Sequences and Linear Codes from Highly Nonlinear Functions

Chunlei Li

Dissertation for the degree of philosophiae doctor(PhD)
at the University of Bergen

2014

Dissertation date: June 16th

Acknowledgements

It is a pleasure to have this opportunity of expressing my sincere appreciation towards those who have, directly or indirectly, contributed to the research during my PhD-studies for making this dissertation possible.

First of all I wish to express my deepest gratitude to my principal supervisor Prof. Tor Helleseth, who always has his office open, ready for offering me invaluable assistance, suggesting me interesting problems and inspiring ideas to attack them and sharing his extensive knowledge and experience.

I am very thankful to my co-supervisors Alexander Kholosha and Lilya Budaghyan from whom I have learned a lot. My sincere thanks also goes to my master supervisor Prof. Xiangyong Zeng for his continuous help and encouragement.

I am very grateful to Lilya Budaghyan, Matthew G. Parker, Gaofei Wu and Yongbo Xia for proofreading my thesis. I would also like to convey thanks to all my friends and colleagues at the Selmer Center for creating such a pleasant environment to work in. Special mention is deserved by Torleiv Kløve, Øyvind Ytrehus, Håvard Raddum, Eirik Rosnes, Jinquan Luo, Nian Li, Guang Yang, Bo Sun, Mohsen Toorani and Oleksandr Kazymyrov. In addition, cordial thanks are due to the administrative staff at the Department of Informatics for their enthusiastic help with practical issues.

Last but not least, I wish to acknowledge my indebtedness to my entire family for their endless support and patience during the whole period of my education. My wife Xinjiao and little daughter Miaomiao deserve a special THANK YOU for all the happy as well as the tough time we have experienced together.

Abstract

Due to optimal nonlinearity and differential uniformity, perfect nonlinear (PN) and almost perfect nonlinear (APN) functions are of great importance in cryptography. It is interesting that they also define optimal objects in other domains of mathematics and information theory.

This dissertation is devoted to exploring the application of highly nonlinear functions, especially PN and APN functions, to the construction of low-correlation sequences and optimal linear codes. For an arbitrary odd prime p, there are only two basic classes of two-level auto-correlation p-ary sequences with no subfield structures: the m-sequences and the Helleseth-Gong sequences, where Helleseth-Gong sequences are closely related to a class of p-ary perfect nonlinear functions. Papers I and II are dedicated to investigating the cross-correlation between the p-ary m-sequences and d-decimated Helleseth-Gong sequences for some decimations d, and to constructing sequence families with low correlation from them. Papers III-IV have focused on the study of linear codes defined from highly nonlinear functions. Paper III utilizes some highly nonlinear functions including PN and APN functions to construct ternary cyclic codes with the optimal minimum (Hamming) distance. Paper IV further investigates the weight distribution of some optimal cyclic codes proposed in Paper III. Paper V examines the covering radius of some linear codes defined from PN and APN functions and presents a number of quasi-perfect linear codes.

LIST OF PAPERS

[I] Guang Gong, Tor Helleseth, Honggang Hu and Chunlei Li,“New Three-Valued Walsh Transforms from Decimations of Helleseth-Gong Sequences", *Proceedings of SETA 2012: The 7th International Conference on SEquences and Their Applications*. LNCS 7280, pp. 327-337, 2012.

[II] Chunlei Li and Tor Helleseth, “New Nonbinary Sequence Families with Low Correlation and Large Linear Span", *Proceedings of ISIT 2012: International Symposium on Information Theory*. IEEE Press 2012, pp. 1411-1415, 2012.

[III] Nian Li, Chunlei Li, Tor Helleseth, Cunsheng Ding and Xiaohu Tang, “Optimal Ternary Cyclic Codes with Minimum Distance Four and Five", *Finite Fields and Their Applications*, vol. 30: 100-120, 2014.

[IV] Chunlei Li, Nian Li, Tor Helleseth and Cunsheng Ding, “The Weight Distributions of Several Classes of Cyclic Codes from APN Monomials", *accepted by IEEE Transaction on Information Theory*, 60(8): 4710-4721, 2014.

[V] Chunlei Li and Tor Helleseth, “Quasi-Perfect Linear Codes from Planar and APN functions", is partly presented at the Sixth International Workshop on Optimal Codes and Related Topics, Varna, Bulgaria 2013.

Contents

Introduction

Scientific Results

Introduction

1 Sequences over Finite Fields with Desirable Correlation

1.1 Periodic Correlation of Sequences

Let $\{s_1(t)\}$ and $\{s_2(t)\}$ be two sequences of period N with symbols in Z_q, i.e., the set of integers modulo q. The periodic correlation between two sequences $\{s_1(t)\}$ and $\{s_2(t)\}$ is the complex inner product of the first sequence with a shifted version of the second sequence, namely,

$$C_{s_1,s_2}(\tau) = \sum_{t=0}^{N-1} \omega^{s_1(t+\tau)-s_2(t)}, \tag{1}$$

where $\omega = e^{2\pi\sqrt{-1}/q}$ is a complex primitive q-th root of unity. Pseudorandom sequences with low-correlation find applications in signal synchronization, navigation, radar ranging, random number generation, spread-spectrum communications, multipath resolution, cryptography, and signal identification in multiple-access communication systems [25]. Excellent introductions to low-correlation sequences and their applications can be found in Golomb [19], Golomb and Gong [20], Helleseth and Kumar [29].

Throughout this section, our discussion will be confined to sequences with symbols in $\mathbb{F}_p$ and period $p^n - 1$, where p is a prime, n is a positive integer and $\mathbb{F}_p$ is the finite field with p elements. Let k be a divisor of the integer n and q be a power of a prime p. The trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^k}$ is defined by

$$\mathrm{Tr}_k^n(x) = x + x^{q^k} + x^{q^{2k}} + \cdots + x^{q^{n-k}}.$$

In particular, we denote the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ by $\mathrm{Tr}_n(x)$ for simplicity.

1.2 Sequences with Ideal Two-Level Autocorrelation

Given a sequence $\{s(t)\}$ over $\mathbb{F}_p$ with period $p^n - 1$, the autocorrelation function $C_s(\tau)$ at shift τ of $\{s(t)\}$ is defined as

$$C_s(\tau) = \sum_{t=0}^{p^n-2} \omega^{s(t+\tau)-s(t)}. \tag{2}$$

These $C_s(\tau)$ for $\tau \in \{1, \cdots, p^n - 2\}$ are called the out-of-phase autocorrelation values. For applications in direct-sequence code-division multiple access, coding theory and cryptography, it is desirable to have sequences $\{s(t)\}$ with minimal value $\max_{1\leq\tau\leq p^n-2}|C_s(\tau)|$. It is possible to construct sequences $\{s(t)\}$ of period p^n-1 with autocorrelation function satisfying

$$C_s(\tau)=\begin{cases} p^n-1 & \text{if } \tau=0,\\ -1 & \text{otherwise.}\end{cases} \tag{3}$$

For obvious reasons, such sequences are said to have an ideal two-level autocorrelation.

Sequences with ideal autocorrelation properties are of considerable interest because of their applications in spread spectrum communication systems, cryptography and their close connections with difference sets. A number of ideal two-level autocorrelation sequences of period p^n-1 have been discovered during the past few decades.

1.2.1 Binary Two-Level Autocorrelation Sequences

Binary sequences with two-level autocorrelation are closely related to cyclic difference sets with Singer parameters. Let α be a primitive element of $\mathbb{F}_{2^n}$. The multiplicative group $\mathbb{F}_{2^n}^*=\mathbb{F}_{2^n}\setminus\{0\}$ is cyclic and can be denoted as $\mathbb{F}_{2^n}^*=\langle\alpha\rangle$. For $k=2^{n-1}$ (resp. $k=2^{n-1}-1$), the k-subset D of $\mathbb{F}_{2^n}^*$ is called a *cyclic difference set with Singer parameters*

$$\begin{aligned}(v,k,\lambda)&=(2^n-1,2^{n-1},2^{n-2}),\\ (resp.)\quad (v,k,\lambda)&=(2^n-1,2^{n-1}-1,2^{n-2}-1),\end{aligned}$$

if for any $g\in\mathbb{F}_{2^n}^*$, $g\neq 1$, the equation $g=x/y$ has exactly λ solutions (x,y) with x and y in D [54].

It is well known that a binary sequence $\{s(t)\}$ of period 2^n-1 has ideal two-level correlation if and only if the set

$$D=\{\alpha^t|s(t)=0,0\leq t<2^n-1\}$$

is a cyclic difference set with Singer parameter $(2^n-1,2^{n-1}-1,2^{n-2}-1)$ of $\mathbb{F}_{2^n}^*$ [54]. The currently known binary sequences with ideal two-level autocorrelation are summarized below.

• ***m*-sequences:** Let $f(x)=\sum_{i=0}^{n}f_ix^i\in\mathbb{F}_2[x]$ be a primitive polynomial with coefficients in $\mathbb{F}_2$. A binary m-sequence $\{s(t)\}$ is generated from a nonzero n-tuple and the linear recurrence relation

$$\sum_{i=0}^{n}f_is(t+i)=0,\qquad \text{for all } t\geq 0.$$

The m-sequence has period $2^n - 1$ and contains every nonzero binary n-tuple exactly once, which leads to many nice pseudo-random properties. With the above linear recursion, the $2^n - 1$ possible nonzero n-tuple $(s_0, s_1, \cdots, s_{n-1})$ generate $2^n - 1$ m-sequences, which are identical under cyclic shift. The binary m-sequence $\{s(t)\}$ can (after a suitable cyclic shift) be described simply by the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ as:

$$s(t) = \mathrm{Tr}_n(\alpha^t),$$

where α is a primitive element in $\mathbb{F}_{2^n}$. The different shifts of the m-sequence are obtained by

$$s(t) = \mathrm{Tr}_n(c\alpha^t),$$

where $c = \alpha^\tau \in \mathbb{F}_{2^n}^*$.

General m-sequences over any finite field $\mathbb{F}_q$ can be described in the same manner via extending $\mathbb{F}_2$ to $\mathbb{F}_q$, where q is a power of a prime. Due to their excellent pseudo-random properties, m-sequences are of great importance and have been intensively studied during the last half century.

- **Gordon-Mills-Welch (GMW) sequences [22]:** Consider a proper subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$, where k is a divisor of n. The GMW sequence $\{s(t)\}$ is defined by

$$s(t) = \mathrm{Tr}_k\Big(\big(\mathrm{Tr}_k^n(\alpha^t)\big)^r\Big),$$

where r is any integer relatively prime to $2^k - 1$ and in the range $1 \leq r < 2^k - 1$. When $r = 1$, the GMW sequence reduces by the transitivity of the trace function to an m-sequence.

- **Kasami-Welch (KW) sequences [14, 37]:** Let k be an integer where $1 \leq k < \lfloor n/2 \rfloor$ with $\gcd(k, n) = 1$. For $d = 2^{2k} - 2^k + 1$, consider a set

$$B_k = \{(x+1)^d + x^d + 1 \mid x \in \mathbb{F}_{2^n}\}.$$

The KW sequence $\{s(t)\}$ is defined as the characteristic sequence of B_k given by

$$s(t) = \begin{cases} 0 & \text{if } \alpha^t \in B_k, \\ 1 & \text{if } \alpha^t \notin B_k. \end{cases}$$

The exponent $d = 2^{2k} - 2^k + 1$ was given by Kasami in [37] and historically due to Welch, but never published by him. Dillon and Dobbertin in [14] proved that KW sequences have ideal two-level autocorrelation. As $\gcd(k, n) = 1$, the $\phi(n)/2$ KW sequences are pairwise inequivalent, where $\phi(\cdot)$ is the Euler-totient function. In particular, when $k = 1$, the KW sequence is identical to an m-sequence.

- **Kasami-Welch-like (KW-like) sequences [14, 48, 49]:** Let $n \not\equiv 0 \pmod 3$ be a positive integer and $k = (n \pm 1)/3$. For $d = 2^{2k} - 2^k + 1$, define

$$B_k = \{(x+1)^d + x^d + 1 \mid x \in \mathbb{F}_{2^n}\}$$

and

$$W_k = \begin{cases} B_k & \text{if } n \text{ is even,} \\ \mathbb{F}_{2^n} \setminus B_k & \text{if } n \text{ is odd.} \end{cases}$$

Then the characteristic sequence given by

$$s(t) = \begin{cases} 0 & \text{if } \alpha^t \in W_k, \\ 1 & \text{if } \alpha^t \notin W_k \end{cases}$$

has an ideal two-level autocorrelation. The KW-like sequences were found by No et al. in [48, 49], where their two-level autocorrelation property was conjectured. This conjecture was later confirmed by Dillon and Dobbertin [14].

- **Hyperoval sequences [43]:** For odd n, consider a set

$$M_k = \{x + x^k \mid x \in \mathbb{F}_{2^n}\}$$

where k is one of the following:

i) $k = 2$ (the Singer Case);

ii) $k = 6$ (the Segre Case);

iii) $k = 2^\sigma + 2^\pi$ where $\sigma = (n+1)/2$ and $4\pi \equiv 1 \pmod n$ (the Glynn I Case);

iv) $k = 3 \cdot 2^\sigma + 4$ where $\sigma = (n+1)/2$ (the Glynn II Case).

Then a characteristic sequence $\{s(t)\}$ of M_k given by

$$s(t) = \begin{cases} 0 & \text{if } \alpha^t \in M_k, \\ 1 & \text{if } \alpha^t \notin M_k \end{cases}$$

has an ideal two-level autocorrelation [43] and this sequence is called the hyperoval sequence.

1.2.2 p-ary Two-Level Autocorrelation Sequences

As mentioned in the last subsection, binary sequences with ideal two-level correlation are equivalent to cyclic difference sets with Singer parameters. But the p-ary case for an odd prime p behaves very differently. It was shown that p-ary sequences with ideal two-level correlation are equivalent to a class of generalized weighing matrices [3], which in turn give rise to a class of relative difference sets that are extensions of Singer parameters. More concretely, given a p-ary sequence $\{s(t)\}$ with ideal two-level correlation, the set

$$D = \left\{ \alpha^t \mid s(t) = 0, 0 \le t < \frac{p^n - 1}{p - 1} \right\}$$

forms a cyclic difference set with Singer parameters [47]

$$\left(\frac{p^n - 1}{p - 1}, \frac{p^{n-1} - 1}{p - 1}, \frac{p^{n-2} - 1}{p - 1} \right).$$

Up to now, only a few families of p-ary sequences $\{s(t)\}$ with ideal two-level correlation and period $p^n - 1$ have been constructed. Aside from the well understood m-sequences and GMW sequences, the p-ary sequences with ideal two-level correlation constructed in the past fifteen years are summarized below.

- **Helleseth-Kumar-Martinsen (HKM) sequence [28]:** Let $p = 3$, $n = 3k$ and $d = 3^{2k} - 3^k + 1$. Define

$$f(x) = x + x^d.$$

Then the ternary sequence $\{s(t)\}$ of period $3^n - 1$ defined by

$$s(t) = \mathrm{Tr}_n(f(\alpha^t))$$

has ideal two-level autocorrelation.

- **Dillon sequence [13]:** Let p be an odd prime and m be an odd integer. For every even integer k with $0 \le k \le n - 1$, let $g_k : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the quadratic form given by

$$g_k(x + x^{p^{2k}}) = \mathrm{Tr}_n(x^{p^k + 1})$$

and let h_k be the related function given by $h_k(x) = x^r g_k(x)$, where r is the odd part of $p^n - 1$. Then the sequence $\{s(t)\}$ defined by

$$s(t) = h_k(\alpha^t)$$

has ideal two-level autocorrelation.

- **Helleseth-Gong (HG) sequence [24]:** Let p be an odd prime, $n = (2m+1)k$, and $s, 1 \leq s \leq 2m$, be an integer such that $\gcd(s, 2m+1) = 1$. Let $b_0 = 1, b_i = b_{2m+1-i}$, and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken mod $2m+1$. Let $u_0 = b_0/2 = (p+1)/2$, and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(p^{2ki}+1)/2}.$$

Then the sequence $\{s(t)\}$ defined by

$$s(t) = \mathrm{Tr}_n(f(\alpha^t))$$

has ideal two-level autocorrelation. Let

$$g(x) = \sum_{i=0}^{m} u_{m-i} x^{(p^{(2i+1)k}+1)/(p^k+1)}.$$

The sequence $\{s'(t)\}$ with

$$s'(t) = \mathrm{Tr}_n(g(\alpha^t))$$

also has ideal two-level autocorrelation. Take $v = (p^{2mk}+1)/2$. A simple calculation implies $\gcd(v, p^{(2m+1)k} - 1) = 1$ and

$$\mathrm{Tr}_n(f(x)) = \mathrm{Tr}_n(g(x^v)).$$

Thus, the sequence $\{s'(t)\}$ is actually some decimation of the sequence $\{s(t)\}$. HG sequences can be viewed as the generalization (within equivalence) of HKM sequences, which are obtained from the HG sequence $\{s'(t)\}$ by letting $p = 3$, $m = 1$ and $g(x) = x + x^{(p^{3k}+1)/p^k+1}$.

- **Lin sequence [2, 32, 41]:** Let $n = 2m+1$ and $d = 2 \cdot 3^m + 1$. Then the sequence defined by

$$s(t) = \mathrm{Tr}_n(\alpha^t + \alpha^{dt})$$

has ideal two-level autocorrelation. This family of sequences was given by Lin and its ideal two-level autocorrelation property was conjectured in his PhD thesis [41] in 1998. Recently, the autocorrelation property of this class of sequences was separately proved by Arasu et al. in [2] via character sum and Hu et al. in [32] via decimation-Hadamard transform.

1.3 Crosscorrelations between Two-level Autocorrelation Sequences and Their Decimations

1.3.1 Crosscorrelation and Sequence Families

Let $\{a(t)\}$ be a p-ary sequence of period $p^n - 1$. Then a sequence $\{b(t)\}$ is called a d-decimation of $\{a(t)\}$, denoted by $\{a(dt)\}$, if elements of $\{b(t)\}$ are given by $b(t) = a(dt)$ for $t = 0, 1, \cdots, p^n - 2$, where the multiplication is computed modulo $p^n - 1$.

Given two p-ary sequences $\{a(t)\}, \{b(t)\}$ of period $p^n - 1$, their crosscorrelation function is defined by

$$C_{a,b}(\tau) = \sum_{t=0}^{p^n-2} \omega^{a(t+\tau)-b(t)}, \tag{4}$$

where $0 \leq \tau \leq p^n - 2$ and $\omega = e^{2\pi\sqrt{-1}/p}$ is a complex primitive p-th root of unity.

The crosscorrelation function is important in code-division multiple-access (CDMA) communication systems. Here each user is assigned a distinct signature sequence. To minimize interference due to the other users, it is desirable that the signature sequences have pairwise low values of crosscorrelation function. To provide the system in addition with a self-synchronizing capability, the signature sequences are required have low values of the autocorrelation function as well. It is worth pointing that in practice, because of data modulation the correlations that one runs into are typically of an aperiodic rather than a periodic nature. The problem of designing for low aperiodic correlation, however, is much more difficult. Therefore, a typical approach has been to design based on periodic correlation, and then to analyze the resulting design for its aperiodic correlation properties.

Let $\mathcal{F}$ be a family of M p-ary sequences $\{s_i(t)\}$ of period $p^n - 1$. Let $C_{i,j}(\tau)$ denote the crosscorrelation between the i-th and j-th sequences at shift τ, i.e.,

$$C_{i,j}(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_i(t+\tau)-s_j(t)}, \quad 0 \leq \tau \leq p^n - 2.$$

The maximum correlation value $C_{\max}$ of $\mathcal{F}$ is defined by

$$C_{\max} = \max\{|C_{i,j}(\tau)| : \text{ either } i \neq j \text{ or } \tau \neq 0 \}. \tag{5}$$

The classical goal in sequence design for CDMA systems has been minimization of the parameter $C_{\max}$ and maximization of the family size M for a given period, which are conflicting requirements. Several bounds due to Welch and Sidelnikov have been given on the best one can do if two of the parameters, family size, period and $C_{\max}$, are fixed [29]. Therefore, for theory and practice, it is interesting to study the crosscorrelation of a pair of (decimated) two-level autocorrelation sequences of period $p^n - 1$.

1.3.2 Crosscorrelation of Binary Sequences

Subsection 1.2.1 summarized the known binary two-level autocorrelation sequences: m-sequences, GMW sequences, KW sequences, KW-like sequences and hyperoval sequences. There has been intensive research concerning crosscorrelation of a pair of them or their decimations. If the maximum crosscorrelation of a pair of binary sequences of period $2^n - 1$ is much larger than the optimum value, then the pair is not so attractive in practice. The pairs of binary sequences having correlation with at most 5 possible values have been of significant interest, see a summary of these cases in [58] and references therein. It is generally challenging to settle the correlation distribution for a pair of binary sequences. The correlation distributions for many pairs leading to 3-valued and 4-valued crosscorrelation have been determined [6, 11, 18, 26, 31, 37, 46]. However, it is more difficult to determine the correlation distribution of those pairs leading to 5-valued crosscorrelation and most of the correlation distributions are left open [30, 35, 36, 58].

1.3.3 Crosscorrelation of p-ary Sequences

Compared to the binary case, the research on the crosscorrelation of a pair of p-ary sequences with ideal two-level autocorrelation is far less developed.

- **A p-ary m-sequence and its decimations:** It was proved by Helleseth [23] that for $d \notin \{1, p, \cdots, p^{n-1}\}$, the crosscorrelation function $C_d(\tau)$ of an m-sequence $\{s(t)\}$ and its d-decimation takes on at least three values. For p-ary sequences of length $p^n - 1$, all the decimations d known to give 3-valued crosscorrelation are listed below:

(i) $d = \frac{p^{2k}+1}{2}$, $\frac{n}{\gcd(n,k)}$ is odd [56];

(ii) $d = p^{2k} - p^k + 1$, $\frac{n}{\gcd(n,k)}$ is odd [56];

(iii) $d = 2 \cdot 3^{\frac{n-1}{2}} + 1$, n is odd and $p = 3$ [16].

Some other families of decimations for p-ary m-sequences that lead to low crosscorrelation $C_d(\tau)$ with few values were recently summarized in [10].

• **A p-ary m-sequence and a subclass of Helleseth-Gong sequences with certain decimations:** Gong, Helleseth and Hu in [21] showed that the crosscorrelation between an m-sequence and a subclass of Helleseth-Gong sequences with decimations $d \in \{1, (p^n+1)/(p^k+1)\}$ takes values from the set $\{0, \pm p^{(n+k)/2}\}$ and they determined the crosscorrelation distribution.

1.4 Summaries of Papers I and II

Crosscorrelation properties of binary sequences with ideal two-level autocorrelation have been extensively studied. The research for the p-ary case is less developed. For p-ary sequences, there are only two basic classes of two-level autocorrelation sequences with no subfield structures for an arbitrary odd prime p. One is the class of p-ary m-sequences and the other is the class of p-ary Helleseth-Gong sequences [24]. For crosscorrelation of p-ary sequences, the research has been mostly directed to finding proper decimations d resulting in low-correlation from m-sequences. Recently, Gong, Helleseth, and Hu studied the crosscorrelation of m-sequences and a subclass of Helleseth-Gong sequences as well as some of their decimations [21]. Many decimations that yield three-valued crosscorrelation have been found by computer search.

Paper I extends the research in [21]. Let $n = (2m+1)k$, and $s, 1 \leq s \leq 2m$, be an integer such that $\gcd(s, 2m+1) = 1$. Let $b_0 = 1$, $b_i = b_{2m+1-i}$, and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken mod $2m+1$. Let $u_0 = b_0/2 = (p+1)/2$, and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Recall that the Helleseth-Gong sequence $\{s(t)\}$ is defined by $s(t) = \mathrm{Tr}_n(f(\alpha^t))$, with

$$f(x) = \sum_{i=0}^{m} u_i x^{(p^{2ki}+1)/2}. \tag{6}$$

For $u_i = (-1)^i$ and $d \in \{1, (p^n+1)/(p^k+1)\}$, the crosscorrelation between the m-sequence $a(t) = \mathrm{Tr}_n(\alpha^t)$ and the sequence $b(t) = \mathrm{Tr}_n(f(\alpha^{dt}))$ is 3-valued and the crosscorrelation distribution is determined [21].

There are two main contributions in Paper I. One contribution in Paper I is that u_i is not limited to $(-1)^i$ as in [21], but is relaxed to that in the definition of Helleseth- Gong sequences. The other contribution in Paper I finds more decimation numbers for three-valued cross-correlation by settling the ranks of the following two quadratic forms over $\mathbb{F}_q$ with $q = p^k$:

$$Q_\lambda(x) = Tr_k^n \left(\sum_{i=0}^{m} u_i x^{q^{2i}+1} + \lambda x^2 \right)$$

and

$$Q_\lambda(x) = Tr_k^n \left(\sum_{i=0}^{m} u_i x^{q^{2i}+1} + \lambda x^{q^{(m+1)s}+1} \right).$$

Paper II concerns the application of Helleseth-Gong sequences to constructing p-ary sequence families with good correlation. In 2004, Jang et al [34] used the Helleseth-Gong sequences and m-sequences to construct a family of p-ary sequences with period $p^n - 1$:

$$\mathcal{F} = \left\{ \{\mathrm{Tr}_n(f(\beta\alpha^{2t}) + \alpha^t)\} \mid \beta \in \mathbb{F}_{p^n} \right\},$$

where $f(x)$ is the function given in (6). It was shown that the maximum nontrivial correlation value $C_{\max}$ (as in (5)) of all pairs of distinct sequences in such a family does not exceed $p^{n/2} + 1$, which is optimal with respect to Welch's bound [29].

Paper II acts as a second attempt to employ p-ary Helleseth-Gong sequences and m-sequences to construct a new p-ary sequence family with good correlation properties. Take $q = p^k$. Starting from the decimations $d = 1$ or $(q^{(m+1)s} + 1)d \equiv 2 \pmod{q^{2m+1} - 1}$, discovered in Paper I, we construct two new families of sequences with period $p^n - 1$:

$$\mathcal{A} = \left\{ \{\mathrm{Tr}_n(f(\alpha^{dt}) + \beta\alpha^t)\} \mid \beta \in \mathbb{F}_{p^n} \right\} \cup \left\{ \{\mathrm{Tr}_n(\alpha^t)\} \right\} \tag{7}$$

and

$$\begin{aligned} \mathcal{B} = \Big\{ \Big\{ \mathrm{Tr}_n \big(f(\alpha^{2t}) + u\alpha^{(q^{(m+1)s}+1)t} + v\alpha^t \big) \Big\} \mid u \in \mathbb{F}_{p^n}, v \in \Gamma \Big\} \cup \\ \Big\{ \{\mathrm{Tr}_n(w\alpha^{(q^{(m+1)s}+1)t} + \alpha^t)\} \mid w \in \mathbb{F}_{p^n} \Big\} \end{aligned} \tag{8}$$

where $f(x)$ is the function given in (6) and $\Gamma = \{1, \alpha, \cdots, \alpha^{(p^n-3)/2}\}$. By the examination of the rank of certain quadratic forms, Paper II shows that Family $\mathcal{A}$ has nontrivial correlation from the set $\{-1, -1 \pm p^{(n+k)/2}, -1 \pm p^{(n+3k)/2}\}$, Family $\mathcal{B}$ has family size $p^n(p^n + 1)/2$ and has the magnitude of nontrivial correlations upper bounded by $1 + p^{(n+3k)/2}$.

2 Linear Codes from Highly Nonlinear Functions

Claude Shannon's landmark paper "A mathematical theory of communication", written in 1948 [53], signified the beginning of the discipline in electronic engineering called information theory and also the branch of it called error-correcting codes. Given a communication channel which may corrupt messages sent over it, the object of an error-correcting code is to provide a systematic way of adding redundancy to a message so that the original message can be recovered if it has been corrupted in transmission [33].

The applications of error-correcting coding to communication channels are too numerous to mention. Error-correcting coding gives high fidelity on compact discs. It has been used to transmit black and white pictures from Mariner space probes as well as colorful pictures from recent Voyager journeys. Since the publication of Shannon's work, mathematicians have developed connections between error-correcting coding and aspects of algebra and combinatorics. Sophisticated mathematical techniques have proved useful for coding and coding problems. Among all types of codes, linear codes have been studied the most. Because of their algebraic structure, they are easier to describe, encode, and decode than nonlinear codes [42]. Linear codes also have found a lot of applications in cryptography [1, 44, 45].

2.1 Basics of Linear Codes

We denote by $\mathbb{F}_q$ the finite field of q elements, where q is a prime power. Let $\mathbb{F}_q^n$ denote the n-dimensional vector space over $\mathbb{F}_q$ consisting of all vectors (words) $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$ with coordinates in $\mathbb{F}_q$.

The *Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$ between any two words $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is the number of positions where they differ, i.e.,

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \,|\, x_i \neq y_i\}|.$$

Related to the Hamming distance is the *Hamming weight* $w_H(\mathbf{x})$ of a vector $\mathbf{x} \in \mathbb{F}_q^n$ which is the number of non-zero positions in $\mathbf{x}$, i.e.,

$$w_H(\mathbf{x}) = |\{i \,|\, x_i \neq 0\}|.$$

Any subset of $\mathbb{F}_q^n$ defines a code $\mathcal{C}$ of length n. The cardinality or the size of $\mathcal{C}$ is denoted by $|\mathcal{C}|$ and an element $\mathbf{c} \in \mathcal{C}$ is called a codeword of

$\mathcal{C}$. The minimum Hamming distance between two different codewords $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ is the minimum distance d of $\mathcal{C}$ defined as

$$d(\mathcal{C}) = \min\{d_H(\mathbf{c}_1, \mathbf{c}_2) \mid \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C},\ \mathbf{c}_1 \neq \mathbf{c}_2\}.$$

The minimum distance d of a code $\mathcal{C}$ defines its error-correcting properties: $t = \lfloor \frac{d-1}{2} \rfloor$, which is known as the *packing radius* of the code $\mathcal{C}$. The *covering radius* ρ of a code $\mathcal{C}$ is the smallest possible integer such that the spheres of this radius around the codewords cover the whole space $\mathbb{F}_q^n$, i.e.,

$$\rho = \max_{x \in \mathbb{F}_q^n} \min_{\mathbf{c} \in \mathcal{C}} d(x, \mathbf{c}).$$

By convention, we use the notation $(n, M, d)_q$ to denote the code $\mathcal{C}$ consisting of M codewords with coordinates in $\mathbb{F}_q$ and length n and having minimum distance d. If $\mathcal{C}$ forms a linear subspace in $\mathbb{F}_q^n$ with dimension k, then the size of $\mathcal{C}$ is $|\mathcal{C}| = q^k$ and we refer to $\mathcal{C}$ as an $[n, k]_q$ linear code over $\mathbb{F}_q$. We also use the notation $[n, k, d]_q$ to emphasize that $\mathcal{C}$ has minimum distance d.

A *parity check matrix* H of an $[n, k]_q$ linear code $\mathcal{C}$ is an $(n-k) \times n$-matrix such that

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H^T = \mathbf{0}\},$$

where T and $\mathbf{0}$ denote the transpose of a matrix and the all-zero vector of size $n-k$, respectively. It follows that $\mathcal{C}$ has minimum distance d if and only if any $d-1$ columns in H are linearly independent and there exist d linearly dependent columns. A *generator matrix* G of an $[n, k]_q$ linear code $\mathcal{C}$ is a $k \times n$-matrix where the k rows form a basis of $\mathcal{C}$. It follows that

$$\mathcal{C} = \{\mathbf{m}G \mid \mathbf{m} \in \mathbb{F}_q^k\}.$$

Let $\mathcal{C}^\perp$ denote the set of vectors in $\mathbb{F}_q^n$ orthogonal to all codewords in an $[n, k]_q$ linear code $\mathcal{C}$, i.e.,

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid (\mathbf{x}, \mathbf{c}) = 0, \forall \mathbf{c} \in \mathcal{C}\},$$

where $(\mathbf{x}, \mathbf{c}) = x_1c_1 + x_2c_2 + \cdots + x_nc_n$ and where all operations are performed in $\mathbb{F}_q$. It follows that $\mathcal{C}^\perp$ is also a linear code with length n and dimension $n-k$, called the *dual code* of $\mathcal{C}$ with parameter $[n, n-k, d^\perp]_q$. Moreover, the above defined matrices G and H connected with the code $\mathcal{C}$ are a parity check matrix and a generator matrix of $\mathcal{C}^\perp$ respectively.

Let $\mathcal{C}$ be an $[n,k]_q$ linear code. Let A_i, $i = 0, 1, \cdots, n$ denote the number of codewords of $\mathcal{C}$ with (Hamming) weight i. The sequence $(A_0, A_1, \cdots, A_n)$ is called the *weight distribution* of $\mathcal{C}$ and the polynomial $A(x) = A_0 + A_1x + \cdots + A_nx^n$ is termed the *weight enumerator* of $\mathcal{C}$. The weight distribution of the dual code $C^{\perp}$, denoted by $A_0^{\perp}, A_1^{\perp}, \cdots, A_n^{\perp}$, can be determined by the MacWilliams identities if the weight distribution of $\mathcal{C}$ is known [42]. The weight distribution $(A_0, A_1, \cdots, A_n)$ is an important research object in coding theory because it allows the computation of the probability of error detection and correction with respect to some algorithms [38].

An $[n,k]_q$ linear code $\mathcal{C}$ is *cyclic* if any cyclic shift of a codeword is also a codeword of $\mathcal{C}$. By identifying $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ with

$$\sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x]/(x^n - 1),$$

any cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ corresponds to an ideal of the polynomial residue class ring $\mathbb{F}_q[x]/(x^n - 1)$ and can be expressed as $\mathcal{C} = \langle g(x) \rangle$, where $g(x)$ is the *generator polynomial* of $\mathcal{C}$. The polynomial $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check polynomial* of $\mathcal{C}$.

The minimum distance d is a simple measure of the goodness of a code. For a given length and number of codewords, a fundamental problem in coding theory is to produce a code with the largest possible d. Alternatively, given n and d, it is of interest to determine the maximum number $A_q(n,d)$ of codewords in a code over $\mathbb{F}_q$ of length n and minimum distance at least d.

Given a code $\mathcal{C}$ over $\mathbb{F}_q$ of length n and minimum distance d, the sphere of radius r about any codeword $\mathbf{c}$ contains in total $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ vectors in $\mathbb{F}_q^n$. The fact that the spheres of radius $t = \lfloor \frac{d-1}{2} \rfloor$ about codewords are pairwise disjoint immediately implies the following elementary inequality, commonly referred to as *the sphere packing bound* or *the Hamming Bound*.

Theorem 1. *(Sphere Packing Bound) Let $\mathcal{C}$ be a code over $\mathbb{F}_q$ of length n and minimum distance d. Then*

$$A_q(n,d) \leq \frac{q^n}{\sum\limits_{i=0}^{t} \binom{n}{i}(q-1)^i}, \tag{9}$$

where $t = \lfloor \frac{d-1}{2} \rfloor$.

From the sphere packing bound, we see that when we get equality in the bound, we actually fill the space $\mathbb{F}_q^n$ with disjoint spheres of radius t. In other words, every vector in $\mathbb{F}_q^n$ is contained in precisely one sphere of radius t centered about a codeword. A code $\mathcal{C}$ that meets the sphere packing bound with equality is called *perfect*. It follows that a code is perfect if and only if its packing radius t equals its covering radius ρ. The parameters for which perfect codes over Galois fields exist have been completely classified in the early 1970s [55, 57, 60].

Theorem 2. *A perfect code $\mathcal{C}$ with parameter $(n, M, d)_q$ satisfies one of the following:*

(1) $(n, q^n, 1)_q$*, the whole space* $\mathbb{F}_q^n$*, where* n *is a positive integer and* q *is a prime power;*

(2) $(2l-1, 2, 2l-1)_2$*, the binary repetition codes, where* l *is a positive integer;*

(3) $(23, 2^{11}, 7)_2$ *the binary Golay code;*

(4) $(11, 3^6, 5)_3$ *the ternary Golay code;*

(5) $\left(\frac{q^s-1}{q-1}, q^{\frac{q^s-1}{q-1}-s}, 3\right)_q$*, where* s *is a positive integer and* q *is a prime power.*

It is worth noting that we make no assumption of linearity on the above codes. The codes of (1) through (4) are unique up to affine equivalence. The Hamming codes occur under (5) and there exist nonlinear perfect codes with the parameters as in (5) but not affine equivalent to a Hamming code.

In the case when the covering radius exceeds the packing radius by one, the code C is called *quasi-perfect*. As the parameters of perfect codes are completely classified, it is particularly interesting to investigate quasi-perfect codes. There has been a lot of research into constructing quasi-perfect codes, e.g. certain double error correcting BCH codes. However, unlike perfect codes, the corresponding classification task for the sets of possible parameters for quasi-perfect codes is much more complicated [33].

2.2 Planar and Almost Perfect Nonlinear Functions

Let $f(x)$ be a function from a finite Abelian group $(A;+)$ to a finite Abelian group $(B;+)$. If for each nonzero $a \in A$, the difference function

$f(x+a) - f(x)$ takes on all the elements of B the same number of times, the function f is called *planar*. Planar functions were introduced for the study of affine and projective planes by Dembowski and Ostrom in 1968 [12]. Taking $A = \mathbb{Z}_r^m$ and $B = \mathbb{Z}_r$, where r and m are positive integers and $\mathbb{Z}_r$ denotes the set of integers modulo r, Nyberg in [50] introduced the so-called *perfect nonlinear* (PN) functions in cryptography. Then, in this context, the bent functions introduced by Rothaus in [52] and later generalized by Kumar et al. in [39] can be seen as a special case of planar function. where q is a power of an odd prime,

Let $f(x)$ be a function from finite field $\mathbb{F}_q$ to itself, where q is a power of an odd prime. Define

$$\Delta_f = \max_{a \in \mathbb{F}_q^*} \max_{b \in \mathbb{F}_q} |\{x \in \mathbb{F}_q : f(x+a) - f(x) = b\}|.$$

Nyberg [51] defined a mapping to be differentially δ-uniform if $\Delta_f = \delta$. This concept is of interest in cryptography since differential and linear cryptanalysis exploit weaknesses in the uniformity of the vectorial Boolean functions which are used as S-boxes in DES and in many other block ciphers. It is desirable that the functions used for cryptography have differential uniformity as small as possible.

In the binary case, the solutions of $f(x+a) - f(x) = b$ come in pairs and therefore $\Delta_f \geq 2$. In this sense, differentially 2-uniform functions, called *almost perfect nonlinear* (APN), are optimal. In the case when p is odd there exist differentially 1-uniform functions, which are perfect nonlinear functions. It is interesting that PN functions and APN functions also define optimal objects in sequence design, coding theory and combinatorics. This fact has led to intensive research and an abundance of results on PN functions and APN functions. Please refer to [5, 7, 27, 59] for more details on these results. In what follows, we shall be concerned mainly with the applications of PN, APN and some other highly nonlinear functions to the construction of linear codes with good properties.

2.3 Three Classes of Linear Codes

Let m be a positive integer and q be a power of a prime. Let α be a primitive element of $\mathbb{F}_{q^m}$. Let $f(x)$ be a mapping from $\mathbb{F}_{q^m}$ to itself with $f(0) = 0$. Define a linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length $n = q^m - 1$, which admits one of the following matrices as its parity-check matrix:

Type I

$$H_1 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^m-2}) \end{bmatrix},$$

Type II

$$H_2 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^m-2}) \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix},$$

Type III

$$H_3 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^m-2}) \\ 1 & -1 & (-1)^2 & \cdots & (-1)^{q^m-2} \end{bmatrix},$$

where each symbol stands for the column of its coordinates with respect to a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}$. We shall say the code $\mathcal{C}$ is of Type I/II/III if it admits the matrix $H_1/H_2/H_3$ as its parity-check matrix. It follows that the dual codes $\mathcal{C}^\perp$ of Type I, II and III have H_1, H_2 and H_3 as their respective generator matrices. Then, the dual code $\mathcal{C}^\perp$ of Type I, II and III can be written in terms of the trace function as:

Type I

$$\mathcal{C}^\perp = \left\{(c_0, c_1, \cdots, c_{q^m-2}) \,|\, c_i = \mathrm{Tr}_m(a\alpha^i + bf(\alpha^i)), a, b \in \mathbb{F}_{q^m}\right\},$$

Type II

$$\mathcal{C}^\perp = \left\{(c_0, c_1, \cdots, c_{q^m-2}) \,|\, c_i = \mathrm{Tr}_m(a\alpha^i + bf(\alpha^i) + c), a, b, c \in \mathbb{F}_{q^m}\right\},$$

Type III

$$\mathcal{C}^\perp = \left\{(c_0, c_1, \cdots, c_{q^m-2}) \,|\, c_i = \mathrm{Tr}_m(a\alpha^i + bf(\alpha^i) + c(-1)^i), a, b, c \in \mathbb{F}_{q^m}\right\}.$$

In the case of $q = 2$, the linear codes $\mathcal{C}$ defined above are binary codes. Carlet, Charpin and Zinoviev in [8] intensively studied the linear code $\mathcal{C}$ of Type I for APN functions and Almost Bent functions (Almost Bent (AB) functions are functions from $\mathbb{F}_{2^m}$ to itself satisfying that for every $u, v \in \mathbb{F}_{2^n}$, $v \neq 0$, the sum $\sum_{x\in\mathbb{F}_{2^n}} (-1)^{v\cdot f(x)+u\cdot x}$ only takes value in $\{0, \pm 2^{\frac{m+1}{2}}\}$, where m is odd. It is well known that all AB functions are APN functions but the inverse is not true [7]). It was shown that $f(x)$ is APN if and only if the linear code $\mathcal{C}$ of Type I has parameters

$[2^m-1, 2^m-1-2m, 5]$ and furthermore $f(x)$ is AB if and only if the dual code $\mathcal{C}^\perp$ of Type I has nonzero weights $2^{m-1}-2^{\frac{m-1}{2}}$, 2^{n-1} and $2^{m-1}+2^{\frac{m-1}{2}}$, which implies that f is AB if and only if the linear code $\mathcal{C}$ of Type I is a *uniformly packed* code with length 2^m-1, minimum distance 5 and covering radius 3 [8].

It is worth noting that for a binary linear code $\mathcal{C}$ with length 2^m-1 and dimension 2^m-1-2m, according to the Hamming bound in (9), its minimum distance d satisfies

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{2^m-1}{i} \leq \frac{2^{2^m-1}}{2^{2^m-1-2m}} = 2^{2m}.$$

It follows that the minimum distance d is less than or equal to 6. On the other hand, the existence of a linear $[n,k,d]$ code implies the existence of a linear $[n-1,k,d-1]$ code. If the minimum distance of a $[2^m-1, 2^m-1-2m]_2$ linear code equals 6, then one deduces a $[2^m-2, 2^m-1-2m, 5]_2$ linear code. But this code does not exist [4]. Thus, the largest possible minimum distance of a binary $[2^m-1, 2^m-1-2m]$ linear code is 5. We shall say in the sequel that a linear code $\mathcal{C}$ is *optimal* if it achieves the largest possible minimum distance for given length and dimensions. In this sense, the binary linear code $\mathcal{C}$ of Type I is optimal if and only if $f(x)$ is APN. Note that the codes $\mathcal{C}$ of Types II and III are exactly the same for the binary case. It is easily seen that if f is APN, this code has parameter $[2^m-1, 2^m-2-2m, 6]$ since any codeword in $\mathcal{C}$ has even weight. The inverse is true as well. This is because the condition that $\mathcal{C}$ has no codeword of weight 4 implies that there do not exist four distinct elements $x, y, z, w \in \mathbb{F}_{2^m}$ satisfying

$$\begin{cases} x+y+z+w &= 0 \\ f(x)+f(y)+f(z)+f(w) &= 0. \end{cases}$$

This is equivalent to saying that $f(x)$ is an APN function [7]. By the Hamming bound in (9), it also follows that the linear codes $\mathcal{C}$ of Types II and III are optimal if and only if $f(x)$ is APN.

Consider the case of $q = p^h$, where p is an odd prime and h is a positive integer. For PN functions f from $\mathbb{F}_{q^m}$ to itself, Carlet, Ding and Yuan [9] in 2006 investigated the properties of the code $\mathcal{C}$ of Type I and its dual.

Theorem 3. *[9] Let $m > 1$ and $q = p^h$ with h a positive integer. Let $f(x)$ be a perfect nonlinear mapping from $\mathbb{F}_{q^m}$ to itself with $f(0) = 0$. Then the code $\mathcal{C}$*

of Type I has parameter $[q^m - 1, q^m - 1 - 2m, d_1]_q$ *with* $2 \le d_1 \le 4$ *and the dual code* $\mathcal{C}^\perp$ *has parameter* $[q^m - 1, 2m, d_1^\perp]_q$ *with* $d_1^\perp \ge \frac{q-1}{q}(q^m - q^{m/2})$. *Furthermore, in the special case that* $q = 3$, *i.e.,* $(p, h) = (3, 1)$, *if* $f(x) = f(-x)$ *for all* $x \in \mathbb{F}_{q^m}$ *and* $f(x) = 0$ *if and only if* $x = 0$, *then the code* $\mathcal{C}$ *has minimum distance* 4.

In [9], Carlet et al studied another class of linear codes $\mathcal{C}$ with parity-check matrix

Type II'

$$H_2' = \begin{bmatrix} 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2} \\ f(0) & f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^m-2}) \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

and its dual when $f(x)$ is a PN function over $\mathbb{F}_{q^m}$. The class is referred to as of Type II′ due to its close connection with the code of Type II.

Theorem 4. *[9] Let* $m > 1$ *and* $q = p^h$ *with* h *a positive integer. Let* $f(x)$ *be a perfect nonlinear mapping from* $\mathbb{F}_{q^m}$ *to itself. Then the code* $\mathcal{C}$ *of Type II′ has parameter* $[q^m, q^m - 1 - 2m, d_2']_q$ *with* $d_2' = 5$ *if* $q = 3$ *and* $3 \le d_2' \le 4$ *otherwise. The dual code* $\mathcal{C}^\perp$ *has parameter* $[q^m, 2m + 1]_q$ *with the minimums distance no less than* $\frac{q-1}{q}(q^m - q^{m/2})$.

For any mapping $f(x)$ with $f(0) = 0$, it is easy to check that if $(c_0, c_1, \cdots, c_{q^m-2})$ is a codeword of the code of Type II, then $(0, c_0, c_1, \cdots, c_{q^m-2})$ is a codeword of the code $\mathcal{C}$ of Type II′. It follows that

$$d_2' \le d_2,$$

where d_2, d_2' are the minimum distances of the codes of Type II and II′ respectively.

Similar to the proof of Theorem 7 in [9], we have the following corollary.

Corollary 1. *Let* $m > 1$ *and* $q = p^h$ *with* h *a positive integer. Let* $f(x)$ *be a perfect nonlinear mapping from* $\mathbb{F}_{q^m}$ *to itself with* $f(0) = 0$. *Then the code* $\mathcal{C}$ *of Type II has parameter* $[q^m - 1, q^m - 2 - 2m, d_2]_q$ *with* $d_2 = 5$ *if* $q = 3$ *and* $3 \le d_2 \le 4$ *otherwise.*

By examining the linear codes $\mathcal{C}$ defined from the following PN functions from $\mathbb{F}_{p^m}$ to itself (which were the only PN functions over $\mathbb{F}_{p^m}$ known until 2005),

- $f(x) = x^{p^k+1}$, where $k \geq 0$ is an integer such that $m/\gcd(m,k)$ is odd;
- $f(x) = x^{\frac{3^k+1}{2}}$, where $p = 3$, k is odd and $\gcd(m,k) = 1$;
- $f(x) = x^{10} - ux^6 - u^2x^2$, where $p = 3$ and m is odd,

the authors in [9] deduced many optimal and almost optimal codes and employed them to construct secret sharing schemes with nice access structures. The weight distributions of the dual codes $\mathcal{C}^{\perp}$ of Types I and II′ defined from the PN functions listed above were completely settled in [17, 40]. As the codes $\mathcal{C}^{\perp}$ of Type II and Type II′ are closely related, one can determine the weight distributions of the code $\mathcal{C}^{\perp}$ of Type II from the above PN functions with the same technique used in [40].

2.4 Summaries of Papers III, IV and V

Papers III, IV and V continued the study on the linear codes $\mathcal{C}$ and their duals of Types I and III defined from certain functions over $\mathbb{F}_{p^m}$.

Note that in the case when $f(x)$ are monomials over $\mathbb{F}_{q^m}$, the linear codes $\mathcal{C}$ defined in the previous subsection become cyclic codes, which have efficient encoding and decoding algorithms in storage and communication systems.

Very recently Ding and Helleseth constructed many optimal ternary cyclic codes of Type I from monomials x^e [15]. It was shown that all APN monomials and a number of other monomials over $\mathbb{F}_{3^m}$, i.e., $q = 3$, can be used to generate cyclic $[3^m - 1, 3^m - 1 - 2m]_3$ codes achieving the largest possible minimum distance 4. At the end of the paper they presented nine monomials, for which the optimality of the ternary codes constructed is confirmed from the numerical results while the theoretical proof is left open.

Summary of Paper III

Starting with attacking one of the nine open problems proposed in [15], Paper III constructed plenty of optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ and $[3^m - 1, 3^m - 2 - 2m, 5]$.

Let $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(1,e,s)}$, where $s = \frac{p^m-1}{2}$, denote the cyclic codes of Types I and III defined from monomials x^e over $\mathbb{F}_{p^m}$, respectively. In other words, $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(1,e,s)}$ are the cyclic codes over $\mathbb{F}_p$ with generator polynomials $m_1(x)m_e(x)$ and $(1+x)m(x)m_e(x)$, where $m_i(x)$ is the minimal polynomial of α^i over $\mathbb{F}_p$ for a primitive element α in $\mathbb{F}_{p^m}$. According to the Hamming bound, one is not likely to find optimal codes $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(1,e,s)}$ if $p > 3$. We are thus interested in the case where $p = 3$.

In Paper III, we are mainly concerned with the monomials x^e, where $e \not\equiv 3^i \pmod{3^m - 1}$ for any $0 \le i \le m-1$, such that the ternary cyclic codes $\mathcal{C}_{(1,e)}$ have parameter $[3^m - 1, 3^m - 1 - 2m, 4]$ and $\mathcal{C}_{(1,e,s)}$ have parameter $[3^m - 1, 3^m - 2 - 2m, 5]$.

In the first part of Paper III, we characterized the conditions for the following integers e to generate cyclic codes $\mathcal{C}_{(1,e)}$ with parameter $[3^m - 1, 3^m - 1 - 2m, 4]$:

(1) $e = r(3^{m-1} - 1)$ ($r = 2$ corresponds to Open problem 7.8 in [15]);

(2) $e = \frac{3^m-1}{2} + r$;

(3) $e = \frac{3^m-1}{2} - r$;

and presented some integers r meeting those conditions. The critical technique used is to determine the degrees of irreducible factors of the following two polynomials over $\mathbb{F}_3$:

$$f(x) = (x+1)^e + x^e + 1, \quad g(x) = (x+1)^e - x^e - 1.$$

It turned out that for each of the eight remaining open problems in [15], the cases of $h = 0, 1, 2, 3$ and $h = m-1, m-2, m-3$ can be settled as well. Nevertheless, new techniques are required for the general case.

In the second part of Paper III, we wished to find integers e such that the corresponding codes $\mathcal{C}_{(1,e,s)}$ have parameter $[3^m - 1, 3^m - 2 - 2m, 5]$, which are optimal in the sense that they achieve the maximum possible minimum distance. The constructed cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameter $[3^m - 1, 3^m - 2 - 2m, 5]$ are closely connected to PN monomials over $\mathbb{F}_{3^m}$. We in this part showed that the cyclic code $\mathcal{C}_{(1,e,s)}$ has parameter $[3^m - 1, 3^m - 2 - 2m, 5]$ if e is one of the following integers:

(1) $e = \frac{3^m-1}{2} + r$, where m is even and x^r is a PN function over $\mathbb{F}_{3^m}$;

(2) $e = 2$, where m is even;

(3) $2ed \equiv 2 \cdot 3^\tau \pmod{3^m - 1}$, where m is odd, τ is an integer with $0 \le \tau \le m-1$ and x^d is a PN function over $\mathbb{F}_{3^m}$.

It is interesting that when m is odd, the following five classes of APN exponents e [27, 59] are covered by Case (3):

(i) $e = \frac{3^{m+1}-1}{8}$ for $m \equiv 3 \pmod 4$; and $e = \frac{3^{m+1}-1}{8} + \frac{3^m-1}{2}$ for $m \equiv 1 \pmod 4$; or

(ii) $e = \frac{3^{(m+1)/2}-1}{2}$ for $m \equiv 3 \pmod 4$; and $e = \frac{3^{(m+1)/2}-1}{2} + \frac{3^m-1}{2}$ for $m \equiv 1 \pmod 4$; or

(iii) $e = \frac{3^m+1}{4} + \frac{3^m-1}{2}$; or

(iv) $e = 3^{(m+1)/2} - 1$; or

(v) $e = (3^{(m+1)/4} - 1)(3^{(m+1)/2} + 1)$ for $m \equiv 3 \pmod 4$,

because one can respectively find integers

(i) $d = 3^k + 1$ for $k = 1$; or

(ii) $d = 3^k + 1$, for $k = (m+1)/2$; or

(iii) $d = (3^k + 1)/2$ for $k = 1$; or

(iv) $d = (3^k + 1)/2$, where $k = (m+1)/2$ if $m \equiv 1 \pmod 4$, and $k = (m-1)/2$ if $m \equiv 3 \pmod 4$; or

(v) $d = (3^k + 1)/2$, where $k = (m+1)/4$ if $m \equiv 3 \pmod 8$, and $k = (3m-1)/4$ if $m \equiv 7 \pmod 8$

satisfying the conditions in Case (3).

As shown in [15], the above APN exponents can be used to generate optimal ternary cyclic codes $\mathcal{C}_{(1,e)}$ as well. The interest in further investigating the cyclic codes $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(1,e,s)}$ defined from the above APN exponents e led us to the work in Paper IV.

Summary of Paper IV

As pointed out in Subsection 2.1, the weight distribution $(A_0, A_1, \cdots, A_n)$ is an interesting research topic in coding theory [38]. It is thus of significant interest to determine the weight distribution of the optimal ternary cyclic codes $\mathcal{C}_{(1,e)}$, $\mathcal{C}_{(1,e,s)}$ and their duals constructed in [15] and Paper III. According to the MacWilliams Identities [42], the weight distribution of a linear code $\mathcal{C}$ will be settled if the weight distribution of its dual code $\mathcal{C}^\perp$ is known. Due to the close connections to certain exponential sums, we focused our attentions on the weight distributions of the cyclic codes $\mathcal{C}_{(1,e)}^\perp$ and $\mathcal{C}_{(1,e,s)}^\perp$ in Paper IV (Paper IV used notation $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(1,e,s)}$ to denote the corresponding cyclic codes instead. Please see the explanation at the bottom of this page[1]). For consistency of notation, we shall adhere to the foregoing convention for the remainder of this section.

Paper IV studied the weight distributions of cyclic codes $\mathcal{C}_{(1,e)}^{\perp}$ and $\mathcal{C}_{(1,e,s)}^{\perp}$ for several classes of integers e, which covers the five APN exponents aforementioned as special cases. At the beginning of Paper IV, we presented a number of classes of three-weight cyclic codes over $\mathbb{F}_p$ via examining the condition for the cyclic codes $\mathcal{C}_{(1,d)}^{\perp}$ and $\mathcal{C}_{(1,e)}^{\perp}$ to have the same weight distribution.

Theorem 5. *Let $m \geq 3$ be odd. (i) Let $p \equiv 3 \pmod 4$. If e is an even integer satisfying $2(p^k+1)e \equiv 2 \pmod{p^m-1}$ for some nonnegative integer k, then $\mathcal{C}_{(1,e)}^{\perp}$ is a $[p^m-1, 2m]$ cyclic code with the weight distribution in Table 1. (ii) Let p be any odd prime. If e is an integer satisfying $(p^k+1)e \equiv 2 \pmod{p^m-1}$ for some positive integer k with $\gcd(m,k)=s$, then $\mathcal{C}_{(1,e)}^{\perp}$ is a $[p^m-1, 2m]$ cyclic code with the weight distribution of*

- *Table 2 when $e \equiv 1+(p-1)/2 \pmod{p-1}$; and*
- *Table 3 when $e \equiv 1 \pmod{p-1}$.*

Using Theorem 5, the weight distributions of the cyclic codes $\mathcal{C}_{(1,e)}^{\perp}$ for the five classes of APN exponents listed in the previous subsection can be determined. Then the weight distributions of the cyclic codes $\mathcal{C}_{(1,e)}$ are then settled via the MacWilliams identities [42].

Apart from Theorem 5, Paper IV studied the value distributions of the following two exponential sums:

$$T(a,b) = \sum_{x \in \mathbb{F}_{p^m}} \omega^{\mathrm{Tr}(ax+bx^e)} \tag{10}$$

[1] Let $m_i(x)$ be the minimal polynomial over $\mathbb{F}_p$ of α^i for a primitive element α in $\mathbb{F}_{p^m}$. In some of the literature, the notation $\mathcal{C}_{(1,e)}$ was used to denote the cyclic code with generator polynomial $m_1(x)m_e(x)$ (*Convention 1*) whilst, elsewhere, the notation $\mathcal{C}_{(1,e)}$ was used to denote the cyclic code with parity-check polynomial $m_{-1}(x)m_{-e}(x)$ (*Convention 2*). In Paper III, we adopted Convention 1 that $\mathcal{C}_{(1,e)}$, $\mathcal{C}_{(1,e,s)}$ denotes the cyclic codes with generator polynomials $m_1(x)m_e(x)$ and $(1+x)m_1(x)m_e(x)$, whilst in Paper IV, we adopted Convention 2 that $\mathcal{C}_{(1,e)}$, $\mathcal{C}_{(1,e,s)}$ denotes the cyclic codes with parity-check polynomial $h(x) = m_{-1}(x)m_{-e}(x)$ and $h(x) = (1+x)m_{-1}(x)m_{-e}(x)$. The reason for doing this is that Paper III studied the minimum distances of cyclic codes $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(1,e,s)}$ and Paper IV focused on the weight distributions of their duals separately.

Table 1: *Weight distribution I*

Hamming weight	Multiplicity
0	1
$(p-1)p^{m-1}-p^{\frac{m-1}{2}}$	$\frac{1}{2}(p-1)(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})$
$(p-1)p^{m-1}+p^{\frac{m-1}{2}}$	$\frac{1}{2}(p-1)(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})$
$(p-1)p^{m-1}$	$(p^m-1)(p^{m-1}+1)$

Table 2: *Weight distribution II*

Hamming weight	Multiplicity
0	1
$(p-1)p^{m-1}-\frac{(p-1)}{2}p^{\frac{m+s-2}{2}}$	$(p^m-1)(p^{m-s}+p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}+\frac{(p-1)}{2}p^{\frac{m+s-2}{2}}$	$(p^m-1)(p^{m-s}-p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}$	$(p^m-1)(p^m-2p^{m-s}+1)$

and

$$S(a,b,c)=\sum_{x\in\mathbb{F}_{p^m}}\omega^{\mathrm{Tr}(ax+bx^e+cx^s)}, \tag{11}$$

where $p\equiv 3 \pmod 4$, e is an integer satisfying $(p^k+1)e\equiv 2p^\tau \pmod{p^m-1}$ for some integer $\tau\in\mathbb{Z}_m$ and positive integer k with $\gcd(m,k)=1$ and $s=(p^m-1)/2$. These two exponential sums are closely related to the exponential sum

$$T_0(a,b)=\sum_{x\in\mathbb{F}_{p^m}}\omega^{\mathrm{Tr}(ax^{p^k+1}+bx^2)}.$$

By settling the distribution of $(T_0(a,b),T_0(-a,b))$ when (a,b) runs through $\mathbb{F}_{p^m}^2$, Paper IV derived the value distributions of $T(a,b)$ and $S(a,b,c)$. The value distribution of $S(a,b,c)$ was later utilized to settle the weight distributions of the cyclic codes $\mathcal{C}_{(1,e,s)}^{\perp}$. For the special case when $p=3$, the weight distributions of the cyclic codes $\mathcal{C}_{(1,e,s)}^{\perp}$ for the last three classes of APN exponents were thus determined.

Summary of Paper V

As introduced in Subsection 2.1, a code $\mathcal{C}$ over $\mathbb{F}_q$ of length n is called a perfect code if its covering radius equals its packing radius, i.e.,

Table 3: *Weight distribution III*

Hamming weight	Multiplicity
0	1
$(p-1)p^{m-1}-(p-1)p^{\frac{m+s-2}{2}}$	$\frac{1}{2}(p^m-1)(p^{m-s}+p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}+(p-1)p^{\frac{m+s-2}{2}}$	$\frac{1}{2}(p^m-1)(p^{m-s}-p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}$	$(p^m-1)(p^m-p^{m-s}+1)$

$\rho = \lfloor (d-1)/2 \rfloor$. The parameters of perfect codes have been completely classified [55, 60]. The next interesting case is when the covering radius exceeds the packing radius by one. Codes satisfying this condition are termed quasi-perfect (QP) codes. Quasi-perfect codes have been extensively studied, but classification of putative sets of parameters for quasi-perfect codes seems to be much more complicated than that for the perfect codes.

Let p be a prime and m be a positive integer. Let f be a mapping from $\mathbb{F}_{p^m}$ to itself with $f(0)=0$. Recall that the linear codes $\mathcal{C}$ of Type I defined in Subsection 2.3 admit the matrix

$$H_1 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^m-2}) \end{bmatrix}$$

as their parity-check matrix, where α is a primitive element of $\mathbb{F}_{p^m}$ and each symbol stands for the column of its coordinate with respect to a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^m}$.

Paper V studied the covering radius of the linear code $\mathcal{C}$ of Type I for certain functions $f(x)$. For the binary case, we proved that the code $\mathcal{C}$ is a quasi-perfect code with parameter $[2^m-1, 2^m-1-2m, 5]$ for any quadratic APN function

$$f(x) = \sum_{i,j=0}^{m-1} a_{i,j} x^{2^i+2^j},\ a_{i,j} \in \mathbb{F}_{2^m},$$

where $m \geq 3$. In the case when p is odd, we investigated the covering radius of the code $\mathcal{C}$ for certain monomials $f(x) = x^e$. It was shown that for odd $m \geq 3$ and arbitrary odd prime p, the code $\mathcal{C}_f$ is quasi-perfect if x^e is a PN monomial over $\mathbb{F}_{p^m}$ with $(e-1)^4 \leq p^m - 1$. In addition, it is also proved that for odd m and $p \equiv 3 \pmod 4$, the code $\mathcal{C}_f$ is quasi-perfect if e is the even solution to $2de \equiv 2 \pmod{p^m-1}$, where x^d is a PN monomial over $\mathbb{F}_{p^m}$ with $(d-1)^4 \leq p^m - 1$. As a consequence, for odd $m \geq 3$ and odd prime p, we derive an abundance of p-ary quasi-perfect linear codes of length $p^m - 1$ and dimension $p^m - 1 - 2m$.

References

[1] J. Adamek. *Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory*. Wiley, 2011.

[2] K. Arasu, J. Dillon, and K. Player. Character sum factorizations yield perfect sequences. *Preprint*, 2010.

[3] K. T. Arasu. Sequences and arrays with desirable correlation properties. *Information Security, Coding Theory and Related Combinatorics*, pages 136 – 171, 2011.

[4] A. Brouwer and L. Tolhuizen. A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters. *Designs, Codes and Cryptography*, 3(2):95–98, 1993.

[5] L. Budaghyan. *Construction and Analysis of Cryptographic Functions*. Habilitation Thesis, University of Paris 8, Paris, France, 2013.

[6] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. *IEEE Transaction on Information Theory*, 46(1):4–8, 2000.

[7] C. Carlet. *"Vectorial Boolean Functions for Cryptography", in: Crama Y. and Hammer P.L. ed., Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.

[8] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[9] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102, 2005.

[10] S. T. Choi and J. S. No. On the cross-correlation distributions of p-ary m-sequences and their decimated sequences. *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences*, 95(11):1808–1818, 2012.

[11] T. W. Cusick and H. Dobbertin. Some new three-valued cross-correlation functions for binary m-sequences. *IEEE Transaction on Information Theory*, 42(4):1238–1240, 1996.

[12] P. Dembowski and T. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103(3):239–258, 1968.

[13] J. Dillon. New p-ary perfect sequences and difference sets with Singer parameters. In T. Helleseth, P. Kumar, and K. Yang, editors, *Sequences and their Applications*, Discrete Mathematics and Theoretical Computer Science, pages 23–33. Springer London, 2002.

[14] J. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3):342 – 389, 2004.

[15] C. Ding and T. Helleseth. Optimal ternary cyclic codes from monomials. *IEEE Transactions on Information Theory*, 59(9):5898–5904, 2013.

[16] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen. Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Transactions on Information Theory*, 47(4):1473–1481, 2001.

[17] K. Feng and J. Luo. Value distributions of exponential sums from perfect nonlinear functions and their applications. *IEEE Transaction on Information Theory*, 53(9):3035–3041, 2007.

[18] R. Gold. Maximal recursive sequences with three-valued recursive cross-correlation functions. *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[19] S. Golomb. *Shift Register Sequences*. Aegean Park Press, 1982.

[20] S. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[21] G. Gong, T. Helleseth, and H. G. Hu. A three-valued Walsh transform from decimations of Helleseth-Gong sequences. *IEEE Transactions on Information Theory*, 58(2):1158–1162, 2012.

[22] B. Gordon, W. H. Mills, and L. R. Welch. Some new difference sets. *Canadian Journal of Mathematics*, 14(4):614 – 625, 1962.

[23] T. Helleseth. Some results about cross-correlation function between two maximal linear sequences. *Discrete Mathematics*, 16(3):209–232, 1976.

[24] T. Helleseth and G. Gong. New nonbinary sequences with ideal two-level autocorrelation. *IEEE Transactions on Information Theory*, 48(11):2868–2872, 2002.

[25] T. Helleseth and P. V. Kumar. *"Pseudonoise Sequences", in: Gibson J., ed., The Mobile Communications Handbook, The electrical engineering handbook series*. A CRC handbook. Springer, 1999.

[26] T. Helleseth and P. Rosendahl. New pairs of m-sequences with 4-level cross-correlation. *Finite Fields and Their Applications*, 11(4): 674–683, 2005.

[27] T. Helleseth, C. Rong, and D. Sandberg. New families of almost perfect nonlinear power mappings. *IEEE Transaction on Information Theory*, 45(2):475–485, 1999.

[28] T. Helleseth, P. V. Kumar, and H. Martinsen. A new family of ternary sequences with ideal two-level autocorrelation function. *Designs Codes and Cryptography*, 23(2):157–166, 2001.

[29] T. Hellesth and P. V. Kumar. *"Sequences with Low Correlation", in: Pless, V. and Huffman, W.C., eds., Handbook in Coding Theory*. Handbook of Coding Theory. Elsevier, 1998.

[30] D. Hertel. Crosscorrelation between GMW and Dillon-Dobbertin sequences. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 89(9):2264–2267, 2006.

[31] H. D. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *Finite Fields and Their Applications*, 7(2):253–286, 2001.

[32] H. Hu, S. Shao, G. Gong, and T. Helleseth. The proof of Lin's conjecture via the decimation-Hadamard transform. *Preprint: http://arxiv.org/pdf/1307.0885v1.pdf*, 2013.

[33] W. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[34] J. W. Jang, Y. S. Kim, J. S. No, and T. Helleseth. New family of p-ary sequences with optimal correlation property and large linear span. *IEEE Transactions on Information Theory*, 50(8):1839–1844, 2004.

[35] A. Johansen and T. Helleseth. A family of m-sequences with five-valued cross correlation. *IEEE Transactions on Information Theory*, 55(2):880–887, 2009.

[36] A. Johansen, T. Helleseth, and A. Kholosha. Further results on m-sequences with five-valued cross correlation. *IEEE Transactions on Information Theory*, 55(12):5792–5802, 2009.

[37] T. 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.

[38] T. Kløve. *Codes for Error Detection*. Series on coding theory and cryptology. World Scientific, 2007.

[39] P. Kumar, R. Scholtz, and L. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*, 40(1): 90 – 107, 1985.

[40] C. Li, L. Qu, and S. Ling. On the covering structures of two classes of linear codes from perfect nonlinear functions. *IEEE Transaction on Information Theory*, 55(1):70–82, 2009.

[41] H. A. Lin. *From Hadamard differences sets to perfectly balanced sequences*. Ph.D. dissertation, University of Southern California, Los Angeles, USA, 1998.

[42] F. MacWilliams and N. Sloane. *The Theory of Error-correcting Codes*. North-Holland Mathematical Library. North-Holland Publishing Company, 1977.

[43] A. Maschietti. Difference sets and hyperovals. *Designs, Codes and Cryptography*, 14(1):89–98, 1998.

[44] J. L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

[45] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[46] Y. Niho. *Multi-valued cross-correlation functions between two maximal linear recursive sequences*. Ph.D. dissertation, University of Southern

California, Los Angeles, USA, 1972.

[47] J. S. No. New cyclic difference sets with Singer parameters constructed from d-homogeneous functions. *Designs, Codes and Cryptography*, 33(3):199–213, 2004.

[48] J. S. No, H. Chung, and M. S. Yun. Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$. *IEEE Transaction on Information Theory*, 44(3):1278–1282, 1998.

[49] J. S. No, S. Golomb, G. Gong, H. K. Lee, and P. Gaal. Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation. *IEEE Transaction on Information Theory*, 44(2):814–817, 1998.

[50] K. Nyberg. Perfect nonlinear s-boxes. In D. Davies, editor, *Advances in Cryptology - EUROCRYPT'91*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer Berlin Heidelberg, 1991.

[51] K. Nyberg. Differentially uniform mappings for cryptography. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer Berlin Heidelberg, 1994.

[52] O. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20(3):300 – 305, 1976.

[53] C. E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.

[54] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377 – 385, 1938.

[55] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM Journal on Applied Mathematics*, 24(1):88–96, 1973.

[56] H. M. Trachtenberg. *On the cross-correlation functions of maximal linear recurring sequences*. Ph.D. dissertation, University of Southern California, Los Angeles, USA, 1970.

[57] J. Van Lint. A survey of perfect codes. *Journal of Mathematics*, 5(2), 1975.

[58] N. Yu and G. Gong. Crosscorrelation properties of binary sequences with ideal two-level autocorrelation. In G. Gong, T. Helle-

seth, H. Y. Song, and K. Yang, editors, *Sequences and Their Applications - SETA 2006*, volume 4086 of *Lecture Notes in Computer Science*, pages 104–118. Springer Berlin Heidelberg, 2006.

[59] Z. Zha and X. Wang. Almost perfect nonlinear power functions in odd characteristic. *IEEE Transaction on Information Theory*, 57(7): 4826–4832, 2011.

[60] V. Zinoviev and V. Leontiev. The nonexistence of perfect codes over Galois fields. *Probl. Control and Inform. Theory*, 2(2), 1973.