 27\cdot 2^{27}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{1350560064235451917531\cdot 2^{29}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{1525687078908582319797\cdot 2^{35}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{1574074125492643607893\cdot 2^{31}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{1527807495741540511021\cdot 2^{32}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{1416479248189991262643\cdot 2^{35}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{2772426507265630694 71\cdot 2^{37}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{1412991546124744969627\cdot 2^{37}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{1523344026874016085421\cdot 2^{36}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{1349247566612720891611\cdot 2^{37}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{137438953471\cdot 2^{37}}$
	x^{13}	Kasami ($i = 2$)	$x^{7265179204414838790 35\cdot 2^{67}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
73	x^{57}	Kasami ($i = 3$)	$x^{1656970695743735162 79 \cdot 2^{64}}$
	x^{241}	Kasami ($i = 4$)	$x^{39189763343316557807 \cdot 2^{61}}$
	x^{993}	Kasami ($i = 5$)	$x^{14171855104684333744 11 \cdot 2^{47}}$
	x^{4033}	Kasami ($i = 6$)	$x^{2341862872734760895 \cdot 2^{55}}$
	x^{16257}	Kasami ($i = 7$)	$x^{1981087495427876014 51 \cdot 2^{53}}$
	x^{65281}	Kasami ($i = 8$)	$x^{12297640999492037291 \cdot 2^{57}}$
	x^{261633}	Kasami ($i = 9$)	$x^{8429516134546581234 65 \cdot 2^{31}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{5381918097927985159 23 \cdot 2^{45}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{8180480210198535407 63 \cdot 2^{36}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{563087392370687 \cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{8378299169530436352 99 \cdot 2^{15}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{8258961928925645764 67 \cdot 2^{68}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{7236802196483870656 91 \cdot 2^{68}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{9463179993487033434 11 \cdot 2^{51}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{3306114218960563574 99 \cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{6746289302282778331 43 \cdot 2^{20}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{1390834457679064390 221 \cdot 2^{59}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{1562017962721437637333 \cdot 2^{8}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1575657889895139683157 \cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{6589359752468348038 95 \cdot 2^{23}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{1666717582189302336333 \cdot 2^{72}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{187649984473771 \cdot 2^{25}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{1888946593147911772571 \cdot 2^{70}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{8586126336853448716 45 \cdot 2^{19}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{4042492709071458741 97 \cdot 2^{68}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{1525723090122000980661 \cdot 2^{63}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{1574218236282672952661 \cdot 2^{46}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{1371029381644178273709 \cdot 2^{53}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{3625495573482857683 89 \cdot 2^{34}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{5468917408053933236 71 \cdot 2^{33}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{7155188095481472892 45 \cdot 2^{27}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{9828956634846873224 5 \cdot 2^{64}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{1423178940103153989213 \cdot 2^{72}}$
	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{1349247566612720891613 \cdot 2^{72}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
73	$x^{68719476739}$	Welch	$x^{4861259614749069842 07\cdot 2^{40}}$
	$x^{68719738879}$	Niho	$x^{6004822409652907\cdot 2^{56}}$
	$x^{4722366482869645213695}$	Inverse	$x^{4722366482869645213695\cdot 2^2}$
75	x^3	Gold ($i=1$)	$x^{1259297728765238723 6523\cdot 2^{74}}$
	x^5	Gold ($i=2$)	$x^{7555786372591432341915\cdot 2^{72}}$
	x^{17}	Gold ($i=4$)	$x^{6666870328757146184045\cdot 2^{69}}$
	x^{129}	Gold ($i=7$)	$x^{3807179179987931025011\cdot 2^{64}}$
	x^{257}	Gold ($i=8$)	$x^{3674993371882992384231\cdot 2^{62}}$
	x^{2049}	Gold ($i=11$)	$x^{3779736960422751659827\cdot 2^{56}}$
	x^{8193}	Gold ($i=13$)	$x^{5399625193643700280173\cdot 2^{50}}$
	x^{16385}	Gold ($i=14$)	$x^{1109042796831394250271\cdot 2^{52}}$
	x^{65537}	Gold ($i=16$)	$x^{5724167926502046423 35\cdot 2^{49}}$
	x^{131073}	Gold ($i=17$)	$x^{2082448579874310448071\cdot 2^{52}}$
	x^{524289}	Gold ($i=19$)	$x^{7205745599498751\cdot 2^{38}}$
	$x^{4194305}$	Gold ($i=22$)	$x^{6111230114923631977901\cdot 2^{37}}$
	$x^{8388609}$	Gold ($i=23$)	$x^{6102750566351538705077\cdot 2^{30}}$
	$x^{67108865}$	Gold ($i=26$)	$x^{3672951716717363229127\cdot 2^{29}}$
	$x^{268435457}$	Gold ($i=28$)	$x^{3682157115369875097 5\cdot 2^{29}}$
	$x^{536870913}$	Gold ($i=29$)	$x^{5652529032222744137115\cdot 2^{38}}$
	$x^{2147483649}$	Gold ($i=31$)	$x^{5437841619149711961243\cdot 2^{33}}$
	$x^{4294967297}$	Gold ($i=32$)	$x^{6293412686747431250773\cdot 2^{34}}$
	$x^{17179869185}$	Gold ($i=34$)	$x^{6246909993641489291957\cdot 2^{36}}$
	$x^{137438953473}$	Gold ($i=37$)	$x^{274877906943\cdot 2^{38}}$
	x^{13}	Kasami ($i=2$)	$x^{2906071681765935516123\cdot 2^{70}}$
	x^{241}	Kasami ($i=4$)	$x^{5486566868064318090669\cdot 2^{61}}$
	x^{16257}	Kasami ($i=7$)	$x^{2883905667831145795239\cdot 2^{35}}$
	x^{65281}	Kasami ($i=8$)	$x^{3144145108246603674055\cdot 2^{37}}$
	$x^{4192257}$	Kasami ($i=11$)	$x^{2883323637381053838891\cdot 2^{40}}$
	$x^{67100673}$	Kasami ($i=13$)	$x^{5396992839936384916333\cdot 2^{73}}$
	$x^{268419073}$	Kasami ($i=14$)	$x^{3918363360048332501561\cdot 2^{73}}$
	$x^{4294901761}$	Kasami ($i=16$)	$x^{3923267720516108767673\cdot 2^{56}}$
	$x^{17179738113}$	Kasami ($i=17$)	$x^{3937355056274553000391\cdot 2^{55}}$
	$x^{274877382657}$	Kasami ($i=19$)	$x^{4047747846588281360969\cdot 2^{59}}$
	$x^{17592181850113}$	Kasami ($i=22$)	$x^{5523307569610008864181\cdot 2^{19}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
75	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{6393357699885124211893 \cdot 2^{72}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{4197659095884158905003 \cdot 2^{73}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{40503728118523120470 49 \cdot 2^{59}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{27017885311953138111 63 \cdot 2^{16}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{2698834831893059057369 \cdot 2^{53}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{62934171903449111381 33 \cdot 2^{66}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{62480629855062503779 41 \cdot 2^{29}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{53969902662545422043 43 \cdot 2^{38}}$
	$x^{137438953475}$	Welch	$x^{21528435436626776594 07 \cdot 2^{43}}$
	$x^{72057731476881407}$	Niho	$x^{24019289638611627 \cdot 2^{57}}$
	$x^{1888946593147858085 4783}$	Inverse	$x^{1888946593147858085 4783 \cdot 2^{2}}$
	$x^{1152956690052710399}$	Dobbertin	$x^{6296584723550364677461 \cdot 2^{1}}$
77	x^{3}	Gold ($i = 1$)	$x^{5037190915060954894 6091 \cdot 2^{76}}$
	x^{5}	Gold ($i = 2$)	$x^{3022314549036572936 7655 \cdot 2^{75}}$
	x^{9}	Gold ($i = 3$)	$x^{1679063638353651631 5367 \cdot 2^{72}}$
	x^{17}	Gold ($i = 4$)	$x^{2666748131502858473 6173 \cdot 2^{70}}$
	x^{33}	Gold ($i = 5$)	$x^{2289632234118615861 1867 \cdot 2^{69}}$
	x^{65}	Gold ($i = 6$)	$x^{2557343079954023254 1877 \cdot 2^{67}}$
	x^{257}	Gold ($i = 8$)	$x^{2175596076154731491 4523 \cdot 2^{63}}$
	x^{513}	Gold ($i = 9$)	$x^{2444952315497422551 1853 \cdot 2^{65}}$
	x^{1025}	Gold ($i = 10$)	$x^{2167220676626225471 7805 \cdot 2^{58}}$
	x^{4097}	Gold ($i = 12$)	$x^{1464313980922039853 4259 \cdot 2^{61}}$
	x^{8193}	Gold ($i = 13$)	$x^{1844449254874022707 1 \cdot 2^{52}}$
	x^{32769}	Gold ($i = 15$)	$x^{1511203389971138808 7091 \cdot 2^{48}}$
	x^{65537}	Gold ($i = 16$)	$x^{8395446292203001409 991 \cdot 2^{49}}$
	x^{131073}	Gold ($i = 17$)	$x^{2513695578519008481 5573 \cdot 2^{53}}$
	x^{262145}	Gold ($i = 18$)	$x^{1462417703837739015 2935 \cdot 2^{57}}$
	x^{524289}	Gold ($i = 19$)	$x^{288229826396946431 \cdot 2^{58}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{2158800224027570324 8603 \cdot 2^{39}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{5857020689176602544 63 \cdot 2^{39}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{4436162462134362995 743 \cdot 2^{34}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{2266735934295428007 1987 \cdot 2^{29}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{2518595495060475460 5397 \cdot 2^{27}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{8333587915085771116 303 \cdot 2^{31}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
77	$x^{536870913}$	Gold ($i = 29$)	$x^{1472860034141598525 43 \cdot 2^{39}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{44445463138547824146 07 \cdot 2^{35}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{25185185972696851862869 \cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{11622867749457200374 39 \cdot 2^{33}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{15082000196881039025779 \cdot 2^{37}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{24373504428849277621941 \cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{21587961065175241907053 \cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{549755813887 \cdot 2^{39}}$
	x^{13}	Kasami ($i = 2$)	$x^{11624286727063742064483 \cdot 2^{74}}$
	x^{57}	Kasami ($i = 3$)	$x^{13255765565949881301603 \cdot 2^{73}}$
	x^{241}	Kasami ($i = 4$)	$x^{21946267472257272362413 \cdot 2^{66}}$
	x^{993}	Kasami ($i = 5$)	$x^{22674968167494933179595 \cdot 2^{49}}$
	x^{4033}	Kasami ($i = 6$)	$x^{24392843682405268806325 \cdot 2^{55}}$
	x^{65281}	Kasami ($i = 8$)	$x^{13451593759632877237837 \cdot 2^{33}}$
	x^{261633}	Kasami ($i = 9$)	$x^{24445199699365237929133 \cdot 2^{29}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{22188148146292569824045 \cdot 2^{35}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{12186157157632183471203 \cdot 2^{54}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{4504149383176191 \cdot 2^{0}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{58120103354809035942 99 \cdot 2^{65}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{13257181459155145282 47 \cdot 2^{65}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{98383388591775503701 \cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{52897653621422185197 99 \cdot 2^{62}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{21588002240550581155547 \cdot 2^{58}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{62107407611254867177 17 \cdot 2^{12}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{13524262717386590332649 \cdot 2^{19}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{13737810873219340725405 \cdot 2^{23}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{30223145490365783054747 \cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{750599937895083 \cdot 2^{26}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{88891607032604867181 63 \cdot 2^{25}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{10762388464430327080119 \cdot 2^{21}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{313556377726093500399 \cdot 2^{52}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{25186338894200921838933 \cdot 2^{48}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{18734938990678900671 \cdot 2^{52}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{15141087985181156782899 \cdot 2^{62}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
77	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{7863164626169887126 19 \cdot 2^{6}}$
	$x^{1888946593134114190 1313}$	Kasami ($i = 37$)	$x^{2277086304122873333 0013 \cdot 2^{38}}$
	$x^{7555786372563944551 2193}$	Kasami ($i = 38$)	$x^{1079398053231274304 6583 \cdot 2^{2}}$
	$x^{274877906947}$	Welch	$x^{6666870328781400117007 \cdot 2^{41}}$
	$x^{274878431231}$	Niho	$x^{96076792050920107 \cdot 2^{39}}$
	$x^{7555786372591432341 9135}$	Inverse	$x^{7555786372591432341 9135 \cdot 2^{2}}$
79	x^{3}	Gold ($i = 1$)	$x^{2014876366024381957 84363 \cdot 2^{78}}$
	x^{5}	Gold ($i = 2$)	$x^{1208925819614629174 70619 \cdot 2^{76}}$
	x^{9}	Gold ($i = 3$)	$x^{6716254553414606526 1455 \cdot 2^{76}}$
	x^{17}	Gold ($i = 4$)	$x^{3555664175337144631 4895 \cdot 2^{72}}$
	x^{33}	Gold ($i = 5$)	$x^{1831705787294892688 9503 \cdot 2^{70}}$
	x^{65}	Gold ($i = 6$)	$x^{1022937231981609309 167477 \cdot 2^{68}}$
	x^{129}	Gold ($i = 7$)	$x^{6091486687980689639 9987 \cdot 2^{66}}$
	x^{257}	Gold ($i = 8$)	$x^{2351995758005115126 015 \cdot 2^{64}}$
	x^{513}	Gold ($i = 9$)	$x^{9072835098472363201 9891 \cdot 2^{65}}$
	x^{1025}	Gold ($i = 10$)	$x^{5897199120071361832 95 \cdot 2^{60}}$
	x^{2049}	Gold ($i = 11$)	$x^{6047579136676402655 4163 \cdot 2^{58}}$
	x^{4097}	Gold ($i = 12$)	$x^{9044075267558795265 9867 \cdot 2^{64}}$
	x^{8193}	Gold ($i = 13$)	$x^{73777970194960891903 \cdot 2^{66}}$
	x^{16385}	Gold ($i = 14$)	$x^{9750353802995010402 4493 \cdot 2^{53}}$
	x^{32769}	Gold ($i = 15$)	$x^{8889214691816805508 2285 \cdot 2^{50}}$
	x^{65537}	Gold ($i = 16$)	$x^{1007453555064360168 87125 \cdot 2^{49}}$
	x^{131073}	Gold ($i = 17$)	$x^{9154126906132608972 863 \cdot 2^{57}}$
	x^{262145}	Gold ($i = 18$)	$x^{3331699854586541216 7567 \cdot 2^{58}}$
	x^{524289}	Gold ($i = 19$)	$x^{8635250306921956264 2285 \cdot 2^{58}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{576460202548658175 \cdot 2^{40}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{9749416647485136691 7813 \cdot 2^{38}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{1774360184068311391 4127 \cdot 2^{36}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{3357717749430007214 1767 \cdot 2^{37}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{8668654146860246809 2269 \cdot 2^{32}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{9778076508668910299 8829 \cdot 2^{31}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{1007438198024189848 67157 \cdot 2^{28}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{6044629143109143489 4131 \cdot 2^{28}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{8700602491356649425 6283 \cdot 2^{30}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
79	$x^{536870913}$	Gold ($i = 29$)	$x^{585058944809248557037783 \cdot 2^{32}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{864358429857166252541 07 \cdot 2^{40}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{587671632950925112263 11 \cdot 2^{37}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{906685141409305917980 67 \cdot 2^{34}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{464914702995536791974 3 \cdot 2^{40}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{100694602970358119837013 \cdot 2^{35}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{100546667976269158001365 \cdot 2^{37}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{999505598938311518727 25 \cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{584964106287842743947 39 \cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{863518442588160905520 27 \cdot 2^{40}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{1099511627775 \cdot 2^{40}}$
	x^{13}	Kasami ($i = 2$)	$x^{464971469082549682579 31 \cdot 2^{75}}$
	x^{57}	Kasami ($i = 3$)	$x^{530230622637995252064 83 \cdot 2^{67}}$
	x^{241}	Kasami ($i = 4$)	$x^{526710419334174536700 43 \cdot 2^{63}}$
	x^{993}	Kasami ($i = 5$)	$x^{444368503685135595795 351 \cdot 2^{66}}$
	x^{4033}	Kasami ($i = 6$)	$x^{975713747296210752211 73 \cdot 2^{62}}$
	x^{16257}	Kasami ($i = 7$)	$x^{486708463392861410704 35 \cdot 2^{50}}$
	x^{65281}	Kasami ($i = 8$)	$x^{433432527199037941116 71 \cdot 2^{57}}$
	x^{261633}	Kasami ($i = 9$)	$x^{906695519884310728408 83 \cdot 2^{29}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{539488309922600057357 3193 \cdot 2^{33}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{232457396533764669691 47 \cdot 2^{38}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{238163443486370707032 21 \cdot 2^{15}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{9008298766360575 \cdot 2^{40}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{877446171020616672677 49 \cdot 2^{1}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{125499093519572182856 11 \cdot 2^{16}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{100740743890787407418 709 \cdot 2^{1}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{538063487717984553791 65 \cdot 2^{77}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{344454924930114159131 71 \cdot 2^{77}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{910835153376115597217 73 \cdot 2^{58}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{431759633047833843747 11 \cdot 2^{21}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{314526598680531628817 1 \cdot 2^{22}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{125422549331440226302 3023 \cdot 2^{75}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{530747920806851642264 7647 \cdot 2^{70}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{890294208243336889859 65 \cdot 2^{74}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
79	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{1066699252601145915898 05 \cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{3002399751580331 \cdot 2^{27}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{1208925819614629711577 09 \cdot 2^{78}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{5495120855586207178505 3 \cdot 2^{19}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{1176012234445416480895 5 \cdot 2^{14}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{9056618511998534717614 1 \cdot 2^{67}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{5301270682903106572963 5 \cdot 2^{61}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{4577063453121279648389 9 \cdot 2^{55}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{74363366128709795775 \cdot 2^{73}}$
	$x^{29514790516217295667 3}$	Kasami ($i = 34$)	$x^{1006946750279435678303 57 \cdot 2^{35}}$
	$x^{11805916206830515650 57}$	Kasami ($i = 35$)	$x^{3935335367748491236696 2^{62}}$
	$x^{47223664828009257369 61}$	Kasami ($i = 36$)	$x^{9996900720082045509909 3 \cdot 2^{66}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{6233345055918153648056 3 \cdot 2^{70}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{2484094150664237966414 9 \cdot 2^{74}}$
	$x^{30223145490310753786265 7}$	Kasami ($i = 39$)	$x^{8635184425881609055202 9 \cdot 2^{78}}$
	$x^{549755813891}$	Welch	$x^{3555664176578945999329 5 \cdot 2^{34}}$
	$x^{576461302059237375}$	Niho	$x^{384307168202631851 \cdot 2^{40}}$
	$x^{30223145490365729367 6543}$	Inverse	$x^{3022314549036572936765 43 \cdot 2^{2}}$
81	x^{3}	Gold ($i = 1$)	$x^{8059505464097527831374 51 \cdot 2^{80}}$
	x^{5}	Gold ($i = 2$)	$x^{4835703278458516698824 71 \cdot 2^{79}}$
	x^{17}	Gold ($i = 4$)	$x^{1422265670134857852595 51 \cdot 2^{77}}$
	x^{33}	Gold ($i = 5$)	$x^{7326823149179570755795 1 \cdot 2^{76}}$
	x^{129}	Gold ($i = 7$)	$x^{3561176832973326251073 09 \cdot 2^{68}}$
	x^{257}	Gold ($i = 8$)	$x^{9407983032020460503551 \cdot 2^{73}}$
	x^{1025}	Gold ($i = 10$)	$x^{2358879648028544731135 \cdot 2^{71}}$
	x^{2049}	Gold ($i = 11$)	$x^{1333417448672065365953 43 \cdot 2^{63}}$
	x^{8193}	Gold ($i = 13$)	$x^{3455760123931968176689 73 \cdot 2^{66}}$
	x^{16385}	Gold ($i = 14$)	$x^{3454495384458769481868 43 \cdot 2^{55}}$
	x^{65537}	Gold ($i = 16$)	$x^{4029814220257440675157 33 \cdot 2^{50}}$
	x^{131073}	Gold ($i = 17$)	$x^{3911233305606643990971 33 \cdot 2^{53}}$
	x^{524289}	Gold ($i = 19$)	$x^{3899772609536796953614 53 \cdot 2^{59}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{2305840810192535551 \cdot 2^{61}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{3998025300574313144265 81 \cdot 2^{38}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{4027785559966033711383 89 \cdot 2^{36}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
81	$x^{33554433}$	Gold ($i = 25$)	$x^{399875463688137319600821 \cdot 2^{33}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{235068909869911187943879 \cdot 2^{32}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{134325091568692104032711 \cdot 2^{29}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{366165031913333383696447 \cdot 2^{35}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{234287931667330784349811 \cdot 2^{39}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{241783319304813888828211 \cdot 2^{35}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{348021863345171870737627 \cdot 2^{41}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{362618687483835422710579 \cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{361725835794636681828787 \cdot 2^{39}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{233985642507192239365351 \cdot 2^{41}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{2199023255551 \cdot 2^{41}}$
	x^{13}	Kasami ($i = 2$)	$x^{185988587633019873031739 \cdot 2^{73}}$
	x^{241}	Kasami ($i = 4$)	$x^{250814485397225969856087 \cdot 2^{68}}$
	x^{993}	Kasami ($i = 5$)	$x^{250794278792158721045177 \cdot 2^{58}}$
	x^{16257}	Kasami ($i = 7$)	$x^{345492363777423223516525 \cdot 2^{40}}$
	x^{65281}	Kasami ($i = 8$)	$x^{258040967057953205300681 \cdot 2^{43}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{258928999719972058262985 \cdot 2^{44}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{250809622574795696870727 \cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{345407397623148373039981 \cdot 2^{40}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{172703693663660745273929 \cdot 2^{1}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{402972198794444701095253 \cdot 2^{67}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{351130483236517776238005 \cdot 2^{78}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{391156699584860217841069 \cdot 2^{64}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{259055573950449221145161 \cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{399839422410951719480021 \cdot 2^{68}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{403073631826605087829333 \cdot 2^{72}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{409174892792644777892533 \cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{268650182136584290871979 \cdot 2^{1}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{268650182136584738264407 \cdot 2^{77}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{260384022686229936689849 \cdot 2^{73}}$
	$x^{461168601627990425 7}$	Kasami ($i = 31$)	$x^{184717527618430669524679 \cdot 2^{14}}$
	$x^{1844674406941458 4321}$	Kasami ($i = 32$)	$x^{184535596135017972135483 \cdot 2^{58}}$
	$x^{2951479051621729 56673}$	Kasami ($i = 34$)	$x^{172724852851046795294425 \cdot 2^{77}}$
	$x^{1180591620683051 565057}$	Kasami ($i = 35$)	$x^{174368558539503924251099 \cdot 2^{76}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
81	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{17409468911460250630908 3\cdot 2^{71}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{20358448057091919312762 3\cdot 2^{73}}$
	$x^{12089258196135296630784 01}$	Kasami ($i = 40$)	$x^{34540737703369363131128 7\cdot 2^{41}}$
	$x^{1099511627779}$	Welch	$x^{14000427690390613334811 1\cdot 2^{47}}$
	$x^{1099512676351}$	Niho	$x^{384307534706158251\cdot 2^{62}}$
	$x^{12089258196146291747061 75}$	Inverse	$x^{12089258196146291747061 75\cdot 2^{2}}$
83	x^{3}	Gold ($i = 1$)	$x^{32238021856390111325498 03\cdot 2^{82}}$
	x^{5}	Gold ($i = 2$)	$x^{19342813113838406795298 83\cdot 2^{80}}$
	x^{9}	Gold ($i = 3$)	$x^{10746007285463370441832 71\cdot 2^{78}}$
	x^{17}	Gold ($i = 4$)	$x^{17067188041618294231146 05\cdot 2^{77}}$
	x^{33}	Gold ($i = 5$)	$x^{14653646298359141511590 03\cdot 2^{77}}$
	x^{65}	Gold ($i = 6$)	$x^{14879087010641589842540 7\cdot 2^{72}}$
	x^{129}	Gold ($i = 7$)	$x^{74972143852070026338431\cdot 2^{70}}$
	x^{257}	Gold ($i = 8$)	$x^{13923814887390285145254 03\cdot 2^{74}}$
	x^{513}	Gold ($i = 9$)	$x^{14516536157555781123178 75\cdot 2^{67}}$
	x^{1025}	Gold ($i = 10$)	$x^{13870212330407843019067 97\cdot 2^{71}}$
	x^{2049}	Gold ($i = 11$)	$x^{15623404442847916323201 81\cdot 2^{62}}$
	x^{4097}	Gold ($i = 12$)	$x^{16122945273064031756404 05\cdot 2^{61}}$
	x^{8193}	Gold ($i = 13$)	$x^{93609488583366379645258 3\cdot 2^{68}}$
	x^{16385}	Gold ($i = 14$)	$x^{5902597837605757419 51\cdot 2^{56}}$
	x^{32769}	Gold ($i = 15$)	$x^{15993576896436699443144 05\cdot 2^{54}}$
	x^{65537}	Gold ($i = 16$)	$x^{53730856270099209001005 5\cdot 2^{52}}$
	x^{131073}	Gold ($i = 17$)	$x^{14507146728582224686415 87\cdot 2^{53}}$
	x^{262145}	Gold ($i = 18$)	$x^{14221278626312952235564 61\cdot 2^{59}}$
	x^{524289}	Gold ($i = 19$)	$x^{14469045051582263763142 67\cdot 2^{61}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{13816321433776449911334 03\cdot 2^{62}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{4611683819406229503\cdot 2^{42}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{93594376013646618019800 3\cdot 2^{40}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{28389651037279329899267 1\cdot 2^{42}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{96702265418274026909880 3\cdot 2^{38}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{18815966624800407748863\cdot 2^{34}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{14653646516715487182748 7\cdot 2^{32}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{96714066289746275697950 7\cdot 2^{30}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{16119010988243051141748 05\cdot 2^{29}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
83	$x^{536870913}$	Gold ($i = 29$)	$x^{28445313455680683658830 3\cdot 2^{30}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{96526635210412949640 1523\cdot 2^{33}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{47177592982539683768 31\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{15995017827036160249924 37\cdot 2^{40}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{16118887951777745093809 49\cdot 2^{35}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{53334854120004885568283 1\cdot 2^{38}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{15644748733916613415827 65\cdot 2^{41}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{94021001703103001619501 5\cdot 2^{39}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{16087466875850533019758 93\cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{53306965276118924092307 9\cdot 2^{39}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{15599042833782549831162 05\cdot 2^{41}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{13816295081360311099626 05\cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{43980465111103\cdot 2^{42}}$
	x^{13}	Kasami ($i = 2$)	$x^{74395435053207949212703 5\cdot 2^{72}}$
	x^{57}	Kasami ($i = 3$)	$x^{84836899622079240330286 7\cdot 2^{69}}$
	x^{241}	Kasami ($i = 4$)	$x^{20065158831778077588484 3\cdot 2^{76}}$
	x^{993}	Kasami ($i = 5$)	$x^{41880209662379902930405 3\cdot 2^{76}}$
	x^{4033}	Kasami ($i = 6$)	$x^{71222607175907734170639 1\cdot 2^{73}}$
	x^{16257}	Kasami ($i = 7$)	$x^{594907212703403605887\cdot 2^{42}}$
	x^{65281}	Kasami ($i = 8$)	$x^{14487628057182284227314 69\cdot 2^{47}}$
	x^{261633}	Kasami ($i = 9$)	$x^{14507128318148455251836 67\cdot 2^{31}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{14241775872566492148104 77\cdot 2^{48}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{50395735813871285699243\cdot 2^{67}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{16111139356857029484004 69\cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{85793783495551809916425 9\cdot 2^{59}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{72061992084422655\cdot 2^{0}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{15992095392479196535467 09\cdot 2^{77}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{55144049487670466172360 3\cdot 2^{53}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{37198852713019806995629 3\cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{14224045638006815637619 65\cdot 2^{59}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{73268203760540236817526 1\cdot 2^{77}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{14573352661910981892317 07\cdot 2^{65}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{13816321433776449911334 05\cdot 2^{19}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{99737094924086227093432 3\cdot 2^{8}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
83	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{194785728640989999222255 \cdot 2^{10}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{741049697138103718061923 \cdot 2^{80}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{865543626429312073807593 \cdot 2^{20}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{879219336893793148560605 \cdot 2^{24}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{193428131138340673321697 3 \cdot 2^{1}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{12009599006321323 \cdot 2^{28}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{568906276531307145500311 \cdot 2^{26}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{374860719260418318459515 \cdot 2^{70}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{688792859473937997309367 \cdot 2^{22}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{156173214513573117829806 9 \cdot 2^{14}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{161192568838444695177352 5 \cdot 2^{52}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{837720390798927844560539 \cdot 2^{56}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{140393293402314520230033 3 \cdot 2^{80}}$
	$x^{472236648280092573696 1}$	Kasami ($i = 36$)	$x^{169343699623203535522043 \cdot 2^{34}}$
	$x^{188894659313411419013 13}$	Kasami ($i = 37$)	$x^{314823233577038319889 1 \cdot 2^{10}}$
	$x^{755578637256394455121 93}$	Kasami ($i = 38$)	$x^{802387655296506826762 15 \cdot 2^{70}}$
	$x^{302231454903107537862657}$	Kasami ($i = 39$)	$x^{156462679411677530624530 1 \cdot 2^{36}}$
	$x^{120892581961352966307840 1}$	Kasami ($i = 40$)	$x^{198727531991506138945003 \cdot 2^{4}}$
	$x^{483570327845631767556915 3}$	Kasami ($i = 41$)	$x^{690814754065816531725751 \cdot 2^{2}}$
	$x^{2199023255555}$	Welch	$x^{568906268057047644457803 \cdot 2^{40}}$
	$x^{4611688217450643455}$	Niho	$x^{1537230138824633003 \cdot 2^{63}}$
	$x^{483570327845851669882 4703}$	Inverse	$x^{483570327845851669882 4703 \cdot 2^{2}}$
85	x^{3}	Gold ($i = 1$)	$x^{128952087425560445301992 11 \cdot 2^{84}}$
	x^{5}	Gold ($i = 2$)	$x^{773712524553362671811952 7 \cdot 2^{83}}$
	x^{9}	Gold ($i = 3$)	$x^{429840291418534817673307 1 \cdot 2^{82}}$
	x^{17}	Gold ($i = 4$)	$x^{682687521664731769245841 3 \cdot 2^{78}}$
	x^{65}	Gold ($i = 6$)	$x^{595163480425663593701503 \cdot 2^{79}}$
	x^{129}	Gold ($i = 7$)	$x^{299888575408280105353471 \cdot 2^{78}}$
	x^{257}	Gold ($i = 8$)	$x^{376319321280818420142000 7 \cdot 2^{75}}$
	x^{513}	Gold ($i = 9$)	$x^{625907792767340173103249 3 \cdot 2^{69}}$
	x^{2049}	Gold ($i = 11$)	$x^{553191238882711719963209 1 \cdot 2^{65}}$
	x^{4097}	Gold ($i = 12$)	$x^{644917810922561270255957 3 \cdot 2^{62}}$
	x^{8193}	Gold ($i = 13$)	$x^{639802557530700854574149 3 \cdot 2^{67}}$
	x^{16385}	Gold ($i = 14$)	$x^{236103913504230293503 9 \cdot 2^{71}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
85	x^{65537}	Gold ($i = 16$)	$x^{5861547956738095527352 63\cdot 2^{54}}$
	x^{262145}	Gold ($i = 18$)	$x^{5568386711356698334031003\cdot 2^{56}}$
	x^{524289}	Gold ($i = 19$)	$x^{6435023715815448347323221\cdot 2^{58}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{18446735277620723711\cdot 2^{64}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{5526523303021069276207981\cdot 2^{42}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{5787614534642752251812275\cdot 2^{41}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{5801899576202084694465331\cdot 2^{39}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{3748607194837845318354547\cdot 2^{34}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{2133398506261957279944463\cdot 2^{35}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{6447604395297220322481493\cdot 2^{30}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{5802843937753099767329587\cdot 2^{31}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{6397428461808960614509269\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{1887102819021037240524 7\cdot 2^{43}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{1135657518253067665423903\cdot 2^{43}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{2148939071404862795736007\cdot 2^{40}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{5688506836744669558828333\cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{3860992050190026634323763\cdot 2^{39}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{2132278610978266811713423\cdot 2^{43}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{5526518032529045423240923\cdot 2^{43}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{8796093022207\cdot 2^{43}}$
	x^{13}	Kasami ($i = 2$)	$x^{2975817402128317968507515\cdot 2^{79}}$
	x^{57}	Kasami ($i = 3$)	$x^{3393475984883169613210323\cdot 2^{77}}$
	x^{241}	Kasami ($i = 4$)	$x^{8026063532711231035393 71\cdot 2^{77}}$
	x^{4033}	Kasami ($i = 6$)	$x^{3443625047293047349159129\cdot 2^{58}}$
	x^{16257}	Kasami ($i = 7$)	$x^{2379628850813073358719\cdot 2^{64}}$
	x^{65281}	Kasami ($i = 8$)	$x^{3383162637425246479162547\cdot 2^{38}}$
	x^{261633}	Kasami ($i = 9$)	$x^{6257971123037242708505773\cdot 2^{33}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{3443575578740794596308557\cdot 2^{34}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{6444455742742811776822613\cdot 2^{50}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{6244530220121750386858645\cdot 2^{47}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{144123984168861695\cdot 2^{43}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{2844253274116409216252055\cdot 2^{17}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{1655731522740350471211637\cdot 2^{73}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{1259300125993781445700 3\cdot 2^{29}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
85	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{2763261651510534637055415 \cdot 2^{23}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{7949101911394441470827 31 \cdot 2^{23}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{2929593404762728861723805 \cdot 2^{70}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{1487364167325607654810309 \cdot 2^{27}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{1499442877041400793121915 \cdot 2^{83}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{2275625140034684599849683 \cdot 2^{29}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{48038396025285291 \cdot 2^{29}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{7737125245533627577112987 \cdot 2^{82}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{6472692326030145278528213 \cdot 2^{72}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{3455086364493172221523785 \cdot 2^{14}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{4013773734891540973 1567 \cdot 2^{15}}$
	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{3351021293899154149665235 \cdot 2^{79}}$
	$x^{1888946593134114190 1313}$	Kasami ($i = 37$)	$x^{5622947397513993750530413 \cdot 2^{72}}$
	$x^{7555786372563944551 2193}$	Kasami ($i = 38$)	$x^{3876118416331090500072243 \cdot 2^{68}}$
	$x^{3022314549031075378 62657}$	Kasami ($i = 39$)	$x^{3209550531861316 47547383 \cdot 2^{82}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{5829340938450448551876301 \cdot 2^{40}}$
	$x^{1934281311382966874878 7713}$	Kasami ($i = 42$)	$x^{5526518032529045423240925 \cdot 2^{84}}$
	$x^{4398046511107}$	Welch	$x^{2275625072414460783007375 \cdot 2^{36}}$
	$x^{4398048608255}$	Niho	$x^{6148914691237915307 \cdot 2^{43}}$
	$x^{1934281311383406679529 8815}$	Inverse	$x^{1934281311383406679529 8815 \cdot 2^{2}}$
	$x^{295150156996346511359}$	Dobbertin	$x^{6447628967124438627308885 \cdot 2^{1}}$
87	x^{3}	Gold ($i = 1$)	$x^{5158083497022417812079 6843 \cdot 2^{86}}$
	x^{5}	Gold ($i = 2$)	$x^{3094850098213450687247 8107 \cdot 2^{84}}$
	x^{17}	Gold ($i = 4$)	$x^{9102500288863090256611215 \cdot 2^{80}}$
	x^{33}	Gold ($i = 5$)	$x^{2344583407737462641854 4027 \cdot 2^{79}}$
	x^{129}	Gold ($i = 7$)	$x^{2279153173102928800686 3725 \cdot 2^{78}}$
	x^{257}	Gold ($i = 8$)	$x^{2589076930412030730576 9685 \cdot 2^{73}}$
	x^{1025}	Gold ($i = 10$)	$x^{8605192956008131179176903 \cdot 2^{71}}$
	x^{2049}	Gold ($i = 11$)	$x^{7552098824337361364787 1 \cdot 2^{66}}$
	x^{8193}	Gold ($i = 13$)	$x^{4551805649148307186786063 \cdot 2^{66}}$
	x^{16385}	Gold ($i = 14$)	$x^{2210877046053612468369 5835 \cdot 2^{72}}$
	x^{65537}	Gold ($i = 16$)	$x^{1544426392145977153767 9987 \cdot 2^{58}}$
	x^{131073}	Gold ($i = 17$)	$x^{2321143476573155949816 7091 \cdot 2^{55}}$
	x^{524289}	Gold ($i = 19$)	$x^{1504336488614498569284 6311 \cdot 2^{63}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
87	$x^{1048577}$	Gold ($i = 20$)	$x^{255873805156386023301024 53\cdot 2^{62}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{36893479351330275327\cdot 2^{44}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{14975083500612422640835815\cdot 2^{44}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{25787270009498314459491669\cdot 2^{39}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{30105316463990736198092 7\cdot 2^{44}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{85968058603962937185694 15\cdot 2^{32}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{11903269614056163888292 47\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{24960901133269316605879725\cdot 2^{34}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{22756242041601903202757933\cdot 2^{39}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{25790220720592575156409685\cdot 2^{36}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{15472361314002408393041715\cdot 2^{40}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{23434380326366923876587 83\cdot 2^{39}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{23150453490581921675529627\cdot 2^{44}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{24958468534015760378025653\cdot 2^{42}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{17592186044415\cdot 2^{44}}$
	x^{13}	Kasami ($i = 2$)	$x^{11903269608513271874030043\cdot 2^{82}}$
	x^{241}	Kasami ($i = 4$)	$x^{16052127065422462070787671\cdot 2^{71}}$
	x^{993}	Kasami ($i = 5$)	$x^{11064167017782225518425817\cdot 2^{61}}$
	x^{16257}	Kasami ($i = 7$)	$x^{22111511281755077648018797\cdot 2^{64}}$
	x^{65281}	Kasami ($i = 8$)	$x^{25588537867231047452043989\cdot 2^{49}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{16117961514422861898805703\cdot 2^{44}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{16571455977568012881063497\cdot 2^{46}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{16049614021287462406237751\cdot 2^{47}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{11053036106226319359849033\cdot 2^{46}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{11810097950558706598760103\cdot 2^{80}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{11159311001051078586110267\cdot 2^{76}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{12897307576122823792030151\cdot 2^{62}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{25592029095145726892919509\cdot 2^{82}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{16579556732822153078805065\cdot 2^{68}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{13029549718260027278731975\cdot 2^{10}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{25796712436902519512935765\cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{16590327037206609141214665\cdot 2^{82}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{17193611656741393184150871\cdot 2^{86}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{16664577451918614454769081\cdot 2^{77}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
87	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{22623182437947218219931061 \cdot 2^{15}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{22151945147706314832047533 \cdot 2^{58}}$
	$x^{118059162068305156505 7}$	Kasami ($i = 35$)	$x^{25790515868497745919300949 \cdot 2^{54}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{11810241264714162629277243 \cdot 2^{83}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{16069704583093241911153081 \cdot 2^{73}}$
	$x^{120892581961352966307840 1}$	Kasami ($i = 40$)	$x^{11142060094399907476164315 \cdot 2^{86}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{25034028704709484276798645 \cdot 2^{78}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{22106072130103615845789111 \cdot 2^{44}}$
	$x^{8796093022211}$	Welch	$x^{91025002888692992634504 13 \cdot 2^{43}}$
	$x^{36893496943512125439}$	Niho	$x^{24595658764947466923 \cdot 2^{44}}$
	$x^{77371252455336267181195263}$	Inverse	$x^{77371252455336267181195263 \cdot 2^2}$
89	x^3	Gold ($i = 1$)	$x^{20632333988089671248318737 1 \cdot 2^{88}}$
	x^5	Gold ($i = 2$)	$x^{12379400392853802748991242 3 \cdot 2^{87}}$
	x^9	Gold ($i = 3$)	$x^{68774446626965570827729127 \cdot 2^{84}}$
	x^{17}	Gold ($i = 4$)	$x^{36410001155452361026444831 \cdot 2^{85}}$
	x^{33}	Gold ($i = 5$)	$x^{18756667261899701134835231 \cdot 2^{80}}$
	x^{65}	Gold ($i = 6$)	$x^{10474877255491679249146437 3 \cdot 2^{79}}$
	x^{129}	Gold ($i = 7$)	$x^{62376823684922261913521779 \cdot 2^{78}}$
	x^{257}	Gold ($i = 8$)	$x^{10356307721648122922307861 3 \cdot 2^{74}}$
	x^{513}	Gold ($i = 9$)	$x^{12065692390695714180305 91 \cdot 2^{72}}$
	x^{1025}	Gold ($i = 10$)	$x^{10326231547209757415012232 5 \cdot 2^{71}}$
	x^{2049}	Gold ($i = 11$)	$x^{30208395297349445458739 1 \cdot 2^{78}}$
	x^{4097}	Gold ($i = 12$)	$x^{92611330739802063523696027 \cdot 2^{69}}$
	x^{8193}	Gold ($i = 13$)	$x^{92849280378477502615100211 \cdot 2^{67}}$
	x^{16385}	Gold ($i = 14$)	$x^{99843622942668906516886957 \cdot 2^{72}}$
	x^{32769}	Gold ($i = 15$)	$x^{18888889488317926637567 \cdot 2^{60}}$
	x^{65537}	Gold ($i = 16$)	$x^{92604193701215752898271667 \cdot 2^{59}}$
	x^{131073}	Gold ($i = 17$)	$x^{10012757262353008616837457 3 \cdot 2^{57}}$
	x^{262145}	Gold ($i = 18$)	$x^{10316206346948740122957141 3 \cdot 2^{55}}$
	x^{524289}	Gold ($i = 19$)	$x^{47613169248619927641743 99 \cdot 2^{58}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{61776168527124332266022707 \cdot 2^{61}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{99834026470247798650099381 \cdot 2^{64}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{14757391740531271270 3 \cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{88424309602375019279529691 \cdot 2^{45}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
89	$x^{16777217}$	Gold ($i = 24$)	$x^{341164763675742650437395 91\cdot 2^{42}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{601734433958288615013237 19\cdot 2^{42}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{341343066705811542559640 47\cdot 2^{45}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{885103043697345683109408 91\cdot 2^{37}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{890941695114920880380591 63\cdot 2^{35}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{928455030040495958746202 11\cdot 2^{33}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{103161670036525148471121 237\cdot 2^{31}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{910250028971082666633735 469\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{910161826364479236008369 73\cdot 2^{37}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{884674223196976916465119 81\cdot 2^{34}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{599100358043693876397416 71\cdot 2^{45}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{343871577260602140504191 43\cdot 2^{39}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{618965297285214535779090 43\cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{239903538829946665092723 1\cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{103149075426307376832752 981\cdot 2^{40}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{937375212943792039958739 1\cdot 2^{45}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{181693743537856501953410 71\cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{102349373326814961304689 333\cdot 2^{43}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{599003244816232971665281 15\cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{884242885204245160608961 09\cdot 2^{44}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{35184372088831\cdot 2^{45}}$
	x^{13}	Kasami ($i = 2$)	$x^{476130784340530874961201 63\cdot 2^{86}}$
	x^{57}	Kasami ($i = 3$)	$x^{108591231516261427622753 19\cdot 2^{72}}$
	x^{241}	Kasami ($i = 4$)	$x^{539351469398194725578543 63\cdot 2^{68}}$
	x^{993}	Kasami ($i = 5$)	$x^{623333353114491579039711\cdot 2^{60}}$
	x^{4033}	Kasami ($i = 6$)	$x^{322300282977845100085316 3\cdot 2^{78}}$
	x^{16257}	Kasami ($i = 7$)	$x^{498389466514290084223089 63\cdot 2^{76}}$
	x^{65281}	Kasami ($i = 8$)	$x^{102354151468924191947205 333\cdot 2^{42}}$
	x^{261633}	Kasami ($i = 9$)	$x^{552436769393633774236607 45\cdot 2^{39}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{201487444261204289301163\cdot 2^{70}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{442337111238200488063891 75\cdot 2^{68}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{928377109845111838232281 15\cdot 2^{50}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{468687607913047900739269 9\cdot 2^{45}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{898504867595192739314208 37\cdot 2^{48}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{1152956688978903039 \cdot 2^{0}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{2375967596900781585553062 9 \cdot 2^{3}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{6420841028658072277135445 \cdot 2^{5}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{1031608828823703006255076 69 \cdot 2^{1}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{4316521178708417760707906 3 \cdot 2^{2}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{6201789466157892217203589 1 \cdot 2^{61}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{9998971698798034083503019 7 \cdot 2^{75}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{8842430960239261146557410 7 \cdot 2^{67}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{9273951543473173251474081 3 \cdot 2^{73}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{3527108616352156160163093 1 \cdot 2^{77}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{5428501179289262909078179 5 \cdot 2^{2}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{2718829327726531510831095 \cdot 2^{23}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{2649288021816961679470875 7 \cdot 2^{3}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{5627003756120276150787849 3 \cdot 2^{24}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{1237940039285380283489058 83 \cdot 2^{88}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{192153584101141163 \cdot 2^{30}}$
89	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{1092300034663570871216566 53 \cdot 2^{84}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{9116612692411715415829137 3 \cdot 2^{83}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{1268133702379510344766820 3 \cdot 2^{24}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{5416838055202498370663966 7 \cdot 2^{14}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{5361693091720364499959240 3 \cdot 2^{61}}$
	$x^{472236648280092573696 1}$	Kasami ($i = 36$)	$x^{2380658462543586158023097 1 \cdot 2^{56}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{1903703536287752178879 9 \cdot 2^{60}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{1031490800379932578211894 61 \cdot 2^{78}}$
	$x^{3022314549031075378626 57}$	Kasami ($i = 39$)	$x^{5509771036569362028320482 9 \cdot 2^{37}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{3584109705786851964423951 1 \cdot 2^{37}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{1023682628017525396281330 77 \cdot 2^{84}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{2166687864624917511338508 3 \cdot 2^{80}}$
	$x^{7737125245532747108817305 7}$	Kasami ($i = 43$)	$x^{9326945501489871110211873 3 \cdot 2^{84}}$
	$x^{3094850098213274765386366 41}$	Kasami ($i = 44$)	$x^{4421214426019466584440363 9 \cdot 2^{2}}$
	$x^{17592186044419}$	Welch	$x^{3185875101102159202399412 7 \cdot 2^{48}}$
	$x^{17592190238719}$	Niho	$x^{2459566462900808362 7 \cdot 2^{68}}$
	$x^{3094850098213450687247810 55}$	Inverse	$x^{3094850098213450687247810 55 \cdot 2^{2}}$
91	x^{3}	Gold ($i = 1$)	$x^{8252933595235868499327494 83 \cdot 2^{90}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
91	x^{5}	Gold ($i = 2$)	$x^{4951760157141521099596496 91\cdot 2^{88}}$
	x^{9}	Gold ($i = 3$)	$x^{2750977865078622833109164 95\cdot 2^{88}}$
	x^{17}	Gold ($i = 4$)	$x^{4369200138654283323173379 65\cdot 2^{85}}$
	x^{33}	Gold ($i = 5$)	$x^{7502666904759880453934086 3\cdot 2^{86}}$
	x^{65}	Gold ($i = 6$)	$x^{4189950902196671699658574 61\cdot 2^{80}}$
	x^{257}	Gold ($i = 8$)	$x^{2408443656197237888908802 31\cdot 2^{78}}$
	x^{513}	Gold ($i = 9$)	$x^{4826276956278285672121343\cdot 2^{82}}$
	x^{1025}	Gold ($i = 10$)	$x^{4130492618883902966004887 89\cdot 2^{72}}$
	x^{2049}	Gold ($i = 11$)	$x^{3540423928849355007764210 83\cdot 2^{79}}$
	x^{4097}	Gold ($i = 12$)	$x^{2399132026342670095850410 11\cdot 2^{68}}$
	x^{32769}	Gold ($i = 15$)	$x^{7555555795327170648473 5\cdot 2^{76}}$
	x^{65537}	Gold ($i = 16$)	$x^{3993549950496896374859916 05\cdot 2^{60}}$
	x^{131073}	Gold ($i = 17$)	$x^{3749530380751916635271788 7\cdot 2^{63}}$
	x^{262145}	Gold ($i = 18$)	$x^{4126482538779496049181545 81\cdot 2^{56}}$
	x^{524289}	Gold ($i = 19$)	$x^{1365375216945547203475904 15\cdot 2^{61}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{3713216836113288531236356 35\cdot 2^{64}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{3536974913933484335430931 01\cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{2951478699949891256 31\cdot 2^{46}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{3993355346272694547675027 65\cdot 2^{45}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{2471035004490707048415166 59\cdot 2^{44}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{3550680001399189672009593 41\cdot 2^{45}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{7282000244654254614007374 3\cdot 2^{34}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{4126466801461005933476140 37\cdot 2^{32}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{2475880079723682056555279 07\cdot 2^{32}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{3704441784236108791489773 07\cdot 2^{36}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{4118438652100080587550993 49\cdot 2^{35}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{6041679059821561139711 99\cdot 2^{35}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{3713817756690913822744051 71\cdot 2^{40}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{2407103008409362070271717 83\cdot 2^{40}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{9596141544225577908535551\cdot 2^{46}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{3640644375427176554359299 65\cdot 2^{45}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{7267749741404975077393974 3\cdot 2^{46}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{2396012979262389532032770 31\cdot 2^{46}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{3536971540815774321107084 43\cdot 2^{46}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
91	$x^{35184372088833}$	Gold ($i = 45$)	$x^{70368744177663 \cdot 2^{46}}$
	x^{13}	Kasami ($i = 2$)	$x^{190452313736212349984480651 \cdot 2^{87}}$
	x^{57}	Kasami ($i = 3$)	$x^{434364926065045710490920 87 \cdot 2^{82}}$
	x^{241}	Kasami ($i = 4$)	$x^{359567646265463150385638829 \cdot 2^{73}}$
	x^{993}	Kasami ($i = 5$)	$x^{24933334124579663139962 55 \cdot 2^{76}}$
	x^{4033}	Kasami ($i = 6$)	$x^{12892011319113804003412651 \cdot 2^{79}}$
	x^{65281}	Kasami ($i = 8$)	$x^{21955652907961172198328227 5 \cdot 2^{58}}$
	x^{261633}	Kasami ($i = 9$)	$x^{17753871321303520073830520 7 \cdot 2^{65}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{80594977704481715720465 1 \cdot 2^{71}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{10115228156508701953078347 7 \cdot 2^{45}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{24565326907007065442862981 1 \cdot 2^{39}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{2305913377957838847 \cdot 2^{46}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{39933550606471650090227064 5 \cdot 2^{87}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{18233459556530348459535375 1 \cdot 2^{19}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{41264589270371536935028872 5 \cdot 2^{75}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{10270853248775149330663415 \cdot 2^{88}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{37138189378409814104190494 7 \cdot 2^{84}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{36459877894633506255435220 5 \cdot 2^{74}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{17684859812275681145883384 7 \cdot 2^{24}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{40050785987053866292548114 1 \cdot 2^{78}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{18970401169634060303053117 1 \cdot 2^{17}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{50725349103002529037243435 \cdot 2^{31}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{14564000679201462924807951 1 \cdot 2^{30}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{768614336404564651 \cdot 2^{31}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{49517601571415211081864314 9 \cdot 2^{90}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{22508000826078090293375298 9 \cdot 2^{26}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{41425230886592601212568648 5 \cdot 2^{76}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{22112549045208048146774202 5 \cdot 2^{15}}$
	$x^{472236648280092573 6961}$	Kasami ($i = 36$)	$x^{18747651903773656817820293 9 \cdot 2^{63}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{21650376848283496641715246 7 \cdot 2^{63}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{75853002588711131545471 \cdot 2^{84}}$
	$x^{12089258196135299663078401}$	Kasami ($i = 40$)	$x^{36413556833184857639178577 3 \cdot 2^{74}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{21570170928953377629630786 9 \cdot 2^{35}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{86667514576304795780089083 \cdot 2^{89}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
91	$x^{309485009821327476538736641}$	Kasami ($i = 44$)	$x^{37307782005863600651978333 \cdot 2^{90}}$
	$x^{123794003928534509052703539 3}$	Kasami ($i = 45$)	$x^{35369715408157743211070844 5 \cdot 2^{90}}$
	$x^{35184372088835}$	Welch	$x^{14108875447737828704040116 7 \cdot 2^{51}}$
	$x^{295147940363724914687}$	Niho	$x^{98382658516032334507 \cdot 2^{69}}$
	$x^{123794003928538027489912422 3}$	Inverse	$x^{12379400392853802748991242 23 \cdot 2^2}$
93	x^3	Gold ($i = 1$)	$x^{33011734380943473997309979 31 \cdot 2^{92}}$
	x^5	Gold ($i = 2$)	$x^{19807040628566084398385987 59 \cdot 2^{91}}$
	x^{17}	Gold ($i = 4$)	$x^{17476800554617133292693518 53 \cdot 2^{86}}$
	x^{33}	Gold ($i = 5$)	$x^{15005333809519760907868172 43 \cdot 2^{87}}$
	x^{129}	Gold ($i = 7$)	$x^{99802917895875619061634827 5 \cdot 2^{80}}$
	x^{257}	Gold ($i = 8$)	$x^{14257986444687648302340108 43 \cdot 2^{79}}$
	x^{1025}	Gold ($i = 10$)	$x^{55073234918452039546731821 5 \cdot 2^{74}}$
	x^{2049}	Gold ($i = 11$)	$x^{15998366149476266314948174 61 \cdot 2^{78}}$
	x^{8193}	Gold ($i = 13$)	$x^{14855884860556400418415972 35 \cdot 2^{69}}$
	x^{16385}	Gold ($i = 14$)	$x^{29072891493256901420883919 9 \cdot 2^{75}}$
	x^{65537}	Gold ($i = 16$)	$x^{14148749668528026017523864 13 \cdot 2^{62}}$
	x^{131073}	Gold ($i = 17$)	$x^{16473755343382173984650472 53 \cdot 2^{61}}$
	x^{524289}	Gold ($i = 19$)	$x^{99035392037129449494748856 3 \cdot 2^{58}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{76171698725694665567232127 \cdot 2^{67}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{95840641037974136637527205 1 \cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{11805914799799397253 11 \cdot 2^{70}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{54586334300129501150155764 7 \cdot 2^{47}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{14562578239936106018830697 41 \cdot 2^{42}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{96525539485151367903319 03 \cdot 2^{38}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{14998119707170153909216467 1 \cdot 2^{41}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{96284225280954358899805024 7 \cdot 2^{35}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{14816670255777146276421697 79 \cdot 2^{36}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{24166713357685826969968 63 \cdot 2^{47}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{16505835708148614086815470 93 \cdot 2^{39}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{29127778695456898108142772 7 \cdot 2^{39}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{16503852068164138798737462 61 \cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{96277505742182194080482736 7 \cdot 2^{47}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{16375899732284719982448094 29 \cdot 2^{44}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{15973419861748295030836238 53 \cdot 2^{46}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
93	$x^{70368744177665}$	Gold ($i = 46$)	$x^{140737488355327 \cdot 2^{47}}$
	x^{13}	Kasami ($i = 2$)	$x^{761809254944849399937922619 \cdot 2^{85}}$
	x^{241}	Kasami ($i = 4$)	$x^{1438270585061852601542585773 \cdot 2^{70}}$
	x^{993}	Kasami ($i = 5$)	$x^{708106689138062433174927065 \cdot 2^{79}}$
	x^{16257}	Kasami ($i = 7$)	$x^{755998567387910153730625191 \cdot 2^{65}}$
	x^{65281}	Kasami ($i = 8$)	$x^{707405144306947286230742729 \cdot 2^{49}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{1031549536923063161053344199 \cdot 2^{47}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{1599762237675530093303911093 \cdot 2^{45}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{714194724007159657313175995 \cdot 2^{47}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{1027175297073550286391702073 \cdot 2^{49}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{1414788626867306341991111533 \cdot 2^{91}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{1637666275351256642507614805 \cdot 2^{1}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{7558576541962068924219036 75 \cdot 2^{83}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{1057011503665768487934661049 \cdot 2^{70}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{8338820343731244792012837 51 \cdot 2^{71}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{1061091483326612430804783689 \cdot 2^{73}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{1032154260071819015904007623 \cdot 2^{11}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{1417724489435190304774385069 \cdot 2^{87}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{1061780930381222882159455689 \cdot 2^{86}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{1066532956922789162027537081 \cdot 2^{91}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{1100391146031449135152540331 \cdot 2^{91}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{7142889895291863137667189 39 \cdot 2^{83}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{1061177793012031133571575369 \cdot 2^{73}}$
	$x^{1888946593134114190 1313}$	Kasami ($i = 37$)	$x^{1650593015529812749462492501 \cdot 2^{58}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{1027175610992934614030134871 \cdot 2^{67}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{1650385280603389624956138837 \cdot 2^{41}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{8254276848707348209050874 31 \cdot 2^{76}}$
	$x^{7737125245532747108817 3057}$	Kasami ($i = 43$)	$x^{1637892204827486445565733589 \cdot 2^{44}}$
	$x^{3094850098213274765387 36641}$	Kasami ($i = 44$)	$x^{1602177837031735412724766133 \cdot 2^{90}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{1414788616326209201665437111 \cdot 2^{47}}$
	$x^{70368744177667}$	Welch	$x^{4369200138654345413241771 67 \cdot 2^{49}}$
	$x^{70368752566271}$	Niho	$x^{3935305402391426935 47 \cdot 2^{47}}$
	$x^{4951760157141521099596496895}$	Inverse	$x^{4951760157141521099596496895 \cdot 2^{2}}$
95	x^{3}	Gold ($i = 1$)	$x^{1320469375237738959892399 1723 \cdot 2^{94}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
95	x^{5}	Gold ($i = 2$)	$x^{792281625142643375935435035 \cdot 2^{92}}$
	x^{9}	Gold ($i = 3$)	$x^{4401564584125796532974663911 \cdot 2^{90}}$
	x^{17}	Gold ($i = 4$)	$x^{2330240073948951105692469135 \cdot 2^{88}}$
	x^{65}	Gold ($i = 6$)	$x^{6094474039558795199503381111 \cdot 2^{84}}$
	x^{129}	Gold ($i = 7$)	$x^{5834632123143497729757112685 \cdot 2^{82}}$
	x^{257}	Gold ($i = 8$)	$x^{1541403939966232248901634555 \cdot 2^{80}}$
	x^{513}	Gold ($i = 9$)	$x^{6409295797937563372577142189 \cdot 2^{83}}$
	x^{2049}	Gold ($i = 11$)	$x^{2184671147904311895576004495 \cdot 2^{81}}$
	x^{4097}	Gold ($i = 12$)	$x^{9669045949995647741464575 \cdot 2^{72}}$
	x^{8193}	Gold ($i = 13$)	$x^{1165262246181966639817170703 \cdot 2^{70}}$
	x^{16385}	Gold ($i = 14$)	$x^{3851402590333325901327907271 \cdot 2^{73}}$
	x^{65537}	Gold ($i = 16$)	$x^{6044536865760130735145 95 \cdot 2^{64}}$
	x^{131073}	Gold ($i = 17$)	$x^{2183605602090284952329511879 \cdot 2^{62}}$
	x^{262145}	Gold ($i = 18$)	$x^{5702027992429259094045715611 \cdot 2^{61}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{6599126223783104442068020053 \cdot 2^{65}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{6550364652460954621205375701 \cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{5659155814552001233755682523 \cdot 2^{71}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{23611831006973510285 35 \cdot 2^{48}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{6589426580066725925144079061 \cdot 2^{45}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{6601540974839607009592653141 \cdot 2^{42}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{6399195417814582453961643701 \cdot 2^{46}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{3834242300701891326290368743 \cdot 2^{40}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{3961408127557891287262901043 \cdot 2^{34}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{6602346877725923472986953045 \cdot 2^{33}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{6408160203427434452816309549 \cdot 2^{35}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{3046867926149522335403934 87 \cdot 2^{41}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{5661915026155090456295398253 \cdot 2^{47}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{6002130661811280048154319 9 \cdot 2^{43}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{5927106282352383502711155867 \cdot 2^{43}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{3960924496357591651916870451 \cdot 2^{42}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{5941144575447351608262629811 \cdot 2^{46}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{3953655859322952718222157427 \cdot 2^{46}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{5926516093587269801044924851 \cdot 2^{46}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{5659154465304917228083665773 \cdot 2^{47}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
95	$x^{140737488355329}$	Gold ($i = 47$)	$x^{2814749767106 55 \cdot 2^{48}}$
	x^{13}	Kasami ($i = 2$)	$x^{3047237019779397599751690555 \cdot 2^{84}}$
	x^{57}	Kasami ($i = 3$)	$x^{3474919408520365683927366243 \cdot 2^{91}}$
	x^{241}	Kasami ($i = 4$)	$x^{1643737811499260116048977 75 \cdot 2^{72}}$
	x^{4033}	Kasami ($i = 6$)	$x^{3526272048428080485505934553 \cdot 2^{63}}$
	x^{16257}	Kasami ($i = 7$)	$x^{8309283206423122076458906 03 \cdot 2^{85}}$
	x^{65281}	Kasami ($i = 8$)	$x^{6068240568792192143848 95 \cdot 2^{48}}$
	x^{261633}	Kasami ($i = 9$)	$x^{4135030975191506919386478 93 \cdot 2^{82}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{2257420089008165261136810703 \cdot 2^{38}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{2830958693380935552231613879 \cdot 2^{73}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{3451207314176079920243567773 \cdot 2^{55}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{3464054982779341928611616979 \cdot 2^{48}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{18447025548686196735 \cdot 2^{0}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{3431140914879174114943486355 \cdot 2^{92}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{5934133484793629778881637579 \cdot 2^{84}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{6447607448737769065895253 \cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{6551568855914095176827874005 \cdot 2^{67}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{1627976200834009644785855221 \cdot 2^{70}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{5659155814552001233755682525 \cdot 2^{22}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{6589502137352869593860123477 \cdot 2^{10}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{6602749826867742294024041813 \cdot 2^{84}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{6399346459790506526113422005 \cdot 2^{1}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{7707113779661481449113203 15 \cdot 2^{22}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{7922816251426433760213388493 \cdot 2^{1}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{3074457345618258603 \cdot 2^{32}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{6990720221846853381754561965 \cdot 2^{88}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{2763773111534701515238651031 \cdot 2^{29}}$
	$x^{472236648280092573 6961}$	Kasami ($i = 36$)	$x^{5816641023244931833802677069 \cdot 2^{18}}$
	$x^{188894659313411419 01313}$	Kasami ($i = 37$)	$x^{1994697166151196233387 2095 \cdot 2^{64}}$
	$x^{302231454903107537862657}$	Kasami ($i = 39$)	$x^{1560827933646351952160586357 \cdot 2^{3}}$
	$x^{483570327845631767556 9153}$	Kasami ($i = 41$)	$x^{3035334839992104064995698531 \cdot 2^{92}}$
	$x^{193428131138296687487877 13}$	Kasami ($i = 42$)	$x^{5942112661728810590370843955 \cdot 2^{35}}$
	$x^{773712524553274710881730 57}$	Kasami ($i = 43$)	$x^{1525851814713849688561214075 \cdot 2^{82}}$
	$x^{309485009821327476538736641}$	Kasami ($i = 44$)	$x^{3001103109837504184691387549 \cdot 2^{43}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
95	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{5969245120938001684422121837 \cdot 2^{47}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{28295772326523178765534775 59 \cdot 2^2}$
	$x^{140737488355331}$	Welch	$x^{233024007395213011719414241 5 \cdot 2^{42}}$
	$x^{2361183382172310962175}$	Niho	$x^{157412216095655399697 1 \cdot 2^{48}}$
	$x^{19807040628566084398385987583}$	Inverse	$x^{19807040628566084398385987583 \cdot 2^2}$
	$x^{75558007841377277706239}$	Dobbertin	$x^{66023531726893482475684713 81 \cdot 2^1}$
97	x^3	Gold ($i = 1$)	$x^{52818775009509558395695966891 \cdot 2^{96}}$
	x^5	Gold ($i = 2$)	$x^{31691265005705735037417580135 \cdot 2^{95}}$
	x^9	Gold ($i = 3$)	$x^{17606258336503186131898655631 \cdot 2^{94}}$
	x^{17}	Gold ($i = 4$)	$x^{93209602957958044227698765 11 \cdot 2^{93}}$
	x^{33}	Gold ($i = 5$)	$x^{24008534095231617452589075867 \cdot 2^{89}}$
	x^{65}	Gold ($i = 6$)	$x^{24377896158235180798013523 19 \cdot 2^{91}}$
	x^{129}	Gold ($i = 7$)	$x^{12283436048723153115278132 47 \cdot 2^{84}}$
	x^{257}	Gold ($i = 8$)	$x^{61656157598649289956065331 1 \cdot 2^{89}}$
	x^{513}	Gold ($i = 9$)	$x^{23783892840539391792213973427 \cdot 2^{83}}$
	x^{1025}	Gold ($i = 10$)	$x^{22724955882140210002440899437 \cdot 2^{78}}$
	x^{2049}	Gold ($i = 11$)	$x^{15853365852048988976746227507 \cdot 2^{78}}$
	x^{4097}	Gold ($i = 12$)	$x^{38676183799982590965850111 \cdot 2^{85}}$
	x^{8193}	Gold ($i = 13$)	$x^{26206312756457507003357026997 \cdot 2^{73}}$
	x^{16385}	Gold ($i = 14$)	$x^{26410999307470968076651640149 \cdot 2^{71}}$
	x^{32769}	Gold ($i = 15$)	$x^{26203876387121880156209507029 \cdot 2^{76}}$
	x^{65537}	Gold ($i = 16$)	$x^{24178147463040522939269 11 \cdot 2^{81}}$
	x^{131073}	Gold ($i = 17$)	$x^{15335107024229904288054890099 \cdot 2^{64}}$
	x^{262145}	Gold ($i = 18$)	$x^{23300142901351140942748019053 \cdot 2^{66}}$
	x^{524289}	Gold ($i = 19$)	$x^{15845662725940711919159030579 \cdot 2^{60}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{15405478143267834209550365127 \cdot 2^{63}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{22807961426484712570160375003 \cdot 2^{70}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{46513787609240336641492334 23 \cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{15334485504627120783142132967 \cdot 2^{72}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{94447324027893705605 11 \cdot 2^{73}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{22636620559713434816549935981 \cdot 2^{48}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{23706064523082759673691426203 \cdot 2^{49}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{23996811357157789635403438 39 \cdot 2^{44}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{23768206998631069480151259955 \cdot 2^{45}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
97	$x^{536870913}$	Gold ($i = 29$)	$x^{154440568316006081003783167 \cdot 2^{49}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{158149239128740576511996903027 \cdot 2^{40}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{233024007416597162421301527 49 \cdot 2^{36}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{264093875109036938898003285 33 \cdot 2^{34}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{237684487552016384821781594 11 \cdot 2^{35}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{465165348095986013527818140 7 \cdot 2^{39}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{154044056250378139172061247 75 \cdot 2^{41}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{226393797716458497422105740 43 \cdot 2^{38}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{255599627512449700018074834349 \cdot 2^{48}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{256326397023018847378062492 61 \cdot 2^{44}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{264093371328936670759504663 89 \cdot 2^{40}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{255967816667186667737482083 09 \cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{873838249844540359004805723 1 \cdot 2^{49}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{880205443634820182672624480 7 \cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{263964859964521258479891689 81 \cdot 2^{45}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{263577057288181806505030888 53 \cdot 2^{46}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{873381319055109414714732037 51 \cdot 2^{46}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{255574717787961098300793053 97 \cdot 2^{47}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{226366178612187038552716551 31 \cdot 2^{49}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{562949953421311 \cdot 2^{49}}$
	x^{13}	Kasami ($i = 2$)	$x^{121889480791175903990067615 95 \cdot 2^{91}}$
	x^{57}	Kasami ($i = 3$)	$x^{138996776340814627357094650 43 \cdot 2^{85}}$
	x^{241}	Kasami ($i = 4$)	$x^{657495124599704046419451887 \cdot 2^{85}}$
	x^{993}	Kasami ($i = 5$)	$x^{686165355108432329611814360 5 \cdot 2^{68}}$
	x^{4033}	Kasami ($i = 6$)	$x^{116691119597007231665175072 23 \cdot 2^{80}}$
	x^{16257}	Kasami ($i = 7$)	$x^{141038507914302142459075069 05 \cdot 2^{66}}$
	x^{65281}	Kasami ($i = 8$)	$x^{242729622751686823405132 7 \cdot 2^{73}}$
	x^{261633}	Kasami ($i = 9$)	$x^{119984033173956709747967213 09 \cdot 2^{53}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{233337255896129407349216607 81 \cdot 2^{55}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{158378953794529090201465126 91 \cdot 2^{45}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{141471956859428523475749904 09 \cdot 2^{40}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{412697838829602686535988565 \cdot 2^{20}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{264061636041925106595315520 85 \cdot 2^{43}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{262014396460167194885376846 93 \cdot 2^{46}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
97	$x^{4294901761}$	Kasami ($i = 16$)	$x^{3689405109737245900 7 \cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{127787163905939679536009411 55 \cdot 2^{18}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{33237510591761207883696271 79 \cdot 2^{22}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{12141334932572525574294481211 \cdot 2^{88}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{13896962871416692937348299347 \cdot 2^{90}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{14105013637864029136990320221 \cdot 2^{93}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{91753202565185309445942534 63 \cdot 2^{94}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{16340340116998851995190795443 \cdot 2^{72}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{11318310279856717408266579383 \cdot 2^{26}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{23876997044374613854516566861 \cdot 2^{17}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{23766529588201190645565934803 \cdot 2^{80}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{79787886628033729994489823 \cdot 2^{92}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{60946600054455143132346037 17 \cdot 2^{16}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{11285182246478494648362673335 \cdot 2^{31}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{61417180243615766258258335 95 \cdot 2^{91}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{27962880887387413272351951693 \cdot 2^{96}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{12297829382473034411 \cdot 2^{33}}$
	$x^{7378697628248271873}$	Kasami ($i = 33$)	$x^{31691265005705735051161475483 \cdot 2^{94}}$
	$x^{29514790516217295 6673}$	Kasami ($i = 34$)	$x^{14405120475026722300605131933 \cdot 2^{28}}$
	$x^{11805916206830515650 57}$	Kasami ($i = 35$)	$x^{30828078983074313571 8228475 \cdot 2^{25}}$
	$x^{47223664828009257369 61}$	Kasami ($i = 36$)	$x^{23741382032092884966732306125 \cdot 2^{79}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{16537095868109154837391440 21 \cdot 2^{70}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{23002056078047262897477105069 \cdot 2^{69}}$
	$x^{30223145490310753786 2657}$	Kasami ($i = 39$)	$x^{26409412690757392852834932053 \cdot 2^{60}}$
	$x^{12089258196135296630 78401}$	Kasami ($i = 40$)	$x^{25558105489835649839529679541 \cdot 2^{64}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{13725173105071253085401599643 \cdot 2^{89}}$
	$x^{19342813113829668748787713}$	Kasami ($i = 42$)	$x^{13901162305712250827041761 19 \cdot 2^{88}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{25790429776936673463326037 \cdot 2^{76}}$
	$x^{30948500982132747653873664 1}$	Kasami ($i = 44$)	$x^{26358007961425997016310524757 \cdot 2^{37}}$
	$x^{12379400392853459052703539 3}$	Kasami ($i = 45$)	$x^{90296979259894673415073881 15 \cdot 2^{47}}$
	$x^{49517601571414507308523192 33}$	Kasami ($i = 46$)	$x^{25634845392506709940675172021 \cdot 2^{47}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{65119037682996473416084303 57 \cdot 2^{92}}$
	$x^{79228162514264056118567239681}$	Kasami ($i = 48$)	$x^{22636617861218703855271655133 \cdot 2^{96}}$
	$x^{281474976710659}$	Welch	$x^{91753202911739965309158069 91 \cdot 2^{55}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
97	$x^{281474993487871}$	Niho	$x^{15741222547815406414 51\cdot 2^{74}}$
	$x^{79228162514264337593543950335}$	Inverse	$x^{79228162514264337593543950335\cdot 2^2}$
99	x^3	Gold ($i=1$)	$x^{21127510003803823358278386756 3\cdot 2^{98}}$
	x^5	Gold ($i=2$)	$x^{12676506002282294014967032053 9\cdot 2^{96}}$
	x^{17}	Gold ($i=4$)	$x^{11185152354954965307323851812 5\cdot 2^{93}}$
	x^{33}	Gold ($i=5$)	$x^{19206827276185293962071260703\cdot 2^{90}}$
	x^{129}	Gold ($i=7$)	$x^{49133744194892612461112527 35\cdot 2^{92}}$
	x^{257}	Gold ($i=8$)	$x^{91251113246000949134976689883\cdot 2^{90}}$
	x^{1025}	Gold ($i=10$)	$x^{61836614645279482999839231 9\cdot 2^{80}}$
	x^{8193}	Gold ($i=13$)	$x^{61347914437994990564316224743\cdot 2^{76}}$
	x^{16385}	Gold ($i=14$)	$x^{10564399722988387230660655240 5\cdot 2^{72}}$
	x^{65537}	Gold ($i=16$)	$x^{90551997878579366512150633325\cdot 2^{81}}$
	x^{131073}	Gold ($i=17$)	$x^{90547853063840743490367108827\cdot 2^{67}}$
	x^{524289}	Gold ($i=19$)	$x^{34953605553806008408982654735\cdot 2^{65}}$
	$x^{1048577}$	Gold ($i=20$)	$x^{10563765076274134131006539912 5\cdot 2^{61}}$
	$x^{8388609}$	Gold ($i=23$)	$x^{94824276535586852859332581811\cdot 2^{71}}$
	$x^{33554433}$	Gold ($i=25$)	$x^{18889465368528660987903\cdot 2^{50}}$
	$x^{67108865}$	Gold ($i=26$)	$x^{10222989198988060334747306155 7\cdot 2^{48}}$
	$x^{268435457}$	Gold ($i=28$)	$x^{63374793122313082749632017203\cdot 2^{44}}$
	$x^{536870913}$	Gold ($i=29$)	$x^{94833700519871938496820563355\cdot 2^{50}}$
	$x^{2147483649}$	Gold ($i=31$)	$x^{48755792339174046609988608 63\cdot 2^{38}}$
	$x^{4294967297}$	Gold ($i=32$)	$x^{61621904179810789692117119431\cdot 2^{38}}$
	$x^{17179869185}$	Gold ($i=34$)	$x^{35212516675056010495163920839\cdot 2^{35}}$
	$x^{34359738369}$	Gold ($i=35$)	$x^{10238716386472965738325733035 7\cdot 2^{36}}$
	$x^{137438953473}$	Gold ($i=37$)	$x^{77352367600527994496487423\cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i=38$)	$x^{10481546777070854412641956117 3\cdot 2^{47}}$
	$x^{1099511627777}$	Gold ($i=40$)	$x^{95073734570855047473384862515\cdot 2^{42}}$
	$x^{2199023255553}$	Gold ($i=41$)	$x^{90897408017516487216075589997\cdot 2^{42}}$
	$x^{8796093022209}$	Gold ($i=43$)	$x^{10252942530232566871495001220 5\cdot 2^{45}}$
	$x^{70368744177665}$	Gold ($i=46$)	$x^{34935252762195865849074796431\cdot 2^{50}}$
	$x^{140737488355329}$	Gold ($i=47$)	$x^{61337932269110198704486862451\cdot 2^{48}}$
	$x^{562949953421313}$	Gold ($i=49$)	$x^{1125899906842623\cdot 2^{50}}$
	x^{13}	Kasami ($i=2$)	$x^{48755792316470361596027046363\cdot 2^{94}}$
	x^{241}	Kasami ($i=4$)	$x^{92049317443958566498723261869\cdot 2^{85}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
99	x^{993}	Kasami ($i=5$)	$x^{65744215419691655767452381881\cdot 2^{82}}$
	x^{16257}	Kasami ($i=7$)	$x^{67643900824136618428885407161\cdot 2^{74}}$
	x^{65281}	Kasami ($i=8$)	$x^{45273929235644626301520557769\cdot 2^{76}}$
	$x^{1047553}$	Kasami ($i=10$)	$x^{67876683702592355206965849545\cdot 2^{53}}$
	$x^{67100673}$	Kasami ($i=13$)	$x^{52749992429950245262038641095\cdot 2^{44}}$
	$x^{268419073}$	Kasami ($i=14$)	$x^{10562465441677004263785776469 3\cdot 2^{58}}$
	$x^{4294901761}$	Kasami ($i=16$)	$x^{90546471529202788329473104749\cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i=17$)	$x^{45273235743518918409108427337\cdot 2^{1}}$
	$x^{274877382657}$	Kasami ($i=19$)	$x^{65748228287508895941077470551\cdot 2^{95}}$
	$x^{1099510579201}$	Kasami ($i=20$)	$x^{10563734853157466830380134126 9\cdot 2^{1}}$
	$x^{70368735789057}$	Kasami ($i=23$)	$x^{45637878183258922329548540379\cdot 2^{73}}$
	$x^{1125899873288193}$	Kasami ($i=25$)	$x^{67909854932902773359003341385\cdot 2^{77}}$
	$x^{4503599560261633}$	Kasami ($i=26$)	$x^{10253952796778120866546075768 5\cdot 2^{12}}$
	$x^{72057593769492481}$	Kasami ($i=28$)	$x^{48374899312929929711384688187\cdot 2^{95}}$
	$x^{288230375614840833}$	Kasami ($i=29$)	$x^{45328489774186517997632515803\cdot 2^{28}}$
	$x^{461168601627990 4257}$	Kasami ($i=31$)	$x^{68258109243058506268268991929\cdot 2^{95}}$
	$x^{1844674069414584321}$	Kasami ($i=32$)	$x^{70425033346012744529503496875\cdot 2^{1}}$
	$x^{29514790516217 2956673}$	Kasami ($i=34$)	$x^{70425033346012744558136612183\cdot 2^{95}}$
	$x^{1180591620683051565057}$	Kasami ($i=35$)	$x^{10726274309623479578190851806 9\cdot 2^{90}}$
	$x^{1888946593134114190 1313}$	Kasami ($i=37$)	$x^{67915378752769570439169797705\cdot 2^{77}}$
	$x^{7555786372563944551 2193}$	Kasami ($i=38$)	$x^{10481550554848752076227278715 7\cdot 2^{85}}$
	$x^{1208925819613529663078401}$	Kasami ($i=40$)	$x^{45708556749735119213052145979\cdot 2^{65}}$
	$x^{4835703278456317675569153}$	Kasami ($i=41$)	$x^{90549256291685991329723805037\cdot 2^{66}}$
	$x^{7737125245532747 1088173057}$	Kasami ($i=43$)	$x^{92046754119920194131391194549\cdot 2^{40}}$
	$x^{4951760157141450730852319233}$	Kasami ($i=46$)	$x^{66057853902775932534397310407\cdot 2^{92}}$
	$x^{1980704062856594366089763225 7}$	Kasami ($i=47$)	$x^{53368450056916575262650633927\cdot 2^{94}}$
	$x^{3169126500570567874242223800 33}$	Kasami ($i=49$)	$x^{90546471444874011206867447223\cdot 2^{50}}$
	$x^{562949953421315}$	Welch	$x^{37283841183184012443954924363\cdot 2^{48}}$
	$x^{18889466494428534276095}$	Niho	$x^{62964890191261625658 03\cdot 2^{75}}$
	$x^{3169126500570573503741758013 43}$	Inverse	$x^{31691265005705735037417580134 3\cdot 2^{2}}$
101	x^{3}	Gold ($i=1$)	$x^{84510040015215293433113547025 1\cdot 2^{100}}$
	x^{5}	Gold ($i=2$)	$x^{50706024009129176059868128215 1\cdot 2^{99}}$
	x^{9}	Gold ($i=3$)	$x^{28170013338405097811037849008 7\cdot 2^{96}}$
	x^{17}	Gold ($i=4$)	$x^{44740609419819861229295407249 3\cdot 2^{94}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
101	x^{33}	Gold ($i = 5$)	$x^{768273091047411758482850427 51 \cdot 2^{96}}$
	x^{65}	Gold ($i = 6$)	$x^{429050972384939182045038007989 \cdot 2^{91}}$
	x^{129}	Gold ($i = 7$)	$x^{373416455881183854704455207789 \cdot 2^{92}}$
	x^{257}	Gold ($i = 8$)	$x^{246624630394597159824261324007 \cdot 2^{91}}$
	x^{513}	Gold ($i = 9$)	$x^{380542285448630268675423574451 \cdot 2^{85}}$
	x^{1025}	Gold ($i = 10$)	$x^{247346458581117931999356723 1 \cdot 2^{91}}$
	x^{2049}	Gold ($i = 11$)	$x^{253653853632783823627939637043 \cdot 2^{80}}$
	x^{4097}	Gold ($i = 12$)	$x^{245671119497489417815079898739 \cdot 2^{85}}$
	x^{8193}	Gold ($i = 13$)	$x^{362362712771208746284056992621 \cdot 2^{76}}$
	x^{16385}	Gold ($i = 14$)	$x^{246489765781332857684986051015 \cdot 2^{76}}$
	x^{32769}	Gold ($i = 15$)	$x^{372840687387459946035131542829 \cdot 2^{76}}$
	x^{65537}	Gold ($i = 16$)	$x^{408939514930882188785621849781 \cdot 2^{81}}$
	x^{131073}	Gold ($i = 17$)	$x^{193426655410073684359249 91 \cdot 2^{68}}$
	x^{262145}	Gold ($i = 18$)	$x^{139741620268917481716041631631 \cdot 2^{69}}$
	x^{524289}	Gold ($i = 19$)	$x^{195023541242347223620418232 95 \cdot 2^{64}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{422550603050965365240261072213 \cdot 2^{62}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{745677179229912340336811087 51 \cdot 2^{64}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{410117710655114384392974607789 \cdot 2^{72}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{744217668151655265024152857 91 \cdot 2^{74}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{408919587458323921677627864493 \cdot 2^{74}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{755578614741145768427 51 \cdot 2^{76}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{362185896573474486143993886427 \cdot 2^{51}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{419223037905894017059691256501 \cdot 2^{49}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{383948888697516739963661824 63 \cdot 2^{51}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{422537305654419009331398358357 \cdot 2^{45}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{362538201978363184167656171227 \cdot 2^{51}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{419261871673112042558675299029 \cdot 2^{40}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{379334838705777540240231263387 \cdot 2^{41}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{380295180083226215708408099635 \cdot 2^{37}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{422550200100672125933377115477 \cdot 2^{35}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{139814404437208341989817257743 \cdot 2^{39}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{982674883912152050856412787 1 \cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{139750749098340629991446864839 \cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{309409461179865566193655807 \cdot 2^{51}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
101	$x^{549755813889}$	Gold ($i = 39$)	$x^{25303878231084148594111603672 3\cdot 2^{49}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{25352999915329450324729575505 9\cdot 2^{43}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{14084979804190740378779677127 1\cdot 2^{42}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{49324549759609366421731412 47\cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{38029131138780130352253643038 7\cdot 2^{47}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{36492737337790991046690337090 7\cdot 2^{46}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{42234377594319796717002756437 3\cdot 2^{46}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{42172329166107284075631389371 7\cdot 2^{47}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{37929702998955008954380155637 9\cdot 2^{51}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{24535172907643265928313671600 7\cdot 2^{51}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{36218588577949668819884512753 3\cdot 2^{50}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{2251799813685247\cdot 2^{51}}$
	x^{13}	Kasami ($i = 2$)	$x^{19502316926588144638410818544 3\cdot 2^{98}}$
	x^{57}	Kasami ($i = 3$)	$x^{22239484214530340377135143982 7\cdot 2^{87}}$
	x^{241}	Kasami ($i = 4$)	$x^{36819726977583426599489304721 3\cdot 2^{90}}$
	x^{993}	Kasami ($i = 5$)	$x^{18638165924805789790384558709 5\cdot 2^{92}}$
	x^{4033}	Kasami ($i = 6$)	$x^{40924400731394859428433122782 9\cdot 2^{73}}$
	x^{16257}	Kasami ($i = 7$)	$x^{37225588764775586902535905617 3\cdot 2^{71}}$
	x^{65281}	Kasami ($i = 8$)	$x^{22482588577752240331074630768 3\cdot 2^{87}}$
	x^{261633}	Kasami ($i = 9$)	$x^{97319642232379767684047397573\cdot 2^{57}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{22627779762615983719199288288 9\cdot 2^{44}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{25340632607124654430945300971 5\cdot 2^{47}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{88438340442346469117126427259\cdot 2^{49}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{37333960942572773381013365409 3\cdot 2^{54}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{44392094781342586770344577275\cdot 2^{57}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{52638134994515538587680856107\cdot 2^{72}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{40891954876539261599659346091 7\cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{29515015697916638003 1\cdot 2^{0}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{21959301795731652589935386972 3\cdot 2^{97}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{22564212108637022122166053397 7\cdot 2^{92}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{42254999858863201867797714261 3\cdot 2^{83}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{52599986189895775824538541 91\cdot 2^{85}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{41012224412694005911079804650 9\cdot 2^{94}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{22087851253355073274970757033 3\cdot 2^{95}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
101	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{263844045627979582437721864 53\cdot 2^{73}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{362185896573475612043900729051\cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{382031696020327186063789176413\cdot 2^{22}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{660314652948385191643159 4837\cdot 2^{7}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{125727326016547894833093014 3\cdot 2^{12}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{422575988919535493624204277077\cdot 2^{88}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{379862112513486018801060914893\cdot 2^{100}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{424194364278707114966181563093\cdot 2^{96}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{230481928459039644604163058845\cdot 2^{31}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{507060240091291760612425177499\cdot 2^{100}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{49191317529892137643\cdot 2^{34}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{149135364750094512245456425683\cdot 2^{33}}$
	$x^{472236648280092573696 1}$	Kasami ($i = 36$)	$x^{176881479119917150917639382199\cdot 2^{30}}$
	$x^{188894659313411419013 13}$	Kasami ($i = 37$)	$x^{222611812723006149783810385 83\cdot 2^{88}}$
	$x^{755578637256394455121 93}$	Kasami ($i = 38$)	$x^{181026632770159632086246958519\cdot 2^{27}}$
	$x^{302231454903107537862657}$	Kasami ($i = 39$)	$x^{194237565461388152910290709603\cdot 2^{24}}$
	$x^{120892581961352966307840 1}$	Kasami ($i = 40$)	$x^{975117706214618416366050143 31\cdot 2^{64}}$
	$x^{483570327845631767556915 3}$	Kasami ($i = 41$)	$x^{144556817068206003233377507795\cdot 2^{2}}$
	$x^{193428131138296687487877 13}$	Kasami ($i = 42$)	$x^{194183703999733461218751 99\cdot 2^{68}}$
	$x^{773712524553274710881730 57}$	Kasami ($i = 43$)	$x^{191975653274573481011378247995\cdot 2^{94}}$
	$x^{309485009821327476538736641}$	Kasami ($i = 44$)	$x^{108510021074311538112314313461\cdot 2^{94}}$
	$x^{123794003928534509052703 5393}$	Kasami ($i = 45$)	$x^{20632329071359838346560 5803\cdot 2^{12}}$
	$x^{495176015714145073085231 9233}$	Kasami ($i = 46$)	$x^{421728127373574636125495274325\cdot 2^{84}}$
	$x^{198070406285659436608976 32257}$	Kasami ($i = 47$)	$x^{380302856751228007327570775251\cdot 2^{44}}$
	$x^{792281625142640561185672 39681}$	Kasami ($i = 48$)	$x^{261445440728279000013650631987\cdot 2^{94}}$
	$x^{316912650057056787424222 380033}$	Kasami ($i = 49$)	$x^{52095230146365622688903058923\cdot 2^{4}}$
	$x^{126765060022822827559679 6362753}$	Kasami ($i = 50$)	$x^{181092942889747218199515721143\cdot 2^{2}}$
	$x^{1125899906842627}$	Welch	$x^{149135364732783734948344796815\cdot 2^{44}}$
	$x^{1125899940397055}$	Niho	$x^{251859545753047968426 67\cdot 2^{51}}$
	$x^{126765060022822940149670 3205375}$	Inverse	$x^{126765060022822940149670 3205375\cdot 2^{2}}$
103	x^{3}	Gold ($i = 1$)	$x^{338040160060861173732454188 1003\cdot 2^{102}}$
	x^{5}	Gold ($i = 2$)	$x^{202824096036516704239472512 8603\cdot 2^{100}}$
	x^{9}	Gold ($i = 3$)	$x^{112680053353620391244151396 0335\cdot 2^{100}}$
	x^{17}	Gold ($i = 4$)	$x^{596541458930931483057272096655\cdot 2^{96}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
103	x^{33}	Gold ($i = 5$)	$x^{153654618209482351696570085 5003 \cdot 2^{97}}$
	x^{65}	Gold ($i = 6$)	$x^{171620388953975672818015203 1925 \cdot 2^{92}}$
	x^{129}	Gold ($i = 7$)	$x^{102198187925376633919114056 8691 \cdot 2^{92}}$
	x^{257}	Gold ($i = 8$)	$x^{169677745711482845959091790 9205 \cdot 2^{89}}$
	x^{513}	Gold ($i = 9$)	$x^{164077972427201622337974839 8509 \cdot 2^{87}}$
	x^{1025}	Gold ($i = 10$)	$x^{145439717645697344015621753 1245 \cdot 2^{91}}$
	x^{2049}	Gold ($i = 11$)	$x^{559275813863503845267457148 815 \cdot 2^{85}}$
	x^{4097}	Gold ($i = 12$)	$x^{151734404284091700877223151 5547 \cdot 2^{88}}$
	x^{8193}	Gold ($i = 13$)	$x^{123778894200242099499251 3023 \cdot 2^{78}}$
	x^{16385}	Gold ($i = 14$)	$x^{297706408890950670549851323 935 \cdot 2^{80}}$
	x^{32769}	Gold ($i = 15$)	$x^{101415142773912118128833871 5443 \cdot 2^{76}}$
	x^{65537}	Gold ($i = 16$)	$x^{151722710960071889548501456 3251 \cdot 2^{82}}$
	x^{131073}	Gold ($i = 17$)	$x^{773706621640294737434378 23 \cdot 2^{86}}$
	x^{262145}	Gold ($i = 18$)	$x^{981411907980391056447992208 615 \cdot 2^{70}}$
	x^{524289}	Gold ($i = 19$)	$x^{985881961178397782366373755 111 \cdot 2^{71}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{985950601169141389411222450 631 \cdot 2^{66}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{152118096205892391262639378 9235 \cdot 2^{65}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{393070047274298371341748634 87 \cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{168937570853077748838704628 8725 \cdot 2^{70}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{558964348806336758339190514 631 \cdot 2^{73}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{144874371582165982825812216 1005 \cdot 2^{76}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{151115725200028900261887 \cdot 2^{52}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{981406955303332782043643367 027 \cdot 2^{50}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{168689318557065071214493792 1365 \cdot 2^{48}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{563331493371017865055704773 063 \cdot 2^{46}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{298268454118181908536610397 967 \cdot 2^{48}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{494692917392595204626605772 7 \cdot 2^{42}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{149120913631556278025906731 6589 \cdot 2^{44}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{164048901207742321988876298 9869 \cdot 2^{39}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{169020080040268850372491852 7317 \cdot 2^{36}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{101412048021209831171873382 0723 \cdot 2^{36}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{153654618211718320676242750 495 \cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{145970953114802418274779759 5355 \cdot 2^{44}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{163575802196361980688213490 6549 \cdot 2^{39}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
103	$x^{549755813889}$	Gold ($i = 39$)	$x^{144892030534844314605442676911 5\cdot 2^{52}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{153580745506276688007895578687\cdot 2^{52}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{169019999435452807361239641 8389\cdot 2^{43}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{149135307842112847274142945 6173\cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{197298199026930680849192719 35\cdot 2^{52}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{169014921789530956325177279 8293\cdot 2^{46}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{779997439282393126571915305 59\cdot 2^{46}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{152093301131441387252183581 3683\cdot 2^{48}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{101213589998656759795445913 3747\cdot 2^{48}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{167689213258538340451142319 1733\cdot 2^{50}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{163567819384288129596955497 0029\cdot 2^{51}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{144874354311797903233887644 6427\cdot 2^{52}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{4503599627370495\cdot 2^{52}}$
	x^{13}	Kasami ($i = 2$)	$x^{780092677063525785536432741771\cdot 2^{99}}$
	x^{57}	Kasami ($i = 3$)	$x^{889579368581213615085405758163\cdot 2^{95}}$
	x^{241}	Kasami ($i = 4$)	$x^{883673447462002238387743313563\cdot 2^{87}}$
	x^{993}	Kasami ($i = 5$)	$x^{152169135495674667329715034 0299\cdot 2^{77}}$
	x^{4033}	Kasami ($i = 6$)	$x^{163697602925579437713733316 4725\cdot 2^{68}}$
	x^{16257}	Kasami ($i = 7$)	$x^{100619815127914573395543227 2691\cdot 2^{71}}$
	x^{65281}	Kasami ($i = 8$)	$x^{167697041766685392554120325 8069\cdot 2^{73}}$
	x^{261633}	Kasami ($i = 9$)	$x^{147211099963897289529924666 7173\cdot 2^{55}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{148902141636139989081688862 5965\cdot 2^{48}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{577899542786090298600659800 783\cdot 2^{42}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{768273100208176668201758911 581\cdot 2^{37}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{905420505003958526582448830 025\cdot 2^{42}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{587219911949463764887464875 671\cdot 2^{62}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{389998724363563046155602850 107\cdot 2^{46}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{389278530781071646198034686 597\cdot 2^{58}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{5903003139583328911 35\cdot 2^{52}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{899622694632725626435834842 211\cdot 2^{20}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{886798112798351017211595168 947\cdot 2^{93}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{177568381485420854199096052 215\cdot 2^{95}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{767903746420849371518058746 171\cdot 2^{90}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{902646146068263614570009536 233\cdot 2^{99}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
103	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{8252934578581835079679126 19 \cdot 2^{35}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{8413644380403700753795803647 1 \cdot 2^{73}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{2083809371460899716300000353 07 \cdot 2^{29}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{7243717823529684400144842377 51 \cdot 2^{27}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{3549913108867550050979077008 59 \cdot 2^{13}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{1686902856958724926744936491 861 \cdot 2^{86}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{8784597961451587118822355706 43 \cdot 2^{97}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{2104241201404116131238236158 3 \cdot 2^{91}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{7222516614157440094666663622 95 \cdot 2^{32}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{1493665823524735418819516676 29 \cdot 2^{1}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{1789624376792794449236493444 525 \cdot 2^{100}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{1967652701195685505 71 \cdot 2^{35}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{2028240960365167042408469023 949 \cdot 2^{102}}$
	$x^{472236648280092573 6961}$	Kasami ($i = 36$)	$x^{9219277098293021687090744783 01 \cdot 2^{29}}$
	$x^{1888946593134114190 1313}$	Kasami ($i = 37$)	$x^{4340593494944910188144338890 13 \cdot 2^{88}}$
	$x^{7555786372563944551 2193}$	Kasami ($i = 38$)	$x^{1638232693706369811319495481 013 \cdot 2^{83}}$
	$x^{3022314549031075378 62657}$	Kasami ($i = 39$)	$x^{9030221614494295633576190756 61 \cdot 2^{15}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{2553232146558626030252326879 \cdot 2^{18}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{1690202412205014381366138983765 \cdot 2^{64}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{2103977977868992226521700987 31 \cdot 2^{81}}$
	$x^{7737125245532747 1088173057}$	Kasami ($i = 43$)	$x^{7752236702761480865447910 3 \cdot 2^{95}}$
	$x^{3094850098213274765387 36641}$	Kasami ($i = 44$)	$x^{1690149222617676037325324997973 \cdot 2^{90}}$
	$x^{1237940039285345090527035393}$	Kasami ($i = 45$)	$x^{7072188305098829761335193570 79 \cdot 2^{47}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{1521180841181214635001209736499 \cdot 2^{37}}$
	$x^{1980704062856594366089763 2257}$	Kasami ($i = 47$)	$x^{7770276316137879918404313362 91 \cdot 2^{93}}$
	$x^{7922816251426405611856723 9681}$	Kasami ($i = 48$)	$x^{2640778819816446714575323682 1 \cdot 2^{90}}$
	$x^{3169126500570567874242223800 33}$	Kasami ($i = 49$)	$x^{1055376091015887750585517837 65 \cdot 2^{94}}$
	$x^{1267650600228228275596796362753}$	Kasami ($i = 50$)	$x^{1528126750960075128334281709261 \cdot 2^{49}}$
	$x^{5070602400912915354186999136257}$	Kasami ($i = 51$)	$x^{1448743543117979032338876446429 \cdot 2^{102}}$
	$x^{2251799813685251}$	Welch	$x^{5965414589309330725630229332 93 \cdot 2^{51}}$
	$x^{151115729703628460523519}$	Niho	$x^{1007438183012191202618 03 \cdot 2^{52}}$
	$x^{5070602400912917605986812821503}$	Inverse	$x^{5070602400912917605986812821503 \cdot 2^{2}}$
105	x^{3}	Gold ($i = 1$)	$x^{1352160640243444694929816752 4011 \cdot 2^{104}}$
	x^{5}	Gold ($i = 2$)	$x^{8112963841460668169578900514 407 \cdot 2^{103}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
105	x^{17}	Gold ($i = 4$)	$x^{2386165835723725932229088386591 \cdot 2^{101}}$
	x^{257}	Gold ($i = 8$)	$x^{6787109828459313838363671636693 \cdot 2^{90}}$
	x^{2049}	Gold ($i = 11$)	$x^{6552930774825478682602772256437 \cdot 2^{84}}$
	x^{8193}	Gold ($i = 13$)	$x^{4951155768009683979970035711 \cdot 2^{92}}$
	x^{65537}	Gold ($i = 16$)	$x^{4048621121427150349971435087475 \cdot 2^{83}}$
	x^{131073}	Gold ($i = 17$)	$x^{5795062596085807583383492867803 \cdot 2^{87}}$
	x^{524289}	Gold ($i = 19$)	$x^{6747611427834899566242525784917 \cdot 2^{68}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{6069357437591606397837575089307 \cdot 2^{70}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{2253326237968844281367666156487 \cdot 2^{73}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{6044629008001154668298 23 \cdot 2^{79}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{5964831747061069303696920897901 \cdot 2^{52}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{3930699235776048712451848982131 \cdot 2^{51}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{6543350466679751731783052600749 \cdot 2^{43}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{2253601067203584671630361391559 \cdot 2^{38}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{6708797022747456939864540009141 \cdot 2^{39}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{6083734459574873313561281337779 \cdot 2^{42}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{5838875455326353366649633205403 \cdot 2^{48}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{1190823217855261100987951643679 \cdot 2^{48}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{5817434113111840746690676673389 \cdot 2^{52}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{3119989757123852236485778392 31 \cdot 2^{53}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{3943526635199530344751978920391 \cdot 2^{50}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{9007199254740991 \cdot 2^{53}}$
	x^{13}	Kasami ($i = 2$)	$x^{3120370708254103142145730967099 \cdot 2^{97}}$
	x^{241}	Kasami ($i = 4$)	$x^{4207968797438105897084491968087 \cdot 2^{92}}$
	x^{65281}	Kasami ($i = 8$)	$x^{6707881670667415702164812966613 \cdot 2^{82}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{6552626125518971261902104777397 \cdot 2^{51}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{4345965345697023423072157003337 \cdot 2^{56}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{3095945108206995223926787624615 \cdot 2^{50}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{2897487086404610150266273894985 \cdot 2^{55}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{6747572704429812092746079841109 \cdot 2^{97}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{2900404375380757654749800722139 \cdot 2^{104}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{4225536387988181434102061494727 \cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{4346230640147910391362136347209 \cdot 2^{82}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{5806380862177967379257836137901 \cdot 2^{12}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
105	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{309904585984037692363962145555 9\cdot 2^{26}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{59305315370132355730455411153 17\cdot 2^{24}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{450720213414481564979659783099 9\cdot 2^{104}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{68648155581590269170509923846 93\cdot 2^{94}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{29257277011115470090504281135579\cdot 2^{91}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{28978518350347292864311205373 05\cdot 2^{73}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{42073106402024950984965336616 25\cdot 2^{74}}$
	$x^{30948500982132747653873664 1}$	Kasami ($i = 44$)	$x^{57951511937513162090902461761 09\cdot 2^{96}}$
	$x^{49517601571414507308523192 33}$	Kasami ($i = 46$)	$x^{43295191190149516977495340200 25\cdot 2^{89}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{33809517961980165613370325365 19\cdot 2^{85}}$
	$x^{20282409603651665920347623915521}$	Kasami ($i = 52$)	$x^{57949741724719096956417523992 87\cdot 2^{53}}$
	$x^{4503599627370499}$	Welch	$x^{20878951062582603893886711928 47\cdot 2^{56}}$
	$x^{4503599694479359}$	Niho	$x^{10074381980241897368234 7\cdot 2^{80}}$
	$x^{20282409603651670423947251286015}$	Inverse	$x^{20282409603651670423947251286015\cdot 2^{2}}$
	$x^{19342822337210501698682879}$	Dobbertin	$x^{67608048131190849088557558652245\cdot 2^{1}}$
107	x^{3}	Gold ($i = 1$)	$x^{54086425609737787797192670096043\cdot 2^{106}}$
	x^{5}	Gold ($i = 2$)	$x^{32451855365842672678315602057627\cdot 2^{104}}$
	x^{9}	Gold ($i = 3$)	$x^{18028808536579262599064223365351\cdot 2^{102}}$
	x^{17}	Gold ($i = 4$)	$x^{28633990028684711186749060639085\cdot 2^{101}}$
	x^{33}	Gold ($i = 5$)	$x^{24584738913517176271451213680027\cdot 2^{99}}$
	x^{65}	Gold ($i = 6$)	$x^{24962965666032825137165847736 95\cdot 2^{96}}$
	x^{129}	Gold ($i = 7$)	$x^{16351710068060261427058249098867\cdot 2^{94}}$
	x^{257}	Gold ($i = 8$)	$x^{15783976345254218228752724736231\cdot 2^{94}}$
	x^{513}	Gold ($i = 9$)	$x^{31629488660665372980814426982 3\cdot 2^{90}}$
	x^{1025}	Gold ($i = 10$)	$x^{90231988090391821593365332551 11\cdot 2^{91}}$
	x^{2049}	Gold ($i = 11$)	$x^{23202522260107132978883531974363\cdot 2^{87}}$
	x^{4097}	Gold ($i = 12$)	$x^{27049813540237424260787840134485\cdot 2^{85}}$
	x^{8193}	Gold ($i = 13$)	$x^{23191213617357359762179647265645\cdot 2^{92}}$
	x^{16385}	Gold ($i = 14$)	$x^{26173406692682997829962812405165\cdot 2^{81}}$
	x^{32769}	Gold ($i = 15$)	$x^{16226422843825938900613419397939\cdot 2^{78}}$
	x^{65537}	Gold ($i = 16$)	$x^{24585114041138421021382877501 75\cdot 2^{81}}$
	x^{131073}	Gold ($i = 17$)	$x^{15703149592811421990968140353139\cdot 2^{86}}$
	x^{262145}	Gold ($i = 18$)	$x^{61896765846845586752222003 1\cdot 2^{72}}$
	x^{524289}	Gold ($i = 19$)	$x^{24275029414412678092321609665947\cdot 2^{73}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
107	$x^{1048577}$	Gold ($i = 20$)	$x^{1247997111921781400653530128511 \cdot 2^{74}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{2433889539294278260202299054899 \cdot 2^{67}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{901440641749057598277076519776 7 \cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{628892807800222192255042027775 \cdot 2^{77}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{2433493060006270862474253130833 9 \cdot 2^{74}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{894342501173321746840716075201 5 \cdot 2^{79}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{231798973807023671132145349895 31 \cdot 2^{80}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{120892581060743005418291 1 \cdot 2^{54}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{157025107388868296902191671 8631 \cdot 2^{54}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{161941745511959566422538063972 35 \cdot 2^{50}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{262475329151743030187959657219 01 \cdot 2^{49}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{157751902769446208126702163214 79 \cdot 2^{51}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{791508290223121258165242449 91 \cdot 2^{54}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{269905995504030881380265826 7 89 \cdot 2^{43}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{476329316450289677850821476 2527 \cdot 2^{44}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{162259276833935729874482015240 19 \cdot 2^{38}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{270432128052624244388469253952 85 \cdot 2^{37}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{477233167148217514742449589838 3 \cdot 2^{38}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{232697412507034292298411626520 13 \cdot 2^{39}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{269904455603717327143579661545 81 \cdot 2^{40}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{990231153602837405988448665 5 \cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{242756325447041291762838334898 43 \cdot 2^{52}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{894812181285082437695642950427 1 \cdot 2^{50}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{270431999096632258013634393101 65 \cdot 2^{44}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{268351869006583616457015953537 81 \cdot 2^{46}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{262111044266461632661409776493 33 \cdot 2^{52}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{270423874863238000553383120622 93 \cdot 2^{47}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{233553518961839371536621620031 63 \cdot 2^{54}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{238593269787952186989132094784 45 \cdot 2^{49}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{476299247052499850851265164878 3 \cdot 2^{50}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{268302741213660618472061029198 93 \cdot 2^{51}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{261708511014860635444966018802 45 \cdot 2^{52}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{231798966898876439295380123062 85 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{18014398509481983 \cdot 2^{54}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
107	x^{13}	Kasami ($i = 2$)	$x^{1248148283301641256858292386847 5\cdot 2^{96}}$
	x^{57}	Kasami ($i = 3$)	$x^{2846653979459883568273298428407\cdot 2^{90}}$
	x^{241}	Kasami ($i = 4$)	$x^{3366375037950484717667593574443\cdot 2^{100}}$
	x^{993}	Kasami ($i = 5$)	$x^{2434706167930794677275440463380 3\cdot 2^{79}}$
	x^{4033}	Kasami ($i = 6$)	$x^{4023289780044963138894430201 5\cdot 2^{72}}$
	x^{16257}	Kasami ($i = 7$)	$x^{1609917042046633174328691319275 5\cdot 2^{73}}$
	x^{65281}	Kasami ($i = 8$)	$x^{1419001258280325196615430030046 7\cdot 2^{73}}$
	x^{261633}	Kasami ($i = 9$)	$x^{6201789408416116177958333 43\cdot 2^{54}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{9246064888140488644425152094931\cdot 2^{62}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{6629115924649542910873674517237\cdot 2^{53}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{1320469296512415554800469060 3\cdot 2^{84}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{3334230261526021748526326240747\cdot 2^{82}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{2624767826848641036109882737989 3\cdot 2^{62}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{1243272666875682385420137989103 5\cdot 2^{57}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{1192966288463926340658866138127 1\cdot 2^{76}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{1308540558396818715541546687190 7\cdot 2^{74}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{47223844972681544335 35\cdot 2^{0}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{6388199495324597956413832903285\cdot 2^{72}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{1444109559839308531186196566191 3\cdot 2^{97}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{6240738440689739920907627679429\cdot 2^{3}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{1405535432051240470240141645256 3\cdot 2^{92}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{1131795797500066228087219641669 5\cdot 2^{1}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{2433889104104779500110398074398 7\cdot 2^{98}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{1346183063398804784199030032367\cdot 2^{86}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{2431110740189603603507038208673 3\cdot 2^{88}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{2317989738070236711321453498953 3\cdot 2^{25}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{5679842308469382854733884785915\cdot 2^{21}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{6249889070478466086918218015355\cdot 2^{14}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{2355410542391982075067085289617 3\cdot 2^{104}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{1423049013143604535820937142128 3\cdot 2^{103}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{1449168255893917022142556128647 3\cdot 2^{25}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{2714843931383725535454991991880 5\cdot 2^{100}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{1475084336642736363581965509750 1\cdot 2^{33}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{3245185536584267267832934595297 3\cdot 2^{1}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
107	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{787061080478274202283 \cdot 2^{36}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{954466334345047625631278239503 1 \cdot 2^{34}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{23898653176395766709813039552877 \cdot 2^{95}}$
	$x^{30223145490310753786 2657}$	Kasami ($i = 39$)	$x^{27069596427117546548309691509589 \cdot 2^{90}}$
	$x^{12089258196135296630784 01}$	Kasami ($i = 40$)	$x^{11585704497216438483324844453303 \cdot 2^{28}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{12287605335968779815991455837341 \cdot 2^{90}}$
	$x^{19342813113829668748787713}$	Kasami ($i = 42$)	$x^{14054615943964526410871073099419 \cdot 2^{72}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{27043219252476339633231211353429 \cdot 2^{66}}$
	$x^{30948500982132747653873 6641}$	Kasami ($i = 44$)	$x^{26191459308340361316380401556149 \cdot 2^{77}}$
	$x^{12379400392855345090527035393}$	Kasami ($i = 45$)	$x^{26171490350258971514661585509045 \cdot 2^{97}}$
	$x^{49517601571414507308523192 33}$	Kasami ($i = 46$)	$x^{27042387561881663746068263392597 \cdot 2^{47}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{14443534116288493279277355710045 \cdot 2^{43}}$
	$x^{79228162514264056118567239681}$	Kasami ($i = 48$)	$x^{23863988597345914601634886659373 \cdot 2^{86}}$
	$x^{31691265005705678742422238 0033}$	Kasami ($i = 49$)	$x^{32679562114086691901597470718 3 \cdot 2^{90}}$
	$x^{12676506002282282755967963627 53}$	Kasami ($i = 50$)	$x^{21126230556701310391670327978 7 \cdot 2^{8}}$
	$x^{50706024009129153541869991362 57}$	Kasami ($i = 51$)	$x^{84430087281047638096733781891 9 \cdot 2^{6}}$
	$x^{20282409603651665920347623915521}$	Kasami ($i = 52$)	$x^{24450028015361044118895821478733 \cdot 2^{102}}$
	$x^{81129638414606672688589750403073}$	Kasami ($i = 53$)	$x^{11589948344943812957569751412151 \cdot 2^{2}}$
	$x^{9007199254740995}$	Welch	$x^{92463926134294380867318269253 27 \cdot 2^{59}}$
	$x^{12089258286218284294471 67}$	Niho	$x^{40297527920967589472938 7 \cdot 2^{81}}$
	$x^{81129638414606681695789005144063}$	Inverse	$x^{81129638414606681695789005144063 \cdot 2^{2}}$
109	x^{3}	Gold ($i = 1$)	$x^{21634570243895115118877068038417 1 \cdot 2^{108}}$
	x^{5}	Gold ($i = 2$)	$x^{12980742146337069071326240823050 3 \cdot 2^{107}}$
	x^{9}	Gold ($i = 3$)	$x^{72115234146317050396256893461391 \cdot 2^{106}}$
	x^{17}	Gold ($i = 4$)	$x^{11453596011473884474699624255633 3 \cdot 2^{102}}$
	x^{33}	Gold ($i = 5$)	$x^{19667791130813741017160970944031 \cdot 2^{100}}$
	x^{65}	Gold ($i = 6$)	$x^{99851862664131300548663390946 55 \cdot 2^{103}}$
	x^{129}	Gold ($i = 7$)	$x^{95594612705583066804340533193069 \cdot 2^{96}}$
	x^{257}	Gold ($i = 8$)	$x^{93441139963904971914216130438363 \cdot 2^{95}}$
	x^{513}	Gold ($i = 9$)	$x^{12651795464266149192325770782 71 \cdot 2^{100}}$
	x^{1025}	Gold ($i = 10$)	$x^{10827838570847018591203839906082 1 \cdot 2^{91}}$
	x^{2049}	Gold ($i = 11$)	$x^{31675798307313492121342705868 7 \cdot 2^{88}}$
	x^{4097}	Gold ($i = 12$)	$x^{10819925416094969704315136053589 3 \cdot 2^{86}}$
	x^{8193}	Gold ($i = 13$)	$x^{62820264384506870337859813088487 \cdot 2^{94}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
109	x^{16385}	Gold ($i = 14$)	$x^{927309043777085099053241677390 99\cdot 2^{83}}$
	x^{32769}	Gold ($i = 15$)	$x^{954472159711897461849936747185 09\cdot 2^{80}}$
	x^{65537}	Gold ($i = 16$)	$x^{360581672603363508313615536583 11\cdot 2^{81}}$
	x^{131073}	Gold ($i = 17$)	$x^{357761941846472286589656488928 71\cdot 2^{86}}$
	x^{262145}	Gold ($i = 18$)	$x^{247587063387382347008835583 9\cdot 2^{91}}$
	x^{524289}	Gold ($i = 19$)	$x^{104683723873732003902290616825 261\cdot 2^{73}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{973397514286081908732423064518 91\cdot 2^{73}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{190893357882857559126223481116 31\cdot 2^{68}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{108172877009886911793249180276 053\cdot 2^{67}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{104844456392501275052752943927 989\cdot 2^{70}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{648957917844685477255374998341 63\cdot 2^{75}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{647767000217211908488753014881 15\cdot 2^{78}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{104683409397637737827778055296 693\cdot 2^{79}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{48357032424297199482961 91\cdot 2^{82}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{927195881411799963506499276542 53\cdot 2^{54}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{107321097094686416032391073458 901\cdot 2^{52}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{630964261726412556695240834562 31\cdot 2^{55}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{108169550096410927602812077135 189\cdot 2^{48}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{107340747603214520129300644584 117\cdot 2^{53}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{927648158262993267115391955956 29\cdot 2^{44}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{499198841020337739430623810367 9\cdot 2^{48}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{357924875359253355493610057275 03\cdot 2^{43}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{108172851221049697755353341842 773\cdot 2^{38}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{973555660977641363590971603812 35\cdot 2^{39}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{934220078713831575833457460788 75\cdot 2^{40}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{251557123002490897451104750822 3\cdot 2^{47}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{357738547133221931701481611938 71\cdot 2^{44}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{396092458489836030259805485 43\cdot 2^{55}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{107962398182723030175060583623 381\cdot 2^{52}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{631008288034277153696251116548 55\cdot 2^{49}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{649036797831880525726982929907 71\cdot 2^{45}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{628911877712454089168867607691 39\cdot 2^{46}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{971097093299876817837064405846 03\cdot 2^{55}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{973545757152736748316991680479 23\cdot 2^{49}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
109	$x^{281474976710657}$	Gold ($i = 48$)	$x^{1049901315095630718011559802075 33 \cdot 2^{54}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{98290915128596178076093750303 03 \cdot 2^{50}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{1905196988209943449484680522908 7 \cdot 2^{55}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{9710003967732460504828319398955 5 \cdot 2^{53}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{6281004264356653763038533345649 9 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{9271958675955051395450001671548 3 \cdot 2^{55}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{36028797018963967 \cdot 2^{55}}$
	x^{13}	Kasami ($i = 2$)	$x^{4992593133206565027433169547327 5 \cdot 2^{103}}$
	x^{57}	Kasami ($i = 3$)	$x^{1138661591783953427309319370443 9 \cdot 2^{100}}$
	x^{241}	Kasami ($i = 4$)	$x^{1346550015180193887067037429777 1 \cdot 2^{101}}$
	x^{993}	Kasami ($i = 5$)	$x^{4771370476750282186338447029621 5 \cdot 2^{96}}$
	x^{4033}	Kasami ($i = 6$)	$x^{1609315912017985255557431295 35 \cdot 2^{91}}$
	x^{16257}	Kasami ($i = 7$)	$x^{9529750723782550247049190252881 3 \cdot 2^{75}}$
	x^{65281}	Kasami ($i = 8$)	$x^{9722482609720301347137705382062 1 \cdot 2^{84}}$
	x^{261633}	Kasami ($i = 9$)	$x^{2480715763366446333475945983 \cdot 2^{82}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{1079614730587082764665689668759 89 \cdot 2^{61}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{4638240787537073149720833511570 3 \cdot 2^{78}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{5281877186049662219201876241 1 \cdot 2^{85}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{1258772113592830975441971311525 9 \cdot 2^{45}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{2651646366552344676838901585790 9 \cdot 2^{51}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{9425817246554486221076649234673 3 \cdot 2^{47}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{3700654517477404638132366280955 5 \cdot 2^{18}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{5621581244714662795256770833857 9 \cdot 2^{55}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{94447689945363091292 15 \cdot 2^{55}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{9421506396656837241835339950198 9 \cdot 2^{1}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{4914545756547637481575507275996 5 \cdot 2^{108}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{5654458071087177654037309752489 1 \cdot 2^{100}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{1081727996386529032054537551435 09 \cdot 2^{1}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{1047677035056073542861072993051 41 \cdot 2^{82}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{6491163354840923902299218661867 5 \cdot 2^{75}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{2499955613227173131171257233019 \cdot 2^{80}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{3377203637639733995486903107243 \cdot 2^{32}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{4635979407058999817532489671826 3 \cdot 2^{29}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{9557738230810791677482971880506 9 \cdot 2^{86}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
109	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{845049222304657664710704884395 \cdot 2^{30}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{5692192186144105228565921761187 5 \cdot 2^{21}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{10817450178100905251167657858389 3 \cdot 2^{96}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{10480607013234204518496272759880 5 \cdot 2^{27}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{13297345651062974392742133126635 \cdot 2^{34}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{45281658659384549625670058488983 \cdot 2^{36}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{38178653376024195134836844974803 \cdot 2^{37}}$
	$x^{472236648280092573696 1}$	Kasami ($i = 36$)	$x^{3148244321913096809131 \cdot 2^{37}}$
	$x^{1888946593134114190 1313}$	Kasami ($i = 37$)	$x^{12980742146337069071348231055605 9 \cdot 2^{106}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{59003373429075338797380766611037 \cdot 2^{29}}$
	$x^{3022314549031075378626 57}$	Kasami ($i = 39$)	$x^{58085032969351489145850948036329 \cdot 2^{27}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{28508224518261202379097526947 75 \cdot 2^{19}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{57951864080336695740557559708233 \cdot 2^{17}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{10732858257283100779428695491669 3 \cdot 2^{18}}$
	$x^{7737125245532747108817305 7}$	Kasami ($i = 43$)	$x^{56755163885155210188267816131027 \cdot 2^{75}}$
	$x^{3094850098213274765387366 41}$	Kasami ($i = 44$)	$x^{49730908186048375539422201262395 \cdot 2^{75}}$
	$x^{1237940039285345090527035393}$	Kasami ($i = 45$)	$x^{52259918450489010108357271194723 \cdot 2^{84}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{25572604869584159712380425419381 \cdot 2^{83}}$
	$x^{1980704062856594366089763225 7}$	Kasami ($i = 47$)	$x^{24963727457851162545082964856517 \cdot 2^{80}}$
	$x^{7922816251426405611856723968 1}$	Kasami ($i = 48$)	$x^{10499129691434829429112505609143 7 \cdot 2^{41}}$
	$x^{3169126500570567874242223800 33}$	Kasami ($i = 49$)	$x^{57774136739842762141984772809949 \cdot 2^{42}}$
	$x^{1267650600228228275596796362753}$	Kasami ($i = 50$)	$x^{13071824842689142086563919462 23 \cdot 2^{105}}$
	$x^{5070602400912915354186999136257}$	Kasami ($i = 51$)	$x^{97357531328286701435404073880787 \cdot 2^{46}}$
	$x^{2028240960365166592034762391552 1}$	Kasami ($i = 52$)	$x^{66930032826432722442733630377267 \cdot 2^{100}}$
	$x^{8112963841460667268858975040307 3}$	Kasami ($i = 53$)	$x^{97800112061443686878779959719517 \cdot 2^{108}}$
	$x^{3245185536584267087687575110942 73}$	Kasami ($i = 54$)	$x^{92719586759550513954500016715485 \cdot 2^{108}}$
	$x^{18014398509481987}$	Welch	$x^{28633990028684712776254811475727 \cdot 2^{57}}$
	$x^{18014398643699711}$	Niho	$x^{16119010928195056557533877 \cdot 2^{55}}$
	$x^{3245185536584267267831560205762 55}$	Inverse	$x^{32451855365842672678315602057625 5 \cdot 2^{2}}$
111	x^{3}	Gold ($i = 1$)	$x^{86538280975580460475508272153668 3 \cdot 2^{110}}$
	x^{5}	Gold ($i = 2$)	$x^{51922968585348276285304963292201 1 \cdot 2^{108}}$
	x^{17}	Gold ($i = 4$)	$x^{15271461348631845966266165674177 5 \cdot 2^{104}}$
	x^{33}	Gold ($i = 5$)	$x^{78671164523254964068643883776063 \cdot 2^{106}}$
	x^{129}	Gold ($i = 7$)	$x^{20125181622228014064071691198591 \cdot 2^{98}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
111	x^{257}	Gold ($i = 8$)	$x^{10101744860962699666401743831295 \cdot 2^{96}}$
	x^{1025}	Gold ($i = 10$)	$x^{433113542833880743648153596242773 \cdot 2^{92}}$
	x^{2049}	Gold ($i = 11$)	$x^{126703193229253968485370823065 5 \cdot 2^{100}}$
	x^{8193}	Gold ($i = 13$)	$x^{42936422820179979474300149677125 3 \cdot 2^{93}}$
	x^{16385}	Gold ($i = 14$)	$x^{15844665421223154191426599321 5 \cdot 2^{84}}$
	x^{65537}	Gold ($i = 16$)	$x^{43269800712403620997633864386696 5 \cdot 2^{81}}$
	x^{131073}	Gold ($i = 17$)	$x^{43184961207355766170321275726510 9 \cdot 2^{87}}$
	x^{524289}	Gold ($i = 19$)	$x^{37088117661003764579202085570852 5 \cdot 2^{74}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{25910803075799169532070703126302 7 \cdot 2^{72}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{43269150803954764717299671900706 1 \cdot 2^{68}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{38178654281829535291728118187140 5 \cdot 2^{70}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{25238571432889857709285589478445 5 \cdot 2^{78}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{38840016114618793449369160743669 9 \cdot 2^{82}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{96714065208882366471208 95 \cdot 2^{56}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{41873361887169984603021886034474 9 \cdot 2^{55}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{37368563064121120308101221210025 1 \cdot 2^{51}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{25961286228312527695334496000081 9 \cdot 2^{50}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{38841012075304442334643422629726 7 \cdot 2^{45}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{41937782318993267664073969338437 3 \cdot 2^{42}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{25240331951224085323364932389728 7 \cdot 2^{41}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{41996053569198456166989447906244 5 \cdot 2^{46}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{25125039106773985053746213216625 9 \cdot 2^{42}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{38174953887789467731385255430794 9 \cdot 2^{55}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{38942224891586895977104288168017 9 \cdot 2^{48}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{37123911882349193623446390748898 7 \cdot 2^{48}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{76356724178696704929818629512975 \cdot 2^{52}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{14421285988483404305627265898183 1 \cdot 2^{53}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{39316366051436200307376154343487 \cdot 2^{56}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{14309479531395223301846365804231 1 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{25124017057426589018442739034442 3 \cdot 2^{56}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{72057594037927935 \cdot 2^{56}}$
	x^{13}	Kasami ($i = 2$)	$x^{19970372532826260109732678189308 3 \cdot 2^{106}}$
	x^{241}	Kasami ($i = 4$)	$x^{26931000303603877741340748595567 1 \cdot 2^{95}}$
	x^{993}	Kasami ($i = 5$)	$x^{26928830635905702202348495565279 3 \cdot 2^{88}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
111	x^{16257}	Kasami ($i = 7$)	$x^{27706941777566358908471461940984 9\cdot 2^{80}}$
	x^{65281}	Kasami ($i = 8$)	$x^{27706937863553058384500825605268 1\cdot 2^{82}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{43184589223483310586682508539784 5\cdot 2^{52}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{27802289637014970678758636122477 7\cdot 2^{58}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{42936300960457362543100316806622 9\cdot 2^{41}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{27814178212446189810133089461511 3\cdot 2^{58}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{43267820008340764396231007579886 9\cdot 2^{49}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{42930438801012138110684958226286 9\cdot 2^{61}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{37087834708137797794709396565898 9\cdot 2^{109}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{19814048678329715586397106368260 3\cdot 2^{109}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{43269135329707962998860977571976 5\cdot 2^{91}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{37164781382101097676409317629482 9\cdot 2^{93}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{21638091495667363638620211828781 5\cdot 2^{77}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{18693274888872763817798801570581 7\cdot 2^{91}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{27815876096946623802557866000852 1\cdot 2^{86}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{42000130808199406597707267195435 7\cdot 2^{21}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{18546251744222036849741291872021 7\cdot 2^{107}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{19814358758576099208133951163346 7\cdot 2^{103}}$
	$x^{29514790516217295667 3}$	Kasami ($i = 34$)	$x^{18724657287113900804645570034428 3\cdot 2^{110}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{43934819572217772241438956918085 3\cdot 2^{108}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{28846093658526820158514974180420 3\cdot 2^{109}}$
	$x^{12089258196135296630784 01}$	Kasami ($i = 40$)	$x^{37955386394683712013023517688773 3\cdot 2^{28}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{19833889756223106687980077498746 3\cdot 2^{19}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{37097455231600760733831830512785 3\cdot 2^{19}}$
	$x^{30948500982132747653873 6641}$	Kasami ($i = 44$)	$x^{18722224844688040660680160176499 79\cdot 2^{73}}$
	$x^{49517601571414507308523 19233}$	Kasami ($i = 46$)	$x^{18543952859788193986558168856749 7\cdot 2^{77}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{26926791853246547097591733005064 7\cdot 2^{106}}$
	$x^{31691265005705678742422238 0033}$	Kasami ($i = 49$)	$x^{27043432883124332355212572337402 3\cdot 2^{92}}$
	$x^{12676506002282282755967963627 53}$	Kasami ($i = 50$)	$x^{26960490477240431259693695130463 3\cdot 2^{91}}$
	$x^{20282409603651665920347623915521}$	Kasami ($i = 52$)	$x^{27057296958573819004506861294944 7\cdot 2^{101}}$
	$x^{81129638414606672688589750403073}$	Kasami ($i = 53$)	$x^{21859717143311465530070815654983 1\cdot 2^{103}}$
	$x^{12980742146337068711038270633410 57}$	Kasami ($i = 55$)	$x^{37087834703820200434829003977055 1\cdot 2^{56}}$
	$x^{36028797018963971}$	Welch	$x^{15271461348631927348960608510433 5\cdot 2^{50}}$
	$x^{96714065929458304166133 75}$	Niho	$x^{64476043712780223545780 91\cdot 2^{56}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
111	$x^{129807421463370690713262408230 5023}$	Inverse	$x^{129807421463370690713262408230 5023\cdot 2^2}$
113	x^3	Gold ($i=1$)	$x^{3461531239023218419020330886146731\cdot 2^{112}}$
	x^5	Gold ($i=2$)	$x^{2076918743413931051412198531688039\cdot 2^{111}}$
	x^9	Gold ($i=3$)	$x^{1153843746341072806340110295382247\cdot 2^{108}}$
	x^{17}	Gold ($i=4$)	$x^{6108584539452738386506466269670 71\cdot 2^{109}}$
	x^{33}	Gold ($i=5$)	$x^{1573423290465099281372877675521243\cdot 2^{107}}$
	x^{65}	Gold ($i=6$)	$x^{1757392782888710889656475680659125\cdot 2^{103}}$
	x^{129}	Gold ($i=7$)	$x^{8050072648891205625628676479411 1\cdot 2^{106}}$
	x^{257}	Gold ($i=8$)	$x^{4040697944385079866560697532467 1\cdot 2^{105}}$
	x^{513}	Gold ($i=9$)	$x^{1680158437654544612740862359942573\cdot 2^{101}}$
	x^{1025}	Gold ($i=10$)	$x^{5774847237785076581975381283235 27\cdot 2^{94}}$
	x^{2049}	Gold ($i=11$)	$x^{1484961424646856510648546046326491\cdot 2^{101}}$
	x^{4097}	Gold ($i=12$)	$x^{1553760299869099016982765071912347\cdot 2^{93}}$
	x^{8193}	Gold ($i=13$)	$x^{3054665062631254628282313231644 31\cdot 2^{92}}$
	x^{16385}	Gold ($i=14$)	$x^{6337866168489261676570639400 95\cdot 2^{99}}$
	x^{32769}	Gold ($i=15$)	$x^{1717297242906419537917346248485589\cdot 2^{84}}$
	x^{65537}	Gold ($i=16$)	$x^{1730792028496144839905354575435093\cdot 2^{82}}$
	x^{131073}	Gold ($i=17$)	$x^{1572667027410928695098614545101 43\cdot 2^{91}}$
	x^{262145}	Gold ($i=18$)	$x^{1004965793771920441802743988067559\cdot 2^{93}}$
	x^{524289}	Gold ($i=19$)	$x^{1980700284970627889782377676 7\cdot 2^{76}}$
	$x^{1048577}$	Gold ($i=20$)	$x^{1717140039140240836920926488320693\cdot 2^{75}}$
	$x^{2097153}$	Gold ($i=21$)	$x^{1494742560046102122998030332028123\cdot 2^{78}}$
	$x^{4194305}$	Gold ($i=22$)	$x^{5769220107193968628973289579770 31\cdot 2^{70}}$
	$x^{8388609}$	Gold ($i=23$)	$x^{1038459495500954696850627007558451\cdot 2^{70}}$
	$x^{16777217}$	Gold ($i=24$)	$x^{1489263442443981501009538439661933\cdot 2^{73}}$
	$x^{33554433}$	Gold ($i=25$)	$x^{1730554395998701092728309998595413\cdot 2^{77}}$
	$x^{67108865}$	Gold ($i=26$)	$x^{1727378641405011800916571414964949\cdot 2^{80}}$
	$x^{134217729}$	Gold ($i=27$)	$x^{1004960722230612768812622088359539\cdot 2^{82}}$
	$x^{268435457}$	Gold ($i=28$)	$x^{3868562608355294605161267 1\cdot 2^{85}}$
	$x^{536870913}$	Gold ($i=29$)	$x^{1483513393679325916095933326407387\cdot 2^{57}}$
	$x^{1073741825}$	Gold ($i=30$)	$x^{1553600637274082357616327460182451\cdot 2^{55}}$
	$x^{2147483649}$	Gold ($i=31$)	$x^{1557435403888301994759250015787443\cdot 2^{55}}$
	$x^{4294967297}$	Gold ($i=32$)	$x^{1557673212048841706973760566440755\cdot 2^{51}}$
	$x^{8589934593}$	Gold ($i=33$)	$x^{3048507437720905421667834124201 27\cdot 2^{57}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
113	$x^{17179869185}$	Gold ($i = 34$)	$x^{25340638647325812998702597427 19\cdot 2^{46}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{10095431270424781728778836911782 15\cdot 2^{49}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{15734232904879956037140742461750 3\cdot 2^{42}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{15576890575642261817454514868846 59\cdot 2^{41}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{17307656195179056981540374496761 17\cdot 2^{39}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{15271461348637401691540291655549 89\cdot 2^{40}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{10062590811114373106957040901668 99\cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{17299213435996534787656446474105 17\cdot 2^{43}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{14836039235725659293276595658658 37\cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{16750162144718575044054683732435 73\cdot 2^{55}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{79881487750655659473414421737535\cdot 2^{51}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{17307654131883185199368469147374 93\cdot 2^{47}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{16798606755295029155907761485366 21\cdot 2^{48}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{10121417066305166157985991098879\cdot 2^{48}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{10096121776488978683201620141818 31\cdot 2^{54}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{57267863541810067532703868838671\cdot 2^{53}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{10383325911708041875555355722934067\cdot 2^{53}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{15269969266428756851603634438413 89\cdot 2^{56}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{10364271615862085434130395601895 55\cdot 2^{55}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{57237918125580784269920460995163 1\cdot 2^{57}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{16749344704951058353686805861922221\cdot 2^{56}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{14835133881528080585685928180755309\cdot 2^{56}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{144115188075855871\cdot 2^{57}}$
	x^{13}	Kasami ($i = 2$)	$x^{79881490131305040438930712757232 3\cdot 2^{110}}$
	x^{57}	Kasami ($i = 3$)	$x^{91092927342716274184745549635440 3\cdot 2^{109}}$
	x^{241}	Kasami ($i = 4$)	$x^{90488161020109029210904915281884 3\cdot 2^{92}}$
	x^{993}	Kasami ($i = 5$)	$x^{44968532712386221153436322690123 7\cdot 2^{106}}$
	x^{4033}	Kasami ($i = 6$)	$x^{16762634539579334421886204365605 65\cdot 2^{91}}$
	x^{16257}	Kasami ($i = 7$)	$x^{92430996546717052081978574930914 5\cdot 2^{74}}$
	x^{65281}	Kasami ($i = 8$)	$x^{74463141173699937590267469300651 9\cdot 2^{98}}$
	x^{261633}	Kasami ($i = 9$)	$x^{15074416636303082447853269280823 41\cdot 2^{87}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{89945362356929055660094248641576 3\cdot 2^{57}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{92437778074974895908566702363194 9\cdot 2^{48}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{78671165461317290387467383461794 9\cdot 2^{42}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
113	$x^{67100673}$	Kasami ($i = 13$)	$x^{6013137907446228635808370402648 47\cdot 2^{45}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{7418019617851023730431125058472 23\cdot 2^{86}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{1352201582521325614984751953783 5\cdot 2^{91}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{1730712800333630575849236008195 413\cdot 2^{66}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{7647667235179335137219299196745 19\cdot 2^{81}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{9212136393039108973545570467544 03\cdot 2^{79}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{7555800784110239875071 9\cdot 2^{0}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{1676253316539625167370223751088 789\cdot 2^{1}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1555597178718490128810676376413 389\cdot 2^{112}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{9109290833925140609440828018328 7\cdot 2^{95}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{3994075934957832080396064708160 59\cdot 2^{93}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{2127525828836679203235261945825 71\cdot 2^{4}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{4225502126721282122551880144 21\cdot 2^{76}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{1727398371074387913916502433377 109\cdot 2^{106}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{1070880526394070734793101125733 171\cdot 2^{82}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{1483513393679325988153527364335 323\cdot 2^{85}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{4267641931913568373387518115786 45\cdot 2^{21}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{1557681196642135921444587253320 915\cdot 2^{94}}$
	$x^{461168601627990425 7}$	Kasami ($i = 31$)	$x^{3986262160106226771448864859347 89\cdot 2^{94}}$
	$x^{1844674406941458432 1}$	Kasami ($i = 32$)	$x^{7863335137054643475498570241702 99\cdot 2^{106}}$
	$x^{7378697628624827187 3}$	Kasami ($i = 33$)	$x^{1077439182806433911671573081291 1\cdot 2^{29}}$
	$x^{2951479051621729566 73}$	Kasami ($i = 34$)	$x^{9274675291051229717420751735826 65\cdot 2^{26}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{2020348984234758214266538210777 55\cdot 2^{33}}$
	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{9440539748652054207580922657763 49\cdot 2^{34}}$
	$x^{1888946593134114190 1313}$	Kasami ($i = 37$)	$x^{2076918743413931051412418434013 595\cdot 2^{112}}$
	$x^{7555786372563944551 2193}$	Kasami ($i = 38$)	$x^{1259297728765238723652 3\cdot 2^{38}}$
	$x^{3022314549030107537862657}$	Kasami ($i = 39$)	$x^{1832575361835821515952974715374 413\cdot 2^{108}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{4025036324445602812857977770978 51\cdot 2^{104}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{1732454171335522975717415852878 677\cdot 2^{94}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{1524797540166795487780531583998 797\cdot 2^{21}}$
	$x^{7737125245532747108817 3057}$	Kasami ($i = 43$)	$x^{5403278235991823501956777279556 3\cdot 2^{33}}$
	$x^{3094850098213274765387366 41}$	Kasami ($i = 44$)	$x^{1287455185235519805580879855551\cdot 2^{76}}$
	$x^{1237940039285345090527035393}$	Kasami ($i = 45$)	$x^{1730766032158264375650689526093141\cdot 2^{70}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{1077239915831441704321576732386 13\cdot 2^{26}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
113	$x^{198070406285659436608976322 57}$	Kasami ($i = 47$)	$x^{198457261809347189182467927 03 \cdot 2^{76}}$
	$x^{792281625142640561185672396 81}$	Kasami ($i = 48$)	$x^{908082467421304382862586966612435 \cdot 2^{105}}$
	$x^{316912650057056787424222380033}$	Kasami ($i = 49$)	$x^{430790857004538820976569766727 59 \cdot 2^{46}}$
	$x^{126765060022822827559679636275 3}$	Kasami ($i = 50$)	$x^{103858613677454321268165043363512 3 \cdot 2^{90}}$
	$x^{507060240091291535418699913625 7}$	Kasami ($i = 51$)	$x^{150939844841595832813655282281918 1 \cdot 2^{93}}$
	$x^{202824096036516659203476239155 21}$	Kasami ($i = 52$)	$x^{795676294772371620168692582378595 \cdot 2^{1}}$
	$x^{811296384146066726885897500403 073}$	Kasami ($i = 53$)	$x^{591770283277576560591893076038355 \cdot 2^{51}}$
	$x^{324518553658426708768757511094 273}$	Kasami ($i = 54$)	$x^{168000522764325063282674096869906 1 \cdot 2^{51}}$
	$x^{129807421463370687110382706334 1057}$	Kasami ($i = 55$)	$x^{156480179298309887950636247540362 9 \cdot 2^{56}}$
	$x^{519229685853482755647290229129 2161}$	Kasami ($i = 56$)	$x^{741756694076403957226870052449719 \cdot 2^{2}}$
	$x^{72057594037927939}$	Welch	$x^{601313790602378935319106711129871 \cdot 2^{63}}$
	$x^{72057594306363391}$	Niho	$x^{644760439529722027774225 1 \cdot 2^{86}}$
	$x^{519229685853482762853049632922 0095}$	Inverse	$x^{519229685853482762853049632922 0095 \cdot 2^{2}}$
115	x^{3}	Gold ($i = 1$)	$x^{138461249560928736760813235445869 23 \cdot 2^{114}}$
	x^{5}	Gold ($i = 2$)	$x^{830767497365572420564879412675215 5 \cdot 2^{112}}$
	x^{9}	Gold ($i = 3$)	$x^{461537498536429122536044118152897 5 \cdot 2^{112}}$
	x^{17}	Gold ($i = 4$)	$x^{733030144734328606380775952360484 5 \cdot 2^{109}}$
	x^{65}	Gold ($i = 6$)	$x^{702957113155484355862590272263646 9 \cdot 2^{104}}$
	x^{129}	Gold ($i = 7$)	$x^{611805521315731627547779412435236 5 \cdot 2^{106}}$
	x^{257}	Gold ($i = 8$)	$x^{598023295768991820250983234805116 3 \cdot 2^{106}}$
	x^{513}	Gold ($i = 9$)	$x^{623480480479035832197813984171461 1 \cdot 2^{101}}$
	x^{2049}	Gold ($i = 11$)	$x^{671020111342129017098523878954360 5 \cdot 2^{100}}$
	x^{4097}	Gold ($i = 12$)	$x^{402507562184686662148226906068133 1 \cdot 2^{92}}$
	x^{8193}	Gold ($i = 13$)	$x^{623100972941711525005637006089297 9 \cdot 2^{93}}$
	x^{16385}	Gold ($i = 14$)	$x^{593477788017334463394074673504021 9 \cdot 2^{100}}$
	x^{65537}	Gold ($i = 16$)	$x^{230772270466152645320713943390253 5 \cdot 2^{84}}$
	x^{131073}	Gold ($i = 17$)	$x^{671944765384260375257953132489450 9 \cdot 2^{87}}$
	x^{262145}	Gold ($i = 18$)	$x^{228952670648594402043562582420878 3 \cdot 2^{94}}$
	x^{524289}	Gold ($i = 19$)	$x^{792280113988251155912940584 95 \cdot 2^{96}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{691968537922959252344591565892283 7 \cdot 2^{75}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{621502201609380495138567688332 4059 \cdot 2^{75}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{121940305245503521105339000556649 5 \cdot 2^{77}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{610798801620769692177982946131486 1 \cdot 2^{79}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{686855025305016757550543179070533 3 \cdot 2^{83}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
115	$x^{268435457}$	Gold ($i = 28$)	$x^{59340536410355197664415867799376 45\cdot 2^{85}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{77371252311221079642210303\cdot 2^{58}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{12193260821446956365153389425538 71\cdot 2^{54}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{31948695596577150197633799316691 1\cdot 2^{52}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{69230096600773840237128865354110 29\cdot 2^{51}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{40204944450305558408786360896790 79\cdot 2^{58}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{16100145298016699200795098426585 5\cdot 2^{44}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{12217169078994368377396401578350 23\cdot 2^{42}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{69230624780716227926160123597509 97\cdot 2^{40}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{41538374868354178891970434712993 79\cdot 2^{40}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{80813958887738347264937058828543\cdot 2^{42}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{41457284824611921535589931982784 51\cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{12675732336979964417069159710 71\cdot 2^{44}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{22896762730760983061236500682433 99\cdot 2^{55}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{62936901607936799409402256297065 5\cdot 2^{48}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{40485668265073234513341728687103\cdot 2^{58}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{41538057953210786119203587195174 91\cdot 2^{52}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{69222172744720248422030134137767 25\cdot 2^{53}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{40381712744442823057002712923650 31\cdot 2^{58}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{69095144105747228526351230187383 89\cdot 2^{55}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{62144025393487702203415709901654 03\cdot 2^{58}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{59340535526112317401664964629439 63\cdot 2^{58}}$
	$x^{144115188075855873}$	Gold ($i = 57$)	$x^{288230376151711743\cdot 2^{58}}$
	x^{13}	Kasami ($i = 2$)	$x^{31952596052522016175572285102892 91\cdot 2^{111}}$
	x^{57}	Kasami ($i = 3$)	$x^{36437170937086509673898219854176 83\cdot 2^{103}}$
	x^{241}	Kasami ($i = 4$)	$x^{60325440680072686140603276854020 29\cdot 2^{97}}$
	x^{4033}	Kasami ($i = 6$)	$x^{67050538158317337687544817462381 33\cdot 2^{98}}$
	x^{16257}	Kasami ($i = 7$)	$x^{87129149474583316544449738488733 9\cdot 2^{95}}$
	x^{65281}	Kasami ($i = 8$)	$x^{36975459377087830577829033547669 25\cdot 2^{76}}$
	x^{261633}	Kasami ($i = 9$)	$x^{15944850183353101137343309027335 09\cdot 2^{91}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{21644803717843311523172113219652 3\cdot 2^{83}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{14489737698074045500106346320861 39\cdot 2^{56}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{62307562611940720297826056528719 87\cdot 2^{41}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{62236410528386770536765375946155 01\cdot 2^{66}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
115	$x^{4294901761}$	Kasami ($i = 16$)	$x^{364371014461216974345989881602551 \cdot 2^{55}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{430895347282276234761786295496789 \cdot 2^{69}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{359781199654123050992983352585769 1 \cdot 2^{57}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{151116015682204798025727 \cdot 2^{58}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{690953426607647380131200539942 3317 \cdot 2^{1}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{623023333972267866815402971643 4123 \cdot 2^{102}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{418299166364760188504139036262 23 \cdot 2^{111}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{610918108092055874970351858648 1965 \cdot 2^{79}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{686981782627907014806231803214 9173 \cdot 2^{90}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{625920718041143659871179405566647 7 \cdot 2^{85}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{296702678183213379966784733835615 1 \cdot 2^{30}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{361885439876035700629163211505167 7 \cdot 2^{96}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{514982074092363251370899118483 1 \cdot 2^{109}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{692316811398457935990288898345096 5 \cdot 2^{100}}$
	$x^{29514790516217295 6673}$	Kasami ($i = 34$)	$x^{363517848356608955617108872669521 9 \cdot 2^{27}}$
	$x^{472236648280092573 6961}$	Kasami ($i = 36$)	$x^{289802615390072260063460363794143 1 \cdot 2^{37}}$
	$x^{188894659313411419 01313}$	Kasami ($i = 37$)	$x^{244343381592332192161607229312783 1 \cdot 2^{38}}$
	$x^{755578637256394455 12193}$	Kasami ($i = 38$)	$x^{503719091506095489460 91 \cdot 2^{39}}$
	$x^{302231454903107537862657}$	Kasami ($i = 39$)	$x^{830767497365572420564901402907770 9 \cdot 2^{114}}$
	$x^{483570327845631767556 9153}$	Kasami ($i = 41$)	$x^{371744210943638439128515120209687 3 \cdot 2^{28}}$
	$x^{193428131138296687487 87713}$	Kasami ($i = 42$)	$x^{318278421391885968835471302544061 1 \cdot 2^{105}}$
	$x^{773712524553274710881 73057}$	Kasami ($i = 43$)	$x^{370891929147073223026241099934778 5 \cdot 2^{18}}$
	$x^{309485009821327476538 736641}$	Kasami ($i = 44$)	$x^{236700252448004562694476114391112 3 \cdot 2^{100}}$
	$x^{198070406285659436608 97632257}$	Kasami ($i = 47$)	$x^{305367678597350856036329118320040 7 \cdot 2^{90}}$
	$x^{792281625142640561185 67239681}$	Kasami ($i = 48$)	$x^{793055336190016063583876541 43 \cdot 2^{106}}$
	$x^{316912650057056787424222380033}$	Kasami ($i = 49$)	$x^{159759323615384914506872963463 1995 \cdot 2^{101}}$
	$x^{507060240091291535418699913 6257}$	Kasami ($i = 51$)	$x^{169020085067006610467223170798 9 \cdot 2^{90}}$
	$x^{202824096036516659203476239155 21}$	Kasami ($i = 52$)	$x^{727325649256900375483789908314363 \cdot 2^{42}}$
	$x^{811296384146066726885897504030 73}$	Kasami ($i = 53$)	$x^{690959363873782740827947560741563 7 \cdot 2^{108}}$
	$x^{324518553658426708768757511094273}$	Kasami ($i = 54$)	$x^{314688469449639627247855435110313 3 \cdot 2^{48}}$
	$x^{519229685853482755647290229 1292161}$	Kasami ($i = 56$)	$x^{170705650143610973505047262435202 1 \cdot 2^{110}}$
	$x^{207691874341393103700067972410245 13}$	Kasami ($i = 57$)	$x^{593405355261123174016649646294396 5 \cdot 2^{114}}$
	$x^{144115188075855875}$	Welch	$x^{244343381578109555805932261495892 3 \cdot 2^{56}}$
	$x^{773712525994514552570511 35}$	Niho	$x^{257904175811888811109690 03 \cdot 2^{87}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
115	$x^{207691874341393105141219853168803 83}$	Inverse	$x^{207691874341393105141219853168803 83\cdot 2^{2}}$
	$x^{49517607474374018270547148 79}$	Dobbertin	$x^{69230628906931657911574806935197 01\cdot 2^{1}}$
117	x^{3}	Gold ($i=1$)	$x^{553844998243714947043252941783476 91\cdot 2^{116}}$
	x^{5}	Gold ($i=2$)	$x^{332306998946228968225951765070086 15\cdot 2^{115}}$
	x^{17}	Gold ($i=4$)	$x^{293212057893731442552310380944193 73\cdot 2^{110}}$
	x^{33}	Gold ($i=5$)	$x^{251747726474415885019660428083398 67\cdot 2^{109}}$
	x^{129}	Gold ($i=7$)	$x^{167441511096937077013076470771748 99\cdot 2^{106}}$
	x^{257}	Gold ($i=8$)	$x^{161627917775403194662427901298680 07\cdot 2^{107}}$
	x^{1025}	Gold ($i=10$)	$x^{238288433390710528435194680318554 69\cdot 2^{98}}$
	x^{2049}	Gold ($i=11$)	$x^{916317493433964700086201792408974 3\cdot 2^{103}}$
	x^{16385}	Gold ($i=14$)	$x^{268015684533073897778819198986950 85\cdot 2^{100}}$
	x^{65537}	Gold ($i=16$)	$x^{251751567781257431258960665516342 3\cdot 2^{86}}$
	x^{131073}	Gold ($i=17$)	$x^{249230883030136173898912730045284 35\cdot 2^{87}}$
	x^{524289}	Gold ($i=19$)	$x^{237363953030424093306893347485684 29\cdot 2^{96}}$
	$x^{1048577}$	Gold ($i=20$)	$x^{237362594836374728576646715275814 03\cdot 2^{79}}$
	$x^{4194305}$	Gold ($i=22$)	$x^{644005965454210451606320697032831\cdot 2^{74}}$
	$x^{8388609}$	Gold ($i=23$)	$x^{166153519280152751496100321083523 07\cdot 2^{72}}$
	$x^{33554433}$	Gold ($i=25$)	$x^{323255845184580727004958736449791\cdot 2^{76}}$
	$x^{268435457}$	Gold ($i=28$)	$x^{160793709966201136027843933841400 07\cdot 2^{87}}$
	$x^{536870913}$	Gold ($i=29$)	$x^{309485009244884317495099391\cdot 2^{88}}$
	$x^{2147483649}$	Gold ($i=31$)	$x^{915806693908316176083865673674848 7\cdot 2^{56}}$
	$x^{4294967297}$	Gold ($i=32$)	$x^{276787217098871908678452254633275 73\cdot 2^{55}}$
	$x^{17179869185}$	Gold ($i=34$)	$x^{244343288371351114267831533186204 61\cdot 2^{54}}$
	$x^{34359738369}$	Gold ($i=35$)	$x^{405450170011980379213445705277 43\cdot 2^{59}}$
	$x^{137438953473}$	Gold ($i=37$)	$x^{274792326051735836256829912139250 45\cdot 2^{45}}$
	$x^{274877906945}$	Gold ($i=38$)	$x^{161538124487834146069533162112577 99\cdot 2^{44}}$
	$x^{1099511627777}$	Gold ($i=40$)	$x^{923074997073697776891271170519495 1\cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i=41$)	$x^{251626693913612693677432901756115 1\cdot 2^{47}}$
	$x^{8796093022209}$	Gold ($i=43$)	$x^{248576301155240689008027279151794 19\cdot 2^{47}}$
	$x^{17592186044417}$	Gold ($i=44$)	$x^{507029292534754101387287596236 7\cdot 2^{59}}$
	$x^{70368744177665}$	Gold ($i=46$)	$x^{488686748592225553396372313257140 7\cdot 2^{51}}$
	$x^{140737488355329}$	Gold ($i=47$)	$x^{276922466110125060231088231775819 09\cdot 2^{48}}$
	$x^{562949953421313}$	Gold ($i=49$)	$x^{237593036047028939103003552278873 23\cdot 2^{59}}$
	$x^{1125899906842625}$	Gold ($i=50$)	$x^{276920386354738328169559751012406 61\cdot 2^{52}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
117	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{249189664573747674567009464450810 11 \cdot 2^{57}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{274742007002787741255625678969473 81 \cdot 2^{57}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{267989515279216921760763729062683 41 \cdot 2^{57}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{576460752303423487 \cdot 2^{59}}$
	x^{13}	Kasami ($i = 2$)	$x^{127810384210088064702289140411571 79 \cdot 2^{109}}$
	x^{241}	Kasami ($i = 4$)	$x^{241301762720290744562413107416385 73 \cdot 2^{94}}$
	x^{993}	Kasami ($i = 5$)	$x^{118800588747141272628613168782025 85 \cdot 2^{91}}$
	x^{16257}	Kasami ($i = 7$)	$x^{126835512607575244377316276881035 91 \cdot 2^{77}}$
	x^{65281}	Kasami ($i = 8$)	$x^{138280964237286651887348228404474 31 \cdot 2^{82}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{237363048453405752854428656669438 53 \cdot 2^{58}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{172355060236936130226908256463475 91 \cdot 2^{55}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{242863865732241537846253007849770 77 \cdot 2^{48}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{172344311912541537081845906760872 25 \cdot 2^{50}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{119821991416601067446899486268828 75 \cdot 2^{55}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{237362142107903343376987370442494 53 \cdot 2^{58}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{118681071053088150775365725939676 89 \cdot 2^{1}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{177324377471978854420853237416298 81 \cdot 2^{113}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{126811865494172233180405442409065 55 \cdot 2^{103}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{177327571404789035942870076592245 21 \cdot 2^{86}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{139902189764039260661673900441379 27 \cdot 2^{86}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{178021606633602127897961182677284 57 \cdot 2^{91}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{173166706676215239218429678010587 59 \cdot 2^{14}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{276787415169183700937836626346427 73 \cdot 2^{12}}$
	$x^{29514790516217295667 3}$	Kasami ($i = 34$)	$x^{237854699877439056725317598037559 49 \cdot 2^{103}}$
	$x^{11805916206830515650 57}$	Kasami ($i = 35$)	$x^{178036090477659893887313774476422 729 \cdot 2^{109}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{281182845262193742345079412748028 69 \cdot 2^{112}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{184614999414571649014418868940745 39 \cdot 2^{1}}$
	$x^{12089258196135296630784 01}$	Kasami ($i = 40$)	$x^{184614999414571649014437194134541 67 \cdot 2^{113}}$
	$x^{48357032784563176755691 53}$	Kasami ($i = 41$)	$x^{178934537894123290583291404261342 01 \cdot 2^{109}}$
	$x^{77371252455327471088173057}$	Kasami ($i = 43$)	$x^{118825910093799327492477466392859 79 \cdot 2^{23}}$
	$x^{30948500982132747653873 6641}$	Kasami ($i = 44$)	$x^{178023417452502351277503110957922 01 \cdot 2^{91}}$
	$x^{49517601571414507308523 19233}$	Kasami ($i = 46$)	$x^{172331470955602914960384591646347 11 \cdot 2^{83}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{276922515627726631645947384019899 73 \cdot 2^{72}}$
	$x^{31691265005705678742422238 0033}$	Kasami ($i = 49$)	$x^{118681297528933393420699071140144 09 \cdot 2^{110}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
117	$x^{126765060022822827559679636275 3}$	Kasami ($i = 50$)	$x^{2769203864030953609485154184667682 1\cdot 2^{102}}$
	$x^{81129638414606672688589750403073}$	Kasami ($i = 53$)	$x^{1198251610196992059120036399366396 3\cdot 2^{103}}$
	$x^{12980742146337068711038270633410 57}$	Kasami ($i = 55$)	$x^{2747927130509768623833599563617352 5\cdot 2^{50}}$
	$x^{51922968585348275564729022912921 61}$	Kasami ($i = 56$)	$x^{2688008364229197214971687688803653 3\cdot 2^{108}}$
	$x^{83076749736557241768257565115809793}$	Kasami ($i = 58$)	$x^{2373621421044492654890830563504479 1\cdot 2^{59}}$
	$x^{288230376151711747}$	Welch	$x^{9773735263124394439641456885274255\cdot 2^{52}}$
	$x^{288230376688582655}$	Niho	$x^{1031616699404483565995076 27\cdot 2^{59}}$
	$x^{83076749736557242056487941267521535}$	Inverse	$x^{8307674973655724205648794126752153 5\cdot 2^{2}}$
119	x^{3}	Gold ($i = 1$)	$x^{2215379992974859788173011767133907 63\cdot 2^{118}}$
	x^{5}	Gold ($i = 2$)	$x^{1329227995784915872903807060280344 59\cdot 2^{116}}$
	x^{9}	Gold ($i = 3$)	$x^{7384599976582865960576705890446359 1\cdot 2^{114}}$
	x^{17}	Gold ($i = 4$)	$x^{3909494105249752567364138412589249 5\cdot 2^{112}}$
	x^{33}	Gold ($i = 5$)	$x^{2013981811795327080157283424667190 3\cdot 2^{110}}$
	x^{65}	Gold ($i = 6$)	$x^{1022483073680704517618313123292575 9\cdot 2^{108}}$
	x^{257}	Gold ($i = 8$)	$x^{1112000074294773979277503960934919 25\cdot 2^{105}}$
	x^{513}	Gold ($i = 9$)	$x^{9975687687664573315165023746743339 5\cdot 2^{103}}$
	x^{1025}	Gold ($i = 10$)	$x^{6484039003828857916603936879421 43\cdot 2^{100}}$
	x^{2049}	Gold ($i = 11$)	$x^{6649383580671248266112260794472222 7\cdot 2^{100}}$
	x^{4097}	Gold ($i = 12$)	$x^{1622196724170021812184289797755 35\cdot 2^{96}}$
	x^{8193}	Gold ($i = 13$)	$x^{9969615567067384400090192097428152 3\cdot 2^{95}}$
	x^{32769}	Gold ($i = 15$)	$x^{2028179065252091722212772836147 1\cdot 2^{90}}$
	x^{65537}	Gold ($i = 16$)	$x^{6633260845346243133393199247215166 7\cdot 2^{90}}$
	x^{262145}	Gold ($i = 18$)	$x^{9772788257170869586073175294708362 9\cdot 2^{95}}$
	x^{524289}	Gold ($i = 19$)	$x^{1071961332467015719959455914948499 65\cdot 2^{97}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{6338246956517813536363129077 75\cdot 2^{80}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{1075098971419743051823113935550793133\cdot 2^{81}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{9773735496148361034682398249616516 5\cdot 2^{74}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{1107690062510894720668286049324455 25\cdot 2^{73}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{1099169304968566588680851670304897 81\cdot 2^{77}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{3665143270544517571054272379089908 7\cdot 2^{86}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{1006499218625723456961164335074409 5\cdot 2^{82}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{9494485719547685863013972430013820 3\cdot 2^{89}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{6189700190662293862198804 47\cdot 2^{60}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{1071958062714209624869417992078517 01\cdot 2^{58}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
119	$x^{4294967297}$	Gold ($i = 32$)	$x^{19509217164114968933019281444847135 \cdot 2^{60}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{51117912186761824139952366372701 43 \cdot 2^{60}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{94956441133733274157117612359231195 \cdot 2^{49}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{95663523833316912840559389405029595 \cdot 2^{52}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{95664136060296353365343913680989339 \cdot 2^{45}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{66461399789366686227151870907069235 \cdot 2^{42}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{11076899964884373322695199070652552 5 \cdot 2^{41}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{10751108789437264018273301011557098 9 \cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{36918497078050564369850478699275207 \cdot 2^{47}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{64317810762722151969567862386007271 \cdot 2^{47}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{94950651108568662766025067157707629 \cdot 2^{59}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{64610760130416372183498617443006695 \cdot 2^{60}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{36922998782523446125135707716219335 \cdot 2^{51}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{99692095722460682813744795335471923 \cdot 2^{50}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{64400576277745856285759278136479347 \cdot 2^{58}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{25759446312553659407645184968459 51 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{11075547639155236057725591775102293 3 \cdot 2^{54}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{11071488680084424778679288483457723 7 \cdot 2^{56}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{11055223056919555640074027970951048 5 \cdot 2^{56}}$
	$x^{144115188075855873}$	Gold ($i = 57$)	$x^{64317483667012060746538286621249139 \cdot 2^{58}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{94944856841779706525039366713564013 \cdot 2^{59}}$
	$x^{576460752303423489}$	Gold ($i = 59$)	$x^{1152921504606846975 \cdot 2^{60}}$
	x^{13}	Kasami ($i = 2$)	$x^{51124153684035225880915656164628795 \cdot 2^{108}}$
	x^{57}	Kasami ($i = 3$)	$x^{58299473499338415478237151766682067 \cdot 2^{105}}$
	x^{241}	Kasami ($i = 4$)	$x^{27577344310890370807132926562180 95 \cdot 2^{96}}$
	x^{993}	Kasami ($i = 5$)	$x^{66929909153319026833021503592854 3 \cdot 2^{90}}$
	x^{4033}	Kasami ($i = 6$)	$x^{48943802969020581980217046479452311 \cdot 2^{109}}$
	x^{65281}	Kasami ($i = 8$)	$x^{86536955348200739263203382395972 3 \cdot 2^{104}}$
	x^{261633}	Kasami ($i = 9$)	$x^{50324951027765932351991762643119261 \cdot 2^{91}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{63444426954288512087537745817 5 \cdot 2^{60}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{25558961045141068635037080235237947 \cdot 2^{58}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{59337639454332849336823175942354505 \cdot 2^{51}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{99692100179105152473143578408569651 \cdot 2^{43}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{47475325863759896471383067188604343 \cdot 2^{91}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
119	$x^{4294901761}$	Kasami ($i = 16$)	$x^{65942162196050547909997715719500595 \cdot 2^{49}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{13940822362506637821290075448760363 \cdot 2^{87}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{96476225500557085230936242710287525 \cdot 2^{63}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{12089269725361337805045 75 \cdot 2^{0}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{68968661196042158343849108042299 73 \cdot 2^{80}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{96520368450574880603982887047997869 \cdot 2^{113}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{11076898644405002409243529270193902 9 \cdot 2^{1}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{10728085099510217497044133768287714 1 \cdot 2^{114}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{37873224126402532991149589505692431 \cdot 2^{113}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{59160715712113978613172705963500765 \cdot 2^{112}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{10014731475515783994493740656960971 5 \cdot 2^{92}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{94944857195476858630139724300138205 \cdot 2^{28}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{10736314109991776038687061364510430 9 \cdot 2^{95}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{38484045387535506862110348867573399 \cdot 2^{102}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{81763385739079794619084297994175 \cdot 2^{14}}$
	$x^{472236648280092573696 1}$	Kasami ($i = 36$)	$x^{99578573622735278912031429063710413 \cdot 2^{112}}$
	$x^{188894695931341141901313}$	Kasami ($i = 37$)	$x^{28446513528470962260604834362526453 \cdot 2^{112}}$
	$x^{755578637256394455121 93}$	Kasami ($i = 38$)	$x^{60419454391373146928517905009686109 \cdot 2^{34}}$
	$x^{3022314549031075378626 57}$	Kasami ($i = 39$)	$x^{13292279957849158729038092593036001 3 \cdot 2^{1}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{20148763660243819578436 3 \cdot 2^{40}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{11728482315749257770209407097292486 85 \cdot 2^{112}}$
	$x^{7737125245532747108817305 7}$	Kasami ($i = 43$)	$x^{58356351034459721294427490631116 71 \cdot 2^{100}}$
	$x^{3094850098213274765387366 41}$	Kasami ($i = 44$)	$x^{58162850940625282639356064031153459 \cdot 2^{19}}$
	$x^{1237940039285345090527035393}$	Kasami ($i = 45$)	$x^{97871274145293674493608446827616845 \cdot 2^{95}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{58287731074072403418790517442956387 \cdot 2^{29}}$
	$x^{1980704062856594366089763225 7}$	Kasami ($i = 47$)	$x^{37894662639457162701494864787036627 \cdot 2^{27}}$
	$x^{7922816251426405611856723968 1}$	Kasami ($i = 48$)	$x^{25562074556590211364859023050165957 \cdot 2^{26}}$
	$x^{1267650600228228275596796362753}$	Kasami ($i = 50$)	$x^{53514156492091822837749140253936739 \cdot 2^{1}}$
	$x^{2028240960365166592034762391552 1}$	Kasami ($i = 52$)	$x^{59155817906100976699229081326659305 \cdot 2^{48}}$
	$x^{8112963841460667268858975040307 3}$	Kasami ($i = 53$)	$x^{13521606200971406005808147376811 \cdot 2^{14}}$
	$x^{3245185536584267087687575110942 73}$	Kasami ($i = 54$)	$x^{11071496602902565150805475770359330 1 \cdot 2^{45}}$
	$x^{1298074214633706871103827063341057}$	Kasami ($i = 55$)	$x^{11055349821980522934509311705944354 1 \cdot 2^{56}}$
	$x^{2076918743413931037000679724102451 3}$	Kasami ($i = 57$)	$x^{23264633795667946269237612610700411 \cdot 2^{110}}$
	$x^{8307674973655724176825756511580979 3}$	Kasami ($i = 58$)	$x^{13656452011488861723709271230371307 \cdot 2^{4}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
119	$x^{3323069989462289676494910127666626 57}$	Kasami ($i = 59$)	$x^{4747242842088985268605893105335 8519 \cdot 2^2}$
	$x^{576460752303423491}$	Welch	$x^{3909494105249752608055485634007 3773 \cdot 2^{59}}$
	$x^{6189700202191508897529855 99}$	Niho	$x^{4126466797617934253242886 83 \cdot 2^{60}}$
	$x^{3323069989462289682259517650700861 43}$	Inverse	$x^{3323069989462289682259517650700861 43 \cdot 2^2}$
121	x^3	Gold ($i = 1$)	$x^{8861519971899439152692047068535630 51 \cdot 2^{120}}$
	x^5	Gold ($i = 2$)	$x^{5316911983139663491615228241121378 31 \cdot 2^{119}}$
	x^9	Gold ($i = 3$)	$x^{2953839990633146384230682356178543 51 \cdot 2^{118}}$
	x^{17}	Gold ($i = 4$)	$x^{1563797642099901026945655365035699 51 \cdot 2^{117}}$
	x^{33}	Gold ($i = 5$)	$x^{8055927247181308320629133698668755 1 \cdot 2^{116}}$
	x^{65}	Gold ($i = 6$)	$x^{4089932294722818070473252493170291 1 \cdot 2^{115}}$
	x^{129}	Gold ($i = 7$)	$x^{2679064177550993232209223533479819 5 \cdot 2^{108}}$
	x^{257}	Gold ($i = 8$)	$x^{4448000297179095917110015843739675 73 \cdot 2^{106}}$
	x^{513}	Gold ($i = 9$)	$x^{4301205600395634208616607641452968 13 \cdot 2^{105}}$
	x^{1025}	Gold ($i = 10$)	$x^{2593615601531543166641574751766527 \cdot 2^{111}}$
	x^{4097}	Gold ($i = 12$)	$x^{6488786896680087248737159191019 51 \cdot 2^{109}}$
	x^{8193}	Gold ($i = 13$)	$x^{7819942560336011848402721873003291 1 \cdot 2^{96}}$
	x^{16385}	Gold ($i = 14$)	$x^{7804194885230937258062022532741481 5 \cdot 2^{103}}$
	x^{32769}	Gold ($i = 15$)	$x^{8112716261008366888851091338035 1 \cdot 2^{106}}$
	x^{65537}	Gold ($i = 16$)	$x^{3977319834191708541380236576605372 67 \cdot 2^{91}}$
	x^{131073}	Gold ($i = 17$)	$x^{3987694128482178782382603680723566 59 \cdot 2^{89}}$
	x^{262145}	Gold ($i = 18$)	$x^{3826566210681281781630727407012036 11 \cdot 2^{92}}$
	x^{524289}	Gold ($i = 19$)	$x^{3977220819257373178645972522300082 19 \cdot 2^{99}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{2535298782607125414545249533951 \cdot 2^{101}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{4287838787177126122181697205191861 01 \cdot 2^{80}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{4294428933836852226160760580648024 85 \cdot 2^{76}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{4430760250043578882673144197213934 93 \cdot 2^{74}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{4300443527425927846612488507892155 33 \cdot 2^{77}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{5172053985942822942459061216346623 \cdot 2^{87}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{4430219154709386086156964554559133 01 \cdot 2^{82}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{4422089272382326602844874220863926 61 \cdot 2^{85}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{4287832257246206423349439755540699 33 \cdot 2^{89}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{2475880076264917542732038143 \cdot 2^{91}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{3797794280745131286633274599333466 69 \cdot 2^{60}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{1465290704404770265877314840415292 31 \cdot 2^{61}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
121	$x^{17179869185}$	Gold ($i = 34$)	$x^{1466057306767051794400759714755090 07 \cdot 2^{57}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{1476917178358223462731691791750885 83 \cdot 2^{55}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{3799646854697984083392255503516537 41 \cdot 2^{60}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{1465392814865416244338410877207766 47 \cdot 2^{48}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{3812514406515249845017001541434924 61 \cdot 2^{46}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{3909494105251174833034273432134730 69 \cdot 2^{44}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{4430759985953749329078074130702882 13 \cdot 2^{42}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{3987683987355352081621229594940014 59 \cdot 2^{43}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{3977614078295782431471805440093339 15 \cdot 2^{46}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{3801488626077486078455001830503968 91 \cdot 2^{45}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{3797852219876157264503288796446205 07 \cdot 2^{47}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{2572804004527611486511140358592794 75 \cdot 2^{59}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{2044718452698410913144785496177881 5 \cdot 2^{61}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{2658455912341678676276523741292265 47 \cdot 2^{51}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{2584609947788357900828193651307606 47 \cdot 2^{52}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{2573116444818803110645282956372277 51 \cdot 2^{53}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{4396677021803488228109490641746889 49 \cdot 2^{59}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{4430726181675810299211386052733392 21 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{1030377852502116975910211054623155 1 \cdot 2^{61}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{2658131433397256506262172838546931 71 \cdot 2^{55}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{2653253533660693316652079958667036 67 \cdot 2^{57}}$
	$x^{144115188075855873}$	Gold ($i = 57$)	$x^{4395872112044603767130040728282344 53 \cdot 2^{58}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{2572699346680482346553655002935861 51 \cdot 2^{61}}$
	$x^{576460752303423489}$	Gold ($i = 59$)	$x^{3797794273671188221472837367736378 51 \cdot 2^{61}}$
	$x^{1152921504606846977}$	Gold ($i = 60$)	$x^{2305843009213693951 \cdot 2^{61}}$
	x^{13}	Kasami ($i = 2$)	$x^{2044966147361409035236626246585145 55 \cdot 2^{115}}$
	x^{57}	Kasami ($i = 3$)	$x^{2331978939973536619129486070667271 23 \cdot 2^{113}}$
	x^{241}	Kasami ($i = 4$)	$x^{1103093772435614832285317062473316 7 \cdot 2^{109}}$
	x^{993}	Kasami ($i = 5$)	$x^{2677196366132761073320860141551583 \cdot 2^{106}}$
	x^{4033}	Kasami ($i = 6$)	$x^{2366441113249614670828002651330080 89 \cdot 2^{94}}$
	x^{16257}	Kasami ($i = 7$)	$x^{2140566459349763028395255510742744 03 \cdot 2^{92}}$
	x^{65281}	Kasami ($i = 8$)	$x^{3461478213928029570528135295838891 \cdot 2^{105}}$
	x^{261633}	Kasami ($i = 9$)	$x^{2774972313499142118081665222066978 1 \cdot 2^{68}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{2537777078171540481300339096575 \cdot 2^{91}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
121	$x^{16773121}$	Kasami ($i = 12$)	$x^{189982421943718904167476272294340023 \cdot 2^{86}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{153936330430623453075638622296118927 \cdot 2^{49}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{231607908393978238374394076813487197 \cdot 2^{45}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{237360693449334481346339682495869513 \cdot 2^{49}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{398766366533046296943770232555359443 \cdot 2^{68}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{102251427744730352020812775196937925 \cdot 2^{20}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{398232877760397023178081036158987467 \cdot 2^{56}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{104664260531398215223731645547625077 \cdot 2^{22}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{241785394507226756205772 7 \cdot 2^{61}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{428783224456730447949463492295841461 \cdot 2^{117}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{138428501658486914861435092618451 63 \cdot 2^{24}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{443075985390278992318387057772025173 \cdot 2^{99}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{385910462027572338845704422534000045 \cdot 2^{106}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{237269783284658188639523742583174889 \cdot 2^{116}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{5408642601266386968417271039044 3 \cdot 2^{41}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{442213992888873416096601106321419093 \cdot 2^{85}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{430042039908775182368837860635350197 \cdot 2^{103}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{189889714037256564331663729429802423 \cdot 2^{32}}$
	$x^{461168601627990425 7}$	Kasami ($i = 31$)	$x^{546258080544344881650447714748881 71 \cdot 2^{32}}$
	$x^{1844674406941458432 1}$	Kasami ($i = 32$)	$x^{151492878082147876247943035169723091 \cdot 2^{105}}$
	$x^{2951479051621729566 73}$	Kasami ($i = 34$)	$x^{230270827625910078358240371054956187 \cdot 2^{113}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{230282964800676485358790434936908243 \cdot 2^{109}}$
	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{390348171365764969123934456122071885 \cdot 2^{31}}$
	$x^{1888946593134114190131 3}$	Kasami ($i = 37$)	$x^{233425404137838884997752712048322 47 \cdot 2^{118}}$
	$x^{7555786372563944551219 3}$	Kasami ($i = 38$)	$x^{391555533642068241630587551864805741 \cdot 2^{116}}$
	$x^{3022314549031075378626 57}$	Kasami ($i = 39$)	$x^{469139292629970308083697644345183053 \cdot 2^{120}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{8059505464097527831374 51 \cdot 2^{41}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{531691198313966349161526342549346715 \cdot 2^{118}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{241677817416611541322742742280989853 \cdot 2^{36}}$
	$x^{7737125245532747108817305 7}$	Kasami ($i = 43$)	$x^{113786054113883849042350337747643157 \cdot 2^{116}}$
	$x^{1237940039285345090527035393}$	Kasami ($i = 45$)	$x^{236721837158473562341113470483479117 \cdot 2^{18}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{263770724503909752997829304592747827 \cdot 2^{20}}$
	$x^{1980704062856594366089763225 7}$	Kasami ($i = 47$)	$x^{164794422078387818639665298145215 \cdot 2^{21}}$
	$x^{7922816251426405611856723968 1}$	Kasami ($i = 48$)	$x^{203697799930054007858909276213227835 \cdot 2^{83}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
121	$x^{3169126500570567874242223800 33}$	Kasami ($i = 49$)	$x^{4654848587348540763505303837 4097399 \cdot 2^{84}}$
	$x^{1267650600228228275596796362753}$	Kasami ($i = 50$)	$x^{2357470267622756654004641256477522 91 \cdot 2^{94}}$
	$x^{5070602400912915354186999136257}$	Kasami ($i = 51$)	$x^{4291208689983640603540816513422690 109 \cdot 2^{116}}$
	$x^{2028240960365166592034762391 5521}$	Kasami ($i = 52$)	$x^{4430726182449522823742230726408492 37 \cdot 2^{53}}$
	$x^{8112963841460667268858975040 3073}$	Kasami ($i = 53$)	$x^{1854334234672465540882509224212983 59 \cdot 2^{54}}$
	$x^{3245185536584267087687575110 94273}$	Kasami ($i = 54$)	$x^{2658780510124698950780061515169923 07 \cdot 2^{96}}$
	$x^{5192296858534827556472902291 292161}$	Kasami ($i = 56$)	$x^{1023981819129586836873239687971 06811 \cdot 2^{115}}$
	$x^{2076918743413931037000679724 1024513}$	Kasami ($i = 57$)	$x^{4396683408815617901419310844376 05077 \cdot 2^{108}}$
	$x^{8307674973655724176825756511 5809793}$	Kasami ($i = 58$)	$x^{9305853518267150026061811085918 3355 \cdot 2^{119}}$
	$x^{3323069898462289676494910127 66662657}$	Kasami ($i = 59$)	$x^{4005892590036732858625553695850 88205 \cdot 2^{58}}$
	$x^{1329227995784915871750885555 673497601}$	Kasami ($i = 60$)	$x^{3797794273671188221472837367736 37853 \cdot 2^{120}}$
	$x^{1152921504606846979}$	Welch	$x^{1368322936837413399086090284673963 67 \cdot 2^{64}}$
	$x^{1152921505680588799}$	Niho	$x^{4126466801461005931686570 67 \cdot 2^{92}}$
	$x^{1329227995784915872903807060280344575}$	Inverse	$x^{1329227995784915872903807060280344575 \cdot 2^{2}}$
123	x^{3}	Gold ($i = 1$)	$x^{3544607988759775661076818827414252203 \cdot 2^{122}}$
	x^{5}	Gold ($i = 2$)	$x^{2126764793255865396646091296448551323 \cdot 2^{120}}$
	x^{17}	Gold ($i = 4$)	$x^{1876557170519881232334786438042839405 \cdot 2^{117}}$
	x^{33}	Gold ($i = 5$)	$x^{1611185449436261664125826739733751003 \cdot 2^{117}}$
	x^{129}	Gold ($i = 7$)	$x^{1566222134568272966522315295834204525 \cdot 2^{110}}$
	x^{257}	Gold ($i = 8$)	$x^{1034418673762580445839538568311552231 \cdot 2^{110}}$
	x^{1025}	Gold ($i = 10$)	$x^{1525045973700547381985245954038717293 \cdot 2^{111}}$
	x^{2049}	Gold ($i = 11$)	$x^{1063901372907399722577961727115552563 \cdot 2^{102}}$
	x^{8193}	Gold ($i = 13$)	$x^{1758675878714571959267334130774923957 \cdot 2^{99}}$
	x^{16385}	Gold ($i = 14$)	$x^{1033853010575707530319567725127416263 \cdot 2^{101}}$
	x^{65537}	Gold ($i = 16$)	$x^{1715216643232658887952288866957448885 \cdot 2^{92}}$
	x^{131073}	Gold ($i = 17$)	$x^{1720178599383706560660360019172502829 \cdot 2^{91}}$
	x^{524289}	Gold ($i = 19$)	$x^{1768845850138351911893080610641980245 \cdot 2^{96}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{1519120606952798262890538977748432603 \cdot 2^{102}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{3121487446793394894988125643125634 71 \cdot 2^{80}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{4121511905199536159162643432390681 5 \cdot 2^{85}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{1595073610787531078100801777831195443 \cdot 2^{77}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{1030409299672246113364755352685168243 \cdot 2^{79}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{1610398359659549252496370723833754 23 \cdot 2^{90}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{1758348854799342240274690949504133845 \cdot 2^{88}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
123	$x^{2147483649}$	Gold ($i = 31$)	$x^{4951760154835678092530286591 \cdot 2^{62}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{10290797399500665225032311701730627771 \cdot 2^{60}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{153061634187314620858058045653171529 1 \cdot 2^{62}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{17722904728250666245907233386483766 61 \cdot 2^{54}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{12977573793454598774329744797245 43 \cdot 2^{50}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{15948144861707955899101997560976244 99 \cdot 2^{51}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{59076799812716657721040970084177965 5 \cdot 2^{44}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{81798645894465660838846768519311423 \cdot 2^{44}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{20688215943168009460639288983814655 \cdot 2^{53}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{16225432522016964354966551740415 9 \cdot 2^{47}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{58611883562246635229461727201275278 3 \cdot 2^{62}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{17723039415611159692732667561030014 29 \cdot 2^{51}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{58642411112698277193000565211863835 1 \cdot 2^{54}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{31216716162141178935931231431034422 3 \cdot 2^{62}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{10633742836021943537506698541174095 87 \cdot 2^{54}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{59069587408827920721470849884624941 5 \cdot 2^{56}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{17714381888135078907656634647158900 05 \cdot 2^{57}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{15908870500732851485194511329135722 75 \cdot 2^{60}}$
	$x^{576460752303423489}$	Gold ($i = 59$)	$x^{17151328977869882278621366129319418 05 \cdot 2^{61}}$
	$x^{2305843009213693953}$	Gold ($i = 61$)	$x^{46116860184273879 03 \cdot 2^{62}}$
	x^{13}	Kasami ($i = 2$)	$x^{81798645894456361409465049863405820 3 \cdot 2^{118}}$
	x^{241}	Kasami ($i = 4$)	$x^{15443312814098607651994438874626410 69 \cdot 2^{109}}$
	x^{993}	Kasami ($i = 5$)	$x^{76032376798170414482312428020064021 7 \cdot 2^{109}}$
	x^{16257}	Kasami ($i = 7$)	$x^{15194914851243695996828658676538689 09 \cdot 2^{82}}$
	x^{65281}	Kasami ($i = 8$)	$x^{88499817111863457207902866175916077 5 \cdot 2^{85}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{15191235101017968182683081839526163 01 \cdot 2^{91}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{81158345368111607269627499963616209 1 \cdot 2^{64}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{17586708873403335696944486236142496 53 \cdot 2^{47}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{88613396838147450265141637169521914 3 \cdot 2^{58}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{17177316224481160552453566710023994 13 \cdot 2^{55}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{15442881917888306277562532255648086 29 \cdot 2^{69}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{17688356891265094574918547449476985 17 \cdot 2^{58}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{75955885473492845707219611089243808 9 \cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{11029210767385974565135632804030991 91 \cdot 2^{122}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
123	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{113487601581582881570711084093961364 1\cdot 2^{118}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{766862309831384099512312705712894267\cdot 2^{104}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{811747240765009887309264817338289863\cdot 2^{118}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{110430168994776810129053324124170284 1\cdot 2^{86}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{175851237182324900654587852823024712 5\cdot 2^{103}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{113933828245505361681756930980843168 9\cdot 2^{95}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{895374016588610485406342137343348423\cdot 2^{22}}$
	$x^{29514790516217295667 3}$	Kasami ($i = 34$)	$x^{759651936462498144862425792437401305\cdot 2^{17}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{177231075515729872866015763058939221 3\cdot 2^{108}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{113943097905702332087838585708002874 5\cdot 2^{113}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{766961962480185376958150864410544603\cdot 2^{118}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{118153599625325855369227489715875567 1\cdot 2^{122}}$
	$x^{773712524553274710881 73057}$	Kasami ($i = 43$)	$x^{114518104252238905973264927038390828 1\cdot 2^{113}}$
	$x^{309485009821327476538736641}$	Kasami ($i = 44$)	$x^{114007859287595123601942107935575700 1\cdot 2^{109}}$
	$x^{495176015714145073085231923 3}$	Kasami ($i = 46$)	$x^{113934987169601504644669042816787719 3\cdot 2^{95}}$
	$x^{198070406285659436608976322 57}$	Kasami ($i = 47$)	$x^{110307492081698693416026344933003002 3\cdot 2^{22}}$
	$x^{316912650057056787424222380033}$	Kasami ($i = 49$)	$x^{177230410001743627543545907354568840 5\cdot 2^{76}}$
	$x^{126765060022822827559679636275 3}$	Kasami ($i = 50$)	$x^{110307222763553247074081261184375560 7\cdot 2^{88}}$
	$x^{202824096036516659203476239155 21}$	Kasami ($i = 52$)	$x^{110292123551349216326756944244568543 3\cdot 2^{116}}$
	$x^{811296384146066726885897504030 73}$	Kasami ($i = 53$)	$x^{811595976300996441974004777855645243\cdot 2^{115}}$
	$x^{129807421463370687110382706334 1057}$	Kasami ($i = 55$)	$x^{110769901089171497230455075232352351 43\cdot 2^{101}}$
	$x^{519229685853482755647290229129 2161}$	Kasami ($i = 56$)	$x^{177143945646425923468648799304487253 3\cdot 2^{102}}$
	$x^{830767497365572417682575651158097 93}$	Kasami ($i = 58$)	$x^{765676539448078763323702005444398555\cdot 2^{113}}$
	$x^{332306998946228967649491012766662657}$	Kasami ($i = 59$)	$x^{172032535310668393458351423021112261 3\cdot 2^{120}}$
	$x^{531691198313966348930938523190768 4353}$	Kasami ($i = 61$)	$x^{151911770946847528529507350536070290 3\cdot 2^{62}}$
	$x^{2305843009213693955}$	Welch	$x^{605971586313711647966873545964719887\cdot 2^{67}}$
	$x^{495176015944736410881019084 7}$	Niho	$x^{165058672058440237267462826 7\cdot 2^{93}}$
	$x^{531691198313966349161522824112137830 3}$	Inverse	$x^{531691198313966349161522824112137830 3\cdot 2^{2}}$
125	x^{3}	Gold ($i = 1$)	$x^{141784319550391026443072753096570088 11\cdot 2^{124}}$
	x^{5}	Gold ($i = 2$)	$x^{850705917302346158658436518579420528 7\cdot 2^{123}}$
	x^{9}	Gold ($i = 3$)	$x^{472614398501303421476909176988566960 7\cdot 2^{120}}$
	x^{17}	Gold ($i = 4$)	$x^{750622868207952492933914575217135761 3\cdot 2^{118}}$
	x^{65}	Gold ($i = 6$)	$x^{719828083871215980403292438797971218 1\cdot 2^{115}}$
	x^{129}	Gold ($i = 7$)	$x^{329730975698583782425750588596674687\cdot 2^{112}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
125	x^{257}	Gold ($i = 8$)	$x^{61237585486744762393700683244043890 83\cdot 2^{111}}$
	x^{513}	Gold ($i = 9$)	$x^{82914806754614635346826171401503231\cdot 2^{108}}$
	x^{2049}	Gold ($i = 11$)	$x^{23457727831909496322206765885669723 03\cdot 2^{107}}$
	x^{4097}	Gold ($i = 12$)	$x^{41216774367711914203978435181355864 19\cdot 2^{109}}$
	x^{8193}	Gold ($i = 13$)	$x^{41169888467030422544619807105668292 87\cdot 2^{102}}$
	x^{16385}	Gold ($i = 14$)	$x^{70896486425166535224174248771449460 05\cdot 2^{99}}$
	x^{65537}	Gold ($i = 16$)	$x^{60768417105618712204700711990624817 73\cdot 2^{94}}$
	x^{131073}	Gold ($i = 17$)	$x^{64416441442751639351239251767341676 7\cdot 2^{97}}$
	x^{262145}	Gold ($i = 18$)	$x^{70892430206291949146361269399099364 69\cdot 2^{91}}$
	x^{524289}	Gold ($i = 19$)	$x^{41350886532983985321704108721978226 95\cdot 2^{101}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{20282399932249725190733259866111\cdot 2^{84}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{70334004897985515037542891152572034 13\cdot 2^{82}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{23627838133044188611793819071682241 99\cdot 2^{83}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{12486687257139560561186713656838379 83\cdot 2^{82}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{64447418937791816064096517690284342 3\cdot 2^{79}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{61000217938283015528638609209589953 09\cdot 2^{89}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{42530103726734440356567938933073149 95\cdot 2^{85}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{42452056935487128580269114554527516 67\cdot 2^{88}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{19807040619342712365826179071\cdot 2^{94}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{60764708407034783652680320453599372 43\cdot 2^{63}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{63635482006050624565199620117914454 03\cdot 2^{63}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{70857527564925760651857486613458896 21\cdot 2^{58}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{63802903233166240196154542861116833 79\cdot 2^{57}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{68612002564734580945082453011970595 01\cdot 2^{62}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{68608664145540984104846846295410172 69\cdot 2^{50}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{16486047613091243455355554618905725 43\cdot 2^{55}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{63802943797685633305939657026365816 83\cdot 2^{45}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{70892159775211632232464578934025311 57\cdot 2^{43}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{23456964631498693187393597656152839 83\cdot 2^{47}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{42452863121192685416110342224172007 55\cdot 2^{47}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{70334055990806387249165838089459698 45\cdot 2^{48}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{64901730057845173084028786239078 3\cdot 2^{63}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{70753833609394019481599053841410732 37\cdot 2^{59}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{63641825246730203640182408842401824 27\cdot 2^{58}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
125	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{6122504669444139914409585378350754971 \cdot 2^{53}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{2074891491839400669560432747452927 9 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{6255188182229217272805654453163748653 \cdot 2^{58}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{4135371479649883602588284635663200711 \cdot 2^{57}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{6880633258610723259681020506716613933 \cdot 2^{58}}$
	$x^{144115188075855873}$	Gold ($i = 57$)	$x^{6379255413087940247446374212028701491 \cdot 2^{59}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{1248589898193267430083677596657000207 \cdot 2^{59}}$
	$x^{576460752303423489}$	Gold ($i = 59$)	$x^{2344465126423788663408025703720018887 \cdot 2^{60}}$
	$x^{2305843009213693953}$	Gold ($i = 61$)	$x^{6076470837873901143815543174829890413 \cdot 2^{62}}$
	$x^{4611686018427387905}$	Gold ($i = 62$)	$x^{9223372036854775807 \cdot 2^{63}}$
	x^{13}	Kasami ($i = 2$)	$x^{3271945835778254456378601994536232803 \cdot 2^{122}}$
	x^{57}	Kasami ($i = 3$)	$x^{7462332607915317181214355426135290 79 \cdot 2^{108}}$
	x^{241}	Kasami ($i = 4$)	$x^{6177325125639443060797775549850564013 \cdot 2^{114}}$
	x^{4033}	Kasami ($i = 6$)	$x^{2214830679810224315872448163918650 03 \cdot 2^{114}}$
	x^{16257}	Kasami ($i = 7$)	$x^{2616429591260214549604590522728319 \cdot 2^{84}}$
	x^{65281}	Kasami ($i = 8$)	$x^{3786287040213793851169693026927326797 \cdot 2^{81}}$
	x^{261633}	Kasami ($i = 9$)	$x^{3050091868095637072271259268721550519 \cdot 2^{109}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{3684160762636183937725029862104059291 \cdot 2^{62}}$
	$x^{16773121}$	Kasami ($i = 12$)	$x^{4220291027245767168108353693742123827 \cdot 2^{56}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{8249488923641977080477040985230224 59 \cdot 2^{53}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{8653828065318056538466850729274 03 \cdot 2^{98}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{8740484923445587551514876078200150 83 \cdot 2^{97}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{3786285181953255202217928143691539677 \cdot 2^{72}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{7089161890990780307958934767712032085 \cdot 2^{55}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{3719500713245947604911084719164464307 \cdot 2^{58}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{1934282233720610364797747 1 \cdot 2^{0}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{7033395379427326865687330013985467093 \cdot 2^{119}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{2423800432797551143679419067905237459 \cdot 2^{2}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{2463020658118729329529721282234709655 \cdot 2^{78}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{2141758082260922140077169865185686 3 \cdot 2^{105}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{6263600536476018185454166326430091629 \cdot 2^{96}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{4254048816199518616396000304955601715 \cdot 2^{85}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{3259090103388237429904747069882820451 \cdot 2^{95}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{6076470840703478369879718063787325147 \cdot 2^{94}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
125	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{6373010938762634461298233272471689805 \cdot 2^{100}}$
	$x^{7378697628624827187 3}$	Kasami ($i = 33$)	$x^{3222369679239009464450081590535679133 \cdot 2^{105}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{7085755291793474142687770585416248661 \cdot 2^{104}}$
	$x^{4722366482800925736961}$	Kasami ($i = 36$)	$x^{3220822072137581967562103324781697339 \cdot 2^{114}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{4439142870268574706468159278564473 17 \cdot 2^{112}}$
	$x^{75557863725639445512193}$	Kasami ($i = 38$)	$x^{6871245940143401135089025189295052469 \cdot 2^{116}}$
	$x^{3022314549031075378626 57}$	Kasami ($i = 39$)	$x^{3806660720679419192662487730507818729 \cdot 2^{35}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{8507059173023461586584368704231414171 \cdot 2^{124}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{3223802185639011132549803 \cdot 2^{42}}$
	$x^{7737125245532747108817305 7}$	Kasami ($i = 43$)	$x^{2502076227360979455649156470339195603 \cdot 2^{41}}$
	$x^{3094850098213274765387366 41}$	Kasami ($i = 44$)	$x^{1648654878492918912129870114983961211 \cdot 2^{112}}$
	$x^{4951760157141450730852319233}$	Kasami ($i = 46$)	$x^{6868570297794777004626784587815934677 \cdot 2^{21}}$
	$x^{1980704062856594366089763225 7}$	Kasami ($i = 47$)	$x^{3038096341679037340649773543107145143 \cdot 2^{33}}$
	$x^{7922816251426405611856723968 1}$	Kasami ($i = 48$)	$x^{7075383400553407647572463179787840341 \cdot 2^{107}}$
	$x^{3169126500570567874242223800 33}$	Kasami ($i = 49$)	$x^{1675924964773296363943009667481172597 \cdot 2^{30}}$
	$x^{5070602400912915354186999136257}$	Kasami ($i = 51$)	$x^{6371727351435864836528312386034756811 \cdot 2^{81}}$
	$x^{2028240960365166592034762391552 1}$	Kasami ($i = 52$)	$x^{2030221663483089186098811345203 1 \cdot 2^{84}}$
	$x^{8112963841460667268858975040307 3}$	Kasami ($i = 53$)	$x^{8824723247714114522899899745976545 71 \cdot 2^{1}}$
	$x^{3245185536584267087687575110942 73}$	Kasami ($i = 54$)	$x^{3730437565403809334613041334683646563 \cdot 2^{121}}$
	$x^{5192296858534827556472902291292161}$	Kasami ($i = 56$)	$x^{6880709634560595927639135230673335597 \cdot 2^{45}}$
	$x^{2076918743413931037000679724102451 3}$	Kasami ($i = 57$)	$x^{1632778048901500799224730226033910469 \cdot 2^{47}}$
	$x^{8307674973655724176825756511580979 3}$	Kasami ($i = 58$)	$x^{3705727147121452826124635267747441821 \cdot 2^{57}}$
	$x^{3323069898462289676494910127666626 57}$	Kasami ($i = 59$)	$x^{3528938129668230217442466837362288 55 \cdot 2^{112}}$
	$x^{5316911983139663489309385231907684353}$	Kasami ($i = 61$)	$x^{6409428144058772492938446138196253517 \cdot 2^{120}}$
	$x^{2126764793255865396184922694605812 5313}$	Kasami ($i = 62$)	$x^{3038235418936950567296085568987557303 \cdot 2^{2}}$
	$x^{4611686018427387907}$	Welch	$x^{1876557170519881232741699910257020687 \cdot 2^{65}}$
	$x^{4611686020574871551}$	Niho	$x^{6602346876188694800893651627 \cdot 2^{63}}$
	$x^{2126764793255865396646091296448551 3215}$	Inverse	$x^{2126764793255865396646091296448551 3215 \cdot 2^{2}}$
	$x^{1267650638007162390353805311999}$	Dobbertin	$x^{7089216083157104489417170184312280405 \cdot 2^{1}}$
127	x^{3}	Gold ($i = 1$)	$x^{5671372782015641057722910123862803 5243 \cdot 2^{126}}$
	x^{5}	Gold ($i = 2$)	$x^{3402823669209384634633746074317682 1147 \cdot 2^{124}}$
	x^{9}	Gold ($i = 3$)	$x^{1890457594005213685907636707954267841 5 \cdot 2^{124}}$
	x^{17}	Gold ($i = 4$)	$x^{1000830490943936657245219433622847681 5 \cdot 2^{120}}$
	x^{33}	Gold ($i = 5$)	$x^{2577896719098018662601322783574001 6027 \cdot 2^{119}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
127	x^{65}	Gold ($i = 6$)	$x^{28793123354848639216131697551918848693 \cdot 2^{116}}$
	x^{129}	Gold ($i = 7$)	$x^{13189239027943351297030023543866984 95 \cdot 2^{120}}$
	x^{257}	Gold ($i = 8$)	$x^{66202795120805148533730468371939353 5 \cdot 2^{112}}$
	x^{513}	Gold ($i = 9$)	$x^{33165922701845854138730468560601190 3 \cdot 2^{118}}$
	x^{1025}	Gold ($i = 10$)	$x^{94615097143870694719084646944442869 19 \cdot 2^{111}}$
	x^{2049}	Gold ($i = 11$)	$x^{27484983760573604540355538081970542261 \cdot 2^{106}}$
	x^{4097}	Gold ($i = 12$)	$x^{25456808753055318294245622938207702427 \cdot 2^{112}}$
	x^{8193}	Gold ($i = 13$)	$x^{24317750010034110869987285811216931693 \cdot 2^{102}}$
	x^{16385}	Gold ($i = 14$)	$x^{28358594570066614089669699508579775829 \cdot 2^{100}}$
	x^{32769}	Gold ($i = 15$)	$x^{28136198027778777709237800934919465685 \cdot 2^{106}}$
	x^{65537}	Gold ($i = 16$)	$x^{25961088157906103686724644661493 75 \cdot 2^{96}}$
	x^{131073}	Gold ($i = 17$)	$x^{28301696176852674917381751260117838549 \cdot 2^{95}}$
	x^{262145}	Gold ($i = 18$)	$x^{28356972082516779658544507759639614805 \cdot 2^{92}}$
	x^{524289}	Gold ($i = 19$)	$x^{13087808306031070870720058896642171 51 \cdot 2^{96}}$
	$x^{1048577}$	Gold ($i = 20$)	$x^{28133622401273705872112459580351273653 \cdot 2^{102}}$
	$x^{2097153}$	Gold ($i = 21$)	$x^{81129599728998900762933035270143 \cdot 2^{106}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{16465296755430976438080589815378202227 \cdot 2^{84}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{28343021167173896570606967170764811605 \cdot 2^{82}}$
	$x^{16777217}$	Gold ($i = 24$)	$x^{24400092241002192912540277794355759469 \cdot 2^{80}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{25521177772600497249612828445273961267 \cdot 2^{79}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{16541503982758135899990814291631305159 \cdot 2^{81}}$
	$x^{134217729}$	Gold ($i = 27$)	$x^{24329527208129015228931449564553749723 \cdot 2^{83}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{25520917935919690046670331261698546483 \cdot 2^{88}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{25018317656025231224773139741006326125 \cdot 2^{92}}$
	$x^{1073741825}$	Gold ($i = 30$)	$x^{25454192841098565347185904709582772659 \cdot 2^{92}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{24305883396768840234452957367014710125 \cdot 2^{94}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{39614081247908796764212166655 \cdot 2^{64}}$
	$x^{8589934593}$	Gold ($i = 33$)	$x^{16465275821310834119358157314151652583 \cdot 2^{64}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{16980822616668798666131651082603783795 \cdot 2^{62}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{27522533034520273146695317468516558253 \cdot 2^{63}}$
	$x^{68719476737}$	Gold ($i = 36$)	$x^{17013988538873049699278083439188194099 \cdot 2^{56}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{25778954898798296629481483560404244 79 \cdot 2^{59}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{20764117450632877819972770370428927 \cdot 2^{64}}$
	$x^{549755813889}$	Gold ($i = 39$)	$x^{28301533443912350002690337518407297877 \cdot 2^{50}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
127	$x^{1099511627777}$	Gold ($i = 40$)	$x^{164865487849297888984383459943061110 91 \cdot 2^{48}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{275228385009593958867796423432489649 09 \cdot 2^{47}}$
	$x^{4398046511105}$	Gold ($i = 42$)	$x^{283568639100846528929858293745868690 77 \cdot 2^{44}}$
	$x^{8796093022209}$	Gold ($i = 43$)	$x^{170141183460488574544801146578772426 75 \cdot 2^{44}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{499467489325242031731899938429733993 5 \cdot 2^{49}}$
	$x^{35184372088833}$	Gold ($i = 45$)	$x^{164679452863002830497612120297480583 43 \cdot 2^{48}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{170120424409290552236509962231552673 79 \cdot 2^{49}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{274422101062041539494139808870304782 53 \cdot 2^{49}}$
	$x^{281474976710657}$	Gold ($i = 48$)	$x^{243062542072061975762242427592770659 47 \cdot 2^{64}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{255170317786940438491570990485485388 03 \cdot 2^{62}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{250207622363145796925275204356258644 93 \cdot 2^{55}}$
	$x^{2251799813685249}$	Gold ($i = 51$)	$x^{283568630649778177294392792405459162 45 \cdot 2^{52}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{257665734079979616183258799920932051 1 \cdot 2^{58}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{829956596735571465308550626700360 63 \cdot 2^{64}}$
	$x^{18014398509481985}$	Gold ($i = 54$)	$x^{945226994118314515167048947747631559 1 \cdot 2^{58}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{500411427577503183626175414218097025 5 \cdot 2^{56}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{938276676269014258373944556164006081 5 \cdot 2^{64}}$
	$x^{144115188075855873}$	Gold ($i = 57$)	$x^{244898614698929589341363655610164461 07 \cdot 2^{59}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{165403495401237798073871523650657468 87 \cdot 2^{61}}$
	$x^{576460752303423489}$	Gold ($i = 59$)	$x^{499435959277306943385063804032858473 5 \cdot 2^{64}}$
	$x^{1152921504606846977}$	Gold ($i = 60$)	$x^{937786050569515451419214761203622081 5 \cdot 2^{64}}$
	$x^{2305843009213693953}$	Gold ($i = 61$)	$x^{274421263645918116077105851360747845 3 \cdot 2^{62}}$
	$x^{4611686018427387905}$	Gold ($i = 62$)	$x^{243058833514956045436391828586746160 27 \cdot 2^{64}}$
	$x^{9223372036854775809}$	Gold ($i = 63$)	$x^{184467440737095516 15 \cdot 2^{64}}$
	x^{13}	Kasami ($i = 2$)	$x^{130877833431130178255144079781449312 11 \cdot 2^{123}}$
	x^{57}	Kasami ($i = 3$)	$x^{298493304316612687248574217045410712 7 \cdot 2^{118}}$
	x^{241}	Kasami ($i = 4$)	$x^{148255803015346633459146613196413538 83 \cdot 2^{111}}$
	x^{993}	Kasami ($i = 5$)	$x^{736764439959735847377900710955040626 1 \cdot 2^{98}}$
	x^{4033}	Kasami ($i = 6$)	$x^{885932271924089726348979265567460011 \cdot 2^{115}}$
	x^{16257}	Kasami ($i = 7$)	$x^{104657183650408581984183615498484 47 \cdot 2^{106}}$
	x^{65281}	Kasami ($i = 8$)	$x^{122000410498989977747894221702188003 11 \cdot 2^{105}}$
	x^{261633}	Kasami ($i = 9$)	$x^{151852662889827240071651138391334724 57 \cdot 2^{85}}$
	$x^{1047553}$	Kasami ($i = 10$)	$x^{147366481685592564793487146980184498 11 \cdot 2^{94}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{274421473114956790314255000908487287 57 \cdot 2^{62}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
127	$x^{16773121}$	Kasami ($i = 12$)	$x^{255190356808944318122795666007889543 23\cdot 2^{69}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{34961938307099097809827410642170239 79\cdot 2^{92}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{34615312261272226153867402917096 11\cdot 2^{99}}$
	$x^{1073709057}$	Kasami ($i = 15$)	$x^{28136177824597336572405923602423425749\cdot 2^{61}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{15191084375805419973127092273765265993\cdot 2^{51}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{11076984805034186399389181769307477 3\cdot 2^{26}}$
	$x^{68719214593}$	Kasami ($i = 18$)	$x^{28356647563963121231835739002128520533\cdot 2^{74}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{15142586099743496909647175139368576217\cdot 2^{61}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{27463734338107847415951433375886953109\cdot 2^{68}}$
	$x^{4398044413953}$	Kasami ($i = 21$)	$x^{38685644674412207298052095\cdot 2^{64}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{13721062528024628248852946202773261411\cdot 2^{23}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{28343011023493214961348899843873615189\cdot 2^{117}}$
	$x^{281474959933441}$	Kasami ($i = 24$)	$x^{24981628855637747375861000069346643245\cdot 2^{118}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{12883286723806021437729024394432065851\cdot 2^{110}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{14878025641896050884823168029859666387\cdot 2^{110}}$
	$x^{18014398375264257}$	Kasami ($i = 27$)	$x^{25486925094524248204003155429393274573\cdot 2^{96}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{25521177487380086894706655542811349811\cdot 2^{116}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{24729984178847061395763199129117477229\cdot 2^{89}}$
	$x^{1152921503533105153}$	Kasami ($i = 30$)	$x^{12884487974160806228460544990248070301\cdot 2^{105}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{25055037290445481112391583137552177741\cdot 2^{101}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{12152941678577379497883766317681175991\cdot 2^{33}}$
	$x^{73786976286248271873}$	Kasami ($i = 33$)	$x^{17545306602006418515732397372812664115\cdot 2^{21}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{17047349552011419047797276742284817203\cdot 2^{10}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{24698249369217983900294184627286226349\cdot 2^{19}}$
	$x^{472236648280092573696 1}$	Kasami ($i = 36$)	$x^{65439041530155354353611553460804447 31\cdot 2^{113}}$
	$x^{188894659313411419013 13}$	Kasami ($i = 37$)	$x^{85671590921090142170694858290823135\cdot 2^{112}}$
	$x^{755578637256394455121 93}$	Kasami ($i = 38$)	$x^{12148491678950586007965983409653228983\cdot 2^{40}}$
	$x^{3022314549031075378626 57}$	Kasami ($i = 39$)	$x^{28384529143161208415725464383424605013\cdot 2^{120}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{65946195139716756485150161358866197 71\cdot 2^{125}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{30024914728318099717356599566037001645\cdot 2^{124}}$
	$x^{1934281311382966874878771 3}$	Kasami ($i = 42$)	$x^{12895208742556044530199211\cdot 2^{43}}$
	$x^{7737125245532747108817305 7}$	Kasami ($i = 43$)	$x^{34028236692093846346337464261614030029\cdot 2^{126}}$
	$x^{3094850098213274765387366 41}$	Kasami ($i = 44$)	$x^{15467380314606868642869836402578844829\cdot 2^{38}}$
	$x^{1237940039285345090527035393}$	Kasami ($i = 45$)	$x^{33101397566568190026730163181576204 75\cdot 2^{30}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
127	$x^{49517601571414507308523192 33}$	Kasami ($i = 46$)	$x^{13036684140211649283492464424059742051 \cdot 2^{113}}$
	$x^{19807040628565943660897632257}$	Kasami ($i = 47$)	$x^{17756571481074298825827647844376087 89 \cdot 2^{118}}$
	$x^{79228162514264056118567239681}$	Kasami ($i = 48$)	$x^{69511343864361694408737266271585513 17 \cdot 2^{26}}$
	$x^{31691265005705678742422238 0033}$	Kasami ($i = 49$)	$x^{65310919231180419238951640641024416 69 \cdot 2^{110}}$
	$x^{12676506002282282755967963627 53}$	Kasami ($i = 50$)	$x^{35298892993951301919181820366661448 11 \cdot 2^{97}}$
	$x^{50706024009129153541869991362 57}$	Kasami ($i = 51$)	$x^{28356864332628417957668117787295700309 \cdot 2^{78}}$
	$x^{20282409603651665920347623915521}$	Kasami ($i = 52$)	$x^{12529613479603473535916650596625856663 \cdot 2^{100}}$
	$x^{81129638414606672688589750403073}$	Kasami ($i = 53$)	$x^{81169252476965124565472682966015 \cdot 2^{117}}$
	$x^{32451855365842670876875751109427 3}$	Kasami ($i = 54$)	$x^{97010437770578575678416410172589572 67 \cdot 2^{94}}$
	$x^{12980742146337068711038270633410 57}$	Kasami ($i = 55$)	$x^{35299253196195937017496805284892670 3 \cdot 2^{115}}$
	$x^{51922968585348275564729022912921 61}$	Kasami ($i = 56$)	$x^{96955453813108086028735631824479075 99 \cdot 2^{50}}$
	$x^{20769187434139310370006797241024513}$	Kasami ($i = 57$)	$x^{15145143229502584778886694880828536413 \cdot 2^{48}}$
	$x^{83076749736557241768257565115809793}$	Kasami ($i = 58$)	$x^{14921740284426271058879294435137899107 \cdot 2^{115}}$
	$x^{33230699894622896764949101276666 2657}$	Kasami ($i = 59$)	$x^{98519257406057199471874585242690249 19 \cdot 2^{60}}$
	$x^{13292279957849158717508855556734976 01}$	Kasami ($i = 60$)	$x^{14115752518672733542273893817774163959 \cdot 2^{124}}$
	$x^{53169119831396634893093852319076843 53}$	Kasami ($i = 61$)	$x^{27525205649706942918711497085232502453 \cdot 2^{62}}$
	$x^{21267647932558653961849226946058125313}$	Kasami ($i = 62$)	$x^{25637712576235089721080221249773024861 \cdot 2^{126}}$
	$x^{85070591730234615856620279821087277057}$	Kasami ($i = 63$)	$x^{24305883351495604543639182858674616029 \cdot 2^{126}}$
	$x^{9223372036854775811}$	Welch	$x^{10008304909439366780791892109889295055 \cdot 2^{58}}$
	$x^{39614081266355540833626750975}$	Niho	$x^{26409387504754779199279639211 \cdot 2^{64}}$
	$x^{85070591730234615865843651857942052863}$	Inverse	$x^{85070591730234615865843651857942052863 \cdot 2^{2}}$
129	x^{3}	Gold ($i = 1$)	$x^{22685491128062564230891640495451214097 1 \cdot 2^{128}}$
	x^{5}	Gold ($i = 2$)	$x^{13611294676837538538534984297270728458 3 \cdot 2^{127}}$
	x^{17}	Gold ($i = 4$)	$x^{40033219637757466289808777344913907231 \cdot 2^{125}}$
	x^{33}	Gold ($i = 5$)	$x^{20623173752784149300810582268592012831 \cdot 2^{120}}$
	x^{129}	Gold ($i = 7$)	$x^{10023821661236946985742817893338908554 9 \cdot 2^{120}}$
	x^{257}	Gold ($i = 8$)	$x^{26481118048322059413492187348775736 31 \cdot 2^{121}}$
	x^{1025}	Gold ($i = 10$)	$x^{11353811657264483366290157633333144251 7 \cdot 2^{111}}$
	x^{2049}	Gold ($i = 11$)	$x^{97318431925656388281863113692052793051 \cdot 2^{109}}$
	x^{8193}	Gold ($i = 13$)	$x^{83066609769544358223696962634391551 \cdot 2^{104}}$
	x^{16385}	Gold ($i = 14$)	$x^{66166592676845281940452334408154626503 \cdot 2^{104}}$
	x^{65537}	Gold ($i = 16$)	$x^{10384435263162441474689857864466431 \cdot 2^{113}}$
	x^{131073}	Gold ($i = 17$)	$x^{37514058593360652438303564253424116679 \cdot 2^{96}}$
	x^{524289}	Gold ($i = 19$)	$x^{37531148182720193611220338495275372303 \cdot 2^{99}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
129	$x^{1048577}$	Gold ($i = 20$)	$x^{679236156150229749781514238659761539 07 \cdot 2^{101}}$
	$x^{4194305}$	Gold ($i = 22$)	$x^{972236261255470716160265125703654347 33 \cdot 2^{86}}$
	$x^{8388609}$	Gold ($i = 23$)	$x^{199774409113546258221559323383905807 67 \cdot 2^{88}}$
	$x^{33554433}$	Gold ($i = 25$)	$x^{110091354302103752873279705801913347373 \cdot 2^{81}}$
	$x^{67108865}$	Gold ($i = 26$)	$x^{113427457330513596272809871134732670293 \cdot 2^{79}}$
	$x^{268435457}$	Gold ($i = 28$)	$x^{109937340160906749726606712542688073397 \cdot 2^{91}}$
	$x^{536870913}$	Gold ($i = 29$)	$x^{378045365755525394475756296411635347 91 \cdot 2^{88}}$
	$x^{2147483649}$	Gold ($i = 31$)	$x^{109768505621935065586628401289328514741 \cdot 2^{94}}$
	$x^{4294967297}$	Gold ($i = 32$)	$x^{158456324991635187048258732031 \cdot 2^{97}}$
	$x^{17179869185}$	Gold ($i = 34$)	$x^{112534326078323354847371464077841619637 \cdot 2^{63}}$
	$x^{34359738369}$	Gold ($i = 35$)	$x^{102068086614361221967778552167802706739 \cdot 2^{61}}$
	$x^{137438953473}$	Gold ($i = 37$)	$x^{113427239295435677136946756736460215637 \cdot 2^{57}}$
	$x^{274877906945}$	Gold ($i = 38$)	$x^{112544751547533805942686208611704990421 \cdot 2^{62}}$
	$x^{1099511627777}$	Gold ($i = 40$)	$x^{110090134668439600934392809540432471469 \cdot 2^{55}}$
	$x^{2199023255553}$	Gold ($i = 41$)	$x^{103066293827015759330276494912669573 75 \cdot 2^{53}}$
	$x^{17592186044417}$	Gold ($i = 44$)	$x^{661660157901830163071315581912573833 67 \cdot 2^{47}}$
	$x^{70368744177665}$	Gold ($i = 46$)	$x^{663318454036926509096789670824247807 \cdot 2^{47}}$
	$x^{140737488355329}$	Gold ($i = 47$)	$x^{113372084658794485000087375749082426709 \cdot 2^{48}}$
	$x^{562949953421313}$	Gold ($i = 49$)	$x^{658614382210226479320035248490573734 15 \cdot 2^{65}}$
	$x^{1125899906842625}$	Gold ($i = 50$)	$x^{979594484052778331408801135065224573 07 \cdot 2^{65}}$
	$x^{4503599627370497}$	Gold ($i = 52$)	$x^{680564713559467474390810746344693563 39 \cdot 2^{53}}$
	$x^{9007199254740993}$	Gold ($i = 53$)	$x^{679245809152942685410914342715793588 35 \cdot 2^{56}}$
	$x^{36028797018963969}$	Gold ($i = 55$)	$x^{102084645172447014294213585588052407091 \cdot 2^{59}}$
	$x^{72057594037927937}$	Gold ($i = 56$)	$x^{101826910570401145114722030868957129883 \cdot 2^{60}}$
	$x^{288230376151711745}$	Gold ($i = 58$)	$x^{523447420730536638600802801287220025 5 \cdot 2^{59}}$
	$x^{576460752303423489}$	Gold ($i = 59$)	$x^{100073270584467492043906855539107786029 \cdot 2^{60}}$
	$x^{2305843009213693953}$	Gold ($i = 61$)	$x^{101816771204690248928893057668047359387 \cdot 2^{65}}$
	$x^{4611686018427387905}$	Gold ($i = 62$)	$x^{658611032750203478432719640653365125 15 \cdot 2^{63}}$
	$x^{18446744073709551617}$	Gold ($i = 64$)	$x^{36893488147419103231 \cdot 2^{65}}$
	x^{13}	Kasami ($i = 2$)	$x^{523511333724520713020576319125797248 59 \cdot 2^{121}}$
	x^{241}	Kasami ($i = 4$)	$x^{705980014358793492662602919982921600 87 \cdot 2^{116}}$
	x^{993}	Kasami ($i = 5$)	$x^{705923137821886439813244402124312705 85 \cdot 2^{112}}$
	x^{16257}	Kasami ($i = 7$)	$x^{972474550479596543797034155211905713 73 \cdot 2^{106}}$
	x^{65281}	Kasami ($i = 8$)	$x^{726320751930325293714658442725223746 01 \cdot 2^{91}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
129	$x^{1047553}$	Kasami ($i = 10$)	$x^{113205809574008089704208739261103123285 \cdot 2^{91}}$
	$x^{4192257}$	Kasami ($i = 11$)	$x^{486117782985987071254062612943165005 53 \cdot 2^{67}}$
	$x^{67100673}$	Kasami ($i = 13$)	$x^{729131993332736325259408209105950756 57 \cdot 2^{68}}$
	$x^{268419073}$	Kasami ($i = 14$)	$x^{567125739764143681696906400914428686 79 \cdot 2^{61}}$
	$x^{4294901761}$	Kasami ($i = 16$)	$x^{729170937341367654175027663738919614 17 \cdot 2^{68}}$
	$x^{17179738113}$	Kasami ($i = 17$)	$x^{708875443652727321446917079518636487 11 \cdot 2^{58}}$
	$x^{274877382657}$	Kasami ($i = 19$)	$x^{705966225265840415290028253186398324 07 \cdot 2^{68}}$
	$x^{1099510579201}$	Kasami ($i = 20$)	$x^{519413397648447671870508285355431255 47 \cdot 2^{67}}$
	$x^{17592181850113}$	Kasami ($i = 22$)	$x^{972235334061592667515975000453959422 53 \cdot 2^{127}}$
	$x^{70368735789057}$	Kasami ($i = 23$)	$x^{705869489112314758710517763475550008 89 \cdot 2^{127}}$
	$x^{1125899873288193}$	Kasami ($i = 25$)	$x^{988344442757229497259227527730695162 05 \cdot 2^{118}}$
	$x^{4503599560261633}$	Kasami ($i = 26$)	$x^{113427452259911270917757116962150110549 \cdot 2^{1}}$
	$x^{72057593769492481}$	Kasami ($i = 28$)	$x^{109937420022894564250363145212467565237 \cdot 2^{91}}$
	$x^{288230375614840833}$	Kasami ($i = 29$)	$x^{708927366970697583750651988143125590 47 \cdot 2^{91}}$
	$x^{4611686016279904257}$	Kasami ($i = 31$)	$x^{110100822603624935651188344702161834677 \cdot 2^{94}}$
	$x^{18446744069414584321}$	Kasami ($i = 32$)	$x^{729176500573163908339232933719239931 61 \cdot 2^{100}}$
	$x^{295147905162172956673}$	Kasami ($i = 34$)	$x^{112554934273977722076293588457051998933 \cdot 2^{110}}$
	$x^{1180591620683051565057}$	Kasami ($i = 35$)	$x^{490803859539775244494868871156500750 99 \cdot 2^{19}}$
	$x^{18889465931341141901313}$	Kasami ($i = 37$)	$x^{113427888330067118634196045368348333397 \cdot 2^{112}}$
	$x^{755578637256394455121 93}$	Kasami ($i = 38$)	$x^{112544792111115110836951203877112621781 \cdot 2^{1}}$
	$x^{1208925819613529663078401}$	Kasami ($i = 40$)	$x^{994977681104796700194203702100558248 21 \cdot 2^{37}}$
	$x^{4835703278456317675569153}$	Kasami ($i = 41$)	$x^{732915867214328998228806933383801289 53 \cdot 2^{127}}$
	$x^{309485009821327476538736641}$	Kasami ($i = 44$)	$x^{756183037602085474363054761369200667 31 \cdot 2^{127}}$
	$x^{495176015714145 0730852319233}$	Kasami ($i = 46$)	$x^{729650299440608791052160204746840754 65 \cdot 2^{113}}$
	$x^{198070406285659436608976322 57}$	Kasami ($i = 47$)	$x^{113455141131071989526791521029283556693 \cdot 2^{108}}$
	$x^{3169126500570567874242223800 33}$	Kasami ($i = 49$)	$x^{566399542173581741142325594704211913 67 \cdot 2^{23}}$
	$x^{1267650600228228275596796362753}$	Kasami ($i = 50$)	$x^{486125316392268967434916562157204743 29 \cdot 2^{25}}$
	$x^{2028240960365166592034762391 5521}$	Kasami ($i = 52$)	$x^{519421401460270267872339223987030039 23 \cdot 2^{86}}$
	$x^{8112963841460667268858975040 3073}$	Kasami ($i = 53$)	$x^{519413602457075263460881336089495179 91 \cdot 2^{85}}$
	$x^{1298074214633706871103827063341057}$	Kasami ($i = 55$)	$x^{490791688144971806719377574355595226 19 \cdot 2^{116}}$
	$x^{5192296858534827556472902291292161}$	Kasami ($i = 56$)	$x^{486607106955839334959569489192918996 11 \cdot 2^{55}}$
	$x^{8307674973655724176825756511580 9793}$	Kasami ($i = 58$)	$x^{726372774357673988332337980438559830 33 \cdot 2^{107}}$
	$x^{3323069989462289676494910127666626 57}$	Kasami ($i = 59$)	$x^{974149058634326100910231264072235370 69 \cdot 2^{108}}$
	$x^{5316911983139663489309385231907684353}$	Kasami ($i = 61$)	$x^{490032985246770221153916720280178726 03 \cdot 2^{128}}$

Table 26: *(continued)*

n	F	F's Family	F^{-1}
129	$x^{21267647932558653961849226946058125313}$	Kasami ($i = 62$)	$x^{57303936908161822750800764025244454599 \cdot 2^{124}}$
	$x^{340282366920938463444927863358058659841}$	Kasami ($i = 64$)	$x^{97223533405982418148204239900827676087 \cdot 2^{65}}$
	$x^{18446744073709551619}$	Welch	$x^{39407700580917505879132243566953172751 \cdot 2^{71}}$
	$x^{18446744078004518911}$	Niho	$x^{26409387510903693889084500651 \cdot 2^{98}}$
	$x^{340282366920938463463374607431768211455}$	Inverse	$x^{340282366920938463463374607431768211455 \cdot 2^{2}}$

References

[1] Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. On Almost Perfect Nonlinear Functions Over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

[2] Thomas Beth and Cunsheng Ding. On Almost Perfect Nonlinear Permutations. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 65–76. Springer, 1993.

[3] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology-CRYPTO*, volume 90, pages 2–21. Springer, 1991.

[4] Céline Blondeau and Kaisa Nyberg. New Links between Differential and Linear Cryptanalysis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 388–404. Springer, 2013.

[5] Antonia W. Bluher. On Existence of Budaghyan–Carlet APN Hexanomials. *Finite fields and their Applications*, 24:118–123, 2013.

[6] George Boole. *An Investigation of the Laws of Thought on which are Founded the Mathematical Theories of Logic and Probabilities*. Walton and Maberly, 1854.

[7] Christina Boura and Anne Canteaut. On the Influence of the Algebraic Degree of $\mathbb{F}^{-1}$ on the Algebraic Degree of $g \circ f$. *IEEE Transactions on Information Theory*, 59(1):691–702, 2013.

[8] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. *Determining the Nonlinearity of a New Family of APN Functions*, pages 72–79. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[9] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. On the Walsh Spectrum of a New APN Function. *Cryptography and Coding*, pages 92–98, 2007.

[10] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary Mcguire. New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[11] Carl Bracken, Chik How Tan, and Yin Tan. On a Class of Quadratic Polynomials with no Zeros and its Application to APN Functions. *Finite Fields and Their Applications*, 25:26–36, 2014.

[12] Carl Bracken and Zhengbang Zha. On the Fourier Spectra of the Infinite Families of Quadratic APN Functions. *arXiv preprint arXiv:0811.4718*, 2008.

[13] Marcus Brinkmann and Gregor Leander. On the Classification of APN Functions up to Dimension Five. *Designs, Codes and Cryptography*, 49(1-3):273–288, 2008.

[14] K.A. Browning, J.F. Dillon, R.E Kibler, and M.T. McQuistan. APN Polynomials and Related Codes. *Special volume of Journal of Combinatorics, Information and System Sciences*, 34:135–159, 2009.

[15] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An APN Permutation in Dimension Six. *Finite Fields: theory and applications*, 518:33–42, 2010.

[16] Lilya Budaghyan. The Equivalence of Almost Bent and Almost Perfect Nonlinear Functions and Their Generalizations. *Ph.D. Thesis, Otto-von-Guericke-Universität Magdeburg, Universitätsbibliothek*, 2005.

[17] Lilya Budaghyan. The Simplest Method for Constructing APN Polynomials EA-inequivalent to Power Functions. In *WAIFI*, pages 177–188. Springer, 2007.

[18] Lilya Budaghyan. Construction and Analysis of Cryptographic Functions. *Habilitation Thesis, University of Paris 8*, 2013.

[19] Lilya Budaghyan and Claude Carlet. Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[20] Lilya Budaghyan and Claude Carlet. On CCZ-equivalence and its Use in Secondary Constructions of Bent Functions. *IACR Cryptology ePrint Archive*, 2009:42, 2009.

[21] Lilya Budaghyan and Claude Carlet. CCZ-equivalence of Single and Multi Output Boolean Functions. In *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq*, volume 9, pages 43–54, 2010.

[22] Lilya Budaghyan, Claude Carlet, Patrick Felke, and Gregor Leander. An Infinite Class of Quadratic APN Functions which are not Equivalent to Power Mappings. In *Information Theory, 2006 IEEE International Symposium on*, pages 2637–2641. IEEE, 2006.

[23] Lilya Budaghyan, Claude Carlet, and Leander Gregor. On Inequivalence between Known Power APN Functions. In *Proc. Conference BFCA 2008, Copenhagen*, 2008.

[24] Lilya Budaghyan, Claude Carlet, and Tor Helleseth. On Bent Functions Associated to AB Functions. In *Information Theory Workshop (ITW), 2011 IEEE*, pages 150–154. IEEE, 2011.

[25] Lilya Budaghyan, Claude Carlet, Tor Helleseth, Nian Li, and Bo Sun. On Upper Bounds for Algebraic Degrees of APN Functions. *IEEE Transactions on Information Theory*, 2017.

[26] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two Classes of Quadratic APN Binomials Inequivalent to Power Functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[27] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing New APN Functions from Known Ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[28] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a Construction of Quadratic APN Functions. In *Information Theory Workshop, 2009. ITW 2009. IEEE*, pages 374–378. IEEE, 2009.

[29] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[30] Lilya Budaghyan and Tor Helleseth. New Perfect Nonlinear Multinomials over $\mathbb{F}_{p^{2k}}$ for Any Odd Prime p. *Lecture Notes in Computer Science*, 5203:403, 2008.

[31] Lilya Budaghyan and Tor Helleseth. New Commutative Semifields Defined by New PN Multinomials. *Cryptography and communications*, 3(1):1–16, 2011.

[32] Lilya Budaghyan and Tor Helleseth. On Isotopisms of Commutative Presemifields and CCZ-equivalence of Functions. *International Journal of Foundations of Computer Science*, 22(06):1243–1258, 2011.

[33] Lilya Budaghyan, Tor Helleseth, Nian Li, and Bo Sun. Some Results on the Known Classes of Quadratic APN Functions. In *International Conference on Codes, Cryptology, and Information Security*, pages 3–16. Springer, 2017.

[34] Marco Calderini, Massimilano Sala, and Irene Villa. A Note on APN Permutations in Even Dimension. *Finite Fields and Their Applications*, 46:1–16, 2017.

[35] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Binary m-sequences with Three-valued Crosscorrelation: a Proof of Welch's Conjecture. *IEEE Transactions on Information Theory*, 46(1):4–8, 2000.

[36] Anne Canteaut, Pascale Charpin, and Gohar M. Kyureghyan. A New Class of Monomial Bent Functions. *Finite Fields and Their Applications*, 14(1):221–241, 2008.

[37] Nadya Markin Carl Bracken, Eimear Byrne and Gary McGuire. On the Fourier Spectrum of Binomial APN Functions. *Journal of Discrete Mathematics*, 23(2):596–608, 2009.

[38] Claude Carlet. Boolean Functions for Cryptography and Error Correcting Codes. *Boolean models and methods in mathematics, computer science, and engineering*, 2:257–397, 2010.

[39] Claude Carlet. Vectorial Boolean Functions for Cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

[40] Claude Carlet. Open Questions on Nonlinearity and on APN Functions. In *International Workshop on the Arithmetic of Finite Fields*, pages 83–107. Springer, 2014.

[41] Claude Carlet. Boolean and Vectorial Plateaued Functions and APN Functions. *IEEE Transactions on Information Theory*, 61(11):6272–6289, 2015.

[42] Claude Carlet. Characterizations of the Differential Uniformity of Vectorial Functions by the Walsh Transform. *IEEE Transactions on Information Theory*, 2017.

[43] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[44] Florent Chabaud and Serge Vaudenay. Links between Differential and Linear Cryptanalysis. In *Advances in Cryptology-EUROCRYPT'94*, pages 356–365. Springer, 1995.

[45] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES-the Advanced Encryption Standard*. Springer Science & Business Media, 2013.

[46] Ulrich Dempwolff and Yves Edel. Dimensional Dual Hyperovals and APN Functions with Translation Groups. *Journal of Algebraic Combinatorics*, 39(2):457–496, 2014.

[47] Whitfield Diffie and Martin Hellman. New Directions in Cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[48] Hans Dobbertin. Almost Perfect Nonlinear Power Functions over $GF(2^n)$: a New Case for n Divisible by 5. In *proceedings of: The fifth Conference on Finite Fields and Applications FQ5*, pages 113–121.

[49] Hans Dobbertin. Almost Perfect Nonlinear Power Functions on $GF(2^n)$: the Niho Case. *Information and Computation*, 151(1-2):57–72, 1999.

[50] Hans Dobbertin. Almost Perfect Nonlinear Power Functions on $GF(2^n)$: the Welch Case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[51] Hans Dobbertin. Another Proof of Kasami's Theorem. *Designs, Codes and Cryptography*, 17(1):177–180, Sep 1999.

[52] Yves Edel, Gohar Kyureghyan, and Alexander Pott. A New APN Function which is not Equivalent to a Power Mapping. *IEEE Transactions on Information Theory*, 52(2):744–747, 2006.

[53] Yves Edel and Alexander Pott. A New Almost Perfect Nonlinear Function which is not Quadratic. *Adv. in Math. of Comm.*, 3(1):59–81, 2009.

[54] Fuxi. I Ching, late 9th century BC.

[55] Robert Gold. Maximal Recursive Sequences with 3-valued Recursive Cross-correlation Functions (corresp.). *IEEE transactions on Information Theory*, 14(1):154–156, 1968.

[56] Faruk Göloğlu. Almost Perfect Nonlinear Trinomials and Hexanomials. *Finite Fields and Their Applications*, 33:258–282, 2015.

[57] Faruk Göloğlu. APN Trinomials and Hexanomials. *arXiv preprint arXiv:1411.2981*, 2014.

[58] Tor Helleseth, Torleiv Kløve, and Vladimir I Levenshtein. Hypercubic 4 and 5-designs from Double-error-correcting BCH Codes. *Designs, Codes and Cryptography*, 28(3):265–282, 2003.

[59] Fernando Hernando and Gary McGuire. Proof of a Conjecture on the Sequence of Exceptional Numbers, Classifying Cyclic Codes and APN Functions. *Journal of algebra*, 343(1):78–92, 2011.

[60] Henk D.L. Hollmann and Qing Xiang. A roof of the Welch and Niho Conjectures on Cross-correlations of Binary m-sequences. *Finite Fields and Their Applications*, 7(2):253–286, 2001.

[61] Xiang-Dong Hou. Affinity of Permutations of $\mathbb{F}_2$. In *Proc. Workshop on Coding and Cryptography 2003*, pages 273–280, 2003.

[62] Xiang-Dong Hou. Affinity of Permutations of $\mathbb{F}_2^n$. *Discrete Applied Mathematics*, 154(2):313–325, 2006.

[63] Heeralal Janwa, Gary Mcguire, and Richard M Wilson. Double-error-correcting Cyclic Codes and Absolutely Irreducible Polynomials over $GF(2)$. *Journal of Algebra*, 178(2):665–676, 1995.

[64] Heeralal Janwa and Richard M. Wilson. Hyperplane Sections of Fermat Varieties in p^3 in Char. 2 and Some Applications to Cyclic Codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.

[65] Tadao Kasami. Weight Distributions of Bose-Chaudhuri-Hocquenghem Codes. *Coordinated Science Laboratory Report no. R-317*, 1966.

[66] Tadao Kasami. The Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed-Muller Codes. *Information and Control*, 18(4):369–394, 1971.

[67] Gohar M. Kyureghyan. Crooked Maps in $\mathbb{F}_{2^n}$. *Finite Fields and their applications*, 13(3):713–726, 2007.

[68] Gohar M. Kyureghyan. The Only Crooked Power Functions are $x^{2^k+2^l}$. *European Journal of Combinatorics*, 28(4):1345–1350, 2007.

[69] Gohar M. Kyureghyan and Valentin Suder. On Inversion in $\mathbb{Z}_{2^n-1}$. *Finite Fields and Their Applications*, 25:234–254, 2014.

[70] Xuejia Lai. Higher Order Derivatives and Differential Cryptanalysis. *Kluwer International Series in Engineering and Computer Science*, pages 227–227, 1994.

[71] Gottfried Leibniz. Explanation of binary arithmetic, which uses only the characters 0 and 1, with some remarks on its usefulness, and on the light it throws on the ancient chinese

figures of fuxi. *Memoires de l'Academie Royale des Sciences*, 1703.

[72] Allan Marquand. A New Logical Machine. In *Proceedings of the American Academy of Arts and Sciences*, volume 21, pages 303–307. JSTOR, 1885.

[73] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[74] Kaisa Nyberg. Perfect Nonlinear S-boxes. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 378–386, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[75] Kaisa Nyberg. Differentially Uniform Mappings for Cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 55–64. Springer, 1993.

[76] Kaisa Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. In *International Workshop on Fast Software Encryption*, pages 111–130. Springer, 1994.

[77] Kaisa Nyberg and Miia Hermelin. Multidimensional walsh transform and a characterization of bent functions. In *Information Theory for Wireless Networks, 2007 IEEE Information Theory Workshop on*, pages 1–4. IEEE, 2007.

[78] Charles S. Peirce. *Three Papers on Logic Read Before the American Academy of Arts and Sciences.* 1867.

[79] Charles S. Peirce. A Boolean Algebra with one Constant. *Collected papers of Charles Sanders Peirce*, 4:1931–35, 1880.

[80] Charles S. Peirce. *Writings of Charles S. Peirce: A Chronological Edition, Volume 8: 1884–1886*, volume 5. Indiana University Press, 1993.

[81] Alexander Pott and Yue Zhou. CCZ and EA Equivalence Between Mappings over Finite Abelian Groups. *Designs, codes and cryptography*, 66(1-3):99–109, 2013.

[82] Longjiang Qu, Yin Tan, and Chao Li. On the Walsh Spectrum of a Family of Quadratic APN Functions with Five Terms. *Science China Information Sciences*, 57(2):1–7, 2014.

[83] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, pages 714–718, 2017.

[84] Claude E. Shannon. A Symbolic Analysis of Relay and Switching Circuits. *Electrical Engineering*, 57(12):713–723, 1938.

[85] Claude E. Shannon. Communication Theory of Secrecy Systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[86] Claude E. Shannon. A Mathematical Theory of Communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[87] Vladimir Michilovich Sidelnikov. On the Mutual Correlation of Sequences. In *Soviet Math. Dokl.*, volume 12, pages 197–201, 1971.

[88] Gustavus J. Simmons. Symmetric and Asymmetric Encryption. *ACM Computing Surveys (CSUR)*, 11(4):305–330, 1979.

[89] Bo Sun. On Equivalence of Known Families of APN Functions in Small Dimensions. *Proceeding of the 20th Conference of FRUCT Association*, 28(4):1345–1350, 2017.

[90] Bo Sun. Quadratic APN Polynomials in Few Terms in Small Dimensions. *Boolean Functions and their Application (BFA) 2017*, July 2017. Presentation.

[91] Yin Tan, Longjiang Qu, San Ling, and Chik How Tan. On the Fourier Spectra of New APN Functions. *SIAM Journal on Discrete Mathematics*, 27(2):791–801, 2013.

[92] Wade Trappe. *Introduction to Cryptography with Coding Theory*. Pearson Education India, 2006.

[93] Edwin R. van Dam and Dmitry Fon-Der-Flaass. Codes, Graphs, and Schemes from Nonlinear Functions. *European Journal of Combinatorics*, 24(1):85–98, 2003.

[94] Guobiao Weng, Yin Tan, and Guang Gong. On Quadratic Almost Perfect Nonlinear Functions and Their Related Algebraic Object. In *Workshop on Coding and Cryptography, WCC*, 2013.

[95] Satoshi Yoshiara. Equivalences of Quadratic APN Functions. *Journal of Algebraic Combinatorics*, 35(3):461–475, 2012.

[96] Satoshi Yoshiara. Equivalences of Power APN Functions with Power or Quadratic APN Functions. *Journal of Algebraic Combinatorics*, 44(3):561–585, 2016.

[97] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix Approach for Constructing Quadratic APN Functions. *IACR Cryptology ePrint Archive*, Report 2013/007, 2013.

[98] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A Matrix Approach for Constructing Quadratic APN Functions. *Designs, codes and cryptography*, 73(2):587–600, 2014.

[99] Yuliang Zheng and Xian-Mo Zhang. Plateaued Functions. In *ICICS*, volume 99, pages 284–300. Springer, 1999.

[100] Yue Zhou and Alexander Pott. A New Family of Semifields with 2 Parameters. *Advances in Mathematics*, 234:43–60, 2013.

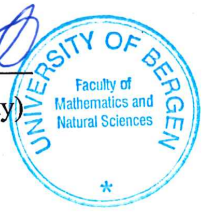
Errata for
On Classification and Some Properties Of APN Functions

Bo Sun

Thesis for the degree philosophiae doctor (PhD)
at the University of Bergen

Bo Sun
1st. Jun. 2018
(date and sign. of candidate)

Bjørke Gjedebo
(date and sign. of faculty)



Errata

Page 69 Incorrect phrasing: instead of "D_aG has to be $2^k - to - 1$ for some $k \geqslant 2$" it should say "D_aG is more than $2 - to - 1$."

Page 72 Incorrect placement of character: instead of "$a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$" it should be "$a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^*$."

Page 80 Misspelling: in the exponent inside the sum it should read "$f(a)$" and "$g(a)$" instead of "$f(z)$" and "$g(z)$."

Page 94 Misspelling: in equation (42), instead of $x \in \mathbb{F}_{2^n}$, it should read $u \in \mathbb{F}_{2^n}$.

Page 101 Misspelling: in two places near the bottom of the page, replace "affine-equivalent" with "affine equivalent."

Page 104 Missing reference number: in the title of the third column of Table 15, it should be "CCZ-equivalent to [55]" instead of just "CCZ-equivalent to."

Page 243 Misspelling: should be "Vladimir Michailovich Sidelnikov" instead of "Vladimir Michilovich Sidelnikov."

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS

uib.no

ISBN: 978-82-308-3708-5