https://doi.org/10.35662/unine-thesis-3145

Université de Neuchâtel

Faculté des Sciences
Institut de mathématiques
Rue Emile-Argand 11, 2000 Neuchâtel

Commutative algebra techniques in post-quantum cryptography

Thèse

présentée à la Faculté des Sciences
pour l'obtention du grade de docteur ès Sciences en mathématiques

par

Giulia Gaggero

Acceptée sur proposition du jury:

Prof. Elisa Gorla, Université de Neuchâtel, directeur de thèse
Prof. Alessio Caminata, Università di Genova, Expert externe
Prof. Jung Kyu Canci, Université de Neuchâtel & HSLU , membre interne
Dr. Carlo Matteotti, DDPS - Swiss Armed Forces, Cyber Command, expert externe
Dr. Lisa Seccia, Université de Neuchâtel, membre interne

Soutenue le 24 octobre 2024

unine
Université de Neuchâtel
Faculté des sciences

Rue Emile-Argand 11
CH-2000 Neuchâtel
doctorat.sciences@unine.ch

IMPRIMATUR POUR THESE DE DOCTORAT

La Faculté des sciences de l'Université de Neuchâtel autorise l'impression de la présente thèse soutenue par

Madame Giulia GAGGERO

Titre :

"Commutative algebra techniques in post-quantum cryptography"

sur le rapport des membres du jury composé comme suit :

- **Prof. Elisa Gorla,** directrice de thèse, Université de Neuchâtel, Suisse
- **Prof. Alessio Caminata,** Università di Genova, Italie
- **Prof. Jung Kyu Canci,** Université de Neuchâtel et HSLU, Suisse
- **Dr Lisa Seccia,** Université de Neuchâtel, Suisse
- **Dr Carlo Matteotti,** DDPS, Suisse

Neuchâtel, le 26 novembre 2024

Le Doyen, Prof. P. Brunner

Acknowledgements

My deepest and most heartfelt acknowledgment goes to my advisor, Elisa Gorla. She believed in me from the very beginning and was always there to provide guidance, both in mathematics and in life. She encouraged me to step outside my comfort zone, supporting me through moments of insecurity and fostering my curiosity.

All the people I met here in Neuchâtel made these four years truly unforgettable. A mosaic of personalities and cultures that I am now honored to call 'friends'. Paraphrasing Orwell, everyone is special, but some are more special than others.

Flavio, my beloved office mate, I think we spent more time talking about lol, cycling, chess, and my questionable decisions in my sentimental life than about math. This is clear evidence that being confined to the same room for four years led to a true and deep friendship. Your empathy has been an anchor for my anxiety. Thank you for all the bites you so generously let me steal from your plate.

Cristina, without you by my side, I am not sure I could have survived the first six months in Neuch (or the following 42, to be honest). You have this incredible talent for making everything sweeter—not just with cakes. The image of you that will stay with me forever is you describing tiny kitchen utensils and miming them with delicate gestures (not to mention your enthusiastic sponsorship of la Fête des Vendanges). Thank you for being my Neuchâtel spicy cake.

Johannes is the person who always says "yes" to my "Swim in the lake?"—no matter the weather or the temperature. Since I met you, I cannot hear the phrase "Let me tell you something" without bursting into laughter. You will forever be the one with crushes on bullfighters and Italian players. Thank you for the hugs when I truly needed them (though, unfortunately, I can't thank you for the cinnamon rolls).

I met Loris at the gym. He probably thinks his piercings make him look intimidating—spoiler: they don't. In fact, after just a couple of weeks, I convinced him to come climbing with me. Since then, he has become my coffee buddy, the person with the weirdest eating schedule, and the friend I can unload all my problems onto, always getting back a smile that makes me feel truly understood (a reminder that you do have a degree in psychology). The special thank to you is for letting me squeeze your biceps without accusing me of harassment.

Lisa, you arrived like a breath of fresh air for my mental health. There are no words to fully express what you mean to me. You are pura vida: what comes naturally to you often takes effort for me. Once, you told me not to take you as a model—and I do not. But, just to be clear, I truly admire you. Your personality is a perfect puzzle of everything I love in people. You have this incredible ability to involve everyone around you in your love for life, while also being the kind of friend who tells you when you are wrong and helps you improve yourself. On top of that, you are a brilliant and passionate mathematician—I love your work. This makes you shine even more. Thank you for making me enjoy beer again. I love them, and I owe you one!

A special mention goes to Oliver and our French-Quebec community—Marc, Lucas, and Jade—who always took care of my English and French, respectively.

Now it is time for my family to step in. Valeria and I chose each other from the very first moment of the first class in elementary school. Twelve years later, we're still here, celebrating together every success we have achieved in life and calling each other sister—because no other

word could describe us better. Thank you for always being by my side. Forever mine, forever yours, forever ours.

Brigitta has taught me the meaning of resilience. Even though I've grown to dislike that word since Covid, it's the only one that truly describes her. B, you are our Jesus—literally. Thank you for reminding me that life always offers new opportunities, and it's up to us to make them count.

Mamma e papà. Siete stati, siete e sarete la mia colonna portante. Il faro cui puntare sempre. Mi mancate tutti i giorni, ogni istante. So quanto siete fieri di me ma anche che tutto sommato mettere al mondo una figlia con sogni più vicini a casa non vi sarebbe dispiaciuto. Sono orgogliosa di voi, di noi, della nostra famiglia. Sono orgogliosa di dire che vi amo da morire e tutte le volte che esco a Genova est mi vengono i lacrimoni perché so che in 5 minuti sarò fra le vostre braccia. Abbiamo uno strano modo noi Gaggero di dimostrarci che ci vogliamo bene: ci riuniamo in grandi tavolate e finiamo sempre con il discutere e urlare, con la garanzia però che tutto si placherà con il caffè e il gelato. Siamo persone semplici nella mia famiglia (e ovviamente in questa categoria includo la zia Fiò, la zia Nenè e lo zio Tino): ci basta stare insieme. Grazie a tutti voi per avermi sempre sostenuto ma soprattutto per avermi insegnato che il più grande valore è la comunità.

Abstract

Post-quantum cryptography aims to find quantum-resistant public-key cryptographic schemes, that is, schemes which remain secure against both quantum and standard computers. In fact in 1994, Shor published an algorithm [85] breaking the nowadays used public-key cryptoschemes in polynomial time on a quantum computer. The security of public-key algorithms is based on computationally hard mathematical problems. Among the post-quantum proposals there is the Multivariate Problem: Solving a multivariate polynomial system over a finite field. The general and the most computationally efficient method for solving such systems is computing a Groöbner basis of the ideal they generate. In 2021, Beullens [22] used a strategy involving the MinRank Problem for breaching the most promising multivariate scheme at the time. All the details regarding public-key schemes and in particular the multivariate one can be found within the Introduction.

The thesis is divided into three blocks. The goal of Chapter 1 is twofold. It is a collection of algebraic concepts and classical facts that are used through these pages, in particular, Section 1.1 serves this scope. In addition, the problem of solving polynomial systems via Grb̈ner basis is fully explained in Section 1.2. In Chapter 2 and Chapter 3, I present the two main works of my PhD, during which I mainly focused on the analysis of multivariate cryptoschemes twofolds. Firstly, together with my advisor Elisa Gorla, we propose a new definition of 'random system' using the concept of generality mutued from algebraic geometry. The details of this work are given in Chapter2. On the other hand, with the help of Daniel Cabarcas (Universidad Nacional de Colombia), we investigated the SupportMinors Modeling, which is a method for modeling the MinRank Problem used by Beullens in his attack. The specifics of this work can be found in Chapter 3.

Keywords: Post-quantum cryptography, Post-quantum signatures, Multivariate Cryptography, MinRank Problem, Random system, Gröbner basis, Macaulay Algorithm.

Résumé

La cryptographie post-quantique vise à découvrir des schémas cryptographiques à clé publique résistants aux ordinateurs quantiques, c'est-à-dire des schémas qui restent sécurisés contre les ordinateurs quantiques et classiques. En effet, en 1994, Shor a publié un algorithme [85] capable de casser les cryptosystèmes à clé publique utilisés de nos jours en temps polynomial sur un ordinateur quantique. La sécurité des algorithmes à clé publique repose sur des problèmes mathématiques computationnellement difficiles. Parmi les propositions post-quantiques, on trouve le Problème Multivarié : résoudre un système polynomiale multivarié sur un corps fini. La méthode générale et la plus efficace sur le plan computationnel pour résoudre de tels systèmes est de calculer une base de Gröbner de l'idéal qu'ils génèrent. En 2021, Beullens [22] a utilisé une stratégie impliquant le Problème de MinRank pour briser le schéma multivarié le plus prometteur à l'époque. Tous les détails concernant les schémas à clé publique, et en particulier le schéma multivarié, peuvent être trouvés dans l'Introduction.

La thèse est divisée en trois parties. L'objectif du Chapitre 1 est double. Il s'agit d'une collection de concepts algébriques et de résultats classiques utilisés tout au long de ces pages, en particulier la Section 1.1, qui sert cet objectif. De plus, le problème de la résolution des systèmes polynomiaux via les bases de Gröbner est entièrement expliqué dans la Section 1.2. Dans le Chapitre 2 et le Chapitre 3, je présente les deux principaux travaux de mon doctorat, durant lequel je me suis principalement concentré sur l'analyse des cryptosystèmes multivariés sous deux angles. Premièrement, avec ma directrice de thèse Elisa Gorla, nous proposons une nouvelle définition de « système aléatoire » en utilisant le concept de généralité emprunté à la géométrie algébrique. Les détails de ce travail sont fournis dans le Chapitre 2. D'autre part, avec l'aide de Daniel Cabarcas (Universidad Nacional de Colombia), nous avons étudié la modélisation SupportMinors, qui est une méthode utilisée pour modéliser le Problème de MinRank utilisé par Beullens dans son attaque. Les spécificités de ce travail se trouvent dans le Chapitre 3.

Mots-clés: Cryptographie post-quantique, Signatures post-quantiques, Cryptographie multivariée, Problème du MinRank, Système aléatoire, Base de Gröbner, Algorithme de Macaulay.

Contents

Introduction

In the basic situation which cryptography arise from there are two people, name them Alice and Bob, that want to safely exchange secret information on a public channel. Imagine Bob wishes to send a secret message to Alice. The idea is to encrypt the original message with respect to an encryption key, i.e. transforming the original 'plaintext' into an alternative scrambled form called 'ciphertext' using the rule encoded in the key. In addition, the encryption process should be done in a way in which only Alice (and possibly Bob) is able to recover the original message from the scrambled one. To be more concrete a cryptographic scheme is given by two functions based on the encryption key:

$$\mathcal{P} : \{\text{plaintext}\} \to \{\text{ciphertext}\} \quad \mathcal{D} : \{\text{ciphertext}\} \to \{\text{plaintext}\},$$

called respectively encryption and decryption function, such that $\mathcal{D}(\mathcal{P}(m)) = m$, for all plaintext m.

If both the encryption and the decryption functions are secret and known by both Alice and Bob, i.e. the receiver and the sender, then the scheme is a 'symmetric-key' scheme and $\mathcal{D} = \mathcal{P}^{-1}$.

Example 1. *An easy example of a symmetric-key cryptosystem is the Shift Chiper scheme, which is based on modular aritmetic. Let* $\{plaintext\} = \{ciphertext\} = \mathbb{Z}_{26}$ *and choose a key* k, $0 \leq k \leq 25$. *Then, for* $x, y \in \mathbb{Z}_{26}$, *the encryption and decryption functions related to* k *are:*

$$\mathcal{P}_k(x) = x + k \mod 26 \quad \textit{and} \quad \mathcal{D}_k(y) = y - k \mod 26.$$

In a symmetric-key cryptosystem the parties have to agree on a prior shared secret key before starting any conversation on the channel, which is the main issue of this type of cryptography. In 1976, Diffie and Helman had the idea to use two different, but related, keys for the encryption and the decryption processes [62]. This couple of keys are associated to the receiver of messages. The 'public key' is published on the channel and allows a sender to encrypt plaintext. The 'private key' is kept secret by the receiver and it is used to decrypt ciphertext. In 'public-key' cryptography the encryption function $\mathcal{P}$ is a one-way trapdoor function based on a computationally hard mathematical problem, that is a function which is easy to compute but practically impossible to invert without knowing extra information, and the related private key is precisely this extra information. Notice that such math problems are computationally hard to solve but theoretically solvable. A 'well-designed' system is a system 'computationally' secure: while it is theoretically possible to break such systems inverting $\mathcal{P}$, it is impossible doing so in practice. RSA is a largely used public-key scheme whose one-way function is described in the next example.

Example 2. *Let be* p, q *two large primes and define* $n = pq$. *Then choose* b *a positive integer such that* $\gcd(b, \phi(n)) = 1$, *where* $\phi(n)$ *is the Euler's totient function of* n, *i.e.,* $\phi(n) = (p-1)(q-1)$. *A function that is believed to be one-way is* $f : \mathbb{Z}_n \to \mathbb{Z}_n$,

$$f(x) = x^b \mod n.$$

The inverse f^{-1} of this function has a similar form:

$$f^{-1}(x) = x^a \mod n,$$

where a is an integer such that

$$ab \equiv 1 \mod \phi(n).$$

The trapdoor is an efficient method for computing the correct exponent a. In particular it is the knowledge of the factorization of $n = pq$. With this extra information, one easily calculates the Euler's totient function of n, that is

$$\phi(n) = \phi(pq) = (p-1)(q-1)$$

and then computes the value of a using the Euclidean Algorithm.

The encryption and decryption functions of RSA are respectively f and f^{-1} of Example 2. Thus, the RSA public key is (n, b) and the private key is (p, q), or equivalently (a). The problem on which it is based is the hardness of factoring: given some prime numbers it is easy to multiply them with each other, but given a large number it is computationally hard to find a prime factorization. In fact, an obvious attack on a RSA primitive is to attempt to factor n. The following is a small example of the RSA cryptosystem.

Example 3. *Alice chooses $p = 97$ and $q = 103$, then $n = 9991$ and $\phi(n) = (p-1)(q-1) = 9792 = 2^6 * 3^2 * 17$. An integer b can be used as encryption exponent if and only if $\gcd(b, \phi(n)) = 1$, that is if and only if $2, 3$ and 17 do not divide b. Suppose Alice chooses $b = 3107$. Then the decryption exponent is*

$$a = b^{-1} \mod \phi(n) = 3659 \mod 9792.$$

Thereby Alice publishes on the channel her public key $(n = 9991, b = 3107)$ and Bob can use it for sending safely to her the plaintext $m = 6472$. He will compute the corresponding ciphertext

$$c = \mathcal{P}(m) = m^b \mod n = 6472^{3107} \mod 9991 \equiv 7768.$$

When Alice receives c, she uses her private key a to decrypt the ciphertext by computing

$$\mathcal{D}(c) = c^a \mod n = 7768^{3659} \mod 9991 \equiv 6472 = m.$$

In order to choose a b coprime with $\phi(n)$, Alice does not need to to factor $\phi(n)$. She will use an upgraded version of the Euclidean Algorithm such as Algorithm 6.3 in [86], and in the meanwhile she will also compute b^{-1}. The security of RSA cryptosystem relies on the belief that the encryption function $\mathcal{P}(p) = p^b$ is a one-way function. The trapdoor that allows Alice to invert it is the knowledge of the factorization of $n = pq$, so that she can easily calculate $\phi(n)$ and then compute a with an extended version of the Euclidean Algorithm. Since both a and b can be as big as $\phi(n) - 1$, it might appear infeasible to both encrypt and decrypt a message since they involves a modular exponentiation, that is the operation $x^c \mod n$. However, Alice and Bob can use the algorithm Square-And-Multiply [86, Algorithm 6.5] for computing the operation efficiently, i.e. in polynomial time.

Another problem on which public-key cryptography relies nowadays is the Discrete Logarithm Problem: given a multiplicative group $(G, \cdot)$, an element $\alpha \in G$ of order n, and an element

$\beta \in \langle\alpha\rangle$, find the unique integer a, $0 \leq a \leq n-1$, such that $\alpha^a = \beta$. The integer a is denoted by $\log_\alpha \beta$ and it is called the *discrete logarithm* of β *to the base* α. A well known scheme based on this problem is the ElGamal Cryptosystem. For this purpose, the group G is $\mathbb{Z}_p^*$, where p is a prime number and α is a primitive element. In this scheme the plaintexts are elements of $\mathbb{Z}_p^*$ and the ciphertexts of $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$. The public key is the triple (p, α, β) and the private key is the integer a. For a chosen random number k in $\mathbb{Z}_{p-1}$, the encryption and decryption functions are:

$$\mathcal{P}_k(x) = (\alpha^k, x\beta^k) \mod p \quad \text{and} \quad \mathcal{D}(y_1, y_2) = y_2(y_1^a)^{-1} \mod p,$$

where $x \in \mathbb{Z}_p^*$ and $y_1, y_2 \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$. The next example shows how a small ElGamal primitive works.

Example 4. *Let* $p = 3119$ *and* $\alpha = 2$*, which can be tested to be a primitive element modulo* p*. Let* $a = 749$*, so*

$$\beta = \alpha^a \mod p = 2^{749} \mod 3119 \equiv 1810.$$

In order to send to Alice the plaintext $m = 1542$*, Bob chooses at random* $k = 925$ *and keeps it secret. Then he send her the ciphertext*

$$(y_1, y_2) = \mathcal{P}_{925}(m) = (\alpha^{925}, 1542\,\beta^{925}) \mod 3119 \equiv (2406, 1972).$$

To recover the original plaintext from (y_1, y_2)*, she computes*

$$1972 * (2406^{749})^{-1} \mod 3119 \equiv 1542 = m.$$

From now on, the public key will be often confused with the encryption function and the private key with the decryption function. Thanks to the asymmetric structure of public-key cryptography, encryption-decryption processes are not the only possible. It is also feasible to generate digital signatures: digital stamps authenticating the identity of the signer and ensuring non-repudiation, meaning that the signer cannot claim that they did not sign the document. A valid signature issued by Alice for a document m is the preimage $\mathcal{P}_A^{-1}(m) = s$ of m via her public key $\mathcal{P}_A$, which she is able to compute using her related private key. Then the signed document is the pair (s, m). To verify the validity of s, one checks whether $\mathcal{P}_A(s) = m$. Notice that, given (s, m) a signed document and m' a document different from m, then s cannot be attached to m' as valid signature since $\mathcal{P}_A(s) = m \neq m'$.

Summing up, the currently used public-key cryptosystems, both encryption and signature schemes, rely on the hardness of Factoring and Discrete Logarithm Problems. It should be noticed that it is just a presumed hardness. In fact, the research of new computationally hard problems is an ongoing process. Moreover, in 1994, Peter Shor published an algorithm that solves both problems in polynomial time on a sufficiently powerful quantum computer. As a consequence, if such a quantum computer can be constructed, present-day public-key cryptography is broken. Even if quantum computation is far from reaching the level required by Shor's Algorithm, finding new problems for the so called 'post-quantum cryptography' is paramount. What we can do it is elaborating cryptosystems that remain secure over a standard computer and are not susceptible to the known quantum attacks. Post-quantum cryptography has focused on several approaches in recent years. The most promising include the following.

- Lattice-based cryptography can be based on two different problems. Given a lattice $\mathcal{L}$, the Shortest Vector Problem asks to find a vector $v \in \mathcal{L}$ such that its norm is minimal.

Instead, the Closest Vector problem asks to find the closest vector $v \in \mathcal{L}$ to a target vector not necessary in the lattice. NTRU [64] and CRYSTALS-Dilithium [46] are two examples of lattice-based schemes.

- Isogeny-based cryptography is based on a key-exchange construction called Supersingular Isogeny Diffie-Hellman (SIDH). It relies on the structure of large graphs whose arrows are special maps between elliptic curves, called precisely isogenies. The most studied isogeny-based system has been SIKE [37].

- Code-based cryptography's foundation is the Decoding Problem: given a linear code $C \subseteq \mathbb{F}_q^n$, a distance over $\mathbb{F}_q^n$, an integer r, and a vector $y \in \mathbb{F}_q^n$ whose distance from C is smaller than r, find a code word $c \in C$ and an error $e \in \mathbb{F}_q^n$ such that $y = c + e$ and its norm is smaller than r. The main representative system of this type of cryptography is Classic McEliece [71].

- MPC-in-the-Head Signatures, in which a proof of knowledge relying on a Multi Party Computation in the Head protocol is turned into a signature scheme via the Fiat-Shamir transform. Moreover, for the MPC-in-the-Head protocol has to be based on a hard problem: for example MIRA [4] is based on the MinRank Problem.

- Multivariate cryptography relies on the hardness of solving a multivariate polynomial system over a finite field. This task is known to be hard already for degree 2 systems, referred to as Multivariate Quadratic (MQ) Problem. Two of the first schemes based on this problem have been HFE [80] and UOV [65].

The NIST (National Institute of Standards and Technology) runs two competitions for setting the post-quantum security standards. The first started in 2016, they called for both encryption and digital signature systems. During the third round almost all the proposals for digital signature schemes got broken or the cryptanalysis was unreliable. Then, during summer 2023, NIST announced an additional competition for digital signature schemes. Proposals using all the above-mentioned post-quantum approaches have been submitted. However, multivariate cryptography is particularly suited for signature schemes: for the same security level, it provides smaller keys and signature than the other methods.

One of the main attacks that convinced the NIST to run a separate new competition for digital signature is the one made by Beullens against Rainbow [23], which is a multivariate scheme. More precisely it is a 'multi-layered' version of UOV. I will not introduce either UOV or Rainbow, as it is beyond the scope of this thesis. The attack mounted by Beullens is based on the MinRank Problem:

MinRank Problem. *Let $\mathbb{F}$ be a field and let m, n, r, k be positive integers. Given as input k matrices $M_1, \ldots, M_k \in \mathbb{F}^{m \times n}$, find $x_1, \ldots, x_k \in \mathbb{F}$ such that*

$$0 < \mathrm{rk}\left(\sum_{\ell=1}^{k} x_\ell M_\ell\right) \leq r.$$

Refer to Chapter 3 for further details on this problem.

During my PhD, I mainly focused on the analysis of multivariate cryptoschemes. First, together with my advisor, we propose a new definition of 'random system' using the concept of

genericity from algebraic geometry. The details of this work are given in Chapter 2. On the other hand, with the help of Daniel Cabarcas (Universidad Nacional de Colombia), we investigated the SupportMinors Modeling, which is a method for modeling the MinRank Problem used by Beullens in his attack. The specifics of this work can be found in Chapter 3.

In multivariate cryptography one always works with finite fields. Let R denote the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$, where $\mathbb{F}_q$ is the finite field of cardinality q. In order to build a typical multivariate one-way function, let $f_1, \ldots, f_m \in R$, and consider the evaluation map

$$\begin{array}{rccc} \mathcal{F}: & \mathbb{F}_q^n & \to & \mathbb{F}_q^m \\ & \alpha = (\alpha_1, \ldots, \alpha_n) & \mapsto & (f_1(\alpha_1, \ldots, \alpha_n), \ldots, f_m(\alpha_1, \ldots, \alpha_n)) \end{array}$$

To hide the structure of $\mathcal{F}$, we compose it with two random invertible linear maps $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $T : \mathbb{F}_q^m \to \mathbb{F}_q^m$. We obtain $\mathcal{P} = T \circ \mathcal{F} \circ S$, a set of m polynomials $p_1, \ldots, p_m$ in n variables over $\mathbb{F}_q$. The public key of the multivariate scheme related to $\mathcal{F}$ is $\mathcal{P} = (p_1, \ldots, p_m)$ and the private key is the triple $\{\mathcal{F}, S, T\}$. The trapdoor consists of constructing $\mathcal{F}$ such that $\mathcal{F}^{-1}$ is efficiently computable. Notice that $\mathcal{P}$ should be hard to invert without the knowledge of S, T, in particular it should be hard to recover the structure of $\mathcal{F}$ from $\mathcal{P}$. Given a document $\beta \in \mathbb{F}_q^n$, a valid signature related to the system $\mathcal{F}$ is a solution of the system

$$\{p_i(x_1, \ldots, x_n) = \beta_i : i = 1, \ldots, m\}.$$

The owner of the private key knows the maps S and T. For them generating a valid signature amounts to finding a solution of the polynomial system $\mathcal{F} = T^{-1} \circ \beta$, which should be computationally easy, and then computing its image via S^{-1}.

The first multivariate cryptosytem was proposed by Matsumoto and Imai [70], but it was broken by Patarin in 1995 [79]. The following year, Patarin proposed a new multivariate cryptoscheme: the Hidden Field Equation (HFE) scheme [80]. it was broken by Kipnis and Shamir [66] just two years later. Patarin subsequently proposed several variations aimed at enhancing the scheme's security, such as the vinegar method and the minus method.

The central map of a Hidden Field Equations scheme is a univariate polynomial F with coefficient in $\mathbb{F}_{q^n}$ and $\deg(F) \leq D \in \mathbb{N}$. Let $\alpha_{i,j}, \beta_i, \gamma \in \mathbb{F}_{q^n}$ for $0 \leq j < i < n$, and let

$$F(X) = \sum_{\substack{0 \leq j < i < n \\ q^i + q^j \leq D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leq i < n \\ q^i \leq D}} \beta_i X^{q^i} + \gamma.$$

The secret key of an HFE protocol consists of the polynomial F and two invertible affine maps $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Let $\{\mu_1, \ldots, \mu_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and define an isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ via $\phi(x_1, \ldots, x_n) = \sum x_i \mu_i$. We call $\phi^{-1}(F(\phi(x_1, \ldots, x_n))$ the *multivariate representation* of F. Because of the choice of the exponents of X and of the fact that the Frobenius morphism is linear over $\mathbb{F}_q$, the multivariate representation of F is a set of n quadratic polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$. In fact

$$F(\phi(x_1, \ldots, x_n)) = F\left(\sum_{k=1}^{n} \mu_k x_k\right) = \sum_{k=1}^{n} \mu_k f_k,$$

where $\mathcal{F} = \{f_1, \ldots, f_n\}$ is a set of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$.

The public key of an HFE scheme is given by a set $\mathcal{P} = (p_1, \ldots, p_m)$ of n quadratic poly-

nomials in n variables over $\mathbb{F}_q$. It is obtained from the secret key by taking the polynomials of

$$T \circ \mathcal{F} \circ S(x_1, \dots, x_n).$$

Here $\mathcal{F}$ is identified with a map $\mathbb{F}_q^n \to \mathbb{F}_q^n$. The map $T \circ \mathcal{F} \circ S : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is in turn identified with a list of n polynomials $p_1, \dots, p_n \in \mathbb{F}_q[x_1, \dots, x_n]$, which we denote again by $T \circ \mathcal{F} \circ S$. The next example is a small example of an HFE central map and the related quadratic systems.

Example 5. *Let $\mathbb{F}_8 = \mathbb{F}_2[z]/(z^3 + z + 1)$, then $\{1, z, z^2\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_8$. Setting $D = 6$, the following polynomial is a possible central map of an HFE scheme:*

$$F(X) = X^6 + zX^5 + z^2X^2 + X + z^2 + 1.$$

For finding the system $\mathcal{F}$, one has to compute

$$F(\phi(x_1, x_2, x_3)) = F(x_1 + zx_2 + z^2x_3)$$

and then extract the coefficients of $1, z, z^2$. In this example one finds:

$$\mathcal{F} = \{x_1x_2 + x_1x_3 + x_2x_3 + 1, x_1x_3 + x_2x_3 + x_1, x_1 + x_2 + 1\}.$$

Let $S, T : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ be two invertible maps represented by the matrices

$$S = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Then the public key of the scheme is the family

$$\mathcal{P} = \{x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2, x_1x_2 + x_1x_3 + x_2x_3 + 1, x_1x_3 + x_2x_3 + x_2 + x_3\}.$$

In order to sign the document $\beta = (\beta_1, \beta_2, \beta_3) \in \mathbb{F}_2^3$, one has to find its preimage via $\mathcal{P}$, i.e. compute a solution of the system

$$\begin{cases} x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 = \beta_1 \\ x_1x_2 + x_1x_3 + x_2x_3 + 1 = \beta_2 \\ x_1x_3 + x_2x_3 + x_2 + x_3 = \beta_3. \end{cases}$$

Notice that the owner of the private key knows the maps S and T. Generating a valid signature for them amounts to finding a solution of the polynomial system $\mathcal{F} = T^{-1} \circ \beta$, where in general β is in $\mathbb{F}_q^n$, and then computing its image via S^{-1}.

In the small example above, it is easy to find a solution of both $\mathcal{P} = \beta$ and $\mathcal{F} = T^{-1} \circ \beta$. But in general it is not possible to solve the systems directly. In fact, as we already said, solving a multivariate polynomial system over a finite field is a hard problem.

The designed signer, i.e. the one related to the public key $\mathcal{P}$, can take advantage of the main feature of a public-key scheme: the inverse of the private key is efficiently computable. In the multivariate case this means that there exists an efficient way of finding a solution of the private system $\mathcal{F}$. In an HFE protocol, the knowledge of $\mathcal{F}$ is equivalent to the one of the central polynomial F. Then solving the system $\mathcal{F} = T^{-1} \circ \beta$ is equivalent to finding a solution

of the univariate polynomial $F(X) = \sum (T^{-1} \circ \beta)_i \mu_i$, where $\{\mu_1, \ldots, \mu_n\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. The efficiency is given by the Berlekamp-Rabin Algorithm, which finds solutions of univariate polynomials over a finite field in polynomial time.

Example 6. *In our small example, the designed signer of the document $\beta = (0, 0, 1)$ in order to generate a valid signature has to find a solution of the polynomial $F(X) = 1\beta_1 + z\beta_2 + z^2\beta_3$, i.e.*

$$X^6 + zX^5 + z^2X^2 + X + z^2 + 1 = z^2,$$

that is $X = z$. Then the solution of the system $\mathcal{F} = T^{-1} \circ \beta$ is $(0, 1, 0)$ and the signature related to the signer for β is $s := S^{-1}(0, 1, 0) = (0, 1, 1)$.
To check whether s is a valid signature for β, one has simply to verify that $\mathcal{P}(s) = \beta$.

The public key of a multivariate protocol is a multivariate polynomial system over a finite field. In fact, measuring the security of this type of schemes amounts to estimating the complexity of solving such a system. For computing a solution of a multivariate polynomial system in $\mathbb{F}_q[x_1, \ldots, x_n]$ there are two methods that always apply. The first is an exhaustive search over $\mathbb{F}_q$. The time complexity of this algorithm is $O(q^n)$: In fact there are only q^n possible solutions over $\mathbb{F}_q$ and one can attempt to try them all. On the other hand, as it is explained in Subsection 1.2.1, this problem can be solved by computing a Gröbner basis of the system, whose complexity will be analyzed in Subsection 1.2.2. Notice that, in the case of systems arising from cryptography, this latter strategy seems more computationally effective.

The thesis is divided into three chapters. The goal of Chapter 1 is twofold. It is a collection of algebraic concepts and classical facts that are used through these pages, in particular, Section 1.1 serves this scope. In addition, the problem of solving polynomial systems via Gröbner basis is discussed in Section 1.2, based on the work of Caminata and Gorla [35]. In Chapter 2 and Chapter 3, I present the main results obtained during my PhD.

1 Preliminaries

From now on, let $\mathbb{F}$ be a field. When $\mathbb{F}$ is thought finite, the notation switches to $\mathbb{F}_q$, which typically denotes the finite field of cardinality q. When it is not specified, $\mathbb{F}$ is an arbitrary field. For a positive integer t, denote by $[t]$ the set $\{1, \dots, t\}$.

In the first section of this chapter, I have included definitions of all objects and invariants used throughout the thesis, along with the main facts about them that are referenced. Section 1.1 should be seen as a comprehensive guide for understanding the content of Chapters 2 and 3. Section 1.2, on the other hand, provides all the details on how to solve a multivariate polynomial system by calculating a Gröbner basis of the ideal it generates, highlighting both theoretical and practical aspects.

1.1 Algebraic Preliminaries

Let R denote $\mathbb{F}[x_1, \dots, x_n]$, that is the polynomial ring over $\mathbb{F}$ in n variables. Given $f \in R$, f is a *polynomial* and it is a finite sum of monomials. An element $a_\mu \mathbf{x}^\mu$, where $\mu \in \mathbb{N}^n$, $a_\mu \in \mathbb{F}$, and $\mathbf{x}^\mu = x_1^{\mu_1} \cdots x_n^{\mu_n}$, is a *monomial* of degree $|\mu| = \mu_1 + \ldots + \mu_n$. A monomial with $a_\mu = 1$ is called *term* and $\mathbb{T}$ is the set of terms of R. Thereby, $f \in R$ is the sum $\sum_{i \in \mathcal{I}} a_i m_i$, where $a_i \in \mathbb{F}$, $a_i \neq 0$, and $m_i \in \mathbb{T}$. The *support* of f is $\mathrm{supp}(f) = \{m_i : i \in \mathcal{I}\}$. The degree of f is the maximum of the degrees of the monomials appearing in f. If all these monomials have the same degree then f is *homogeneous*.

A *term order* on R is a total order τ on $\mathbb{T}$ with the following additional properties:

1. $m \leq_\tau n$ implies $p \cdot m \leq_\tau p \cdot n$ for all $p, m, n \in \mathbb{T}$;
2. $1 \leq_\tau m$ for all $m \in \mathbb{T}$.

Moreover, if it holds the property that $m <_\tau n$ whenever $\deg(m) < \deg(n)$, the term order τ is called *degree-compatible*.

Example 7 (Lexicographic order)**.** *Let $\mathbf{x}^\alpha$ and $\mathbf{x}^\beta$ be two terms in R. We say that $\mathbf{x}^\alpha >_{lex} \mathbf{x}^\beta$ if the lefmost non-zero entry in the vector $\alpha - \beta \in \mathbb{Z}^n$ is positive. This term order is called* lexicographic *and it is not degree-compatible.*

Example 8 (Degree reverse lexicographic order)**.** *Let $\mathbf{x}^\alpha$ and $\mathbf{x}^\beta$ be two terms in R. We say that $\mathbf{x}^\alpha >_{drl} \mathbf{x}^\beta$ if $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and the rightmost non-zero entry in $\alpha - \beta \in \mathbb{Z}^n$ is negative. This term order is called* degree reverse lexicographic *and it is degree-compatible.*

Definition 9. *Let $\mathcal{F} = \{f_1, \dots, f_r\} \subseteq R$ be a system of polynomials. The* ideal generated by $\mathcal{F}$ *is*

$$(\mathcal{F}) = (f_1, \dots, f_r) := \left\{ \sum_{i=1}^{r} p_i f_i : p_i \in R \right\}.$$

The system $\mathcal{F}$ is a *minimal system of generators* for the ideal $I = (\mathcal{F})$ if the ideal generated by any non-empty proper subset of $\mathcal{F}$ is strictly contained in I. If the polynomials $f_1, \dots, f_r$ are homogeneous, then the ideal I is *homogeneous*.

Example 10. *Let $R = \mathbb{F}[x, y, z]$, $\mathcal{F} = \{x^2, x, y^2 + z^2\}$ and $\mathcal{G} = \{x, y^2 + z^2\}$. Then $(\mathcal{F}) = (\mathcal{G})$, but $\mathcal{F}$ is not a minimal generating set for this ideal, whereas $\mathcal{G}$ is. In sfact $\mathcal{G} \subsetneq \mathcal{F}$, but they generate the same ideal. In addition, $(x) \subsetneq (\mathcal{G})$ and $(y^2 + z^2) \subsetneq (\mathcal{G})$. Notice moreover that $(\mathcal{G})$ is a homogeneous ideal since its generators are homogeneous.*

Let f be a polynomial, $f = \sum_i a_i m_i \in R$, where $a_i \in \mathbb{F} \setminus \{0\}$ and $m_i \in \mathbb{T}$. Fix a term order τ on R. The *leading term* of f with respect to τ, denoted $\mathrm{in}_\tau(f)$, is the largest term appearing in f, i.e. $\mathrm{in}_\tau(f) = \max_\tau\{m_i : m_i \in \mathrm{supp}(f)\}$. For example, the leading term of the polynomial $f = x^2 + xy^2$ with respect to the lexicographic order is x^2 and with respect to the degree reverse lexicographic's is xy^2. Given an ideal I of R, the *initial ideal* of I is

$$\mathrm{in}_\tau(I) = (\mathrm{in}_\tau(f) : f \in I \setminus \{0\}).$$

Definition 11. *Let $I \subseteq R$ be an ideal. A set of polynomials $\mathcal{G} \subseteq I$ is a* Gröbner basis *of I with respect to τ if $\mathrm{in}_\tau(I) = (\mathrm{in}_\tau(g) : g \in \mathcal{G})$. A Gröbner basis is* reduced *if $m \notin (\mathrm{in}_\tau(h) : h \in \mathcal{G} \setminus \{g\})$ for all $g \in \mathcal{G}$ and $m \in \mathrm{supp}(g)$.*

Thanks to its monomial nature, $\mathrm{in}_\tau(I)$ is a finitely generated ideal, then every ideal I has a finite Gröbner basis. In subsection 1.2.2, an algorithm to compute these objects will be illustrated. Notice moreover that the property of being a Gröbner basis in general depends on the term order. In all the introduced notation, when the term order is clear, the reference to it will be removed.

Example 12. *Let $R = \mathbb{F}[x, y, z]$ with $x > y > z$, $f_1 = x^2 - y^2$, and $f_2 = xz - y^2$. Consider first the lexicographic order. Then $\{f_1, f_2\}$ is not a Gröbner basis of $I = (f_1, f_2)$, since $g = zf_1 - xf_2 = xy^2 - y^2z \in I$ but $\mathrm{in}_{lex}(g) = xy^2 \notin (\mathrm{in}_{lex}(f_1), \mathrm{in}_{lex}(f_2)) = (x^2, xz)$. Now fix the degree reverse lexicographic order. Then $\mathrm{in}_{drl}(f_1) = x^2$ and $\mathrm{in}_{drl}(f_2) = y^2$ are coprime, and so it is easy to see that $\{f_1, f_2\}$ are a drl-Gröbner basis for I. But it is not reduced since $y^2 \in \mathrm{supp}(f_1) \cap \{\mathrm{in}_{drl}(f_1), \mathrm{in}_{drl}(f_2)\}$*

The polynomial ring R can be given a $\mathbb{Z}^r$*-grading*, which means that the degree of each variable is a vector in $\mathbb{Z}^r_{>0}$, i.e., $\deg_{\mathbb{Z}^r}(x_i) = \mathbf{r}_i \in \mathbb{Z}^r_{>0}$ for all $i \in [n]$. It is not necessary for all the vectors $\mathbf{r}_i$ to be distinct. The monomial $a_\mu \mathbf{x}^\mu$, $\mu \in \mathbb{N}^n$, has $\mathbb{Z}^r$-degree $\mu_1\mathbf{r}_1 + \ldots \mu_n\mathbf{r}_n \in \mathbb{Z}^r$. The *standard grading* over R is the $\mathbb{Z}$-grading in which $\deg_{\mathbb{Z}}(x_i) = 1$ for all $i \in [n]$.

Another important algebraic notion that will occur several times within these pages is the the one of module over the polynomial ring R.

Definition 13. *An R-*module *M consists of an abelian group $(M, +)$ together with an operation of scalar multiplication $\cdot : R \times M \to M$ such that for all $f, g \in R$ and $m_1, m_2 \in M$:*

- $f \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$;
- $(f + g) \cdot m_1 = f \cdot m_1 + g \cdot m_2$;
- $(fg) \cdot m_1 = f(g \cdot m_1)$;
- $1 \cdot m_1 = m_1$.

Let M, N be R-modules, $\phi : M \to N$ is an homomorpism of R-modules if it preserves the R-module structure, i.e., if it respects the group structure and it is linear in R.

Modules can be regarded as a generalization of vector spaces with scalars in a ring instead of a field. An R-module M is *finitely generated* if there exist $m_1, \dots, m_c \in M$ such that the smallest module containing $m_1, \dots, m_c$, i.e., the module $\langle m_1, \dots, m_c \rangle = \left\{ \sum_{i=1}^{c} r_i m_i : r_i \in R \right\}$, is equal to M. The module M is *free* if it is finitely generated and $m_1, \dots, m_c$ are linearly independent. In this case $\{m_1, \dots, m_c\}$ is a *basis* of M and its cardinality is the *rank* of the M, denoted $\operatorname{rank}(M)$.

Example 14.
- *Given an ideal $I \subseteq R$, I and R/I are R-modules.*
- *R is a free module over itself with basis $\{1\}$.*
- *$R^k = R \oplus \cdots \oplus R$ is a free R-module of rank k and basis $\{e_1, \dots, e_k\}$, where $(e_i)_j = \delta_{ij}$.*
- *Given a free R-module M with basis $\{m_1, \dots, m_c\}$, its* dual module *M^* is the set of R-module homomorphisms from M to R. It is an R-module itself with basis $\{m_1^*, \dots, m_c^*\}$, where $m_i^* : M \to R$, $m_i^*(m_j) = \delta_{ij}$.*

Let me just mention also the concept of *R-algebra*. An R-algebra A is a ring A which is also an R-module with the ring addition and the scalar multiplication satisfies $f \cdot (a_1 a_2) = (f \cdot a_1) a_2 = a_1 (f \cdot a_2)$ for all $f \in R$ and $a_1, a_2 \in A$. Let A, B be R-algebras, $\rho : A \to B$ is an homomorphism of R-algebras if it is an homomorpism of rings and R-modules.

Let d be a positive integer, then R_d denotes the d-th homogeneous component of R, that is the $\mathbb{F}$-vector space generated by the monomials in R of degree d. If an R-module M is such that $M = \bigoplus_{k \in \mathbb{Z}} M_k$ as an abelian group and $R_d M_k \subseteq M_{d+k}$ for all $d, k \in \mathbb{Z}$ then M is *graded*. If M is finitely generated, then each graded component M_k is an $\mathbb{F}$-vector space of finite dimension [47, Section 1.9]. Let $f : M \to N$ be a homomorphism of graded R-modules, f is *homogeneous* if $f(M_i) \subseteq N_i$ for all i. A homogeneous ideal $I \subseteq R$ is a graded R-module with $I_d = I \cap R_d$, which is the $\mathbb{F}$-vector space of homogeneous polynomials of degree d in I. The *dth shift of M*, noted $M(d)$, is the alteration of the graded R-module M by 'shifting' its grading d steps. Precisely, $M(d)$ is isomorphic to M as a module and its graded component are defined by

$$M(d)_k = M_{d+k}.$$

Given a graded module M, the function

$$\mathrm{HF}_M(-) : \mathbb{N} \to \mathbb{N}, \quad \mathrm{HF}_M(d) = \dim_{\mathbb{F}} (M)_d$$

is called *Hilbert function* of M. For large d, the Hilbert function of M is a polynomial in d called *Hilbert polynomial* and denoted $\mathrm{HP}_M(d)$. The generating series of HF_M is called *Hilbert series* of M:

$$\mathrm{HS}_M(z) = \sum_{d \in \mathbb{N}} \mathrm{HF}_M(d) z^d.$$

Further details can be found in [28, Chapter 4.4].

An important invariant associated to a graded module M is the *Castelnuovo-Mumford regularity of M*, denoted $\operatorname{reg}(M)$. An invariant associated to a module is a quantity that does not vary under coordinates changes of R. The definition of the Castelnuovo-Mumford regularity is technical and involves algebraic concepts as free resolutions and Betti numbers, the interested reader may refer to [47, Chapter 20] for full details. However in the case of a homogeneous

ideal $I = (f_1, \dots, f_r)$ such that $R_d = I_d$ for an integer $d \gg 0$, then the Castelnuovo-Mumford regularity can be computed as

$$\operatorname{reg}(I) = \min\{d \in \mathbb{Z}_{\geq 0} : R_d = I_d\}.$$

It is also denoted $\operatorname{reg}(f_1, \dots, f_r)$.

Definition 15. *The* index of regularity *of I is the smallest positive integer $i_{\text{reg}}(I)$ such that $\operatorname{HF}_{R/I}(d) = \operatorname{HP}_{R/I}(d)$ for all $d \geq i_{\text{reg}}(I)$.*

The Castelnuovo-Mumford regularity and the index of regularity of a homogeneous ideal I are related via the Grothendieck-Serre's Formula [28, Theorem 4.4.3]. In particular, it holds that

$$i_{\text{reg}}(I) < \operatorname{reg}(I).$$

Moreover, if $R_d = I_d$ for $d \gg 0$, then $i_{\text{reg}}(I) = \operatorname{reg}(I) - 1$ by [47, Corollary 4.15].

The last definition of this subsection is a classical concept on which the work presented in Chapter 2 is based.

Definition 16. *A sequence $\{f_1, \dots, f_r\} \subseteq R$ is* regular *if:*

- *for all $i = 1, \dots, r$ given $g \in R/(f_1, \dots, f_{i-1})$, if $f_i g \in (f_1, \dots, f_{i-1})$ then $g \in (f_1, \dots, f_{i-1})$;*
- $R/(f_1, \dots, f_r) \neq 0$.

Let $I \subseteq R$ an ideal, a sequence $\{f_1, \dots, f_r\} \subseteq R$ is regular modulo I *if:*

- *for all $i = 1, \dots, r$ given $g \in R/I + (f_1, \dots, f_{i-1})$, if $f_i g \in I + (f_1, \dots, f_{i-1})$ then $g \in I + (f_1, \dots, f_{i-1})$;*
- $R/I + (f_1, \dots, f_r) \neq 0$.

One can think about regular sequences as sequences that are as independent as possible. Thanks to this maximal independence, an important remark is that if an ideal I of R contains a regular sequence of length n, then $I_d = R_d$ for some integer d.

Example 17.
- *The sequence $\{x_1^{u_1}, \dots, x_n^{u_n}\} \subseteq R$, with $u_i \in \mathbb{Z}_{\geq 0}$ is a regular sequence.*
- *$x^3, xyz \in \mathbb{F}[x, y, z]$ is not regular since $x^2 \cdot xyz \in (x^3)$ but $x^2 \notin (x^3)$.*

The Hilbert series of R modulo the ideal generated by a regular sequence $f_1, \dots, f_r$, $\deg(f_i) = d_i$ and $r \leq n$, is well known and it is

$$\operatorname{HS}_{R/(f_1,\dots,f_r)}(z) = \frac{(1 - z^{d_1}) \cdots (1 - z^{d_r})}{(1 - z)^n}.$$

In particular, one gets also information on the invariants just introduced:

$$\operatorname{reg}(f_1, \dots, f_r) = i_{\text{reg}}(f_1, \dots, f_r) + 1 = \sum_{i=1}^{r} (d_i - 1) + 1.$$

The *depth* of R/I, denoted $\operatorname{depth}(R/I)$, is the maximal length of a regular sequence modulo the ideal I. Notice again that the formal definition involves some technical algebraic tools which are beyond the scope of this dissertation. The interested reader may refer to [28, Section 1.2].

1.1.1 Buchsbaum-Rim complex

A piece of work presented in Chapter 3 is based on a modification of the so-called Buchsbaum-Rim complex. For a full introduction to it, the interest reader may refer to [47, Section A2.6]. However, within this subsection I introduce some basic notions for ensuring that the reader knows all the tools involved, starting from the concepts of complex and free resolution of a module. I then move to some multilinear algebra and I eventually give the Buchsbaum-Rim complex.

Recall that, given two R-modules M and N, a homomorphism of R-modules $\phi : M \to N$ is a map preserving the module structure. If M and N are also graded, then ϕ is homogeneous if $\phi(M_i) \subseteq N_i$.

Definition 18. *A* complex $C_\bullet$ *of R-modules consists of:*

- *a family* $\{C_k\}_{k\in\mathbb{Z}}$ *of R-modules;*
- *a family* $\{\delta_k : C_k \to C_{k-1}\}_{k\in\mathbb{Z}}$ *of homomorphisms such that*

$$\delta_{k-1} \circ \delta_k : C_k \to C_{k-2}$$

is the zero map for all $k \in \mathbb{Z}$.

The complex $C_\bullet$ is exact *whenever* $\ker(\delta_k) = \mathrm{Im}(\delta_{k+1})$ *for all* $k \in \mathbb{Z}$.

If the families defining a complex $C_\bullet$ have finite cardinality, then the complex is *finite* and it is usually noted

$$0 \to C_c \xrightarrow{\delta_c} \cdots \xrightarrow{\delta_3} C_2 \xrightarrow{\delta_2} C_1 \xrightarrow{\delta_1} C_0 \to 0.$$

If the modules $C_1, \ldots, C_c$ are graded and the map δ_k is homogeneous for all $k \in \{1, \ldots, c\}$, then one may consider the 'd-homogeneous' complex $C_{\bullet,d}$, $d \in \mathbb{Z}$, which is the complex

$$0 \to (C_c)_d \xrightarrow{\delta_c} \cdots \xrightarrow{\delta_3} (C_2)_d \xrightarrow{\delta_2} (C_1)_d \xrightarrow{\delta_1} (C_0)_d \to 0,$$

where $(C_1)_d, \ldots, (C_c)_d$ are the d-graded components of $C_1, \ldots, C_c$. Moreover, notice that if $C_\bullet$ is exact then also the complex $C_{\bullet,d}$ is exact. Finally, if $C_\bullet$ is exact and $C_1, \ldots, C_c$ are finitely generated, thanks to a classical result, see e.g. [9, Proposition 2.11], it holds that

$$\sum_{k=0}^{c} (-1)^k \dim_{\mathbb{F}}((C_k)_d) = 0 \quad \text{for all } d \in \mathbb{Z}. \tag{1.1.1}$$

Thus, combining all these equations, it is easy to see that

$$\sum_{k=0}^{c} (-1)^k \mathrm{HS}_{C_k}(z) = 0. \tag{1.1.2}$$

Definition 19. *A* finite free resolution *of an R-module M is a finite complex $F_\bullet$ such that:*

- F_k *is a free R-module for all* $k = 0, \ldots, c$;
- *there exists an* augmentation map $\varepsilon : F_0 \to M$ *such that* $F_\bullet \xrightarrow{\varepsilon} M \to 0$ *is an exact complex.*

The *length* of a finite free resolution is the greatest index k such that $F_k \neq 0$. The *projective dimension* of M, denoted projdim(M), is the minimal length among all its finite free resolutions.

Example 20. *Set $M = R/(f)$, where $f \in R$ a homogeneous polynomial of degree d, $f \neq 0$. A free resolution of M is*

$$0 \to R \xrightarrow{\delta_1} R \xrightarrow{\varepsilon} R/(f) \to 0,$$

such that $\varepsilon(1) = \overline{1}$ and $\delta_1(1) = f$.

Remark 21. *Every free R-module M has a free resolution. In order to produce it, let $\{m_1, \ldots, m_s\}$ a basis of M over R and $F_0 = R^s$ with the standard basis $\{e_1, \ldots, e_s\}$. Then define the map ε as*

$$\begin{array}{rcl} \varepsilon : R^s & \to & M \\ e_i & \mapsto & m_i. \end{array}$$

Trivially,

$$0 \to \ker(\varepsilon) \to F_0 \to M \to 0$$

is an exact sequence. For computing an entire free resolution of M, one proceeds with $\ker(\varepsilon)$ *as described for M. Moreover, define the* syzygy module *of M as*

$$\mathrm{Syz}(M) := \ker(\varepsilon).$$

For more information on the syzygy module and related concepts, the interested reader may refer to [67, Chapter 2.3].

Definition 22. *A* graded free resolution *of a graded R-module M is a free resolution of M in which all the maps are homogeneous.*

Example 23. *Consider again the resolution of Example 20. Unless $d = 0$, the map δ_1 is not homogeneous, since $\delta_1(R_i) \subseteq R_{i+d}$. In order to recover a graded resolution from the one given in the previous example, one should twist the modules involved. With this notion, a graded free resolution of M is:*

$$0 \to R(-d) \xrightarrow{\delta_1} R \xrightarrow{\varepsilon} R/(f) \to 0,$$

such that $\varepsilon(1) = \overline{1}$ and $\delta_1(1) = f$. In this way, $\delta_1(R(-d)_i) = \delta_1(R_{i-d}) \subseteq R_i$.

As in the non graded case, every graded free module has a free graded resolution. The process for producing it is the same described in Remark 21, but one should consider shifted modules for obtaining homogeneous maps and choose homogeneous generators for all modules involved. For example, with the same notation of Remark 21, let $\deg(m_i) = d_i$, then $F_0 = \bigoplus_{i=1}^{m} R(-d_i)$.

The main tool of multilinear algebra is the tensor product of two modules.

Definition 24. *Let M and N be R-modules. The* tensor product *of M and N over R, denoted $M \otimes_R N$, is the R-module generated by symbols $m \otimes n$ for $m \in M$ and $n \in N$, with relations*

$$\begin{gathered} rm \otimes n = m \otimes rn \\ (m + m') \otimes n = m \otimes n + m' \otimes n \\ m \otimes (n + n') = m \otimes n + m \otimes n'. \end{gathered}$$

If M and N are free modules with basis $\{m_1, \dots, m_c\}$ and $\{n_1, \dots, n_k\}$, then $M \otimes_R N$ is free with basis $\{m_i \otimes n_j : i = 1, \dots, c \text{ and } j = 1, \dots, k\}$, for a proof see e.g. [25, Corollary II.3.7.2]. In particular, $R^c \otimes_R R^k \cong R^{ck}$. More in general the module $R^{c_1} \otimes_R R^{c_2} \otimes_R \dots \otimes_R R^{c_k}$ is free of rank $c_1 \cdots c_k$ and basis $\{e_{1,j_1} \otimes \dots e_{k,j_k} : 1 \le j_i \le c_i\}$, where $\{e_{i,j} : j = 1, \dots c_i\}$ is the basis of R^{c_i}. When the ring which we tensor over is clear, the subscript is omitted from the notation.

Definition 25. *Let M be an R-module. We can define several R-modules:*

- $M^{\otimes c} = M \otimes \cdots \otimes M$ *is the* c-th power *of M;*
- $T(M) := \oplus_{c=0}^{+\infty} M^{\otimes c}$ *is the* graded module *of M. It is possible to define a product over $T(M)$ in order to make it a ring;*
- *let $J = (m_1 \otimes m_2 - m_2 \otimes m_1 : m_1, m_2 \in M) \subseteq T(M)$ an ideal, then $S_c(M) := M^{\otimes c}/(J \cap M^{\otimes c})$ is the* c-th symmetric power *of M;*
- *let $I = (m \otimes m : m \in M) \subseteq T(M)$ an ideal, then $\bigwedge^c M := M^{\otimes c}/(I \cap M^{\otimes c})$ is the* c-th external power *of M. An element $\overline{m_1 \otimes \cdots \otimes m_c}$ in $\bigwedge^c M$ is denoted $m_1 \wedge \dots \wedge m_c$*

Example 26. *Let $M = R^c$ with basis $\{e_1, \dots, e_c\}$.*

- *A basis for $M^{\otimes k}$ is $\{e_{i_1} \otimes \cdots \otimes e_{i_k} : 1 \le i_j \le c \text{ for all } j = 1, \dots, k\}$. Then $T(M)$ is isomorphic to the non-commutative polynomial ring over R having $e_1, \dots, e_c$ as variables, denoted $R\langle e_1, \dots, e_c\rangle$.*
- *The ideal J contains the commutativity relations among the 'variables' $e_1, \dots, e_c$, then $T(M)/J$ is isomorphic to the polynomial ring $R[e_1, \dots, e_c]$. The d-th symmetric power $S_d(R^c)$ corresponds to select $R[e_1, \dots, e_c]_d$. Then also this R-module is free and a basis is given by the monomials in the 'variables' $e_1, \dots, e_c$ of degree d.*
- *In the module $T(M)/I$ all the non-squarefree monomials in $R\langle e_1, \dots, e_c\rangle$ are zero. For this reason, the d-external power $\bigwedge^d R^c$ is a free R-module with basis $\{e_{i_1} \wedge \dots \wedge e_{i_d} : 1 \le i_1 < \dots < i_k \le c\}$. In particular, $\bigwedge^c R^c = \langle e_1 \wedge \dots \wedge e_c\rangle \cong R$. Notice moreover that $J \subseteq I$, then the $\wedge$ product is commutative.*

Given a function $f : R^m \to R^n$ of free R-modules with $m \ge n$ and $\{e_1, \dots, e_m\}$ a basis of R^m over R, one can consider the n-external power of f, whose definition over a basis of $\bigwedge^n R^m$ is the following:

$$\begin{array}{rccc} \bigwedge^n f : & \bigwedge^n R^m & \to & \bigwedge^n R^n \\ & e_{i_1} \wedge \dots \wedge e_{i_n} & \mapsto & f(e_{i_1}) \wedge \dots \wedge f(e_{i_n}), \end{array}$$

for all $1 \le i_1 < \dots < i_n \le m$. Let M the $n \times m$ matrix representing f and call $I_n(f)$ the ideal of R generated by the $n \times n$ minors of M. Then $\bigwedge^n f(\bigwedge^n R^m) \cong I_n(f)$. Let us see an example to clarify the last isomorphism.

Example 27. *Set $m = 4$, $n = 2$, and $R = \mathbb{F}[x, y, z]$. Let $\{e_1, e_2, e_3, e_4\}$, $\{f_1, f_2, f_3\}$ be the bases of R^4 and R^3 respectively, and define the map $f : R^4 \to R^3$ such that*

$$f(e_1) = xf_1,\ f(e_2) = yf_2,\ f(e_3) = zf_3,\ f(e_4) = yzf_1 + xf_2 + y^2 f_3.$$

Thus the matrix M representing f is

$$\begin{pmatrix} x & 0 & 0 & yz \\ 0 & y & 0 & x \\ 0 & 0 & z & y^2 \end{pmatrix}$$

A basis of $\bigwedge^3 R^4$ is $\{e_1 \wedge e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_4, e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4\}$ and the map $\bigwedge^3 f : \bigwedge^3 R^4 \to \bigwedge^3 R^3 \cong R$ is defined over it as follow:

$$\begin{aligned}
&\bigwedge^3 f(e_1 \wedge e_2 \wedge e_3) = xf_1 \wedge yf_2 \wedge zf_3 = xyz(f_1 \wedge f_2 \wedge f_3),\\
&\bigwedge^3 f(e_1 \wedge e_2 \wedge e_4) = xf_1 \wedge yf_2 \wedge (yzf_1 + xf_2 + y^2 f_3) = xy^3(f_1 \wedge f_2 \wedge f_3),\\
&\bigwedge^3 f(e_1 \wedge e_3 \wedge e_4) = xf_1 \wedge zf_3 \wedge (yzf_1 + xf_2 + y^2 f_3) = x^2 z(f_1 \wedge f_2 \wedge f_3),\\
&\bigwedge^3 f(e_2 \wedge e_3 \wedge e_4) = yf_2 \wedge zf_3 \wedge (yzf_1 + xf_2 + y^2 f_3) = y^2 z^2(f_1 \wedge f_2 \wedge f_3).
\end{aligned}$$

The equalities follow from the R-linearity of an R-module and the relations contained in the ideal I. Notice now that the monomials collected at common factor in the image of $e_{i_1} \wedge e_{i_2} \wedge e_{i_3}$, with $i_1, i_2, i_3 \in \{1, 2, 3, 4\}$, are the 3-minors of the matrix M involving the columns i_1, i_2, i_3 and all the rows.

We are now ready for describing the Buchsbaum-Rim complex.

Lemma 28. *Let $f : F \to G$ be a map of free R-modules with* $\operatorname{rank}(F) = m \geq \operatorname{rank}(G) = n$. *Then the Buchsbaum-Rim Complex is*

$$0 \to \bigwedge^m F \otimes S_{m-n-1}(G^*) \xrightarrow{d_{m-n+1}} \cdots \xrightarrow{d_3} \bigwedge^{n+1} F \otimes S_0(G^*) \xrightarrow{\varepsilon} F \xrightarrow{f} G,$$

where ε is a suitable composite:

$$\bigwedge^{n+1} F \otimes S_0(G^*) \xrightarrow{\sim} \bigwedge^{n+1} F \otimes \bigwedge^n (G^*) \xrightarrow{1 \otimes \bigwedge^n f^*} \bigwedge^{n+1} F \otimes \bigwedge^n F^* \to F.$$

For an example of the use of this lemma refer to Subsection 3.2.1 of Chapter 3. Since the explicit description of the maps in the previous lemma will not be used, I decided to skip the details. Denote by $I_t(f)$ the ideal generated by the t-minors of the matrix representing f. The main result about the above complex is that it is a free resolution of $G/f(F)$ if and only if the the ideal $I_t(f)$ contains a regular sequence of length $m - n + 1$ and, in this case, it holds that $G/f(F) \cong I_n(f)$ [47, Theorem A2.10].

1.1.2 Zero loci

The *algebraic closure* $\overline{\mathbb{F}}$ of $\mathbb{F}$ is an algebraic extension of $\mathbb{F}$ that is algebraically closed, i.e., every non-constant polynomial in $\overline{\mathbb{F}}[X]$ has a root in $\overline{\mathbb{F}}$. Since it is unique up to isomorphism, one can think of $\overline{\mathbb{F}}$ as the largest algebraic extension of $\mathbb{F}$.

Definition 29. *The* affine zero locus *of an ideal $I = (f_1, \ldots, f_r) \subseteq R$ over the algebraic closure*

$\overline{\mathbb{F}}$ *of* $\mathbb{F}$ *is*

$$\mathcal{Z}(I) = \{P \in \overline{\mathbb{F}}^n : f(P) = 0 \text{ for all } f \in I\} = \{P \in \overline{\mathbb{F}}^n : f_1(P) = \ldots = f_r(P) = 0\}.$$

It is also denoted $\mathcal{Z}(f_1, \ldots, f_r)$.

Now, we focus on the projective case. The *projective space* of dimension ℓ over the field $\mathbb{F}$, denoted $\mathbb{P}^\ell(\mathbb{F})$ or simply $\mathbb{P}^\ell$ when the field $\mathbb{F}$ is clear, is the space of lines through the origin in $\mathbb{F}^{\ell+1}$. More precisely,

$$\mathbb{P}^\ell(\mathbb{F}) = \frac{\mathbb{F}^{\ell+1} \setminus \{0\}}{\sim},$$

where $\sim$ is the equivalence relation defined as follows: for two vectors $v, w \in \mathbb{F}^{\ell+1} \setminus \{0\}$, we say that $v \sim w$ if and only if $v = \lambda w$ for some $\lambda \in \mathbb{F} \setminus \{0\}$.

Definition 30. *The* projective zero locus *of a homogeneous ideal* $I = (f_1, \ldots, f_r) \subseteq R$ *over the algebraic closure* $\overline{\mathbb{F}}$ *of* $\mathbb{F}$ *is*

$$\begin{aligned}\mathcal{Z}_+(I) &= \{P \in \mathbb{P}^n(\overline{\mathbb{F}}) : f(P) = 0 \text{ for all } f \in I\} \\ &= \{P \in \mathbb{P}^n(\overline{\mathbb{F}}) : f_1(P) = \ldots = f_r(P) = 0\}.\end{aligned}$$

It is also denoted $\mathcal{Z}_+(f_1, \ldots, f_r)$.

The set $\{\mathbb{P}^n(\overline{\mathbb{F}}) \setminus \mathcal{Z}_+(f_1, \ldots, f_r) \mid f_1, \ldots, f_r \in R\}$ defines a topology on $\mathbb{P}^n(\overline{\mathbb{F}})$ called *(projective) Zariski topology*.

Both the definition of zero loci and Zariski topology make sense also over the field $\mathbb{F}$ itself. However, working on an algebraically closed, or at least infinite, field ensures that every non-empty open set in the Zariski topology is dense, i.e., its closure is equal to the entire space. A non-empty open subset of $\mathbb{P}^n(\overline{\mathbb{F}})$ is often called a *generic set* and a property which holds on a non-empty open set is *generic*. Intuitively, a generic set is almost the whole space and a generic property holds almost everywhere in $\mathbb{P}^n(\overline{\mathbb{F}})$.

The problem of extending this definition to a finite field is that a nonempty Zariski-open set is no longer dense, so the algebraic-geometric intuition of genericity is lost.

A homogeneous degree d polynomial $g \in R$ can be viewed as a point in the projective space $\mathbb{P}^{\binom{n+d-1}{d}}$: the correspondence sends g to the ordered list of coefficients of the monomials of degree d in the expression of g. Thereby, a polynomial family $\{g_1, \ldots, g_s\} \subseteq R$, $\deg(g_i) = d_i$, corresponds to a point into the product of projective spaces $\mathbb{P}^s_{d_1,\ldots,d_s} = \mathbb{P}^{\binom{n+d_1-1}{d_1}} \times \ldots \times \mathbb{P}^{\binom{n+d_s-1}{d_s}}$. It is well-known that the set of regular sequences of length $s \leq n$ of degree $d_1, \ldots, d_s$ is a dense open Zariski set in $\mathbb{P}^s_{d_1,\ldots,d_s}$. Thus, being a regular sequence is a generic property.

1.2 System solving via Gröbner basis

1.2.1 Lexicographic Gröbner basis

In this section we follow [35, Section 2]. Let $\mathcal{F}$ be a polynomial system in R. It is well-known that a method for solving $\mathcal{F}$ is finding a Gröbner basis of the ideal $(\mathcal{F})$ generated by the system itself. The main link between the two problems is given by the Shape Lemma.

Theorem 31 (Shape Lemma – [67], Theorem 3.7.25)**.** *Let $\mathbb{F}$ be a field and let $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ be such that the corresponding ideal $I = (f_1, \ldots, f_r)$ is radical, in normal x_n-position, and $|\mathcal{Z}(I)| = d < \infty$. The reduced lexicographic Gröbner basis of I is of the form*

$$\{g_n(x_n), x_{n-1} - g_{n-1}(x_n), \ldots, x_1 - g_(x_n)\},$$

where $g_1, \ldots, g_n$ are univariate polynomials in x_n and $\deg(g_1), \ldots, \deg(g_{n-1}) < \deg(g_n) = d$.

When the hypotheses of the Shape Lemma are met, solving a system of equations has the same complexity as computing the reduced lexicographic Gröbner basis of the ideal generated by the system [35, Theorem 3].

The Shape Lemma assumes that the ideal I is in *normal x_n-position*, that is if any two distinct zeros $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathcal{Z}(I)$ satisfy $a_n \neq b_n$. Any ideal I with a finite affine zero locus can be brought into normal x_n-position through a suitable linear change of coordinates [67, Proposition 3.7.22]. This may require passing to a field extension, as the next example shows.

Example 32. *Let $I = (x^2 + x, xy, y^2 + y) \subseteq \mathbb{F}_2[x, y]$. Then $\mathcal{Z}(I) = \{(0, 0), (0, 1), (1, 0)\}$. A linear change of coordinates over $\mathbb{F}_2$ sends y to either $x, y, x+1, y+1, x+y$ or $x+y+1$. All these linear forms take the same value on at least two of the elements of $\mathcal{Z}(I)$. Then I cannot be brought in normal y-position by a linear change of coordinates over $\mathbb{F}_2$.*

Another hypothesis of the Shape Lemma is that $|\mathcal{Z}(I)| < \infty$. If $\mathbb{F}$ is a finite field of cardinality q, adding the field equations $\{x_i^q - x_i : i = 1, \ldots, n\}$ to I generates a new ideal J such that $\mathcal{Z}(J) = \mathcal{Z}(I) \cap \mathbb{F}^n$, in particular $|\mathcal{Z}(J)| \leq q^n < \infty$. As it will be discussed in Chapter 2, this is not always advantageous or computationally feasible, even in the case of systems coming from cryptography.

Finally, the Shape Lemma assumes that the ideal I is radical. For an ideal I being *radical* means that $f^e \in I$ for some $e > 0$ implies $f \in I$. This assumption is not always verified for ideals generated by systems arising in cryptography. Again in the case of finite fields, a solution may be adding the field equations to I. This approach ensures that the resulting ideal is radical. However, there is a more general version of the Shape Lemma for overcoming this problem. Making use of the Elimination Theorem [44, Chapter 3.1, Theorem 2], one can prove the next result.

Theorem 33. *[35, Theorem 5] Let I be a proper ideal of $R = \mathbb{F}[x_1, \ldots, x_n]$ with finite affine zero locus. The reduced lexicographic Gröbner basis of I has the form*

$$\begin{aligned}
&p_{n,1}(x_n),\\
&p_{n-1,1}(x_{n-1}, x_n), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, x_n),\\
&p_{n-2,1}(x_{n-2}, x_{n-1}, x_n), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, x_{n-1}, x_n),\\
&\vdots\\
&p_{1,1}(x_1, \ldots, x_n), \ldots, p_{1,t_1}(x_1, \ldots, x_n),
\end{aligned}$$

where $p_{i,t_j} \in \mathbb{F}[x_1, \ldots, x_n]$ for every $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, t_i\}$, and $t_1, \ldots, t_{n-1} \geq 1$. Moreover,

for any $1 \leq \ell \leq n$, *let* $a = (a_{\ell+1}, \ldots, a_n) \in \mathbb{F}^{n-\ell}$ *be a solution of the equations*

$$\begin{aligned}
&p_{n,1}(x_n),\\
&p_{n-1,1}(x_{n-1}, x_n), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, x_n),\\
&p_{n-2,1}(x_{n-2}, x_{n-1}, x_n), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, x_{n-1}, x_n),\\
&\vdots\\
&p_{\ell+1,1}(x_{\ell+1}, \ldots, x_n), \ldots, p_{\ell+1,t_{\ell+1}}(x_{\ell+1}, \ldots, x_n),
\end{aligned}$$

and let

$$p_\ell(x_\ell) = \gcd\{p_{\ell,1}(x_\ell, a_{\ell+1}, \ldots, a_n), \ldots, p_{\ell,t_\ell}(x_\ell, a_{\ell+1}, \ldots, a_n)\}.$$

Then $p_\ell(x_\ell) \notin \mathbb{F}$.

Thanks to Theorem 33, only assuming that the system has finitely many solutions over the algebraic closure, an algorithm computing the affine zero locus of an ideal I from its reduced lexicographic Gröbner basis can be built.

Corollary 34. *[35, Corollary 1] Let* $I \subseteq R = \mathbb{F}[x_1, \ldots, x_n]$ *be an ideal with finite affine zero locus* $\mathcal{Z}(I)$. *Then* $\mathcal{Z}(I)$ *can be computed as follows:*

1. *Compute the reduced lexicographic Gröbner basis* $\mathcal{G}$ *of* I *to obtain the monic polynomial* $p_n \in \mathbb{F}[x_n]$ *such that* $(p_n) = I \cap \mathbb{F}[x_n]$.
2. *If* $p_n = 1$, *then* $\mathcal{Z}(I) = \emptyset$. *Else, factor* p_n.
3. *For every root* α *of* p_n *compute*

$$p_{n-1}(x_{n-1}) = \gcd\{p_{n-1,1}(x_{n-1}, \alpha), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, \alpha)\}.$$

4. *Factor* p_{n-1}.
5. *For every root* β *of* p_{n-1} *compute*

$$p_{n-2}(x_{n-2}) = \gcd\{p_{n-2,1}(x_{n-2}, \beta, \alpha), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, \beta, \alpha)\}.$$

6. *Proceed similarly, until all the elements of* $\mathcal{Z}(I)$ *are found.*

1.2.2 Gröbner basis method and solving degree

The relation between solving a system and computing a lexicographic Gröbner basis of the ideal that it generates has been discussed in Subsection 1.2.1. Within this section the problem of estimating the complexity of computing a Gröbner basis of an ideal is addressed. In order to estimate this complexity, one should refer to the algorithms used to perform the computation since it depends on the algorithm employed. The first algorithm for computing Gröbner bases appeared in the doctoral thesis of Buchberger [30]. Modern algorithms for computing Gröbner bases are based on linear algebra and are more efficient than Buchberger's. Examples of linear-algebra-based algorithms are F_4 [49], F_5 [50], the *XL Algorithm* [42], *MutantXL* [31], and their variants. In all of these systems, one computes the reduced row echelon form of the Macaulay matrix associated to the polynomial equations in a given degree, for one or more degrees.

We now describe the main object of linear-algebra-based algorithms [17, Section 1.2]. Fix a term order over R. Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a system of homogeneous polynomials. The columns of the *homogeneous Macaulay matrix* M_d of $\mathcal{F}$ are labelled by the monomials of R_d and arranged in decreasing order. The rows of M_d are labelled by polynomials of the form $m_{i,j}f_j$, where $m_{i,j} \in R$ is a monomial such that $\deg(m_{i,j}f_j) = d$. The entry (i, j) of M_d is the coefficient of the monomial of column j within the polynomial corresponding to the i-th row.

Let now $f_1, \ldots, f_m$ be arbitrary (not necessarily homogeneous) polynomials. The columns of the *Macaulay matrix* $M_{\leq d}$ of $\mathcal{F}$ are labelled by the monomials of R of degree $\leq d$, arranged in decreasing order. The rows of $M_{\leq d}$ correspond to polynomials of the form $m_{i,j}f_j$, where $m_{i,j} \in R$ is a monomial such that $\deg(m_{i,j}f_j) \leq d$. The entries of $M_{\leq d}$ are defined as in the homogeneous case. The rationale behind the use of homogeneous Macaulay matrices for homogeneous systems is that, for a homogeneous system, the Macaulay matrix $M_{\leq d}$ is a block matrix with blocks $M_d, \ldots, M_0$.

One computes the reduced row echelon form of the Macaulay matrix, or of its homogeneous version, in one or more degrees. For large enough degree, this produces a reduced Gröbner basis with respect to the chosen order. Some algorithms, as e.g. *MutantXL*, use a variation called *mutant strategy* in the non-homogeneous case: If the reduction of the Macaulay matrix $M_{\leq d}$ produces new polynomials $g_1, \ldots, g_\ell$ of degree strictly smaller than d, one appends to the reduction of $M_{\leq d}$ the polynomials $m_{i,j}g_j$, where $m_{i,j} \in R$ is a monomial such that $\deg(m_{i,j}g_j) \leq d$, then computes the reduced row echelon form again. Throughout Chapter 2, we refer to the algorithms that employ the mutant strategy as *mutant algorithms* and to the others as *standard algorithms*.

Notice that, for solving a polynomial system one is interested in computing a lexicographic Gröbner basis of the ideal that it generates. However, the lexicographic order is generally computationally slower than other term orders. Conversely, computing a Gröbner basis with respect to the degree reverse lexicographic order is typically faster than with respect to any other term order. Therefore, it is often more efficient to compute a degree reverse lexicographic Gröbner basis and then convert it to a lexicographic's using the FGLM Algorithm [53] or a similar method, rather than computing the lexicographic Gröbner basis directly.

The computational complexity of computing the reduced row echelon form of the Macaulay matrices $M_{\leq d}$ and M_d depends on their size, and hence on the degree d. This motivates the next definition.

Definition 35. *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ and let τ be a term order on R. The* solving degree *of $\mathcal{F}$ with respect to τ is the least degree d such that Gaussian elimination on the Macaulay matrix $M_{\leq d}$ produces a τ-Gröbner basis of $\mathcal{F}$. We denote by* $\operatorname{solv.deg}^s_\tau(\mathcal{F})$ *the solving degree of $\mathcal{F}$ with respect to a standard algorithm and by* $\operatorname{solv.deg}^m_\tau(\mathcal{F})$ *the solving degree of $\mathcal{F}$ with respect to a mutant algorithm. When τ is the degree reverse lexicographic order, the subscript τ is omitted.*

In general, the solving degree is not invariant under coordinate change. Moreover, it may depend on the algorithm used to perform the Gröbner basis computation. In particular, for mutant algorithms it may be smaller than for standard ones. Finally, the solving degree depends on the choice of a term order on R.

Remark 36. *Given a polynomial system $\mathcal{F} \subseteq R$, the complexity of linear-algebra-based algorithms for computing a degree reverse lexicographic Gröbner basis of the ideal $(\mathcal{F})$ is dominated by the cost of Gaussian elimination in degree* $\operatorname{solv.deg}^s(\mathcal{F})$ *or* $\operatorname{solv.deg}^m(\mathcal{F})$ *respectively if one uses a standard or mutant algorithm. Therefore, an upper bound on the solving degree*

with respect to the degree reverse lexicographic order yields an upper bound on the complexity of computing a lexicographic Gröbner basis, since the complexity of the FGLM Algorithm is negligible with respect to the one of the Gaussian elimination. Hence, assuming that $\mathcal{F}$ has at least one solution over the algebraic closure $\overline{\mathbb{F}}$, an upper bound on the solving degree with respect to the degree reverse lexicographic order results in an upper bound on the complexity of solving the polynomial system thanks to Corollary 34.

As explained in the previous remark, the complexity of solving an arbitrary polynomial system $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R = \mathbb{F}[x_1, \dots, x_n]$ via Gröbner basis method is given by the complexity of the Gaussian elimination over the Macaulay matrix $\mathcal{M}_{\leq \text{solv.deg}(\mathcal{F})}$. Then it is

$$O(m^2(n + \text{solv. deg}(\mathcal{F}))^{3\cdot \text{solv.deg}(\mathcal{F})}),$$

where the specification of standard or mutant algorithm is omitted.

For $f \in R$ a polynomial, we denote by f^{top} the homogeneous part of f of largest degree. E.g., if $f = x^3 + 2xy^2 - y + 1 \in \mathbb{F}[x, y]$, then $f^{\text{top}} = x^3 + 2xy^2$. For a polynomial system $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq R$, we denote by $\mathcal{F}^{\text{top}} \subseteq R$ the homogeneous system $\{f_1^{\text{top}}, \dots, f_m^{\text{top}}\}$. Up to doing Gaussian elimination in a matrix whose rows correspond to $f_1, \dots, f_m$, we may suppose that $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ are linearly independent.

The *degree of regularity* was introduced in [16, Definition 4] and [12, Definition 3.2.2 and Definition 3.5.1].

Definition 37. *Let $\mathcal{F} \subseteq R$ be a polynomial system. The* degree of regularity *of $\mathcal{F}$ is*

$$d_{\text{reg}}(\mathcal{F}) = i_{\text{reg}}(\mathcal{F}^{\text{top}}) + 1 = \begin{cases} \min\{d \geq 0 \mid (\mathcal{F}^{\text{top}})_d = R_d\} & \text{if } \left(\mathcal{F}^{\text{top}}\right)_d = R_d \text{ for } d \gg 0 \\ +\infty & \text{otherwise.} \end{cases}$$

In the cryptographic literature, the degree of regularity is often used as a proxy for the solving degree. This is the case, e.g., in the specification documents of GeMSS [38]. However, this does not always produce reliable estimates. In fact, there are examples in which the gap between the degree of regularity and the solving degree is large, see e.g. [24, Examples 3.2 and 3.3]. A recent result by Semaev and Tenti [84, 88] however shows that, under suitable assumptions, the solving degree of a system with respect to a standard algorithm is at most twice the degree of regularity. Thanks to this result, an upper bound for the degree of regularity yields a proven upper bound for the solving degree.

Theorem 38 ([88, Corollary 3.67] and [84, Theorem 2.1])**.** *Let $\mathbb{F} = \mathbb{F}_q$. Let $\mathcal{F} = \{f_1, \dots, f_m, x_1^q - x_1, \dots, x_n^q - x_n\} \subseteq R$ be a polynomial system. If $d_{\text{reg}}(\mathcal{F}) \geq \max\{q, \deg(f_1), \dots, \deg(f_m)\}$, then for standard algorithms*

$$\text{solv. deg}^s(\mathcal{F}) \leq 2d_{\text{reg}}(\mathcal{F}) - 2.$$

Notice that, in almost all systems of cryptographic interest, the field size and the degrees of the polynomials are relatively small. Therefore, one expects that Theorem 38 applies to such systems.

Another recent result by Salizzoni [82] shows that the solving degree of a mutant algorithm is at most the degree of regularity plus one, unless the system contains polynomials of large degree.

Theorem 39 ([82, Proposition 3.10]). *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a polynomial system, then for mutant algorithms*

$$\text{solv. deg}^m(\mathcal{F}) \leq \max\{d_{\text{reg}}(\mathcal{F}) + 1, \deg(f_1), \ldots, \deg(f_m)\}.$$

Remark 40. *Given a polynomial system $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$, the complexity of a standard linear-algebra-based algorithms for computing a degree reverse lexicographic Gröbner basis of the ideal $(\mathcal{F})$ is dominated by the cost of Gaussian elimination in degree* $\text{solv. deg}^s(\mathcal{F})$*, which is*

$$O(m^2(n + \text{solv. deg}^s(\mathcal{F}))^{3 \cdot \text{solv.deg}^s(\mathcal{F})}).$$

Instead, the complexity of a mutant algorithm is more complicated and related with the degree of regularity of the system, provided that it is large enough. In [83, Proposition 3.13], Salizzoni shows that this complexity is

$$O((n+1)^{4(d_{\text{reg}}(\mathcal{F})+1)}).$$

Thanks to Theorem 38, if the degree of regularity of $\mathcal{F}$ is large enough, $d_{\text{reg}}(\mathcal{F})$ translates into an upper bound on the standard solving degree with respect to the degree reverse lexicographic order. Therefore, knowing the degree of regularity of a system yields an upper bound on the complexity of computing a lexicographic Gröbner basis, since the complexity of the FGLM Algorithm is negligible with respect to the one of the Gaussian elimination. Hence, assuming that $\mathcal{F}$ has at least one solution over the algebraic closure $\overline{\mathbb{F}}$, the degree of regularity results in an upper bound on the complexity of solving the polynomial system thanks to Corollary 34.

In Section 1.1, we discussed the relation between the index of regularity and the Castelnuovo-Mumford regularity. In particular, this relation yields the following observations.

Remark 41. *If $\mathbb{F} = \mathbb{F}_q$ and the system $\mathcal{F}$ contains the field equations $x_1^q - x_1, \ldots, x_n^q - x_n$, then $\left(\mathcal{F}^{\text{top}}\right)_d = R_d$ for $d \gg 0$, therefore the degree of regularity is finite.*

Remark 42. *If $\left(\mathcal{F}^{\text{top}}\right)_d = R_d$ for $d \gg 0$, then*

$$d_{\text{reg}}(\mathcal{F}) = \text{reg}(\mathcal{F}^{\text{top}}).$$

Therefore:

- *By Theorem 39*

  $$\text{solv. deg}^m(\mathcal{F}) \leq \max\{\text{reg}(\mathcal{F}^{\text{top}}) + 1, \deg(f_1), \ldots, \deg(f_m)\}$$

  for mutant algorithms.

- *If $d_{\text{reg}}(\mathcal{F}) \geq \max\{q, \deg(f_1), \ldots, \deg(f_m)\}$, then by Theorem 38*

  $$\text{solv. deg}^s(\mathcal{F}) \leq 2\,\text{reg}(\mathcal{F}^{\text{top}}) - 2$$

  for standard algorithms.

The advantage of focusing on the Castelnuovo-Mumford regularity instead of on the solving degree is that it has been extensively studied in the algebraic literature. In fact, algebraic results related to this invariant will be used throughout Chapter 2 to derive cryptographic bounds for estimating the security of various schemes.

2 Random System

Randomness plays a fundamental role within cryptography. For example, it plays a pivotal role within key generation and cryptographic algorithms are subject to randomness tests. In multivariate cryptography, the public key consists of a multivariate polynomial system and the goal of the attacker is to find a solution of the system. In this context, one typically wishes for the system be as close as possible to, or at least appear as, a random system. A random system is expected to be hard to solve, since the Multivariate Quadratic Problem is not only NP-complete, but also known to be hard to solve on average for a wide range of parameters. From this point of view, e.g., a digital signature scheme whose public keys are sufficiently random is expected to be secure.

In this chapter I discuss what it means for a polynomial system to be random and how hard it is to solve a random polynomial system. The content of this chapter appears in [60]. In Definition 43, we propose a mathematical formulation for the concept of random system. The definition of randomness that we propose, which we call algebraic randomness, is broad enough to include a vast majority of the systems which are of interest in cryptography. We then specify our definition further in Definition 48. One advantage of this definition is that the property of being random according to Definition 48 can be computationally tested, at least in principle.

In Theorem 58, Corollary 62, Corollary 64, Theorem 70, and Proposition 68, we prove upper bounds for the degree of regularity and the solving degree of an algebraically random polynomial system, depending on parameters of the system such as the number of equations, the number of variables, and the degrees of the equations. The usefulness of our bounds is twofold: On the one side, our bounds can be used to directly produce bounds on the complexity of computing a Gröbner basis, hence of solving, many systems which are of interest in cryptography. Bounds on the complexity produced in this way have the advantage of being widely applicable and the disadvantage of not always being close to the actual complexity for each system to which they apply. On the other side, our bounds give us an idea of what security one can hope to achieve for a system with given parameters. In fact, our bounds on the degree of regularity are sharp, i.e., for any choice of the parameters there are systems that meet the bounds. Therefore, our bounds can be used as a point of comparison for the optimality of a given public key, in the following sense. Say that, in order to forge a signature produced with a given multivariate digital signature scheme, one has to find a solution of a system of m equations of degree D in n variables. Suppose that such a system is algebraically random. Our results provide an upper bound B for the degree of regularity or the solving degree of such a system. Say that one can compute or estimate by a different method the degree of regularity or the solving degree of the specific system and suppose that this turns out to be C. Clearly, it must always be that $C \leq B$. However, how far C is from B gives us a measure of how close to optimal the digital signature scheme is, for the given choice of parameters. In fact, since our bounds on the degree of regularity are sharp, there are systems of m equations of degree D in n variables whose degree of regularity is exactly B. In other words, if B and C are close, then there is not much space for improvement, since any system with the same parameters as our public key can have degree of regularity or solving degree at most B. If on the contrary B and C are far apart, then potentially there is a lot of space for finding a more robust system with the same parameters, since a system

with those parameters can have degree of regularity or solving degree up to B.

2.1 Random polynomial systems

Consider a system of m equations of degrees $d_1, \ldots, d_m$ in n variables. Over a finite field, one often defines a random system as a polynomial system whose coefficients are chosen uniformly at random in the given field. Here, a different definition of randomness for a polynomial system is proposed. This definition still captures the intuitive idea of randomness, while allowing us to estimate the degree of regularity of a random system.

Over an infinite field, one may use the concept of genericity from algebraic geometry to define randomness. More precisely, suppose the m equations to be homogeneous, fix a nonempty Zariski-open subset of $\mathbb{P}^{\binom{n+d_1}{n}-1} \times \ldots \times \mathbb{P}^{\binom{n+d_m}{n}-1}$. Define a random system as an element of that open set. This makes sense, since every nonempty Zariski-open set is dense, hence a system of m equations of degrees $d_1, \ldots, d_m$ in n variables whose coefficients are chosen uniformly at random is generic with high probability according to this definition. However, recall that the problem of extending this definition to a finite field is that, over a finite field, a nonempty Zariski-open set is no longer dense, so the connection with the intuitive idea of randomness is lost. Nevertheless, as explained in Subsection 1.1.2, for a finite field $\mathbb{F}_q$, one may define randomness using a Zariski-dense open set defined over the algebraic closure $\overline{\mathbb{F}_q}$. While it is not necessarily the case that almost every polynomial system of given degrees with coefficients in $\mathbb{F}_q$ is random, this is the case whenever q is large enough, or if we consider a finite extension of $\mathbb{F}_q$ of large enough cardinality.

Definition 43. *Let $\mathbb{F}$ be a field and let $\overline{\mathbb{F}}$ be its algebraic closure. Denote by $\mathbb{P}^t$ the t-dimensional projective space over $\overline{\mathbb{F}}$. Let $d_1, \ldots, d_m$ be positive integers and let $\mathcal{U} \subseteq \mathbb{P}^{\binom{n+d_1-1}{n-1}-1} \times \ldots \times \mathbb{P}^{\binom{n+d_m-1}{n-1}-1}$ be a nonempty Zariski-open set. For a homogeneous polynomial f, denote by $[f] \in \mathbb{P}^{\binom{n+\deg(f)-1}{n-1}-1}$ the projective point, whose coordinates are the coefficients of f. A homogeneous system $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ with $\deg(f_i) = d_i$ for $1 \leq i \leq m$ is **generic with respect to $\mathcal{U}$** if $([f_1], \ldots, [f_m]) \in \mathcal{U}$. It is **generic** if it is generic with respect to $\mathcal{U}$, for some nonempty Zariski-open set $\mathcal{U}$. An arbitrary system $\mathcal{F}$ is **generic** or **generic with respect to $\mathcal{U}$** if $\mathcal{F}^{\text{top}}$ is.*

In the cryptographic literature, random sequences of polynomials are often assumed to be cryptographic semiregular sequences, see e.g. [12, 15]. This is the case in the cryptoanalysis of several systems, as e.g. [38]. The next definition appears in [12, Definition 3.2.1 and Definition 3.2.4], [16, Definition 5], and [18, Definition 5 and Definition 9].

Definition 44. *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a homogeneous system.*

*If $\mathbb{F} \neq \mathbb{F}_2$, we say that $f_1, \ldots, f_m$ are a **cryptographic semiregular sequence** if for all $1 \leq i \leq m$ and all $g_i \in R$ such that $g_i f_i \in (f_1, \ldots, f_{i-1})$ and $\deg(g_i f_i) < d_{\text{reg}}(\mathcal{F})$, one has that $g_i \in (f_1, \ldots, f_{i-1})$.*

*If $\mathbb{F} = \mathbb{F}_2$, we say that $f_1, \ldots, f_m \in R/(x_1^2, \ldots, x_n^2)$ are a **cryptographic semiregular sequence** if for all $1 \leq i \leq m$ and all $g_i \in R/(x_1^2, \ldots, x_n^2)$ such that $g_i f_i \in (f_1, \ldots, f_{i-1})$ and $\deg(g_i f_i) < d_{\text{reg}}(\mathcal{F} \cup \{x_1^2 + x_1, \ldots, x_n^2 + x_n\})$, one has that $g_i \in (f_1, \ldots, f_i)$.*

*Arbitrary polynomials $f_1, \ldots, f_m$ are a **cryptographic semiregular sequence** if $f_1^{\text{top}}, \ldots, f_m^{\text{top}}$ are a cryptographic semiregular sequence.*

In this chapter, the name 'cryptographic semiregular sequence' is used in order to distinguish the concept of semiregularity used in the cryptographic literature from the concept of semiregularity originally introduced by Pardue [78], which inspired it. The original definition by Pardue

is given over an infinite field $\mathbb{F}$. As we are interested also in dealing with finite fields, it is extended in the natural way.

Definition 45. *Let $\mathbb{F}$ be an infinite field and let $R = \mathbb{F}[x_1, \ldots, x_n]$. Let I be a homogeneous ideal and let $A = R/I$. A polynomial $f \in R_d$ is **semiregular** on A if for every $e \geq d$, the vector space map $A_{e-d} \to A_e$ given by multiplication by f has maximal rank (that is, it is either injective or surjective). If $\mathbb{F}$ is a finite field, let $\overline{R} = \overline{\mathbb{F}}[x_1, \ldots, x_n]$. Then f is **semiregular** on A if it is semiregular on $\overline{R}/I\overline{R}$.*

*A sequence of homogeneous polynomials $f_1, \ldots, f_m$ is a **semiregular sequence** if f_i is semiregular on $A/(f_1, \ldots, f_{i-1})$ for all $1 \leq i \leq m$.*

It follows from [78, Proposition 1] that, if $\mathbb{F} \neq \mathbb{F}_2$, then a semiregular sequence is also a cryptographic semiregular sequence. The converse does not hold, as shown in [78], see the example just below [78, Proposition 1].

The next proposition presents a simple situation in which cryptographic semiregular sequences and semiregular sequences coincide.

Proposition 46. *Let $q > 2$ and let $f_1 = x_1^q - x_1, \ldots, f_n = x_n^q - x_n, f_{n+1} = f \in R = \mathbb{F}_q[x_1, \ldots, x_n]$. The sequence $f_1, \ldots, f_{n+1}$ is cryptographic semiregular if and only if the sequence $f_1^{\text{top}} = x_1^q, \ldots, f_n^{\text{top}} = x_n^q, f_{n+1}^{\text{top}} = f^{\text{top}}$ is semiregular.*

Proof. It suffices to show that, if the sequence $f_1, \ldots, f_{n+1}$ is cryptographic semiregular, then the sequence $x_1^q, \ldots, x_n^q, f^{\text{top}}$ is semiregular. We start by observing that the sequence $x_1^q, \ldots, x_n^q$ is regular. Therefore, in order to show that $x_1^q, \ldots, x_n^q, f^{\text{top}}$ is semiregular, it suffices to show that f^{top} is semiregular on $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$. If $f_1, \ldots, f_{n+1}$ is cryptographic semiregular and $d = \deg(f)$, then the Hilbert series of $R/(\mathcal{F}^{\text{top}})$ is $[(1 - z^d)(1 + z + \ldots + z^{q-1})^n]$ by [18, Proposition 6]. Here for $p(z) = \sum_{i=0}^{\infty} p_i z^i \in \mathbb{Z}[[z]]$, we denote by $\delta(p) = \min\{i \geq 0 \mid p_i \leq 0\} - 1$ and define $[p(z)] = \sum_{i=0}^{\delta(p)} p_i z^i$. Then f^{top} is semiregular on $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ and $\mathcal{F}^{\text{top}}$ is a semiregular sequence by [78, Proposition 1]. □

Pardue in [78] shows that Fröberg's Conjecture [57], a conjecture which has attracted a lot of attention within the commutative algebra community and that is widely believed to hold, is equivalent to the following

Conjecture 47. *Let $\mathbb{F}$ be an infinite field. A generic sequence of polynomials of degrees $d_1, \ldots, d_m$ in $R = \mathbb{F}[x_1, \ldots, x_n]$ is semiregular.*

In other words, Fröberg conjectures that the set of semiregular sequences of polynomials of given degrees contains a dense Zarisky-open set. If the conjecture is true, then a sequence of polynomials of given degrees is semiregular with high probability, provided that the ground field has large enough cardinality. It follows that, if $\mathbb{F} = \mathbb{F}_q$ with $q \gg 0$ and Fröberg's Conjecture holds, then a sequence of polynomials of given degrees is a cryptographic semiregular sequence with high probability. In addition, most cryptographic semiregular sequences are also semiregular sequences, as the set of semiregular sequences conjecturally contains a dense open set.

In [12, Section 3.2], Bardet conjectures that a sequence of polynomials with coefficients in $\mathbb{F}_2$ is cryptographic semiregular with high probability. This conjecture is motivated by experimental evidence, see also [15, Conjecture 2]. The conjecture was later disproved by Hodges, Molina, and Schlather, who in [63] prove that there are choices of the parameters for which no

cryptographic semiregular sequence exists over $\mathbb{F}_2$. This is the case, e.g., for $m = 1$ and $n > 3d_1$. In the sequel, we propose a notion of randomness which applies to any choice of the system parameters.

Together Professor Gorla, we propose two dense Zariski-open sets, which can be used to formalize the intuitive idea of a random system. The set $\mathcal{V}$ corresponds to systems of m polynomials in n variables which contain a regular sequence of length n, while the set $\mathcal{U}$ parametrizes systems of m polynomials which contain a regular sequence of n polynomials of the smallest possible degrees. Notice that $\mathcal{V}$ contains $\mathcal{U}$ and, if $m \geq n$, it also contains the set of cryptographic semiregular sequences and that of semiregular sequences.

Definition 48. *Fix $m \geq n \geq 1$ and $1 \leq d_1 \leq \ldots \leq d_m$. For any multiset Δ of cardinality n contained in the multiset $\{d_1, \ldots, d_m\}$, let $\mathcal{U}_\Delta$ be the subset of $\mathbb{P}^{\binom{n+d_1-1}{n-1}-1} \times \ldots \times \mathbb{P}^{\binom{n+d_m-1}{n-1}-1}$ whose points correspond to polynomials $f_1, \ldots, f_m \in R$ such that $(f_1^{\text{top}}, \ldots, f_m^{\text{top}})$ contains a regular sequence in the degrees of Δ. Let*

$$\mathcal{U} = \mathcal{U}_{\{d_1,\ldots,d_n\}} \quad \text{and} \quad \mathcal{V} = \bigcup_{\Delta \subseteq \{d_1,\ldots,d_m\}, |\Delta|=n} \mathcal{U}_\Delta.$$

*An **algebraically random system** of m polynomials of degrees $d_1, \ldots, d_m$ in n variables is a system $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ such that $\deg(f_i) = d_i$ for all $1 \leq i \leq m$ and $([f_1], \ldots, [f_m]) \in \mathcal{U}$.*

It is well-known that $\mathcal{U}_{\{d_1,\ldots,d_n\}}$ is a dense open set for any choice of $1 \leq d_1 \leq \ldots \leq d_n$, if $m = n$. This implies that any $\mathcal{U}_\Delta$ as in Definition 48 is a dense open set, hence also $\mathcal{U}$ and $\mathcal{V}$ are. Notice that the degree of regularity is finite for all systems in $\mathcal{U}_\Delta$ for any choice of Δ, therefore it is also finite for the systems in $\mathcal{U}$ and $\mathcal{V}$. In particular, the degree of regularity of an algebraically random system is finite. Notice moreover that, if $\mathcal{F}$ is homogeneous, then $\mathcal{V}$ is the set of polynomial systems of degrees $d_1, \ldots, d_m$ for which the degree of regularity is finite. Notice moreover that, if $m = n$, a random system is a system for which $\mathcal{F}^{\text{top}}$ is a regular sequence. Since this case is well-studied in the cryptographic literature, in the sequel we often assume $m > n$.

Remark 49. *For any system $\mathcal{F}$ of equations of degree at least q, one has*

$$\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\} \in \mathcal{U}_{\{q,\ldots,q\}}.$$

Unlike semiregular systems [63], algebraically random systems exist for any choice of the parameters and over every finite field.

Remark 50. *Algebraic random systems over $\mathbb{F}_q$ exist for any choice of n, m and $1 \leq d_1 \leq \ldots \leq d_m$. This corresponds to the existence of regular sequences of any given degrees in $\mathbb{F}_q[x_1, \ldots, x_n]$, as any system of m equations in $\mathbb{F}_q[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_m$ which contains a regular sequence in degrees $d_1, \ldots, d_n$ is algebraically random. Some regular sequences in $\mathbb{F}_q[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_n$ are for example*

$$x_1^{d_1} + g_1, x_2^{d_2} + g_2, \ldots, x_n^{d_n} + g_n,$$

where $g_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ and $\deg(g_i) \leq d_i$.

2.2 The degree of regularity of a random system

The goal of this section is to establish an upper bound for the degree of regularity of an algebraically random system $\mathcal{F}$ consisting of m polynomials of equal degree D. In combination with Theorem 38 and Theorem 39, this provides an upper bound for the solving degree of a system of algebraically random polynomials of the same degree.

Remark 51. *Notice that $\mathcal{F} \in \mathcal{U}_{\{d,\dots,d\}}$ for a given $d > 0$ if and only if $T \circ \mathcal{F} \circ S \in \mathcal{U}_{\{d,\dots,d\}}$, where the maps T and S are the ones defined in the introduction. In other words, when deciding whether a system of polynomials of equal degree is algebraically random, one can safely ignore the random linear transformations S and T used to disguise the internal system $\mathcal{F}$. This also shows that, for system whose equations are all of the same degree, being an algebraically random system is an intrinsic property of the system and it is not affected by the invertible linear transformations used to disguise the system.*

In [24, Section 4], the authors provide an upper bound for the degree of regularity of a system of quadratic polynomials which contains a regular sequence. In this section, we follow the same basic approach and extend it to systems of polynomials of the same degree and systems of polynomials of the same degree to which one adds the field equations. The cases that we treat in this work are technically more challenging and require the use of more sophisticated results from commutative algebra.

We start by introducing the family of lex-segment ideals. A conjecture by Eisenbud, Green, and Harris will allow us to reduce to these ideals, when estimating the regularity of ideals generated by algebraically random systems. Throughout the section, we fix the lexicographic term order on R with $x_1 > x_2 > \dots > x_n$.

Definition 52. *A monomial ideal $I \subseteq R$ is a **lex-segment ideal** if it has the property that if $u, v \in R$ are monomials of the same degree such that $u \geq_{\text{lex}} v$ and $v \in I$, then $u \in I$.*

*Let C and $c_1 \leq \dots \leq c_n$ be non negative integers. An ideal $\mathcal{L} \subseteq R$ is a **$(c_1, \dots, c_n; C)$-LexPlusPowers (LPP) ideal** if $\mathcal{L} = (x_1^{c_1}, \dots, x_n^{c_n}) + L$, where L is a lex-segment ideal generated in degree C.*

Notation 53. *Let $I \subseteq R$ be a homogeneous ideal containing a regular sequence of polynomials of degrees $c_1 \leq \dots \leq c_n$. For each $C \geq 0$, we denote by $\text{LPP}(I; c_1, \dots, c_n; C)$ the $(c_1, \dots, c_n; C)$-LPP ideal $\mathcal{L} = (x_1^{c_1}, \dots, x_n^{c_n}) + L$ such that $\dim(I_C) = \dim(\mathcal{L}_C)$. We make L unique by choosing the largest lex-segment ideal generated in degree C for which the equality $\mathcal{L} = (x_1^{c_1}, \dots, x_n^{c_n}) + L$ holds.*

Example 54. *Let $I \subseteq \mathbb{F}[x, y, z]$ be generated by a homogeneous regular sequence of polynomials of degrees $1, 3, 4$. The $(1, 3, 4; 3)$-LPP ideal $\mathcal{L}$ such that $\dim(I_3) = 7 = \dim(\mathcal{L}_3)$ is $\mathcal{L} = (x, y^3, z^4)$.*

For any lex-segment ideal L generated in degree 3 with $\dim(L_3) \leq 7$, one has $L \subseteq \mathcal{L}$. Hence one may write

$$\mathcal{L} = (x, y^3, z^4) + L$$

as in Definition 52 and choose e.g. $L = (x^3, x^2y, x^2z, xy^2, xyz, xz^2)$, or $L = (x^3)$. However, Notation 53 prescribes that we choose the largest L with respect to containment, i.e.

$$L = (x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^3)$$

is the lex-segment ideal generated by the first 7 cubic monomials in the lexicographic order.

The next conjecture appears as [48, Conjecture (V_m)]. It has been settled in several cases and it is widely believed to hold within the commutative algebra community. For an introduction to the conjecture and an excellent survey of known cases, we refer the interested reader to [40]. Here we state it in a weak form, which is what we need in the sequel.

Conjecture 55 (Eisenbud-Green-Harris Conjecture)**.** *Let $I \subseteq R$ be a homogeneous ideal containing a regular sequence of polynomials of degrees $c_1 \leq \ldots \leq c_n$. Then*

$$\operatorname{reg}(I) \leq \operatorname{reg}(\operatorname{LPP}(I; c_1, \ldots, c_n; C))$$

for all $C \geq c_n$.

In order to estimate the degree of regularity of our systems, we use the following result by Caviglia and De Stefani.

Proposition 56 ([39, Lemma 2.3])**.** *Let $c_1 \leq \ldots \leq c_n$ and $2 \leq C \leq \sum_{i=1}^{n}(c_i - 1)$. Let $\mathcal{L} = (x_1^{c_1}, \ldots, x_n^{c_n}) + L$ be a $(c_1, \ldots, c_n; C)$-LPP ideal, and assume that $\mathcal{L} \neq (x_1^{c_1}, \ldots, x_n^{c_n})$. Let $u = x_k^{t_k} v$, with $t_k \neq 0$ and $v \in \mathbb{F}[x_{k+1}, \ldots, x_n]$, be the smallest monomial with respect to the lexicographic order which belongs to L and has degree C. Then*

$$\operatorname{reg}(\mathcal{L}) = t_k + \sum_{i=k+1}^{n}(c_i - 1).$$

The first result is an explicit bound for the degree of regularity of an algebraically random systems of polynomials of the same degree. In order to make the proof more readable, we introduce the following notation.

Notation 57. *If $u \in R_D$ is a monomial that only involves the variables $x_k, \ldots, x_n$ and has degree a in x_k, we say that u is a (D, k, a)-*type *monomial.*

In the next theorem, we provide an explicit formula for the degree of regularity of an LPP ideal with given parameters. Thanks to Conjecture 55, this yields an upper bound for the degree of regularity of an algebraically random system of polynomials of the same degree. In the statement of the theorem, $\sigma_{k,t}$ is the position of the smallest $(D, k, D-t)$-type monomial in the ordered list of monomials of degree D different from $x_1^D, \ldots, x_n^D$, sorted in decreasing lexicographic order. In particular, $\sigma_{1,0} = 0$ and $\sigma_{n-1,D-1}$ is the number of monomials of degree D different from $x_1^D, \ldots, x_n^D$.

Theorem 58. *Assume that Conjecture 55 holds. Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq R$ be a polynomial system and assume without loss of generality that $f_1^{\text{top}}, \ldots, f_m^{\text{top}}$ are linearly independent of degree D. If $m = n$, then let $k = 0$, $t = D - 1$. Else, let $1 \leq k \leq n - 1$ and $0 \leq t \leq D - 1$ be such that $m - n$ belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$, where*

$$\sigma_{k,t} = \sum_{i=1}^{k}\sum_{j=1}^{D-1}\binom{n-i-1+j}{j} - \sum_{j=t+1}^{D-1}\binom{n-k-1+j}{j}.$$

If $\mathcal{F}$ is an algebraically random polynomial system, then

$$d_{\text{reg}}(\mathcal{F}) \leq (D - t) + (n - k)(D - 1).$$

Proof. If $m = n$, then $\mathcal{F}^{\text{top}}$ is a regular sequence of n polynomials of degree D, hence

$$d_{\text{reg}}(\mathcal{F}) = n(D-1)+1.$$

Suppose therefore that $m > n$ and let J be the ideal generated by $\mathcal{F}^{\text{top}}$. Consider the lexicographic order on R and let

$$\mathcal{L} = \text{LPP}(J; D, \dots, D; D) = (x_1^D, \dots, x_n^D) + L,$$

be the LPP ideal with L the largest lex-segment ideal generated in degree D such that $\dim(\mathcal{L}_D) = m$. Since both $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ and $x_1^D, \dots, x_n^D$ are linearly independent, we have

$$\dim\left(\mathcal{L}_D/\langle x_1^D, \dots, x_n^D\rangle\right) = m - n.$$

For $1 \le k \le n-1$ and $0 \le t \le D-1$, the number of $(D, k, D-t)$-type monomials is

$$\dim(\mathbb{F}_q[x_{k+1}, \dots, x_n]_t) = \binom{n-k-1+t}{t},$$

hence

$$\begin{aligned}\sigma_{k,t} &= \sum_{i=1}^{k-1}\sum_{j=1}^{D-1}\binom{n-i-1+j}{j} + \sum_{j=1}^{t}\binom{n-k-1+j}{j} \\ &= \sum_{i=1}^{k-1}\sum_{j=1}^{D-1}\dim(\mathbb{F}_q[x_{i+1}, \dots, x_n])_j + \sum_{j=1}^{t}\dim(\mathbb{F}_q[x_{k+1}, \dots, x_n])_j\end{aligned}$$

is the number of degree D monomials in $\mathbb{F}_q[x_1, \dots, x_n]$ different from $x_1^D, \dots, x_n^D$ and bigger than or equal to $x_k^{D-t}x_n^t$, the smallest $(D, k, D-t)$-type monomial. In other words, the monomial $x_k^{D-t}x_n^t$ is in position $\sigma_{k,t}$ is the ordered list of degree D monomials in $\mathbb{F}_q[x_1, \dots, x_n]/(x_1^D, \dots, x_n^D)$. Notice moreover that $\sigma_{1,0} = 0$ and $\sigma_{k,0} = \sigma_{k-1,D-1}$ for $2 \le k \le n-1$.

If u is the smallest monomial in $\mathcal{L}_D/\langle x_1^D, \dots, x_n^D\rangle$, then u is in position $m-n$ in the ordered list of degree D monomials in $\mathbb{F}_q[x_1, \dots, x_n]/(x_1^D, \dots, x_n^D)$. If $\sigma_{k,t-1} < \ell \le \sigma_{k,t}$ for some $1 \le k \le n-1$ and $1 \le t \le D-1$, then u is a $(D, k, D-t)$-type monomial. Since $0 = \sigma_{1,0} < \ell \le \dim(\mathbb{F}_q[x_1, \dots, x_n]_D)/(x_1^D, \dots, x_n^D)_D = \sigma_{n-1,D-1}$, then $m-n$ always belong to one of the intervals above.

The ideal L is generated by the degree D monomials which are greater than or equal to u, unless the monomial following u in lexicographic decreasing order is a pure power. In that case, $u = x_k x_n^{D-1}$ for some $1 \le k \le n-1$, i.e. $m - n = \sigma_{k,D-1}$, and the smallest degree D monomial in L is x_{k+1}^D. Then L is generated by the degree D monomials which are greater than or equal to x_{k+1}^D, which is a $(D, k+1, D)$-type monomial. In both situations

$$\text{reg}(\mathcal{L}) = (D-t) + (n-k)(D-1)$$

by Proposition 56. The thesis now follows from observing that

$$d_{\text{reg}}(\mathcal{F}) = \text{reg}(J) \le \text{reg}(\mathcal{L}), \tag{2.2.1}$$

where the inequality follows from Conjecture 55. □

Example 59. *In this example we show how to compute the bound from Theorem 58 for concrete choices of the parameters. Let $n = 6$ and $D = 3$, so $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq \mathbb{F}_q[x_1, \dots, x_6]_3$. Then $1 \le k \le 5$ and $0 \le t \le 2$. The values of $\sigma_{k,t}$ are*

$\sigma_{k,t}$	$t = 0$	$t = 1$	$t = 2$
$k = 1$	0	5	20
$k = 2$	20	24	34
$k = 3$	34	37	43
$k = 4$	43	45	48
$k = 5$	48	49	50

If $m = 12$, then $m - n = 6$ and $\sigma_{1,1} < 6 \le \sigma_{1,2}$. Hence $k = 1$, $t = 2$, and $d_{\mathrm{reg}}(\mathcal{F}) \le 11$.
If $m = 42$, then $m - n = 36$ and $\sigma_{3,0} < 36 \le \sigma_{3,1}$. Hence $k = 3$, $t = 1$ and $d_{\mathrm{reg}}(\mathcal{F}) \le 8$.
If $m = 54$, then $m - n = 48$ and $\sigma_{4,1} < 48 \le \sigma_{4,2}$. Hence $k = 4$, $t = 2$, and $d_{\mathrm{reg}}(\mathcal{F}) \le 5$.

Remark 60. *The upper bound of Theorem 58 is decreasing as a function of m, as one would expect. In particular, as $m - n$ passes from an interval $(\sigma_{k,t-1}, \sigma_{k,t}]$ to the next, the upper bound decreases by one. The largest value of the bound is obtained in the case $m = n$, which corresponds to $\mathcal{F}^{\mathrm{top}}$ being a regular sequence. In this case, the value for the bound is well-know and is $n(D-1)+1$. The smallest value for the bound is obtained in the case $m - n = \sigma_{n-1,D-1}$, which corresponds to $\langle \mathcal{F}^{\mathrm{top}} \rangle + \langle x_1^D, \dots, x_n^D \rangle = R_D$. In this case, the value for the bound is easily seen to be D.*

Remark 61. *The upper bound produced in Theorem 58 is sharp for all values of m, n, D. In fact, it is met by any system $\mathcal{F}$ such that $(f_1^{\mathrm{top}}, \dots, f_m^{\mathrm{top}})$ is a $(D, \dots, D; D)$-LPP ideal.*

Combining Theorem 58 and Theorem 39, we obtain the following.

Corollary 62. *Let $\mathcal{F} \subseteq R$ be an algebraically random system of degree D polynomials. If $m = n$, then let $k = 0$, $t = D - 1$. Else, let $1 \le k \le n - 1$ and $1 \le t \le D - 1$ be such that $m - n$ belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$. If Conjecture 55 holds, then*

$$\mathrm{solv.deg}^m(\mathcal{F}) \le D - t + 1 + (n - k)(D - 1).$$

Proof. The upper bound found in Theorem 58 for the degree of regularity of $\mathcal{F}$ is bigger than or equal to D for all k and t. The thesis then follows from Theorem 39. □

We now wish to apply Theorem 58 to a system which contains the field equations.

Remark 63. *After reducing the equations of $\mathcal{F}$ modulo the field equations, they have degree at most $q - 1$ in each variable, hence total degree at most $n(q - 1)$. Therefore, when adding the field equations to a polynomial system of degree D, we may always assume that*

$$D \le n(q - 1).$$

Combining Theorem 58 and Theorem 38, one obtains the following. By Remark 63, we may assume without loss of generality that $D \le n(q - 1)$.

Corollary 64. *Assume that Conjecture 55 holds. Let $\mathcal{F} \subseteq R$ be an algebraically random system of degree D polynomials, with $D \leq n(q-1)$. If $m = n0$, then let $k = 0$, $t = D-1$. Else, let $1 \leq k \leq n-1$ and $1 \leq t \leq D-1$ be such that $m-n$ belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$. If $d_{\mathrm{reg}}(\mathcal{F}) \geq q$, then*

$$\text{solv. deg}^s(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq 2 \min\{n(q-1), (n-k+1)(D-1) - t\}.$$

Proof. First, since $(x_1^q, \ldots, x_n^q)_{n(q-1)+1} = R_{n(q-1)+1}$, one has

$$d_{\mathrm{reg}}(\mathcal{F}^{\mathrm{top}} \cup \{x_1^q, \ldots, x_n^q\}) \leq n(q-1)+1.$$

If $D < q$, then

$$(\mathcal{F}^{\mathrm{top}} \cup \{x_1^q, \ldots, x_n^q\})_{q-1} = (\mathcal{F}^{\mathrm{top}})_{q-1} \neq R_{q-1},$$

since $d_{\mathrm{reg}}(\mathcal{F}) \geq q$ by assumption. Therefore, $d_{\mathrm{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \geq q = \max\{D, q\}$. If $q \leq D \leq n(q-1)$, then

$$(\mathcal{F}^{\mathrm{top}} \cup \{x_1^q, \ldots, x_n^q\})_{D-1} = (x_1^q, \ldots, x_n^q)_{D-1} \neq R_{D-1},$$

hence $d_{\mathrm{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \geq D = \max\{D, q\}$. This shows that the assumptions of Theorem 38 are satisfied. The thesis now follows by combining Theorem 58, Theorem 38, and the observation that

$$d_{\mathrm{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq d_{\mathrm{reg}}(\mathcal{F}).$$

□

Remark 65. *While the estimates of Corollary 62 and of Corollary 64 hold for every D, they are most relevant for $D \leq q$. In fact, for $D > q$ we obtain tighter upper bounds on the degree of regularity - hence on the solving degree - of $\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}$ in Theorem 70 by inspecting the degree D part of the system $\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\} \in \mathcal{U}_{\{q,\ldots,q\}}$. This corresponds to the fact that, whenever the degree of the equations of the system is larger than or comparable to the field size, it is convenient to add the field equations to the system before computing a Gröbner basis.*

Next we estimate the degree of regularity and the solving degree of $\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}$ in the case when $D \geq q$. By Remark 63, we may assume that $D \leq n(q-1)$.

First, we observe that one can easily derive a lower bound on the degree of regularity.

Remark 66. *Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a polynomial system of degree $q \leq D \leq n(q-1)$. Since $(\mathcal{F}^{\mathrm{top}} \cup \{x_1^q, \ldots, x_n^q\})_{D-1} = (x_1^q, \ldots, x_n^q)_{D-1} \neq R_{D-1}$, then*

$$d_{\mathrm{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \geq D.$$

We now want to derive an upper bound. We start by computing the number of linearly independent homogeneous polynomials of degree D as a function of n, D, q.

Remark 67. *Assume that $q \leq D \leq n(q-1)$. A standard Hilbert function computation shows that the number of homogeneous polynomials in n variables of degree D which are linearly*

independent modulo $(x_1^q, \dots, x_n^q)$ *is*

$$\dim(R/(x_1^q, \dots, x_n^q))_D = \sum_{i=0}^{\lfloor \frac{D}{q} \rfloor} (-1)^i \binom{n}{i} \binom{n+D-1-iq}{n-1}.$$

It follows that the assumption that $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ *are linearly independent modulo* $(x_1^q, \dots, x_n^q)$ *holds on a dense open set, whenever*

$$m \leq \sum_{i=0}^{\lfloor \frac{D}{q} \rfloor} (-1)^i \binom{n}{i} \binom{n+D-1-iq}{n-1}. \tag{2.2.2}$$

If inequality (2.2.2) is not satisfied, then $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ *cannot be linearly independent.*

The simplest case to treat is that of very overdetermined systems, more specifically the case when $f_1^{\text{top}}, \dots, f_m^{\text{top}}$ are too many to be linearly independent modulo $(x_1^q, \dots, x_n^q)$. This happens when m is larger than the bound from Remark 67. The next proposition shows that, in such a situation, the degree of regularity is equal to the degree of the equations of the system.

Proposition 68. *Let* $\mathcal{F} = \{f_1, \dots, f_m\}$ *be a polynomial system of degree* D*, where* $q \leq D \leq n(q-1)$*. If* $m > \sum_{k=0}^{\lfloor \frac{D}{q} \rfloor} (-1)^k \binom{n}{k} \binom{n+D-1-kq}{n-1}$*, then there is a dense open set* $\mathcal{W}$ *such that, if* $\mathcal{F} \in \mathcal{W}$*, then*

$$d_{\text{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \dots, x_n^q - x_n\}) = D.$$

Moreover,

$$\text{solv.deg}^s(\mathcal{F} \cup \{x_1^q - x_1, \dots, x_n^q - x_n\}) \leq 2D - 2$$

and

$$\text{solv.deg}^m(\mathcal{F} \cup \{x_1^q - x_1, \dots, x_n^q - x_n\}) \leq D + 1.$$

Proof. Since by assumption

$$m > \sum_{k=0}^{\lfloor \frac{D}{q} \rfloor} (-1)^k \binom{n}{k} \binom{n+D-1-kq}{n-1} = \dim(R/(x_1^q, \dots, x_n^q))_D,$$

then there is an open set $\mathcal{W}$ of m-tuples of polynomials of degree D such that

$$\langle f_1^{\text{top}}, \dots, f_m^{\text{top}} \rangle + (x_1^q, \dots, x_n^q)_D = R_D.$$

Since $(\mathcal{F}^{\text{top}} \cup \{x_1^q, \dots, x_n^q\})_{D-1} = (x_1^q, \dots, x_n^q)_{D-1} \neq R_{D-1}$, then

$$d_{\text{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \dots, x_n^q - x_n\}) = D.$$

The rest of the statement now follows from Theorem 38 and Theorem 39. □

The next theorem yields an upper bound on the degree of regularity of an algebraically random system of equations of degree larger than the field size to which we add the field equations. For such a system, the bound is tighter than the one from Corollary 64. We start with a preparatory lemma, whose proof follows directly from the definition.

Lemma 69. *Let u, v be monomials of type (D, k, a) and (D, h, b), respectively. If $u \geq v$, then either $k < h$ or $k = h$ and $a \geq b$. In particular, if u, v, w are monomials such that $u \geq v \geq w$ and u and w have the same type, then v also has the same type as u and w.*

Theorem 70. *Assume that Conjecture 55 holds. Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a polynomial system of degree D, with $q \leq D \leq n(q-1)$. Assume that $m \leq \sum_{i=0}^{\lfloor \frac{D}{q} \rfloor} (-1)^i \binom{n}{i} \binom{n+D-1-iq}{n-1}$ and that $f_1^{\text{top}}, \ldots, f_m^{\text{top}}$ are linearly independent modulo $(x_1^q, \ldots, x_n^q)_D$. Let $1 \leq t \leq q-1$ and $1 \leq k \leq n-1$ be such that m belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$, where*

$$\sigma_{k,t} = \sum_{i=1}^{k-1} \sum_{j=1}^{q-1} \eta_{i,j} + \sum_{j=1}^{t} \eta_{k,j}$$

and

$$\eta_{k,t} = \sum_{i=0}^{\left\lfloor \frac{D+t}{q} \right\rfloor - 1} (-1)^i \binom{n-k}{i} \binom{n-k-1+D-(i+1)q+t}{n-k-1}.$$

Let

$$B = q - t + (n-k)(q-1).$$

If $m = \sigma_{k,t}$ and either $t \neq q-1$ and $D \geq 2q-t-1$, or $t = q-1$ and $D \geq 2q-1$, then

$$d_{\text{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq B - 1,$$

$$\text{solv.deg}^s(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq 2(B-2),$$

and

$$\text{solv.deg}^m(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq B + 1.$$

In any other case

$$d_{\text{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq B,$$

$$\text{solv.deg}^s(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq 2(B-1),$$

and

$$\text{solv.deg}^m(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) \leq B + 1.$$

Proof. We start by proving that $\eta_{k,t}$ is the number of $(D, k, q-t)$-type monomials in R which are linearly independent modulo $(x_1^q, \ldots, x_n^q)_D$, that is

$$\eta_{k,t} = \dim \left[\frac{\mathbb{F}_q[x_{k+1}, \ldots, x_n]}{(x_{k+1}^q, \ldots, x_n^q)} \right]_{D-q+t}. \tag{2.2.3}$$

Since $x_{k+1}^q, \ldots, x_n^q$ is a regular sequence in $\mathbb{F}_q[x_{k+1}, \ldots, x_n]$, a standard computation involving Hilbert series yields the explicit formula

$$\dim \left[\frac{\mathbb{F}_q[x_{k+1}, \ldots, x_n]}{(x_{k+1}^q, \ldots, x_n^q)} \right]_{D-q+t} = \sum_{i=0}^{\left\lfloor \frac{D+t}{q} \right\rfloor - 1} (-1)^i \binom{n-k}{i} \binom{n-k-1+D-(i+1)q+t}{n-k-1},$$

where we notice that $\eta_{k,t} \neq 0$ only if $D + t - q \leq (n-k)(q-1)$. This establishes the equality in

(2.2.3). Similarly to the proof of Theorem 58, we notice that

$$\sigma_{k,t} = \sum_{i=1}^{k-1} \sum_{j=1}^{q-1} \eta_{i,j} + \sum_{j=1}^{t} \eta_{k,j}$$

is the number of monomials of degree D which do not belong to $(x_1^q, \dots, x_n^q)$ and are greater than or equal to $x_k^{q-t} x_n^{D-q+t}$, the smallest $(D, k, q-t)$-type monomial. Moreover, $\sigma_{k-1,q-1} = \sigma_{k,0}$ for $2 \leq k \leq n-1$.

Let $I \subseteq \mathbb{F}_q[x_1, \dots, x_n]$ be the ideal generated by $\mathcal{F}^{\text{top}} \cup \{x_1^q, \dots, x_n^q\}$. Let $\mathcal{L} = (x_1^q, \dots, x_n^q) + L$ be the $(q, \dots, q; D)$-LPP ideal such that

$$\dim(I_D) = \dim(\mathcal{L}_D) = m + \dim(x_1^q, \dots, x_n^q)_D.$$

Hence $\mathcal{L}$ is minimally generated by $x_1^q, \dots, x_n^q$ and m monomials of degree D that do not belong to $(x_1^q, \dots, x_n^q)$. Recall that, by assumption, L is the largest lex-segment ideal generated in degree D such that $\mathcal{L} = (x_1^q, \dots, x_n^q) + L$, i.e., $L_D \supseteq (x_1^q, \dots, x_n^q)_D$.

Let u be the smallest degree D monomial in $\mathcal{L}/(x_1^q, \dots, x_n^q)$. Notice that u is a $(D, k, q-t)$-type monomial, since m belongs to the interval $(\sigma_{k,t-1}, \sigma_{k,t}]$. Let v be the smallest degree D monomial in L. If u is the smallest monomial in $(R/(x_1^q, \dots, x_n^q))_D$, then $u = x_k^{q-t} x_{k+1}^{q-1} \cdots x_n^{q-1}$ and $D = q - t + (n-k)(q-1)$. Moreover, $\mathcal{L}_D = R_D$ and $v = x_n^D$ is a (D, n, D)-type monomial.

Assume now that u is not the smallest monomial in $(R/(x_1^q, \dots, x_n^q))_D$ and let w be the monomial in $(R/(x_1^q, \dots, x_n^q))_D$ which follows u in decreasing lexicographic order. Then $u \geq v \geq w$ and v is the degree D monomial next to w in increasing lexicographic order. If $m \neq \sigma_{k,t}$, then w has type $(D, k, q-t)$, hence so does v by Lemma 69. Suppose therefore that $m = \sigma_{k,t}$. Write $D-q+t = (n-\ell)(q-1)+r$, where $0 \leq r < q-1$. Notice that $D-q+t < (n-k)(q-1)$, since u is not the smallest monomial in $(R/(x_1^q, \dots, x_n^q))_D$. Then $\ell > k$. In this situation, $u = x_k^{q-t} x_\ell^r x_{\ell+1}^{q-1} \cdots x_n^{q-1}$ and $w = x_k^{q-t-1} x_{k+1}^{q-1} \cdots x_{k+n-\ell}^{q-1} x_{k+n-\ell+1}^{r+1}$. Notice that w is a $(D, k, q-t-1)$-type monomial if $t \neq q-1$ and a $(D, k+1, q-1)$-type monomial if $t = q-1$. If w is not the smallest degree D monomial of its type in R_D, then v has the same type as w. If w is the smallest degree D monomial of its type in R_D, then $w = x_k^{q-t-1} x_{k+1}^{D-q+t+1}$ in the case $t \neq q-1$ and $w = x_{k+1}^{q-1} x_{k+2}^{D-q+1}$ in the case $t = q-1$. Since $w \notin (x_1^q, \dots, x_n^q)$, this is only possible if $D \leq 2q-t-2$ for $t \neq q-1$ and $D \leq 2q-2$ for $t = q-1$. In this situation, v has type $(D, k, q-t)$ in the case $t \neq q-1$ and type $(D, k+1, q)$ in the case $t = q-1$.

If Conjecture 55 holds, then

$$d_{\text{reg}}(\mathcal{F} \cup \{x_1^q - x_1, \dots, x_n^q - x_n\}) \leq \text{reg}(\mathcal{L}). \tag{2.2.4}$$

Moreover, by Proposition 56

$$\text{reg}(\mathcal{L}) = \begin{cases} q-t-1+(n-k)(q-1) & \text{if } m = \sigma_{k,t} \text{ and} \\ & \text{either } t \neq q-1 \text{ and } D \geq 2q-t-1, \\ & \text{or } t = q-1 \text{ and } D \geq 2q-1, \\ q-t+(n-k)(q-1) & \text{else.} \end{cases} \tag{2.2.5}$$

The bound on the degree or regularity now follows from (2.2.4) and (2.2.5). The bounds on the solving degree follow from the bound on the degree of regularity, Theorem 38, and Theorem 39.

□

Example 71. *In this example we show how to compute the bound from Theorem 70 for concrete choices of the parameters. Let* $q = 2$, $n = 6$ *and* $D = 4$, *so* $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq \mathbb{F}_q[x_1, \dots, x_6]_4$, *with* $m \leq 15$. *Then* $k = 1, 2, 3, 4, 5$ *and* $t = 0, 1$. *The values of* $\eta_{k,t}$ *are*

$\eta_{k,t}$	$t = 0$	$t = 1$
$k = 1$	*10*	*10*
$k = 2$	*6*	*4*
$k = 3$	*3*	*1*
$k = 4$	*1*	*0*
$k = 5$	*0*	*0*

and the values of $\sigma_{k,t}$ *are*

$\sigma_{k,t}$	$t = 0$	$t = 1$
$k = 1$	*0*	*10*
$k = 2$	*10*	*14*
$k = 3$	*14*	*15*
$k = 4$	*15*	*15*
$k = 5$	*15*	*15*

If $m = 7$, *then* $\sigma_{1,0} < 7 \leq \sigma_{1,1}$. *Hence* $k = 1$, $t = 1$, *and* $d_{\text{reg}}(\mathcal{F} \cup \{x_1^2 - x_1, \dots, x_6^2 - x_6\}) \leq 6$.
If $m = 10$, *then* $\sigma_{1,1} = 10$ *and* $D \geq 3$. *Hence* $k = 1$, $t = 1$, *and* $d_{\text{reg}}(\mathcal{F} \cup \{x_1^2 - x_1, \dots, x_6^2 - x_6\}) \leq 5$.
If $m = 12$, *then* $\sigma_{2,0} < 12 \leq \sigma_{2,1}$. *Hence* $k = 2$, $t = 1$ *and* $d_{\text{reg}}(\mathcal{F} \cup \{x_1^2 - x_1, \dots, x_6^2 - x_6\}) \leq 5$.

2.3 Applications to the study of GeMSS and Rainbow

GeMSS and Rainbow were the only multivariate schemes in Round 3 of the first NIST Post-Quantum Cryptography Standardization process. They are based on modifications of HFE (Hidden Field Equation) and UOV (Unbalanced Oil and Vinegar), respectively. They were subsequently revealed to be insecure and susceptible to a MinRank attack, see e.g. [10, 14, 22, 23], therefore they were excluded from the NIST competition.

In this section, the previous results are used to show that these systems are far being (algebraically) random. Together with Professor Gorla, we do so by computing their degree of regularity or solving degree for small instances and comparing it with the upper bounds obtained in Theorem 58 and Theorem 70. The degree of regularity and solving degree of the systems associated to GeMSS and Rainbow are much smaller than the corresponding invariants for an algebraically random system with the same parameters, which reveals the presence of a hidden structure that may be used to mount an ad-hoc attack, as it was done with the MinRank attack by Beullens [23].

We used Magma to compute the solving degree and Singular to compute the degree of regularity. In particular, the algorithm we used in Magma for computing Gröbner bases is F4, therefore, the computed solving degree should be understood with respect to a standard algorithm. The values that we obtain (and that we indicate in the tables below) are almost always the same for systems with the same parameters. For each choice of the parameters in the table, we produce ten instances of the public key $\mathcal{PK} = \{p_1, \dots, p_m\} \subseteq \mathbb{F}_q[x_1, \dots, x_n]$ of the chosen

scheme. For each one of them, we choose a random vector $s = (s_1, \dots, s_m) \in \mathbb{F}_q^m$ as a message to be signed (in case a valid signature cannot be produced for the chosen vector, we replace it with another randomly chosen vector). In order to forge the signature, an attacker may want to solve the system $\mathcal{PK}s = \{p_1 - s_1, \dots, p_m - s_m\}$. We make the system $\mathcal{PK}s$ square by assigning random values to the last $n - m$ variables. This yields a system $\mathcal{F} = \{f_1, \dots, f_m\} \subseteq \mathbb{F}_q[x_1, \dots, x_m]$.

Since in GeMSS we work over $\mathbb{F}_2$, we add to the system $\mathcal{F}$ the field equations $\mathcal{E} = \{x_1^2 + x_1, \dots, x_m^2 + x_m\}$. In the next table we compare the experimental results we obtained for GeMSS with the bounds from Theorem 70, in fact GeMSS systems are of degree 2. The experiments show that both the solving degree and the degree of regularity of $\mathcal{F}$ can be more than twice the solving degree of $\mathcal{F} \cup \mathcal{E}$. This confirms the intuition that adding the field equations is a good strategy in order to solve the system $\mathcal{F}$ over $\mathbb{F}_2$.

Unfortunately we were able to compute the degree of regularity of $\mathcal{F} \cup \mathcal{E}$ only for small values of the parameters. In the next table the first three columns contain the parameters of the cryptosystem, and the fourth the number of polynomials and variables that appear in $\mathcal{F}$. The columns labelled '$d_{\text{reg}}(\mathcal{F} \cup \mathcal{E})$' and 'sd$(\mathcal{F} \cup \mathcal{E})$' contain the values computed, respectively, with Singular and Magma. The columns labelled 'max sd$(\mathcal{F} \cup \mathcal{E})$' and 'max $d_{\text{reg}}(\mathcal{F} \cup \mathcal{E})$' are the bounds given by the Theorem 70 for the chosen parameters and a standard Gröbner basis algorithm. We omit the exponent 's' in the notation of the solving degree for space reason.

n, D, a, v, m	$d_{\text{reg}}(\mathcal{F} \cup \mathcal{E})$	max $d_{\text{reg}}(\mathcal{F} \cup \mathcal{E})$	sd$(\mathcal{F} \cup \mathcal{E})$	max sd$(\mathcal{F} \cup \mathcal{E})$
12, 4, 1, 1, 11	5	10	3	18
8, 9, 1, 1, 7	3	6	3	10
8, 9, 1, 2, 7	3	6	3	10
8, 9, 2, 1, 6	3	5	3	8
8, 9, 2, 2, 6	3	5	3	8
24, 4, 1, 1, 23		22	4	42
24, 4, 1, 2, 23		22	4	42
24, 4, 1, 3, 23		22	4	42
24, 4, 2, 1, 22		21	4	40
24, 4, 2, 2, 22		21	4	40
24, 4, 3, 1, 21		20	4	38

While GeMSS is random according to Definition 48, the experimental results make it clear that both the degree or regularity and the solving degree of GeMSS are far from the largest values that one can find for a system of those parameters according to Theorem 70. This indicates that, for the same parameters, one should be able to find systems for which the complexity of computing a Gröbner basis is much larger. More importantly, it reveals the presence of a hidden algebraic structure, which may be exploited in ad-hoc attack (as it was in fact done in the MinRank attacks mentioned in the opening paragraph).

For Rainbow, we choose to work over $\mathbb{F}_4$ and $\mathbb{F}_9$. Since $\mathcal{F}$ is a square system, $\mathcal{F}$ is algebraically random if and only if $\mathcal{F}^{\text{top}}$ is a regular sequence. This turns out to be the case in most of the examples that we computed and in that case

$$d_{\text{reg}}(\mathcal{F}) = m + 1 \tag{2.3.6}$$

by Theorem 58. This is confirmed by our computations.

Since the systems coming from this scheme are quadratic, adding the field equations may increase the solving degree of the system. However, for the small values of q that we tried in our experiments, we find that in all cases but one the solving degree decreases when adding the field equations. This makes sense, as the degree q of the equations that we add is never larger than the solving degree of the system to which we add them. In the next table we summarize the results that we obtained in our computational experiments. Since in our experiments the solving degree of $\mathcal{F} \cup \mathcal{E}$ is almost always smaller than that of $\mathcal{F}$, in our examples $\mathcal{F} \cup \mathcal{E}$ is the relevant system to consider, that is, the system that one wants to try to solve. Therefore, we consider the degree of regularity and solving degree of $\mathcal{F} \cup \mathcal{E}$. In our table, we compare the degree of regularity and the solving degree of $\mathcal{F} \cup \mathcal{E}$ with the upper bounds from Theorem 58 and Corollary 64. The first three columns contain the chosen values for the parameters and the number of polynomials and variables that appear in $\mathcal{F}$. The columns labelled '$d_{\text{reg}}(\mathcal{F})$' and 'sd$(\mathcal{F} \cup \mathcal{E})$' contain the values computed with Singular and Magma. The column labelled 'max sd$(\mathcal{F} \cup \mathcal{E})$' contains the bounds from Corollary 64. Again, we omit the notation to indicate the usage of standard algorithm for computing the solving degree. We do not include the values of the degree of regularity and solving degree of $\mathcal{F}$ in the table, as we find that the system $\mathcal{F} \cup \mathcal{E}$ can always be solved more efficiently than the system $\mathcal{F}$.

q	$[v_1, o_1, o_2]$	m	$d_{\text{reg}}(\mathcal{F})$	$d_{\text{reg}}(\mathcal{F} \cup \mathcal{E})$	sd$(\mathcal{F} \cup \mathcal{E})$	max sd$(\mathcal{F} \cup \mathcal{E})$
4	$[3, 2, 2]$	4	4/5	4	4	8
4	$[3, 3, 3]$	6	6/7	5	5	12
4	$[7, 5, 5]$	10	10/11	6	6	20
9	$[3, 2, 2]$	4	5	5	9	–
9	$[7, 5, 5]$	10	11	9/10	10	20

Notice that Corollary 64 does not apply to the case $q = 9$ and $[v_1, o_1, o_2] = [3, 2, 2]$, since $d_{\text{reg}}(\mathcal{F}) = 5$. For these parameters, the bound from Corollary 64 would yield solv. deg$(\mathcal{F} \cup \mathcal{E}) \leq 8$. However, the bound does not hold in this case, as our experiments show.

As for GeMSS, we observe that the values that we computed for the solving degree of $\mathcal{F} \cup \mathcal{E}$ are far from the upper bounds predicted by Corollary 64. We conclude that, also in this case, one expects to find systems with the same parameters as these instances of Rainbow and for which the complexity of computing a Gröbner basis is larger. Once again it reveals the presence of a hidden algebraic structure, which may be exploited in ad-hoc attack (as it was in fact done in the attacks that we mentioned at the beginning of the section).

3 SupportMinors Modeling

The MinRank Problem arises naturally within cryptography and coding theory, as well as in numerous other applications. The problem in its general form can be stated as follows.

MinRank Problem. *Let $\mathbb{F}$ be a field and let m, n, k be positive integers. Given as input k matrices $M_1, \ldots, M_k \in \mathbb{F}^{m \times n}$, find $x_1, \ldots, x_k \in \mathbb{F}$ such that the matrix $\sum_{\ell=1}^{k} x_\ell M_\ell$ is nonzero and has least possible rank.*

In situations when the least possible rank (or a tight upper bound for it) is known, one may rephrase the problem as follows.

MinRank Problem. *Let $\mathbb{F}$ be a field and let m, n, r, k be positive integers. Given as input k matrices $M_1, \ldots, M_k \in \mathbb{F}^{m \times n}$, find $x_1, \ldots, x_k \in \mathbb{F}$ such that*

$$0 < \operatorname{rk}\left(\sum_{\ell=1}^{k} x_\ell M_\ell\right) \leq r.$$

The MinRank Problem plays a central role within multivariate cryptography, both in the cryptanalysis and in the design of schemes, as it is NP-complete [32] and believed to be quantum-resistant. For example, it is a central tool in the cryptanalysis of HFE and its variants [21,34,45,66,89], the TTM Cryptosystem [61], and the ABC Cryptosystem [75,76]. More recently, both GeMSS and Rainbow were subject to attacks which exploit the MinRank Problem, see [11,22,23,87].

On the constructive side, a zero-knowledge protocol based on the MinRank Problem was proposed by Courtois in [43]. This produces a signature scheme following [56]. Recently, a scheme relying on the MinRank Problem for its security was proposed in [81] and cracked in [26]. Digital signature relying on the MinRank Problem for their security were submitted to the NIST Call for Additional Digital Signature Schemes in 2023 [1,5], see also [19].

In addition, the MinRank Problem is closely related to Minimum Distance Decoding in the rank-metric. Notice in fact that, if $C \subseteq \mathbb{F}^{m \times n}$ is a linear rank-metric code with basis $M_1, \ldots, M_k \in \mathbb{F}^{m \times n}$, i.e. C is the $\mathbb{F}^{m \times n}$-vector space $\langle M_1, \ldots, M_k \rangle$, and minimum distance $d(C)$, then Minimum Distance Decoding in the rank-metric can be phrased as follows.

Minimum Rank-Distance Decoding. *Given a received matrix $M_0 \in \mathbb{F}^{m \times n}$ and a basis $M_1, \ldots, M_k \in \mathbb{F}^{m \times n}$ of the code C, find $x_1, \ldots, x_k \in \mathbb{F}$ such that*

$$\operatorname{rk}\left(\sum_{\ell=1}^{k} x_\ell M_\ell - M_0\right) \leq \frac{d(C) - 1}{2}.$$

One sees immediately that Minimum Rank-Distance Decoding is an instance of the MinRank Problem in its second formulation. Therefore, estimates on the complexity of the MinRank Problem have a direct impact on understanding the complexity of decoding a general code with respect to the rank-metric and hence on complexity estimates in rank-metric code-based

cryptography. Similarly to the MinRank Problem, Minimum Rank-Distance Decoding is known to be NP-hard [43] and believed to be quantum-resistant.

Rank-metric code-based cryptography may be traced back to [58], where Gabidulin codes were used. The weakness of this proposal and of some related attempts were later exposed in [20, 55, 69, 77]. Rank-metric code-based cryptography has become relevant again in recent years, when several new cryptographic schemes based on Minimum Rank-Distance Decoding were proposed in the context of the NIST Post-Quantum Cryptography Standardization process, see [6–8, 59, 72–74]. While none of these proposals was selected, NIST expressed interest in further study of rank-based cryptosystems. In addition, two digital signatures [3,41] which base their security on Minimum Rank-Distance Decoding were submitted this year to the NIST Call for Additional Digital Signature Schemes.

In order to solve a MinRank instance one often *models* it, i.e. one writes a multivariate polynomial system whose solution returns a solution for the original MinRank instance.

Main modelings for the MinRank Problem are the Kipnis-Shamir [66] and the Minors Modeling [36, 51, 52, 54]. In the past few years, variations of the Minors Modeling such as the MaxMinors Modeling [13] and the SupportMinors Modeling [14] were introduced. Their advantage is that experimentally they appear to have significantly lower complexity compared to the classical Minors Modeling. However, their complexity is significantly less well-understood and current estimates heavily rely on heuristic assumptions.

In [33], together with Daniel Cabarcas and Elisa Gorla, we worked on making the heuristics of [14] rigorous, therefore establishing a rigorous upper bound on the complexity of MinRank.

In the following there are two main parts. First, I introduce the SupportMinors Modeling following the original description in [14, Section 3.1]. Then, I present the details of our work. Even though the MinRank Problem makes sense over any field, the relevant cases in this discussion use a finite field. Therefore, fix $\mathbb{F}_q$, the finite field of cardinality q, for the rest of the chapter.

3.1 SupportMinors Modeling

For a square matrix M, denote by $|M|$ the determinant of M. For a rectangular $m \times n$ matrix R, $n \geq m$, denote by $|R|_{*,J}$ the determinant of the submatrix of R containing all the rows of R and the columns index in $J \subseteq [n]$, $|J| = m$.

Given k matrices $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$, a target rank $r \in \mathbb{Z}_{>0}$, and the related MinRank instance, there exists a couple of matrices $(S, C) \in \mathbb{F}_q^{m \times r} \times \mathbb{F}_q^{r \times n}$ which is solution of the matrix equation

$$SC = \sum_{i=1}^{k} x_i M_i =: M_{\mathbf{x}}. \tag{3.1.1}$$

The existence of the matrices S and C is ensured by asking the rank of $M_{\mathbf{x}}$ to be smaller than r. Looking at $M_{\mathbf{x}}$ as a linear function $\overline{M} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, bounding the rank of $M_{\mathbf{x}}$ corresponds to bounding the dimension of the image of the associated function $\mathrm{Im}(\overline{M})$, which can be regarded as a vector subspace of $\mathbb{F}_q^r$. In this correspondence, C is the matrix associated to the restricted function $\mathbb{F}_q^n \to \mathrm{Im}(\overline{M}) \subseteq \mathbb{F}_q^r$, and S is an embedding of $\mathbb{F}_q^r$ into $\mathbb{F}_q^m$.

Alternatively, one can regard C as a matrix whose rows are a basis for the row space of $M_{\mathbf{x}}$. In this setting, the entries of the i-th row of S are the coordinates of the i-th row of $M_{\mathbf{x}}$ in this

basis. Then, denoting r_i be the i-th row of $M_{\mathbf{x}}$, r_i is in the row space of C. Thus the maximal minors of the matrices

$$\begin{pmatrix} r_i \\ C \end{pmatrix}, \quad i \in [m]$$

are equal to zero. SupportMinors adresses the problem of solving the MinRank instance related to $M_{\mathbf{x}}$ by solving the system

$$\left\{ \begin{vmatrix} r_i \\ C \end{vmatrix}_{*,J} : J \subseteq [n], |J| = r+1, r_i \; i\text{-th row of } M_{\mathbf{x}}, i \in [m] \right\}. \tag{3.1.2}$$

Notice that the entries of r_i are linear forms $m_{hj}(\mathbf{x}) = \sum_{\ell=1}^{k} m_{hj}^{\ell} x_\ell$, where m_{hj}^{ℓ} is the entry of M_ℓ in position (h, j). Moreover, all the entries of $C = (c_{ij})$, $i \in [m]$, $j \in [n]$, are unknowns. Notice that if $(\mathbf{x}, C)$ is a solution for (3.1.2), also $(\mathbf{x}, AC)$ is a solution for every $r \times r$ invertible matrix A. However, considering the maximal minors of C as new variables instead of directly all its entries, i.e.

$$c_T := |C|_{*,T}, \quad T \subseteq [n], |T| = r,$$

the dimension of the solution space for C while solving the system (3.1.2) becomes one.

In [14], the authors wants to solve the system, or at least find the vector $\mathbf{x}$, by direct linearization, i.e., recovering enough linear form in the x variables while performing the Gaussian elimination in the Macaulay matrix of the system (3.1.2). Thereby, the system (3.1.2) should be 'dehomogenized': as explained in [14, Section 3.3], we can suppose C be the matrix

$$\begin{pmatrix} I_r & C' \end{pmatrix}.$$

The direct linearization provides enough linear form in the x if the number of rows of the Macaulay matrix is at least the number of columns minus 1. Since each maximal minor of the system (3.1.2) can be expressed via cofactor expansion with respect to its first row, the system (3.1.2) has $m\binom{n}{r+1}$ affine bilinear equations in $k + \binom{n}{r} - 1$ variables: $x_1, \ldots, x_k$ and c_T, $T \subseteq [n], |T| = r, T \neq \{1, \ldots, r\}$. Moreover, while building the Macaulay matrix of the system (3.1.2), the columns index by the c_T variables can be discarded since they do not appear in the equations, so the number of columns of this matrix is $k\binom{n}{r}$. Then the system (3.1.2) is solvable by direct linearization whenever

$$m\binom{n}{r+1} \geq k\binom{n}{r} - 1.$$

If the previous inequality does not hold, one may skip to a 'higher degree' version of the SupportMinors Modeling, introduced in [14, Section 5.2]:

$$\left\{ \mu f : \mu = \mu(x_1, \ldots, x_k) \text{ monomial}, \deg(\mu) = b - 1, f \in (3.1.2) \right\}. \tag{3.1.3}$$

Notice that, in the case $b = 1$, the systems (3.1.2) and (3.1.3) coincide. In general, the system (3.1.3) contains $m\binom{n}{r+1}\binom{k+b-2}{b-1}$ homogeneous equations of bi-degree $(b, 1)$ respectively in the $x_1, \ldots, x_k$ and in the c_T, $T \subseteq [n], |T| = r$. However, one cannot assume that the equations are linearly independent as in the case $b = 1$. In practice, the dimension of the vector space generated by the system (3.1.3) does not eequal the number of the polynomials that it contains, as it did for $b = 1$. In order to understand the dimension of this vector space, and so when the system is effectively solvable by linearization one should compute the dimension of the space

of syzygies of the family $\{c_T : T \subseteq [n], |T| = r\}$ in the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$.

In [14, Section 5], the authors make heuristics on the number of these syzygies, and so on the expected degree b for which the system (3.1.3) is solvable by linearization. More precisely [14, Heuristic 2] predicts the dimension of the $\mathbb{F}$-vector space generated by system (3.1.3). Experimentally, this seems to be the case with overwhelming probability. The aim of our work was to provide a rigorous proof of their conjecture, or to find proven results on the investigated dimension.

Knowing the dimension of the space generated by (3.1.3) allows us to estimate the complexity of solving the system (3.1.3) at the 'right' degree b by linearization. Working over a finite field, the most efficient algorithm is the Wiedemann algorithm, whose complexity is

$$O\left(k(r+1)\left(\binom{n}{r}\binom{k+b-1}{b}\right)^2\right).$$

This 'right' degree b is the smallest integer such that the dimension of the vector space generated by the system (3.1.3) is greater than $\binom{n}{r}\binom{k+b-1}{b}$, which is the number of monomials of bi-degree $(b, 1)$.

3.2 Two special cases

In [33], we prove [14, Heuristic 2] for $b = 2$. Moreover, we compute the dimension of the vector space generated by the system (3.1.3) for $r = n - 1$ and any b. We refer to this choice of parameters as the 'sub-maximal case'. However, in this case, our result does not coincide with the estimate from [14, Heuristic 2].

The following is divided into three parts: In the first we analyze, respectively, the $b = 2$ and the sub-maximal cases for an $n \times (m + r)$ matrix of variables $\{c_{ij}, y_{hj} : i \in [r], j \in [n], h \in [m]\}$. In the second part, we specialize the variables y_{hj} to the entries of the matrix $M_{\mathbf{x}}$, that are the linear form $m_{hj}(\mathbf{x})$, recovering the system (3.1.3). In the third part we study the complexity of the SupportMinors Modeling described in the previous section. In particular, the dimension of the vector space generated by the system (3.1.3) in the cases studied is given in Theorem 86.

3.2.1 $b = 2$ and sub-maximal cases of a matrix of variables

We first analyze the system (3.1.2) where each entry of $M_{\mathbf{x}}$ is a distinct variable y_{hj}, and only later we specialize our results under $y_{hj} \mapsto m_{hj}(\mathbf{x})$. Notice that, for our purpose, we prefer using as variables the entries c_{ij} of the matrix C and not its minors c_T, then considering the polynomial ring $R = \mathbb{F}[y_{hj}, c_{ij} : h \in [m], i \in [r], j \in [n]]$.

In this setting we are working with two matrices, $C = (c_{ij})$ and $Y = (y_{hj})$, of sizes respectively $r \times n$ and $m \times n$. In addition, define the $(m + r) \times n$ matrix D as

$$D = \begin{pmatrix} Y \\ C \end{pmatrix}.$$

Let $\mathcal{F} \subseteq R$ be the set of $(r + 1)$-minors of D and let $\mathcal{G}$ be the set of $(r + 1)$-minors of D that involve the last r rows.

Let $I \subseteq [m+r]$ and $J \subseteq [n]$ be multisets with $|I| = |J|$. Throughout the chapter, I abuse notation and write that a multiset is included in $[u]$ if its underlying set is included in $[u]$. Denote by $D_{I,J}$ the submatrix of D consisting of the rows indexed by the elements of I and of the columns

indexed by the elements of J, where a row or column appears with the same multiplicity as it appears in the corresponding index multiset. Finally, let $E_{I,J}$ be the standard basis of $R^{\binom{r+m}{r+1}\binom{n}{r+1}}$, for $I \subseteq [m+r]$ and $J \subseteq [n]$ subsets with $|I| = |J| = r+1$. I often refer to the position of the only nonzero entry of $E_{I,J}$ as position (I, J).

Define the map

$$\begin{aligned} \phi : R^{\binom{r+m}{r+1}\binom{n}{r+1}} &\to R \\ E_{I,J} &\mapsto |D_{I,J}|. \end{aligned}$$

The image of the standard basis of $R^{\binom{r+m}{r+1}\binom{n}{r+1}}$ is $\mathcal{F}$ and the syzygy module of $\mathcal{F}$ is

$$\mathrm{Syz}(\mathcal{F}) = \ker(\phi).$$

Similarly, the syzygy module of $\mathcal{G}$ is

$$\mathrm{Syz}(\mathcal{G}) = \ker(\varphi),$$

where φ is the restriction of ϕ to the submodule of $R^{\binom{r+m}{r+1}\binom{n}{r+1}}$ generated by $\{E_{I,J} : I \supseteq [m+1, \ldots, m+r]\}$. This is precisely the subset of the standard basis of $R^{\binom{r+m}{r+1}\binom{n}{r+1}}$ whose elements are mapped to the elements of $\mathcal{G}$ via ϕ.

Notice that $\mathrm{Syz}(\mathcal{F}) \subseteq R^{\binom{r+m}{r+1}\binom{n}{r+1}}$ and $\mathrm{Syz}(\mathcal{G}) \subseteq R^{m\binom{n}{r+1}}$. Throughout the section $\mathrm{Syz}(\mathcal{G})$ will be identified with its natural embedding into $R^{\binom{r+m}{r+1}\binom{n}{r+1}}$, then the syzygies of $\mathcal{G}$ are the syzygies of $\mathcal{F}$ which only involve the elements of $\mathcal{G}$. For the purpose of our work, we are interested in the submodule

$$\mathbf{U} = \mathrm{Syz}(\mathcal{G}) \cap \mathbb{F}[y_{hl} : 1 \le h \le m,\ 1 \le l \le n]^{m\binom{n}{r+1}} \subseteq \mathrm{Syz}(\mathcal{G}) \subseteq \mathrm{Syz}(\mathcal{F})$$

of syzygies of $\mathcal{G}$ which only involve the y-variables.

$b = 2$ case

In this subsection the goal is finding a set of generators for $\mathbf{U}_{r+2}$. This will translate into knowing the dimension of the $\mathbb{F}$-vector space generated by the system (3.1.3) for $b = 2$.

Let $I \subseteq [m+r]$ and $J \subseteq [n]$ be ordered multisets with $|I| = |J|$. Let $1 \le i, j \le |I|$. If the i-th element of I appears more than once in I, then developing the determinant of $D_{I,J}$ with respect to the i-th row yields a syzygy of $\mathcal{F}$, denoted by $|D_{I,J}|_{i,\bullet}$. Similarly, if the j-th element of J appears more than once in J, then developing the determinant of $D_{I,J}$ with respect to the j-th column yields a syzygy of $\mathcal{F}$, denoted by $|D_{I,J}|_{\bullet,j}$. Finally, if I and J are sets, then the difference of an expansion of $|D_{I,J}|$ with respect to the i-th and the j-th row produces a syzygy of $\mathcal{F}$, which is denoted by $|D_{I,J}|_{i,\bullet} - |D_{I,J}|_{j,\bullet}$. The difference of an expansion of $|D_{I,J}|$ with respect to the i-th row and the j-th column also produces a syzygy of $\mathcal{F}$, which is denoted by $|D_{I,J}|_{i,\bullet} - |D_{I,J}|_{\bullet,j}$. Notice that, when writing $D_{I,J}$, I and J are thought as ordered multiset. However, the order only affects the determinant by a sign, hence any reordering of I and J produces an equivalent syzygy. So the ordering will be ignored throughout the section, in the hope that this does not confuse the reader.

In [68, Theorem 5.1], Kurano proved that the following elements are a system of generators of $\mathrm{Syz}(\mathcal{F})$ as an R-module.

Type I: For each $I \subseteq [m+r]$ and $J \subseteq [n]$ subsets with $|I| = r+1$, $|J| = r+2$ and for each $h \in I$, one has a syzygy $|D_{\{h\}\cup I,J}|_{1,\bullet}$, where $D_{\{h\}\cup I,J}$ is the matrix obtained from $D_{I,J}$ by adding a

copy of the h-th row as first row. Similarly, exchanging the roles of rows and columns, for each $I \subseteq [m+r]$ and $J \subseteq [n]$ subsets with $|I| = r+2$, $|J| = r+1$ and for each $k \in J$, one has a syzygy $|D_{I,\{k\}\cup J}|_{\bullet,1}$, where $D_{I,\{k\}\cup J}$ is the matrix obtained from $D_{I,J}$ by adding a copy of the k-th column as first column.

Type II: For each $I \subseteq [m+r]$ and $J \subseteq [n]$ subsets with $|I| = |J| = r+2$ and for each $h, k \in [r+2]$, one has a syzygy $|D_{I,J}|_{h,\bullet} - |D_{I,J}|_{\bullet,k}$.

Notice that all the above relations yield linear syzygies. Since the syzygies are homogeneous of degree $r+2$, then $\mathrm{Syz}(\mathcal{F})_{r+2}$ is generated as $\mathbb{F}$-vector space by the syzygies described above.

The polynomial ring R can be given a $\mathbb{Z}^{m+r} \oplus \mathbb{Z}^n$-grading 'by rows and columns' by setting $\deg(y_{hj}) = e_h + f_j \in \mathbb{Z}^{m+r} \oplus \mathbb{Z}^n$ and $\deg(c_{ij}) = e_{m+i} + f_j \in \mathbb{Z}^{m+r} \oplus \mathbb{Z}^n$, where $\{e_1, \dots, e_{m+r}\}$ is the standard basis of $\mathbb{Z}^{m+r}$ and $\{f_1, \dots, f_n\}$ that of $\mathbb{Z}^n$. The multidegree of a monomial $\mu = \prod_{i=1}^{r}\prod_{h=1}^{m}\prod_{l=1}^{n}\prod_{j=1}^{n} y_{hl}^{\alpha_{hl}} c_{ij}^{\beta_{ij}} \in R$, where $\alpha_{hl}, \beta_{ij} \in \mathbb{Z}_{\geq 0}$, is

$$\deg(\mu) = \sum_{h=1}^{m}\sum_{l=1}^{n} \alpha_{hl} e_h + \sum_{i=1}^{r}\sum_{j=1}^{n} \beta_{ij} e_{m+i} + \sum_{l=1}^{n}\sum_{h=1}^{m} \alpha_{hl} f_l + \sum_{j=1}^{n}\sum_{i=1}^{r} \beta_{ij} f_l \in \mathbb{Z}^{m+r} \oplus \mathbb{Z}^n.$$

I often use the word multigraded to mean homogenoeus with respect to the multigrading. The polynomials in $\mathcal{F}$ are multigraded. In fact, the minor that involves the rows and columns indexed by I and J has multidegree

$$\deg(|D_{I,J}|) = \sum_{i\in I} e_i + \sum_{j\in J} f_j.$$

Every minor in $\mathcal{G}$ involves the last r rows of D, hence it corresponds to an I of the form $I = \{h, m+1, \dots, m+r\}$ for some $h \in [r]$. Therefore it is homogeneous of multidegree

$$\deg(|D_{I,J}|) = e_h + \sum_{i=m+1}^{m+r} e_i + \sum_{j\in J} f_j,$$

for some $h \in [m]$ and subset $J \subseteq [n]$ with $|J| = r+1$.

One can divide Kurano's relations in four disjoint sets:

$$\begin{aligned}
\mathbf{S}_1 &= \left\{ |D_{\{h\}\cup I,J}|_{1,\bullet} : |I| = r+1, |J| = r+2, h \in I \right\}, \\
\mathbf{S}_2 &= \left\{ |D_{I,\{k\}\cup J}|_{\bullet,1} : |I| = r+2, |J| = r+1, k \in J \right\}, \\
\mathbf{S}_3 &= \left\{ |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{h,\bullet} : |I| = |J| = r+2, 2 \leq h \leq r+2 \right\}, \\
\mathbf{S}_4 &= \left\{ |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{\bullet,k} : |I| = |J| = r+2, 2 \leq k \leq r+2 \right\}.
\end{aligned}$$

Example 72. *Let $r = 1$, $m = 2$ and $n = 3$, then $\mathrm{Syz}(\mathcal{F}) \subseteq R^9$. In the following tables we computed the syzygies given by Kurano, divided respectively in the four sets just introduced. In all tables, the first column contains the parameters chosen for computing the determinantal relation and the others are index by the 2-minors $F_{I,J}$ and $G_{I,J}$, with $I, J \subseteq [3]$ and $|I| = |J| = 2$, belonging respectively to $\mathrm{Syz}(\mathcal{F}) \setminus \mathrm{Syz}(\mathcal{G})$ and to $\mathrm{Syz}(\mathcal{G})$.*

$\mathbf{S}_1 : h, I, J$	$F_{\{1,1\},\{1,2\}}$	$F_{\{1,1\},\{1,3\}}$	$F_{\{1,2\},\{2,3\}}$	$G_{\{1,3\},\{1,2\}}$	$G_{\{1,3\},\{1,3\}}$	$G_{\{1,3\},\{2,3\}}$	$G_{\{2,3\},\{1,2\}}$	$G_{\{2,3\},\{1,3\}}$	$G_{\{2,3\},\{2,3\}}$
$1,\{1,2\},\{1,2,3\}$	$y_{1,3}$	$-y_{1,2}$	$y_{1,1}$	0	0	0	0	0	0
$2,\{1,2\},\{1,2,3\}$	$y_{2,3}$	$-y_{2,2}$	$y_{2,1}$	0	0	0	0	0	0
$1,\{1,3\},\{1,2,3\}$	0	0	0	$y_{1,3}$	$y_{1,2}$	$y_{1,1}$	0	0	0
$3,\{1,3\},\{1,2,3\}$	0	0	0	$c_{1,3}$	$-c_{1,2}$	$c_{1,1}$	0	0	0
$2,\{2,3\},\{1,2,3\}$	0	0	0	0	0	0	$y_{2,3}$	$-y_{2,2}$	$y_{2,1}$
$3,\{2,3\},\{1,2,3\}$	0	0	0	0	0	0	$c_{1,3}$	$-c_{1,2}$	$c_{1,1}$

$\mathbf{S}_2 : I, k, J$	$F_{\{1,1\},\{1,2\}}$	$F_{\{1,1\},\{1,3\}}$	$F_{\{1,2\},\{2,3\}}$	$G_{\{1,3\},\{1,2\}}$	$G_{\{1,3\},\{1,3\}}$	$G_{\{1,3\},\{2,3\}}$	$G_{\{2,3\},\{1,2\}}$	$G_{\{2,3\},\{1,3\}}$	$G_{\{2,3\},\{2,3\}}$
$\{1,2,3\},1,\{1,2\}$	$c_{1,1}$	0	0	$-y_{2,1}$	0	0	$y_{1,1}$	0	0
$\{1,2,3\},2\{1,2\}$	$c_{1,2}$	0	0	$-y_{2,2}$	0	0	$y_{1,2}$	0	0
$\{1,2,3\},1,\{1,3\}$	0	$c_{1,1}$	0	0	$-y_{2,1}$	0	0	$y_{1,1}$	0
$\{1,2,3\},3,\{1,3\}$	0	$c_{1,3}$	0	0	$-y_{2,3}$	0	0	$y_{1,3}$	0
$\{1,2,3\},2,\{2,3\}$	0	0	$c_{1,2}$	0	0	$-y_{2,2}$	0	0	$y_{1,2}$
$\{1,2,3\},3,\{2,3\}$	0	0	$c_{1,3}$	0	0	$-y_{2,3}$	0	0	$y_{1,3}$

$\mathbf{S}_3 : I, J, h$	$F_{\{1,1\},\{1,2\}}$	$F_{\{1,1\},\{1,3\}}$	$F_{\{1,2\},\{2,3\}}$	$G_{\{1,3\},\{1,2\}}$	$G_{\{1,3\},\{1,3\}}$	$G_{\{1,3\},\{2,3\}}$	$G_{\{2,3\},\{1,2\}}$	$G_{\{2,3\},\{1,3\}}$	$G_{\{2,3\},\{2,3\}}$
$\{1,2,3\},\{1,2,3\},2$	0	0	0	$y_{2,3}$	$-y_{2,2}$	$y_{2,1}$	$y_{1,3}$	$-y_{1,2}$	$y_{1,1}$
$\{1,2,3\},\{1,2,3\},3$	$-c_{1,3}$	$c_{1,2}$	$-c_{1,1}$	0	0	0	$y_{1,3}$	$-y_{1,2}$	$y_{1,1}$

$\mathbf{S}_4 : I, J, k$	$F_{\{1,1\},\{1,2\}}$	$F_{\{1,1\},\{1,3\}}$	$F_{\{1,2\},\{2,3\}}$	$G_{\{1,3\},\{1,2\}}$	$G_{\{1,3\},\{1,3\}}$	$G_{\{1,3\},\{2,3\}}$	$G_{\{2,3\},\{1,2\}}$	$G_{\{2,3\},\{1,3\}}$	$G_{\{2,3\},\{2,3\}}$
$\{1,2,3\},\{1,2,3\},2$	0	$c_{1,2}$	0	0	$-y_{2,2}$	0	$y_{1,3}$	0	$y_{1,1}$
$\{1,2,3\},\{1,2,3\},3$	$-c_{1,3}$	0	0	$y_{2,3}$	0	0	0	$-y_{1,2}$	$y_{1,1}$

Notice that $\mathbf{S}_3 \cup \mathbf{S}_4$ is smaller than the set of Type II relations, however it is an easy exercise to check that every Type II relation is a linear combination of elements of $\mathbf{S}_3 \cup \mathbf{S}_4$. The $\mathbf{S}_4$-type relation corresponding to $k = 1$, in particular, is a sum with alternating signs of all the elements of $\mathbf{S}_3 \cup \mathbf{S}_4$. Therefore, the set

$$\mathbf{S} = \mathbf{S}_1 \cup \mathbf{S}_2 \cup \mathbf{S}_3 \cup \mathbf{S}_4$$

generates $\mathrm{Syz}(\mathcal{F})$. Notice moreover that all the elements of $\mathbf{S}$ are multigraded. Using the notation introduced above, the multidegree of an element of $\mathbf{S}_1$ is

$$\deg(|D_{\{h\}\cup I,J}|_{1,\bullet}) = e_h + \sum_{i\in I} e_i + \sum_{j\in J} f_j,$$

the multidegree of an elements of $\mathbf{S}_2$ is

$$\deg(|D_{I,\{k\}\cup J}|_{\bullet,1}) = \sum_{i\in I} e_i + f_k + \sum_{j\in J} f_j,$$

and that of an element of $\mathbf{S}_3 \cup \mathbf{S}_4$ is

$$\deg(|D_{I,J}|_{1,\bullet} - |D_{I,J}|_{h,\bullet}) = \deg(|D_{I,J}|_{1,\bullet} - |D_{I,J}|_{\bullet,k}) = \sum_{i\in I} e_i + \sum_{j\in J} f_j.$$

Since the multidegrees of the elements of $\mathbf{S}_1 \cup \mathbf{S}_2$ are pairwise distinct, then the elements of $\mathbf{S}_1 \cup \mathbf{S}_2$ are $\mathbb{F}$-linearly independent. For the same reason, the elements of $\mathbf{S}_1 \cup \mathbf{S}_2$ are linearly independent from those of $\mathbf{S}_3 \cup \mathbf{S}_4$.

In the next theorem a system of generators for $\mathbf{U}_{r+2}$ is produced.

Theorem 73. *A set of generators for* $\mathbf{U}_{r+2}$ *is given by* $\mathbf{S}' := \mathbf{S}'_1 \cup \mathbf{S}'_3$, *where*

$$\mathbf{S}'_1 = \left\{ |D_{\{h\}\cup I,J}|_{1,\bullet} : |I| = r+1, |J| = r+2, I \cap [m] = \{h\} \right\},$$
$$\mathbf{S}'_3 = \left\{ |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{2,\bullet} : |I| = |J| = r+2, |I \cap [m]| = 2 \right\},$$

where $I \subseteq [m+r]$ *and* $J \subseteq [n]$ *are subsets.*

Proof. It is easy to check that $\mathbf{S}'_1 \cup \mathbf{S}'_3 \subseteq \mathbf{U}_{r+2}$. Then the only fact to be proven is that every element of $\mathbf{U}_{r+2}$ can be written as a linear combination of the elements of $\mathbf{S}'_1 \cup \mathbf{S}'_3$.

Let $T \in \mathbf{U}_{r+2}$. Since $\mathbf{U}$ is multigraded, by considering each homogeneous component one may assume without loss of generality that T is multigraded. Since $T \in \mathrm{Syz}(\mathcal{G})_{r+2}$, then T is an element of $\mathrm{Syz}(\mathcal{F})_{r+2}$ which belongs to the submodule generated by $E_{H,K}$ with $H \supseteq \{m+1, \dots, m+r\}$, i.e., an element whose multidegree is bigger than $\sum_{i=m+1}^{m+r} e_i + \sum_{j\in K} f_j$ for some subset $K \subseteq [n]$ of $|K| = r$. In other words

$$\deg(T) = e_h + \sum_{i=m+1}^{m+r} e_i + e_{i^*} + \sum_{j\in J} f_j + f_{j^*},$$

for some $h \in [m]$, $i^* \in [m+r]$, $J \subseteq [n]$, $|J| = r+1$, and $j^* \in [n]$. Since in addition $T \in \mathbf{U}$, then its entries only involve the variables $y_{i,j}$. This forces $i^* \in [m]$.

Since $T \in \mathbf{U}_{r+2} \subseteq \mathrm{Syz}(\mathcal{F})_{r+2}$, T can be written as linear combination of elements in $\mathbf{S}$. By comparing the degree of T with those of the elements of $\mathbf{S}$, one sees that either $T \in \mathbf{S}_1$ or $T \in \langle \mathbf{S}_3 \cup \mathbf{S}_4 \rangle$. In the first case, by inspecting the multidegree one sees that $i^* = h$. This yields the set $\mathbf{S}'_1$ consisting of the elements of $\mathbf{S}_1$ with $I = \{h, m+1, \dots, m+r\}$. In the second case, by inspecting the multidegree one sees that $I = \{h, m+1, \dots, m+r\}$, $h \in [m]$, $i^* \in [m] \setminus \{h\}$, and $j^* \notin J$.

Consider therefore $T \in \langle \mathbf{S}_3 \cup \mathbf{S}_4 \rangle$ of multidegree $\sum_{i\in I} e_i + \sum_{j\in J} e_j$ for some fixed subsets $\{m+1, \dots, m+r\} \subseteq I \subseteq [m+r]$ and $J \subseteq [n]$ of $|I| = |J| = r+2$. For ease of notation, denote by $S_{h,\bullet} = |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{h,\bullet} \in \mathbf{S}_3$ and $S_{\bullet,k} = |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{\bullet,k} \in \mathbf{S}_4$. Write

$$T = \sum_{h=2}^{r+2} \alpha_h S_{h,\bullet} + \sum_{k=2}^{r+2} \beta_k S_{\bullet,k} \tag{3.2.4}$$

for some $\alpha_h, \beta_k \in \mathbb{K}$. The element $S_{\bullet,k}$ has an entry $c_{r,k}$ in position $I \setminus \{m+r\}, J \setminus \{k\}$ and no other element appearing in the sum (3.2.4) has a nonzero entry in the same position. For $3 \le h \le r+2$, the element $S_{h,\bullet}$ has an entry $c_{h-2,1}$ in position $I \setminus \{m+h-2\}, J \setminus \{1\}$ and no other element in the sum (3.2.4) has a nonzero entry in the same position. Since T does not involve the variables $c_{i,j}$, this proves that $\beta_k = 0$ for $2 \le k \le r+2$ and $\alpha_h = 0$ for $3 \le h \le r+2$. This yields the set $\mathbf{S}'_3$. □

Example 74. *Consider the parameters of Example 72. For this choice, the sets* $\mathbf{S}'_1$ *and* $\mathbf{S}'_3$ *are the subsets of* $\mathbf{S}_1$ *and* $\mathbf{S}_3$ *reported in the following two tables.*

$\mathbf{S}'_1 : h, I, J$	$F_{\{1,1\},\{1,2\}}$	$F_{\{1,1\},\{1,3\}}$	$F_{\{1,2\},\{2,3\}}$	$G_{\{1,3\},\{1,2\}}$	$G_{\{1,3\},\{1,3\}}$	$G_{\{1,3\},\{2,3\}}$	$G_{\{2,3\},\{1,2\}}$	$G_{\{2,3\},\{1,3\}}$	$G_{\{2,3\},\{2,3\}}$
$1, \{1,3\}, \{1,2,3\}$	0	0	0	$y_{1,3}$	$y_{1,2}$	$y_{1,1}$	0	0	0
$2, \{2,3\}, \{1,2,3\}$	0	0	0	0	0	0	$y_{2,3}$	$-y_{2,2}$	$y_{2,1}$

$\mathbf{S}'_3 : I, J, h$	$F_{\{1,1\},\{1,2\}}$	$F_{\{1,1\},\{1,3\}}$	$F_{\{1,2\},\{2,3\}}$	$G_{\{1,3\},\{1,2\}}$	$G_{\{1,3\},\{1,3\}}$	$G_{\{1,3\},\{2,3\}}$	$G_{\{2,3\},\{1,2\}}$	$G_{\{2,3\},\{1,3\}}$	$G_{\{2,3\},\{2,3\}}$
$\{1,2,3\}, \{1,2,3\}, 2$	0	0	0	$y_{2,3}$	$-y_{2,2}$	$y_{2,1}$	$y_{1,3}$	$-y_{1,2}$	$y_{1,1}$

Sub-maximal case

Using the notation set at the beginning of the section, the final goal is counting the relations in $\mathbf{U}$ for $r = n-1$ and any b. The approach used it is completely different with respect to the one of the case $b = 2$. In particular, in this subsection we give a graded free resolution of $\mathrm{Syz}(\mathcal{G})$ for $r = n-1$, from which one can extract the homogeneous component corresponding to $\mathbf{U}$. For the sub-maximal case, the matrix of variable considered is the $n \times (m+r)$ matrix $D^* = \left(Y|C\right)$ with $r = n-1$. In this case the $(r+1)$-minors are maximal. Our result is built on [2] by Andrade and Simis. In their paper, the authors give a free resolution of the module generated by the maximal minors of a $n \times \ell$ matrix fixing $n-1$ columns. The free resolution presented in the next theorem is a modification of the Buchsbaum-Rim complex 28.

Theorem 75. *[2, Theorem] Let $f : F \to G$ be a map of free modules, with $\mathrm{rank}(F) = \ell \geq \mathrm{rank}(G) = n$. Let there be given a decomposition $F = F' \oplus F''$ into free modules, with $\mathrm{rank}(F') = n-1$. Set $f' : F' \to G$ for the restriction map. Then the following conditions are equivalent.*

(i) $\mathrm{grade}(I_n)(f) \geq \ell - n + 1$ *and* $\mathrm{grade}(I_{n-1}(f')) \geq 2$.

(ii) The complex

$$0 \to \bigwedge^{\ell} F \otimes S_{\ell-n-1}(G^*) \xrightarrow{d_{\ell-n+1}} \cdots \xrightarrow{d_3} \bigwedge^{n+1} F \otimes S_0(G^*) \to F'' \xrightarrow{\varphi} \mathrm{Im}(f)/\mathrm{Im}(f') \to 0 \quad (3.2.5)$$

is exact and $\mathrm{Im}(f)/\mathrm{Im}(f') \cong (\bigwedge^n f)(F'')$ (where F'' sits naturally inside $\bigwedge^n F = \bigwedge^n (F' \oplus F'') = \bigoplus_{i=0}^{n} (\bigwedge^i F' \otimes \bigwedge^{n-1} F'')$ as $\bigwedge^{n-1} F' \otimes \bigwedge^1 F''$).

The definition of grade of an ideal is quite technical. However, in our case the ideal $I_n(f)$ and $I_{n-1}(f')$ are ideals of minors of matrices of variables, whose grade is well-known, see e.g. [29, Theorem 2.5].

Thanks to the identification of F'' with $\bigwedge^{n-1} F' \otimes \bigwedge^1 F''$, $(\bigwedge^n f)(F'') \subseteq R$ is the R-module, i.e. the ideal of R, generated by the maximal minors fixing the $n-1$ columns corresponding to F' of the matrix representing f. In the following example I highlight this fact using the map f of Example 27.

Example 76. *Recall that $R = \mathbb{F}[x, y, z]$, $F = R^4$, and $G = R^3$ with bases respectively $\{e_1, e_2, e_3, e_4\}$, $\{f_1, f_2, f_3\}$. The map $f : R^4 \to R^3$ is represented by the matrix*

$$M = \begin{pmatrix} x & 0 & 0 & yz \\ 0 & y & 0 & x \\ 0 & 0 & z & y^2 \end{pmatrix}.$$

Set $F' = \langle e_3, e_4 \rangle$, $F'' = \langle e_1, e_2 \rangle$, then the columns corresponding to F' are the last two. Thanks to the isomorphisms

$$F'' \cong \bigwedge^2 F' \otimes \bigwedge^1 F'' \cong \langle e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4 \rangle \subseteq \bigwedge^3 R^4,$$

it follows that $\bigwedge^3 f(F'') = \langle x^2 z, y^2 z^2 \rangle \subseteq R$, that is precisely the ideal generated by the 3-minors of M fixing the last two columns.

The image of an element e_i of a basis of F'' via the map φ is the maximal minor of the matrix representing $f : F \to G$ involving all the $n-1$ columns corresponding to F' and the i-th column among the ones corresponding to F''.

From now on, let $f : R^{m+r} \to R^n$ be the function represented by D^*. The polynomial ring R can be given a $\mathbb{Z}^2$-grading by setting $\deg(y_{hj}) = (1,0) \in \mathbb{Z}^2$ and $\deg(c_{ij}) = (0,1) \in \mathbb{Z}^2$.

Lemma 77. *Let $F = R(-(1,0))^m \oplus R(-(0,1))^{n-1}$ be a graded free R-module with decomposition $F' \oplus F''$, where $F' = R(-(0,1))^{n-1}$ and $F'' = R(-(1,0))^m$, and let $G = R^n$. Then*

$$(\bigwedge^n f)(F'') = (\mathcal{G}),$$

and the complex

$$0 \quad \to \quad \bigwedge^{m+n-1} F \otimes S_{m-2}(G^*) \quad \xrightarrow{d_{m-2}} \quad \cdots \quad \xrightarrow{d_3} \quad \bigwedge^{n+1} F \otimes S_0(G^*) \tag{3.2.6}$$

is a graded free resolution of the R-module $\mathrm{Syz}(\mathcal{G}(0, n-1))$.

Proof. The fact that $(\bigwedge^n f)(F'') = (\mathcal{G})$ has been already explained. Now, notice that the choice of F and G makes the function f homogeneous. Moreover, in the complex (3.2.5) all the maps d_i are homogeneous. In order to make the function $\varphi : R(-(1,0))^m \to (\mathcal{G})$ homogeneous, one needs to consider the shifted ideal $(\mathcal{G})(0, n-1)$ instead of $(\mathcal{G})$.

$\mathrm{grade}(I_n(f)) = m - n + 1$ and $\mathrm{grade}(I_{n-1}(f')) = 2$ by [29, Theorem 2.5]. Then, applying Theorem 75, one obtains that the complex

$$0 \quad \to \quad \bigwedge^{m+n-1} F \otimes S_{m-2}(G^*) \quad \xrightarrow{d_{m-2}} \quad \cdots \quad \xrightarrow{d_3} \quad \bigwedge^{n+1} F \otimes S_0(G^*) \quad \to \quad F'' \tag{3.2.7}$$

is a graded free resolution of the shifted ideal $(\mathcal{G})(0, n-1)$ with augmentation map φ.

Combining Remark 21 and the definition given at the beginning of Section 3.2, the module $\ker(\varphi)$ is the syzygy module $\mathrm{Syz}((\mathcal{G})(0, n-1))$. Then, since the complex (3.2.10) is exact, one obtains the thesis. □

3.2.2 From Y to $M_{\mathbf{x}}$

In this subsection we discuss the case when the entries of $M_{\mathbf{x}}$ are linear forms in $x_1, \ldots, x_k$. Let $P = \mathbb{K}[x_\ell, c_{ij} : \ell \in [k], i \in [r], j \in [n]]$ and consider the R-algebra homomorphism $\rho : R \to P$ given by $c_{ij} \mapsto c_{ij}$ and $y_{hj} \mapsto m_{hj}(\mathbf{x})$, where $m_{hj}(\mathbf{x})$ are the entries of the matrix $M_{\mathbf{x}}$. Abusing notation, ρ denotes also the homomorphism $R^t \to P^t$, $t \in \mathbb{N}$, that acts as ρ componentwise. 'Specializing' will often be used as a synonym for computing the image of an object via ρ.

Remember that the goal is to compute the dimension of the vector space generated by the system (3.1.3). In other words, we are interested in the syzygies of the $(r+1)$-minors of the matrix

$$\rho(D) = \begin{pmatrix} M_{\mathbf{x}} \\ C \end{pmatrix}$$

which involve the last r rows, that is, the syzygies of $\rho(\mathcal{G})$. In particular, we want to compute the module of syzygies of $\rho(\mathcal{G})$ that only involve the x-variables. Since ρ is a homomorphism,

specializing the elements of $\mathbf{U}$ yields syzygies of $\rho(\mathcal{G})$ in the x-variables. In other words,

$$\rho(\mathbf{U}) \subseteq \operatorname{Syz}(\rho(\mathcal{G})) \cap \mathbb{K}[x_1, \dots, x_k] \subseteq P^{\binom{r+m}{r+1}\binom{n}{r+1}}.$$

The case $b = 2$

In the following, we argue that there exists a subset of the coefficients of the linear forms m_{hj} that is dense in the Zariski topology, for which $\rho(\mathbf{S}')$ generates $\operatorname{Syz}(\rho(\mathcal{G})) \cap \mathbb{K}[x_1, \dots, x_k]$. Before that, we prove a preliminary lemma on the supports of the syzygies before specialization. I follow the notation of the previous subsections. For brevity, we say that $S \in \mathcal{F}$ is supported on $\mathcal{H}$ to mean that S is supported on the positions corresponding to $\mathcal{H}$, for $\mathcal{H} \subseteq \mathcal{F}$.

Lemma 78. *Each $S \in \mathbf{S}$ falls into one of these mutually exclusive cases:*

i) S is supported on the positions corresponding to $\mathcal{G}$.

ii) S is supported on the positions corresponding to $\mathcal{F} \setminus \mathcal{G}$.

iii) S does not fall into case i) or ii) and it involves a variable c_{ij} in a position that corresponds to an element of $\mathcal{F} \setminus \mathcal{G}$.

Proof. Let $S \in \mathbf{S} = \mathbf{S}_1 \cup \mathbf{S}_2 \cup \mathbf{S}_3 \cup \mathbf{S}_4$. If $S \in \mathbf{S}_1$, then $S = \left|D_{\{h\}\cup I,J}\right|_{1,\bullet}$ where $I \subseteq [m+r]$, $J \subseteq [n]$ are subsets, $|I| = r+1$, $|J| = r+2$, and $h \in I$. In particular, $|I \cap [m]| \geq 1$. If $|I \cap [m]| > 1$, then S is supported on $\mathcal{F} \setminus \mathcal{G}$ and it falls in case ii). If $|I \cap [m]| = 1$, then S is supported on $\mathcal{G}$ and it falls in case i).

If $S \in \mathbf{S}_2$, then $S = \left|D_{I,\{k\}\cup J}\right|_{\bullet,1}$ where $I \subseteq [m+r]$, $J \subseteq [n]$ are subsets, $|I| = r+2$, $|J| = r+1$, and $k \in J$. Notice that $|I \cap [m]| \geq 2$. If $|I \cap [m]| > 2$, then S is supported on $\mathcal{F} \setminus \mathcal{G}$ and it falls in case ii). If $|I \cap [m]| = 2$, then S is the sum with alternating signs over $i \in I$ of $d_{ik}E_{I\setminus\{i\},J}$. Since $r \geq 1$, then $|I| \geq 3$, so there exists $i^* \in I \setminus [m]$. Let $\iota = \min(I)$. Then $E_{I\setminus\{\iota\},J}$ is supported on $\mathcal{G}$ and $d_{\iota k} = y_{\iota k}$. Moreover, $E_{I\setminus\{i^*\},J}$ is supported on $\mathcal{F} \setminus \mathcal{G}$ and $d_{i^*k} = c_{i^*-mk}$, so S falls in case iii).

If $S \in \mathbf{S}_3$, then $S = \left|D_{I,J}\right|_{1,\bullet} - \left|D_{I,J}\right|_{h,\bullet}$ where $I \subseteq [m+r]$, $J \subseteq [n]$ are subsets, $|I| = |J| = r+2$, and $2 \leq h \leq r+2$. Notice that $|I \cap [m]| \geq 2$. If $|I \cap [m]| > 2$, then S is supported on $\mathcal{F} \setminus \mathcal{G}$ and it falls in case ii). If $|I \cap [m]| = 2$ and $h = 2$, then S is supported on $\mathcal{G}$ and it falls in case i). If $|I \cap [m]| = 2$ and $h > 2$, then

$$S = \sum_{j\in J}(-1)^j d_{i_1 j}E_{I\setminus\{i_1\},J\setminus\{j\}} - \sum_{j\in J}(-1)^{j+h} d_{i_h j}E_{I\setminus\{i_h\},J\setminus\{j\}},$$

where $I = \{i_1, \dots, i_{r+2}\}$ with $i_1 < \cdots < i_{r+2}$. Notice that $E_{I\setminus\{i_1\},J\setminus\{j\}}$ is supported on $\mathcal{G}$ and $d_{i_1 j} = y_{i_1 j}$ for all $j \in J$. Moreover, $E_{I\setminus\{i_h\},J\setminus\{j\}}$ is supported on $\mathcal{F} \setminus \mathcal{G}$ and $d_{i_h j} = c_{i_h - mj}$ for all $j \in J$, so S falls in case iii).

If $S \in \mathbf{S}_4$, then $S = \left|D_{I,J}\right|_{1,\bullet} - \left|D_{I,J}\right|_{\bullet,k}$ where $I \subseteq [m+r]$, $J \subseteq [n]$ are subsets, $|I| = |J| = r+2$, and $k \in [r+2]$. Notice that $|I \cap [m]| \geq 2$. If $|I \cap [m]| > 2$, then S is supported on $\mathcal{F} \setminus \mathcal{G}$ and it falls in case ii). If $|I \cap [m]| = 2$, then

$$S = \sum_{t=1}^{r+2}(-1)^{t+1} d_{i_1 j_t}E_{I\setminus\{i_1\},J\setminus\{j_t\}} - \sum_{s=1}^{r+2}(-1)^{s+k} d_{i_s j_k}E_{I\setminus\{i_s\},J\setminus\{j_k\}},$$

where $I = \{i_1, \dots, i_{r+2}\}$ with $i_1 < \cdots < i_{r+2}$ and $J = \{j_1, \dots, j_{r+2}\}$ with $j_1 < j_2 < \cdots < j_{r+2}$. For $s > 2$, $E_{I\setminus\{i_s\},J\setminus\{j_k\}}$ is supported on $\mathcal{F} \setminus \mathcal{G}$ and $d_{i_s j_k} = c_{i_s - m, j_k}$. Moreover, $E_{I\setminus\{i_1\},J\setminus\{j_t\}}$ is supported on

$\mathcal{G}$ and has coefficient $d_{i_1 j_t} = y_{i_1 j_t}$ in the expression of T, provided that $t \neq k$ ($E_{I\setminus\{i_1\},J\setminus\{j_k\}}$ cancels in the expression of T, since it appears twice with the same coefficient $y_{i_1 j_k}$ and opposite signs). Hence S falls in case iii). □

In the next theorem we prove that every syzygy of $\mathcal{F}$ which specializes to a nonzero syzygy of $\rho(\mathcal{G})$ is in fact a syzygy of $\mathcal{G}$.

Theorem 79. *Let $P = \mathbb{K}[x_\ell, c_{ij} : \ell \in [k], i \in [r], j \in [n]]$ be an R-algebra with homomorphism $\rho : R \to P$ given by $c_{ij} \mapsto c_{ij}$ and $y_{hj} \mapsto m_{hj}$. Let $T \in \mathrm{Syz}(\mathcal{F})$. If $\rho(T) \in \mathrm{Syz}(\rho(\mathcal{G})) \setminus \{0\}$, then $T \in \mathrm{Syz}(\mathcal{G})$.*

Proof. Let $\mathbf{T}_1$ be the set of elements of $\mathbf{S}$ that fall into case i) of Lemma 78, let $\mathbf{T}_2$ be the set of those that fall into case ii), and let $\mathbf{T}_3$ be the set of those that fall into case iii). By Lemma 78, $\mathbf{S} = \mathbf{T}_1 \cup \mathbf{T}_2 \cup \mathbf{T}_3$. Let $T \in \mathrm{Syz}(\mathcal{F})$ and suppose that $\rho(T) \in \mathrm{Syz}(\rho(\mathcal{G}))$. Since $\mathbf{S}$ generates $\mathrm{Syz}(\mathcal{F})$, by Lemma 78 we can write

$$T = \sum_{S\in\mathbf{T}_1} \alpha_S S + \sum_{S\in\mathbf{T}_2} \alpha_S S + \sum_{S\in\mathbf{T}_3} \alpha_S S. \tag{3.2.8}$$

Up to replacing T by $T - \sum_{S\in\mathbf{T}_1} \alpha_S S$, we may assume that $\alpha_S = 0$ for every $S \in \mathbf{T}_1$. In particular,

$$\rho(T) = \sum_{S\in\mathbf{T}_2} \alpha_S \rho(S) + \sum_{S\in\mathbf{T}_3} \alpha_S \rho(S). \tag{3.2.9}$$

The thesis corresponds to proving that $T = 0$. In fact, this implies that for any $T \in \mathrm{Syz}(\mathcal{F})$ for which $\rho(T) \in \mathrm{Syz}(\rho(\mathcal{G}))$, one has $T \in \langle \mathbf{T}_1 \rangle = \mathrm{Syz}(\mathcal{G})_{r+2}$.

The first matter is how the support changes when passing from T to $\rho(T)$. Since $\rho(c_{ij}) = c_{ij}$ for all i and j, if one entry of T involves a c-variable with a nonzero coefficient, then the corresponding entry of $\rho(T)$ involves the same c-variable with the same coefficient. In particular, when looking at the c-variables, the supports of T and $\rho(T)$ coincide. Since $\rho(T) \in \mathrm{Syz}(\mathcal{G})$, the positions of T corresponding to elements of $\mathcal{F} \setminus \mathcal{G}$ cannot involve any c variable.

A coefficient c_{ij} in position (I, J) can only come from an element of $\mathbf{T}_2$ or $\mathbf{T}_3$ corresponding to the multisets $I \cup \{i\}$ and $J \cup \{j\}$. Therefore, if $c_{ij}E_{I,J}$ comes from a syzygy $\rho(S)$ and cancels in (3.2.8), then it cancels with a summand $c_{ij}E_{I,J}$ coming from a different syzygy $\rho(S')$ which corresponds to the same multisets $I \cup \{i\}$ and $J \cup \{j\}$. Therefore, one may restrict to $D_{I\cup\{i\},J\cup\{j\}}$ and only discuss which cancellations occur in (3.2.8) for syzygies that originate from it.

Let $S \in \mathbf{T}_3$ and let I, J be the multisets from which S originates. Then $I \subseteq [m + r]$, $J \subseteq [n]$, $|I| = |J| = r + 2$ and one of the following must hold:

1. I is a set with $|I \cap [m]| = 2$, J contains one element k with multiplicity two and every other element has multiplicity one, and $S \in \mathbf{S}_2$.
2. I and J are sets of cardinality $r + 2$, $|I \cap [m]| = 2$, and $S \in \mathbf{S}_3$ with $h > 2$.
3. I and J are sets of cardinality $r + 2$, $|I \cap [m]| = 2$, and $S \in \mathbf{S}_4$ with $k > 1$.

In case 1., there exists exactly one syzygy $\Sigma \in \mathbf{T}_3$ that originates from those I and J. Write $I = \{i_1, \ldots, i_{r+2}\}$ with $i_1 < \ldots < i_{r+2}$, $J = \{k, j_1, \ldots, j_{r+1}\}$ with $j_1 < \ldots < j_{r+1}$ and $k \in \{j_1, \ldots, j_{r+1}\}$. We have $\alpha_\Sigma = 0$, since otherwise the element $\alpha_\Sigma c_{i_3 k} E_{I\setminus\{i_3\},\{j_1,\ldots,j_{r+1}\}}$ does not cancel in (3.2.8), as there is exactly one syzygy in $\mathbf{T}_3$ where $c_{i_3 k}$ appears in position $I \setminus \{i_3\}, \{j_1, \ldots, j_{r+1}\}$.

In cases 2. and 3., assume for ease of notation that $I = \{1, 2, m+1, \dots, m+r\}$ and $J = [r+2]$. Because of what it is discussed above, when studying cancellations among the c-variables, one may restrict their attention to the syzygies that originate from the I and J that had been just fixed. For $h > 2$, $c_{h-2,1}E_{I\setminus\{m+h-2\},\{2,\dots,r+2\}}$ only appears in syzygies obtained from developing the determinant of $D_{I,J}$ with respect to row h or column 1. Since $k > 1$, the only syzygy that it appears in is $\Sigma_h = |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{h,\bullet}$. Therefore no cancelation is possible and $\alpha_{\Sigma_h} = 0$ for $h > 2$. For a fixed $2 \leq k \leq r+2$, $c_{1,k}E_{I\setminus\{m+1\},J\setminus\{k\}}$ only appears in syzygies obtained from developing the determinant of $D_{I,J}$ with respect to row 3 or column k. Since $\alpha_{\Sigma_3} = 0$, the only syzygy in which it appears is $\Theta_k = |D_{I,J}|_{1,\bullet} - |D_{I,J}|_{\bullet,k}$. Again, no cancelation is possible, showing that $\alpha_{\Theta_k} = 0$ for $k > 1$.

This proves that, if $\rho(T) \in \mathrm{Syz}(\mathcal{G})$, then there is an expression of T as in (3.2.8) that does not involve any element of $\mathbf{T}_3$. Since the support of $\rho(S)$ is disjoint from $\mathcal{G}$ for every $S \in \mathbf{T}_2$, then by (3.2.9) we deduce that $\rho(T) \in \mathrm{Syz}(\mathcal{G})$ forces $T = 0$. □

The next theorem is one of the two main results of this chapter. It shows that, for k sufficiently large and for a generic choice of $M_1, \dots, M_k$, the linear syzygies of $\rho(\mathcal{G})$ which only involve the x-variables are generated by the specializations of the linear syzygies of $\mathcal{G}$ which only involve the y-variables.

Theorem 80. *For $k \geq m(n-r)$ and generic $M_1, \dots, M_k$, the set $\rho(\mathbf{S}')$ generates $\mathrm{Syz}(\rho(\mathcal{G}))_{r+2} \cap \mathbb{K}[x_1, \dots, x_k]$ as a $\mathbb{K}$-vector space.*

Proof. For $k \geq m(n-r)$ and generic $M_1, \dots, M_k$, one has that $\mathrm{grade}(\rho(\mathcal{F})) = \mathrm{grade}((\mathcal{F}))$. Since the ideal $(\mathcal{F}) \subseteq R$ is a perfect R-module, see e.g. [27, Theorem 3.4.9], a minimal free R-resolution of $(\mathcal{F})$ specializes to a minimal free P-resolution of $(\rho(\mathcal{F}))$ by [29, Theorem 3.5] (as tensoring with P over R corresponds to specializing via ρ). In particular,

$$\mathrm{Syz}(\rho(\mathcal{F})) = \rho(\mathrm{Syz}(\mathcal{F})).$$

Since ρ is a homomorphism, then $\rho(\mathrm{Syz}(\mathcal{G})) \subseteq \mathrm{Syz}(\rho(\mathcal{G}))$. Conversely, let $S \in \mathrm{Syz}(\rho(\mathcal{G})) \subseteq \mathrm{Syz}(\rho(\mathcal{F})) = \rho(\mathrm{Syz}(\mathcal{F}))$, $S \neq 0$. Then there is $T \in \mathrm{Syz}(\mathcal{F})$ such that $\rho(T) = S \in \mathrm{Syz}(\rho(\mathcal{G}))$. By Theorem 79, $T \in \mathrm{Syz}(\mathcal{G})$. This proves that

$$\rho(\mathrm{Syz}(\mathcal{G})) = \mathrm{Syz}(\rho(\mathcal{G})).$$

Finally, let $0 \neq S \in \mathrm{Syz}(\rho(\mathcal{G}))_{r+2} \cap \mathbb{K}[x_1, \dots, x_k]^{m\binom{n}{r+1}}$ and let $T \in \mathrm{Syz}(\mathcal{G})$ be such that $\rho(T) = S$. Since ρ is the identity on the c-variables and maps the y-variables into linear forms in the x-variables and $S \in \mathbb{K}[x_1, \dots, x_k]^{m\binom{n}{r+1}}$, then $T \in \mathbb{K}[y_{kl} : k \in [m], l \in [n]]^{m\binom{n}{r+1}}$. Therefore $T \in \mathrm{Syz}(\mathcal{G}) \cap \mathbb{K}[y_{kl} : k \in [m], l \in [n]]^{m\binom{n}{r+1}} = \mathbf{U}$. This proves that

$$\mathrm{Syz}(\rho(\mathcal{G}))_{r+2} \cap \mathbb{K}[x_1, \dots, x_k]^{m\binom{n}{r+1}} = \rho(\mathbf{U})_{r+2} = \langle \rho(\mathbf{S}') \rangle,$$

where the last equality follows from Theorem 73. □

The sub-maximal case

In the following, we prove that there exists a Zariski-open subset of the coefficients of the linear forms m_{h_j} for which the specialized free graded resolution of $\mathrm{Syz}((\mathcal{G}(0, n-1)))$ given in Theorem 77 is a graded free resolution of $\mathrm{Syz}(\rho((\mathcal{G})(0, n-1)))$.

Let $S = \mathbb{F}[y_{hj}, c_{ij}, x_\ell : h \in [m], j \in [n], i \in [n-1], \ell \in [k]]$ and $P = \mathbb{F}[c_{ij}, x_\ell : h \in [m], j \in [n], i \in [n-1], \ell \in [k]]$ with a $\mathbb{Z}^2$-grading defined by setting $\deg(y_{hj}) = \deg(x_\ell) = (1,0) \in \mathbb{Z}^2$ and $\deg(c_{ij}) = (0,1) \in \mathbb{Z}^2$.

Remark 81. *Denote by $C_\bullet$ the graded complex which solves the ideal $(\mathcal{G})(0, n-1)$. With the notation introduced in Lemma 77, $C_\bullet$ is the complex*

$$0 \to \bigwedge^{m+n-1} F \otimes S_{m-2}(G^*) \xrightarrow{d_{m-2}} \cdots \xrightarrow{d_3} \bigwedge^{n+1} F \otimes S_0(G^*) \to F''. \quad (3.2.10)$$

Let C_0 be the module $F'' = R(-(1,0))^m$ and C_i the module $\bigwedge^{n+i} F \otimes S_{i-1}(G^*)$, for $i \in [m-1]$. Reasoning as in Example 26 with weighted bases for both F and G, one finds that

$$C_i = \bigoplus_{j=0}^{n+i} R(-j, j-n-i)^{\binom{m}{j}\binom{n-1}{n+i-j}\binom{n}{i-1}}.$$

Notation 82. *$C_\bullet^{(P)}$ is the complex whose modules are*

$$C_0^{(P)} = P(-(1,0))^m \text{ and } C_i^{(P)} = \bigoplus_{j=0}^{n+i} P(-j, j-n-i)^{\beta_{i,(-j,j-n-i)}},$$

where $\beta_{i,(-j,j-n-i)} = \binom{m}{j}\binom{n-1}{n+i-j}\binom{n}{i-1}$, for $i \in [m-1]$.

Proposition 83. *For $k \geq m + 1 - (n-1)n$ and generic $M_1, \ldots, M_k$, the complex $C_\bullet^{(P)}$ is a free graded resolution of the ideal $\rho((\mathcal{G}))(0, n-1) \subseteq P$.*

Proof. If $k \geq m + 1 - (n-1)n$, then it holds that

$$\operatorname{depth}(S/(\mathcal{G})S) \geq mn,$$

where $(\mathcal{G})S$ is the ideal generated by $\mathcal{G}$ in the ring S. In fact, thanks to the Cohen-Macaulyness of polynomial ring [28, Corollary 2.1.4] and the Auslander-Buchsbaum Formula [28, Theorem 1.3.3], one has that

$$\operatorname{depth}(S/(\mathcal{G})S) = \operatorname{depth}(R/(\mathcal{G})) + k = \dim(R) - \operatorname{projdim}(R/(\mathcal{G})).$$

Moreover, the dimension of R is equal to the number of variables, which is $(n-1)n + mn$. Since $C_\bullet$ is a free resolution of $(\mathcal{G})$ of length m, the projective dimension of the ring $R/(\mathcal{G})$ is at least $m+1$. Therefore, for generic $M_1, \ldots, M_k$ one can suppose that $S/(\mathcal{G})S$ contains a regular sequence of the form $\{y_{hj} - m_{hj}(\mathbf{x}) : h \in [m], j \in [n]\}$. Call L the ideal $(y_{hj} - m_{hj}(\mathbf{x}) : h \in [m], j \in [n]) \subseteq S$. Then, using [28, Proposition 1.1.5], one obtains that the complex

$$C_\bullet \otimes_S S/L \to (\mathcal{G})(0, n-1) \otimes_S S/L \to 0$$

is graded and exact.

Notice that $(S/L)^u \cong P^u$ for every $u \in \mathbb{Z}_{\geq 0}$ via the S-algebra homomorphism $\rho' : S \to P$ given by $c_{ij} \mapsto c_{ij}$, $x_k \mapsto x_k$, and $y_{hj} \mapsto m_{hj}(\mathbf{x})$. The homomorphism ρ' is homogeneous with respect

to the $\mathbb{Z}^2$-grading, thus the shifting are respected. Thereby, again using the homomorphism ρ', one obtains that

$$(\mathcal{G})(0,n-1)\otimes_S S/L = (\mathcal{G})S(0,n-1)+L/L \cong \rho((\mathcal{G})(0,n-1)).$$

Now the thesis follow from the fact that, since ρ is homogeneous, it holds that

$$\rho((\mathcal{G})(0,n-1)) = \rho((\mathcal{G}))(0,n-1).$$

□

Remark 84. *As in Lemma 77, thanks to Proposition 83, the complex*

$$(C_{m-1}^{(P)})^{\beta_{m-1,(-j,j-n-i)}} \to \cdots \to (C_1^{(P)})^{\beta_{1,(-j,j-n-i)}} \tag{3.2.11}$$

is a free graded resolution of the module $\mathrm{Syz}(\rho(\mathcal{G})(0,n-1))$.

Finally, in the next theorem, we compute the number of relations in the system (3.1.3), that is the dimension as $\mathbb{F}$-vector space of the component $\rho(\mathbf{U})_{n-1+b}$ with respect to the standard grading.

Theorem 85. *For $k \geq m+1-(n-1)n$, generic $M_1,\dots,M_k$, and any $b>0$, the dimension of the $\mathbb{F}_q$-vector space $\rho(\mathbf{U})_{n-1+b}$ is*

$$\sum_{i=1}^{\min\{m-n,n+1,b-n\}} (-1)^{i-1}\binom{m}{n+i}\binom{n}{i-1}\binom{k+b-n-i-1}{k-1}. \tag{3.2.12}$$

Proof. First notice that the vector space $\mathbf{U}_{n-1+b}$ is the component of degree $(b,0)$ of the module $\mathrm{Syz}(\rho((\mathcal{G}))(0,n-1))$. Since the complex (3.2.11) is exact also the complex

$$(C_{m-1}^{(P)})^{\beta_{m-1,(-j,j-n-i)}}_{(b,0)} \to \cdots \to (C_1^{(P)})^{\beta_{1,(-j,j-n-i)}}_{(b,0)} \to \mathrm{Syz}(\rho((\mathcal{G}))(0,n-1))_{(b,0)} \to 0$$

is exact. The dimension of the modules involved is the following:

$$\begin{aligned}\dim_{\mathbb{F}_q}((C_i^{(P)})_{(b,0)}) &= \sum_{j=0}^{n+i}\beta_{i,(-j,j-n-i)}\dim_{\mathbb{F}_q}P_{(b-j,j-n-i)}\\ &= \beta_{i,(-n-1,0)}\binom{k+b-n-i-1}{k-1}\\ &= \binom{m}{n+i}\binom{n}{i-1}\binom{k+b-n-i-1}{k-1},\end{aligned}$$

where the second equality comes from the fact that $\dim_{\mathbb{F}_q}P_{(b-j,j-n-i)}\neq 0$ if and only if $j\geq n+i$, then the only case to be considered in the sum is $j=n+i$. Thereby, the dimension of the $\mathbb{F}_q$-vector space $\mathrm{Syz}(\rho((\mathcal{G}))(0,n-1)))_{(b,0)}$ is

$$\sum_{i=1}^{\min\{m-n,n+1,b-n\}} (-1)^{i-1}\binom{m}{n+i}\binom{n}{i-1}\binom{k+b-n-i-1}{k-1}, \tag{3.2.13}$$

since the three binomials are different from zero if and only, respectively, $i \leq m-n$, $i \leq n+1$, and $i \leq b-n$. □

3.2.3 Complexity estimates and conclusions

In this section we study the complexity of the SupportMinors Algorithm described in Section 3.1. The algorithm entails solving a system of polynomial equations in $x_1, \ldots, x_k$ and new variables $c_T = |C|_{*,T}$ for $T \subseteq [n]$ of cardinality r. The variables c_T are the Plücker coordinates of the matrix C, i.e., C_T corresponds to the maximal minor of C of columns indexed by T. Let Q be the corresponding polynomial ring, i.e., $Q = \mathbb{F}_q[x_1, \ldots, x_k, c_T \mid T \subseteq [n], |T| = r]$. In this context, one needs to estimate the rank of the Macaulay matrix considered in the SupportMinors Algorithm, or equivalently, the dimension of the module generated by the elements of $\rho(\mathcal{G})$ over $\mathbb{F}_q[x_1, \ldots, x_k]$ for a given degree b in $x_1, \ldots, x_k$ and degree one in the Plücker coordinates. The results contained in the previous sections allow us to make the estimates of [14, Sections 5.2 and 5.3] rigorous for $b = 1, 2$, where b is the degree in $x_1, \ldots, x_k$ of the equations that we consider. In the sequel, for brevity we say that b is the degree in x of the equations that we consider. Moreover, they allow us also to provide dimension of the space generated by system (3.1.3) for $r = n-1$ and any b. This result, however, does not agree with the estimates of [14, Sections 5.2 and 5.3].

Throughout this section, saying that the entries of $M_{\mathbf{x}}$ are generic, depending on whether we are considering the case $b = 2$ or the sub-maximal one, it means that the coefficients of the entries of $M_{\mathbf{x}}$ belong to the Zariski-dense open sets considered in Subsection 3.2.2 and in Subsection 3.2.2.

Theorem 86. *Consider the SupportMinors Algorithm and assume that the entries of $M_{\mathbf{x}}$ are generic. Let b denote the degree in x of the equations that we consider. Then the number of linearly independent equations available for linearization for $b = 1, 2$ is as predicted in [14, Sections 5.2 and 5.3], namely it is*

$$\min\left\{m\binom{n}{r+1}, k\binom{n}{r}\right\}$$

for $b = 1$. For $b = 2$ assume that $m\binom{n}{r+1} \leq k\binom{n}{r}$. Then the number of linearly independent equations available for linearization is

$$\min\left\{km\binom{n}{r+1} - \binom{m+1}{2}\binom{n}{r+2}, \binom{k+1}{2}\binom{n}{r}\right\}.$$

Let

$$t_b = \sum_{i=1}^{\min\{m-n, n+1, b-n\}} (-1)^{i-1}\binom{m}{n+i}\binom{n}{i-1}\binom{k+b-n-i-1}{k-1}.$$

For $r = n-1$ and any b, assume that $t_{b-1} \leq n\binom{k+b-2}{b-1}$. Then the number of linearly independent equations available for linearization is

$$\min\left\{m\binom{k+b-2}{b-1} - t_b, n\binom{k+b-1}{b}\right\}.$$

Proof. The first formula in the statement follows from observing that the cardinality of $\rho(\mathcal{G})$ is

$m\binom{n}{r+1}$ and the number of Plücker coordinates of C is $\binom{n}{r}$, hence $\dim_{\mathbb{F}_q}(Q_{(1,1)}) = k\binom{n}{r}$.

To prove the second formula, we need to estimate the dimension in bi-degree $(2,1)$ of the vector space generated by $\rho(\mathcal{G})\mathbb{F}_q[x_1,\ldots,x_k]_1$. Notice that, since the Plücker relations are homogeneous quadratic relations, we may treat the Plücker coordinates as independent variables. For a generic $M_{\mathbf{x}}$, the elements of $\rho(\mathcal{G})$ are linearly independent provided that $m\binom{n}{r+1} \leq k\binom{n}{r}$. In such a situation,

$$\dim_{\mathbb{F}_q}(\langle\rho(\mathcal{G})\rangle) = |\rho(\mathcal{G})| = m\binom{n}{r+1}.$$

Since $\dim_{\mathbb{F}_q}(\mathbb{F}_q[x_1,\ldots,x_k]_1) = k$, then the dimension of the vector space generated by $\rho(\mathcal{G})\mathbb{F}_q[x_1,\ldots,x_k]_1 \subseteq Q_{(2,1)}$ is the minimum between the dimension of $Q_{(2,1)}$ and

$$km\binom{n}{r+1} - \dim(\mathrm{Syz}(\rho(\mathcal{G}))_{r+2} \cap \mathbb{F}[x_1,\ldots,x_k]).$$

The thesis now follows since $\dim(Q_{(2,1)}) = \binom{k+1}{2}\binom{n}{r}$ and

$$\dim(\mathrm{Syz}(\rho(\mathcal{G})) \cap \mathbb{F}[x_1,\ldots,x_k]_{r+2}) = \binom{m+1}{2}\binom{n}{r+2}$$

by Theorem 80.

To prove the last formula, we need to estimate the dimension in bi-degree $(b,1)$ of the vector space generated by $\rho(\mathcal{G})\mathbb{F}_q[x_1,\ldots,x_k]_{b-1}$.
Since $\dim_{\mathbb{F}_q}(\mathbb{F}_q[x_1,\ldots,x_k]_{b-1}) = \binom{k+b-2}{b-1}$, then the dimension of the vector space generated by $\rho(\mathcal{G})\mathbb{F}_q[x_1,\ldots,x_k]_{b-1} \subseteq Q_{(b,1)}$ is the minimum between the dimension of $Q_{(b,1)}$ and

$$m\binom{n}{r+1}\binom{k+b-2}{b-1} - \dim_{\mathbb{F}_q}(\mathrm{Syz}(\rho(\mathcal{G}))_{b+n-1} \cap \mathbb{F}[x_1,\ldots,x_k]).$$

The thesis now follows since $\dim_{\mathbb{F}_q}(Q_{(b,1)}) = n\binom{k+b-1}{b}$ and

$$\dim_{\mathbb{F}_q}(\mathrm{Syz}(\rho(\mathcal{G})) \cap \mathbb{F}[x_1,\ldots,x_k]_{b+n-1}) = t_b$$

by Theorem 85.

□

Corollary 87. *Assume that the entries of $M_{\mathbf{x}}$ are generic and let b denote the degree in x of the equations that we consider. Then the SupportMinors Algorithm outputs a solution to MinRank in degree $b = 1$ provided that*

$$m\binom{n}{r+1} \geq k\binom{n}{r} - 1.$$

If the SupportMinors Algorithm does not output a solution to MinRank in degree $b = 1$, then it outputs one in degree $b = 2$ provided that

$$km\binom{n}{r+1} - \binom{m+1}{2}\binom{n}{r+2} \geq \binom{k+1}{2}\binom{n}{r} - 1.$$

Name

$$t_b = \sum_{i=1}^{\min\{m-n,n+1,b-n\}} (-1)^{i-1} \binom{m}{n+i} \binom{n}{i-1} \binom{k+b-n-i-1}{k-1}.$$

For $r = n - 1$, if the SupportMinors Algorithm does not output a solution to MinRank in degree $b - 1$, then it outputs one in degree b provided that

$$m\binom{k+b-2}{b-1} - t_b \geq n\binom{k+b-1}{b} - 1.$$

Notice that the case $b = 2$ is of high interest, as this is the relevant degree in the attacks to ROLLO-I-256 and many instances of GeMSS, see [14, Sections 6.1 and 6.2]. Moreover, notice that if $b \leq n$, the number t_b is equal to 0. This means that, in the sub-maximal case, the equations of the system (3.1.3) are linearly independent if $b \leq n$.

Bibliography

[1] G. Adj, L. Rivera-Zamarripa, J. Verbel, E. Bellini, S. Barbero, A. Esser, C. Sanna, and F. Zweydinger. MiRitH (MinRank in the Head). 2023.

[2] J. Andrade and A. Simis. A complex that resolves the ideal of minors having n-1 columns in common. *Proceedings of the American Mathematical Society*, 81(2):217–219, 1981.

[3] N. Aragon, M. Bardet, L. Bidoux, J.-J. Chi-Domínguez, V. Dyseryn, T. Feneuil, P. Gaborit, A. Joux, M. Rivain, J.-P. Tillich, and A. Vinçotte. RYDE specifications. 2023.

[4] N. Aragon, L. Bidoux, J.-J. Chi-Domínguez, T. Feneuil, P. Gaborit, R. Neveu, and M. Rivain. MIRA: a Digital Signature Scheme based on the MinRank problem and the MPC-in-the-Head paradigm. *arXiv preprint arXiv:2307.08575*, 2023.

[5] N. Aragon, L. Bidoux, J.-J. Chi-Domínguez, T. Feneuil, P. Gaborit, R. Neveu, and M. Rivain. MIRA: a Digital Signature Scheme based on the MinRank problem and the MPC-in-the-Head paradigm. *arXiv preprint: arXiv:2307.08575*, 2023.

[6] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor. LAKE-Low rAnk parity check codes Key Exchange. 2017.

[7] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor. LOCKER-LOw rank parity ChecK codes EncRyption. 2017.

[8] N. Aragon, O. Blazy, P. Gaborit, A. Hauteville, and G. Zémor. Durandal: a rank metric based signature scheme. In *Advances in Cryptology - EUROCRYPT 2019*, pages 728–758. Springer, 2019.

[9] M. Atiyah and I. MacDonald. *Introduction To Commutative Algebra*. Avalon Publishing, 1994.

[10] J. Baena, P. Briaud, D. Cabarcas, R. Perlner, D. Smith-Tone, and J. Verbel. Improving support-minors rank attacks: applications to GeMSS and Rainbow. In *Annual International Cryptology Conference*, pages 376–405. Springer, 2022.

[11] J. Baena, P. Briaud, D. Cabarcas, R. Perlner, D. Smith-Tone, and J. Verbel. Improving support-minors rank attacks: applications to GeMSS and Rainbow. In *Advances in Cryptology - CRYPTO 2022*, pages 376–405. Springer, 2022.

[12] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Pierre et Marie Curie-Paris VI, 2004.

[13] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J.-P. Tillich. An algebraic attack on rank metric code-based cryptosystems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 64–93. Springer, 2020.

[14] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich, and J. Verbel. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In *Proceedings of Advances in Cryptology–ASIACRYPT 2020*, pages 507–536. Springer, 2020.

[15] M. Bardet, J.-C. Faugere, and B. Salvy. Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over $\mathbb{F}$_2 with solutions in $\mathbb{F}$_2. 2003.

[16] M. Bardet, J. C. Faugère, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[17] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the F5 Gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015.

[18] M. Bardet, J.-C. Faugere, B. Salvy, and B.-Y. Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proceedings of MEGA*, volume 5, 2005.

[19] E. Bellini, A. Esser, C. Sanna, and J. Verbel. MR-DSS – Smaller MinRank-based (Ring-)Signatures. In *International Conference on Post-Quantum Cryptography*, pages 144–169. Springer, 2022.

[20] T. Berger and P. Loidreau. Designing an efficient and secure public-key cryptosystem based on reducible rank codes. In *Progress in Cryptology - INDOCRYPT 2004*, pages 218–229. Springer, 2005.

[21] L. Bettale, J.-C. Faugere, and L. Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69:1–52, 2013.

[22] W. Beullens. Improved cryptanalysis of UOV and Rainbow. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 348–373. Springer, 2021.

[23] W. Beullens. Breaking Rainbow takes a weekend on a laptop. In *Annual International Cryptology Conference*, pages 464–479. Springer, 2022.

[24] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou. Semi-regular sequences and other random systems of equations. In *Women in Numbers Europe III: Research Directions in Number Theory*, pages 75–114. Springer, 2021.

[25] N. Bourbaki. *Algebra I: Chapters 1-3*. Springer Berlin, Heidelberg, 1989.

[26] P. Briaud, J.-P. Tillich, and J. Verbel. A polynomial time key-recovery attack on the Sidon cryptosystem. In *Selected Areas in Cryptography - 28th International Conference SAC 2021*, pages 419–438. Springer, 2021.

[27] W. Bruns, A. Conca, C. Raicu, and M. Varbaro. *Determinants, Gröbner bases and cohomology*, volume 24. Springer, 2022.

[28] W. Bruns and H. J. Herzog. *Cohen-Macaulay rings*. Number 39. Cambridge university press, 1998.

[29] W. Bruns and U. Vetter. *Determinantal rings*, volume 1327. Springer, 1988.

[30] B. Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3-4):475–511, 2006.

[31] J. A. Buchmann, J. Ding, M. S. E. Mohamed, and W. S. A. E. Mohamed. MutantXL: Solving multivariate polynomial equations for cryptanalysis. In *Dagstuhl seminar proceedings*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2009.

[32] J. F. Buss, G. S. Frandsen, and J. O. Shallit. The Computational Complexity of Some Problems of Linear Algebra. In *BRICS Report Series RS-96-33*, pages 1–39. 1996.

[33] D. Cabarcas, G. Gaggero, and E. Gorla. SupportMinors modeling. *Draft*, 2024.

[34] D. Cabarcas, D. Smith-Tone, and J. A. Verbel. Key recovery attack for ZHFE. In *Post-Quantum Cryptography*, pages 289–308. Springer, 2017.

[35] A. Caminata and E. Gorla. Solving multivariate polynomial systems and an invariant from commutative algebra. In *Arithmetic of Finite Fields: 8th International Workshop, WAIFI 2020*, pages 3–36. Springer, 2021.

[36] A. Caminata and E. Gorla. The complexity of MinRank. In *Women in Numbers Europe III: Research Directions in Number Theory*, pages 163–169. Springer, 2021.

[37] M. Campagna, C. Costello, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, D. Urbanik, et al. Supersingular isogeny key encapsulation, 2019.

[38] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. GeMSS: a great multivariate short signature. 2017.

[39] G. Caviglia and A. De Stefani. Linearly presented modules and bounds on the Castelnuovo-Mumford regularity of ideals. *Proceedings of the American Mathematical Society*, 150(4):1397–1404, 2022.

[40] G. Caviglia, A. De Stefani, and E. Sbarra. The Eisenbud-Green-Harris Conjecture. In *Commutative Algebra: Expository Papers Dedicated to David Eisenbud on the Occasion of his 75th Birthday*, pages 159–187. Springer, 2021.

[41] T. Chou, R. Niederhagen, E. Persichetti, T. H. Randrianarisoa, K. Reijnders, S. Samardjiska, and M. Trimoska. Take your meds: Digital signatures from matrix code equivalence. In *International Conference on Cryptology in Africa*, pages 28–52. Springer, 2023.

[42] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.

[43] N. T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 402–421. Springer, 2001.

[44] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. 4th Edition*. Springer, 2015.

[45] J. Ding, R. Perlner, A. Petzoldt, and D. Smith-Tone. Improved cryptanalysis of HFEv^- via projection. In *Post-Quantum Cryptography*, pages 375–395. Springer, 2018.

[46] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268, 2018.

[47] D. Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 1994.

[48] D. Eisenbud, M. Green, and J. Harris. Higher Castelnuovo theory. *Journées de Géométrie Algébrique d'Orsay*, (218):187–202, 1993.

[49] J.-C. Faugere. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[50] J. C. Faugere. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.

[51] J.-C. Faugere, M. S. El Din, and P.-J. Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 257–264, 2010.

[52] J.-C. Faugère, M. S. El Din, and P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. *Journal of Symbolic Computation*, 55:30–58, 2013.

[53] J.-C. Faugere, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[54] J.-C. Faugere, F. Levy-dit Vehel, and L. Perret. Cryptanalysis of MinRank. In *Proceedings of the 28th Annual conference on Cryptology: Advances in Cryptology*, pages 280–296. Springer, 2008.

[55] C. Faure and P. Loidreau. A new public-key cryptosystem based on the problem of reconstructing p-Polynomials. In *International workshop on coding and cryptography*, pages 304–315. Springer, 2005.

[56] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptography - CRYPTO'86*, pages 186–194. Springer, 1986.

[57] R. Fröberg. An inequality for Hilbert series of graded algebras. *Mathematica Scandinavica*, 56(2):117–144, 1985.

[58] E. M. Gabidulin, A. Paramonov, and O. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Advances in Cryptology—EUROCRYPT'91*, pages 482–489. Springer, 1991.

[59] P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. RankSign: an efficient signature algorithm based on the rank metric. In *PQCrypto 2014*, pages 88–107. Springer, 2014.

[60] G. Gaggero and E. Gorla. The complexity of solving a random polynomial system. *arXiv preprint arXiv:2309.03855*, 2023.

[61] L. Goubin and N. T. Courtois. Cryptanalysis of the TTM cryptosystem. In *Advances in Cryptology - ASIACRYPT 2000*, pages 44–57. Springer, 2000.

[62] M. Hellman. New directions in cryptography. volume 22, pages 644–654. 1976.

[63] T. J. Hodges, S. D. Molina, and J. Schlather. On the existence of semi-regular sequences. *Journal of Algebra*, 476:519–547, 2017.

[64] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In *International algorithmic number theory symposium*, pages 267–288. Springer, 1998.

[65] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer, 1999.

[66] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Annual International Cryptology Conference*, pages 19–30. Springer, 1999.

[67] M. Kreuzer and L. Robbiano. *Computational commutative algebra*, volume 1. Springer, 2000.

[68] K. Kurano. The first syzygies of determinantal ideals. *Journal of Algebra*, 124(2):414–436, 1989.

[69] P. Loidreau. Designing a rank metric based McEliece cryptosystem. In *PQCrypto 2010*, pages 142–152. Springer, 2010.

[70] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25–27, 1988 Proceedings 7*, pages 419–453. Springer, 1988.

[71] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. volume 42-44, pages 114–116, 1978.

[72] C. A. Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, and J.-C. Deneuville. ROLLO-Rank-Ouroboros, LAKE & LOCKER. 2019.

[73] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, G. Zémor, and I. Bourges. Ouroboros-R. *NIST Submission*, 2017.

[74] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, and G. Zémor. Rank quasi-cyclic (RQC). 2017.

[75] D. Moody, R. Perlner, and D. Smith-Tone. An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In *Post-Quantum Cryptography*, pages 180–196. Springer, 2014.

[76] D. Moody, R. Perlner, and D. Smith-Tone. Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme. In *Post-Quantum Cryptography*, pages 255–271. Springer, 2017.

[77] R. Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of cryptology*, 21(2):280–301, 2008.

[78] K. Pardue. Generic sequences of polynomials. *Journal of Algebra*, 324(4):579–590, 2010.

[79] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *Advances in Cryptology—CRYPT0'95: 15th Annual International Cryptology Conference Santa Barbara, California, USA, August 27–31, 1995 Proceedings 15*, pages 248–261. Springer, 1995.

[80] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer, 1996.

[81] N. Raviv, B. Langton, and I. Tamo. Multivariate public key cryptosystem from sidon spaces. In *Public-Key Cryptography - PKC 2021*, pages 242–265. Springer, 2021.

[82] F. Salizzoni. An upper bound for the solving degree in terms of the degree of regularity. *arXiv preprint arXiv:2304.13485*, 2023.

[83] F. Salizzoni. An upper bound for the solving degree in terms of the degree of regularity. *arXiv preprint arXiv:2304.13485*, 2023.

[84] I. Semaev and A. Tenti. Probabilistic analysis on macaulay matrices over finite fields and complexity of constructing gröbner bases. *Journal of Algebra*, 565:651–674, 2021.

[85] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[86] D. R. Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.

[87] C. Tao, A. Petzoldt, and J. Ding. Efficient key recovery for all HFE signature variants. In *Advances in Cryptology - CRYPTO 2021*, pages 70–93. Springer, 2021.

[88] A. Tenti. Sufficiently overdetermined random polynomial systems behave like semiregular ones. 2019.

[89] J. Vates and D. Smith-Tone. Key recovery attack for all parameters of HFE$^-$. In *Post-quantum cryptography*, pages 272–288. Springer, 2017.