Sufficiently overdetermined random polynomial systems behave like semiregular ones

Andrea Tenti

Thesis for the degree of Philosophiae Doctor (PhD)
University of Bergen, Norway
2019

UNIVERSITY OF BERGEN

Sufficiently overdetermined random polynomial systems behave like semiregular ones

Andrea Tenti

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

Date of defense: 18.12.2019

Year: 2019

Title: Sufficiently overdetermined random polynomial systems behave like semiregular ones

Name: Andrea Tenti

Print: Skipnes Kommunikasjon / University of Bergen

Acknowledgements

First of all, I want to thank my supervisor, Igor Semaev for his help and support during the whole project. His insightful ideas, suggestions, and feedback, made my Ph.D. experience productive and stimulating.

I would like to thank my co-supervisor Tor Helleseth for his support and encouragement and Lilya Budaghyan for her sensible leadership of Selmer Center.

My sincere thanks go to my colleagues Isaac, Alessandro, and Morten, with whom I first shared ideas and whose feedback has been incredibly beneficial for writing this thesis.

I heartily thank my colleagues at Selmer centre: Sachin, Wrya, Nikolay, Diana, Bo, Navid, Irene, Dan, and Marco. They created a positive and stimulating environment that, more than anything, made Bergen feel as home.

I am grateful to Mirjam, Erlend, Eugenia, Emanuele, Daniel, Jacopo, Tiziano, Denis, and Daniel for the quality time they shared with me during the past three years.

I thank my parents and my family, who helped me becoming the person I am today and never lessen their support despite the distance.

Finally, my greatest thanks go to Francesca, for reasons so deep that I have no suitable words to fully describe.

Abstract

Solving systems of polynomial equations over finite fields is a fundamental problem in several areas of pure and applied mathematics. Gröbner basis methods is a family of techniques to computationally solve such systems but their complexity is poorly understood. A key parameter to estimate the complexity is the degree of regularity, that is known to be easy to compute only for a family of systems, called semiregular systems. It is not known a way to establish a priori if a system is semiregular, but it is conjectured that (under certain restrictions) a random system is semiregular with probability tending to 1.

In this thesis we show that with probability tending to 1 a sufficiently overdetermined system with leading forms taken uniformly and independently at random has degree of regularity the smallest possible, as if it were semiregular. Using previously established results, this implies that sufficiently overdetermined systems of polynomial equations are solvable in polynomial time with high probability.

The definition of degree of regularity was introduced in 2003 by Bardet, Faugère, and Salvy for sequences of polynomials in a multivariate polynomial ring modulo a homogeneous ideal. We extend the definition to sequences defined over a multivariate polynomial ring modulo any ideal and use this language to improve upon the known upper bounds for the complexity of computing a Gröbner basis of an ideal in the case of sufficiently overdetermined systems.

We present an algorithm for computing one of the zeros of an ideal, if a Gröbner basis satisfying some properties is provided. The time complexity of this algorithm depends on the degree of regularity and it is negligible com-

pared to the cost of constructing a Gröbner basis in the first place.

Lastly, we describe a reduction to an optimisation problem of the hard mathematical problem at the base of the security assumption of the AJPS cryptosystem, one of the candidates to the first round of the NIST Post-Quantum Cryptography Standardization Process.

Contents

Chapter 1

Introduction

Systems of multivariate polynomial equations over fields are among the most fundamental subjects in algebraic geometry and commutative algebra. An efficient computation of the solution is also crucial in applied sciences.

Finding such solutions is easy if the system is linear (i.e. all the polynomials have degree 1). On the other hand the complexity already spikes for quadratic polynomials over $\mathbb{F}_2$ (finite field with two elements): determining whether the system has solutions is an **NP**-complete problem [FY79].

Especially starting from the twentieth century, different methods were developed to find solutions to polynomial equation systems. One of the major contributions in this direction was given by Buchberger in his Ph.D. thesis [Buc65], where he introduced the concept of Gröbner basis of a polynomial ideal together with an algorithm to compute one of them from a set of generators. This is known as the Buchberger algorithm. A Gröbner basis for an ideal I is a set of generators, that facilitates finding representatives for the polynomials modulo I.

Gröbner bases were defined mostly for the need of performing computations in quotient algebras $K[x_1,\dots,x_n]/(P)$, where K is a field and $P = \{P_1,\dots,P_m\} \subseteq K[x_1,\dots,x_n]$. Eventually, they turned out to be a powerful tool for answering many questions about ideals such as the membership problem, the implicitization problem, the problem of deciding if two sets of polynomials generate the same ideal, and the problem of solving systems of polynomial

equations.

Over time, alternatives to the Buchberger algorithm were developed (for example linear algebra based [Laz83], Hilbert-driven [Tra96], F4 [Fau99], and F5 [Fau02]) for computing Gröbner bases, but their complexity still remains unclear. The time complexity is characterised by the highest degree of any polynomial appearing during the algorithm, called the solving degree. For general fields, known worst case scenario lower bounds for the solving degree are doubly exponential in n (see e.g. [Huy86]). Under some specific hypotheses that are common in applications, it is possible to find upper bounds on the solving degree that are linear in the number of variables and the degree of the initial polynomials [CG17]. This still implies that the complexity of finding a Gröbner basis is at most exponential in the number of variables.

In [BFS03], Bardet, Faugère and Salvy introduced the term "degree of regularity" (denoted by d_{reg}) for a family of polynomials $P_1, \ldots, P_m \in \mathbb{F}_2[x_1, \ldots, x_n]$, a parameter that provides an upper bound on the complexity of finding a Gröbner basis for homogeneous ideals. The degree of regularity is the smallest degree for which the Hilbert series of a particular graded algebra has non positive coefficient. Computing such Hilbert series is generally hard. However, for a certain family of generators, called semiregular sequences in [BFS03], there is a explicit formula for the Hilbert series that depends only on the number of variables, the number of generators, and their degrees.

It is natural to generalise the definition of degree of regularity to a family of polynomials $P_1, \ldots, P_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ as follows. Let $f_1, \ldots, f_m$ be the leading forms of $P_1, \ldots, P_m$ and let $I \subseteq R^h = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ be the ideal generated by $f_1, \ldots, f_m$. By I_d we denote the $\mathbb{F}_q$-vector space containing all the homogeneous polynomials of degree d in I. The degree of regularity of $P_1, \ldots, P_m$ is the smallest degree d for which $\dim(I_d)$ is equal to the number of monomials in R^h of total degree d. It corresponds to the smallest degree for which the Hilbert series of R^h/I vanishes.

It is not known if there is an efficient way to establish whether a set of generators is a semiregular sequence. Nonetheless, in was conjectured in [BFS03]

that a random sequence is semiregular with probability tending to 1. This conjecture, as formulated, was disproved in [HMS17] and reformulated in a more precise and restrictive way that is still believed to hold: a significant portion of algebraic cryptanalysis is performed under this assumption (see e.g. [CFMR+17] and [ACFP14]).

In some cases, it is possible to extract the solutions of a system directly from one of its Gröbner bases. Let us consider the system of polynomial equations in n variables with coefficients in the algebraically closed field K

$$P_1(x_1,\dots,x_n) = 0,\dots,P_m(x_1,\dots,x_n) = 0. \tag{1.1}$$

Let G be a Gröbner basis for the ideal $I = (P_1,\dots,P_m)$. The system 1.1 has no solutions in K^n if and only if $1 \in G$. Let I be radical. The system 1.1 has exactly one solution in K^n if and only if G contains linear polynomials $l_1,\dots,l_n$, with the leading monomial of l_i being x_i for every i (this is a trivial consequence of the definition of Gröbner bases [Buc65] and Hilbert's Nullstellensatz [AM69]).

If a system admits more than one solution, it is possible to find them using an algorithm described in [KR00]: one applies linear transformations to the ideal until it is in x_n-normal position. This property means that if $(a_1,\dots,a_n)$ and $(b_1,\dots,b_n)$ are distinct solutions, then $a_n \neq b_n$. It can be efficiently verified by using a Gröbner basis for the ideal according to the lexicographic ordering.

Gröbner basis methods are not the only strategies for finding solutions to multivariate systems over finite fields: other approaches include eXtended Linearization [CKPS00], SAT solvers [BCJ07], and Agreeing-Gluing methods [RS06].

The problem of solving non-linear systems of polynomial equations has been of great interest in cryptography and cryptanalysis. The security of some digital signature schemes is based on this very problem: for instance, Unbalanced Oil and Vinegar [KPG99] and HFE- [Pat96].

On the other hand in cryptanalysis, algebraic attacks try to break a cipher by finding zeros of a polynomial system. It is possible to reduce some of the hard mathematical problems in cryptology to solving systems of polynomial

equations (such as for AES [CP02] or ECC [Sem15]). A particularly successful attack using a Gröbner basis method was performed on Hidden Field Equations (HFE) in [FJ03]. The authors showed that the largest degree that appears in the computations of a Gröbner basis for the systems generated by HFE remains constant as the problem scales.

Solving large systems of multivariate polynomial equations using quantum methods still appears to be difficult. Hence several cryptosystems based on the hardness of solving such systems were submitted to the NIST Post-Quantum Cryptography Standardization Process (https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization). Four of them are candidates to the second round for digital signatures: G*e*MSS [CFMR$^+$17], LUOV [BSVP17], MQDSS [CHR$^+$18], and Rainbow [DS05].

The candidates submitted for the NIST PQC Standardization Process can be grouped in families. Another such family is NTRU-like cryposystems. They are based on NTRU, designed in [HPS98] which uses lattice-based cryptography for encryption and decryption. One of the proposals in this family that was accepted for the first round of the competition (but does not appear in the second round) is the AJPS cryptosystem, first introduced in [AJPS17], and then refined in [AJPS18] after a successful attack in [BCGN17]. The hard mathematical problem behind the AJPS cryptosystem is the Mersenne Low Hamming Combination Search Problem (MLHCombSP): let $q = 2^N - 1$ be a Mersenne prime and let $F, G \in \mathbb{Z}_q$ whose binary representation has Hamming weight h. Given $R, T \in \mathbb{Z}_q$ such that $RF + G = T$, find F and G.

The main cryptanalysis of the first version of the AJPS cryptosystem is done in [BCGN17] where the authors describe a lattice attack and a family of weak keys, and then in [dBDJdW18], where the complexity of the lattice attack is analysed and a Meet-in-the-Middle attack is proposed.

1.1 Contributions

The main result of this thesis is a probabilistic analysis on the degree of regularity for sufficiently overdetermined systems of polynomials. Let $l_q(n,\delta)$ be the number of monomials of degree δ in $\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^q,\ldots,x_n^q)$. We prove the following:

Theorem 1.1. *Let q and D be fixed and let $f_1,\ldots,f_m \in \mathbb{F}_q[x_1,\ldots,x_n]/(x_1^q,\ldots,x_n^q)$ be homogeneous polynomials of degree D with coefficients taken independently and uniformly at random from $\mathbb{F}_q$. If there exists $d < D$ such that*

$$m \geq \frac{l_q(n,d+D)}{l_q(n,d)},$$

then

$$\mathbb{P}(d_{reg} \leq d+D) \geq 1 - q^{l_q(n,d+D)-ml_q(n,d)} + O(n^d q^{-Cn^D})$$

for a positive constant C as $n \to \infty$.

This result complies with the degree of regularity computed in [BFS03] for semiregular sequences, but it does not use semiregularity as hypothesis. A particular case of this theorem was first proved in [Sem16] for $q = D = 2$ and $d = 1$. Our generalisation was facilitated by using the language of multisets and a deeper analysis of the function in $O(n^d q^{-Cn^D})$.

Theorem 1.1 has the following important consequence. Let $P_1,\ldots,P_m$ be a sequence of not necessarily homogeneous polynomials in $\mathbb{F}_q[x_1,\ldots,x_n]$ of degree D with leading forms taken uniformly and independently at random and with $m \geq \frac{l_q(n,d+D)}{l_q(n,d)}$. Then one can compute a total degree Gröbner basis for the ideal

$$I = (P_1,\ldots,P_m,x_1^q - x_1,\ldots,x_n^q - x_n)$$

in polynomial time (in n and m) with probability tending to 1. As a consequence, one can determine if

$$P_1 = 0,\ldots,P_m = 0$$

admits $\mathbb{F}_q$-rational solutions and compute one of them (if they exist) in polynomial time (in n and m) with probability tending to 1.

As an example, by applying the theorem for $q = 2$, $D = 2$, and $d = 1$, it follows that a sequence of $m \geq \frac{(n-1)(n-2)}{6} + 1$ quadratic polynomials has degree of regularity ≤ 3 with probability tending to 1. Similarly, for $q = 2$, $D = 3$, and $d = 2$, one needs $m \geq \frac{(n-2)(n-3)(n-4)}{60} + 1$ cubic polynomials with random leading forms to have degree of regularity ≤ 5 with probability tending to 1. Therefore, with these parameters, one can solve systems with random leading forms in polynomial time (in n and m) with probability tending to 1.

We extend the definition of the degree of regularity to families of polynomials $F = \{f_1, \ldots, f_m\}$ in the quotient algebras $K[x_1, \ldots, x_n]/I$ where I is a not necessarily a homogeneous ideal. The degree of regularity in this setting does not exist for every ideal. This definition still satisfies the property of being the smallest degree for which a Hilbert series vanishes. Moreover the degree of regularity depends only on the leading forms of the family F. In particular, we prove that

Theorem 1.2. *If $\{f_1, \ldots, f_m, g_1, \ldots, g_t\} \subseteq K[x_1, \ldots, x_n]$ admits a degree of regularity d_{reg}, then $\{f_1 + I, \ldots, f_m + I\} \subseteq K[x_1, \ldots, x_n]/I$ also admits a degree of regularity d'_{reg} and $d'_{reg} \leq d_{reg}$, where $I = (g_1, \ldots, g_t)$.*

An upper bound for the complexity of constructing a Gröbner basis that depends on the degree of regularity was proved in [ST19a]. For example, over $\mathbb{F}_2$ for a sequence with $d_{\text{reg}} = 3$, the upper bound is in $O(n^{14})$. Using the language of quotient algebras, we improve upon this method to obtain a better upper bound. In the example considered, the upper bound found is in $O(n^9)$.

When using the algorithm described in [KR00] to find the set of zeros of an ideal, depending on the size of this set, it might be necessary to work with coefficients in an extension of the base field. Moreover, one might need to try several linear transformations before finding one that puts the ideal in x_n-normal position. We suggest a different approach that finds only one of the zeros (if they exist) with time complexity that depends on the degree of regularity and whose complexity is negligible compared to the cost of computing a Gröbner

basis in the first place:

Theorem 1.3. *Let G be a Gröbner basis for an ideal I according to a total degree ordering and an integer d such that*

- *$deg(g) \leq d$ for every $g \in G$,*
- *every monomial of degree $\geq d$ in $\mathbb{F}_q[x_1, \ldots, x_n]$ is divisible by the leading monomial of some $g \in G$.*

Then one can prove $Z(I) = \emptyset$ or compute $(a_1, \ldots, a_n) \in Z(I)$ in $O(nL_q(n,d)^3)$, where $L_q(n,\delta) = \sum_{i=0}^{\delta} l_q(n,i)$.

A Gröbner basis constructed with the method described in [ST19a] satisfies the properties of the previous theorem for $d = d_{\text{reg}}$.

Lastly, we present the reduction described in [BT19] of the MLHCombSP to an Integer Linear Programming problem. In [BCGN17], it was found that for the parameters suggested in the first version of the AJPS cryptosystem, one key every $\sim 2^{34}$ is weak. Using this reduction we extend the family of weak keys and show for those same parameters that one key is weak with probability $\sim 2^{-11}$ in the sense that they can be recovered by solving an Integer Linear Programming of dimension 3.

Theorem 1.1 and Theorem 1.3 have been presented as part of an extended abstract at the Eleventh International Workshop on Coding and Cryptography [ST19b] and as a poster at SIAM Conference on Applied Algebraic Geometry 2019. A full paper containing these results has been submitted to a journal and is currently available on the Cryptology ePrint Archive [ST19a]. The reduction of the MLHCombSP to Integer Linear Programming problem was presented at AFRICACRYPT 2019 [BT19], and most of the results in the thesis were reported in internal seminars at the Department of Informatics of the University of Bergen.

1.2 Outline

In Chapter 2, we introduce the notation and present the well-known results that will be used throughout the thesis.

Chapter 3 contains the definition and the properties of the Gröbner basis of an ideal. The concept of the degree of regularity is introduced for ideals in $K[x_1,\ldots,x_n]$. The definition is then extended to quotient algebras $K[x_1,\ldots,x_n]/I$, and some conditions for the existence of the degree of regularity are proved (such as Theorem 1.2). In the last section of the chapter, we describe the method from [ST19a] for computing a Gröbner basis with an algorithm that uses the degree of regularity as main parameter for an upper bound on its complexity. We also describe how to find one of the zeros of the ideal (if they exist) from a Gröbner basis with negligible time complexity compared to computing the Gröbner basis in the first place.

The core result of the thesis is proved in Chapter 4, where we show that the degree of regularity of a sufficiently overdetermined system of equations, whose leading forms are randomly chosen, is the smallest possible with probability tending to 1. The first section contains the proof from [Sem16] for the case for $q = D = 2$, $d = 1$, while in the second section, we generalise this result to Theorem 1.1. We also present a hybrid method, that employs guessing some of the variables if the number of equations is not large enough for the main theorem to apply. Lastly we show how for overdetermined systems it is possible to improve upon the complexity given in [ST19a] to compute a Gröbner basis, by considering also the forms of lower degree.

Chapter 5 contains a reduction of the Mersenne Low Hamming Combination Search Problem to an Integer Linear Programming problem, and describes how this extends the family of weak keys of the AJPS cryptosystem.

Chapter 2

Mathematical tools

In this chapter we present the mathematical tools and the basic results used throughout the thesis. All the results here stated are well known. The main sources are: [AM69, Har77] for commutative algebra, [Rom05] for linear algebra, [CB02] for combinatorics, [And02] for theory of multisets, and [AB09] for complexity theory.

2.1 Commutative algebra

Definition 2.1. Let R be a commutative ring. An *ideal* I of R is a subset of R satisfying the following conditions.

- If $a, b \in I$, then $a + b \in I$,
- If $a \in I$ and $x \in R$, then $ax \in I$.

Definition 2.2. Let $I \subseteq R$ be an ideal. The *quotient ring* $R/I = \{a + I | a \in R\}$ is defined as the ring with sum given by $(a + I) + (b + I) = (a + b) + I$ and product given by $(a + I)(b + I) = ab + I$. An ideal I is called *maximal* if R/I is a field.

Definition 2.3. Let G be a subset of an ideal $I \subseteq R$. The subset $G \subseteq I$ is said to be a *basis* for I if for every $f \in I$, $f = \sum_{i=1}^{t} x_i g_i$ for $x_i \in R$, $g_i \in G$, $t \in \mathbb{N}$. Notation-wise, it is said that I is *generated* by G or that $I = (G)$. The ring R is called *Noetherian* if every ideal of R admits a finite basis.

Proposition 2.4 (Ascending Chain Condition, [AM69])**.** *Let R be a Noetherian ring and let $I_1,\dots,I_n,\dots$ be ideals of R such that $I_j \subseteq I_{j+1}$ for every j. Then there exists k such that $I_k = I_{k+1} = I_{k+2} = \dots$.*

Let R be a ring. The *polynomial ring* $R[x]$ is the set of formal sums of the form $f = a_0 + a_1 x + \dots + a_n x^n$ for some n with $a_i \in R$. The (multivariate) polynomial ring $R[x_1,\dots,x_n]$ is defined recursively as $R[x_1,\dots,x_j] = (R[x_1,\dots,x_{j-1}])[x_j]$.

Let K be a field and let us consider the polynomial ring $R = K[x_1,\dots,x_n]$. The affine n-space over K is the set $K^n = \{(a_1,\dots,a_n) | a_i \in K\}$. It is possible to interpret the elements of R as functions from K^n to K, as $f : (a_1,\dots,a_n) \mapsto f(a_1,\dots,a_n)$.

Definition 2.5. Let $S \subseteq R$ be a set of polynomials. The *set of zeros* of S is the set $Z(S) = \{P \in K^n | f(P) = 0 \text{ for every } f \in S\}$.

Proposition 2.6. *Let G be a basis for the ideal $I \subseteq R$. Then $Z(G) = Z(I)$.*

Proof. Since $I \supseteq G$, then clearly $Z(I) \subseteq Z(G)$. Let $P \in Z(G)$ and assume by contradiction that there exists $f \in I$ for which $f(P) \neq 0$. By the fact that G is a basis for I, there exist $p_1,\dots p_m \in R$, $g_1,\dots,g_m \in G$ for which $f = \sum_{i=1}^m p_i g_i$. By the properties of the evaluation operation, one concludes that $f(P) = \sum_{i=1}^n p_i(P) g_i(P) = 0$, since $P \in Z(G)$. ∎

Corollary 2.7. *Let*

$$\begin{cases} P_1(x_1,\dots,x_n) = 0, \\ \vdots \\ P_m(x_1,\dots,x_n) = 0. \end{cases} \tag{2.1}$$

be a system of polynomial equations in n variables over the field K. The set of solutions S is equal to the set of zeros of the ideal $I = (P_1,\dots,P_m) \in K[x_1,\dots,x_n]$.

Corollary 2.7 indicates that, when looking for the solutions of a system of polynomial equations as (2.1), it is possible to solve an equivalent system, by choosing a different basis for the ideal I.

Theorem 2.8 (Theorem 11 and Corollary 12 of Chapter 4, §5 of [CLO13])**.** *Let $I = (P_1,\dots,P_m)$ be a maximal ideal of the polynomial ring $\overline{K}[x_1,\dots,x_n]$, where $\overline{K}$ is an algebraically closed field. Then there exist $a_1,\dots,a_n \in \overline{K}$ such that $I = (x_1 - a_1,\dots,x_n - a_n)$ and $Z(I) = \{(a_1,\dots,a_n)\}$.*

Similarly, the set of zeros of an ideal I of the polynomial ring over an algebraically closed field is empty if and only if $I = \overline{K}[x_1,\dots,x_n]$.

Generally, in cryptography the systems of equations that need to be solved have exactly one solution (or none at all) in the base field $\mathbb{F}_q$, but can have many in the algebraic closure $\overline{\mathbb{F}}_q$. In order to use Theorem 2.8 in those situations, it is common to add the polynomials $x_i^q - x_i$ for $i = 1,\dots,n$ to the system.

Remark 2.9. As $\mathbb{F}_q \setminus \{0\}$ is a cyclic group with respect to the multiplication, it holds that $a \in \overline{\mathbb{F}}_q$ is in the subfield $\mathbb{F}_q$ if and only if $a^q - a = 0$. It follows that for every ideal $I \subseteq \mathbb{F}_q[x_1,\dots,x_n]$ there is a 1-to-1 correspondence between $Z(I) \subseteq \mathbb{F}_q^n$ and $Z(\overline{I} + (x_1^q - x_1,\dots,x_n^q - x_n))$, where $\overline{I}$ is the image of I in $\overline{\mathbb{F}}_q[x_1,\dots,x_n]$. A solution $(a_1,\dots,a_n) \in Z(I)$ is mapped to $(i(a_1),\dots,i(a_n)) \in \overline{\mathbb{F}}_q^n$, where $i : \mathbb{F}_q \to \overline{\mathbb{F}}_q$ is the canonical embedding.

Definition 2.10. Let R be a ring. An *R-module* is a pair $(\cdot, M)$, where M is an abelian group and $\cdot : R \times M \to M$ is a function satisfying the following conditions:

- $1 \cdot a = a$,
- $x \cdot (a + b) = x \cdot a + x \cdot b$,
- $(x + y) \cdot a = x \cdot a + y \cdot a$,
- $(xy) \cdot a = x \cdot (y \cdot a)$

for every $x, y \in R, a, b \in M$.

Example 2.11. Every ideal I of the ring R, together with the ring multiplication, is an R-module.

Definition 2.12. A *graded ring* is a ring R and a family $\{R_d\}_{d \geq 0}$ of subgroups of the underlying additive group of R, such that $R = \bigoplus_{d \geq 0} R_d$ and for all integers

$a, b \geq 0$, $R_a R_b \subseteq R_{a+b}$. The *degree* of $r \in R$, $\deg(r)$, is the largest d for which $\pi_d(r) \neq 0$, where $\pi_d : R \to R_d \subseteq R$ is the canonical projection. The *homogeneous components* of $r \in R$ are the projections $\pi_d(r)$ for $d \leq \deg(r)$. The *leading form* of $r \in R$ is the homogeneous component $\pi_{\deg(r)}(r)$. An element $r \in R$ is said to be *homogeneous of degree d* if $\deg(r) = d$ and it is equal to its leading form.

Example 2.13. The ring of polynomials $R = K[x_1, \ldots, x_n]$ is a graded ring, where R_d is the group of homogeneous polynomials of degree d.

Definition 2.14. Let $R = \bigoplus_{d \geq 0} R_d$ be a graded ring. An ideal $I \subseteq R$ is called *homogeneous* if for every $a \in I$, the homogeneous components of a are also in I.

Proposition 2.15. *Let $R = \bigoplus_{d \geq 0} R_d$ be a graded Noetherian ring. An ideal $I \subseteq R$ is homogeneous if and only if it is generated by a finite set of homogeneous elements.*

Proof. ($\Rightarrow$) As R is Noetherian, $I = (r_1, \ldots, r_n)$. Each r_i can be decomposed in its homogeneous components, i.e. $r_i = \sum_d \pi_d(r_i)$. Only finitely many of the $\pi_d(r_i)$ are different from zero. Let I' be the ideal generated by those nonzero $\pi_d(r_i)$. Clearly, $I \subseteq I'$. On the other hand, $\pi_d(r_i) \in I$, since I is a homogeneous ideal.

($\Leftarrow$) Let $\{r_1, \ldots, r_n\}$ be a set of homogeneous generators for I. Then, every $g \in I$ is of the form $g = \sum_{i=1}^{n} a_i r_i$ for some $a_i \in R$. We can decompose each a_i into the finite sum $a_i = \sum_d \pi_d(a_i)$. Hence, we obtain that $g = \sum_{i,d} \pi_d(a_i) r_i$. Each of the terms of the sum is a homogeneous polynomial and belongs to the ideal I. ■

We denote with I_d the subgroup $I \cap R_d \subseteq R_d$.

Proposition 2.16. *Let $R = \bigoplus_{d \geq 0} R_d$ be a graded ring and I a homogeneous ideal. Then R/I is a graded ring, with grading $R/I = \bigoplus_{d \geq 0} \frac{R_d + I}{I}$.*

Proof. As I is homogeneous, we can write $I = \bigoplus_d (I_d)$ as an R-module. We notice that:

$$\frac{R}{I} \cong \frac{\bigoplus_d R_d}{\bigoplus_d (I_d)} \cong \bigoplus_d \frac{R_d}{I_d} \cong \bigoplus_d \frac{R_d + I}{I}. \tag{2.2}$$

The second isomorphism follows from the fact that for abelian groups, quotients and direct sums commute, while the third isomorphism follows from the

Second Isomorphism Theorem (e.g. Proposition 2.1 in [AM69]). The multiplication in the quotient is inherited from the multiplication in R. ■

2.2 Linear Algebra

Let V and W be vector spaces over the field K with bases $B = \{v_1, \ldots, v_n\}$ and $C = \{w_1, \ldots, w_m\}$ respectively. Let $f : V \to W$ be a K-linear function. One can associate a matrix M of size $m \times n$ to f as follows: the i-th column of M is the sequence of coefficients $a_1, \ldots, a_m$ for which $f(v_i) = a_1 w_1 + \cdots + a_m w_m$.

Here we list some of the classical results from Linear Algebra.

Definition 2.17. Let V and W be vector spaces over K and let $f : V \to W$ be a K-linear map. The *rank* of f, $\mathrm{rk}(f)$ is the dimension of the image of f, $\mathrm{Im}(f)$ and the *kernel* of f, $\ker(f)$ is the vector space $\{v \in V | f(v) = 0\}$.

Proposition 2.18. *Let f be as above and let M be the matrix representation of f under some bases. Then $\mathrm{rk}(f)$ is equal to the rank of the matrix M.*

Theorem 2.19 (Rank-Nullity theorem)**.** *Let $f : V \to W$ be a linear map between vector spaces. The following holds:*

$$\dim(\ker(f)) + \mathrm{rk}(f) = \dim(V).$$

Definition 2.20. A matrix M is said to be in *row echelon form* if:

- All 0-rows appear at the bottom of the matrix,
- The leftmost nonzero coefficient of any nonzero row is a 1. Such entry is called *leading entry*,
- The leading entry of a given row is to the right with respect to the leading entries of all the rows above it.

We say that M is in *reduced row echelon form* if it is in row echelon form and if every column containing a leading entry has all other entries equal to 0.

Proposition 2.21 (Theorem 0.2 in [Rom05])**.** *For every matrix M there exists a unique matrix $\tilde{M}$ in reduced row echelon form that is row equivalent to M, that is one can transform M in $\tilde{M}$ with a sequence of elementary row operations.*

Proposition 2.22. *Let M be a matrix and let $\tilde{M}$ be its reduced row echelon form. Then* $\mathrm{rk}(M) = \mathrm{rk}(\tilde{M})$.

An important family of vector spaces that appear often in commutative algebra are the so-called K-algebras.

Definition 2.23. Let K be a field. A *K-algebra* is a K-module A equipped with a commutative product $\cdot : A \times A \to A$, satisfying:

- $(a+b)\cdot c = a\cdot c + b\cdot c$,
- $(xa)\cdot(yb) = (xy)(a\cdot b)$

for all $a,b,c \in A$ and $x,y \in K$. We say that the algebra *has a unity* if there exists $e \in A$ such that $e \cdot a = a$ for every $a \in A$.

Throughout the thesis, every time we introduce a K-algebra, we mean a K-algebra with unity.

We say that a K-algebra A is *graded* if $A = \bigoplus_{d\geq 0} A_d$, where each A_d is a K-vector space and $A_i \cdot A_j \subseteq A_{i+j}$. An element of a has degree $\deg(a) = \max\{d | \pi_d(a) \neq 0\}$, where π_d is the canonical projection of vector spaces $\pi_d : A \to A_d$.

An example of graded algebra is $R = K[x_1,\dots,x_n]$, with decomposition $R = \bigoplus_{d\geq 0} R_d$, where R_d is the set of homogeneous polynomials of degree d (0 polynomial included). Example 2.13 shows that it is a graded ring. The following proposition shows that each R_d (and hence the whole R) is a K-vector space.

Proposition 2.24. *The set R_d is a K-vector space, with basis $B = \{x_1^{a_1}\dots x_n^{a_n} | a_i \geq 0, \sum_{i=1}^n a_i = d\}$.*

Proof. The structure of vector space is inherited from the K-module structure of R and from the fact that summing two homogeneous polynomials of the same

degree and multiplying times a constant are operations that do not change the degree and preserves homogeneity.

The set B is a basis by definition of a polynomial as the sum of monomials and by the fact that a polynomial is zero if and only if all its monomials have coefficients equal to 0. ■

As a consequence, $R = \bigoplus_{d\geq 0} R_d$ is a K-vector space, with a basis

$$\bigcup_{d\geq 0} \{x_1^{a_1} \dots x_n^{a_n} | \sum_{i=1}^{n} a_i = d\}.$$

Definition 2.25. Let $b_1, \dots, b_n \in \mathbb{R}^m$ be linearly independent vectors. The *lattice* of $\mathbb{R}^m$ with basis $b_1, \dots, b_n$ is the $\mathbb{Z}$-module $\mathcal{L} := \{\sum_{i=1}^{n} a_i b_i | a_i \in \mathbb{Z}\}$. Let M be the matrix whose rows are the vectors $b_1, \dots, b_n$. The *determinant* of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det(MM^T)}$, where M^T is the transposed of M.

Lattices play a prominent role in cryptology and complexity theory, since they are hosts of interesting computational problems, such as the shortest vector problem.

Definition 2.26. Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice and let $|| \bullet || : \mathcal{L} \to \mathbb{R}$ be the restriction of a norm function over $\mathbb{R}^m$. The *Shortest Vector Problem* on $\mathcal{L}$ is to identify the vector $v \in \mathcal{L} \setminus \{0\}$ that minimises $|| \bullet ||$.

2.3 Combinatorics and Multisets

In this section we present the basic tools of finite combinatorics that will be used later in the thesis.

Definition 2.27. Let Ω be a finite set, and let $\mathcal{B}$ be the family of subsets of Ω. A function $P : \mathcal{B} \to \mathbb{R}$ is said to be a *probability function* if $P(A) = \sum_{x\in A} p(x)$, where $p(x)$ satisfies the following conditions:

(i) $p(x) \geq 0$,

(ii) $\sum_{x\in\Omega} p(x) = 1$.

Example 2.28. Let us consider a finite set Ω. The *uniform probability function* on Ω is the probability function P induced by

$$p(x) = \frac{1}{|\Omega|}.$$

Example 2.29. Let us consider an urn with N balls of two different color. There are w white balls and b black balls. We can model this example with a set $U = \{a_1, \ldots, a_N\}$ and a color function $c : U \to \{W, B\}$ such that $|c^{-1}(W)| = w$ and $|c^{-1}(B)| = b$. Let $\Omega = \{(b_1, \ldots, b_n) | b_i \neq b_j, b_i \in U\}$ be the set of sequences without repetitions from U of length n.

The color map induces a map $\tilde{c} : \Omega \to \{W, B\}^n$ sending

$$\tilde{c} : (t_1, \ldots, t_n) \mapsto (c(t_1), \ldots, c(t_n)).$$

We equip $\{W, B\}^n$ with the probability function induced by

$$p(x) = \frac{|\tilde{c}^{-1}(x)|}{|\Omega|}. \tag{2.3}$$

Definition 2.30. Let Ω be a finite set equipped with a probability function. A *random variable* over Ω is a function $X : \Omega \to \mathbb{R}$.

Random variables are used to measure probabilities of events given a probability function on the set Ω.

Definition 2.31. Let X be a random variable over Ω, equipped with a probability function P. We define the *probability* of an event $E \subseteq \mathbb{R}$ to be $\mathbb{P}_\Omega(X \in E) = P(X^{-1}(E))$. If the set Ω is clear from the context, we omit it from the notation.

Example 2.32. Let Ω be the set of matrices with n rows and n columns over $\mathbb{F}_2$. Then $|\Omega| = 2^{n^2}$. We equip Ω with the uniform probability function. Let $\mathrm{rk} : \Omega \to \mathbb{R}$ be the random variable that associates to a matrix its rank. Then

$$\mathbb{P}_\Omega(\mathrm{rk} = 0) = 2^{-n^2}.$$

Example 2.33. Let us consider a model as in Example 2.29, with $\{W,B\}^n$ equipped with the probability function P from Example 2.29.

An element of $\{W,B\}^n$ can be represented as a vector of integers $s = (w_1,b_1,w_2,b_2,\ldots,w_k,b_k)$, with $w_1,b_k \geq 0$, $w_i,b_j > 0$ for $i > 1$ and $j < k$, and $\sum_{j=1}^{k}(w_j + b_j) = n$. The vector s represents the sequence

$$(\underbrace{W,\ldots,W}_{w_1 \text{ copies}},\underbrace{B,\ldots,B}_{b_1 \text{ copies}},W,\ldots,\underbrace{W,\ldots,W}_{w_k \text{ copies}},\underbrace{B,\ldots,B}_{b_k \text{ copies}}).$$

We say that a random variable X over $\{W,B\}^n$ follows the *hypergeometric distribution* if $X(s) = \sum_{j=1}^{k} w_j$. Then

$$\mathbb{P}(X = k) = \frac{\binom{w}{k}\binom{b}{n-k}}{\binom{N}{n}}.$$

Example 2.34. Let us consider the same urn as in the previous example and the set $\{W,B\}^n$ of all the possible sequences with the probability function (2.3).

We say that a random variable X over $\{W,B\}^n$ follows the *negative hypergeometric distribution* if for $s = (w_1,b_1,\ldots,w_k,b_k)$, $X(s) = w_1$. Then

$$\mathbb{P}(X = k) = \frac{\binom{w}{k}}{\binom{N}{k}}\frac{N-w}{N-k}.$$

Definition 2.35. Let X be a random variable over a finite set Ω, equipped with a distribution P. The *expected value* of X is the real number

$$\mathbb{E}(X) = \sum_{e \in \mathrm{Im}(X)} e\mathbb{P}(X = e).$$

Example 2.36. Let X be a random variable following the hypergeometric distribution as in Example 2.33. The expected value of X is equal to nw/N (see e.g. [CB02]).

Example 2.37. Let X be a random variable following the negative hypergeomet-

ric distribution as in Example 2.34. The expected value of X is equal to

$$\mathbb{E}(X) = \frac{w}{N - w + 1}$$

(see e.g. [PJ68]).

Definition 2.38. A multiset is a couple $(A, \mathfrak{m})$, where A is a set and $\mathfrak{m}$ is a function from A to the set of non negative integers. A multiset can be represented as $\{a^{\mathfrak{m}(a)}\}_{a \in A}$. The set A is called the *ground set* of $(A, \mathfrak{m})$.

We define the following operations on multisets with ground set A

- **Inclusion**: $(A, \mathfrak{n}) \subseteq (A, \mathfrak{m})$ if $\mathfrak{n}(a) \leq \mathfrak{m}(a)$ for every $a \in A$.
- **Sum**: $(A, \mathfrak{m}) + (A, \mathfrak{n}) = (A, \mathfrak{r})$, where $\mathfrak{r}(a) = \mathfrak{m}(a) + \mathfrak{n}(a)$.
- **Difference**: Let $(A, \mathfrak{n}) \subseteq (A, \mathfrak{m})$. $(A, \mathfrak{m}) - (A, \mathfrak{n}) = (A, \mathfrak{r})$, where $\mathfrak{r}(a) = \mathfrak{m}(a) - \mathfrak{n}(a)$.
- **Size**: $|(A, \mathfrak{m})| = \sum_{a \in A} \mathfrak{m}(a)$.

Let $\mathcal{A}$ be the family of all the multisets with ground set A. Then $(\mathcal{A}, +)$ is a monoid.

Throughout the thesis, we will consider only multisets that have $A = \{1, \ldots, n\}$ as a base set for some n. In this case, we use the notation $(a_1, \ldots, a_n)$ to represent $\{i^{a_i}\}_{i=1,\ldots,n}$.

Proposition 2.39. *Let $\mathcal{X}^d$ be the family of multisets $\{(a_1, \ldots, a_n) | \sum_{i=1}^n a_i = d\}$. Then $\mathcal{X}^d$ contains $\left(\!\binom{n}{d}\!\right) = \binom{n+d-1}{d}$ elements.*

Proof. The proof is performed by induction on n. For $n = 1$, $\mathcal{X}^d = \{1^d\}$ and the statement holds. Let us assume, by inductive hypothesis, that the proposition holds for $n - 1$. We can decompose $\mathcal{X}^d$ in disjoint sets as follows:

$$\mathcal{X}^d = \bigcup_{i=0}^{d} \left\{ (i, a_2, \ldots, a_n) \middle| \sum_{j=2}^{n} a_j = d - i \right\}.$$

It follows that

$$|\mathcal{X}^d| = \sum_{i=0}^{d} \left(\!\!\binom{n-1}{d-i}\!\!\right) = \left(\!\!\binom{n}{d}\!\!\right).$$

The last equality is obtained by using the relation $\left(\!\!\binom{n}{j}\!\!\right) = \left(\!\!\binom{n-1}{j}\!\!\right) + \left(\!\!\binom{n}{j-1}\!\!\right)$ repeatedly. ■

It is possible to define the lexicographic ordering on $\mathcal{X}^d$. Let $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$. We say that $a > b$ if there exists i such that $a_i > b_i$ and $a_j = b_j$ for every $j < i$.

Proposition 2.40. *Let us consider the monoid $(M, \cdot)$, where M is the set of monomials in $K[x_1, \ldots, x_n]$ and $\cdot$ is the product of monomials. Let $(Y, +)$ be the monoid, where Y is the family of multisets with ground set $\{1, \ldots, n\}$ and $+$ is the sum of multisets. There exists a monoid isomorphism $\varphi : M \to Y$ satisfying $\deg(m) = |\varphi(m)|$ for every $m \in M$.*

Proof. Let us consider the function φ that maps the monomial $m = x_1^{a_1} \ldots x_n^{a_n}$ to the multiset $A = (a_1, \ldots, a_n)$: it is a clearly a bijection. φ is a monoid homomorphism for the fact that

$$x_1^{a_1} \ldots x_n^{a_n} \cdot x_1^{b_1} \ldots x_n^{b_n} = x_1^{a_1+b_1} \ldots x_n^{a_n+b_n}.$$

The property of the degree follows from the fact that $\deg(m) = \sum_{i=1}^{n} a_i$. ■

Let $1 \leq k_1 \leq k_2 \leq \cdots \leq k_n$ be integers. Let us consider the family of multisets $\mathcal{X} = \{(a_1, \ldots, a_n) | 0 \leq a_i \leq k_i\}$. It is possible to partition $\mathcal{X}$ as follows:

$$\mathcal{X} = \bigcup_{d \geq 0} \mathcal{X}^d,$$

where $\mathcal{X}^d = \{(a_1, \ldots, a_n) \in \mathcal{X} | \sum_j a_j = d\}$.

Definition 2.41. Let $\mathcal{B}$ be a family of multisets in $\mathcal{X}^d$. For a positive integer i the collection

$$\nabla^i(\mathcal{B}) = \{a \in \mathcal{X}^{d+i} | a \supseteq b \text{ for some } b \in \mathcal{B}\}$$

is called the i-th *shade* of $\mathcal{B}$. The first shade is denoted simply by $\nabla(\mathcal{B})$. The collection $C(\mathcal{B})$ is called the *compression* of $\mathcal{B}$ and it is the family of the largest $|\mathcal{B}|$ multisets of $\mathcal{X}^d$ according to the lexicographic ordering.

Theorem 2.42 (Generalized Macaulay Theorem, Corollary 1 in [CL69])**.** *If $\mathcal{B} \subseteq \mathcal{X}^d$, then $\nabla(C(\mathcal{B})) \subseteq C(\nabla(\mathcal{B}))$.*

As the name suggests, Theorem 2.42 is a generalization of a theorem proved by Macaulay in [Mac27], that states: $\nabla(C(\mathcal{B})) \subseteq C(\nabla(\mathcal{B}))$ for $\mathcal{B} \subseteq \mathcal{Y}^d$, where $\mathcal{Y}^d = \{(a_1, \ldots, a_n) | a_i \geq 0, \sum a_i = d\}$.

An equivalent statement of Theorem 2.42 was proved in [ST19a], whose authors were not aware of the existence of the proof by Clements and Lindström.

Corollary 2.43. *Let B_v the family of subsets of $\mathcal{X}^d$ of cardinality v. Let T_v be the family of the largest v multisets according to the lexicographic ordering. Then*

$$\min_{\mathcal{B} \in B_v} |\nabla(\mathcal{B})| = |\nabla(T_v)|.$$

Proof. For every $\mathcal{B} \in B_v$, $C(\mathcal{B}) = T_v$. Using Theorem 2.42, we get that

$$|\nabla(\mathcal{B})| = |C(\nabla(\mathcal{B}))| \geq |\nabla(C(\mathcal{B}))| = |\nabla(T_v)|.$$

■

Corollary 2.44. *For every i Theorem 2.42 and Corollary 2.43 hold for the ∇^i operator.*

Proof. First we show the extension of the theorem by induction. The case $i = 1$ is Theorem 2.42. We notice that if $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{X}^d$, then $\nabla(\mathcal{A}) \subseteq \nabla(\mathcal{B})$. Hence

$$\nabla^{i+1}(C(\mathcal{B})) = \nabla(\nabla^i(C(\mathcal{B}))) \subseteq \nabla(C(\nabla^i(\mathcal{B}))) \subseteq C(\nabla^{i+1}(\mathcal{B})).$$

Both $\subseteq$ symbols follow from the inductive hypothesis.

Let X_v be as above. Then for every $\mathcal{B} \subseteq \mathcal{X}^d$ of size v we have

$$|\nabla^i(\mathcal{B})| = |C(\nabla^i(\mathcal{B}))| \geq |\nabla^i(C(\mathcal{B}))| = |\nabla^i(X_v)|.$$

■

2.4 Complexity theory

Definition 2.45. Let $f : \mathbb{N} \to \mathbb{R}$ be a function. The set $O(f)$ is the family of functions satisfying the following property: $g \in O(f)$ if there exist $n_0 \in \mathbb{N}$ and $C \in \mathbb{N}$ such that $|g(n)| < C|f(n)|$ for every $n \geq n_0$.

By abusing notation, we will write $f = g + O(h)$ to intend that $f = g + h'$, for some $h' \in O(h)$.

We introduce the notation

$$l_q(n,d) = |\{(a_1,\dots,a_n)|0 \leq a_i < q, \sum_{i=1}^{n} a_i = d\}|.$$

Proposition 2.46. $l_q(n,d) = \left(\!\binom{n}{d}\!\right) + O(n^{d-q+1})$ *as* $n \to \infty$.

Proof. Obviously,

$$l_q(n,d) = [t^d]\frac{(1-t^q)^n}{(1-t)^n}, \tag{2.4}$$

where $[t^d]\sum_{i=0}^{\infty}\alpha_i t^i = \alpha_d$, the coefficient at the monomial t^d in the power series.

By (2.4), $l_q(n,d) =$

$$[t^d]\left(\sum_{i=0}^{n}(-1)^i\binom{n}{i}t^{qi}\cdot\sum_{j=0}^{\infty}\left(\!\binom{n}{j}\!\right)t^j\right) = \sum_{i=0}^{\lfloor d/q\rfloor}(-1)^i\binom{n}{i}\left(\!\binom{n}{d-iq}\!\right)$$

$$= \left(\!\binom{n}{d}\!\right) + \sum_{i=1}^{\lfloor d/q\rfloor}(-1)^i\binom{n}{i}\left(\!\binom{n}{d-iq}\!\right) = \left(\!\binom{n}{d}\!\right) + O(n^{d-q+1}).$$

■

Definition 2.47. Let $\{0,1\}^*$ be the union of all the sequences of finite length: $\{0,1\}^* = \bigcup_{n\geq 1}\{0,1\}^n$. Let $f : L \subseteq \{0,1\}^* \to \{0,1\}^*$ be a function. An *algorithm* A for computing f is a finite set of rules that allows one to produce $f(x)$ for every $x \in L$. Each rule may be applied finitely many times and the number of applications may depend on the input.

Since there are no restrictions on the function f, one can potentially construct algorithms for functions with any countable domain D, by precompos-

ing f with a suitable embedding $D \to \{0,1\}^*$. Similarly one can postcompose f with an embedding $\mathrm{Im}(f) \to C$ for any compatible set C.

Definition 2.48. Let $f : L \subseteq \{0,1\}^* \to \{0,1\}^*$ and $T : \mathbb{N} \to \mathbb{N}$ be functions. Let A be an algorithm for computing f. The *time complexity* of A is T if A produces $f(x)$ after at most $T(|x|)$ steps.

Definition 2.49. A set $A \subseteq \{0,1\}^*$ is in **NP** if there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$, a function $f : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$, and an algorithm that computes f with polynomial time complexity such that for every $x \in \{0,1\}^*$,

$$x \in A \Leftrightarrow \text{ there exists } y \in \{0,1\}^{p(|x|)} \text{ such that } f(x,y) = 1.$$

Definition 2.50. Let $A, B \subseteq \{0,1\}^*$. The set A is said to be *polynomial time reducible* to B if there exists a function $f : \{0,1\}^* \to \{0,1\}^*$ and an algorithm that computes f with polynomial time complexity such that for every $x \in \{0,1\}^*$, $x \in A$ if and only if $f(x) \in B$. A set $A \subseteq \{0,1\}^*$ is ***NP*-complete** if $A \in$ **NP** and every subset $B \in$ **NP** is polynomial time reducible to A.

Example 2.51 (kSAT). Let us consider variables $x_1, \ldots, x_n$ that can assume values in $\{\text{TRUE}, \text{FALSE}\}$, the binary operators AND ($\wedge$) and OR ($\vee$) and the unary operator NOT ($\bar{\bullet}$). A boolean formula in k-Conjunctive Normal Form (kCNF) is a function $F : \{\text{TRUE}, \text{FALSE}\}^n \to \{0,1\}$ of the form

$$F(x_1, \ldots, x_n) = \bigwedge_i \left(\bigvee_{j=1}^{k_i} v_{i,j} \right),$$

where each $v_{i,j}$ is a variable x_t or its negation $\bar{x}_t$ and $k_i \leq k$ for every i.

kSAT is the subset of the kCNF that encodes in $\{0,1\}^*$ all the functions F such that $1 \in \mathrm{Im}(F)$.

Theorem 2.52 ([Coo71, Lev73, FY79])**.** *kSAT is **NP**-complete for every $k > 2$. The set of systems of quadratic equations over $\mathbb{F}_2$ with at least one solution over $\mathbb{F}_2$ is **NP**-complete.*

Chapter 3

Gröbner basis

In the first two sections of this chapter we present the definition of a Gröbner basis of an ideal in a polynomial ring, together with the properties that make this family of generators important for understanding the ideal itself. The presentation of this subject loosely follows [CLO13] and [BW93]. Whenever other references are used, they will be explicitly mentioned.

Section 3.3 contains the definition of degree of regularity given in [BFS03] and its ties with Hilbert series and Macaulay matrices. From that we expand the definition so that it applies to arbitrary quotients of a multivariate polynomial ring, maintaining the connection with Hilbert series and Macaulay matrices.

The degree of regularity can be used to give an upper bound on the complexity of computing a Gröbner basis and finding one of the zeros of a system of polynomial equations. This is proved constructively in Section 3.4.

3.1 Relations and Monomial ordering

Definition 3.1. Let S be a set. A *relation* on S is a subset $Z \subseteq S \times S$. A relation Z is called

- *reflexive* if for every $s \in S$, $(s,s) \in Z$,
- *transitive* if for every $s,t,u \in S$ with $(s,t),(t,u) \in Z$, then $(s,u) \in Z$,

- a *partial ordering* if Z is reflexive, transitive, and for any pair $s,t \in S$ such that $(s,t),(t,s) \in Z$, then $s = t$,
- a *total ordering* if Z is a partial ordering and $s,t \in S$ implies $(s,t) \in Z$ or $(t,s) \in Z$.

For every ordering (partial or total) Z over S, one can define a *strict ordering* $\hat{Z}$ over S as follows: $\hat{Z} = Z \setminus \{(s,s)\}_{s\in S}$. We are going to denote orderings with the symbol $\leq$, i.e. $(s,t) \in Z$ will be written as $s \leq t$. The strict orderings will be denoted by $<$, i.e. $(s,t) \in \hat{Z}$ will be written as $s < t$.

Let Z be a relation over S.

- The *reflexive closure* of Z is defined as $Z' = Z \cup \{(s,s)\}_{s\in S}$,
- The *transitive closure* of Z is defined as

$$Z'' = Z \cup \{(s,u) | \exists t \in S \text{ such that } (s,t),(t,u) \in Z\}.$$

- The reflexive-transitive closure of Z is defined as $Z'' \cup \{(s,s)\}_{s\in S}$, where Z'' is the transitive closure of Z.

It is immediate to prove the following

Proposition 3.2. *Let Z be a relation. The reflexive closure of Z is reflexive, the transitive closure of Z is transitive and the reflexive-transitive closure of Z is both reflexive and transitive.*

Definition 3.3. Let us consider a polynomial ring $R = K[x_1,\ldots,x_n]$. A *Monomial ordering* $\leq$ for R is a total ordering on the family of multisets $Y = \{(a_1,\ldots,a_n) | a_i \geq 0\}$ satisfying the following additional properties:

- for every $a,b,c \in Y$, $a < b$ implies $a + c < b + c$,
- every nonempty subset of Y contains a smallest element.

This ordering induces an ordering on the set of monomials of R thanks to Proposition 2.40.

The fact that a monomial ordering is total forces 1 to be the smallest monomial of R.

Example 3.4 (Lexicographic Ordering). Let $a = x_1^{a_1} \dots x_n^{a_n}$ and $b = x_1^{b_1} \dots x_n^{b_n}$. We say that $a \leq b$ according to the *lexicographic* ordering if $a = b$ or if there exists $i \in \{1, \dots, n\}$ for which $a_i < b_i$ and $a_j = b_j$ for every $0 < j < i$.

Example 3.5 (Graded Lexicographic Ordering). Let $a = x_1^{a_1} \dots x_n^{a_n}$ and $b = x_1^{b_1} \dots x_n^{b_n}$. We say that $a \leq b$ according to the *graded lexicographic* ordering if $a = b$, if $\deg(a) < \deg(b)$, or if $\deg(a) = \deg(b)$ and there exists $i \in \{1, \dots, n\}$ for which $a_i < b_i$ and $a_j = b_j$ for every $0 < j < i$.

Example 3.6 (Graded Reverse Lex Ordering). Let $a = x_1^{a_1} \dots x_n^{a_n}$ and $b = x_1^{b_1} \dots x_n^{b_n}$. We say that $a \leq b$ according to the *grevlex* (Graded reverse lexicographic) ordering if $a = b$, if $\deg(a) < \deg(b)$, or if $\deg(a) = \deg(b)$ and there exists $i \in \{1, \dots, n\}$ for which $a_i > b_i$ and $a_j = b_j$ for every $i < j \leq n$.

Let $\leq$ be a fixed monomial ordering for R and let $f = \sum_{\alpha \in S} a_\alpha x^\alpha \in R$, with $a_\alpha \in K$, be a polynomial. Here, S is a finite subset of Y and $x^\alpha = \varphi^{-1}(\alpha)$, where φ is the monoid isomorphism defined in Proposition 2.40 that associates $x_1^{a_1} \dots x_n^{a_n}$ to $(a_1, \dots, a_n)$.

- The *multidegree* of f is $\mathrm{md}(f) = \max_{\leq}\{\alpha \in S | a_\alpha \neq 0\}$,
- The *leading monomial* of f is $\mathrm{LM}(f) = x^{\mathrm{md}(f)}$,
- The *leading coefficient* of f is $\mathrm{LC}(f) = a_{\mathrm{md}(f)}$,
- The *leading term* of f is $\mathrm{LT}(f) = a_{\mathrm{md}(f)} x^{\mathrm{md}(f)}$,
- The *set of monomials* of f is $M(f) = \{x^\alpha | a_\alpha \neq 0\}$.

We will use the same notation for sets of polynomials: let $G = \{f_1, \dots, f_m\}$. Then $\mathrm{md}(G) = \{\mathrm{md}(f_1), \dots, \mathrm{md}(f_m)\}$. The same applies to the other operators.

Definition 3.7. Let $f, g, p \in R = K[x_1, \dots, x_n]$ with $p \neq 0$. Let G be a finite subset of R. We say that:

- f *reduces to* g *modulo* p (in symbols, $f \underset{p}{\to} g$) if there exists $x^\alpha \in M(f)$ and a monomial s such that $s\,\mathrm{LM}(p) = x^\alpha$ and $g = f - \frac{a_\alpha}{\mathrm{LC}(p)} sp$,

- *f reduces to g modulo G* (in symbols, $f \underset{G}{\to} g$) if $f \underset{p}{\to} g$ for some $p \in G$.

We notice that $\underset{G}{\to}$ is a relation over R: (f,g) is in the relation if $f \underset{G}{\to} g$. We define $\overset{*}{\underset{G}{\to}}$ to be the reflexive-transitive closure of $\underset{G}{\to}$.

Example 3.8. Let $R = K[x,y,z]$ be equipped with the graded lexicographic ordering and let $f = xy + x$, $g = xz + x$, and $p = y - z$. Then $f \underset{p}{\to} g$, for $xy + x - x(y - z) = xz + x$.

Let $G = \{y - z, z + 1\}$. We notice that f does not reduce to 0 modulo G. On the contrary, we notice that $f \underset{y-z}{\to} xz + x \underset{z+1}{\to} 0$. Hence, $f \overset{*}{\underset{G}{\to}} 0$. From now on, by abusing notation, we say that *f reduces to g modulo G* if $f \overset{*}{\underset{G}{\to}} g$.

Definition 3.9. Let us consider a polynomial $f \in R$ and an ordered sequence of polynomials $G = (g_1, \dots, g_t)$. A *multivariate division algorithm* according to a monomial ordering is an algorithm which produces $q_1, \dots, q_t, r \in R$ such that $f = \sum_{i=1}^{t} q_i g_i + r$, the monomials of r are not divisible by any of the $\mathrm{LM}(g_i)$, and $\mathrm{md}(f) \geq \mathrm{md}(q_i g_i)$ for every i. Using the notation of [CLO13], we refer to the remainder as $\overline{f}^G = r$. An example of multivariate division algorithm is Algorithm 1 (Chapter 2, § 3 Theorem 2 from [CLO13]).

Proposition 3.10. *Let $\alpha = \mathrm{md}(f)$ and β be the largest multidegree among the g_i. Let l be the number of monomials of multidegree $\leq \alpha$ and L the number of monomials of multidegree $\leq \beta$. Then it takes $O(lL)$ operations in K to perform the multivariate polynomial division.*

Proof. Potentially, one has to repeat the outer **while** loop a number of times equal to the number of monomials of multidegree $\leq \alpha$, since every monomial in $p - \mathrm{LT}(p)/LT(g_i)g_i$ has multidegree strictly smaller than $\mathrm{md}(p)$. Indeed

$$p - \mathrm{LT}(p)/LT(g_i)g_i = (p - \mathrm{LT}(p)) - (g_i - \mathrm{LT}(g_i))\frac{\mathrm{LT}(p)}{\mathrm{LT}(g_i)}.$$

Clearly $\mathrm{md}(p) > \mathrm{md}(p - \mathrm{LT}(p))$. Similarly, $\mathrm{md}(g_i) > \mathrm{md}(g_i - \mathrm{LT}(g_i))$ and, by definition of monomial ordering, we have that

$$\mathrm{md}\left((g_i - \mathrm{LT}(g_i))\frac{\mathrm{LT}(p)}{\mathrm{LT}(g_i)}\right) < \mathrm{md}\left(\mathrm{LT}(g_i)\frac{\mathrm{LT}(p)}{\mathrm{LT}(g_i)}\right) = \mathrm{md}(p).$$

input : A polynomial f, a sequence of polynomials $(g_1,\ldots,g_t)$
output: $q_1,\ldots,q_t,r$
$q_1 := 0;\ldots;q_t := 0;r := 0$;
$p := f$;
while $p \neq 0$ **do**
  $i := 1$;
  division := *false* ;
  while $i \leq t$ **and** *division* = *false* **do**
    if $\mathrm{LT}(g_i)$ **divides** $\mathrm{LT}(p)$ **then**
      $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(g_i)$;
      $p := p - \mathrm{LT}(p)/\mathrm{LT}(g_i)g_i$;
      division := *true* ;
    else
      $i := i + 1$
    end
  end
  if *division* = *false* **then**
    $r := r + LT(p)$;
    $p := p - LT(p)$;
  end
end

Algorithm 1: Multivariate division algorithm

Therefore $\mathrm{md}(p) > \mathrm{md}(p - \mathrm{LT}(p)/\mathrm{LT}(g_i)g_i)$.

In each inner **while** loop, one has to perform less than L shifts (multiplication times $\mathrm{LT}(p)/\mathrm{LT}(g_i)$) and a sum of vectors over a K-vector space of dimension L. ■

Let $G = (g_1,\ldots,g_t)$ and $G' = \{g_1,\ldots,g_t\}$; polynomial division by G and reduction modulo G' are related. Indeed, let $r = \overline{f}^G$, then $f \xrightarrow[G']{*} r$, as it will be shown in Proposition 3.21.

3.2 Properties of Gröbner bases

Definition 3.11. Let $R = K[x_1,\ldots,x_n]$ be a polynomial ring equipped with a monomial ordering. Let $I \subseteq R$ be a nonzero ideal and let $G = \{g_1,\ldots,g_t\}$ be a subset of I. G is said to be a *Gröbner basis* of I if

$$(\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)) = (\mathrm{LT}(I)).$$

Theorem 3.12 (Corollary 6, Chapter 2, §5 of [CLO13]). *Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring equipped with a monomial order. Then every nonzero ideal $I \subseteq R$ has a Gröbner basis. Moreover, $I = (G)$.*

Gröbner bases are not unique: given a Gröbner basis G for I, $G \cup \{a\}$ is a Gröbner basis for I for every $a \in I$. Nevertheless by adding a condition to the definition of Gröbner bases, we get uniqueness.

Definition 3.13. Let G be a Gröbner basis for I. We say that G is a *reduced Gröbner basis* if

(i) $\mathrm{LC}(g) = 1$ for every $g \in G$,

(ii) For every $g \in G$, no monomial of g is in $(\mathrm{LT}(G \setminus \{g\}))$.

Theorem 3.14 (Theorem 5, Chapter 2, §7 of [CLO13]). *Let $I \subseteq K[x_1, \ldots, x_n]$ be a nonzero ideal. Then for any given monomial ordering, there exists a reduced Gröbner basis, and it is unique.*

Proof. **Existence**. The proof of existence is constructive. Let G be a Gröbner basis for I. From G, we remove all the polynomials g such that $\mathrm{LT}(g) \in \mathrm{LT}(G \setminus \{g\})$. By construction, the modified G is still a Gröbner basis for I. Next, we replace all g with $g/\mathrm{LC}(g)$. In this way all polynomials are monic. Lastly, for every $g \in G$, let $g' = \overline{g}^{G \setminus \{g\}}$. We replace g with g'. Each polynomial undergoes this reduction only once and its leading coefficient does not change. This implies that every monomial of $h \in G$ not divisible by $\mathrm{LT}(g)$ is also not divisible by $\mathrm{LT}(g')$. After this change, G is a reduced Gröbner basis for I.

Uniqueness. Let $G = \{g_1, \ldots, g_t\}, G' = \{g'_1, \ldots, g'_s\}$ be two reduced Gröbner bases for I. First we prove that $\mathrm{LT}(G) = \mathrm{LT}(G')$. $(\mathrm{LT}(I)) = (\mathrm{LT}(G)) = (\mathrm{LT}(G'))$, so $\mathrm{LT}(g_1)$ is divisible by $\mathrm{LT}(g'_i)$ for some i. On the other hand, $\mathrm{LT}(g'_i)$ also belongs to $(\mathrm{LT}(I))$, so it is divisible by $\mathrm{LT}(g_j)$ for some j. This implies that $\mathrm{LT}(g_1)$ is divisible by $\mathrm{LT}(g_j)$ and by construction, $j = 1$. This means that $\mathrm{LT}(g_1) = \mathrm{LT}(g'_i)$. Repeating this for every $j = 1, \ldots, t$, one can see that $\mathrm{LT}(G) \subseteq \mathrm{LT}(G')$ and the equality holds by symmetry.

Therefore, for every $g \in G$, there exists g' such that $\mathrm{LT}(g) = \mathrm{LT}(g')$. Since $\mathrm{LT}(g) = \mathrm{LT}(g')$, $g - g'$ is a linear combination of the elements in the set $M(g) \cup$

$M(g') \setminus \{\mathrm{LM}(g), \mathrm{LM}(g')\}$. None of them is divisible by the leading terms of any $h \in G$. Since $(\mathrm{LT}(G)) = (\mathrm{LT}(I))$, it has to be the case that $g - g' = 0$. Hence we have shown that $G \subseteq G'$. Since $|G| = |G'|$ we conclude $G = G'$ as stated. ■

Definition 3.15. Let $f, g \in R$ be two polynomials. The *S-polynomial* of f and g is defined as

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g,$$

where $\mathrm{lcm}(a,b)$ is the least common multiple of the monomials a and b.

Gröbner bases behave particularly well with respect to S-polynomials, as the following theorem (also known as the *Buchberger Criterion*) shows.

Theorem 3.16 (Theorem 5.48 of [BW93])**.** *Let G be a finite subset of $R = K[x_1, \ldots, x_n]$. Then G is a Gröbner basis for $I = (G)$ if and only if*

$$S(g_i, g_j) \xrightarrow[G]{*} 0,$$

for every $g_i, g_j \in G$, $g_i \neq g_j$.

Lemma 3.17. *Let $f \in R$ and a finite set $G \subseteq R$ be such that $f \xrightarrow[G]{*} 0$. Then for any finite set $F \subseteq R$, $f \xrightarrow[G \cup F]{*} 0$.*

Proof. By the definition of $\xrightarrow{*}$, there exists a sequence of polynomials $f = f_0, \ldots, f_n = 0 \in R$ and $p_1, \ldots, p_n \in G$ such that:

$$f = f_0 \xrightarrow[p_1]{} f_1 \xrightarrow[p_2]{} \ldots \xrightarrow[p_n]{} f_n = 0.$$

Since $p_1, \ldots, p_n \in G \cup F$, the statement holds. ■

Proposition 3.18. *Let $f, g \in R$ be such that* $\gcd(\mathrm{LM}(f), \mathrm{LM}(g)) = 1$. *Then*

$$S(f,g) \xrightarrow[\{f,g\}]{*} 0.$$

Proof. Let $f = \mathrm{LT}(f) + f'$ and $g = \mathrm{LT}(g) + g'$. By definition, the S-polynomial of f and g is: $S(f,g) = \frac{\mathrm{LM}(g)}{\mathrm{LC}(f)} f' - \frac{\mathrm{LM}(f)}{\mathrm{LC}(g)} g'$. It follows that

$$\frac{\mathrm{LM}(g)}{\mathrm{LC}(f)} f' - \frac{\mathrm{LM}(f)}{\mathrm{LC}(g)} g' \underset{g}{\to} -\frac{g'f'}{\mathrm{LC}(f)\mathrm{LC}(g)} - \frac{\mathrm{LM}(f)}{\mathrm{LC}(g)} g' \underset{f}{\to}$$
$$\underset{f}{\to} -\frac{g'f'}{\mathrm{LC}(f)\mathrm{LC}(g)} + \frac{f'g'}{\mathrm{LC}(g)\mathrm{LC}(f)} = 0.$$

■

From Lemma 3.17 and Proposition 3.18 one can deduce the following

Corollary 3.19. *Let $G = \{g_1, \ldots, g_n\} \subseteq R$. If there exist i, j such that $\mathrm{LM}(g_i)$ and $\mathrm{LM}(g_j)$ are coprime, then $S(g_i, g_j) \underset{G}{\overset{*}{\to}} 0$.*

Lemma 3.20. *Let $f, g \in R$ and $G \subseteq R$ be such that $f \underset{G}{\overset{*}{\to}} g$. Then $f \underset{G \cup \{g\}}{\overset{*}{\to}} 0$.*

Proof. By definition, there exists a chain

$$f \underset{g_1}{\to} f_1 \underset{g_2}{\to} \cdots \underset{g_n}{\to} g,$$

with $g_i \in G$ that can be extended by $g \underset{g}{\to} 0$. Hence the statement holds. ■

Proposition 3.21. *Let $f \in R$ and $G = (g_1, \ldots, g_n)$ be a sequence of elements in R. Let $G' = \{g_1, \ldots, g_n\}$. Then $f \underset{G'}{\overset{*}{\to}} \overline{f}^G$.*

Proof. For the fact that $\underset{G'}{\overset{*}{\to}}$ is transitive, it is enough to show that at each step of the division algorithm, $p + r$ at the beginning of the outer **while** loop reduces modulo G' to $p + r$ at the end of the loop. In this way one creates a chain that starts from $f = p + 0$ in the first step and terminates to $\overline{f}^G = 0 + r$ in the last step.

Let us consider p and r at the beginning of the outer **while** loop. Say that for p in the algorithm there exists g_i such that $\mathrm{LM}(p)$ is divisible by $\mathrm{LM}(g_i)$. Then we replace p with $p - mg_i$, where m is a monomial for which $\mathrm{LM}(mg_i) = \mathrm{LM}(p)$. Hence, $p + r \underset{g_i}{\to} p - mg_i + r$. On the other hand, if there is no such g_i, then $p + r \underset{G'}{\overset{*}{\to}} (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p))$ by symmetry of the relation $\underset{G'}{\overset{*}{\to}}$. ■

Corollary 3.22. *Let $f \in R$ and $G = (g_1, \ldots, g_n)$ be a sequence of elements in R. Let $G' = \{g_1, \ldots, g_n\}$. If the remainder of f divided by G is zero, then f reduces to zero modulo G'.*

Using the previous results, one can define Algorithm 2 (Buchberger Algorithm, Table 5.4 from [BW93]) to compute a Gröbner basis of the ideal generated by the polynomials $f_1, \ldots, f_m$.

input : $f_1, \ldots, f_m \in R$
output: G a Gröbner basis for $(f_1, \ldots, f_m)$
$G \leftarrow \{f_1, \ldots, f_m\}$;
$B \leftarrow \{\{g_1, g_2\} | g_1, g_2 \in G, g_1 \neq g_2\}$;
while $B \neq \emptyset$ **do**
  choose $\{g_1, g_2\} \in B$;
  $B \leftarrow B \setminus \{\{g_1, g_2\}\}$;
  if $\gcd(\mathrm{LM}(g_1), \mathrm{LM}(g_2)) \neq 1$ **then**
    $h \leftarrow S(g_1, g_2)$;
    $r \leftarrow \overline{h}^{G}$;
    if $r \neq 0$ **then**
      $B \leftarrow B \cup \{\{g, r\} | g \in G\}$;
      $G \leftarrow G \cup \{r\}$;
    end
  end
end

Algorithm 2: Buchberger Algorithm

Theorem 3.23. *Algorithm 2 is correct (i.e. produces a Gröbner basis of (F)) and terminates.*

Proof. Termination. Let us consider a **while** loop during which G was incremented with r. Let us call G_o the set G at the beginning of the loop. If we show that $\mathrm{LM}(r) \notin (\mathrm{LM}(G_o))$, then by the Ascending Chain Condition there can be only finitely many r that are added to G and the loop will terminate.

Since r is a remainder after division by G_o, then $\mathrm{LM}(r)$ is not divisible by any of the leading terms of G_o. Hence the claim holds and Termination is proven.

Correctness. We claim that at the end of each step of the **while** loop the following conditions hold:

(i) G is a finite generating set for (F),

(ii) For every $g_1, g_2 \in G$ with $\{g_1, g_2\} \notin B$, $S(g_1, g_2) \xrightarrow[G]{*} 0$.

If this is the case, when the algorithm terminates, we have $B = \emptyset$, so by Theorem 3.16 the output of the algorithm is a Gröbner basis for (F). (i) holds for the fact that G is initialized as F (hence is a basis for (F)) and the fact that the polynomials we add are algebraic combinations of the elements of F. (ii) is true because of Lemma 3.20 and Proposition 3.21. ■

Remark 3.24. Using the Ascending Chain Condition in order to prove termination for this algorithm, does not provide hints about its complexity, which is still an open problem for algorithms that are meant to compute a Gröbner basis of a set of polynomials.

One of the key factors in estimating the complexity for this algorithm (and for others in this family), is the degrees of the elements in the Gröbner basis that is produced. Say, for example, that for an ideal I every set of generators contains an element f of degree D. In that case, dividing $S(g,h)$ by f may require up to $O\left(\left(\!\binom{n}{d}\!\right)\left(\!\binom{n}{D}\!\right)\right)$ operations, where $d = \deg(S(g,h))$.

The natural parameters that are generally considered in the literature in order to establish the complexity of computing a Gröbner basis are the size of the input, the degree of the input polynomials, the number of variables, and - for large fields - the size of the coefficients.

There is no general theory that provides a formula to compute the degrees of the polynomials appearing in the computations of the Buchberger algorithm (or any other algorithm that is able to compute a Gröbner basis). It is possible, though, to establish a lower bound.

Theorem 3.25 (Theorem II in [Huy86])**.** *For every positive integer m, there exists a family $F \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ with bounded degree and of cardinality $O(m)$ such that any Gröbner basis of the ideal (F) contains at least 2^{2^m} elements and there exists at least one element with degree 2^{2^m}.*

Under certain conditions, though, it is possible to establish an upper bound for the degree of the elements appearing in certain Gröbner bases. An example in this sense is given by the classical theorem by Lazard.

Theorem 3.26 (Theorem 3 in [Laz83]). *Let $I = (f_1, \ldots, f_m) \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ be an ideal, with $m \geq n$ and $\deg(f_i) \geq \deg(f_{i+1})$. Let $\overline{I} = (f_1^h, \ldots, f_m^h)$ be the ideal generated by the homogenisation of $f_1, \ldots, f_m$. If $\overline{I}$ is zero dimensional (i.e. $Z(\overline{I}) \subseteq \overline{K}^n$ is finite), then the elements of any reduced Gröbner basis for the graded reverse lexicographic order have degree at most $d_1 + \cdots + d_{n+1} - n + 1$, with $d_{n+1} = 1$ if $n = m$.*

This result alone does not give a precise bound for the complexity of a Gröbner basis algorithm, for higher degree polynomials can appear in the computations before reduction. Nonetheless, the theorem was adapted in [CG17] to tackle this issue:

Theorem 3.27 (Corollary 3.26 in [CG17]). *Let $I = (f_1, \ldots, f_m)$ be an ideal of $\mathbb{F}_q[x_1, \ldots, x_n]$. Let $\overline{I} = (f_1^h, \ldots, f_m^h)$. If $\overline{I}$ is zero dimensional, then all the polynomials appearing in the computation of a Gröbner basis for I have degree smaller than or equal to $d_1 + \cdots + d_m - m + 1$.*

In the next two sections we define the concept of degree of regularity - which is tightly related with Lazard's work - and show how one can use it to estimate the complexity of a Gröbner basis algorithm.

3.3 Degree of Regularity

Let $I \subseteq R = \mathbb{F}_2[x_1, \ldots, x_n]$ be a homogeneous ideal containing $x_1^2, \ldots, x_n^2$. The degree of regularity of I is a term introduced in [BFS03], defined as the smallest degree d for which $(R/I)_d = 0$. Although the term was used for the first time by Bardet, Faugère, and Salvy, the concept describes the smallest degree for which the coefficients of the Hilbert series of a graded algebra related to the ideal vanish.

The definition can be naturally adapted to any field K. As a consequence, we also lift the condition that $x_1^2, \ldots, x_n^2 \in I$.

Definition 3.28. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. Let I be a homogeneous ideal of R. The *degree of regularity* (d_{reg}) of I is the smallest d for which $(R/I)_d = 0$.

Let $P_1,\dots,P_m \in R$. The degree of regularity of the sequence $P_1,\dots,P_m$ is the degree of regularity of the homogeneous ideal I generated by the leading forms of $P_1,\dots,P_m$.

The degree of regularity is not defined for every homogeneous ideal. If that is the case, we say that such ideal *does not admit a degree of regularity*.

Example 3.29. Let $I = (x,yz) \subseteq R = K[x,y,z]$. It is easy to see that $y^d, z^d \in R_d \setminus I_d$ for every d. Therefore, I does not admit a degree of regularity.

Proposition 3.30. *Let $I \subseteq R = K[x_1,\dots,x_n]$ be a homogeneous ideal. Then I admits a degree of regularity if and only if there exists d such that $x_i^d \in I$ for every $i = 1,\dots,n$.*

Proof. Assume that there exists a degree of regularity d_{reg} for I. Then $x_i^{d_{\text{reg}}} \in I$ for every $i = 1,\dots,n$. On the other hand, if there exists d such that $x_i^d \in I$ for every i, then every monomial in R_{nd} is a multiple of at least one of the x_i^d. This means that $R_{nd}/I_{nd} = 0$. ∎

As mentioned above, the degree of regularity has deep connections with the Hilbert series of a graded algebra.

Definition 3.31. ([Sta78]) Let $A = \bigoplus_d A_d$ be a graded K-algebra such that each A_d is a finite dimensional K-vector space. The *Hilbert function* of A is the function $H_A : \mathbb{N} \to \mathbb{N}$ sending $d \mapsto \dim_K(A_d)$. The *Hilbert series* of A is the polynomial series $HS_A(t) = \sum_{i\geq 0} H_A(i)t^i$.

Proposition 3.32. *Let $I \subseteq R$ be a homogeneous ideal. Then $H_{R/I}(d) = H_R(d) - \dim(I_d)$.*

Proof. By Proposition 2.16, $(R/I)_d \cong R_d/(I \cap R_d)$. By the definition of Hilbert function, we have:

$$\begin{aligned}\dim((R/I)_d) &= \dim(R_d/(R_d \cap I)) = \\ &= \dim(R_d) - \dim(R_d \cap I) = H_R(d) - \dim(I_d),\end{aligned}$$

since $R_d \cap I = I_d$, the degree d part of I. ∎

Example 3.33. Let $R = \mathbb{F}_q[x_1,\dots,x_n]$ and let us consider the $\mathbb{F}_q$-algebra $R^h = R/(x_1^q,\dots,x_n^q)$. First we notice that by Proposition 2.24 and Proposition 2.39, $H_R(d) = \left(\!\binom{n}{d}\!\right)$. In order to compute the Hilbert function of R^h it is sufficient to study the dimension of the homogeneous components of $I = (x_1^q,\dots,x_n^q)$. Clearly,

$$\dim(I_d) = |\{x_1^{a_1}\dots x_n^{a_n} | \sum_i a_i = d, a_j \geq q \text{ for some } j\}|.$$

By Proposition 3.32,

$$H_{R^h}(d) = \left(\!\binom{n}{d}\!\right) - \dim(I_d) = |\{x_1^{a_1}\dots x_n^{a_n} | \sum_i a_i = d, 0 \leq a_i < q\}|.$$

In particular, if $d > (q-1)n$, then $H_{R^h}(d) = 0$.

Corollary 3.34. *Let $R = \mathbb{F}_q[x_1,\dots,x_n]$ and let I be a homogeneous ideal. The degree of regularity of I is the smallest i for which $H_{R/I}(i) = 0$.*

The degree of regularity of a system is sometimes used to assess the complexity of computing a Gröbner basis for that system. When it was first introduced, the authors claimed that the largest polynomials appearing in the Gröbner basis computation for that system are of degree d_{reg}. This holds for homogeneous systems, but no evidence was presented in the general case and it is easy to find counterexamples to this statement.

Example 3.35. Let us consider the following sequence in $\mathbb{F}_2[x,y,z]$:

$$P_1 = xy + 1, \quad P_2 = xz, \quad P_3 = yz, \quad P_4 = x^2 - x, \quad P_5 = y^2 - y, \quad P_6 = z^2 - z.$$

The degree of regularity is 2, as the ideal I generated by the leading forms of $P_1,\dots,P_6$ is such that $I_2 = \mathbb{F}_2[x,y,z]_2$. On the other side, $z \in (P_1,\dots,P_6)$, as $z = zP_1 + yP_2$, but in order to find it, it is necessary to compute a polynomial of degree 3.

Such situations are not specifically crafted to disprove the claim: this can happen in some applications in cryptology, as pointed out by Caminata and Gorla in [CG17] with an example coming from elliptic curve cryptography.

In general, the degree of regularity of a sequence is hard to compute. Unless one assumes that the sequence has specific properties, it is required to compute the so called Macaulay Matrix, introduced by Macaulay ([Mac16]) as a tool to eliminate variables from a set of generators.

Definition 3.36. Let $f_1,\dots,f_m$ be a sequence of homogeneous polynomials in $R = K[x_1,\dots,x_n]$. The *Homogeneous Macaulay matrix* of degree d of the sequence is the matrix $\overline{M}_d$ with entries in K such that:

(i) the columns of $\overline{M}_d$ are indexed by the monomials of degree d in R,

(ii) the rows of $\overline{M}_d$ are indexed by all the pairs (x^α, f_j), where x^α is a monomial such that $|\alpha| + \deg(f_j) = d$. The entries of the row indexed by (x^α, f_j) are the coefficients of $x^\alpha f_j$.

Example 3.37. Let us consider homogeneous polynomials in $K[x,y,z]$ $f_1 = x + y$ and $f_2 = xy + yz$. The homogeneous Macaulay matrices of degree 2 and 3 of f_1, f_2 are

$$\overline{M_2} = \begin{array}{c} \\ xf_1 \\ yf_1 \\ zf_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & xz & y^2 & yz & z^2 \end{array} \\ \left(\begin{array}{cccccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \end{array}$$

$$\overline{M_3} = \begin{array}{c} \\ x^2f_1 \\ xyf_1 \\ xzf_1 \\ y^2f_1 \\ yzf_1 \\ z^2f_1 \\ xf_2 \\ yf_2 \\ zf_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^3 & x^2y & x^2z & xy^2 & xyz & xz^2 & y^3 & y^2z & yz^2 & z^3 \end{array} \\ \left(\begin{array}{cccccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \end{array}$$

Proposition 3.38. *Let $I = (f_1, \ldots, f_m) \subseteq K[x_1, \ldots, x_n]$ be a homogeneous ideal with homogeneous f_i. Then d_{reg} - if it exists - is the smallest integer d for which $\overline{M}_d$ has linearly independent columns.*

Proof. First we prove that I_d is generated (as a K-vector subspace) by $\{x^\alpha f_j \,|\, |\alpha| + \deg(f_j) = d\}$. Clearly all the vectors in the set belong to I_d, as they are in the ideal I and of degree d.

On the other hand, for $g \in I_d$, we have that

$$g = \sum_\alpha a_\alpha x^\alpha f_1 + \cdots + \sum_\alpha a_\alpha x^\alpha f_m,$$

with $a_\alpha \in K$ and x^α monomials in $K[x_1, \ldots, x_n]$.

Without loss of generality, we can assume that each product $x^\alpha f_j$ has degree d, since I is homogeneous. The inclusion follows from the fact that each of the x^α in the sum of the polynomial f_j has degree exactly $d - \deg(j)$, since the polynomials $f_1, \ldots, f_m$ are homogeneous.

To conclude, $\overline{M}_d$ is the matrix whose rows generate I_d in R_d. Therefore, $I_d = R_d$ if and only if $\overline{M}_d$ has rank equal to the number of its columns. ■

The previous proposition shows that one can compute the degree of regularity of an ideal by constructing $\overline{M}_d$ for increasing d until the matrix has the right rank. It is possible to be certain of the existence of the degree of regularity if an ideal already includes among its generators one polynomial of the form $x_i^{d_i}$ for each $i = 1, \ldots, n$, as per Proposition 3.30.

It is not known, so far, a way to predict the degree of regularity of a sequence of homogeneous generators without computing the Macaulay matrix first. Though, some partial results were already provided in [BFS03]. These involve the so-called semiregular sequences. Unfortunately, with the mathematical tools currently at our disposal, determining whether a sequence is semiregular or not requires the construction of the Macaulay matrices. However, it is conjectured that random sequences with some constraints on the parameters (e.g. number of polynomials, their degree) are actually semiregular (see e.g. [BFS03] and [HMS17]).

Definition 3.39 ([BFS03])**.** Let $I = (f_1,\dots,f_m,x_1^2,\dots,x_n^2) \subseteq R = \mathbb{F}_2[x_1,\dots,x_n]$ be an ideal with homogeneous f_i and degree of regularity d_{reg}. We say that the sequence $f_1,\dots,f_m,x_1^2,\dots,x_n^2$ is a *semiregular sequence* if

- $I \neq R$,
- For $i = 1,\dots,m$, if $gf_i = 0$ in $R/(f_1,\dots,f_{i-1},x_1^2,\dots,x_n^2)$ and $\deg(gf_i) < d_{\text{reg}}$ then $g = 0$ in $R/(f_1,\dots,f_{i-1},f_i,x_1^2,\dots,x_n^2)$.

Theorem 3.40 (Corollary 7 in [BFS03])**.** *Let $d_i = \deg(f_i)$. The Hilbert series of a semi-regular sequence $f_1,\dots,f_m,x_1^2,\dots,x_n^2$ is*

$$HS_I(t) = \left[\frac{(1+t)^n}{\prod_{i=1}^m (1+t^{d_i})}\right],$$

where $[\sum_i a_i t^i] = \sum_i b_i t^i$, with $b_i = a_i$ if $a_i > 0$ and $b_i = 0$ otherwise.

3.3.1 The non homogeneous case

Using the language of graded algebras, it is possible to generalise the concept of Macaulay matrices. This is going to be especially useful, for it allows to work with arbitrary quotients of the polynomial ring.

Let $B = \bigoplus_d B_d$ be a graded K-algebra over the field K such that $\dim(B_d)$ is finite for every d and let $\varphi : B \to A$ be a surjective homomorphism of K-algebras. Then we can associate to each element $a \in A$, the natural number $\deg(a) = \min\{\deg(b) | b \in \varphi^{-1}(a)\}$. We call the map φ a *semigrading* on A (or, equivalently, we say that A is a *semigraded algebra*) and we denote by A_d the set $\{a \in A | \deg(a) \leq d\}$.

Proposition 3.41. *Let $\varphi : B \to A$ be a semigrading on A. Then A is a filtered algebra, i.e. $A = \bigcup_{d\geq 0} A_d$, every A_d is a K-module, and $A_i A_j \subseteq A_{i+j}$.*

Proof. The first condition is satisfied, since φ is surjective. We prove that A_d are K-modules. Let $a, b \in A_d$, then there exist $x, y \in B$ such that $\varphi(x) = a$ and $\varphi(y) = b$ with $\deg(x), \deg(y) \leq d$. In particular $x + y$ has degree $\leq d$ and is mapped to $a + b$ by linearity. Hence $\deg(a + b) \leq d$.

In order to prove the last condition, let us consider $a \in A_i$ and $b \in A_j$. By definition, there exist $x, y \in B$ with $\deg(x) = i$, $\varphi(x) = a$, $\deg(y) = j$, and $\varphi(y) = b$. Since φ is a map of algebras, $\varphi(xy) = ab$. Since B is graded, $\deg(xy) \leq i + j$ and, by definition of degree in semigraded algebras, $\deg(ab) \leq i + j$. ■

Example 3.42. Let I be an ideal (not necessarily homogeneous) of the graded K-algebra $R = K[x_1, \ldots, x_n]$. Then the projection $\pi : R \to R/I$ is a semigrading.

Definition 3.43. Let A be a semigraded K-algebra. A linear *filtered basis* for A is a filtration $\mathcal{B}_0 \subseteq \mathcal{B}_1 \subseteq \ldots$ such that

$$\mathcal{B} = \bigcup_{i \geq 0} \mathcal{B}_i$$

is a basis of A (as a K-vector space) and such that $\mathcal{B}_i$ is a basis for A_i (as a K-vector space).

Every filtered algebra admits filtered bases, since every set of linearly independent vectors in a space can be completed to form a basis.

Proposition 3.44. *Let A be a semigraded K-algebra and let $\mathcal{B} = \bigcup_{i \geq 0} \mathcal{B}_i$ be a filtered basis for A. If $b \in \mathcal{B}_i \setminus \mathcal{B}_{i-1}$, then $\deg(b) = i$.*

Proof. Clearly, $\deg(b) \leq i$, otherwise the linear span of $\mathcal{B}_i$ would contain more than A_i. On the other hand, suppose by contradiction that $\deg(b) < i$. Then $b \in A_{i-1}$ and that implies $\{b\} \cup \mathcal{B}_{i-1}$ is not a linearly independent set. Hence $\mathcal{B}_i$ is not a basis. So $\deg(b) = i$. ■

Proposition 3.45. *Let us consider the K-linear maps*

- $\cdot : A_d \otimes A_{d'} \to A_{d+d'}$ *the product in A,*
- $\pi : A_{d+d'} \to A_{d+d'} / A_{d+d'-e}$ *the canonical projection for some $e < d$,*
- $\pi \otimes \mathrm{Id} : A_d \otimes A_{d'} \to A_d / A_{d-e} \otimes A_{d'}$, *the canonical projection on the first coordinate.*

Then there is a well defined K-linear map $\psi : A_d/A_{d-e} \otimes A_{d'} \to A_{d+d'}/A_{d+d'-e}$ *such that*

$$\begin{array}{ccc} A_d \otimes A_{d'} & \longrightarrow & A_{d+d'} \\ \downarrow & & \downarrow \\ A_d/A_{d-e} \otimes A_{d'} & \xrightarrow[\psi]{} & A_{d+d'}/A_{d+d'-e} \end{array}$$

commutes.

Proof. The map ψ is the unique linear map induced by the bilinear map $\xi : A_d/A_{d-e} \times A_{d'} \to A_{d+d'}/A_{d+d'-e}$ defined by $\xi(f + A_{d-e}, g) = \pi(fg)$. In order to complete the proof we need to show that ξ is bilinear and well defined. First we prove bilinearity:

$$\begin{aligned} \xi(f + f' + A_{d-e}, g) &= \pi((f+f')g) = \pi(fg + f'g) = \pi(fg) + \pi(f'g), \\ \xi(f + A_{d-e}, g + g') &= \pi(f(g+g')) = \pi(fg + fg') = \pi(fg) + \pi(fg'). \end{aligned}$$

ξ is also well defined: let f, f' be such that $f - f' \in A_{d-e}$. Then

$$\xi(f + A_{d-e}, g) - \xi(f' + A_{d-e}, g) = \pi(fg) - \pi(f'g) = \pi((f-f')g) = 0,$$

since $A_{d-e}A_{d'} \subseteq A_{d+d'-e}$. ∎

Definition 3.46. Let A be a semigraded K-algebra. Let $f_1, \ldots, f_m$ be a family of elements in A and let $\mathcal{B}$ be a filtered basis for A. The *Macaulay matrix* of $f_1, \ldots, f_m$ of degree d is defined as a matrix M_d whose columns are labelled by the elements of $\mathcal{B}_d$ and whose rows are labelled by all the pairs (a_α, f_j), where a_α runs over all the elements of $\mathcal{B}_{d-\deg(f_j)}$. The row labelled by (a_α, f_j) is the representation of the vector $a_\alpha f_j \in A_d$ with respect to the basis $\mathcal{B}_d$.

Example 3.47. Let $A = K[x,y]/(x^2 - x)$ with the semigrading given by the canonical projection from $K[x,y]$ and equipped with basis $\mathcal{B} = \{y^s, xy^s\}_{s \geq 0}$. Let

$$f_1 = xy + x, \qquad f_2 = y^2 + y + 1.$$

The Macaulay matrix of degree 3 is

$$M_3 = \begin{array}{c} \\ xf_1 \\ yf_1 \\ xf_2 \\ yf_2 \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} xy^2 & y^3 & xy & y^2 & x & y & 1 \end{array} \\ \left(\begin{array}{ccc|cccc} 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right) \end{array}$$

One can think of the Macaulay matrix of $f_1, \ldots, f_m$ as the representation of the function

$$M_d : \bigoplus_{i=1}^{m} A_{d-\deg(f_i)} \to A_d,$$

sending $(p_1, \ldots, p_m) \mapsto f_1 p_1 + \cdots + f_m p_m$, under the filtered basis $\mathcal{B}$.

It is natural to consider the composition $\overline{M}_d$

$$\begin{array}{ccc} \bigoplus_{i=1}^{m} A_{d-\deg(f_i)} & \xrightarrow{M_d} & A_d \\ & \searrow^{\overline{M}_d} & \downarrow \pi \\ & & A_d / A_{d-1}, \end{array}$$

sending $(p_1, \ldots, p_m) \mapsto \pi(f_1 p_1 + \cdots + f_m p_m) = \pi(p_1 f_1) + \cdots + \pi(p_m f_m)$. The composition $\overline{M}_d$ is called the *homogeneous Macaulay matrix* of degree d of $f_1, \ldots, f_m$.

Definition 3.48. Let A be a semigraded algebra with a filtered basis $\mathcal{B}$. Let $f_1, \ldots, f_m \in A$. The *degree of regularity* d_{reg} of $f_1, \ldots, f_m$ is the smallest integer d for which the composition $\overline{M}_d$ is surjective. If no such d exists, we say that the set $\{f_1, \ldots, f_m\}$ does not admit a degree of regularity.

As $\overline{M}_d$ represents a linear transformation between spaces, a change of basis does not influence the dimension of the image. This, in particular, means that d_{reg} does not depend on the basis $\mathcal{B}$.

Example 3.49. Using the same polynomials of Example 3.47, the degree of reg-

ularity of f_1, f_2 is at most 3, as $\overline{M_3}$ has rank $2 = \dim(A_3/A_2)$.

On the other hand, the set $\{f_1\}$ does not admit a degree of regularity, since for every d, $\dim(A_d/A_{d-1}) = 2$, while $\pi(y^{d-3}xf) = \pi(y^{d-3}f) = 0$, so $\overline{M}_d$ for $\{f_1\}$ has rank 1 for every d.

Proposition 3.50. *Let $d_i = \deg(f_i)$ and let $\pi_i : A_{d_i} \to A_{d_i}/A_{d_i-1}$ be the canonical projections. The degree of regularity of $f_1, \ldots, f_m$ depends only on $\pi_1(f_1), \ldots, \pi_m(f_m)$.*

Proof. Let us consider $f_1', \ldots, f_m'$ such that $\pi_i(f_i - f_i') = 0$ for every i. Let $\overline{M}_d$ be the homogeneous Macaulay matrix generated by $f_1, \ldots, f_m$ and let $\overline{M}_d'$ be the one generated by $f_1', \ldots, f_m'$. We claim that for any $p = (p_1, \ldots, p_m) \in \bigoplus_{i=1}^m A_{d-\deg(f_i)}$, $\overline{M}_d(p) = \overline{M}_d'(p)$. By definition of the homogeneous the Macaulay matrix it is sufficient to show that for every i, $\pi(p_i f_i) = \pi(p_i f_i')$. Since $p_i \in A_{d-d_i}$ and $f_i, f_i' \in A_{d_i}$, by Proposition 3.45 we have

$$\pi(p_i f_i) = \psi(p_i \otimes \pi_i(f_i)) = \psi(p_i \otimes \pi_i(f_i')) = \pi(p_i f_i').$$

■

As in the homogeneous case, one can connect the degree of regularity with the smallest degree d at which the Hilbert series of a graded algebra vanishes.

Let U be a filtered algebra. The *associated graded algebra* of U is $G(U) = \bigoplus_{d \geq 0} U_d/U_{d-1}$, with $U_{-1} = 0$ equipped with a product defined as follows. Let $u + U_{n-1} \in U_n/U_{n-1}$ and $v + U_{m-1} \in U_m/U_{m-1}$, then $(u + U_{n-1})(v + U_{m-1}) = uv + U_{m+n-1}$.

Definition 3.51. Let $f \in A$ an element of a semigraded algebra. Let $d = \deg(f)$ and let $\pi_d : A_d \to A_d/A_{d-1}$. The *leading form* of f is f^L, the image of $\pi_d(f)$ in $G(A)_d$.

Proposition 3.52. *The degree of regularity of $f_1, \ldots, f_m \in A$ is the smallest d for which $H_{G(A)/J}(d) = 0$, where J is the homogeneous ideal generated by $f_i^L \in G(A)$ for $i = 1, \ldots, m$.*

Proof. In order to prove the proposition, it is enough to show that for any d, $\mathrm{rk}(\overline{M}_d) = \dim(G(A)_d)$ is equivalent to $(G(A)/J)_d = 0$. Since J is a homoge-

neous ideal, $(G(A)/J)_d = 0$ if and only if $G(A)_d = J_d$, thanks to Proposition 3.32. It suffices to show $J_d = \mathrm{Im}(\overline{M}_d)$ for every d to prove the statement.

First, let $g \in J_d$, then $g = \sum_i a_i f_i^L$ for some $a_i \in A_{d-\deg(f_i)}/A_{d-\deg(f_i)-1}$. For every $i = 1,\ldots,m$, let p_i be any preimage of a_i in $A_{d-\deg(f_i)}$. Then $\overline{M}_d(p_1,\ldots,p_m) = g$, as the multiplication map $\cdot : A_{d-\deg(f_i)} \otimes A_{\deg(f_i)} \to G(A)_d$ factors through $G(A)_{d-\deg(f_i)} \otimes G(A)_{\deg(f_i)}$:

$$\begin{array}{ccc} A_{d-\deg(f_i)} \otimes A_{\deg(f_i)} & \longrightarrow & G(A)_d \\ \downarrow & \nearrow & \\ G(A)_{d-\deg(f_i)} \otimes G(A)_{\deg(f_i)} & & \end{array}$$

by applying Proposition 3.45 twice. Hence $\mathrm{Im}(\overline{M}_d) \supseteq J_d$.

On the other hand using the same factorisation, $\pi_d(p_i f_i) = a_i \pi_i(f_i) = a_i f_i^L$. This shows that $\mathrm{Im}(\overline{M}_d) \subseteq J_d$ and the proof is complete. ∎

This allows us to establish a relationship between the degree of regularity of $f_1,\ldots,f_m$ in $K[x_1,\ldots,x_n]/(g_1,\ldots,g_t)$ and the degree of regularity of $f_1,\ldots,f_m,g_1,\ldots,g_t \in K[x_1,\ldots,x_n]$:

Theorem 3.53. *Let $f_1,\ldots,f_m,g_1,\ldots,g_t \in R = K[x_1,\ldots,x_n]$ and $J = (g_1,\ldots,g_t)$. If $f_1,\ldots,f_m,g_1,\ldots,g_t$ admits a degree of regularity d_{reg}, then $f_1 + J,\ldots,f_m + J$ admits a degree of regularity d'_{reg} in R/J. Moreover, if d_{reg} exists, then $d_{reg} \geq d'_{reg}$.*

Proof. Let $I = (f'_1,\ldots,f'_m,g'_1,\ldots,g'_t)$ be the ideal generated by the unique homogeneous polynomials f'_i and g'_i such that $f_i - f'_i \in R_{\deg_{f_i}-1}$ and $g_i - g'_i \in R_{\deg_{g_i}-1}$. Let $\overline{I}$ be the ideal generated by all the $(f_i + J)^L$ in $G(R/J)_{\deg(f_i+J)}$. We claim that $H_{R/I}(d) = 0$ implies that $H_{G(R/J)/\overline{I}}(d) = 0$. By Proposition 3.52, this implies the theorem.

First, we notice that $H_{G(R/J)/\overline{I}}(d) = 0$ is equivalent to $G(R/J)_d \subseteq \overline{I}_d$, as $\overline{I}$ is a homogeneous ideal of $G(R/J)$. Let us consider the linear map $\psi : R_d \to G(R/J)_d$ sending a homogeneous polynomial g to $(g + J) + (R/J)_{d-1}$. We claim that this map is surjective. Indeed, let $(f + J) + (R/J)_{d-1}$ be an element of $G(R/J)_d$ with $f \in \bigoplus_{i=0}^d R_i$ not necessarily homogeneous. We can decompose

uniquely $f = f' + f''$, with $f' \in R_d$ and f'' of degree lower than d. Then

$$\psi(f') = (f + J) + (R/J)_{d-1} - (f'' + J) + (R/J)_{d-1} = (f + J) + (R/J)_{d-1},$$

as $f'' + J$ has a representative in R of degree smaller than d, so it lies in $(R/J)_{d-1}$. Let d be such that $H_{R/I}(d) = 0$. Let $a \in G(R/J)_d$; we show that $a \in \overline{I_d}$. Since ψ is surjective and $R_d = I_d$, there exist $a_i, b_j \in R$ such that

$$\begin{aligned} a =& (\sum_i a_i f_i' + J) + (\sum_j b_j g_j' + J) + (R/J)_{d-1} = (\sum_i a_i f_i' + J) + (R/J)_{d-1} = \\ =& (\sum_i a_i f_i + J) + (R/J)_{d-1} = \\ =& \sum_i \Big((a_i + J + (R/J)_{d-\deg(f_i)-1})(f_i + J + (R/J)_{\deg(f_i)-1}) \Big) + (R/J)_{d-1} \in \overline{I}_d, \end{aligned}$$

as claimed, since $f_i + J + (R/J)_{\deg(f_i)-1} = (f_i + J)^L$. The second equality follows from the fact that for every j, $b_j g_j' + J$ has a representative of degree $< d$, namely $b_j g_j' - b_j g_j$.

Therefore, if $H_{R/I}(d) = 0$ then $H_{G(R/J)/\bar{I}}(d) = 0$. This means if d_{reg} exists, then d'_{reg} exists as well and $d_{\text{reg}} \geq d'_{\text{reg}}$. ■

Definition 3.54. We say that an ideal $I \subseteq R$ is *zero-dimensional* if $Z(I) \subseteq \overline{K}^n$ is finite.

Zero-dimensional ideals are rather important, for there are good criterion to identify them and because they have nice computational properties, e.g. the dimension of R/I is finite and one can apply the Shape Lemma (given some additional hypothesis) to find $Z(I)$.

Proposition 3.55 ([KR00], Proposition 3.7.1)**.** *Let I be an ideal of R equipped with any monomial ordering $\leq$. The following are equivalent.*

(i) I is zero-dimensional.

(ii) For $i = 1, \ldots, n$, $I \cap K[x_i] \neq (0)$.

(iii) The K-vector space R/I has finite dimension.

(iv) There exists d such that $x_i^d \in \mathrm{LM}(I)$ for every $i = 1, \ldots, n$.

Proposition 3.56. *Let $I = (f_1, \ldots, f_m) \subseteq R$. If $f_1, \ldots, f_m$ admits a degree of regularity, then I is zero-dimensional.*

Proof. Let $f_1^L, \ldots, f_m^L$ be the leading forms of $f_1, \ldots, f_m$. By Proposition 3.30, there exists d such that for $i = 1, \ldots, n$, $x_i^d = \sum_{j=1}^m a_{i,j} f_j^L$, $a_{i,j} \in R$. This means that the polynomial $g_i = \sum_{j=1}^n a_{i,j} f_j$ has as leading monomial x_i^d. By Proposition 3.55, the ideal $I = (f_1, \ldots, f_m)$ is zero-dimensional. ■

The opposite is, though, not true, as the following example shows:

Example 3.57. Let us consider the sequence $xy - x, y \in K[x, y]$. The ideal I generated by these two polynomials is zero dimensional, as $x, y \in I$. On the other hand, for every d, $\mathrm{Im}(\overline{M}_d)$ does not contain x^d and so the sequence does not admit a degree of regularity.

Example 3.58. Let us consider $xy - x \in K[x, y]/(y)$. Such sequence has degree of regularity 1, as $-xy + x$ and x represent the same element in $K[x, y]/(y)$.

Remark 3.59. These examples enhance Theorem 3.53, as they are witnesses of the fact that $f_1 + J, \ldots, f_m + J$ in R/J can admit a degree of regularity even though $f_1, \ldots, f_m, g_1, \ldots, g_t$ does not admit one in R.

Moreover, this offers a solid framework for some probabilistic analysis: say that from an application, we get an ideal $(f_1, \ldots, f_m, g_1, \ldots, g_t)$, where $g_1, \ldots, g_t$ are fixed in every instance of the application, while $f_1, \ldots, f_m$ are randomly chosen. Given a good knowledge of $R/(g_1, \ldots, g_t)$, it is possible to perform a probabilistic analysis on the degree of regularity of $(f_1, \ldots, f_m, g_1, \ldots, g_t)$ without taking into account the portion of $\overline{M}_d$ induced by the non-random part.

Proposition 3.60. *Let $J \subseteq R$ be a zero-dimensional ideal. Then every sequence of polynomials in R/J admits a degree of regularity.*

Proof. By Proposition 3.55, R/J has finite dimension. This means that there exists d, for which $(R/J)_d = (R/J)_{d-1}$. For such d, $\dim_K((R/J)_d/(R/J)_{d-1}) = 0$ and for every choice of $\{f_1, \ldots, f_m\} \subseteq R/J$, its associated function $\overline{M}_d$ is surjective. ■

Corollary 3.61. *Let $f_1,\dots,f_m \in \mathbb{F}_q[x_1,\dots,x_n]/(x_1^q - x_1,\dots,x_n^q - x_n)$. Then the sequence $f_1,\dots,f_m$ admits a degree of regularity.*

Proof. By Proposition 3.60, it is sufficient to prove that $(x_1^q - x_1,\dots,x_n^q - x_n) \subseteq \overline{\mathbb{F}}_q[x_1,\dots,x_n]$ has finitely many solutions. Thanks to Remark 2.9, $Z(x_1^q - x_1,\dots,x_n^q - x_n) = \mathbb{F}_q^n \subseteq \overline{\mathbb{F}}_q$, which is finite. ■

Our goal is to use the degree of regularity of a system of generators $f_1,\dots,f_m$ to estimate the complexity of computing the Gröbner basis of the ideal $(f_1,\dots,f_m)$. The main reason for that is that it only depends on the leading forms and, therefore, one can work only on $\overline{M}_d$ and a probabilistic bound (i.e. that applies in a fraction of the cases) can be taken over the space of the leading forms instead of the space of all the possible polynomials.

3.3.2 Notation in the literature

In the literature, one can find the use of the phrase "degree of regularity" to refer to several different concepts that are not necessarily related to each other, if not by heuristical arguments based on experiments performed for small parameters (most importantly in [DS13]).

In e.g. [PQ12] and [HKYY18], the authors use the term degree of regularity to describe the largest degree of the Macaulay matrices one needs to reduce to compute a Gröbner basis. Ding and Schmidt refer to it using *Solving degree* (D_{solv}). By its very definition, the solving degree determines the complexity of finding a Gröbner basis, but it is of difficult usage, for it generally depends on the algorithm used (e.g. F_4 [Fau99] does not build the Macaulay matrix of all the generators at the same time).

In [DG10], Dubois and Gama use the term degree of regularity to describe what is commonly referred to as the *first fall degree* (D_{ff}) in other works (e.g. in [CG17], [HMS17], [HPS14]). The first fall degree can be vaguely defined as the smallest degree d for which there is a nontrivial degree drop. More precisely, using the definition of Ding and Schmidt that applies to quadratic systems over $\mathbb{F}_q$, we have the following:

Definition 3.62. Let $(f_1,\dots,f_m)$ be a sequence of homogeneous quadratic polynomials in $B := \mathbb{F}_q[x_1,\dots,x_n]/(x_1^q,\dots,x_n^q)$. By B_d^m we denote the direct sum of m copies of B_d and we equip it with a standard basis $e_1 = (1,0,\dots,0),\dots,e_m = (0,\dots,0,1)$ (as a B_d-module). Let $\psi_d : B_d^m \to B_{d+2}$ be the linear transformation sending a homogeneous sequence $(p_1,\dots,p_m)$ to $f_1p_1 + \cdots + f_mp_m$. Let T_d be the subspace of $\ker(\psi_d)$ of the trivial syzygies, i.e. the one generated by

$$\{p(f_ie_j - f_je_i) | 1 \le i < j \le m, p \in B_{d-2}\} \qquad \text{(trivial by commutativity of } B\text{)}$$

and by

$$\{p(f_i^{q-1}e_i) | 1 \le i \le m, p \in B_{d-2(q-1)}\}. \qquad \text{(trivial since } f_i^q = 0\text{)}$$

The first fall degree of $f_1,\dots,f_m$ is the smallest d for which $\ker(\psi_{d-2})/T_{d-2} \neq 0$. In the case of $f_1,\dots f_m$ being non homogeneous, the first fall degree of $f_1,\dots,f_m$ is defined as the first fall degree of the sequence given by their leading forms.

The first fall degree is widely used to estimate the complexity to compute the solutions of a system of polynomial equations, especially when it comes to multivariate cryptosystems, as in G*e*MSS [CFMR+17], where the authors use the bound on the first fall degree obtained in [DY13]. The reason for this choice is that as soon as a nontrivial degree drop occurs, one can expect that many more will follow either at D_{ff} or at $D_{ff}+1$.

This is, in general, a very conservative point of view and it is easy to construct systems that have arbitrary solving degree and constant first fall degree. A family of examples is presented in [DS13]:

$$f_1(x_1,\dots,x_n) = g_1(x_1,x_2), \qquad f_2(x_1,\dots,x_n) = g_2(x_1,x_2),$$
$$f_3(x_1,\dots,x_n) = g_3(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n) = g_m(x_1,\dots,x_n).$$

Adjusting g_1 and g_2 it is easy to find a nontrivial degree drop that involves just them. At the same time, by modifying the number of variables and the other polynomials, the solving degree can increase indefinitely.

It is not easy to establish relationships between d_{reg}, D_{ff}, and D_{solv}. As mentioned above, it is accepted as good heuristic that the solving degree and the first fall degree are close for the vast majority of random polynomial systems. This is corroborated by the experiments in [DS13]. It is worth noticing, though, that the authors themselves raise doubts about how large the distance between the two can reach, once the number of variables increases.

There is a more obvious relationship between D_{ff} and d_{reg}: the first fall degree is at most $d_{\text{reg}} + 1$. Indeed, every polynomial in the ideal of degree $d_{\text{reg}} + 1$ can be reduced to a polynomial of degree smaller than d_{reg}.

We will prove a relationship between the solving degree and the degree of regularity in the next section. Even though it is, for most of the experiments performed, not a tight bound, it holds for every system of polynomials and depends on no assumptions, but the fact that the sequence of polynomials of the system admits a degree of regularity.

3.4 Complexity of and finding a solution of a system

In this section, we present the joint work with I. Semaev. This covers section 2 of [ST19a]. The goal is to present an algorithm that takes as input a system of polynomials in $R = \mathbb{F}_q[x_1, \ldots, x_n]$, computes a Gröbner basis according to a total degree ordering of the generators of the system, and finds one of its q-rational roots if they exist and identifies a system with no solutions. The complexity will be expressed as a function of the number of variables and the degree of regularity or the largest degree among the polynomials in the system.

Let $f_1 = 0, \ldots, f_m = 0$ be a system of polynomials in R. By Remark 2.9, the q-rational solutions of the system are the elements of the set $Z(I)$, where $I = (f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n)$. Let us equip R with a total degree monomial ordering and let $J = (x_1^q - x_1, \ldots, x_n^q - x_n) \subseteq R$

The overview of the process is the following:

(i) Compute the Macaulay matrices M_d of the sequence $f_1 + J, \ldots, f_m + J$ for $d \leq d_{\text{reg}}$ in the semigraded algebra $\mathbb{F}_q[x_1, \ldots, x_n]/J$ and put them in re-

duced row echelon form.

(ii) Choose a set of generators B for I for which every elements of B has degree $\leq d_{\text{reg}}$ and every monomial of degree $\geq d_{\text{reg}}$ in R is divisible by at least one monomial in $\text{LM}(B)$. Then perform the Buchberger algorithm on B to obtain a Gröbner basis G satisfying some properties described in Remark 3.66.

(iii) Compute the reduced Gröbner basis of I using G.

(iv) Find a solution of the system or prove that no solutions exist by progressively guessing values for each variable.

We choose as representative of f_i in $R/(x_1^q - x_1, \ldots, x_n^q - x_n)$ the polynomial g_i spanned by the monomials of the form $x_1^{a_1} \ldots x_n^{a_n}$, with $0 \leq a_i < q$ for every i. We assume that $g_1, \ldots, g_m$ are linearly independent. If not one first uses Gaussian reduction on them. Let d_{reg} be the degree of regularity of $f_1, \ldots, f_m \in R/(x_1^q - x_1, \ldots, x_n^q - x_n)$. It exists because of Corollary 3.61.

We denote by $l_q(n,d)$ the number of monomials of degree d in $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ and with $L_q(n,d) = \sum_{i=0}^{d} l_q(n,i)$. Let D be the largest degree among $\deg(g_1), \ldots, \deg(g_m)$. By assumption, $m \leq L_q(n,D)$.

Proposition 3.63. *One can construct a set of generators B for I with the property that the degree of every element in B is smaller than or equal to d_{reg} in*

$$O(d_{reg}^2 L_q(n, d_{reg})^4) + O(L_q(n,D)^2 L_q(n, d_{reg}))$$

operations in $\mathbb{F}_q$.

Proof. For every given degree $d \leq d_{\text{reg}}$ we consider only the polynomials f_i of degree $\leq d$. Hence to compute the matrix M_d we use up to $L_q(n,d)$ polynomials. This means that the Macaulay matrix $M_{d_{\text{reg}}}$ has up to

$$\sum_{i=1}^{d_{\text{reg}}} l_q(n,i) l_q(n, d_{\text{reg}} - i) \leq d_{\text{reg}} L_q(n, d_{\text{reg}})^2$$

rows and has exactly $L_q(n, d_{\text{reg}})$ columns. The matrices M_d for $d < d_{\text{reg}}$ have the same upper bounds on the number of columns and rows.

In order to put in reduced row echelon form all the matrices M_d for $d \leq d_{\text{reg}}$ one requires

$$O(d_{\text{reg}}(d_{\text{reg}} L_q(n,d)^2) L_q(n,d)^2) = O(d_{\text{reg}}^2 L_q(n,d_{\text{reg}})^4)$$

operations.

The ideal I is generated by

$$f_1, \ldots, f_m, U_1, \ldots U_r, x_1^q - x_1, \ldots, x_n^q - x_n,$$

where U_j are the linearly independent polynomials induced by the rows of the reduced row echelon form of $M_{d_{\text{reg}}}$.

There are up to $L_q(n, d_{\text{reg}})$ of them. If $q \leq d_{\text{reg}}$ and $\deg(f_i) \leq d_{\text{reg}}$ for every $i = 1, \ldots, m$, then the proof is complete.

Let assume that $\deg(f_i) > d_{\text{reg}}$. Then one replaces f_i with its remainder after division by $(U_1, \ldots, U_r)$ if $q > d_{\text{reg}}$ or with its remainder after division by $(U_1, \ldots, U_r, x_1^q - x_1, \ldots, x_n^q - x_n)$ if $q \leq d_{\text{reg}}$. This takes up to $L_q(n, \deg(f_i))(L_q(n, d_{\text{reg}}) + n)$ operations, by Proposition 3.10. By hypothesis, $m \leq L_q(n, D)$, where $D = \max_i\{\deg(f_i)\}$ and one has to perform at most m divisions. Overall, for constant q, the complexity becomes

$$O(d_{\text{reg}}^2 L_q(n, d_{\text{reg}})^4) + O(L_q(n, D)^2 L_q(n, d_{\text{reg}})).$$

Lastly, for every i, one has to replace $x_i^q - x_i$ with its remainder after division by $(U_1, \ldots, U_r)$ if $q > d_{\text{reg}}$. In the division algorithm after each outer **while** loop, the intermediate polynomials incorporate only monomials of the form $x_i^b x_1^{a_1} \ldots x_n^{a_n}$, with $b, a_j < q$ for $j = 1, \ldots, n$ and $\sum_j a_j < d_{\text{reg}}$. Therefore, one uses up to $q L_q(n, d_{\text{reg}})$ monomials at each division step. This means that every division requires at most $q L_q(n, d_{\text{reg}})^2$ operations and n divisions are needed. This cost is negligible compared to the cost of performing Gaussian reduction. ■

Remark 3.64. The basis B constructed in Proposition 3.4 has also the following properties:

- Every monomial in R of degree at least d_{reg} is divisible by some $g \in \text{LM}(B)$,
- If $g \in B$, with $\deg(g) = d_{\text{reg}}$, then $\deg(g - LT(g)) < d_{\text{reg}}$.

Theorem 3.65 ([ST19a]). *Let $B = \{Q_1, \ldots, Q_t\} \in R = \mathbb{F}_q[x_1, \ldots, x_n]$ be a set of nonzero generators for I such that every monomial in R is divisible by at least one element from $\text{LM}(B)$, $\deg(Q_i) \leq d_{reg}$, and $\deg(Q_i - \text{LT}(Q_i)) < d_{reg}$ for $i = 1, \ldots, t$. Assuming constant q, the time complexity to construct a Gröbner basis for I with respect to a total degree ordering is*

$$O(L_q(n, d_{reg})^2 L_q(n, d_{reg} - 1)^2 L_q(n, 2d_{reg} - 2)).$$

Proof. Using Buchberger Algorithm, one considers less than $L_q(n, d_{\text{reg}})^2/2$ pairs at every step of the algorithm. The number of nonzero remainders one can get is $\leq L_q(n, d_{\text{reg}} - 1)$. This means that in total one has to compute less than $L_q(n, d_{\text{reg}})^2 L_q(n, d_{\text{reg}} - 1)/2$ divisions.

Each pair (Q_i, Q_j) generates an S-polynomial of degree up to $2d_{\text{reg}} - 2$. Indeed, the S polynomial of the pair $S(Q_i, Q_j)$ has the following shape

$$S(Q_i, Q_j) = \frac{\text{lcm}(\text{LM}(Q_i), \text{LM}(Q_j))}{\text{LT}(Q_i)} Q_i' - \frac{\text{lcm}(\text{LM}(Q_i), \text{LM}(Q_j))}{\text{LT}(Q_j)} Q_j',$$

where $Q_k' = Q_k - \text{LT}(Q_k)$, for $k = i, j$. By Proposition 3.18 we consider only the cases in which

$$\gcd(\text{LM}(Q_i), \text{LM}(Q_j)) \neq 1,$$

so the degree of the quotient is at most $d_{\text{reg}} - 1$. On the other hand, $\deg(Q_i'), \deg(Q_j') < d_{\text{reg}}$ by hypothesis. Therefore, $S(Q_i, Q_j)$ has degree at most $2d_{\text{reg}} - 2$.

Moreover, dividing such S-polynomial by B only requires up to $L_q(n, d_{\text{reg}} - 1)$ outer **while** loops, since for every $g \in B$, $\deg(g - \text{LT}(g)) < d_{\text{reg}}$.

Overall, the cost is the one stated. ■

Remark 3.66. The Gröbner basis G that one gets from Theorem 3.65 has the property that the degree of all its elements is at most d_{reg}. In particular, $|G| \leq L_q(n, d_{\text{reg}})$. Moreover, every monomial in R of degree at least d_{reg} is divisible by $\text{LM}(g)$ for some $g \in G$.

Corollary 3.67. *Let $f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n$ be a sequence of polynomials in $R = \mathbb{F}_q[x_1, \ldots, x_n]$ and let d_{reg} be the degree of regularity of the sequence given by the projections of $f_1, \ldots, f_m$ in $R/(x_1^q - x_1, \ldots, x_n^q - x_n)$. If $\deg(f_i) \leq d_{reg}$ for every i and $q \leq d_{reg}$, then the solving degree (i.e. the largest degree of polynomials appearing in the computation) is $D_{solv} \leq 2d_{reg} - 2$.*

Lemma 3.68. *Let G be a Gröbner basis for an ideal I satisfying the properties of Remark 3.66. Then one can compute a reduced Gröbner basis G' for I in $O(L_q(n, d_{reg})^3)$ operations.*

Proof. Given the Gröbner basis G, we use the algorithm described in Theorem 3.14 to measure the complexity. The first step is to remove all the redundant polynomials by looking at their leading monomials. As $|G| \leq L_q(n, d_{\text{reg}})$, this requires less than $L_q(n, d_{\text{reg}})^2$ monomial divisions. Turning every polynomial into a monic one requires less than $L_q(n, d_{\text{reg}})^2$ divisions in $\mathbb{F}_q$.

Lastly, one needs to perform $|G|$ polynomial divisions and all the monomials involved have degree $\leq d_{\text{reg}}$. This means that each polynomial division requires $\leq L_q(n, d_{\text{reg}})^2$ operations and one requires up to $L_q(n, d_{\text{reg}})$ of them. The overall cost is in $O(L_q(n, d_{\text{reg}})^3)$, as claimed. ■

Theorem 3.69. *Let G be a Gröbner basis for $I = (f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n) \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ satisfying the properties of Remark 3.66. Then one can compute $(a_1, \ldots, a_n) \in Z(I) \subseteq \mathbb{F}_q^n$ or prove $Z(I) = \emptyset$ in $O(nL_q(n, d_{reg})^3)$ operations.*

Proof. We spend $O(L_q(n, d_{\text{reg}})^3)$ operations to compute the reduced Gröbner basis from G, which is negligible with respect to the complexity stated. $G' = \{1\}$ if and only if $Z(I) = \emptyset$. We notice that G' still satisfies the properties of Remark 3.66.

The algorithm we employ is the following. If $G' = \{1\}$, then the system has no solutions. Otherwise, we take $a_n \in \mathbb{F}_q$ and compute the reduced Gröbner basis G'_n of $I + (x_n - a_n)$. If $G'_n = \{1\}$, we take another a_n and compute the reduced Gröbner basis, repeating if necessary until a valid a_n is found. Notice that as $G' \neq \{1\}$, there exists at least one $a_n \in \mathbb{F}_q$ such that $I + (x_n - a_n) \neq \{1\}$. If $G'_n \neq \{1\}$, we replace I with $I + (x_n - a_n)$ and repeat the previous step by guessing the value of x_{n-1}. This repeats until a solution $(a_1, \ldots, a_n)$ is found.

Obviously, the algorithm produces a zero of I if it exists or proves $Z(I) = \emptyset$. One has to compute up to qn reduced Gröbner bases of ideals $J + (x_n - a_n)$. We will now prove that it is possible to compute the reduced Gröbner basis G'_i in $O(L_q(n, d_{\text{reg}})^3)$ operations at any step.

Let $I_{\leq d}$ denote the space of polynomials in I of degree $\leq d$. From the properties of polynomial division and Gröbner basis, we have the following:

Lemma 3.70. *The set of polynomials $x^\alpha g_i$ such that $\deg(g_i) \leq d$ and $|\alpha| + \deg(g_i) \leq d$ generates $I_{\leq d}$ as a vector space over $\mathbb{F}_q$.*

Lemma 3.71. *Let g be a linear polynomial. The vector space $(I + (g))_{\leq d_{reg}}$ is generated by $x^\alpha g_i$ and $x^\beta g$, with $|\alpha| + \deg(g_i) \leq d_{reg}$ and $|\beta| < d_{reg}$.*

Proof. First we show that every $f \in (I + (g))$ may be represented as $f = p + gr$ for some $p \in I$ and r with $\deg(r) < d_{\text{reg}}$. Obviously, $f = f_1 + f_2 g$ with $f_1 \in I$, $f_2 \in \mathbb{F}_q[x_1, \ldots, x_n]$. Let r be a remainder of f_2 after division by G. Then $f_2 = h + r$, where $h \in I$ and $\deg(r) < d_{\text{reg}}$. Hence $f = p + rg$, with $p = f_1 + gh \in I$.

Therefore, $f = p + gr$ is in $(I + (g))_{\leq d_{\text{reg}}}$ if and only if $\deg(p) \leq d_{\text{reg}}$. Hence

$$(I + (g))_{\leq d_{\text{reg}}} \subseteq I_{\leq d_{\text{reg}}} + (g)_{\leq d_{\text{reg}}}.$$

The first subspace is generated by $x^\alpha g_i$ with $|\alpha| + \deg(g_i) \leq d_{\text{reg}}$ thanks to Lemma 3.70. On the other hand, $(g)_{\leq d_{\text{reg}}}$ is trivially generated by $x^\beta g$ with $|\beta| + \deg(g) \leq d_{\text{reg}}$. The proof is complete. ∎

Corollary 3.72. *Let $B = \{b_1, \ldots, b_k\}$ be a basis for the vector space $(I + (g))_{\leq d_{reg}}$ with the property that $\text{LM}(b_i) \neq \text{LM}(b_j)$ for $i \neq j$. Then B is a Gröbner basis for $(I + (g))$.*

Moreover B satisfies the properties of Remark 3.66.

Proof. Obviously, B is a set of generators for $I + (g)$. Let $f \in I + (g)$. If $\deg(f) \leq d_{\text{reg}}$, then $\text{LM}(f) = \text{LM}(b_i)$ for some $b_i \in B$, since B is a linear basis for $(I + (g))_{\leq d_{\text{reg}}}$. If $\deg(f) > d_{\text{reg}}$, then $\text{LT}(f)$ is divisible by $\text{LT}(b_i)$ for some i since by construction $\text{LM}(B)$ contains all the monomials of degree equal to d_{reg}.

Therefore, any leading term of $f \in I + (g)$ is divisible by the leading term of one of the elements in B. Hence the latter is a Gröbner basis for $I + (g)$ and trivially satisfies the properties of Remark 3.66. ■

In order to compute B, one triangulates a matrix with $\leq L_q(n, d_{\text{reg}})$ columns and $\leq L_q(n, d_{\text{reg}})$ rows. So each computation of a reduced Gröbner basis that we perform has a cost of $O(L_q(n, d_{\text{reg}})^3)$ operations. In order to find one zero in $Z(I)$, we need to perform at most qn iterations. Hence the total cost is in $O(nL_q(n, d_{\text{reg}})^3)$ as claimed. ■

Remark 3.73. The algorithm just presented returns only one of the zeros in $Z(I)$. The entire set can be found by using the Shape Lemma after a linear change of coordinates in an extension of $\mathbb{F}_q$. This approach has the drawback that if the system has many solutions, then the extension has a very bulky size and one has to try random linear changes of coordinates in the extension. The full algorithm is described in chapter 3.7 of [KR00].

Chapter 4

Overdetermined systems

In this chapter we present our original work on a probabilistic bound for the degree of regularity for overdetermined systems of polynomials.

Sections 4.1 and 4.2 are based on the joint work with I. Semaev [ST19a]. Here we prove the following theorem:

Theorem 4.1. *Let q and D be fixed. Let $A = \mathbb{F}_q[x_1,\dots,x_n]/(x_1^q - x_1,\dots,x_n^q - x_n)$ and let $P_1,\dots,P_m$ be elements chosen uniformly and independently at random from $G(A)_D$. If there exists $d < D$ such that*

$$m \geq \frac{l_q(n,d+D)}{l_q(n,d)},$$

then

$$\mathbb{P}(d_{reg} \leq d+D) \geq 1 - q^{l_q(n,d+D) - m l_q(n,d)} + O(n^d q^{-Cn^D})$$

for a positive constant C as $n \to \infty$.

The case of $q = 2$, $D = 2$, $d = 1$ was first proved by Semaev [Sem16]. His proof is reported in Section 4.1, as it is a good example of some of the concepts that appear in the generalization, that follows the same line of thought.

Sections 4.3 and 4.4 are devoted to explore the implications of Theorem 4.1 in different contexts in order to expand the set of parameters on which it applies and in order to reduce the cost of computing a Gröbner basis of an ideal with respect to the method presented in [ST19a].

4.1 The case of $q = 2$, $D = 2$, and $d = 1$

Let M be the homogeneous Macaulay matrix of degree 3 of the quadratic homogeneous polynomials $f_1, \dots f_m \in \mathbb{F}_2[x_1, \dots, x_n]/(x_1^2, \dots, x_n^2)$. The columns of M are labelled by triplets rst, with $1 \le r < s < t \le n$. The rows of M are labelled by pairs ij, where $i = 1, \dots, n$, $j = 1, \dots, m$.

Theorem 4.2. *Let p be the probability that the columns of M are linearly dependent. Then*

$$p \le \sum_{v=0}^{n-1} 2^{\binom{n-v}{3}+(n-v+1)v-(n-v)m}.$$

Proof. We represent M as the vertical concatenation of m blocks M_j:

$$M = \begin{pmatrix} M_1 \\ \vdots \\ M_m \end{pmatrix}$$

The rows of M_j contain the coefficients of the cubic homogeneous polynomial $x_i f_j$ for $i = 1, \dots, n$. So M_j is the homogeneous Macaulay matrix of degree 3 of the single polynomial f_j.

Let u be a fixed binary column vector of length $\binom{n}{3}$ with entries u_{irs} and let $p_u = \mathbb{P}(Mu = 0)$. Obviously, $p \le \sum_{u \ne 0} p_u$.

Let p_{uj} denote the probability that $M_j u = 0$. As $Mu = 0$ if and only if $M_j u = 0$ for every j, and M_j are identically and independently distributed, we have

$$p_u = \prod_{j=1}^{m} p_{uj} = p_{u1}^m.$$

Therefore it is sufficient to find an expression for p_{u1}. We represent $M_1 u$ in an equivalent form. Let c denote a vector of length $\binom{n}{2}$ whose entries c_{rs} are the coefficients of the polynomial f_1. Then $M_1 u = 0$ is equivalent to

$$\sum_{r,s \ne j} c_{rs} u_{jrs} = 0, \qquad j = 1, \dots, n.$$

Let $Y^{(u)}$ denote the matrix of size $n \times \binom{n}{2}$, whose rows are indexed by $j = 1, \dots, n$

and the columns by pairs rs, where $1 \le r < s \le n$. The entries of $Y^{(u)}$ are defined by

$$Y^{(u)}_{j,rs} = \begin{cases} u_{jrs}, & \text{if } j \neq r,s, \\ 0 & \text{otherwise.} \end{cases}$$

$M_1 u = 0$ is equivalent to a system of linear equations $Y^{(u)}x = 0$. As u is fixed and the entries of c are uniformly distributed, $\mathbb{P}(Y^{(u)}c = 0) = p_{u1} = 2^{-\operatorname{rk}(Y^{(u)})}$. Then

$$p \le \sum_{u \neq 0} p_u = \sum_{u \neq 0} p_{u1}^m = \sum_{u \neq 0} 2^{-m \operatorname{rk}(Y^{(u)})} = \sum_{v=0}^{n-1} N_v 2^{-m(n-v)},$$

where N_v is the number of vectors u such that $\operatorname{rk}(Y^{(u)}) = n - v$.

Lemma 4.3. *Let s_{nv} be the number of subspaces of dimension v in a $\mathbb{F}_2$-vector space of dimension n. Then $N_v \le s_{nv} 2^{\binom{n-v}{3}}$.*

Proof. Obviously, N_v is upper bounded by the number of vectors u such that $\operatorname{rk}(Y^{(u)}) \le n - v$. The latter holds if there exists a subspace of rows, V, of dimension v such that $b_i Y^{(u)} = 0$ for a basis $b_1, \dots b_v$ of V. Let us fix a subspace V of dimension v and one of its basis $b_1, \dots, b_v$. Denote $b_i = (b_{i1}, \dots, b_{in})$. We look at $b_i Y^{(u)} = 0$, for $i = 1, \dots, v$, as a system of linear equations, the variables of which are the entries of u:

$$\sum_{j \neq r,s} b_{ij} u_{jrs} = 0, \quad 1 \le i \le k, 1 \le r < s \le n. \tag{4.1}$$

We rewrite 4.1 in a matrix form as uA_V, where A_V is a matrix of size $\binom{n}{3} \times v\binom{n}{2}$. The matrix $A_V = (A_1, \dots, A_v)$ is a concatenation of the matrices A_i, which represent $b_i Y^{(u)} = 0$ as a system of linear equations $uA_i = 0$. The matrix A_i is of size $\binom{n}{3} \times \binom{n}{2}$. The number of solutions of $uA_V = 0$ is $2^{\binom{n}{3} - \operatorname{rk}(A_V)}$. Therefore, $N_v \le \sum_{\dim(V)=v} 2^{\binom{n}{3} - \operatorname{rk}(A_V)}$, where the sum is over all subspaces V of dimension v in an $\mathbb{F}_2$-vector space of dimension n. In order to finish the proof of Lemma 4.3, we need to prove

Lemma 4.4. $\operatorname{rk}(A_V) \le \binom{n}{3} - \binom{n-v}{3}$.

Proof. Let B denote the matrix of size $v \times n$, whose rows are the vectors $b_1, \ldots, b_v$. The rank of B is k. One can apply row operations on B to get another basis for V and the number of solutions to 4.1 (and the rank of A_V as well) won't change. Permuting columns by a permutation π is equivalent to reordering the variables u_{jrs} and that does not change the rank of A_V either, as one gets $\sum_{j \neq r,s} b_{i\pi j} u_{\pi(j)\pi(r)\pi(s)} = 0$ from 4.1. Therefore, one can assume that the first v columns in B form the identity matrix, that is

$$B = \begin{pmatrix} 1 & 0 & \ldots & 0 & * & \ldots & * \\ 0 & 1 & \ldots & 0 & * & \ldots & * \\ \vdots & & & & & & \\ 0 & 0 & \ldots & 1 & * & \ldots & * \end{pmatrix}$$

By the definition of $A = A_i$, the entries $A_{jrs,rs} = b_{ij}$ and all other entries of A_i are zeros. As $b_{11} = 1$, the matrix A_1 contains an identity submatrix E_1 in the rows indexed by triplets $1rs$, where $1 < r < s \leq n$ and in the columns indexed by pairs rs, where $1 < r < s \leq n$. Therefore $\mathrm{rk}(A_1) \geq \binom{n-1}{2} = \binom{n}{3} - \binom{n-1}{3}$. As $b_{21} = 0$, the matrix A_2 contains a zero sub-matrix in the same rows and columns, where A_1 contains the above identity submatrix. As $b_{22} = 1$, the matrix A_2 contains an identity submatrix E_2 in the rows indexed by triplets $2rs$ and in the columns indexed by pairs rs, where $2 < r < s \leq n$. These columns in A_2 are linearly independent with the above columns in A_1. Therefore,

$$\mathrm{rk}(A_1|A_2) \geq \binom{n-1}{2} + \binom{n-2}{2} = \binom{n}{3} - \binom{n-2}{3}.$$

We continue this argument. For instance,

$$(A_1|A_2|A_3) = \left(\begin{array}{cc|ccc|cccc} * & E_1 & * & 0 & 0 & * & 0 & 0 & 0 \\ * & * & * & * & E_2 & * & * & 0 & 0 \\ * & * & * & * & * & * & * & * & E_3 \\ * & * & * & * & * & * & * & * & * \end{array}\right),$$

where E_i are identity matrices of size $\binom{n-i}{2} \times \binom{n-i}{2}$.

Finally

$$\mathrm{rk}(A_V) = \mathrm{rk}(A_1|\ldots|A_v) \geq \sum_{i=1}^{v} \binom{n-i}{2} = \binom{n}{3} - \binom{n-v}{3}.$$

That proves Lemma 4.4. ■

The proof of Lemma 4.3 is complete. ■

We return to the proof of the theorem. By Lemma 4.3, we get $p \leq \sum_{v=0}^{n-1} s_{nv} 2^{\binom{n-v}{3} - m(n-v)}$, where

$$s_{nv} = \frac{(2^n-1)(2^n-2)\ldots(2^n-2^{v-1})}{(2^v-1)(2^v-2)\ldots(2^v-2^{v-1})} < 2^{(n-v+1)v}.$$

The theorem follows. ■

Corollary 4.5. *Let $m \geq \binom{n}{3}/n$. Then*

$$p \leq 2^{\binom{n}{3} - nm} + (n-1)2^{2(n-1)-m}.$$

Proof. By Theorem 4.2,

$$p \leq 2^{\binom{n}{3} - nm} + \sum_{v=1}^{n-1} 2^{\binom{n-v}{3} + (n-v+1)v - (n-v)m}.$$

It is easy to check that for $m \geq \binom{n}{3}/n$ the function $\binom{n-v}{3} + (n-v+1)v - (n-v)m$ achieves its maximum in the interval $1 \leq v \leq n-1$ at $v = n-1$. That implies the corollary. ■

4.2 The case of any q, $d < D$

Let $P_1, \ldots, P_m$ be a sequence of polynomials of degree D in the semigraded algebra $A = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$. By Proposition 3.50 and Corollary 3.61, the degree of regularity of $P_1, \ldots, P_m$ exists and depends only on the leading forms $f_1, \ldots, f_m \in G(A)_D$ of $P_1, \ldots, P_m$. Therefore, it makes sense to perform the probabilistic analysis only on the space of the leading forms.

Let $f_1, \ldots, f_m \in G(A)_D$ be taken independently and uniformly at random, let $d < D$ be a natural number, and let p denote the probability that the columns of $\overline{M}_{d+D}$ are linearly dependent. Our goal is to prove that if $m \geq l_q(n, d+D)/l_q(n,d)$, then

$$p \leq q^{l_q(n,d+D) - m l_q(n,d)} + O(n^d q^{-Cn^D})$$

for a positive constant C as n tends to infinity. This implies Theorem 4.1.

For simplicity, we choose as a basis for $G(A)_D$, the set of monomials $\{x_1^{a_1} \ldots x_n^{a_n} | \sum_i a_i = D, 0 \leq a_i < q\}$. Similarly, as a basis for $G(A)_{d+D}$, we choose the set of monomials $\{x_1^{a_1} \ldots x_n^{a_n} | \sum_i a_i = d+D, 0 \leq a_i < q\}$. We use multisets to index the monomials: $(a_1, \ldots, a_n)$ is the index of $x_1^{a_1} \ldots x_n^{a_n}$.

More specifically, let $\mathcal{X} = \{(a_1, \ldots, a_n) | 0 \leq a_i < q\}$, then the columns of $\overline{M}_{d+D}$ are indexed by $\mathcal{X}^{d+D}$ (the $d+D$-multisets in $\mathcal{X}$) and its rows are indexed by $\mathcal{X}^D$ (the D-multisets in $\mathcal{X}$).

Example 4.6. let $q = 3, n = 3, D = 2$ and

$$f = c_{(2,0,0)} x_1^2 + c_{(1,1,0)} x_1 x_2 + c_{(1,0,1)} x_1 x_3 + c_{(0,2,0)} x_2^2 + c_{(0,1,1)} x_2 x_3 + c_{(0,0,2)} x_3^2.$$

The degree 3 Macaulay matrix for f is in Table 4.1.

Table 4.1: The degree 3 homogeneous Macaulay matrix for f

	(0,1,2)	(0,2,1)	(1,0,2)	(1,1,1)	(1,2,0)	(2,0,1)	(2,1,0)
(0,0,1)	$c_{(0,1,1)}$	$c_{(0,2,0)}$	$c_{(1,0,1)}$	$c_{(1,1,0)}$	0	$c_{(2,0,0)}$	0
(0,1,0)	$c_{(0,0,2)}$	$c_{(0,1,1)}$	0	$c_{(1,0,1)}$	$c_{(1,1,0)}$	0	$c_{(2,0,0)}$
(1,0,0)	0	0	$c_{(0,0,2)}$	$c_{(0,1,1)}$	$c_{(0,2,0)}$	$c_{(1,0,1)}$	$c_{(1,1,0)}$

As in the base case, we split $\overline{M}_{d+D}$ into blocks, each being the homogeneous Macaulay matrix of a single f_j. The blocks are independent, as f_j are taken independently. Let u be a vector over $\mathbb{F}_q$ and of length $|\mathcal{X}^{d+D}|$. Its entries are indexed by the multisets in $\mathcal{X}^{d+D}$. Then

$$p_u = \mathbb{P}(Mu = 0) = p_{1u}^m,$$

where $p_{ju} = \mathbb{P}(M_j u = 0)$. Therefore, $p \leq \sum_{u \neq 0} p_u = \sum_{u \neq 0} p_{1u}^m$.

For simplicity, we call M the homogeneous Macaulay matrix of f_1 of degree $d + D$. Let c denote the vector of coefficients of f_1. It is of length $|\mathcal{X}^D|$, and its entries c_L are indexed by the multisets $L \in \mathcal{X}^D$. Let m_{JI} denote the entry of M_1 in the row $J \in \mathcal{X}^d$ and the column $I \in \mathcal{X}^{d+D}$. By the definition of M_1, we have $m_{JI} = c_{I \setminus J}$ if $J \subseteq I$ and $m_{JI} = 0$ otherwise. So $M_1 u = 0$ is equivalent to the following equalities which hold for every row of M_1 indexed by $J \in \mathcal{X}^d$.

$$\sum_{I \in \mathcal{X}^{d+D}} m_{JI} u_I = \sum_{J \subseteq I} c_{I \setminus J} u_I = \sum_{L+J \in \mathcal{X}^{d+D}} c_L u_{L+J} = 0, \tag{4.2}$$

where the second sum is over all $I \in \mathcal{X}^{d+D}$ such that $J \subseteq I$, and the third sum is over all $L \in \mathcal{X}^D$ such that $L + J \in \mathcal{X}^{d+D}$.

Let $Y^{(u)}$ be a matrix of size $|\mathcal{X}^d| \times |\mathcal{X}^D|$, whose rows and columns are labelled by the multisets from $\mathcal{X}^d$ and $\mathcal{X}^D$ respectively. The entries of $Y^{(u)}$ are defined by

$$Y^{(u)}_{J,L} = \begin{cases} u_{J+L} & \text{if } J + L \in \mathcal{X}^{d+D}, \\ 0 & \text{otherwise.} \end{cases}$$

For $n = 3, q = 3$, $d = 1$, and $D = 2$ the matrix $Y^{(u)}$ is in Table 4.2.

Table 4.2: Matrix $Y^{(u)}$

	(0,0,2)	(0,1,1)	(0,2,0)	(1,0,1)	(1,1,0)	(2,0,0)
(0,0,1)	0	$u_{(0,1,2)}$	$u_{(0,2,1)}$	$u_{(1,0,2)}$	$u_{(1,1,1)}$	$u_{(2,0,1)}$
(0,1,0)	$u_{(0,1,2)}$	$u_{(0,2,1)}$	0	$u_{(1,1,1)}$	$u_{(1,2,0)}$	$u_{(2,1,0)}$
(1,0,0)	$u_{(1,0,2)}$	$u_{(1,1,1)}$	$u_{(1,2,0)}$	$u_{(2,0,1)}$	$u_{(2,1,0)}$	0

By (4.2), the equality $M_1 u = 0$ is equivalent to $Y^{(u)} c = 0$. So $p_{u1} = q^{-\operatorname{rk}(Y^{(u)})}$ and therefore

$$p \leq \sum_{u \neq 0} q^{-m \operatorname{rk}(Y^{(u)})} = \sum_{v=0}^{|\mathcal{X}^d|-1} N_v q^{-m\left(|\mathcal{X}^d|-v\right)}, \tag{4.3}$$

where N_v denotes the number of vectors u such that $\operatorname{rk}(Y^{(u)}) = |\mathcal{X}^d| - v$. The

value N_v is upper bounded by the size of the set

$$S_v = \left\{ u | \operatorname{rk}(Y^{(u)}) \leq |\mathcal{X}^d| - v \right\}.$$

In particular, $u \in S_v$ if and only if there exists a row vector subspace $V \subseteq \mathbb{F}_q^{|\mathcal{X}^d|}$ of dimension v in the kernel of $Y^{(u)}$. Let $B = (b_1, \ldots, b_v)$ be a basis of this subspace.

We index the coordinates of b_i with $J \in \mathcal{X}^d$ according to the lexicographic ordering from left to right. Then $b_i Y^{(u)} = 0$ is equivalent to the following equality holding for every $L \in \mathcal{X}^D$:

$$\sum_{J+L \in \mathcal{X}^{d+D}} b_{i,J} \, u_{J+L} = 0, \tag{4.4}$$

where the sum is over all $J \in \mathcal{X}^d$ such that $J + L \in \mathcal{X}^{d+D}$. The basis B may be represented as a matrix of size $v \times |\mathcal{X}^d|$ in reduced row echelon form.

$$B = \begin{pmatrix} 0 & \ldots & 0 & 1 & * & \ldots & * & 0 & * & \ldots \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 1 & * & \ldots \\ \ldots & & & & & & & & & \end{pmatrix}.$$

For each vector b_i, $i = 1, \ldots, v$ in the basis B we now define a matrix A_i. The matrix A_i has $|\mathcal{X}^{d+D}|$ rows and $|\mathcal{X}^D|$ columns, indexed by $I \in \mathcal{X}^{d+D}$ and by $L \in \mathcal{X}^D$ respectively. The indices are ordered according to the lexicographic ordering from left to right and from top to bottom. The entry I, L of A_i is defined by

$$A_{i,I,L} = \begin{cases} b_{i,I \setminus L} & \text{if } L \subseteq I, \\ 0 & \text{otherwise.} \end{cases}$$

For $n = 3$, $q = 3$ and $d = 1$, $D = 2$ the matrix A_i constructed for $b_i = (b_{(1,0,0)}, b_{(0,1,0)}, b_{(0,0,1)})$ is in Table 4.3. Let A_V denote the horizontal concatenation of the matrices $A_1, \ldots, A_v$, that is $A_V = A_1 | A_2 | \ldots | A_v$. The equalities (4.4)

Table 4.3: Matrix A_i

	(0,0,2)	(0,1,1)	(0,2,0)	(1,0,1)	(1,1,0)	(2,0,)0
(0,1,2)	$b_{(0,1,0)}$	$b_{(0,0,1)}$	0	0	0	0
(0,2,1)	0	$b_{(0,1,0)}$	$b_{(0,0,1)}$	0	0	0
(1,0,2)	$b_{(1,0,0)}$	0	0	$b_{(0,0,1)}$	0	0
(1,1,1)	0	$b_{(1,0,0)}$	0	$b_{(0,1,0)}$	$b_{(0,0,1)}$	0
(1,2,0)	0	0	$b_{(1,0,0)}$	0	$b_{(0,1,0)}$	0
(2,0,1)	0	0	0	$b_{(1,0,0)}$	0	$b_{(0,0,1)}$
(2,1,0)	0	0	0	0	$b_{(1,0,0)}$	$b_{(0,1,0)}$

are equivalent to $uA_V = 0$ and therefore

$$|S_v| \le \sum_{\dim(V)=v} q^{|\mathcal{X}^{d+D}|-\mathrm{rk}(A_V)},$$

where the sum is over all the subspaces V of dimension v in $\mathbb{F}_q^{|\mathcal{X}^d|}$. Let the multiset $J_i \in \mathcal{X}^d$ index the first nonzero entry of the vector $b_i \in B$. As B is in reduced row echelon form, then the multisets $J_1, \dots, J_v$ are pairwise different. We denote $\mathcal{I} = \bigcup_{i=1}^{v} \left\{ I \in \mathcal{X}^{d+D} | I \supseteq J_i \right\} = \nabla^D(\{J_1, \dots, J_v\})$.

Lemma 4.7. $\mathrm{rk}(A_V) \ge |\mathcal{I}|$.

Proof. For $I \in \mathcal{I}$ we fix some multiset $J_k \subseteq I$ and take a column in the block A_k indexed by $L = I \setminus J_k$. We show that those $|\mathcal{I}|$ columns in A_V are linearly independent. It is enough to prove that the row with index I has 1 in the column L of the block A_k and all entries above it in this column are zeros. The latter formally means $A_{k,I',L} = 0$ if $I' < I$. First of all, $A_{k,I,L} = b_{k,J_k} = 1$ since $J_k = I \setminus L$. Let $I' < I$. We consider two cases:

(i) Let $I' \not\supseteq L$, then $A_{k,I',L} = 0$ by definition of A_k.

(ii) Let $I' \supseteq L$, so $I' = L + J$ for some d-multiset J. As $I = L + J_k$ and $I' < I$, then $J < J_k$ by the properties of the lexicographic ordering. Then $A_{k,I',L} = b_{k,J} = 0$.

The lemma is proved. ■

Let T_v be the family from $\mathcal{X}^d$containing the v largest multisets and let $\ell(v) = |\nabla^D(T_v)|$. By Lemma 4.7 and Corollary 2.44, $\mathrm{rk}(A_V) \geq |\mathcal{I}| \geq \ell(v)$. So

$$N_v \leq \sum_{\dim(V)=v} q^{|\mathcal{X}^{d+D}|-\mathrm{rank}(A_V)} \leq s_v q^{|\mathcal{X}^{d+D}|-\ell(v)},$$

where s_v is the number of subspaces of dimension v in $\mathbb{F}_q^{|\mathcal{X}^d|}$. It is easy to see that $s_v \leq q^{(|\mathcal{X}^d|-v+1)v}$. By (4.3), we get

$$\begin{aligned} p \leq & \sum_{v=0}^{|\mathcal{X}^d|-1} q^{(|\mathcal{X}^d|-v+1)v+|\mathcal{X}^{d+D}|-\ell(v)-(|\mathcal{X}^d|-v)m} = q^{|\mathcal{X}^{d+D}|-m|\mathcal{X}^d|} \\ & + \sum_{v=1}^{|\mathcal{X}^d|-1} q^{(|\mathcal{X}^d|-v+1)v+|\mathcal{X}^{d+D}|-\ell(v)-(|\mathcal{X}^d|-v)m}. \end{aligned} \tag{4.5}$$

In order to complete the proof of Theorem 4.1, it is necessary to show that (4.5) $\in O(n^d q^{-Cn^D})$ for some positive constant C.

Let s be a positive integer and let $l_{s,q}(n,d)$ denote the number of monomials of degree d in $\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^s,x_2^q,\ldots,x_n^q)$. Obviously,

$$l_{s,q}(n,d) = \sum_{i=0}^{s-1} l_q(n-1,d-i). \tag{4.6}$$

Let $S = \{1,\ldots,l_q(n,d)-1\}$ and let X_v denote the v-th largest multiset in the family of d-multisets $\mathcal{X}^d$ according to the lexicographic order. We will partition S into disjoint intervals, on which the second term (4.5) will be analysed.

Let $0 \leq \delta \leq d$. By division with remainder, $d-\delta = \sigma(q-1)+t$ for some $\sigma \geq 0$ and $0 \leq t < q-1$. We consider the family of all d-mutisets of the form

$$(q-1,\ldots,q-1,u,a_{\sigma+2},\ldots,a_n),$$

where $u \geq t$, for some $a_{\sigma+2},\ldots,a_n$. Let v_δ denote the largest index v such that X_v belongs to that family. If that does not exist we set $v_\delta = v_{\delta-1}$, where $v_{-1} = 0$. Obviously, $v_\delta = l_{q-t,q}(n-\sigma,\delta)$. In particular, $v_0 = 1, v_d = l_q(n,d)$, and $v_{-1} < v_0 \leq v_1 \leq \ldots \leq v_d$.

Let I_δ denote all v such that $v_{\delta-1} < v \le v_\delta$. Clearly, $v \in I_\delta$ if and only if X_v belongs to the family of d-multisets

$$(q-1,\dots,q-1,t,a_{\sigma+2},\dots,a_n)$$

for some $a_{\sigma+2},\dots,a_n$. So $|I_\delta| = v_\delta - v_{\delta-1} = l_q(n-\sigma-1,\delta)$. We have $S = \bigcup_{\delta=0}^{d} I_\delta$. Let $0 \le x \le n-\sigma-1$. We consider a family of all d-multisets

$$(q-1,\dots,q-1,t,0,\dots,0,a_{\sigma+x+2},\dots,a_n),$$

where $a_{\sigma+x+2} \neq 0$. Let $v_{\delta,x}$ denote the largest v such that X_v belongs to that family. If the family is empty we put $v_{\delta,x} = v_{\delta,x-1}$, where $v_{\delta,-1} = v_{\delta-1}$. Then $v_{\delta-1} = v_{\delta,-1} \le v_{\delta,0} \le \dots \le v_{\delta,n-\sigma-1} = v_\delta$. Obviously, $v_{\delta,x} = v_\delta - l_q(n-\sigma-x-2,\delta)$. Let $I_{\delta,x}$ denote the set of all v such that $v_{\delta,x-1} < v \le v_{\delta,x}$. Then $I_\delta = \bigcup_{x=0}^{n-\sigma-1} I_{\delta,x}$.

Proposition 4.8. *If $\delta = 0$, then $\ell(v_{0,n-\sigma-1}) = l_{q-t,q}(n-\sigma,\delta+D)$, and $\ell(v_{0,x}) = 0$ for $x < n-\sigma-1$. If $\delta > 0$, then*

$$\ell(v_{\delta,x}) = l_{q-t,q}(n-\sigma,\delta+D) - l_q(n-\sigma-x-2,\delta+D).$$

Proof. For $\delta = 0$ the statement is obviously correct. Let $\delta > 0$. We notice that the family of d-multisets T_v, where $1 \le v \le v_{\delta,x}$, consists of all and only the d-multisets of the form

$$(q-1,\dots,q-1,t+a_{\sigma+1},a_{\sigma+2},\dots,a_n),$$

where at least one among $a_{\sigma+1},\dots,a_{\sigma+x+2}$ is non-zero and $\sum a_i = \delta$. The D-th shade of this family consists of all and only the $(d+D)$-multisets of the form

$$(q-1,\dots,q-1,t+a_{\sigma+1},a_{\sigma+2},\dots,a_n),$$

where at least one among $a_{\sigma+1},\dots,a_{\sigma+x+2}$ is non-zero and $\sum a_i = \delta + D$. The number of such $(d+D)$-multisets is $l_{q-t,q}(n-\sigma,\delta+D) - l_q(n-\sigma-x-2,\delta+$

D). That implies the statement for $\delta > 0$. ■

Lemma 4.9. *Let $v \in I_{\delta,x}$. Then $\ell(v+1) - \ell(v) \leq l_q(n-\sigma-x-2, D)$.*

Proof. Since $v \in I_{\delta,x}$, then

$$X_v = (q-1,\dots,q-1,t,0,\dots,0,a_{\sigma+x+2},\dots,a_n),$$

for some $a_{\sigma+x+2},\dots,a_n$, where $a_{\sigma+x+2} \neq 0$. It follows that

$$X_{v+1} = (q-1,\dots,q-1,t,0,\dots,0,a_{\sigma+x+2},\dots,a_{j-1},a_j-1,b_{j+1},\dots,b_n),$$

for $j \geq \sigma+x+2$ and some $b_{j+1},\dots,b_n$. Any $(d+D)$-multiset in the D-th shade of X_{v+1} and not in the D-th shade of $\{X_1,\dots X_v\}$ is in the family of $(\delta+D)$-multisets of the form

$$(q-1,\dots,q-1,t,0,\dots,0,a_{\sigma+x+2},\dots,a_{j-1},a_j-1,c_{j+1},\dots,c_n),$$

for some $c_{j+1},\dots,c_n$. The size of that family is at most $l_q(n-\sigma-x-2, D)$. That implies the lemma. ■

Lemma 4.10. *Let $1 < s \leq q$, then*

(i) $l_{s,q}(n,\delta) - l_q(n-x,\delta) \geq x l_q(n-x,\delta-1)$.

(ii) for $x \leq \sqrt{n}$ and large enough n,

$$l_{s,q}(n,\delta) - l_q(n-x,\delta) \leq x(l_q(n-1,\delta-1) + (q-2)l_q(n-1,\delta-2)).$$

Proof. By (4.6),

$$\begin{aligned}
&l_{s,q}(n,\delta) - l_q(n-x,\delta) = \\
=&(l_{s,q}(n,\delta) - l_q(n-1,\delta)) + \sum_{i=1}^{x-1}(l_q(n-i,\delta) - l_q(n-i-1,\delta)) = \\
=&\sum_{j=1}^{s-1} l_q(n-1,\delta-j) + \sum_{i=1}^{x-1}\sum_{j=1}^{q-1} l_q(n-i-1,\delta-j) \geq x l_q(n-x,\delta-1)
\end{aligned}$$

by considering only summands for $j = 1$. On the other hand for $x < \sqrt{n}$ and n large enough $l_q(n-x,\delta-i) > l_q(n-x,\delta-i-1)$. Therefore,

$$\begin{aligned}
&l_{s,q}(n,\delta) - l_q(n-x,\delta) = \\
=&\sum_{j=1}^{s-1} l_q(n-1,\delta-j) + \sum_{i=1}^{x-1}\sum_{j=1}^{q-1} l_q(n-i-1,\delta-j) \leq \\
\leq&\sum_{i=0}^{x-1}\sum_{j=1}^{q-1} l_q(n-i-1,\delta-j) \leq \\
\leq& x l_q(n-1,\delta-1) + (q-2)\sum_{i=0}^{x-1} l_q(n-i-1,\delta-2) \leq \\
\leq& x(l_q(n-1,\delta-1) + (q-2)l_q(n-1,\delta-2)).
\end{aligned}$$

As stated. ■

We consider the exponent of (4.5). As $m \geq \frac{l_q(n,d+D)}{l_q(n,d)}$,

$$\big(l_q(n,d) - v + 1\big)v + l_q(n,d+D) - \ell(v) - \big(l_q(n,d) - v\big)m \leq E(v),$$

where $E_n(v) = Pv - v^2 - \ell(v)$ and $P = \left(l_q(n,d) + 1 + \frac{l_q(n,d+D)}{l_q(n,d)}\right)$. Assume $v \in I_\delta$, that is $v_{\delta-1} < v \leq v_\delta$. First, let $\delta = 0$, then $v = 1$ and

$$E_n(1) = l_q(n,d) + \frac{l_q(n,d+D)}{l_q(n,d)} - \ell(1).$$

By Proposition 4.8, $\ell(1) = l_{t,q}(n-\sigma,D) = \frac{n^D}{D!} + O(n^{D-1})$ for large n. Therefore,

$$E_n(1) = -n^D\left(\frac{1}{D!} - \frac{d!}{(d+D)!}\right) + O(n^{D-1}). \tag{4.7}$$

From now on, we assume $\delta > 0$ and $v \in I_{\delta,x}$, that is $v_{\delta,x-1} < v \leq v_{\delta,x}$.

Lemma 4.11. *Let $0 < \alpha < \sqrt[D]{\frac{d!D!}{(d+D)!}}$. Then for $x > n(1-\alpha)$ and $v \in I_{\delta,x}$, we have $E_n(v+1) - E_n(v) > 0$ for all n large enough. In particular, the maximum on the given intervals of the function E_n can be found at $v = v_\delta$.*

Proof. Using Lemma 4.9, we can see that

$$\begin{aligned} E_n(v+1) - E_n(v) =& P - 2v - 1 - \ell(v+1) + \ell(v) \geq \\ \geq& \frac{l_q(n,d+D)}{l_q(n,d)} - l_q(n,d) - l_q(n-\sigma-x-2,D). \end{aligned}$$

As $x > n(1-\alpha_0)$,

$$\begin{aligned} E_n(v+1) - E_n(v) \geq& \frac{\left(\!\!\binom{n}{d+D}\!\!\right)}{\left(\!\!\binom{n}{d}\!\!\right)} - \left(\!\!\binom{\alpha n - \sigma - 2}{D}\!\!\right) + O(n^{D-1}) \geq \\ \geq& n^D\left(\frac{d!}{(d+D)!} - \frac{\alpha^D}{D!}\right) + O(n^{D-1}). \end{aligned}$$

So for n large enough we have $E_n(v+1) - E_n(v) > 0$ for $v \in I_{\delta,x}$ and $x > n(1-\alpha)$. ■

Proposition 4.12. *There exist positive C and n_0 such that $E_n(v) < -Cn^D$ for $n \geq n_0$ and $1 \leq v \leq l_q(n,d) - 1$.*

Proof. Let $v \in I_{\delta,x}$, that is $v_{\delta,x-1} < v \leq v_{\delta,x}$. Then $E_n(v) < Pv_{\delta,x} - \ell(v_{\delta,x-1})$. Let $0 < \alpha < \sqrt[D]{\frac{d!D!}{(d+D)!}}$ be a fixed number. We will divide I_δ into three disjoint intervals:

$$I_\delta = \bigcup_{0 \leq x \leq \sqrt{n}} I_{\delta,x} \quad \cup \quad \bigcup_{\sqrt{n} < x \leq n(1-\alpha)} I_{\delta,x} \quad \cup \quad \bigcup_{n(1-\alpha) < x \leq n-\sigma-1} I_{\delta,x}$$

and bound $E_n(v)$ from above on each of them.

Case 1. Let $0 \leq x \leq \sqrt{n}$. By Lemma 4.10, if $v \in I_{\delta,x}$, then

$$\begin{aligned} &E_n(v) \leq Pv_{\delta,x} - \ell(v_{\delta,x-1}) \leq \\ \leq& P(x+2)(l_q(n-\sigma-1,\delta-1) + (q-2)l_q(n-\sigma-1,\delta-2)) - \\ -&(x+1)l_q(n-\sigma-x-1,\delta+D-1)) \leq \\ \leq& (x+1)\left(n^{\delta+D-1}\left(\frac{2d!}{(d+D)!(\delta-1)!} - \frac{1}{(\delta+D-1)!}\right) + O(n^{\delta+D-3/2})\right). \quad (4.8) \end{aligned}$$

The main term of the last expression is negative for every $x \geq 0$, since

$$2(\delta+D-1)! = (2\delta)(\delta+D-1)\dots(\delta+1)(\delta-1)! < (d+D)\dots(d+1)(\delta-1)!.$$

Hence, for n sufficiently large the maximum of (4.8) is achieved for $x = 0$.

Case 2. Let $\sqrt{n} < x \leq n(1-\alpha_0)$. For simplicity, we replace $n-\sigma-x-2$ with y, so $\alpha_0 n - 2 - \sigma \leq y < n - \sqrt{n} - 2 - \sigma$. By rearranging the terms, if $v \in I_{\delta,x}$, then

$$\begin{aligned} &E_n(v) \leq P v_{\delta,x} - \ell(v_{\delta,x-1}) = \\ =&P l_{q-t,q}(n-\sigma,\delta) - l_{q-t,q}(n-\sigma,\delta+D) - P l_q(y,\delta) + l_q(y+1,\delta+D). \end{aligned}$$

We have

$$\begin{aligned} &P l_{q-t,q}(n-\sigma,\delta) - l_{q-t,q}(n-\sigma,\delta+D) = \\ =&n^{\delta+D}\left(\frac{d!}{(D+d)!\delta!} - \frac{1}{(D+\delta)!}\right) + O(n^{\delta+D-1}). \end{aligned} \tag{4.9}$$

Then

$$\begin{aligned} &-P l_q(y,\delta) + l_q(y+1,\delta+D) = \\ =&\left(\!\binom{y}{\delta}\!\right)\left(-\frac{\left(\!\binom{n}{d+D}\!\right)}{\left(\!\binom{n}{d}\!\right)} + \frac{\left(\!\binom{y}{\delta+D}\!\right)}{\left(\!\binom{y}{\delta}\!\right)}\right) + O(n^{\delta+D-1}) = \\ \leq&\left(\!\binom{y}{\delta}\!\right)\left(-\frac{n^D d!}{(D+d)!} + \frac{(n-\sqrt{n})^D \delta!}{(D+\delta)!}\right) + O(n^{\delta+D-1}) = \qquad (4.10) \\ =&\left(\!\binom{y}{\delta}\!\right)\left(\frac{n^D \delta!}{(D+\delta)!} - \frac{n^D d!}{(D+d)!} - \frac{n^{D-1/2} D \delta!}{(\delta+D)!}\right) + O(n^{\delta+D-1}). \qquad (4.11) \end{aligned}$$

We notice that for n large enough (this choice depends only on δ, d, and D) the sum in the parenthesis is positive if $\delta < d$ and negative if $\delta = d$. If $\delta < d$, then

$$\begin{aligned} &- P l_q(y,\delta) + l_q(y+1,\delta+D) \leq \\ \leq&n^{\delta+D}\left(\frac{1}{(\delta+D)!} - \frac{d!}{(D+d)!\delta!}\right) - \frac{n^{\delta+D-1/2} D}{(\delta+D)!} + O(n^{\delta+D-1}). \end{aligned} \tag{4.12}$$

If $\delta = d$, then

$$-Pl_q(y,d) + l_q(y+1,d+D) \leq -\frac{n^{d+D-1/2}D\alpha^d}{(d+D)!} + O(n^{d+D-1}). \tag{4.13}$$

Overall for $\delta < d$, by putting together (4.9) and (4.12), we have

$$E_n(v) \leq -\frac{n^{\delta+D-1/2}D}{(\delta+D)!} + O(n^{\delta+D-1}) \tag{4.14}$$

for n large enough. For $\delta = d$, by putting together (4.9) and (4.13), we have

$$E_n(v) \leq -\frac{n^{d+D-1/2}D\alpha^d}{(d+D)!} + O(n^{d+D-1}) \tag{4.15}$$

for n large enough.

Case 3. Let $n(1-\alpha) < x \leq n - \sigma - 1$. Then, by Lemma 4.11, $E_n(v) \leq E_n(v_\delta)$ if $v \in I_{\delta,x}$.

For $\delta = d$, since $v_d = l_q(n,d)$ is not in the domain of E_n, we use $E_n(v_d - 1)$ as an upper bound, where

$$\begin{aligned} E_n(v_d - 1) = 2l_q(n,d) - 2 - \tfrac{l_q(n,d+D)}{l_q(n,d)} = \\ -\tfrac{n^D d!}{(d+D)!} + O(n^{D-1}) \end{aligned} \tag{4.16}$$

as $l_q(n,d+D) = \ell(v_d - 1)$. For $\delta < d$, the maximum of E_n on the interval is achieved at v_δ:

$$\begin{aligned} E_n(v_\delta) \leq Pl_{q-t,q}(n-\sigma,\delta) - l_{q-t,q}(n-\sigma,\delta+D) = \\ -n^{\delta+D}\left(\tfrac{1}{(\delta+D)!} - \tfrac{d!}{(D+d)!\delta!}\right) + O(n^{\delta+D-1}). \end{aligned} \tag{4.17}$$

Overall, by combining (4.7), (4.8), (4.14), (4.15), (4.16), (4.17), we conclude that there exists a positive constant C and a natural number n_0 such that for every $n > n_0$ and $v \in \{1,\ldots,l_q(n,d)-1\}$, $E_n(v) < -Cn^D$. ■

We can conclude the proof of Theorem 4.1:

$$p \leq q^{l_q(n,d+D)-ml_q(n,d)} + \sum_{v=1}^{l_q(n,d)-1} q^{E_n(v)} \leq q^{l_q(n,d+D)-ml_q(n,d)} + O(n^d q^{-Cn^D}).$$

The presented result is asymptotic and it is of interest for applications to understand how big should n be for the second term to actually be irrelevant. In Table 4.4 we present, for choices of d and D, what is the smallest n for which the exponent of (4.5) is negative and the value of the entire sum (4.5). In these experiments, $m = \frac{l_q(n,d+D)}{l_q(n,d)}$.

Table 4.4: Values of n for which (4.5)< 1. $q = 2$.

d	D	n	(4.5)
1	2	20	$\leq 5.42 \cdot 10^{-4}$
1	3	12	$\leq 1.70 \cdot 10^{-5}$
1	4	10	$\leq 6.80 \cdot 10^{-3}$
2	3	68	$\leq 2.38 \cdot 10^{-7}$
2	4	26	$\leq 6.57 \cdot 10^{-19}$
3	4	> 295	?

4.3 Hybrid method

As Theorem 4.1 covers only the cases of $d < D$, a strategy that one can employ if $m < \frac{l_q(n,2D-1)}{l_q(n,D-1)}$ is to guess some of the variables of the system and then use Theorem 4.1 to get a bound on the degree of regularity of the reduced system.

More precisely, let $A = \mathbb{F}_q[x_1,\ldots,x_n]/(x_1^q - x_1,\ldots,x_n^q - x_n)$ and let $f_1,\ldots,f_m \in G(A)_D$ be a sequence of forms of degree D such that there exists $t < n$ and $d < D$ such that

$$m > \frac{l_q(n-t,d+D)}{l_q(n-t,d)}.$$

Then one can guess t variables and compute q^t Macaulay matrices of sequences in $A/(x_i - a_i)_{i=1,\ldots,t}$. Under an additional hypothesis, the degree of regularity is the same for all the sequences obtained in this way (as shown in Theorem 4.13), and with probability tending to 1 it is $\leq d + D$ by Theorem 4.1. From there one

proceeds with the algorithm described in Section 3.4 to find a Gröbner basis for each of the q^t guesses.

Let $f_1,\dots,f_m$ be polynomials of degree D in the semigraded algebra $A = K[x_1,\dots,x_n]/(x_1^q - x_1,\dots,x_n^q - x_n)$, such that $f_i(0,\dots,0,x_{t+1},\dots x_n)$ has degree D for every i. Let $\mathfrak{a} = (a_1,\dots,a_t) \in \mathbb{F}_q^t$ and let $A_\mathfrak{a} = A/(x_i - a_i)_{i=1,\dots,t}$. The map $\pi_\mathfrak{a} : A \to A_\mathfrak{a}$ is the canonical projection.

Theorem 4.13. *The degree of regularity of the sequence $\pi_\mathfrak{a}(f_1),\dots,\pi_\mathfrak{a}(f_m)$ does not depend on $\mathfrak{a} \in \mathbb{F}_q^t$.*

Proof. First, we notice that $A_\mathfrak{a}$ inherits the structure of semigraded algebra from A. Indeed, $\mathbb{F}_q[x_1,\dots,x_n] \to A \to A_\mathfrak{a}$ is a chain of surjective $\mathbb{F}_q$-algebra morphisms. The filtration $\mathcal{B}_0 \subseteq \mathcal{B}_1 \subseteq \dots$, with

$$\mathcal{B}_\delta = \{x_{t+1}^{c_{t+1}} \dots x_n^{c_n} + (x_i - a_i)_{i=1,\dots,t} | 0 \le c_j < q, \sum_j c_j \le \delta\}$$

is a filtered basis for $A_\mathfrak{a}$. Let us consider the family of multisets $\mathcal{Y} = \{(c_{t+1},\dots,c_n) | 0 \le c_j < q\}$. One can index the elements of $\mathcal{B}_D$ with multisets I from $\bigcup_{\delta=0}^D \mathcal{Y}^\delta$: the basis element w_I is the monomial that has the entries of the multiset I as powers of the variables.

For every δ there is an obvious one-to-one correspondence between the families of multisets:

$$\mathcal{Y}^\delta \quad \text{and} \quad \{(0,\dots,0,c_{t+1},\dots,c_n) | 0 \le c_j < q, \sum c_j = \delta\} \subseteq \mathcal{X},$$

where $\mathcal{X} = \{(c_1,\dots,c_n) | 0 \le c_j < q\}$. Then a polynomial $f \in A_D$ can be written as an $\mathbb{F}_q$-linear combination of the monomials w_J indexed by elements in $\mathcal{X}$:

$$f = \sum_{\delta=0}^{D} \sum_{J \in \mathcal{X}^\delta} \alpha_J w_J = \sum_{I \in \mathcal{Y}^D} \alpha_I w_I + \sum_{\delta=0}^{D} \sum_{J \in \mathcal{X}^\delta \setminus \mathcal{Y}^D} \alpha_J w_J.$$

It follows that

$$\pi_\mathfrak{a}(f) = \sum_{I \in \mathcal{Y}^D} \alpha_I w_I + \sum_{\delta=0}^{D-1} \sum_{J \in \mathcal{Y}^\delta} \gamma_J v_J + (x_i - a_i)_{i=1,\dots,t},$$

for some $\gamma_J \in \mathbb{F}_q$, where v_J are the elements from $\mathcal{B}_\delta$.

In particular, if at least one of the α_I is different from 0 for each f_i (holds by hypothesis), the leading forms $(\pi_\mathfrak{a}(f_j))^L \in G(A_\mathfrak{a})_D$ do not depend on the choice of $\mathfrak{a}$.

Let $p = x_{t+1}^{c_{t+1}} \dots x_n^{c_n} + (x_i - a_i)_{i=1,\dots,t} \in \mathcal{B}_d$. Let P be the multiset $(c_{t+1}, \dots, c_n)$. Then we have that

$$p\pi_\mathfrak{a}(f) = \left(\sum_{I+P \in \mathcal{X}^{d+D}} \alpha_I w_{I+P} \right) + h + (x_i - a_i)_{i=1,\dots,t},$$

where h is a polynomial of degree smaller than $d + D$ and the sum is performed over all $I \in \mathcal{Y}^D$ such that $I + P \in \mathcal{X}^{d+D}$.

It follows that the image of $p\pi_\mathfrak{a}(f)$ in $G(A_\mathfrak{a})_{d+D}$ does not depend on $\mathfrak{a}$. Therefore, we conclude that at every degree the homogeneous parts of the Macaulay matrices have the same rank for any projection $\pi_\mathfrak{a}$. So the theorem is proved. ■

Remark 4.14. The condition that all the leading forms of the sequence should have at least one monomial that does not depend on $x_1, \dots, x_t$ is likely to hold. By choosing $t = \gamma n$ for fixed $\gamma < 1$, it is easy to see that the probability that this happens tends to 1 as $n \to \infty$.

Example 4.15. Let $t = n/2$ and $m > \frac{l_q(n/2, D+1)}{n/2}$. This means that for n sufficiently large, one is required to construct $\sqrt{q^n}$ Macaulay matrices of degree $D + 1$ each one with $n/2$ variables.

More specifically, if one has a system with $m \geq \binom{n/2}{3}/n + 1$ (for example, $m = n^2/24$) quadratic polynomials over $\mathbb{F}_2[x_1, \dots, x_n]$, whose leading forms are chosen uniformly and independently at random, it is possible to find a solution of the system by computing $2^{n/2}$ Gröbner bases. If each leading form depends at least on one of the guessed variables, the sequences obtained by the quotients will have the same degree of regularity and with probability described by Theorem 4.1, it will be at most 3.

4.4 Truncated polynomials

In this section we show how to use Macaulay matrices defined over quotient algebras to improve upon the complexity of computing a Gröbner basis given in [ST19a] for sufficiently overdetermined systems. First, we present the general idea of this method and then we formalise it. Let us consider a system over $\mathbb{F}_2$:

$$P_1 = 0, \dots, P_m = 0, x_1^2 - x_1 = 0, \dots, x_n^2 - x_n = 0. \tag{4.18}$$

with $P_1, \dots, P_m \in R = \mathbb{F}_2[x_1, \dots, x_n]$ and with $\deg(P_j) = D$ for every j. Our goal is to construct a homogeneous Macaulay matrix that does not only depend on the forms of degree D, but also on the ones of degree $D-1$. For every i we can write $P_i = f_i + g_i + h_i$, where $h_i \in R_{D-2}$, g_i is homogeneous of degree $D-1$, and f_i is homogeneous of degree D.

We consider the following system of polynomials in $\mathbb{F}_2[z, x_1, \dots, x_n]$, equivalent to (4.18):

$$\begin{aligned} &f_1 + zg_1 + h_1 = 0, \dots, f_m + zg_m + h_m = 0, \\ &z^2 - 1 = 0, x_1^4 - x_1 = 0, \dots, x_n^4 - x_n = 0, \\ &z - 1 = 0, x_1^2 - x_1 = 0, \dots, x_n^2 - x_n = 0. \end{aligned} \tag{4.19}$$

There is a one-to-one correspondence between the sets of solutions of the two systems: a solution $(a_1, \dots, a_n)$ for (4.18) corresponds to the solution $(1, a_1, \dots, a_n)$ for (4.19).

In particular, we will construct the Macaulay matrices M_d of $f_1 + zg_1 + h_1, \dots, f_m + zg_m + h_m$ in $\mathbb{F}_q[z, x_1, \dots, x_n]/(x_1^4 - x_1, \dots, x_n^4 - x_n, z^2 - 1)$. Thus we are guaranteed that the degree of regularity exists.

Let $\mathcal{Y}_0 = \{(0, a_1, \dots, a_n) | 0 \le a_i < q\}$ and $\mathcal{Y}_1 = \{(1, a_1, \dots, a_n) | 0 \le a_i < q\}$ be subfamilies of multisets of $\mathcal{Y} = \{(b, a_1, \dots, a_n) | 0 \le b < 2, 0 \le a_i < q\}$. By con-

struction, $M_{d_{\text{reg}}}$ has the following shape:

$$
\begin{array}{c|ccccc}
 & y_1^{d_{\text{reg}}} & y_0^{d_{\text{reg}}} & y^{d_{\text{reg}}-1} & y^{d_{\text{reg}}-2} & \dots \\
\hline
y_1^{D-d_{\text{reg}}}(f_1+zg_1+h_1) & T(f_1) & 0 & 0 & * & * \\
\vdots & & & & & \\
y_1^{D-d_{\text{reg}}}(f_m+zg_m+h_m) & T(f_m) & 0 & 0 & * & * \\
\hline
y_0^{D-d_{\text{reg}}}(f_1+zg_1+h_1) & S(g_1) & S'(f_1) & 0 & * & * \\
\vdots & & & & & \\
y_0^{D-d_{\text{reg}}}(f_m+zg_m+h_m) & S(g_m) & S'(f_m) & 0 & * & * \\
\hline
y^{D-d_{\text{reg}}-1}(f_1+zg_1+h_1) & 0 & 0 & * & * & * \\
\vdots & & & & & \\
y^{D-d_{\text{reg}}-1}(f_m+zg_m+h_m) & 0 & 0 & * & * & * \\
\hline
\vdots & & & & &
\end{array}
$$

where $y_i^d(f_j+zg_j+h_j)$ is the submatrix of $M_{d_{\text{reg}}}$ containing the coefficients of $x^\alpha(f_j+zg_j+h_j)$ for $\alpha \in y_i^d$. The submatrices $T(f_j)$, $S(g_j)$, and $S'(f_j)$ have coefficients that depend only on f_j, g_j, and f_j respectively. By definition of degree of regularity, the block matrix

$$
\begin{pmatrix}
T(f_1) & 0 \\
\vdots & \vdots \\
T(f_m) & 0 \\
S(g_1) & S'(f_1) \\
\vdots & \vdots \\
S(g_m) & S'(f_m)
\end{pmatrix}
$$

represents a surjective linear transformation. Therefore the reduced row eche-

lon form of $M_{d_{\text{reg}}}$ is as follows:

$$\begin{array}{c} \begin{array}{ccccc} y_1^{d_{\text{reg}}} & y_0^{d_{\text{reg}}} & y^{d_{\text{reg}}-1} & y^{d_{\text{reg}}-2} & \dots \end{array} \\ \left(\begin{array}{ccccc} \text{Id} & 0 & 0 & * & * \\ 0 & \text{Id} & 0 & * & * \\ 0 & 0 & 0 & * & * \\ \hline 0 & 0 & * & * & * \\ \vdots & & & & \end{array}\right) \end{array}. \tag{4.20}$$

We compose the linear transformation induced by (4.20) with the canonical projection

$$\begin{aligned} \pi :&\mathbb{F}_q[z,x_1,\dots,x_n]/(x_1^4-x_1,\dots,x_n^4-x_n,z^2-1) \to R/(x_1^2-x_1,\dots,x_n^2-x_n) \cong \\ \cong&\mathbb{F}_q[z,x_1,\dots,x_n]/(x_1^2-x_1,\dots,x_n^2-x_n,z-1) \end{aligned}$$

We choose the set of monomials $X = \{x_1^{a_1}\dots,x_n^{a_n} | 0 \le a_i < 2\}$ with associate multiset family $\mathcal{X}$ as a basis for the codomain. The composition is the linear map represented by the matrix

$$M = \begin{array}{c} \begin{array}{cccc} \mathcal{X}^{d_{\text{reg}}} & \mathcal{X}^{d_{\text{reg}}-1} & \mathcal{X}^{d_{\text{reg}}-2} & \dots \end{array} \\ \left(\begin{array}{cccc} 0 & \text{Id} & * & * \\ \text{Id} & * & * & * \\ 0 & 0 & * & * \\ \hline 0 & * & * & * \\ \vdots & & & \end{array}\right) \end{array}.$$

The row vectors of M represent polynomials that, together with $x_1^2 - x_1,\dots,x_n^2 - x_n$, generate the ideal $(P_1,\dots,P_m,x_1^2 - x_1,\dots,x_n^2 - x_n)$. We call this set of generators B.

Let $Q_1,\dots,Q_r$ be the polynomials from B of degree d_{reg} and let $R_1,\dots,R_s$ be the ones of degree $d_{\text{reg}} - 1$. Before beginning the Buchberger algorithm, one performs polynomial division of each Q_i by $(R_1,\dots,R_s,x_1^2 - x_1,\dots,x_n^2 - x_n)$

and replaces $Q_1, \ldots, Q_r$ in B with their remainder after the division. This has an overall cost of $O(L_2(n, d_{\text{reg}})^2 L_2(n, d_{\text{reg}} - 1))$ operations over $\mathbb{F}_2$. Lastly, one applies Theorem 3.65 to get that the cost of constructing a Gröbner basis is

$$O(L_2(n, d_{\text{reg}} - 1)^2 L_2(n, d_{\text{reg}} - 2)^2 L_2(n, 2d_{\text{reg}} - 4)),$$

for $n \to \infty$ as the "effective" degree of regularity is $d_{\text{reg}} - 1$.

Some questions that need to be answered for the generalisation of this method are the following: can we apply the same probabilistic analysis as in Section 4.2? Does one need a larger m than the one of Theorem 4.1 to speed up the construction of a Gröbner basis as described?

The first step towards formalising the previous method is proving a generalisation of Theorem 3.65:

Corollary 4.16. *Let $r \leq d$ and q be fixed integers. Let $B = \{Q_1, \ldots, Q_t\}$ be a set of generators for an ideal $I \subseteq R = \mathbb{F}_q[x_1, \ldots, x_n]$ satisfying the following properties:*

- *$g \in B$ implies $\deg(g) \leq d$,*
- *B contains $f_1, \ldots, f_n$, with $\text{LM}(f_i) | x_i^q$ for $i = 1, \ldots, n$,*
- *Every monomial in the set $\{x_1^{a_1} \ldots x_n^{a_n} | 0 \leq a_i < q, d - r + 1 \leq \sum_{i=1}^n a_i \leq d\}$ is divisible by $\text{LM}(g)$ for some $g \in B$.*

Then the cost of computing a total degree Gröbner basis for I is

$$\begin{aligned} &O(L_q(n, d)^2 L_q(n, d - r + 1)) + \\ &O(L_q(n, d - r + 1)^2 L_q(n, d - r)^2 L_q(n, 2(d - r + 1) - 2)). \end{aligned}$$

for $n \to \infty$.

Proof. First, one divides each polynomial in B of degree $> d - r + 1$ by the polynomials in B of degree $\leq d - r + 1$ and replaces the former with the remainder of the divisions. One needs to perform up to $L_q(n, d)$ divisions, each of them has a cost of $O(L_q(n, d) L_q(n, d - r + 1))$. The resulting set of generators is such that every element has degree smaller than or equal to

$d-r+1$ and all the monomials of degree $d-r+1$ are divisible by the leading monomial of one of the generators. Then one performs a Gaussian reduction with cost $O(L_q(n,d-r+1)^3)$ so that all the generators $g \in B$ satisfy $\deg(g-\mathrm{LT}(g)) < d-r+1$. Lastly, by Theorem 3.65 the complexity of building a Gröbner basis is $O(L_q(n,d-r+1)^2 L_q(n,d-r)^2 L_q(n,2(d-r+1)-2))$. Overall, the time complexity is the one stated, as the Gaussian reduction has cost negligible compared to applying Theorem 3.65. ■

Let us consider the quotient algebra $A = \mathbb{F}_q[z,x_1,\ldots,x_n]/(x_1^s - x_1,\ldots,x_n^s - x_n, z^r-1)$, with $s \geq q$, $2 \leq r < s$ and let $\mathcal{Y} = \{(b,a_1,\ldots,a_n) | b < r, a_i < s\}$ be the family of multisets that corresponds to the basis of A, $\{z^b x_1^{a_1}\ldots x_n^{a_n} | b < r, a_i < s\}$. Let $f_1,\ldots,f_m \in A_D/A_{D-1}$ for some $D \geq r$ be with coefficients taken uniformly and independently at random from $\mathbb{F}_q$ and let d_{reg} be their degree of regularity.

Theorem 4.17. *Let s and D be fixed integers. If there exists $d < D$ such that*

$$m \geq \frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|},$$

then

$$\mathbb{P}(d_{reg} \leq d+D) \geq 1 - q^{|\mathcal{Y}^{d+D}| - m|\mathcal{Y}^d|} + O(n^d q^{-Cn^D})$$

for a positive constant C as $n \to \infty$.

Proof. Let p be the probability that the homogeneous Macaulay matrix $\overline{M}_{d+D}$ has linearly dependent columns. Then

$$\begin{aligned} p \leq & \sum_{v=0}^{|\mathcal{Y}^d|-1} q^{(|\mathcal{Y}^d|-v+1)v + |\mathcal{Y}^{d+D}| - \ell(v) - (|\mathcal{Y}^d|-v)m} = q^{|\mathcal{Y}^{d+D}| - m|\mathcal{Y}^d|} \\ & + \sum_{v=1}^{|\mathcal{Y}^d|-1} q^{(|\mathcal{Y}^d|-v+1)v + |\mathcal{Y}^{d+D}| - \ell(v) - (|\mathcal{Y}^d|-v)m}. \end{aligned} \tag{4.21}$$

This holds, because in the proof of Theorem 4.1, we never used the hypothesis that all the variables had multiplicity bounded by the same q. By setting z to be the first variable (for the lexicographic ordering), Corollary 2.44 (and hence Lemma 4.7) still apply.

In order to complete the proof, it is necessary to show that for some positive constant C, (4.21) $\in O(n^d q^{-Cn^D})$. First, we need to slightly adjust the definitions of v_δ and $v_{\delta,x}$. Let $0 \le \delta \le d$. We define σ and t as follows: if $d - \delta < r - 1$, then $\sigma = 0$ and $t = d - \delta$. On the other hand, if $d - \delta \ge r - 1$, then σ and t are the unique non negative integers such that

$$d - \delta = r - 1 + (\sigma - 1)(s - 1) + t, \quad t < s - 1.$$

We consider the family of all multisets in $\mathcal{Y}^d$ of the form

$$(r-1, q-1, \ldots, q-1, u, a_{\sigma+1}, \ldots, a_n)$$

where $u \ge t$ and for some $a_{\sigma+1}, \ldots, a_n$. We denote by v_δ the largest index v such that X_v belongs to that family. The same conventions as for the case without z apply here.

Let $0 \le x \le n + 1 - \sigma - 1$. We consider the family of all multisets in $\mathcal{Y}^d$ of the form

$$(r-1, q-1, \ldots, q-1, t, 0, \ldots, 0, a_{\sigma+x+1}, \ldots, a_n)$$

where $a_{\sigma+x+1} \neq 0$. We denote by $v_{\delta,x}$ the largest v such that X_v belongs to that family.

We notice that asymptotically, for every e, $|\mathcal{Y}^e|$ and $|\mathcal{X}^e|$ behave similarly:

$$|\mathcal{X}^e| = l_q(n,d) = \left(\!\!\binom{n}{e}\!\!\right) + O(n^{e-1}),$$
$$|\mathcal{Y}^e| = l_{r,s}(n+1,e) = \left(\!\!\binom{n}{e}\!\!\right) + O(n^{e-1}).$$

Using this fact and essentially the same proofs of Section 4.2, one can prove the following statements:

Lemma 4.18. *If $\delta = 0$ then $\ell(v_{0,x}) = 0$ for $x < n - \sigma$ and*

$$\ell(v_{0,n-\sigma}) = l_{b,q}(n - \sigma, \delta + D),$$

where $b = q - t$ if $\sigma > 0$ and $r - t$ otherwise.

If $\delta > 0$, then

$$\ell(v_{\delta,x}) = l_{b,q}(n+1-\sigma,\delta+D) - l_q(n+1-\sigma-x-2,\delta+D),$$

where $b = q-t$ if $\sigma > 0$ and $r-t$ otherwise.

Lemma 4.19. *Let $v \in I_{\delta,x}$. Then $\ell(v+1) - \ell(v) \leq l_s(n+1-\sigma-x-2, D)$.*

Lemma 4.20. *Lemma 4.11 applies in this new setting, with $E_n(v) = Pv - v^2 - \ell(v)$, where $P = \left(|\mathcal{Y}^d| + 1 + \frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|}\right)$.*

Using these three lemmas and the fact that the asymptotical behaviour of $|\mathcal{X}^e|$ and $|\mathcal{Y}^e|$ is the same, it is possible to replicate the arguments in Section 4.2 to conclude that for every $v \in \{1,\ldots,|\mathcal{Y}^d|-1\}, E(n) < -Cn^D$ for some positive constant C. As a consequence if $m \geq \frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|}$, then

$$p \leq q^{|\mathcal{Y}^{d+D}| - m|\mathcal{Y}^d|} + O(n^d q^{-Cn^D}).$$

■

In order for Theorem 4.17 to work, one needs $m \geq \frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|} \geq \frac{l_q(n,d+D)}{l_q(n,d)}$ polynomials. We show that for n sufficiently large,

$$\frac{l_{r,s}(n+1-j,d+D)}{l_{r,s}(n+1-j,d)} < \frac{l_q(n,d+D)}{l_q(n,d)}$$

for a constant j that depends on q, d, and D.

This implies that it is possible to use the hybrid method described in the previous section by guessing a constant amount of variables if one has access to only $m \geq \frac{l_q(n,d+D)}{l_q(n,d)}$ equations instead of $m \geq \frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|}$.

Proposition 4.21. *Let $2 \leq r < s$, $q \leq s$, and $d < D$ be fixed positive integers. Then there exists n_0 sufficiently large such that for every $n \geq n_0$,*

- *If $q > 2$, then*

$$\frac{l_{r,s}(n-1,d+D)}{l_{r,s}(n-1,d)} < \frac{l_q(n,d+D)}{l_q(n,d)},$$

- *If $q = 2$, then*
$$\frac{l_{r,s}(n-2d-D,d+D)}{l_{r,s}(n-2d-D,d)} < \frac{l_q(n,d+D)}{l_q(n,d)}.$$

Proof. First we analyse $\frac{l_{r,s}(n+1-j,d+D)}{l_{r,s}(n+1-j,d)}$. Since $r \geq 2$ and $s > r$, we have that for every constant $j \geq 1$,

$$\begin{aligned}
&\frac{l_{r,s}(n+1-j,d+D)}{l_{r,s}(n+1-j,d)} \leq \frac{l_s(n-j,d+D)+l_s(n-j,d+D-1)+O(n^{d+D-2})}{l_s(n-j,d)} = \\
&= \frac{d!}{(d+D)!}(n-j+d)\dots(n-j+d+D-1)+ \\
&+ \frac{d!(d+D)}{(d+D)!}(n-j+d)\dots(n-j+d+D-2)+O(n^{D-2}) = \\
&= \frac{d!}{(d+D)!}\left(n^D + n^{D-1}\left(\sum_{i=0}^{D-1} -j+d+i\right) + (d+D)n^{D-1}+\right) + O(n^{D-2}).
\end{aligned}$$

For $q > 2$ we have that

$$\frac{l_q(n,d+D)}{l_q(n,d)} = \frac{n^D + n^{D-1}(\sum_{i=0}^{D-1} d+i) + O(n^{D-2})}{(d+D)\dots(d+1)}.$$

The smallest j that satisfies the claim of the theorem is $j = 2$. Indeed

$$\begin{aligned}
&\frac{l_{r,s}(n-j+1,d+D)}{l_{r,s}(n-j+1,d)} - \frac{l_q(n,d+D)}{l_q(n,d)} \leq \\
&\leq n^{D-1}\frac{(d-j)D+d+D-dD}{(d+D)\dots(d+1)} + O(n^{D-2}) = \frac{n^{D-1}(d+D-jD)}{(d+D)\dots(d+1)} + O(n^{D-2}),
\end{aligned}$$

which for n sufficiently large is smaller than 0 for $j > d/D + 1$, that is equivalent to $j > 1$ as $d < D$.

On the other hand, if $q = 2$, then

$$\frac{l_q(n,d+D)}{l_q(n,d)} = \frac{n^D - n^{D-1}(\sum_{i=0}^{D-1} d+i) + O(n^{D-2})}{(d+D)\dots(d+1)}.$$

By repeating similar calculations as above, one gets that the smallest j that

satisfies the claim is $j = 2d + D + 1$. Indeed

$$\begin{aligned}&\frac{l_{r,s}(n-j+1,d+D)}{l_{r,s}(n-j+1,d)} - \frac{l_q(n,d+D)}{l_q(n,d)} \leq \\ \leq & n^{D-1}\frac{(-j+d)D+d+D+D(D-1)+dD}{(d+D)\dots(d+1)} + O(n^{D-2}) = \\ = & \frac{n^{D-1}(D(-j+2d+D)+d)}{(d+D)\dots(d+1)} + O(n^{D-2}),\end{aligned}$$

which for n sufficiently large is smaller than 0 for $j > 2d + D + d/D$, that is $j > 2d + D$. ■

Remark 4.22. Let $r \leq D$ be positive integers and let us consider a system of polynomial equations with coefficients in $\mathbb{F}_q$

$$P_1 = 0, \dots, P_m = 0, x_1^q - x_1 = 0, \dots, x_n^q - x_n = 0, \tag{4.22}$$

where $\deg(P_i) = D$ and $P_i = f_{i,D} + f_{i,D-1} + \cdots + f_{i,D-r+1} + g_i$, with $f_{i,j}$ be homogeneous of degree j and $\deg(g_i) \leq D - r$. Let $P_i' = f_{i,D} + z f_{i,D-1} + \cdots + z^{r-1} f_{i,D-r+1} + g_i \in \mathbb{F}_q[z, x_1, \dots, x_n]$.

Solving (4.22) is equivalent to solving

$$\begin{cases} P_1' = 0, \dots, P_m' = 0, & \\ z^r - 1 = 0, & x_1^s - x_1 = 0, \dots, x_n^s - x_n = 0, \\ z - 1 = 0, & x_1^q - x_1 = 0, \dots, x_n^q - x_n = 0, \end{cases} \tag{4.23}$$

where s is the smallest multiple of q such that $s > r$.

Let $I = (z^r - 1, x_1^s - x_1, \dots, x_n^s - x_n)$ and let us assume that there exists $d < D$ for which the degree of regularity of $P_1' + I, \dots, P_m' + I \in \mathbb{F}_q[z, x_1, \dots, x_n]/I$ is $d_{\text{reg}} = d + D$. Let $Q_1 + I, \dots, Q_l + I$ be the set of generators of the ideal $(P_1' + I, \dots, P_m' + I)$ given by the nonzero row vectors of the reduced row echelon form of M_{d+D}, the Macaulay matrix of $P_1' + I, \dots, P_m' + I$. We choose as filtered basis for $\mathbb{F}_q[z, x_1, \dots, x_n]/I$ the set $\{(b, a_1, \dots, a_n) | 0 \leq b < r, 0 \leq a_i < s\}$. We notice that $l \leq L_s(n, D) L_{r,s}(n+1, d)$.

Let $Q'_i + (x_1^q - x_1, \ldots, x_n^q - x_n, z-1)$ be the projection of $Q_i + I$ to

$$\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^q - x_1,\ldots,x_n^q - x_n) \cong \mathbb{F}_q[z,x_1,\ldots,x_n]/(x_1^q - x_1,\ldots,x_n^q - x_n, z-1)$$

so that no monomials of Q'_i is divisible by any among $x_1^q,\ldots,x_n^q$.

Then $Q'_1,\ldots,Q'_l,x_1^q - x_1,\ldots,x_n^q - x_n$ is a set of generators for the ideal $(P_1,\ldots,P_m,x_1^q - x_1,\ldots,x_n^q - x_n)$. This set of generators satisfies the hypotheses of Corollary 4.16 using the same argument described for the case $r = 2$ and $q = 2$. As a consequence, by choosing $r = D$, the overall cost of computing a Gröbner basis can be broken down as follows for constant d, D and q and $n \to \infty$:

- Cost of Gaussian reduction of d matrices with at most $L_{r,s}(n+1, d+D)$ columns and at most $L_q(n,D)L_{r,s}(n+1,d)$ rows. Overall it is in $O(n^{3(d+D)})$.
- Cost of applying the steps described in Corollary 4.16 (i.e. division, Gaussian reduction, and application of Theorem 3.65). Overall it is $O(n^{6(d+1)-4})$.

The cost of the second step is negligible compared to the first one as $d < D$. So, the total complexity is $O(n^{3(d+D)})$.

By Theorem 4.17, if for every $i = 1,\ldots,m$ and $j = D,\ldots,D-r+1$ the coefficients of the polynomials $f_{i,j}$ are chosen uniformly and independently at random from $\mathbb{F}_q$ and if

$$\left|\bigcup_{\delta=0}^{D} \mathcal{Y}^\delta\right| \geq m \geq \frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|},$$

then from the previous complexity analysis we can deduce that the cost of computing a Gröbner basis of $(P_1,\ldots,P_m,x_1^q - x_1,\ldots,x_n^q - x_n)$ is $O(n^{3(d+D)})$ operations with probability tending to 1.

Lastly, by using Proposition 4.21, the same complexity is required also in the case of

$$\frac{|\mathcal{Y}^{d+D}|}{|\mathcal{Y}^d|} \geq m \geq \frac{l_q(n,d+D)}{l_q(n,d)}.$$

Chapter 5

Mersenne Low Hamming Combination search problem

The following is based on the joint work with Alessandro Budroni [BT19]. In this chapter we present our approach to the cryptanalysis of the AJPS cryptosystem designed by Aggarwal, Joux, Prakash, and Santha [AJPS18]. This public-key encryption scheme is similar to the NTRU cryptosystem [HPS98] and employs the properties of the Mersenne primes.

This is the second iteration of the cryptosystem, first presented in [AJPS17]. The previous version was successfully attacked by Beunardeau, Connolly, Géraud, and Naccache [BCGN17]. This led the authors to redefine the protocol and the parameters. The hard mathematical problem that the last version is based upon is called *Mersenne Low Hamming Combination Search Problem* (MLHCombSP).

Our approach targets the current version of the proposal and employs a reduction of MLHCombSP to an Integer Linear Programming problem.

5.1 Description of the Problem

Definition 5.1. Let N be a prime number and let $q = 2^N - 1$. Then q is called a *Mersenne number*. If q is also prime, then it is called *Mersenne prime*.

Let $q = 2^{N-1}$ be a Mersenne prime and let $\text{seq}_N : \{0,...,q-1\} \to \{0,1\}^N$

be the map that associates to each $A \in \{0,\dots,q-1\}$ the corresponding N-bit binary representation $\mathrm{seq}_N(A)$ with the most-significant bit to the left.

We extend the function seq_N also to elements in $\mathbb{Z}_q$: let us consider an integer $0 \leq A < q$, seq_N maps $A + (q) \in \mathbb{Z}_q$ to the N-bit binary representation of A. We define the *Hamming weight* $w(A)$ of A as the Hamming weight of $\mathrm{seq}_N(A)$, i.e. the number of '1'-valued bits in $\mathrm{seq}_N(A)$.

Lemma 5.2. *Let $k \geq 0$ be an integer and let $A \in \mathbb{Z}_q$. Then $\mathrm{seq}_N(2^k A)$ corresponds to a cyclic rotation of $\mathrm{seq}_N(A)$ of k positions to the left and $\mathrm{seq}_N(2^{-k}A)$ corresponds to a cyclic rotation of k positions to the right.*

Proof. Clearly it is sufficient to prove the statement for $k = 1$. We write $\mathrm{seq}_N(A) = (A_{N-1},...,A_1,A_0)$, with $A_i \in \{0,1\}$ and we set A_{N-1} to be the most significant bit of A. This means that

$$A = A_{N-1} \cdot 2^{N-1} + ... + A_1 \cdot 2 + A_0 + (q).$$

It follows that

$$\begin{aligned} 2 \cdot A &= A_{N-1} \cdot 2^N + A_{N-2} \cdot 2^{N-1} + ... + A_1 \cdot 2^2 + A_0 \cdot 2 + (q) = \\ &= A_{N-2} \cdot 2^{N-1} + ... + A_1 \cdot 2^2 + A_0 \cdot 2 + A_{N-1} + (q). \end{aligned}$$

Then $\mathrm{seq}_N(2 \cdot A) = (A_{N-2},...,A_0,A_{N-1})$, i.e. the left cyclic rotation of 1 position of $\mathrm{seq}_N(A)$. The second part of the statement follows trivially. ■

The security of the first version of the AJPS cryptosystem ([AJPS17]) relies on the assumption that the following problem is hard to solve.

Mersenne Low Hamming Ratio Search Problem Let $q = 2^N - 1$ be a Mersenne prime, $h < N$ be an integer, F and G be two elements of $\mathbb{Z}_q$ such that $w(F) = w(G) = h$. Let $H \in \mathbb{Z}_q$ be defined as

$$H = \frac{F}{G}. \tag{5.1}$$

The *Mersenne Low Hamming Ratio Search Problem* (MLHRatioSP) is the problem of finding (F, G) knowing h and H.

The most recent version of their proposal, instead, is based on the assumption that the following problem is hard to solve.

Mersenne Low Hamming Combination Search Problem Let $q = 2^N - 1$ be a Mersenne prime, $h < N$ be an integer, R be a random element from $\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\}$, and $F, G \in Z_q$ be such that $w(F) = w(G) = h$. Let $T \in \mathbb{Z}_q$ be defined as

$$T = RF + G. \tag{5.2}$$

The *Mersenne Low Hamming Combination Search Problem* (MLHCombSP) is the problem of finding (F, G) knowing h and the pair (R, T).

In [AJPS17], the authors suggest to choose N and h to be such that $\binom{N-1}{h-1} \geq 2^\lambda$ and $4h^2 < N$, for a desired λ-bit security level. After the publications of the attacks by Beunardeau et al. [BCGN17] and De Boer et al. [dBDJdW18], the authors revised the choice of the parameters in [AJPS18]) to be such that $h = \lambda$ and $10h^2 < N$.

5.1.1 Previous Attacks

Brute force attack In [AJPS17], Aggarwal et al. show that a brute force attack to the MLHRatioSP would require $\binom{N-1}{h-1}$ divisions in $\mathbb{Z}_q$. This attack consists in assuming that one of the two secret numbers, say F, has a 1 in the most significant bit (condition that can be obtained by a rotation of $\text{seq}_N(F)$). Then one should check, for every N-bit number L with 1 as most significant bit and weight h, if $G = L/H$ has weight h. If that is the case, then (L, G) is a correct solution. This approach does not apply to the MLHCombSP, which instead requires $\binom{N}{h}$ trials.

Meet-in-the-Middle attack De Boer et al. show in [dBDJdW18] that a Meet-in-the-Middle attack to MLHRatioSP is possible and has complexity $\tilde{O}\left(\sqrt{\binom{N-1}{h-1}}\right)$

on classical computers and $\tilde{O}\left(\sqrt[3]{\binom{N-1}{h-1}}\right)$ on quantum computers. Here, $f \in \tilde{O}(g)$ if $f \in O(g\log(g)^k)$ for some k.

Weak Keys and Lattice attack Using the parameters' setting in [AJPS17], Beunardeau et al. describe in [BCGN17] a weak key attack against the MLHRatioSP in the case of both F and G having all their '1'-valued bits in the right halves of $\mathrm{seq}_N(F)$ and $\mathrm{seq}_N(G)$, i.e. $F, G < \sqrt{2^N}$. This event happens with probability $\approx 2^{-2h}$.

Following the above idea, Beunardeau et al. also present a more general attack to the MLHRatioSP which consists in guessing a decomposition of $\mathrm{seq}_N(F)$ and $\mathrm{seq}_N(G)$ into substrings such that all the '1'-valued bits are "close" to the right-most bit of such substrings. Then F and G can be recovered through a lattice reduction algorithm such as LLL ([LLL82]). The asymptotical complexity of this attack (under some heuristical assumptions) is presented in [dBDJdW18].

In [AJPS18], the authors state that the above attack likely generalises to the MLHCombSP. Building directly on the work presented in [dBDJdW18], we show in the next subsection that this is true. However we refer the reader to [BCGN17] and [dBDJdW18] for a more detailed description.

5.1.2 Generalization of the Beunardeau et al. attack on MLHCombSP

Let us consider an interval-like partition $\mathcal{P} = \{P_1, \ldots, P_k\}$ of $\{0, \ldots, N-1\}$, i.e. each element of $\mathcal{P}$ is of the form $P_i = \{a_i, a_i + 1, \ldots, b_i - 1, b_i\}$, with $0 \leq a_i < b_i \leq N-1$ and such that their union is disjoint and equal to $\{0, \ldots, N-1\}$. This induces a partition of the string $\mathrm{seq}_N(A)$ for $A \in \mathbb{Z}_q$ into substrings. By abusing notation we call $P_1, \ldots, P_k$ these substrings. Overall, the sum of the weights of the substrings is $w(A)$.

Let $F, G \in \mathbb{Z}_q$ be such that $w(F) = w(G) = h$. Let us consider two interval-like partitions $\mathcal{P} = \{P_1, \ldots, P_k\}$, $\mathcal{Q} = \{Q_1, \ldots, Q_l\}$ of $\{0, \ldots, N-1\}$ such that

in every substring $P_1,\ldots,P_k$ of $\mathrm{seq}_N(F)$ and in every substring $Q_1,\ldots,Q_l$ of $\mathrm{seq}_N(G)$, the '1'-valued bits appear on the right half of the substring. If this is the case, then they represent relatively short vectors in a space $\mathbb{R}^{k+l}$. Our goal is to construct a lattice that contains the integer representations of the substrings $P_1,\ldots,P_k,Q_1,\ldots,Q_l$ and such that the solution (F,G) corresponds to the shortest vector in the lattice.

Let $\mathcal{P}=\{P_1,..,P_k\}$ and $\mathcal{Q}=\{Q_1,...,Q_l\}$ be two interval-like partitions of $\{0,...,N-1\}$ and let $(R,T)\in\mathbb{Z}_q^2$ be the public parameters of an MLHCombSP instance. Let p_i,q_i be the smallest elements of P_i,Q_i respectively. Let us consider the following integer lattice in $\mathbb{R}^{k+l+1}$:

$$\mathcal{L}_{\mathcal{P},\mathcal{Q},R,T}=\left\{(x_1,...,x_k,y_1,...,y_l,u)\mid R\cdot\sum_{i=1}^{k}2^{p_i}\cdot x_i+\sum_{j=1}^{l}2^{q_i}\cdot y_i-uT=0\right\}.$$

The above defined lattice has determinant $\det(\mathcal{L}_{\mathcal{P},\mathcal{Q},R,T})=q$ and dimension $d=k+l+1$. Let $(F,G)\in\mathbb{Z}_q^2$ be such that $w(F)=w(G)=h$ and $RF+G=T$ as in a MLHCombSP instance. Let us define the vector

$$\mathbf{s}=(f_1,...,f_k,g_1,...,g_l,1)\in\mathcal{L}_{\mathcal{P},\mathcal{Q},R,T},$$

where $0\le f_i<2^{|P_i|}$ and $0\le g_j<2^{|Q_j|}$ are the unique natural numbers such that $\sum_{i=1}^{k}f_i\cdot 2^{p_i}+(q)=F$ and $\sum_{j=1}^{l}g_j\cdot 2^{q_j}+(q)=G$. One wishes to find the vector $\mathbf{s}$ through some lattice reduction algorithm applied to $\mathcal{L}_{\mathcal{P},\mathcal{Q},R,T}$.

The lattice $\mathcal{L}_{\mathcal{P},\mathcal{Q},R,T}$ is very similar to the one defined in [dBDJdW18] for the MLHRatioSP and their success probability analysis of the attack holds for this case too. Therefore the following conclusions follow directly from the work of de Boer et al..

Proposition 5.3. *Let us assume Heuristic 3 of [dBDJdW18], and let $\mathcal{P}$ and $\mathcal{Q}$ be interval-like partitions of $\{0,...,N-1\}$ with block size at least $N/d+\Theta(\log N)$, where $d=k+l+1$ with $k=|\mathcal{P}|$ and $l=|\mathcal{Q}|$. The success probability of finding the vector $\mathbf{s}\in\mathcal{L}_{\mathcal{P},\mathcal{Q},R,T}$ using a SVP-oracle is $2^{-2h+o(1)}$.*

Here, $f\in\Theta(g)$ if there exist positive integers n_0, C_1, and C_2 such that for

every $n \geq n_0$, $C_1 g(n) \leq |f(n)| \leq C_2 g(n)$.

Remark 5.4. The above attack is actually a simplified version of the attack of Beunardeau et al. Indeed, a more general attack can be mounted by considering partitions of varying size. This variation increases the number of secret keys that can be successfully attacked.

This lattice attack is successful against the parameters chosen in the first version of the AJPS cryptosystem. However, in the most recent versionthe authors revisited the parameters in order to withstand the attack by de Boer et al..

5.1.3 Integer Linear Programming

An *Integer Linear Programming* (ILP) problem of dimension n in its *canonical form* is defined as follows. Given a matrix $A = (a_{ij}) \in \mathbb{Q}^{m \times n}$ and two vectors $(c_1, \ldots, c_n) \in \mathbb{Q}^n$ and $(b_1, \ldots, b_m) \in \mathbb{Q}^m$, find $(x_1, \ldots, x_n)$ that minimizes (or maximises) the quantity

$$\sum_{j=1}^{n} c_j x_j$$

subject to

$$\begin{cases} \sum_{j=1}^{n} a_{ij} x_j \leq b_i, & \text{for } i = 1, \ldots, m \\ x_j \geq 0, & \text{for } j = 1, \ldots, n \\ x_j \in \mathbb{Z} & \text{for } j = 1, \ldots, n. \end{cases}$$

An *ILP-oracle* is an oracle that solves any ILP instance.

Solving a general ILP problem is proved to be **NP**-hard [Pap81]. Nevertheless, understanding the complexity of specific families of ILP problems is not an easy task: it can widely vary from case to case [Sch86]. For example, when the number of variables is fixed, or when the problem can be reduced to a simple *Linear Programming* problem, there are algorithms that find a solution in polynomial time (see e.g. [Len83, Wol98]).

Nowadays there exist families of ILP solving algorithms, for example *Branch and Bound* [MJSS16], *Lagrange relaxation* [Fis81], *Column Generation* [App69], and

the *Cutting Planes* [MMWW02], whose implementations [CO18, GO18] are able to solve in practice relatively challenging instances.

5.2 ILP Reduction

Let $\varphi : \mathbb{Z}_q \to \mathbb{Z}_q$ be a bijection. It induces a bijection $\tilde{\varphi}$ from the family of k-subsets of $\mathbb{Z}_q$ to the family of k-subsets of $\mathbb{Z}_q$ sending $\mathcal{U} \overset{\tilde{\varphi}}{\mapsto} \varphi(\mathcal{U})$.

Proposition 5.5. *Let k be a positive integer. Let us consider the uniform probability function on $\Omega = \{\mathcal{U} \subseteq \mathbb{Z}_q | |\mathcal{U}| = k\}$ and let $\mathcal{V}$ be a fixed subset of $\mathbb{Z}_q$. Then $\mathbb{E}_\Omega(|\varphi(\mathcal{U}) \cap \mathcal{V}|) = \frac{k|\mathcal{V}|}{q}$.*

Proof. As $\tilde{\varphi}$ is a bijection on the k-subsets of $\mathbb{Z}_q$, as $\mathcal{U}$ varies, $\varphi(\mathcal{U})$ runs over all the possible k-subsets of $\mathbb{Z}_q$ once. The random variable given by the size of the intersection $\varphi(\mathcal{U}) \cap \mathcal{V}$ can be modelled by a hypergeometric distribution in k draws from an urn with $q - |\mathcal{V}|$ black balls and $|\mathcal{V}|$ white balls. By Example 2.36, the expected value of the size of the intersection is $\frac{k|\mathcal{V}|}{q}$, as stated. ■

Proposition 5.6. *Let $\mathcal{U}, \mathcal{V} \subseteq \mathbb{Z}_q$ and let us consider the uniform probability function on $\Omega = \{\varphi : \mathbb{Z}_q \to \mathbb{Z}_q | \varphi \text{ is bijective}\}$. Then $\mathbb{E}_\Omega(|\varphi(\mathcal{U}) \cap \mathcal{V}|) = \frac{|\mathcal{U}||\mathcal{V}|}{q}$.*

Proof. It is sufficient to show that $\varphi(\mathcal{U})$ is uniformly distributed in the family of $|\mathcal{U}|$-subsets of $\mathbb{Z}_q$. In that case, the expected value is the one of a hypergeometric distribution. Let $\mathcal{U}'$ be a $|\mathcal{U}|$-subset of $\mathbb{Z}_q$. We claim that the number of bijections sending $\mathcal{U}$ to $\mathcal{U}'$ does not depend on $\mathcal{U}'$. Indeed the number of these functions is the product

$$|\{\text{bij} : \mathcal{U} \to \mathcal{U}'\}||\{\text{bij} : \mathbb{Z}_q \setminus \mathcal{U} \to \mathbb{Z}_q \setminus \mathcal{U}'\}| = k!(n-k)!,$$

which is independent of $\mathcal{U}'$. ■

Because of the two previous propositions, we are going to use the following heuristic:

Heuristic 5.7. let $\mathcal{U}$, $\mathcal{V}$ be subsets of $\mathbb{Z}_q$ with no particular structure with respect to the ring operations and let $\varphi : \mathbb{Z}_q \to \mathbb{Z}_q$ be a bijection defined by $\varphi(X) = -RX + T$. Then the linear equation with constraints

$$\begin{cases} \varphi(X) = Y, \\ X \in \mathcal{U}, \\ Y \in \mathcal{V} \end{cases} \tag{5.3}$$

has $\leq \left\lceil \frac{|\mathcal{U}||\mathcal{V}|}{q} \right\rceil$ solutions.

Let $R \in \mathbb{Z}_q^*$ and $T = FR + G$ for some F and G chosen independently at random from $\mathbb{Z}_q$ according to some distribution. Let $\mathcal{U}$ and $\mathcal{V}$ be such that $|\mathcal{U}||\mathcal{V}| < q$, then assuming Heuristic 5.7, (5.3) has a unique solution. Moreover, that solution is (F, G) with probability $\mathbb{P}(F \in \mathcal{U}) \cdot \mathbb{P}(G \in \mathcal{V})$.

Let $R \in \mathbb{Z}_q^*$ and $T = FR + G$ for some F and G of weight h. Let us consider the systems

$$\begin{cases} T - RX = Y, \\ X \in \mathcal{U}, \\ Y \in \mathcal{V} \end{cases} \tag{5.4}$$

and

$$\begin{cases} T' + qa - R'x = y, \\ x \in \mathcal{U}', \\ y \in \mathcal{V}', \\ a \in \mathbb{Z}, \end{cases} \tag{5.5}$$

where T' and R' are the integer representatives of T and R in $\{0, \ldots, q-1\}$ and $\mathcal{U}'$ and $\mathcal{V}'$ are the sets of representatives of $\mathcal{U}$ and $\mathcal{V}$ in $\{0, \ldots, q-1\}$.

Proposition 5.8. *There is a one-to-one correspondence between the solutions of* (5.4) *and the solutions of* (5.5).

Proof. First, we notice that given $x, y \in \{0, \ldots, q-1\}$ there exists at most one a such that (x, y, a) is a solution of (5.5).

Let us consider the map $\varphi : \{0,\dots,q-1\}^2 \times \mathbb{Z} \to \mathbb{Z}_q^2$ sending $(x,y,a) \mapsto (x \bmod q, y \bmod q)$. We claim that the restriction of φ to the set of solutions of (5.5) is a bijection onto the set of solutions of (5.4). Clearly the restriction of φ maps a solution to a solution. Injectivity is granted by the fact that $x,y \in \{0,\dots,q-1\}$ and for the fact that if (x,y,a) and (x,y,a') are solutions, then $a = a'$. Lastly the restriction is surjective: let (X,Y) be a solution of (5.4) and let (x,y) be their unique representatives in $\{0,\dots,q-1\}$, then $RX + Y - T = 0$ if and only if for every pair of representatives x of X and y of Y in $\mathbb{Z}$, there exists a such that $R'x + y - T' = qa$. ■

If $\mathcal{U}'$ and $\mathcal{V}'$ are intervals, then given an optimisation vector (c_1,c_2,c_3) an ILP-oracle produces a solution to (5.5). If the system of inequalities has a unique solution, then an ILP-oracle will produce it for every nonzero optimising vector.

Finding good choices of intervals $\mathcal{U}'$ and $\mathcal{V}'$ (i.e. small and containing F and G with high probability) is difficult for the system (5.5). At the cost of increasing the number of variables, one can split $\mathcal{U}'$ in a union of disjoint intervals, in order to decrease the size of $\mathcal{U}'$ and at the same time increase the probability that $F \in \mathcal{U}'$.

One such way is to fully exploit the fact that F used to generate (5.5) has weight exactly h to establish the following system of linear inequalities in the integer variables $x,y,a,n_1,\dots,n_N$:

$$\begin{cases} T' + qa - R'x = y, \\ x = \sum_{i=1}^{N} n_i 2^{i-1}, \\ 0 \le n_i \le 1, \quad \text{for } i = 1,\dots,N \\ \sum_{i=1}^{n} n_i = h, \\ y \in \mathcal{V}' \end{cases} \tag{5.6}$$

for an interval $\mathcal{V}'$. Using these constraints results in having $\mathcal{U}'$ of (5.5) of size $|\mathcal{U}'| = \binom{N}{h}$ and $F \in \mathcal{U}'$ with probability 1. On the other hand, the number of variables increases from 3 to $N+3$. We notice that $\mathcal{U}'$ is no longer an interval.

We could achieve this, while at the same time maintaining the linearity of the inequalities, only by adding the dummy variables $n_1, \dots n_N$.

In 5.2.1, we present a way to perform a size-probability trade-off in order to choose in advance either the number of variables of the ILP problem to be solved or the success probability.

Let $\Omega = \{A \in \mathbb{Z}_q | w(A) = h\}$ be equipped with the uniform probability function and let $E : \Omega \to \mathbb{R}$ be the random variable that associates to $A \in \mathbb{Z}_q$ the number of '0'-valued bits in $\text{seq}_N(A)$ before the first '1'-valued bit (counting from the most significant bit) .

Proposition 5.9. *Let $R \in \mathbb{Z}_q^*$ and let (F, G) be taken at random from the space of all the possible keys $\Omega = \{(F, G) \in \mathbb{Z}_q^2 | w(F) = w(G) = h\}$ with uniform probability function. Let $\mathcal{U} \subseteq \mathbb{Z}_q$ be such that $(F, G) \in \Omega$ implies $F \in \mathcal{U}$. Let $\mathcal{V} = \{2^h, \dots, 2^{N-t} - 2^{N-t-h}\} \subseteq \mathbb{Z}_q$ for some t. The data R, F, G, $\mathcal{U}$ and $\mathcal{V}$ induce a system (5.4). The probability that (F, G) is a solution of this system is equal to*

$$1 - C(t-1),$$

where $C(t) = \mathbb{P}(E \leq t)$ is the cumulative distribution function of the negative hypergeometric distribution of an urn with h black balls and $N - h$ white balls.

Proof. By the choice of $\mathcal{U}$ and $\mathcal{V}$, the system (5.4) admits (F, G) as solution if and only if $G \in \mathcal{V}$, i.e. if $E(G) \geq t$.

The probability $\mathbb{P}(E \geq t)$ is given by $1 - C(t-1)$, since the number of '0'-valued bits before the first '1'-valued bit is modelled by the negative hypergeometric distribution (see Example 2.34) induced by an urn with N balls, $N - h$ of whom are white. ■

In particular, assuming Heuristic 5.7, if (F, G) is a solution of (5.4) and t is so that $t \geq \log_2(|\mathcal{U}|)$, then (F, G) is the unique solution.

Using a similar argument, we conclude the following

Proposition 5.10. *Let R, F, and G be as in Proposition 5.9. Let $\mathcal{U} = \{2^h, \dots, 2^{N-t_1} - 2^{N-t_1-h}\}$ and $\mathcal{V} = \{2^h, \dots, 2^{N-t_2} - 2^{N-t_2-h}\}$ be intervals of $\mathbb{Z}_q$ for some t_1, t_2. The*

probability that (F,G) *is a solution of the system* (5.4) *induced by* R, F, G, $\mathcal{U}$ *and* $\mathcal{V}$ *is equal to*

$$\mathbb{P}(E \geq t_1)\mathbb{P}(E \geq t_2).$$

In particular, assuming Heuristic 5.7, if (F,G) is a solution of (5.4) and $t_1 + t_2 > N$, then (F,G) is the unique solution.

Example 5.11. Let $q = 2^N - 1$ and let us consider $R \in \mathbb{Z}_q$ and let (F,G) be taken uniformly at random from the space of keys Ω. Let $\mathcal{U}' = \mathcal{V}' = \{2^h - 1, \ldots, 2^{(N-1)/2} - 1\}$. According to Heuristic 5.7, (5.4) induced by R, F, G, $\mathcal{U}$ and $\mathcal{V}$ has at most one solution. The probability that (F,G) is a solution (and, therefore, the unique one) is given by

$$\begin{aligned}&\mathbb{P}(E \geq (N-1)/2)\mathbb{P}(E \geq (N-1)/2) = \\ &= \left(\frac{\left(\frac{N-1}{2}\right)\left(\frac{N-1}{2}-1\right)\ldots\left(\frac{N-1}{2}-h+1\right)}{(N)(N-1)\ldots(N-h+1)}\right)^2 = \left(\frac{1}{2} + O\left(\frac{1}{\sqrt{N}}\right)\right)^{2h}.\end{aligned}$$

5.2.1 Merging

A possible approach to reduce the number of variables in the system of linear inequalities (5.6) is to merge more than one bit in a single dummy variable n_i. Say, for example, that we merge the bits in pairs; this means that each one of the n_i can assume values in $\{0,1,2,3\}$ and that the sum of all n_i varies between h and $2h$, as we prove in Proposition 5.13. At the same time, the number of variables in (5.6) goes from $N+3$ to $\lceil N/2 \rceil + 3$.

Example 5.12. Let us consider $\text{seq}_N(A) = (00010011)$. By merging the bits of the sequence in pairs, one gets $n_1 = 0$, $n_2 = 1$, $n_3 = 0$, $n_4 = 3$. The total sum is $n_1 + n_2 + n_3 + n_4 = 4 \leq 2h = 6$.

Using this method, it is possible to merge an arbitrary number of bits together. Let $S = \lceil N/s \rceil$. The system of linear inequalities that emerges after

merging bits in groups of s is the following:

$$\begin{cases} T' + aq - R'x = y, \\ x = \sum_{i=1}^{S} 2^{s(i-1)} n_i, \\ 0 \leq n_i \leq 2^s - 1, \text{ for } 0 \leq i \leq S, \\ h \leq \sum_{i=1}^{S} n_i \leq 2^{s-1} h, \\ y \in \mathcal{V}', \end{cases} \tag{5.7}$$

for an interval $\mathcal{V}'$.

Hence the number of variables can be established a priori. The more bits one merges, the harder it is that the ILP-oracle will return the correct solution, since the size of $\mathcal{V}'$ has to decrease in order to have at most one solution.

The following proposition shows that a solution to $-R'x + T' \equiv y \bmod q$ with $y \in \mathcal{V}'$ and $w(x) = h$ induces a solution to the system of inequalities (5.7) and, therefore, it can be obtained via an ILP-oracle.

Proposition 5.13. *Let $F, G \in \mathbb{Z}_q$ be such that $RF + G = T$, $w(F) = h$, and the representative of G in $\{0, \ldots, q-1\}$ is in the interval $\mathcal{V}'$. Then there exists a solution $(x, y, a, n_1, \ldots, n_S)$ of the system 5.7 with x and y representatives of F and G from $\{0, \ldots, q-1\}$.*

Proof. $y \in \mathcal{V}'$ by construction. The first equation is satisfied by definition. The second equation and the first inequality represent the fact that we are writing x in base 2^s. Hence the only statement remaining to prove is that $h \leq \sum_{i=1}^{S} n_i \leq 2^{s-1} h$ holds.

Let $F = F_0 2^0 + \ldots + F_{N-1} 2^{N-1}$, with $F_i \in \{0, 1\}$. We notice that $n_i = \sum_{j=0}^{s-1} F_{(i-1)s+j} 2^j$. For the fact that $\sum_{i=0}^{N-1} F_i = h$, we conclude that

$$\sum_{i=1}^{S} n_i = \sum_{i=1}^{S} \sum_{j=0}^{s-1} F_{(i-1)s+j} 2^j \geq \sum_{i=1}^{S} \sum_{j=0}^{s-1} F_{(i-1)s+j} = h. \tag{5.8}$$

We prove that $\sum_{i=1}^{S} n_i \leq 2^{s-1} h$ by induction on h. For $h = 1$, there is only one n_i with weight different from 0. We call it n_j. The string $\text{seq}_s(n_j)$ has weight 1,

so $n_j \leq 2^{s-1}$. If $h = 2$, either there is only one nonzero n_i, with $n_i \leq 2^{s-1} + 2^{s-2} \leq 2^{s-1} \cdot 2$, or there are two distinct n_i, n_j, each smaller than or equal to 2^{s-1}. In both case the statement holds.

Let us assume that the inequality holds for $h-2$. If $n_i \leq 2^{s-1}$ for every i, the inequality is satisfied, since at most h among the n_i can be different from 0. Hence we assume that there exists one j for which $n_j > 2^{s-1}$. This means that the Hamming weight of $\mathrm{seq}_s(n_j) \geq 2$. Then one gets:

$$\sum_i n_i \leq 2^s + \sum_{i \neq j} n_i.$$

The sum of the Hamming weights of $\mathrm{seq}_s(n_j)$, $j \neq i$ is at most $h-2$. By the inductive hypothesis, it follows that

$$\sum_i n_i \leq 2^s + 2^{s-1}(h-2) = 2^{s-1}h.$$

The proposition is proved. ■

The following proposition determines the size of $\mathcal{U}$ that one obtains from considering the system of linear inequalities (5.7).

Proposition 5.14. *Let $\mathcal{U}'$ be the set containing all $0 \leq A < q$, whose 2^s-ary representation $(n_1, \ldots, n_S)$ satisfies $0 \leq n_i \leq 2^s - 1$, for $0 \leq i \leq S$ and $h \leq \sum_{i=1}^{S} n_i \leq 2^{s-1}h$. Then*

$$|\mathcal{U}'| = \sum_{d=h}^{2^{s-1}h} l_{2^s}(S, d),$$

where $l_t(n, d)$ is the number of integer solutions of $z_1 + \ldots + z_n = d$, $0 \leq z_i < t$.

Proof. Let d be one of the values of $\sum_{i=1}^{S} n_i$. For each d, we consider all the possible configurations of $n_1, \ldots, n_S$. Since each of these is bounded by $2^s - 1$, the number of possible configurations is $l_{2^s}(S, d)$. ■

Examples

In Table 5.1 and Table 5.2 we present the size of the resulting ILP instances depending on the value of s and the corresponding success probability in two con-

crete cases. We select different choices of s and set $\mathcal{V} = \{2^h, \ldots, 2^{N-t} - 2^{N-t-h}\}$ for t satisfying $\log_2(|\mathcal{U}'|) + t \geq N$, where $|\mathcal{U}'|$ is constructed as in Proposition 5.14. The probability of $G \in \mathcal{V}$ is reported and corresponds to the success probability according to Proposition 5.9.

Table 5.1: $N = 1279$ and $h = 17$

s	Probability of success	Number of variables in ILP
1	$2^{-2.56}$	1282
2	$2^{-3.97}$	643
3	$2^{-6.13}$	430
4	$2^{-9.13}$	323
5	$2^{-12.94}$	259
6	$2^{-17.33}$	217
7	$2^{-21.73}$	186
8	$2^{-26.07}$	163
9	$2^{-30.47}$	146
10	$2^{-34.06}$	131

We notice that for the parameters of Table 5.1, $N < 10h^2$, so it violates the guidelines given in [AJPS18]. The reason for which these where chosen is to compare the success probability with the attack by Beunardeau et al. [BCGN17], which is performed against the previous version of the protocol.

By setting $10h^2 < N$ (for example $h = 11$), we get the results reported in Table 5.2.

Table 5.2: $N = 1279$ and $h = 11$

s	Probability of success	Number of variables in ILP
1	$2^{-1.36}$	1282
2	$2^{-1.78}$	643
3	$2^{-2.80}$	430
4	$2^{-4.29}$	323
5	$2^{-6.26}$	259
6	$2^{-8.64}$	217
7	$2^{-11.18}$	186
8	$2^{-13.71}$	163
9	$2^{-16.27}$	146
10	$2^{-18.42}$	131

Remark 5.15. It is possible to generalise all the presented approaches used to account for the weight of F to also account for the weight of G. However this would increase the dimension of the ILP problem. One would nonetheless significantly improve the probability of success.

5.3 A new family of weak keys

In [BCGN17] the authors introduce a family of weak keys for the MLHRatioSP. Those are the ones for which all the '1'-valued bits appeare in the right hand side of $\mathrm{seq}_N(F)$ and $\mathrm{seq}_N(G)$. As noted in [AJPS18], one can break keys in this family by performing a rational reconstruction ([Wan81]) of the quotient $H = F/G$. Aggarwal et al. also claim that the family of weak keys described in [BCGN17] extends to the MLHCombSP as well. This is easily verifiable using an ILP instance with constraints induced by (5.4) and by setting $\mathcal{U} = \mathcal{V} = \{2^h, \ldots, 2^{\lfloor N/2 \rfloor} - 2^{\lfloor N/2 \rfloor - h}\}$. Indeed $|\mathcal{U}||\mathcal{V}| < q$ and by construction $F \in \mathcal{U}$ and $G \in \mathcal{V}$. A key in this family appears with probability $\approx 2^{-2h}$.

By the properties of Mersenne numbers, cyclic shifts of seq_N of elements in $\mathbb{Z}_q$ and multiplication times powers of 2 behave well with respect to each other. This allows us to perform rotations when attacking the problem.

Let us consider a MLHCombSP instance $RF + G = T$ and let u, v be two integers. An equivalent problem is

$$(2^{v-u}R)(2^uF) + (2^vG) = 2^vT. \tag{5.9}$$

Since q is a Mersenne prime, $w(2^uF) = w(2^vG) = h$. This implies that among the N^2 possible shifts to the equation to solve, there is one for which 2^uF and 2^vG have representatives that are the smallest possible. In this sense, by choosing $\mathcal{U}$ and $\mathcal{V}$ as in Proposition 5.10 one can hope to get at least one successful instance (i.e. the solution of (5.4) is the solution of the MLHCombSP) for smaller values of t_1 and t_2. Our goal is to measure the likelihood of having at least one successful instance among the N^2.

Let $\Omega = \{A \in \mathbb{Z}_q | w(A) = h\}$ be equipped with the uniform probability func-

tion. Let $\mathcal{E}:\Omega\to\mathbb{R}$ be the random variable that associates to A the length of the longest sequence of '0'-valued bits in $\mathrm{seq}_N(A)$. The distribution of $\mathcal{E}$ is more difficult to compute than the one of E. To approximate the distribution $\mathcal{E}$, we use the following distribution. Let Ω' be the family of multisets

$$\Omega'=\left\{(a_1,\ldots,a_h)|a_1\geq a_i\geq 0 \text{ for } i>1,\sum_{i=1}^{h}a_i=N-h\right\},$$

equipped with the uniform probability function. This family represents all the possible sequences of zeros and ones of length N and weight h after the best shift. Let $\psi:\{A\in\mathbb{Z}_q|w(A)=h\}\to\Omega'$ be the function that assigns an element of weight h in $\mathbb{Z}_q$ to the corresponding multiset in Ω'. Let $\mathcal{A}:\Omega'\to\mathbb{R}$ be the random variable defined by $\mathcal{A}((a_1,\ldots,a_h))=a_1$. Due to symmetries, ψ is not balanced, so $\mathbb{P}(\mathcal{A}=k)$ is not necessarily equal to $\mathbb{P}(\mathcal{E}=k)$.

Proposition 5.16. *The cumulative distribution function of $\mathcal{A}$ is*

$$\mathbb{P}(\mathcal{A}\leq k)=\frac{\sum_{i=0}^{k}l_{i+1}(h-1,N-h-i)}{\sum_{i=0}^{N-h}l_{i+1}(h-1,N-h-i)}.$$

Proof. Let us consider $\mathcal{A}^{-1}(k)$ for some k. It is the subset of Ω' containing the multisets of the form $(k,a_2,\ldots,a_h)$ under the condition that $a_i<k+1$ for every i and that $\sum_{i=2}^{h}a_i=N-h-k$. The number of such multisets is $l_{k+1}(h-1,N-h-k)$. From this we can conclude the proof, since

$$|\mathcal{A}^{-1}(\{0,\ldots,k\})|=\sum_{i=0}^{k}|\mathcal{A}^{-1}(i)|.$$

■

Heuristic 5.17. For every k, $|\mathbb{P}(\mathcal{E}\geq k)-\mathbb{P}(\mathcal{A}\geq k)|<\varepsilon$ for some small positive ε.

These computations reveal a new family of weak keys: namely, (F,G) such that $\mathcal{E}(F)+\mathcal{E}(G)\geq N$. One can perform N^2 rotations and guess up to $N-\lceil N/h\rceil-h$ possible t_1 to find a unique solution to (5.4), where $\mathcal{U}=$

$\{2^h,\dots,2^{N-t_1}-2^{N-t_1-h}\}$ and where $\mathcal{V}=\{2^h,\dots,2^{t_1}-2^{t_1-h}\}$. Such solution is obtained by querying to an ILP-oracle one instance of dimension 3.

For $N=1279$ and $h=17$, and according to Heuristic 5.17 the expected $\mathcal{E}$ is ≈ 256. For these parameters and using the described heuristic, it follows that the proportion of keys (F,G) such that $\mathcal{E}(F)+\mathcal{E}(G)\geq N$ is close to 2^{-11}. This improves upon Beunardeau et al. work for which approximately 1 over 2^{34} keys is weak.

5.4 Verification of the heuristics

To conclude, we want to address Heuristic 5.7 and Heuristic 5.17 and present some experimental evidence of them. The code of all the experiments, together with a record of all the random choices done by the programs can be found at https://git.app.uib.no/Andrea.Tenti/verification-of-heuristic.

Verification of Heuristic 5.7 In order to verify this assumption, we selected Mersenne primes q. For each of them, we took $\mathcal{U}=\{0,\dots,l\}$ and $\mathcal{V}=\{s,\dots,s+\lfloor q/l\rfloor\}$ for some l. Then, for all the possible $q-1$ group automorphisms $\varphi:\mathbb{Z}_q\to\mathbb{Z}_q$, we computed the size of $S=\varphi(\mathcal{U})\cap\mathcal{V}$ and compared it with $\frac{|\mathcal{U}||\mathcal{V}|}{q}$. For each q and l the experiments were repeated for 100 different s picked at random in $\{0,\dots,q-1\}$.

In Table 5.3 we report the results of the experiments. The Variance column contains the variance observed in the 100 different instances of s. In most of the observed cases the size of S was constant for fixed q, $\mathcal{U}$, and $|\mathcal{V}|$. The Difference column contains the difference between $\frac{|\mathcal{U}||\mathcal{V}|}{q}$ and the average number of elements in S. Lastly, in the column labelled "good systems", we report the average (over the 100 observations) probability that for a specific instance of φ, $|S|\leq 1$. The choices of q are: $q=8191=2^{13}-1$, $q=131071=2^{17}-1$, and $q=524287=2^{19}-1$, all of whom are Mersenne primes.

Table 5.3: Verification of Heuristic 5.7

q	$\lvert\mathcal{U}\rvert$	$\lvert\mathcal{V}\rvert$	Variance	Difference	good systems
8191	91	90	0	0.0109	0.7711
	102	80	0	0.0096	0.7774
	117	70	0.0097	−0.0014	0.7728
	136	60	0	0.0072	0.7770
131071	362	362	0	0.0028	0.7738
	374	350	0	0.0027	0.7736
	397	330	0	0.0025	0.7736
	409	320	0	0.0024	0.7733
524287	724	724	0	0.0014	0.7729
	748	700	0	0.0014	0.7730
	771	680	0	0.0015	0.7723
	819	640	0	0.0016	0.7730

Verification of Heuristic 5.17 For the verification of Heuristic 5.17, we chose Mersenne primes $2^N - 1$ and weights h. For each of them we computed the cumulative distribution function of the random variable $\mathcal{A}$. Then we sampled 10000 $F \in \{0, 2^N - 1\}$ such that $w(F) = h$ and computed the empirical distribution function of $\hat{\mathcal{E}}_{10^5}$ associated to the sample. In Table 5.4 we report the maximum and minimum distance between $\mathbb{P}(\mathcal{A} \leq k)$ and $\mathbb{P}(\hat{\mathcal{E}}_{10^5} \leq k)$ for $k = \lceil N/h \rceil, \ldots, N - h$. We chose the Mersenne primes $q = 2^{107} - 1$, $q = 2^{127} - 1$, and $q = 2^{521} - 1$, each with different values of h. Let $\mathrm{Diff} : \{\lceil N/h \rceil, \ldots, N - h\} \to \mathbb{R}$ be the function defined by $\mathrm{Diff}(k) = \mathbb{P}(\mathcal{A} \leq k) - \mathbb{P}(\hat{\mathcal{E}}_{10^5} \leq k)$.

Table 5.4: Verification of Heuristic 5.17

N	h	max(Diff)	min(Diff)
107	5	0.0133	−0.0058
	7	0.0153	−0.0031
	10	0.0329	−0.0005
	12	0.0237	−0.0031
127	5	0.0134	−0.0009
	7	0.0065	−0.0024
	10	0.0188	−0.0010
	12	0.0227	−0.0011
521	5	0.0064	−0.0039
	7	0.0076	−0.0013
	10	0.0103	−0.0076
	12	0.0120	−0.0017

Bibliography

[AB09] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009. 2

[ACFP14] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. Algebraic algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018, 2014. https://eprint.iacr.org/2014/1018. 1

[AJPS17] Divesh Aggarwal, Antoine Joux, Anupam Prakash, and Miklos Santha. A new public-key cryptosystem via Mersenne numbers. Cryptology ePrint Archive, Report 2017/481 , version:20170530.072202, 2017. 1, 5, 5.1, 5.1, 5.1.1, 5.1.1

[AJPS18] Divesh Aggarwal, Antoine Joux, Anupam Prakash, and Miklos Santha. A new public-key cryptosystem via Mersenne numbers. In *CRYPTO 2018. LCNS 10993*, pages 459–482. Springer International Publishing, 2018. 1, 5, 5.1, 5.1.1, 5.2.1, 5.3

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., 1969. 1, 2, 2.4, 2.1

[And02] Ian Anderson. *Combinatorics of finite sets*. Courier Corporation, 2002. 2

[App69] Leif Appelgren. A column generation algorithm for a ship scheduling problem. *Transportation Science*, 3:53–68, 02 1969. 5.1.3

[BCGN17] Marc Beunardeau, Aisling Connolly, Rémi Géraud, and David Naccache. On the hardness of the Mersenne low hamming ratio

assumption. Cryptology ePrint Archive, Report 2017/522, 2017. 1, 1.1, 5, 5.1, 5.1.1, 5.2.1, 5.3

[BCJ07] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF(2) via SAT-solvers. Cryptology ePrint Archive, Report 2007/024, 2007. https://eprint.iacr.org/2007/024. 1

[BFS03] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. Complexity of Gröbner basis computation of semi-regular overdetermined sequences over F_2 with solutions in F_2. In *INRIA Research Report 5049*, pages 71–74, 2003. 1, 1.1, 3, 3.3, 3.3, 3.39, 3.40

[BSVP17] Ward Beullens, Alan Szepieniec, Frederik Vercauteren, and Bart Preneel. Luov: Signature scheme proposal for nist pqc project. 2017. 1

[BT19] Alessandro Budroni and Andrea Tenti. The Mersenne low hamming combination search problem can be reduced to an ILP problem. In *AFRICACRYPT 2019. LCNS 11627*, pages 41–55. Springer, Heidelberg, 2019. 1.1, 5

[Buc65] Bruno Buchberger. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, (an algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal). *PhD thesis, University of Innsbruck*, 1965. 1, 1

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases, a Computational Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer-Verlag, 1993. 3, 3.16, 3.2

[CB02] George Casella and Roger L. Berger. *Statistical inference*, volume 2. Duxbury, 2002. 2, 2.36

[CFMR+17] Antoine Casanova, Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. Gemss: A Great Multivariate Short Signature, 2017. 1, 1, 3.3.2

[CG17] Alessio Caminata and Elisa Gorla. Solving multivariate polynomial systems and an invariant from commutative algebra. *CoRR*, abs/1706.06319, 2017. 1, 3.2, 3.27, 3.3, 3.3.2

[CHR+18] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. MQDSS specifications, 2018. 1

[CKPS00] Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *EUROCRYPT 2000. LNCS 1807*, pages 392–407. Springer, Heidelberg, 2000. 1

[CL69] George F. Clements and Bernt Lindström. A generalization of a combinatorial theorem of Macaulay. *Journal of Combinatorial Theory*, 7(3):230–238, 1969. 2.42

[CLO13] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, Heidelberg, 4 edition, 2013. 2.8, 3, 3.9, 3.12, 3.14

[CO18] IBM CPLEX Optimizer. IBM ILOG CPLEX Optimization Studio, 2018. 5.1.3

[Coo71] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158. ACM, 1971. 2.52

[CP02] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *ASIACRYPT 2002. LNCS 2501*, pages 267–287. Springer, Heidelberg, 2002. 1

[dBDJdW18] Koen de Boer, Léo Ducas, Stacey Jeffery, and Ronald de Wolf. Attacks on the AJPS Mersenne-based cryptosystem. In *PQCrypto. LCNS 10786*, pages 101–120. Springer International Publishing, 2018. 1, 5.1, 5.1.1, 5.1.1, 5.1.2, 5.3

[DG10] Vivien Dubois and Nicolas Gama. The degree of regularity of HFE systems. In *ASIACRYPT 2010. LCNS 6477*, pages 557–576. Springer, Heidelberg, 2010. 3.3.2

[DS05] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *ACNS 2005. LCNS 3531*, pages 164–175. Springer, Heidelberg, 2005. 1

[DS13] Jintai Ding and Dieter Schmidt. Solving degree and degree of regularity for polynomial systems over a finite fields. In *Number Theory and Cryptography. LCNS 8260*, pages 34–49. Springer, Heidelberg, 2013. 3.3.2, 3.3.2

[DY13] Jintai Ding and Bo-Yin Yang. Degree of regularity for HFEv and HFE-. In *PQCrypto 2013. LCNS 7932*, pages 52–66. Springer, Heidelberg, 2013. 3.3.2

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999. 1, 3.3.2

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *ISSAC 2002*, pages 75–83. ACM Press, 2002. 1

[Fis81] Marshall L. Fisher. The lagrangian relaxation method for solving integer programming problems. *Management science*, 27(1):1–18, 1981. 5.1.3

[FJ03] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner

bases. In *CRYPTO 2003. LCNS 2729*, pages 44–60. Springer, Heidelberg, 2003. 1

[FY79] Aviezri S. Fraenkel and Yaacov Yesha. Complexity of problems in games, graphs and algebraic equations. *Discrete Applied Mathematics*, 1(1-2):15–30, 1979. 1, 2.52

[GO18] LLC Gurobi Optimization. Gurobi optimizer reference manual, 2018. 5.1.3

[Har77] Robin Hartshorne. *Algebraic Geometry; Graduate Texts in Mathematics*. Springer, Heidelberg, 1977. 2

[HKYY18] Ming-Deh A. Huang, Michiel Kosters, Yun Yang, and Sze L. Yeo. On the last fall degree of zero-dimensional weil descent systems. *Journal of Symbolic Computation*, 87:207–226, 2018. 3.3.2

[HMS17] Timothy J. Hodges, Sergio D. Molina, and Jacob Schlather. On the existence of homogeneous semi-regular sequences in -F2[x1,...,xn]/(x12,...,xn2). *Journal of Algebra*, 476:519 – 547, 2017. 1, 3.3, 3.3.2

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory (ANTS III)*, 12 1998. 1, 5

[HPS14] Timothy J. Hodges, Christophe Petit, and Jacob Schlather. First fal degree and Weil descent. *Finite Fields and Their Applications*, 30:155 – 177, 2014. 3.3.2

[Huy86] Dung T. Huynh. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Information and Control*, 68(1-3):196–206, 1986. 1, 3.25

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT 99. LCNS 1666*, pages 206–222. Springer, Heidelberg, 1999. 1

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer, Heidelberg, 2000. 1, 1.1, 3.55, 3.73

[Laz83] Daniel Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *EUROCAL 1983. LNCS 162*, pages 146–156. Springer, Heidelberg, 1983. 1, 3.26

[Len83] Hendrik W. Lenstra. Integer programming with a fixed number of variables. *Mathematics of operations research*, 8(4):538–548, 1983. 5.1.3

[Lev73] Leonid A. Levin. Universal sequential search problems. *Problems of Information Transmission (translated from Problemy peredachi informatsii)*, 9(3):115–116, 1973. 2.52

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, and Lászloó Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, Dec 1982. 5.1.1

[Mac16] Francis S. Macaulay. *The algebraic theory of modular systems*. Cambridge University Press, 1916. 3.3

[Mac27] Francis S. Macaulay. Some properties of enumeration in the theory of modular systems. *Proceedings of the London Mathematical Society*, 2(1):531–555, 1927. 2.3

[MJSS16] David R. Morrison, Sheldon H. Jacobson, Jason J. Sauppe, and Edward C. Sewell. Branch-and-bound algorithms. *Discret. Optim.*, 19(C):79–102, February 2016. 5.1.3

[MMWW02] Hugues Marchand, Alexander Martin, Robert Weismantel, and Laurence Wolsey. Cutting planes in integer and mixed integer programming. *Discrete Appl. Math.*, 123(1-3):397–446, November 2002. 5.1.3

[Pap81] Christos H. Papadimitriou. On the complexity of integer programming. *J. ACM*, 28(4):765–768, October 1981. 5.1.3

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *EUROCRYPT 96. LCNS 1070*, pages 33–48. Springer, Heidelberg, 1996. 1

[PJ68] Ganapati P. Patil and Sharadchandra W. Joshi. *Dictionary and bibliography of discrete distributions*. Oliver & Boyd, 1968. 2.37

[PQ12] Christophe Petit and Jean-Jacques Quisquater. On polynomial systems arising from a Weil descent. In *Advances in Cryptology – ASIACRYPT 2012. LCNS 7658*, pages 451–456. Springer, Heidelberg, 2012. 3.3.2

[Rom05] Steven Roman. *Advanced linear algebra*, volume 3. Springer, Heidelberg, 2005. 2, 2.21

[RS06] Håvard Raddum and Igor Semaev. New technique for solving sparse equation systems. Cryptology ePrint Archive, Report 2006/475, 2006. https://eprint.iacr.org/2006/475. 1

[Sch86] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Inc., New York, NY, USA, 1986. 5.1.3

[Sem15] Igor Semaev. New algorithm for the discrete logarithm problem on elliptic curves. *CoRR*, abs/1504.01175, 2015. 1

[Sem16] Igor Semaev. "Personal communication", 2016. 1.1, 1.2, 4

[ST19a] Igor Semaev and Andrea Tenti. Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases. Cryptology ePrint Archive, Report 2019/903, 2019. https://eprint.iacr.org/2019/903. 1.1, 1.1, 1.2, 2.3, 3.4, 3.65, 4, 4, 4.4

[ST19b] Igor Semaev and Andrea Tenti. Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases. In *WCC 2019*, 2019. 1.1

[Sta78] Richard Stanley. Hilbert functions of graded algebras. *Advances in Mathematics*, 28:57–83, 1978. 3.31

[Tra96] Carlo Traverso. Hilbert functions and the Buchberger algorithm. *Journal of Symbolic Computation*, 22(4):355 – 376, 1996. 1

[Wan81] Paul S. Wang. A p-adic algorithm for univariate partial fractions. In *Proceedings of the Fourth ACM Symposium on Symbolic and Algebraic Computation*, SYMSAC '81, pages 212–217, New York, NY, USA, 1981. ACM. 5.3

[Wol98] L.A. Wolsey. *Integer Programming*. Wiley Series in Discrete Mathematics and Optimization. Wiley, 1998. 5.1.3

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS

uib.no

ISBN: 9788230845073 (print)
9788230852439 (PDF)