Admissible Parameters for the Crossbred Algorithm and Semi-regular Sequences over Finite Fields

John Baena[1], Daniel Cabarcas[1], Sharwan K. Tiwari[2], Javier Verbel[2], and Luis Villota[1]

[1] Universidad Nacional de Colombia sede Medellín, Medellín, Colombia
{jbbaena,dcabarc,ldvillotav}@unal.edu.co
[2] Technology Innovation Institute, UAE
{sharwan.tiwari,javier.verbel}@tii.ae

Abstract. Multivariate public key cryptography (MPKC) is one of the most promising alternatives to build quantum-resistant signature schemes, as evidenced in NIST's call for additional post-quantum signature schemes. The main assumption in MPKC is the hardness of the Multivariate Quadratic (MQ) problem, which seeks for a common root to a system of quadratic polynomials over a finite field. Although the Crossbred algorithm is among the most efficient algorithm to solve MQ over small fields, its complexity analysis stands on shaky ground. In particular, it is not clear for what parameters it works and under what assumptions. In this work, we provide a rigorous analysis of the Crossbred algorithm over any finite field. We provide a complete explanation of the series of admissible parameters proposed in previous literature and explicitly state the regularity assumptions required for its validity. Moreover, we show that the series does not tell the whole story, hence we propose an additional condition for Crossbred to work. Additionally, we define and characterize a notion of regularity for systems over a small field, which is one of the main building blocks in the series of admissible parameters.

Keywords: Admissible parameters · Crossbred · Semi-regular · MQ Problem · Post-quantum · Cryptography

1 Introduction

The Multivariate Quadratic (MQ) problem lies at the heart of several cryptographic constructions. In its search version, it consists in finding a common root to a system of m quadratic polynomials in n variables over a finite field of size q. Its decision version is NP-complete, it is expected to be hard on average for a wide range of parameters, and it is believed to be hard even on quantum computers. That is why, it has become specially relevant in the quest for post-quantum primitives, giving rise to an area of research called multivariate public key cryptography (MPKC), cf. [DY09]. In fact, several of the submissions to the latest

NIST Post-Quantum Standarization process, include among their assumptions the hardness of some sort of MQ problem [CSD].

In order to tune the parameters of MQ-based cryptosystems, it is important to estimate precisely the concrete hardness of the MQ problem. There are several algorithms to solve MQ with different tradeoffs depending on the parameters, the structure of the polynomials, and the computational resources available. We refer the reader to [BMSV22] for a recent survey.

In this paper, we focus our attention on a particular algorithm and on a specific scenario, that nevertheless, has a significant impact on cryptanalysis. The Crossbred algorithm [JV18] stands as one of the most efficient to solve random MQ instances over small finite fields. In theory, it is the most efficient algorithm to attack several cryptosystems, as shown by Bellini et al. in [BMSV22]. In practice, it has been used to solve some of the largest known instances, as reported in the Fukuoka MQ-challenge [YDH+15]. We concentrate on the complexity of Crossbred for random instances where the size of the field is larger than 2, but still small, say less than 2^5. Such instances are relevant for UOV, MQDSS, MAYO, and MQOM [KPG99, CHR+16, Beu22, BFR23] among other cryptosystems.

The Crossbred algorithm builds upon algebraic matrix-based methods such as F4, F5 and XL. Those methods search for a "good" representation of the ideal generated by the polynomials, on a large enough subspace, usually capped by total degree. Their complexity is thus bounded by the complexity of doing linear algebra on the so called Macaulay matrix

$$\binom{n+d}{d}^{\omega},$$

where d is a cap on the degree that guarantees the presence of the desired representation and ω is the linear algebra constant. Hybrid algorithms such as BooleanSolve [BFSS13] traverse all possible values of $n-k$ variables, checking consistency of the partially evaluated polynomials. They check the consistency using a matrix-based approach, therefore their complexity is in order of

$$q^{n-k}\binom{k+d}{d}^{\omega},$$

where d is expected to be smaller.

The Crossbred algorithm, first described by Joux and Vitse in [JV18], splits the work in a different fashion. It first finds, in the Macaulay matrix of degree D, a number of polynomials of degree less than or equal to d in the first k variables, and then it traverse all possible values of $n-k$ variables, checking consistency of the partially evaluated polynomials. The values of k, D, and d must be so that, after assigning values to the last $n-k$ variables, the resulting system can be solved at degree d. Its complexity is thus in the order of

$$\binom{n+D}{D}^{\omega} + q^{n-k}\binom{k+d}{d}^{\omega}. \tag{1}$$

The rationale behind this approach is that the initial work on the larger matrix of size $\binom{n+D}{D}$ might substantially reduce the size of the remaining q^{n-k} matrices of size $\binom{k+d}{d}$.

Despite its apparent efficiency, the complexity of the Crossbred algorithm is not well established. One important missing ingredient is a complete and formal discussion on the notion of semi-regularity for finite fields of size $q > 2$. Bardet et al. [BFSY05] precisely defines and characterize a notion of semi-regularity for sequences of polynomials over GF(2). Although other works, such as [YC04] consider similar notions for finite fields of size $q > 2$, to the best of our knowledge, there is no complete rigorous treatment of the subject.

Perhaps more crucial, it is not trivial to predict "admissible parameters", i.e, values of k, D, and d for which the Crossbred algorithm succeeds. Joux and Vitse in [JV18] did predict admissible parameters for $d = 1$, assuming the sequence of polynomials is regular or semi-regular, which is a plausible assumption for random quadratic systems, c.f. [BFSY05]. For $d \geq 1$ and GF(2), Joux and Vitse stated that k, D, and d are admissible if the coefficient of $x^D y^d$ in the series

$$\frac{(1+x)^{n-k}}{(1-x)(1-y)}\left(\frac{(1+xy)^k}{(1+x^2y^2)^m}-\frac{(1+x)^k}{(1+x^2)^m}\right)-\frac{(1+y)^k}{(1-x)(1-y)(1+y^2)^m} \tag{2}$$

is non-negative. However, they did not explain where the series come from, neither state the necessary assumptions. Other works have expanded the original complexity analysis of Crossbred. Duarte [Dua23] and Nakamura et al. [Nak23] try without success to explain the series (2). Bellini et al. [BMSV22] state a similar series for $q > 2$, but they provide no further details.

Our Contribution

We state four equivalent conditions for a sequence of polynomials over a finite field to be semi-regular. Because the notion depends on the field size, we call a sequence that satisfies these conditions q-semi-regular. This generalizes the work over GF(2) of Bardet et al. [BFSY05] and complements the work for arbitrary finite fields of Yang and Chen [YC04]. Our complete treatment of the subjects reaffirms the correctness of the notion of regularity and provides solid ground for a complexity analysis. Moreover, the sequence of vector spaces that we use to analyze the polynomial system is different from previous approaches, effectively decoupling the syzygies coming from commutativity from the syzygies coming from the Frobenious maps, as in

$$0 \to (R/S_i)_{d-2q} \xrightarrow{\times f_i^{q-1}} (R/S_{i-1})_{d-2} \xrightarrow{\times f_i} (R/S_{i-1})_d \to (R/S_i)_d \to 0,$$

where R is the underlying ring and $S_i = \langle f_1, \ldots, f_i \rangle$. We believe that this approach simplifies and illuminates the proofs and makes it easier to extend to other cases.

We then provide a rigorous analysis of admissible parameters for Crossbred. We identify two necessary conditions for Crossbred to work under regularity

assumptions. For the first condition, corresponding to Joux-Vitse's condition (2) above, we explain in detail what it guarantees and we state the necessary assumptions. Next, we explain why this condition is not sufficient, which leads to a second condition. Just as an example, in the case of GF(2), the new condition can be simply stated as

$$[y^D]\left[\frac{(1+y)^k}{(1-y)(1+y^2)^m}\right]_+ = 0,$$

where $[\cdot]_+$ denotes the truncated series from the first non-positive coefficient. Intuitively, we need this condition to hold, so that it is possible to solve the system of m equations in k variables that results after partially evaluating the last $n-k$ variables at degree D. Although, Crossbred does not explicitly construct the degree D Macaulay matrix of the partially evaluated polynomials, all the polynomials used to check the consistency correspond to vectors in its span, hence D must reach such a threshold. For this condition we also explicitly state the assumptions that allow it to operate. Finally, we provide empirical evidence that confirms that randomly chosen polynomials satisfy all the proposed assumptions with high probability. Based on this analysis and on the experimental evidence, we concluded that the two conditions predict all admissible parameters.

As a consequence of our analysis, given an instance of the MQ problem, the set of parameters for which Crossbred works is a subset of what was predicted prior to this work. This yields higher estimates of the complexity of Crossbred. In Section 6, we show evidence indicating that the changes in the complexity are relative small for cryptographically large instances. For instance, the security of the UOV signature scheme against the direct attack using Crossbred is at most four bits higher than estimated before for all its parameter sets.

Related Work

There are two lines of work that are specially relevant to our contributions, works that discuss semi-regularity for polynomials over a finite field and those that discuss the admissible parameters and complexity of the Crossbred algorithm.

The notion of semi-regular for the specific case of a sequence of polynomials over GF(2) was introduced by Bardet et al. in [BFSY05]. Their original definition is for homogeneous polynomials over the quotient ring $\mathbb{F}[x_1,\ldots,x_n]/\langle x_1^2,\ldots,x_n^2\rangle$, and they prove that their definition is equivalent to a specific Hilbert series. Some additional details are provided in [Bar04]. Our contribution is directly influenced by these works, as we generalize this notion and characterization for fields of size $q > 2$. On a more recent work, Bardet et al. use a slightly different definition for semi-regularity over GF(2). Aiming at a more precise complexity analysis of their algorithm to solve a system of polynomial equations over GF(2), they consider a homogenized version, where the ring is simply the polynomial ring $\mathbb{F}[x_1,\ldots,x_n,h]$ and the ideal includes the homogenized field equations $x_1^2 - x_1h,\ldots,x_n^2 - x_nh$. Our work does not use this definition, but our results could be easily extended in this direction.

Other works have established the Hilbert series of what we call a q-semi-regular sequence. For example, Yang and Chen [YC04, Theorem 2] implicitly establish the result as a means for a bound on the number of linearly independent XL equations. However, the assumptions necessary for the result are not explicitly stated. They seem to suggest that they are assuming that the sequence is generic, which makes no sense over a finite field, and they use without proving a form of the principle of inclusion-exclusion that is not true in general for vector spaces. Our work does not contradict their findings, but it provides a more solid ground. Moreover, their work only establishes the form of the Hilbert series, while we also establish the other implication that given such a Hilbert series, we can infer regularity. Similarly, in [YCBC07, Proposition 3.4], Yang et al. actually use the term q-semi-regular without properly defining it and citing back to [YC04]. In conclusion, it seems that the idea of q-semi-regularity and its Hilbert series has become Folklore knowledge, yet to the best of our knowledge, it has not been precisely defined or characterized.

Studies on the Crossbred algorithm's complexity and parameter selection have provided valuable insights. Joux and Vitse [JV18] introduced a bivariate series which aims to predict parameter admissibility for systems over $\mathbb{F}_2$ under some unspecified regularity assumptions. Bellini et al. [BBSV22] provided a generalized series over $\mathbb{F}_q$. Chen et al. [CHR+20] investigated the algorithm's complexity and proposed a validation condition for parameter triples (D, d, k), although it may overlook certain valid parameters. Duarte [Dua23] attempted to derive the generating series of admissible parameters for solving polynomial systems over $\mathbb{F}_q$, but his study has some inaccuracies. Nakamura [Nak23] focused on parameter selection, offering two validation formulas for parameter sets. We discuss these studies in more detail in Section 2.2.

Organization

In Section 2, we establish some notation and basic definitions. In Section 2.1, we describe the Crossbred algorithm, including a discussion about previous works on admissible parameters, and its complexity. In Section 3, we define the notion of q-semi-regular and establish four equivalent statements for it. In Section 4, we provide a rigorous analysis of the Crossbred algorithm over any finite field, including a formal definition of admissible parameters and the assumptions that allow us to precisely predict admissibility. Finally, in Section 5, we describe experimental results that test the assumptions, and in Section 6, we discuss implications to cryptography.

2 Preliminaries

Notation. Let $\mathbb{F}_q$ denote the finite field of order q. For the description of the Crossbred algorithm we will consider a polynomial ring over $\mathbb{F}_q$ in n variables partitioned into two sets $\mathbf{x} = (x_1, \ldots, x_k)$ and $\mathbf{y} = (y_1, \ldots, y_{n-k})$, which we will denote by $\mathbb{F}_q[\mathbf{x}, \mathbf{y}]$. The total degree of a polynomial $f \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ is denoted

by $\deg(f)$, and its degree in the first k variables by $\deg_k(f)$. The left-kernel of a matrix M will be denoted by $\mathsf{ker}(\mathrm{M})$, its rank by $\mathsf{rank}(\mathrm{M})$, its corank by $\mathsf{corank}(\mathrm{M})$ and its number of columns by $\mathsf{ncols}(\mathrm{M})$. The dimension of a vector space V over $\mathbb{F}_q$ will be denoted by $\mathsf{dim}(\mathrm{V})$. Given a power series $H(z)$ and a non-negative integer d, we denote by $[z^d]H(z)$ the coefficient of z^d in H, by $[H(z)]_d$ the series H truncated up to degree d, and by $[H(z)]_+$ the series H truncated at its first non-positive coefficient. In our analysis, we utilize the following two power series:

$$M_{n,q}(z) = \left(\frac{1-z^q}{1-z}\right)^n, \quad H_{n,m,q}(z) = \left(\frac{1-z^q}{1-z}\right)^n \left(\frac{1-z^2}{1-z^{2q}}\right)^m.$$

For a subset S of a ring R, we denote by $\langle S \rangle$ the ideal of R generated by S.

Definition 1 (MQ problem). *Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a sequence of quadratic polynomials in n variables $x_1, \ldots, x_n$ over a finite field $\mathbb{F}_q$. Given a vector $\mathbf{t} = (t_1, \ldots, t_m) \in \mathbb{F}_q^m$, the multivariate quadratic (MQ) problem aims to find a solution in $\mathbb{F}_q^n$ that satisfies the system of equations:*

$$f_i(x_1, \ldots, x_n) = t_i, \quad i = 1, \ldots, m. \tag{3}$$

This definition of the problem is known as the search version of MQ problem. The decisional version of the problem seeks to determine if the system (3) has a solution. The MQ problem over a finite field is known to be NP-complete [GJ90].

Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a sequence of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$, let σ be a monomial order and D a positive integer. Consider the set S of all polynomials of the form $\mathfrak{m} f_i$, where $\mathfrak{m}$ is a monomial in $\mathbb{F}_q[x_1, \ldots, x_n]$ and $\deg(\mathfrak{m} f) \leq D$. The Macaulay matrix of $\mathcal{F}$ of degree D, denoted as $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$, is a matrix whose rows are labeled by polynomials in S and whose columns are labeled by monomials in the support of S. The columns are sorted according to σ in decreasing order from left to right, and the order of the rows does not matter for our purposes. The entry of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ in the row labeled $\mathfrak{m} f_i$ and column $\mathfrak{t}$ is thus the coefficient of $\mathfrak{t}$ in the polynomial $\mathfrak{m} f_i$.

2.1 The Crossbred Algorithm

The Crossbred algorithm, introduced by Joux and Vitse in 2018 [JV18], is designed to solve the MQ problem over a finite field. It is parameterized by a triple of positive integers (D, d, k). For a given sequence $\mathcal{F}$ of m quadratic polynomials in n variables, the algorithm proceeds in two steps. In the preprocessing step, it finds a sufficient number of linearly independent polynomials within the ideal generated by $\mathcal{F}$ —ensuring that each of these polynomials satisfies the condition that every specialization of the last $n-k$ variables yields a polynomial of degree at most d in the first k variables. Then, in the linearization step, for every $\mathbf{b} \in \mathbb{F}_q^{n-k}$, the algorithm specializes $\mathbf{b}$ in each of the found polynomials and, if $d > 1$, in the original polynomials in $\mathcal{F}$. The algorithm then tries to solve the resulting k-variate specialized system by direct linearization.

In Algorithm 1 we present a slightly modified version of the Crossbred algorithm. In this version r is the maximum number of polynomials that can be obtained in the preprocessing step, while in the original version r is a parameter. Our choice simplifies the analysis of the admissible parameters, but in practice one might decide to control r for efficiency.

The pseudocode of Algorithm 1 involves two submatrices of the Macaulay matrix $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$:

- $\mathrm{Mac}^k_{D,d}(\mathcal{F})$: the row submatrix of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ whereby each row $(\mathfrak{m}, f)$ has the property $\deg_k(\mathfrak{m}) \geq d-1$.
- $\mathrm{M}^k_{D,d}(\mathcal{F})$: the column submatrix of $\mathrm{Mac}^k_{D,d}$ of columns corresponding to monomials $\mathfrak{m}$ with $\deg_k(\mathfrak{m}) > d$.

Algorithm 1 The Crossbred Algorithm

Require: A quadratic sequence in n variables $\mathcal{F} = (f_1, \ldots, f_m) \subset \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ and positive integers D, d, k

Preprocessing step:

Construct the matrices $\mathrm{Mac}^k_{D,d}(\mathcal{F})$ and $\mathrm{M}^k_{D,d}(\mathcal{F})$.
Find a basis $(\mathbf{v}_1, \ldots, \mathbf{v}_{r'})$ for the left-kernel of $\mathrm{M}^k_{D,d}(\mathcal{F})$.
Compute the set of polynomials $\mathcal{P} = \{p_1, \ldots, p_r\}$ corresponding to a basis of the vector space spanned by $\{\mathbf{v}_i \cdot \mathrm{Mac}^k_{D,d}(\mathcal{F}) : i = 1, \ldots, r'\}$.

Linearization step:

for $\mathbf{b} \in \mathbb{F}_q^{n-k}$ **do**
  $\mathcal{P}|_{\mathbf{b}} \leftarrow \big(p_1(\mathbf{x}, \mathbf{b}), \ldots, p_r(\mathbf{x}, \mathbf{b})\big)$
  $\mathcal{F}|_{\mathbf{b}} \leftarrow \big(f_1(\mathbf{x}, \mathbf{b}), \ldots, f_m(\mathbf{x}, \mathbf{b})\big)$
  $\mathrm{M}_{\mathbf{b}} \leftarrow \mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}} \cup \mathcal{P}|_{\mathbf{b}})$
  Test the consistency of the linear system $\mathrm{M}_{\mathbf{b}} \cdot (\mathbf{z}, 1)^\top = \mathbf{0}$.
  if the linear system is consistent **then**
    Find $(\mathbf{c}, 1)$ such that $\mathrm{M}_{\mathbf{b}} \cdot (\mathbf{c}, 1)^\top = \mathbf{0}$.
    Define $\mathbf{a}$ as the last k coordinates of $\mathbf{c}$.
    if $\mathcal{F}(\mathbf{a}, \mathbf{b}) = \mathbf{0}$ **then**
      return $(\mathbf{a}, \mathbf{b})$.
return $\perp$.

In the linearization step, if the linear system $\mathrm{M}_{\mathbf{b}} \cdot (\mathbf{z}, 1)^\top = \mathbf{0}$ is inconsistent, then the specialized polynomial system $\mathcal{F}|_{\mathbf{b}}$ is inconsistent. However, the converse is not true. For the Crossbred algorithm to work effectively, the parameters (D, d, k) must be chosen so that for most $\mathbf{b} \in \mathbb{F}^{n-k}$, the inconsistency of the system $\mathcal{F}|_{\mathbf{b}}$ implies the inconsistency the linear system $\mathrm{M}_{\mathbf{b}} \cdot (\mathbf{z}, 1)^\top = \mathbf{0}$. In Section 4, we propose a definition for admissible parameters aiming at this goal, and in Section 5, we report experimental results that confirm its effectiveness.

Remark 1. We highlight that when $d = 1$, $\mathrm{Mac}^k_{D,d}(\mathcal{F})$ is equal to $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$. As for any monomial u of $\deg \leq D-2$, each row of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ corresponding

to polynomials $u \cdot f_i$ satisfies $\deg_k(u) \geq d-1 = 0$, implying that all the rows are included in $\mathrm{Mac}^k_{D,d}(\mathcal{F})$. As the new polynomials p_i obtained during the preprocessing phase correspond to linear combinations $\mathbf{v}_i \cdot \mathrm{Mac}^k_{D,d}(\mathcal{F})$, after specifying the original system $\mathcal{F}$, at some $\mathbf{b} \in \mathbb{F}_q^{n-k}$, the system $\mathcal{F}|_{\mathbf{b}}$, will not contribute independent polynomials from $\mathcal{P}|_{\mathbf{b}}$ for solving the specified system. Therefore, in Step 7 of the Algorithm 1, only $\mathrm{Mac}_{\mathrm{d}}(\mathcal{P}|_{\mathbf{b}})$ is considered during the linearization phase.

2.2 Admissible Parameters

For the Crossbred algorithm to work effectively, the parameters (D, d, k) must be chosen so that it becomes feasible to verify the consistency of the system $\mathcal{F}|_{\mathbf{b}}$ through linearization at degree d. Joux and Vitse refer to such a triple (D, d, k) as admissible [JV18]. In this subsection, we present and explain previous works that have attempted to predict these admissible parameters.

It has already been observed in [JV18] that finding such a triple (D, d, k) for a given number of variables n and a number of polynomials m over $\mathbb{F}_2$ is a non-trivial task.

Joux and Vitse predict admissible parameters (D, d, k) by using the bi-variate series

$$S_{k,2}(w,z) := \frac{(1+w)^{n-k}}{(1-z)(1-w)} \left(\frac{(1+wz)^k}{(1+w^2z^2)^m} - \frac{(1+w)^k}{(1+w^2)^m} \right) - \frac{(1+z)^k}{(1-w)(1-z)(1+z^2)^m}. \quad (4)$$

More precisely, (D, d, k) are predicted admissible if $[w^D z^d] S_{k,q}(w,z) \geq 0$. Bellini et al. introduced a generalized approach for series over $\mathbb{F}_q$, which is expressed as

$$S_{k,q}(w,z) := \frac{H_{k,m,q}(wz) \cdot M_{n-k,q}(w) - H_{n,m,q}(w) - H_{k,m,q}(z)}{(1-z)(1-w)}, \quad (5)$$

where $H_{n,m,q}(z) = M_{n,q}(z) \cdot \left(\frac{1-z^2}{1-z^{2q}}\right)^m$ and $M_{n,q}(z) = \left(\frac{1-z^q}{1-z}\right)^n$ [BBSV22]. We highlight that neither work ([JV18] nor [BBSV22]) provides an explanation for the series $S_{k,q}(w,z)$ or describes the claimed regularity assumption under which the series effectively detects admissible parameters.
In [CHR+20], Chen et al. consider the the following condition

$$\dim\big(\ker\big(\mathrm{M}^k_{D,d}(\mathcal{F})\big)\big) - \dim\big(\ker\big(\mathrm{Mac}^k_{D,d}(\mathcal{F})\big)\big) \geq \sum_{i=0}^{d} \binom{k+i-1}{i}. \quad (6)$$

We believe that the mentioned condition aims to ensure the validity of the parameter triple (D, d, k) for a specific input system $\mathcal{F}$. We stress that the condition in Equation (6) does not count for the polynomials associated with $\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}})$

for some $\mathbf{b} \in \mathbb{F}_q^{n-k}$, which are not in the row-span of $\mathrm{Mac}^k_{D,d}(\mathcal{F})$. This omission may lead to potential failure in detecting some valid parameter sets.

In Duarte's study [Dua23], an attempt was made to explain and derive the generating series of admissible parameters shown in Equation (5). However, the analysis lacks rigorousness; it does not provide the necessary regularity assumptions for the series in Equation (5) to hold, and it is flawed. For instance, in Section 6, the author claims that the coefficients of the initial part of the series expressed as $\frac{(1+wz)^k(1+w)^{n-k}}{(1+w^2z^2)^m}$, "represent the formal power series of the corank of $\mathrm{M}^k_{D,d}$." This claim is proven inaccurate by the following example.

Example 1. Consider the values $n = m = 5$, $k = 4$, $D = 4$, and $d = 2$. The $\mathsf{corank}(\mathrm{M}^k_{D,d})$ is 0, while the coefficient of w^4z^2 in $\frac{(1+wz)^k(1+w)^{n-k}}{(1+w^2z^2)^m}$ is 5.

Let $\mathrm{Lac}^k_{D,d}(\mathcal{F})$ denotes the row submatrix of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ whereby each row $(\mathfrak{m}, f)$ has the property $\deg_k(\mathfrak{m}) < d-1$. Then, this series characterizes the formal power series of the corank of $\mathrm{L}^k_{D,d}$, where $\mathrm{L}^k_{D,d}$ denotes the column submatrix of $\mathrm{Lac}^k_{D,d}$ with columns corresponding to monomials $\mathfrak{m}$ having $\deg_k(\mathfrak{m}) \leq d$. Further discussion on this will be presented in Section 4.

In Nakamura's work [Nak23], the investigation focuses on parameter selection in the Crossbred algorithm, presenting two formulas to validate parameter sets. To derive the first formula, the author assumes that, in the preprocessing phase, the newly computed polynomials in $\mathcal{P}$ do not correspond to any vector in $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$, where $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$ denotes the vector space spanned by the rows of $\mathrm{Lac}^k_{D,d}(\mathcal{F})$. Let $\mathrm{V}_{\leq d,D}(\mathcal{F})$ be a vector space spanned by rows of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ whose corresponding polynomials have $\deg_k \leq d$ and $\deg \leq D$. Then, with the above assumption, the author estimates the $\mathsf{rank}(\mathcal{P})$ by the dimension of a vector space V such that

$$\mathrm{V} \oplus \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) = \mathrm{V}_{\leq d,D}(\mathcal{F}). \tag{7}$$

Using the above equation, the author mentions that the algorithm works, i.e., the parameters D, d, k are admissible if

$$\begin{aligned} \mathsf{rank}(\mathcal{P}) = \mathsf{dim}(\mathrm{V}) &= \mathsf{dim}(\mathrm{V}_{\leq d,D}(\mathcal{F})) - \mathsf{dim}(\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})) \\ &\geq \binom{k+d}{d} - \mathsf{rank}\big(\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}})\big) - 1. \end{aligned} \tag{8}$$

The author states that a parameter set is admissible if and only if the above inequality holds. Note that the author derived the above inequality (8) with the assumption that the newly computed polynomials in $\mathcal{P}$ do not belong to $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$ since from (7), $\mathrm{V} \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) = \{0\}$, but that may not hold in general, as the vector space spanned by the newly computed polynomials $\mathcal{P}$ might have a non-trivial intersection with $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$, see Figure 1. However, for practical purposes, we are interested only in those new polynomials in $\mathcal{P}$, which are independent of $\mathrm{Lac}^k_{D,d}(\mathcal{F})$. Further, to derive the second formula, the author considers a vector space V' such that

$$\mathrm{V}' \oplus \big(\mathrm{V}_{\deg_k \leq d,D}(\mathcal{F}) \cap \mathrm{V}_{\deg_k \leq d,D}(\mathcal{F}|_{\mathbf{b}})\big) = \mathrm{V}_{\deg_k \leq d,D}(\mathcal{F}),$$

where $\mathrm{V}_{\deg_k \le d,D}(\mathcal{F}|_{\mathbf{b}})$ denotes the vector space spanned by

$$(u \cdot g \mid g \in \mathcal{F}|_{\mathbf{b}}, \deg_k(u) \le d-2, \deg(u) \le D-2).$$

Here, the author calculates $\mathsf{rank}(\mathcal{P})$ by the dimension of V', indicating independence from $\mathrm{V}_{\deg_k \le d,D}(\mathcal{F}|_{\mathbf{b}})$, which contributes to the rank of $\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}})$. We treat a general scenario in the Section 4.

2.3 Complexity of the algorithm

We briefly provide below an estimate for the complexity of the Crossbred algorithm, similar to the one given in [BMSV22]. In the preprocessing phase of the algorithm, we need to find r linearly independent vectors in the kernel of the matrix $\mathrm{M}^k_{D,d}(\mathcal{F})$ that are not in the kernel of $\mathrm{Mac}^k_{D,d}(\mathcal{F})$. This can be done by finding the kernel of $\mathrm{M}^k_{D,d}(\mathcal{F})$ using Gaussian elimination on the matrix. In this case, the complexity of the preprocessing step is $\mathcal{O}(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F}))^\omega)$, where $2 \le \omega \le 3$. Alternatively, these kernel vectors can be found by repeatedly using the block Wiedemann algorithm. The complexity of finding a kernel vector with the block Wiedemann algorithm [Kal95] is given by

$$3\binom{n+2}{2} \cdot \left(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F}))\right)^2.$$

The required number of kernel vectors r can be upper bounded by $\binom{k+d}{d}$; then, the complexity of the preprocessing step is upper bounded by

$$3\binom{k+d}{d}\binom{n+2}{2} \cdot \left(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F}))\right)^2.$$

Therefore, the complexity of the preprocessing step is

$$\min\left(\mathcal{O}(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F})^\omega),\ 3\binom{k+d}{d}\binom{n+2}{2} \cdot \left(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F}))\right)^2\right).$$

The complexity of the linearization phase is upper-bounded by $\mathcal{O}(q^{n-k}\binom{k+d}{d}^\omega)$. Finally, the complexity of the Crossbred algorithm, as the number of multiplications over $\mathbb{F}_q$, is given by

$$\min\left(\mathcal{O}(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F}))^\omega),\ 3\binom{k+d}{d}\binom{n+2}{2} \cdot \left(\mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F}))\right)^2\right) + \mathcal{O}\left(q^{n-k}\binom{k+d}{d}^\omega\right).$$

3 Semi-regular Sequences over $\mathbb{F}_q$

In this section, we prove the equivalence of four statements about a sequence of polynomials over $\mathbb{F}_q$. These statements naturally generalize the notion of

semi-regularity; thus we define a sequence that satisfies them as q-semi-regular. Throughout this section we denote by R the quotient ring

$$R = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q, \ldots, x_n^q \rangle.$$

For $\bar{f} \in R$, its degree is $\deg(\bar{f}) = \min\{\deg(g) : g \in \bar{f}\}$. We will mostly omit the bar to denote elements in R for ease in notation. With this notion of degree, R is a graded ring, and we denote by R_d its degree d subgroup [3]. We first define the notions of degree of regularity and trivial syzygies in this context.

Definition 2. *The* ***degree of regularity*** *of a homogeneous ideal $I \subseteq R$, denoted as $d_{reg}(I)$, is the minimum integer d, if any, such that $\mathsf{dim}(I_d) = \mathsf{dim}(R_d)$, where $I_d = R_d \cap I$.*

Let $\mathcal{F} = (f_1, \ldots, f_m) \in R^m$ be a fixed sequence. A syzygy of $\mathcal{F}$ is an sequence $\mathbf{s} = (s_1, \ldots, s_m)$ such that $\sum_{i=1}^m s_i f_i = 0$. The set of all syzygies of $\mathcal{F}$ is an R-submodule of R^m. The degree of $\mathbf{s}$, denoted by $\deg_{\mathcal{F}}(\mathbf{s})$, is $\deg_{\mathcal{F}}(\mathbf{s}) = \max\{\deg(s_i) + \deg(f_i) : 1 \leq i \leq m\}$. Sometimes we omit the reference to $\mathcal{F}$, when it is clear from the context.

For $i \neq j \in \{1, \ldots, m\}$, commutativity induces a syzygy of the form

$$f_i e_j - f_j e_i, \tag{9}$$

where e_i is the canonical basis vector of R^m. Furthermore, the Frobenius map induced a syzygy of the form

$$f_i^{q-1} e_i. \tag{10}$$

Definition 3. *Given $\mathcal{F} = (f_1, \ldots, f_m) \in R^m$, we define the trivial syzygies of $\mathcal{F}$, denoted as $Syz_{triv}(\mathcal{F})$, to be the R-submodule generated by the syzygies of types (9) and (10).*

For the remaining of this section, let us assume that $f_1, \ldots, f_m \in R$ are homogeneous quadratic polynomials. For $i = 1, \ldots, m$, let $\mathcal{F}_i := (f_1, \ldots, f_i)$, $S_i := \langle \mathcal{F}_i \rangle$, and let $S_0 = 0$ and $\mathcal{F} = \mathcal{F}_m$. We now state and prove several lemmas that lead to the equivalence of four statements about $\mathcal{F}$.

Lemma 1. *Let $i \in \{1, \ldots, m\}$. Suppose that for all $g \in R$, $f_i g \in S_{i-1}$ and $\deg(f_i) + \deg(g) < d_{reg}(S_i)$, imply $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$. Then, for all $g \in R$, $f_i^{q-1} g \in S_{i-1}$ and $\deg(f_i^{q-1} g) < d_{reg}(S_i)$, imply $g \in S_i$.*

Proof. Suppose $g \in R$ is such that $f_i^{q-1} g \in S_{i-1}$ and $\deg(f_i^{q-1} g) < d_{reg}(S_i)$. Since the $f_i's$ are homogeneous, we may assume that g is also homogeneous.

[3] We naturally extend this notation. For any homogeneous ideal or graded ring M and any non-negative integer d, M_d denotes its degree d homogeneous component. If $d < 0$, then $M_d = 0$.

Since $f_i(f_i^{q-2}g) \in S_{i-1}$ and $\deg(f_i(f_i^{q-2}g)) < d_{reg}(S_i)$, by hypothesis, we have $f_i^{q-2}g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$. Thus,

$$f_i^{q-2}g = \sum_{k=1}^{i-1} \alpha_k f_k + \beta_1 f_i^{q-1}$$

for some α_k's and β_1 in R, equivalently

$$f_i^{q-2}(g - \beta_1 f_i) = f_i^{q-2}g - \beta_1 f_i^{q-1} = \sum_{k=1}^{i-1} \alpha_k f_k. \tag{11}$$

Since the f_i's and g are homogeneous, we may assume that the α_k's and β_1 are also homogeneous. Let us note that $f_i^{q-2}(g-\beta_1 f_i) \in S_{i-1}$. If $q = 2$, then $g \in S_i$, and we obtain the desired result.
Now, let us assume that $q > 2$. For some homogeneous α_k's and β_1 in Equation (11) we have that $f_i^{q-2}g - \beta_1 f_i^{q-1}$ is either homogeneous or zero. That is,

$$\deg(f_i f_i^{q-3}(g - \beta_1 f_i)) \leq \deg(f_i^{q-2}g) < d_{reg}(S_i).$$

So, by the hypothesis, we have

$$f_i^{q-3}(g - \beta_1 f_i) - \beta_2 f_i^{q-1} = \sum_{k=1}^{i-1} \alpha'_k f_k,$$

for some $\alpha'_k, \beta_2 \in R$. If $q = 3$, it follows that $g \in S_i$. In general, applying the hypothesis $q-1$ times, we get

$$g - \beta_1 f_i - \beta_2 f_i^2 - \cdots - \beta_{q-1} f_i^{q-1} = \sum_{k=1}^{i-1} \alpha''_k f_k,$$

and we conclude that $g \in S_i$.

Lemma 2. *Let $i \in \{1, \ldots, m\}$. For all $g \in R$, $f_i g \in S_{i-1}$ and $\deg(f_i)+\deg(g) < d_{reg}(S_i)$, imply $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$, if and only if, for all $d < d_{reg}(S_i)$, the following sequence is exact*

$$0 \to (R/S_i)_{d-2q} \xrightarrow[\chi_{d,i}]{\times f_i^{q-1}} (R/S_{i-1})_{d-2} \xrightarrow[\phi_{d,i}]{\times f_i} (R/S_{i-1})_d \xrightarrow{\pi_i} (R/S_i)_d \to 0. \tag{12}$$

Proof. Fix $i \in \{1, \ldots, m\}$. ($\Longrightarrow$) Let $d < d_{reg}(S_i)$. First, note that since π_i is the canonical map, it is clearly surjective. Next, let us show that $\chi_{d,i}$ is injective. Let $g \in R$ of degree $d-2q$ be such that $g + S_i \in \mathsf{ker}(\chi_{d,i})$. Then $g f_i^{q-1} \in S_{i-1}$ and

$$\deg(f_i^{q-1}g) \leq 2(q-1) + (d-2q) = d - 2 < d < d_{reg}(S_i),$$

so by Lemma 1, $g \in S_i$ and it follows that $g + S_i = 0$.
Now, let us show that $\mathsf{ker}(\phi_{d,i}) = \mathrm{Im}(\chi_{d,i})$. Let $g \in R$ of degree $d-2$ be such

that $g + S_{i-1} \in \ker(\phi_{d,i})$. Then $gf_i \in S_{i-1}$ and $\deg(g) + \deg(f_i) = d < d_{reg}(S_i)$, so by hypothesis $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$, hence

$$g - h_i f_i^{q-1} = \sum_{k=1}^{i-1} h_k f_k \in S_{i-1},$$

for some $h_1, \ldots, h_i \in R$. Therefore $g + S_{i-1} \in \mathrm{Im}(\chi_{d,i})$ [4]. The other inclusion follows immediately from the fact that $f_i^q = 0$.

($\Longleftarrow$) If the sequence (12) is exact, then for $d < d_{reg}(S_i)$, we have that $\ker(\phi_{d,i}) \subseteq \mathrm{Im}(\chi_{d,i})$. Let $g \in R$ be such that $f_i g \in S_{i-1}$ and $\deg(f_i) + \deg(g) < d_{reg}(S_i)$. Then with $d = \deg(g) + \deg(f_i) < d_{reg}(S_i)$ we have that $g + S_{i-1} \in \ker(\phi_{d,i}) \subseteq \mathrm{Im}(\chi_{d,i})$, so $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$.

Lemma 3. *Let $i \in \{1, \ldots, m\}$. Suppose that for all $g \in R$, $f_i g \in S_{i-1}$ and $\deg(f_i) + \deg(g) < d_{reg}(S_i)$, imply $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$. Then, every $\mathbf{s} \in Syz(\mathcal{F}_i)$ of degree less than $d_{reg}(S_i)$ belongs to $Syz_{triv}(\mathcal{F}_i)$.*

Proof. Fix $i \in \{1, \ldots, m\}$ and let $\mathbf{s} = (g_1, \ldots, g_i) \in R^i$ be a syzygy of $\mathcal{F}_i$ such that $\deg_{\mathcal{F}_i}(\mathbf{s}) < d_{reg}(S_i)$, so that

$$g_1 f_1 + g_2 f_2 + \cdots + g_i f_i = 0. \tag{13}$$

It follows that $g_i f_i \in S_{i-1}$ and

$$\deg(f_i g_i) \leq \deg(s) = \max_{1 \leq k \leq i} \big(\deg(f_k) + \deg(g_k) \big) < d_{reg}(S_i).$$

Then,

$$g_i = \sum_{k=1}^{i-1} \alpha_{i,k} f_k + \beta_i f_i^{q-1},$$

for some $\alpha_{i,k}, \beta_i \in R$. Now, multiplying by f_i, replacing in (13) and grouping like terms we obtain

$$f_1(g_1 + \alpha_{i,1} f_i) + f_2(g_2 + \alpha_{i,2} f_i) + \ldots + f_{i-1}(g_{i-1} + \alpha_{i,i-1} f_i) = 0. \tag{14}$$

We can then apply again the hypothesis to $f_{i-1}(g_{i-1} + \alpha_{i,i-1} f_i)$, noting that

$$\begin{aligned} \deg\left(f_{i-1}(g_{i-1} + \alpha_{i,i-1} f_i)\right) &\leq \max \begin{Bmatrix} \deg(f_{i-1}) + \deg(g_{i-1}), \\ \deg(\alpha_{i,i-1}) + \deg(f_i) + \deg(f_{i-1}) \end{Bmatrix} \\ &< d_{\mathrm{reg}}(S_i), \end{aligned}$$

from which we conclude that

$$g_{i-1} + \alpha_{i,i-1} f_i = \sum_{k=1}^{i-2} \alpha_{i-1,k} f_k + \beta_{i-1} f_{i-1}^{q-1},$$

[4] Note that this is also true if $d - 2q < 0$, in which case $(R/S_i)_{d-2q} = 0$ and h_i must be zero so that $g \in S_{i-1}$ and hence $\phi_{d,i}$ is injective.

Multiply f_{i-1} and replacing in (14) we get

$$\begin{aligned} f_1(g_1+\alpha_{i,1}f_i+\alpha_{i-1,1}f_{i-1})+f_2(g_2+\alpha_{i,2}f_i+\alpha_{i-1,2}f_{i-1})+\dots \\ +f_{i-2}(g_{i-2}+\alpha_{i,i-2}f_i+\alpha_{i-1,i-2}f_{i-1})= \quad 0. \end{aligned}$$

After repeating the same procedure i times, in the last step we get

$$g_1=-\sum_{k=2}^{i}\alpha_{k,1}f_k+\beta_1 f_1^{q-1},$$

and

$$f_1(g_1+\alpha_{i,1}f_i+\alpha_{i-1,1}f_{i-1}+\alpha_{i-2,1}f_{i-2}+\ldots+\alpha_{2,1}f_2)=0,$$

thus we conclude that for $1\leq j\leq i$,

$$g_j=\sum_{k=1}^{j-1}\alpha_{j,k}f_k-\sum_{k=j+1}^{i}\alpha_{k,j}f_k+\beta_j f_j^{q-1}.$$

Now, denoting by e_k the k-th canonical basis vector of R^i, we have

$$\begin{aligned} &(g_1,\dots,g_i)= \\ &\left(-\sum_{k=2}^{i}\alpha_{k,1}f_k+\beta_1 f_1^{q-1}\right)e_1+\left(\alpha_{2,1}f_1-\sum_{k=3}^{i}\alpha_{k,2}f_k+\beta_2 f_2^{q-1}\right)e_2+ \\ &\cdots+\left(\sum_{k=1}^{i-1}\alpha_{i,k}f_k+\beta_i f_i^{q-1}\right)e_i \\ &=\alpha_{2,1}(f_1e_2-f_2e_1)+\cdots+\alpha_{i,1}(f_1e_i-f_ie_1) \\ &+\alpha_{3,2}(f_2e_3-f_3e_2)+\cdots+\alpha_{i,i-1}(f_{i-1}e_i-f_ie_{i-1})+\sum_{k=1}^{i}\beta_k f_k^{q-1}e_k \\ &=\sum_{j<k\leq i}\alpha_{k,j}(f_je_k-f_ke_j)+\sum_{k=1}^{i}\beta_k f_k^{q-1}e_k. \end{aligned}$$

It follows that $(g_1,g_2,\dots,g_i)\in Syz_{triv}$.

Lemma 4. *Let $i\in\{1,\dots,m\}$. Suppose that every $\mathbf{s}\in Syz(\mathcal{F}_i)$ of degree less than $d_{reg}(S_i)$ belongs to $Syz_{triv}(\mathcal{F}_i)$. Then, for all $g\in R$, $f_ig\in S_{i-1}$ and $\deg(f_i)+\deg(g)<d_{reg}(S_i)$, imply $g\in S_{i-1}+\left\langle f_i^{q-1}\right\rangle$.*

Proof. Fix $i\in\{1,\dots,m\}$ and let $g\in R$ be such that $gf_i\in S_{i-1}$ and $\deg(g)+\deg(f_i)<d_{reg}(S_i)$. Since the f_i's are homogeneous, there exist polynomials $g_1,\dots,g_{i-1}$ of degree $\deg(g)$ such that

$$\sum_{k=1}^{i-1}g_kf_k-gf_i=0.$$

Therefore, $(g_1, \ldots, g_{i-1}, -g)$ is a syzygy of $\mathcal{F}_i$ of degree $\deg(g) + \deg(f_i) < d_{reg}(S_i)$. Then, by hypothesis, this syzygy belongs to Syz_{triv}, and there exist $\alpha_{jk}, \beta_j \in R$ such that

$$(g_1, \ldots, g_{i-1}, -g) = \sum_{j<k\leq i} \alpha_{jk}(f_j e_k - f_k e_j) + \sum_{j\leq i} \beta_j f_j^{q-1} e_j.$$

Looking at the i-th position of the expression, it follows that

$$-g = \sum_{j=1}^{i-1} \alpha_{ji} f_j + \beta_i f_i^{q-1},$$

which implies that $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$.

Lemma 5. *Suppose that for all $i \in \{1, \ldots, m\}$ and $d < d_{reg}(S_i)$, the sequence (12):*

$$0 \to (R/S_i)_{d-2q} \xrightarrow[\chi_{d,i}]{\times f_i^{q-1}} (R/S_{i-1})_{d-2} \xrightarrow[\phi_{d,i}]{\times f_i} (R/S_{i-1})_d \xrightarrow{\pi_i} (R/S_i)_d \to 0$$

is exact. Then, for all $i \in \{1, \ldots, m\}$, the Hilbert series of R/S_i is

$$[H_{n,i,q}(y)]_+ = \left[\frac{(1-y^q)^n}{(1-y)^n} \left(\frac{1-y^2}{1-y^{2q}} \right)^i \right]_+.$$

Proof. The dimension of R_δ for $\delta \in \mathbb{Z}$ is given by the coefficient of y^δ in the series:

$$\frac{(1-y^q)^n}{(1-y)^n}.$$

In other words, the Hilbert function of R, denoted by HF_R, is expressed as:

$$HF_R(\delta) = [y^\delta] \frac{(1-y^q)^n}{(1-y)^n} \text{ for all } \delta \in \mathbb{Z}. \tag{15}$$

The relationship (15) is established in Lemma 1 of [YC04]. Now, since the sequence (12) is exact, we can deduce the following relationship between the Hilbert functions for all $k \in \{1, \ldots, m\}$ and $d < d_{reg}(S_k)$

$$HF_{R/S_k}(d) - HF_{R/S_k}(d-2q) = HF_{R/S_{k-1}}(d) - HF_{R/S_{k-1}}(d-2).$$

Knowing that Equation (12) holds for $d < D := d_{reg}(S_i)$, we have

$$\sum_{d=0}^{D-1} (HF_{R/S_i}(d) - HF_{R/S_i}(d-2q)) y^d = \sum_{d=0}^{D-1} (HF_{R/S_{i-1}}(d) - HF_{R/S_{i-1}}(d-2)) y^d,$$

$$(1-y^{2q}) \sum_{d=0}^{D-1} HF_{R/S_i}(d) y^d = (1-y^2) \sum_{d=0}^{D-1} HF_{R/S_{i-1}}(d) y^d.$$

Hence,

$$\sum_{d=0}^{D-1} HF_{R/S_i}(d)y^d = \frac{1-y^2}{1-y^{2q}} \sum_{d=0}^{D-1} HF_{R/S_{i-1}}(d)y^d. \tag{16}$$

By recursively applying the relation Equation (16), from i down to 1, we obtain

$$\begin{aligned}
\sum_{d=0}^{D-1} HF_{R/S_i}(d)y^d &= \left(\frac{1-y^2}{1-y^{2q}}\right)^i \sum_{d=0}^{D-1} HF_R(d)y^d \\
&= \left(\frac{1-y^2}{1-y^{2q}}\right)^i \left[\left(\frac{1-y^q}{1-y}\right)^n\right]_{D-1} \\
&= \left[\left(\frac{1-y^2}{1-y^{2q}}\right)^i \left(\frac{1-y^q}{1-y}\right)^n\right]_{D-1}.
\end{aligned}$$

Since $D = d_{reg}(S_i)$, $\sum_{d=0}^{D-1} HF_{R/S_i}(d)y^d = HS_{R/S_i}(y)$, then

$$HS_{R/S_i}(y) = \left[\left(\frac{1-y^q}{1-y}\right)^n \left(\frac{1-y^2}{1-y^{2q}}\right)^i\right]_{D-1}.$$

It remains to show that D is the degree of the first non-positive coefficient of $H_{n,i,q}(y)$. Note that $D \leq d_{reg}(S_{i-1}) \leq d_{reg}(S_{i-2}) \leq \cdots \leq d_{reg}(S_1)$. Thus, there exists $j \in \{1, \ldots, i\}$ such that at degree $d = D$, the sequence (12) is not exact for $j \leq k \leq i$ and it is exact for $1 \leq k < j$. Using a similar argument as above, we can deduce that for $1 \leq k < j$, $HF_{R/S_k}(D) = \left[y^D\right] H_{n,k,q}(y)$.

Let $g \in R$ of degree $D-2q$ be such that $g+S_k \in \mathsf{ker}(\chi_{D,k})$, for $j \leq k \leq i$. Then $f_k^{q-1}g \in S_{k-1}$ and $\deg(f_k^{q-1}g) = D-2 < D \leq d_{reg}(S_k)$. This is equivalent to $f_k(f_k^{q-2}g) \in S_{k-1}$ and $\deg(f_k(f_k^{q-2}g)) < d_{reg}(S_k)$. Therefore, by Lemma 1, $\chi_{D,k}$ is injective. Furthermore, it always holds that $\mathrm{Im}(\chi_{D,k}) \subseteq \mathsf{ker}(\phi_{D,k})$ and that π_k is surjective. Since the sequence is not exact in degree $d = D$ for $j \leq k \leq i$, the condition that is not satisfied is $\mathsf{ker}(\phi_{D,k}) \subseteq \mathrm{Im}(\chi_{D,k})$. Hence, we have $\mathsf{rank}(\chi_{D,k}) < \mathsf{null}(\phi_{D,k})$, where $\mathsf{rank}(\chi_{D,k})$ and $\mathsf{null}(\phi_{D,k})$ denote the dimension over $\mathbb{F}_q$ of the image space of $\chi_{D,k}$ and the kernel space of $\phi_{D,k}$, respectively. Therefore,

$$\begin{aligned}
HF_{R/S_{j-1}}(D) &= \mathsf{null}(\pi_j) + \mathsf{rank}(\pi_j) \\
&= \mathsf{rank}(\phi_{D,j}) + HF_{R/S_j}(D) \\
&= HF_{R/S_{j-1}}(D-2) - \mathsf{null}(\phi_{D,j}) + HF_{R/S_j}(D) \\
&< HF_{R/S_{j-1}}(D-2) - \mathsf{rank}(\chi_{D,j}) + HF_{R/S_j}(D) \\
&= HF_{R/S_{j-1}}(D-2) - HF_{R/S_j}(D-2q) + HF_{R/S_j}(D).
\end{aligned}$$

Notice that $(1-y^{2q})H_{n,j,q}(y) = (1-y^2)H_{n,j-1,q}(y)$. It thus follows that

$$\begin{aligned} HF_{R/S_j}(D) &> HF_{R/S_{j-1}}(D) - HF_{R/S_{j-1}}(D-2) + HF_{R/S_j}(D-2q) \\ &= \left[y^D\right] H_{n,j-1,q}(y) - \left[y^{D-2}\right] H_{n,j-1,q}(y) + \left[y^{D-2q}\right] H_{n,j,q}(y) \\ &= \left[y^D\right] H_{n,j-1,q}(y) - \left[y^D\right] y^2 H_{n,j-1,q}(y) + \left[y^D\right] y^{2q} H_{n,j,q}(y) \\ &= \left[y^D\right] H_{n,j,q}(y). \end{aligned}$$

This last inequality can be used inductively from j down to i to prove that $HF_{R/S_i}(D) \geq \left[y^D\right] H_{n,i,q}(y)$. With this inequality and knowing that $HF_{R/S_i}(D)$ is zero since $D = d_{reg}(S_i)$, we have the desired result.

Lemma 6. *Suppose that for all $i \in \{1,\ldots,m\}$, the Hilbert series of R/S_i is*

$$[H_{n,i,q}(y)]_+ = \left[\frac{(1-y^q)^n}{(1-y)^n}\left(\frac{1-y^2}{1-y^{2q}}\right)^i\right]_+. \tag{17}$$

Then, for all $i \in \{1,\ldots,m\}$ and $d < d_{reg}(S_i)$, the sequence (12):

$$0 \to (R/S_i)_{d-2q} \xrightarrow[\chi_{d,i}]{\times f_i^{q-1}} (R/S_{i-1})_{d-2} \xrightarrow[\phi_{d,i}]{\times f_i} (R/S_{i-1})_d \xrightarrow{\pi_i} (R/S_i)_d \to 0$$

is exact.

Proof. Since $[H_{n,i,q}(y)]_+$ equals $HS_{R/S_i}(y)$ by hypothesis, its first non-positive coefficient appears in y^D, with $D = d_{reg}(S_i)$. Since HS_{R/S_i} is a polynomial of degree $D-1$, we have that

$$\begin{aligned} HS_{R/S_i}(y) &= \left[\frac{(1-y^q)^n}{(1-y)^n}\left(\frac{1-y^2}{1-y^{2q}}\right)^{i-1}\frac{1-y^2}{1-y^{2q}}\right]_{D-1} \\ &= \left[HS_{R/S_{i-1}}(y)\right]_{D-1}\left[\frac{1-y^2}{1-y^{2q}}\right]_{D-1}. \end{aligned}$$

The previous expression gives us the relation

$$(1-y^{2q})HS_{R/S_i}(y) = (1-y^2)\left[HS_{R/S_{i-1}}(y)\right]_{D-1}. \tag{18}$$

Then

$$(1-y^{2q})\sum_{d=0}^{D-1} HF_{R/S_i}(d)y^d = (1-y^2)\sum_{d=0}^{D-1} HF_{R/S_{i-1}}(d)y^d,$$

$$\sum_{d=0}^{D-1}(HF_{R/S_i}(d) - HF_{R/S_i}(d-2q))y^d = \sum_{d=0}^{D-1}(HF_{R/S_{i-1}}(d) - HF_{R/S_{i-1}}(d-2))y^d.$$

Therefore

$$HF_{R/S_i}(d) - HF_{R/S_i}(d-2q) = HF_{R/S_{i-1}}(d) - HF_{R/S_{i-1}}(d-2), \tag{19}$$

for $1 \leq i \leq m$ and for all $d < d_{reg}(S_i)$. Now, we apply induction on d to show that Equation (12) is exact. For the base case $d = 2$

$$0 \to 0 \xrightarrow[\chi_{2,i}]{\times f_i^{q-1}} (R/S_{i-1})_0 \xrightarrow[\phi_{2,i}]{\times f_i} (R/S_{i-1})_2 \xrightarrow[\pi_i]{} (R/S_i)_2 \to 0$$

is clearly exact. Suppose Equation (12) is exact for $d < d^* < d_{reg}(S_i)$ and we will show it is exact for d^* and for $1 \leq i \leq m$. Fix $i \in \{1, \ldots, m\}$. Note that

$$\begin{aligned} HF_{i-1}(d^*) &= \mathsf{null}(\pi_i) + \mathsf{rank}(\pi_i) \\ &= \mathsf{rank}(\phi_{d^*,i}) + HF_i(d^*) \\ &= HF_{i-1}(d^* - 2) - \mathsf{null}(\phi_{d^*,i}) + HF_i(d^*). \end{aligned} \tag{20}$$

From the inductive hypothesis and Lemma 1, we have that $f_i^{q-1} g \in S_{i-1}$ and $\deg(f_i^{q-1} g) < d_{reg}(S_i)$ imply $g \in S_i$, that is, for $d < d_{reg}(S_i)+2$, $\chi_{d,i}$ is injective. Since $d^* < d^* + 1 < d_{reg}(S_i) + 2$, then $\chi_{d^*,i}$ is injective, and hence $\mathsf{rank}(\chi_{d^*,i}) = HF_i(d^* - 2q)$. It thus follows from Equation (19) that

$$HF_{R/S_{i-1}}(d^*) = HF_{R/S_{i-1}}(d^* - 2) - \mathsf{rank}(\chi_{d^*,i}) + HF_{R/S_i}(d^*). \tag{21}$$

Then, from Equation (20) and Equation (21), it follows that $\mathsf{null}(\phi_{d^*,i}) = \mathsf{rank}(\chi_{d^*,i})$. Since $\mathrm{Im}(\chi_{d^*,i}) \subseteq \mathsf{ker}(\phi_{d^*,i})$, it follows that $\mathrm{Im}(\chi_{d^*,i}) = \mathsf{ker}(\phi_{d^*,i})$. Therefore the sequence is exact.

We now state the main theorem of this section, whose proof follows from the lemmas 2, 3, 4, 5, and 6.

Theorem 1. *Let $f_1, \ldots, f_m \in R$ be homogeneous quadratic, for $i = 1, \ldots, m$, $\mathcal{F}_i = (f_1, \ldots, f_i)$, $S_i := \langle \mathcal{F}_i \rangle$, and $\mathcal{F} = \mathcal{F}_m$. Then the following statements are equivalent.*

1. *For all $i \in \{1, \ldots, m\}$ and for all $g \in R$, if $f_i g \in S_{i-1}$ and $\deg(f_i) + \deg(g) < d_{reg}(S_i)$, then $g \in S_{i-1} + \left\langle f_i^{q-1} \right\rangle$.*
2. *The following sequence is exact for all $i \in \{1, \ldots, m\}$ and $d < d_{reg}(S_i)$*

$$0 \to (R/S_i)_{d-2q} \xrightarrow[\chi_{d,i}]{\times f_i^{q-1}} (R/S_{i-1})_{d-2} \xrightarrow[\phi_{d,i}]{\times f_i} (R/S_{i-1})_d \xrightarrow{\pi_i} (R/S_i)_d \to 0.$$

3. *For all $i \in \{1, \ldots, m\}$, every $\mathbf{s} \in Syz(\mathcal{F}_i)$ of degree less than $d_{reg}(S_i)$ belongs to $Syz_{triv}(\mathcal{F}_i)$.*
4. *For all $i \in \{1, \ldots, m\}$, the Hilbert series of R/S_i is*

$$[H_{n,i,q}(y)]_+ = \left[\frac{(1-y^q)^n}{(1-y)^n} \left(\frac{1-y^2}{1-y^{2q}} \right)^i \right]_+ .$$

Definition 4 (q-semi-regularity). *A sequence of homogeneous quadratic polynomials $(f_1, \ldots, f_m) \in R^m$ is called q-semi-regular if it satisfies the equivalent conditions of Theorem 1. A non-homogeneous quadratic sequence $(f_1, \ldots, f_m) \in R^m$ is called q-semi-regular if the sequence formed by the homogeneous part of largest degree is q-semi-regular.*

4 Revisiting Admissible Parameters

We now come back to the question of what are admissible parameters for the Crossbred algorithm. Intuitively a triple (D, d, k) is admissible, if the Crossbred algorithm works for such a triple, that is, if the consistency of the specialized system $\mathcal{F}|_{\mathbf{b}}$ can be verified by checking the consistency of the linearized system $\mathrm{M}_{\mathbf{b}} \cdot (\mathbf{z}, 1)^\top = 0$ in Step 8 of the algorithm. However, it is impossible to determine a priory if this is the case. Instead, we would like to establish conditions, on n, m and q, that allow Crossbred to work for most systems. We have identified two such conditions. So, we will define admissible based on these conditions, we will then explain the rationale behind them and test them experimentally.

Definition 5 (Admissibility condition). *Let m, n, q be positive integers, where q is a prime power, and let*

$$S_{k,q}(w, z) := \frac{H_{k,m,q}(wz) \cdot M_{n-k,q}(w) - H_{n,m,q}(w) - H_{k,m,q}(z)}{(1-z)(1-w)}.$$

A triple of integers (D, d, k) is admissible for Crossbred to solve generic MQ instances of m equations in n variables over $\mathbb{F}_q$ if

i) $[w^D z^d] S_{k,q}(w, z) \geq 0$ *and*
ii) $[z^D] \left[\frac{H_{k,m,q}(z)}{1-z} \right]_+ = 0.$

Note that condition i) above is precisely the condition initially established for $\mathbb{F}_2$ by Joux and Vitse in [JV18], and generalized by Bellini et al. in [BMSV22]. Next, we formally explain the rationale behind Definition 5. First, we define two additional submatrices of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ and their corresponding vector spaces:

- $\mathrm{Lac}^k_{D,d}(\mathcal{F})$: the row submatrix of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ whereby each row $(\mathfrak{m}, f)$ has the property $\deg_k(\mathfrak{m}) < d - 1$.
- $\mathrm{L}^k_{D,d}(\mathcal{F})$: the column submatrix of $\mathrm{Lac}^k_{D,d}$ of columns corresponding to monomials $\mathfrak{m}$ with $\deg_k(\mathfrak{m}) \leq d$.
- $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$: the row space of $\mathrm{Lac}^k_{D,d}(\mathcal{F})$.
- $\mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F})$: the row space of $\mathrm{Mac}^k_{D,d}(\mathcal{F})$.

Figure 1 illustrates how the submatrices $\mathrm{Lac}^k_{D,d}$ and $\mathrm{L}^k_{D,d}$ relate with their counterparts $\mathrm{Mac}^k_{D,d}$ and $\mathrm{M}^k_{D,d}$ inside $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$. The following lemma provides a sufficient condition for Crossbred to produce a specific number of linearly independent polynomials in the preprocessing step.

Lemma 7. *Let $\mathcal{F} \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]^m$ be a quadratic sequence and D, d, k positive integers, and set $I = \dim\big(\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) \cap \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F})\big)$. The preprocessing step of Algorithm 1 produces at least*

$$t := \dim\left(\ker(\mathrm{M}^k_{D,d}(\mathcal{F}))\right) - \dim\left(\ker(\mathrm{Mac}^k_{D,d}(\mathcal{F}))\right) - I \tag{22}$$

linearly independent polynomials, none of which are in $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$.

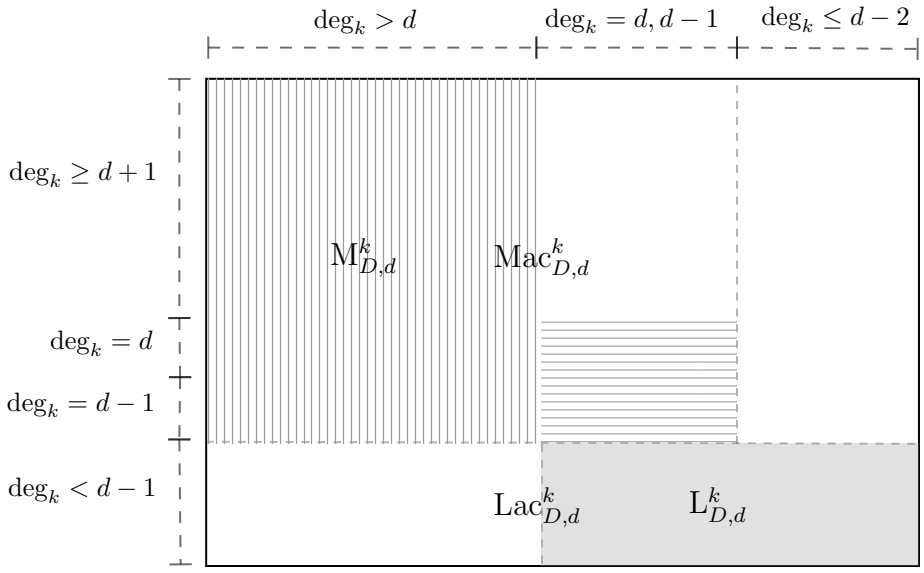

Fig. 1. Visualization of Macaulay matrix $\mathrm{Mac}_{\mathrm{D}}$, $\mathrm{Mac}^k_{D,d}$, and $\mathrm{Lac}^k_{D,d}$. Here $\mathrm{M}^k_{D,d}$ corresponds to the part marked with vertical lines.

Proof. The number of linearly independent polynomials found at step 3 of Algorithm 1 is given by the dimension of the vector space

$$O_0 := \left\{ \mathbf{v}_i \cdot \mathrm{Mac}^k_{D,d}(\mathcal{F}) \mid \mathbf{v}_i \in \mathsf{ker}(\mathrm{M}^k_{D,d}) \right\},$$

which is

$$\begin{aligned} \mathsf{dim}(O_0) &= \mathsf{dim}(\mathsf{ker}(\mathrm{M}^k_{D,d})) - \mathsf{dim}(\mathsf{ker}(\mathrm{Mac}^k_{D,d})) \\ &= \mathsf{rank}(\mathrm{Mac}^k_{D,d}(\mathcal{F})) - \mathsf{rank}(\mathrm{M}^k_{D,d}(\mathcal{F})). \end{aligned}$$

Step 3 of Algorithm 1 finds polynomials p_i corresponding to elements in O_0 but we are only interested in those corresponding to vectors in $O_0 \setminus \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$. We highlight that in general $O_0 \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) \neq \emptyset$.

Consider the quotient space

$$O_1 := O_0/(O_0 \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})).$$

Hence, $\mathsf{dim}(O_1)$ indicates how many of the linearly independent polynomials found in step 3 of Algorithm 1 correspond to vectors that are not in $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$. Then, to conclude the proof, it remains to shows that $\mathsf{dim}(O_1) = t$, with t as in (22). Note that $\mathsf{dim}(O_1) = \mathsf{dim}(O_0) - \mathsf{dim}(O_0 \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}))$.

Next, we show that $O_0 \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) = \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F}) \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$. It is clear that $O_0 \subseteq \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F})$. Now, suppose that $\mathbf{c} \in \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F}) \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$ is a

nonzero vector. On one side, we have that $\mathbf{c} = \mathbf{v} \cdot \mathrm{Mac}^k_{D,d}(\mathcal{F})$ for some vector $\mathbf{v}$. On the other side, since $\mathbf{c} \in \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$, the coordinates of $\mathbf{c}$ corresponding to monomials of $\deg_k > d$ are zero. Therefore, $\mathbf{v} \in \mathsf{ker}(\mathrm{M}^k_{D,d}(\mathcal{F}))$, which implies that $\mathbf{c} \in O_0$.

Finally, since $O_0 \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) = \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F}) \cap \mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$, it holds that $\mathsf{dim}(O_1) = \mathsf{dim}(O_0) - I$, where $I = \mathsf{dim}\big(\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) \cap \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F})\big)$.

Lemma 7 above provides a precise count for the number of "useful" polynomials produced in the preprocessing step of Crossbred. For Crossbred to work, this number must be enough so that it is possible to check the consistency of the system $\mathcal{F}|_{\mathbf{b}}$ by linearization in Step 8. That means that preprocessing must produce at least $\mathsf{corank}(\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}}))$ useful polynomials. Condition i) in Definition 5 captures precisely this requirement under the regularity assumptions a), b), and c) in Theorem 2.

Theorem 2 (Generic admissibility condition). *Let $\mathcal{F}$ be a quadratic sequence in $\mathbb{F}_q[\mathbf{x}, \mathbf{y}]^m$. Given a triple of integers (D, d, k) and a vector $\mathbf{b} \in \mathbb{F}_q^{n-k}$. Suppose that the following assumptions hold:*

a) $\mathcal{F}$ is q-semi-regular.
b) The specialized sequence $\mathcal{F}|_{\mathbf{b}} \in \mathbb{F}_q[\mathbf{x}]^m$ is q-semi-regular.
c) The corank of $\mathrm{L}^k_{D,d}(\mathcal{F})$ is the maximum between zero and the coefficient of $w^D z^d$ in the series $\frac{H_{k,m,q}(wz) \cdot M_{n-k,q}(w)}{(1-z)(1-w)}$.

If $D < \deg_{reg}(\mathcal{F})$, $d < \deg_{reg}(\mathcal{F}|_{\mathbf{b}})$ and $[w^D z^d] S_{k,q}(w, z) \geq 0$, then the preprocessing step of Algorithm 1 produces at least

$$\mathsf{corank}(\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}})) \tag{23}$$

linearly independent polynomials, none of which are in $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$.

Proof. From the regularity assumptions, we obtain that

$$\mathsf{corank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) = [w^D] \frac{H_{n,m,q}(w)}{1-w} = [w^D z^d] \frac{H_{n,m,q}(w)}{(1-z)(1-w)},$$

$$\mathsf{corank}(\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}})) = [z^d] \frac{H_{k,m,q}(z)}{1-z} = [w^D z^d] \frac{H_{k,m,q}(z)}{(1-z)(1-w)}, \text{ and}$$

$$\mathsf{corank}(\mathrm{L}^k_{D,d}(\mathcal{F})) = [w^D z^d] \frac{H_{k,m,q}(wz) \cdot M_{n-k,q}(w)}{(1-z)(1-w)}.$$

Define

$$T_{k,q}(w, z) := \frac{H_{k,m,q}(wz) \cdot M_{n-k,q}(w) - H_{n,m,q}(w)}{(1-z)(1-w)},$$

and set $I = \mathsf{dim}\big(\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F}) \cap \mathrm{V}_{\mathrm{Mac}^k_{D,d}}(\mathcal{F})\big)$.

$$
\begin{aligned}
[w^D z^d]T_{k,q}(w,z) &= \mathsf{corank}(\mathrm{L}^k_{D,d}(\mathcal{F})) - \mathsf{corank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) \\
&= \mathsf{ncols}(\mathrm{L}^k_{D,d}(\mathcal{F})) - \mathsf{rank}(\mathrm{L}^k_{D,d}(\mathcal{F})) - \mathsf{ncols}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) + \mathsf{rank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) \\
&= \mathsf{ncols}(\mathrm{L}^k_{D,d}(\mathcal{F})) - \mathsf{rank}(\mathrm{Lac}^k_{D,d}(\mathcal{F})) - \mathsf{ncols}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) + \mathsf{rank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) \\
&= \Big(\mathsf{rank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) - \mathsf{rank}(\mathrm{Lac}^k_{D,d}(\mathcal{F}))\Big) - \big(\mathsf{ncols}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) - \mathsf{ncols}(\mathrm{L}^k_{D,d}(\mathcal{F}))\big) \\
&= \Big(\mathsf{rank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) - \mathsf{rank}(\mathrm{Lac}^k_{D,d}(\mathcal{F}))\Big) - \mathsf{ncols}(\mathrm{M}^k_{D,d}(\mathcal{F})) \\
&\leq \Big(\mathsf{rank}(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})) - \mathsf{rank}(\mathrm{Lac}^k_{D,d}(\mathcal{F}))\Big) - \mathsf{rank}(\mathrm{M}^k_{D,d}(\mathcal{F})) \\
&= \mathsf{rank}(\mathrm{Mac}^k_{D,d}(\mathcal{F})) - I - \mathsf{rank}(\mathrm{M}^k_{D,d}(\mathcal{F})), \\
&= \mathsf{dim}\left(\mathsf{ker}(\mathrm{M}^k_{D,d}(\mathcal{F}))\right) - \mathsf{dim}\left(\mathsf{ker}(\mathrm{Mac}^k_{D,d}(\mathcal{F}))\right) - I.
\end{aligned}
$$

Now if $[w^D z^d]S_{k,q}(w,z) \geq 0$, then

$$
\begin{aligned}
\mathsf{corank}(\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}})) &= [z^d]\frac{H_{k,m,q}(z)}{1-z} \\
&= [w^D z^d]\frac{H_{k,m,q}(z)}{(1-z)(1-w)} \\
&\leq [w^D z^d]\frac{H_{n,m,q}(w)\cdot M_{n-k,q}(w) - H_{k,m,q}(wz)}{(1-z)(1-w)} \\
&\leq \mathsf{rank}(\mathrm{Mac}^k_{D,d}(\mathcal{F})) - \mathsf{rank}(\mathrm{M}^k_{D,d}(\mathcal{F})) - I \\
&= \mathsf{dim}\left(\mathsf{ker}(\mathrm{M}^k_{D,d}(\mathcal{F}))\right) - \mathsf{dim}\left(\mathsf{ker}(\mathrm{Mac}^k_{D,d}(\mathcal{F}))\right) - I.
\end{aligned}
$$

The result then follows from Lemma 7.

Remark 2. The admissibility condition $[w^D z^d]S_{k,q}(w,z) \geq 0$ given in Theorem 2 can be expressed in terms of univariate power series only. This representation allows to compute admissible parameters using state-of-the-art software libraries that do not support bi-variate power series currently such as [tea23]. The condition $[w^D z^d]S_{k,q}(w,z) \geq 0$ can be rephrased as

$$
C(D,d) - [w^D]\frac{H_{n,m,q}(w)}{1-w} - [z^d]\frac{H_{k,m,q}(z)}{1-z} \geq 0,
$$

where

$$
C(D,d) := \sum_{i=0}^{d} [z^i]H_{k,m,q}(z)\cdot[w^{D-i}]\frac{M_{n-k,q}(w)}{(1-w)}.
$$

We emphasize that condition i) of Definition 5 is a necessary condition for Crossbred to work but it is not sufficient. In order to test if a vector $\mathbf{b}$ (chosen in Step 4) is not part of any solution one can checks the inconsistency of the system $\mathcal{F}_{\mathbf{b}}$. For this to happen, the constant polynomial 1 must be in the span of the set of polynomials represented by $\mathrm{M}_{\mathbf{b}} = \mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}} \cup \mathcal{P}|_{\mathbf{b}})$. Although we cannot test this a priory, notice that the rows of $\mathrm{M}_{\mathbf{b}}$ are in the span of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F}|_{\mathbf{b}})$. Condition ii) of Definition 5 provides a sufficient condition for the polynomial 1 to be in the span of the polynomials associated with the rows of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F}|_{\mathbf{b}})$ under Assumption 1.

Assumption 1 *For most quadratic sequences $\mathcal{F} \in \mathbb{F}_q[\mathbf{x}]^m$, the corank of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F})$ is given by $[z^D]\left[\frac{H_{k,m,q}(z)}{1-z}\right]_+$, where $[\cdot]_+$ denotes the truncated series from the first non-positive coefficient.*

Note that this assumption goes beyond q-semi-regular, because we are considering non-homogeneous sequences and we are not restricting D to be below the degree of regularity. We test this assumption in Section 5 below.

Moreover, in Definition 5, neither condition i) implies condition ii), nor ii) implies i).

Example 2. For $q = 16$, $n = m = 8$, $k = 7$, $D = 7$, $d = 4$, condition i) is satisfied but not condition ii). Then, when we generate random sequences with these parameters, the corank of $\mathrm{Mac}_{\mathrm{D}}(\mathcal{F}|_{\mathbf{b}})$ is positive for all $\mathbf{b} \in \mathbb{F}_q^{n-k}$, which implies that the corank of $\mathrm{M}_{\mathbf{b}}$ is positive for all $\mathbf{b} \in \mathbb{F}_q^{n-k}$. Therefore, we are unable to test the consistency of the system $\mathcal{F}|_{\mathbf{b}}$ by linearization in Step 8 of Crossbred.

On the other hand, with $q = 16$, $n = m = 8$, $k = 7$, $D = 7$, $d = 2$, condition ii) is satisfied but not condition i). So we have that less than $\mathsf{corank}(\mathcal{F}|_{\mathbf{b}})$ polynomials p_i can be obtained in the preprocesing. Therefore, the corank of $\mathrm{M}_{\mathbf{b}}$ is positive for all $\mathbf{b} \in \mathbb{F}_q^{n-k}$. As a result when we generate random sequences with these parameters, we are unable to test the consistency of the system by linearization in Step 8 of Crossbred.

If (D, d, k) is admissible, then Crossbred most likely can test the consistency of the specialized system $\mathcal{F}|_{\mathbf{b}}$ efficiently. By Theorem 2, Crossbred finds at least $\mathsf{corank}(\mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}}))$ linearly independent polynomials in the preprocessing step of Algorithm 1, which correspond to vectors that are not in $\mathrm{V}_{\mathrm{Lac}^k_{D,d}}(\mathcal{F})$. Moreover, by Assumption 1 and since $[z^D]\left[\frac{H_{k,m,q}(z)}{1-z}\right]_+ = 0$, in Step 7, when the polynomials in $\mathcal{F} \cup \mathcal{P}$ are specialized, one expects that the corank of $\mathrm{M}_{\mathbf{b}} = \mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}} \cup \mathcal{P}|_{\mathbf{b}})$ is zero so that it is possible to test the consistency of the specialized system $\mathcal{F}|_{\mathbf{b}}$ by simply computing the rank of $\mathrm{M}_{\mathbf{b}}$. Although there is no guarantee that this is the case, we believe that it is a reasonable assumption.

Assumption 2 *Let (D, d, k) be a triple of admissible parameters for Crossbred to solve generic MQ instances of m equations in n variables over $\mathbb{F}_q$. Let $\mathcal{F} \in \mathbb{F}_q[x_1, \ldots, x_n]^m$, $\mathbf{b} \in \mathbb{F}_q^{n-k}$, and $\mathrm{M}_{\mathbf{b}} = \mathrm{Mac}_{\mathrm{d}}(\mathcal{F}|_{\mathbf{b}} \cup \mathcal{P}|_{\mathbf{b}})$. If for all $\mathbf{a} \in \mathbb{F}_q^k$, $(\mathbf{a}, \mathbf{b})$*

is not a solution for $\mathcal{F}(\mathbf{x},\mathbf{y})=0$*, then* $\mathsf{corank}(\mathrm{M}_{\mathbf{b}})=0$*. If there exists* $\mathbf{a}\in\mathbb{F}_q^k$ *such that* $(\mathbf{a},\mathbf{b})$ *is a solution for* $\mathcal{F}(\mathbf{x},\mathbf{y})=0$*, then* $\mathsf{corank}(\mathrm{M}_{\mathbf{b}})>0$.

Experimentally we verify that Assumption 2 holds for the vast majority of $(\mathbf{a},\mathbf{b})\in\mathbb{F}_q^k\times\mathbb{F}_q^{n-k}$ when they are not a solution of $\mathcal{F}$, while it always holds for a solution vector $(\mathbf{a}_0,\mathbf{b}_0)$. We describe more details of these experiments in Section 5.

5 Experiments

We now present empirical evidence that supports several of our theoretical results.

In all of our experiments, we choose $m=n$, $q\in\{3,16\}$, and $n\in\{2,\ldots,10\}$ for $q=16$ and $n\in\{2,\ldots,16\}$ for $q=3$. We varied k from 1 to $n-1$, and D from 2 to the minimum between $D_{max}=7$ and one unit less than the $\deg(H_{n,m,q})+1$, which is the degree of regularity of a q-semi-regular sequence of m polynomials in n variables. This upper bound $D_{max}=7$ was a restriction we used in order to keep manageable the sizes of all matrices involved in the experiments. And finally, d ranged from 1 to $\min\{D-1,\deg(H_{k,m,q})\}$. For each set of parameters (q,n,m,D,d,k), we repeated five times all the experiments described in this section.

Recall that we set $\mathbf{x}=(x_1,\ldots,x_k)$ and $\mathbf{y}=(x_{k+1},\ldots,x_n)$. In this section, for a given homogeneous sequence $\mathcal{F}\in\mathbb{F}_q[\mathbf{x},\mathbf{y}]$, we use $\mathrm{L}_{D,d}^k(\mathcal{F})^h$, $\mathrm{Mac}_{D,d}^k(\mathcal{F})^h$ and $\mathrm{M}_{D,d}^k(\mathcal{F})^h$ to denote the submatrices of $\mathrm{L}_{D,d}^k(\mathcal{F})$, $\mathrm{Mac}_{D,d}^k(\mathcal{F})$ and $\mathrm{M}_{D,d}^k(\mathcal{F})$ formed by the rows and columns corresponding to polynomials and monomials of degree D, respectively. Similarly, we define $\mathrm{Mac}_{\mathrm{d}}(\mathcal{F})^h$ as the submatrix of $\mathrm{Mac}_{\mathrm{d}}(\mathcal{F})$ formed by the rows and columns corresponding to polynomials and monomials of degree d, respectively.

5.1 Regularity assumptions in Theorem 2

We perform the following experiment to verify the frequency of the regularity conditions in Theorem 2.

1. Sample a quadratic sequence $\mathcal{F}\in\mathbb{F}_q[\mathbf{x},\mathbf{y}]^m$ and denote by $\mathcal{F}^h$ the sequence formed by the homogeneous part of largest degree of each polynomial in $\mathcal{F}$.
2. Use Theorem 1 to check if $\mathcal{F}$ is q-semi-regular.
3. Sample $\mathbf{b}\in\mathbb{F}_q^{n-k}$.
4. Use Theorem 1 to check if $\mathcal{F}|_{\mathbf{b}}\in\mathbb{F}_q[\mathbf{x}]^m$ is q-semi-regular.
5. Compute $\mathsf{corank}\left(\mathrm{L}_{D,d}^k(\mathcal{F})\right)$.

In 99.99% of the instances that we considered, we obtained that

$$\mathsf{corank}\left(\mathrm{Mac}_{\mathrm{D}}(\mathcal{F}^h)^h\right)=[w^D]H_{n,m,q}(w),$$

which implies that $\mathcal{F}$ was q-semi-regular in 99.99% of the instances considered in the experiments, according to Theorem 1. Also, the condition

$$\mathsf{corank}\left(\mathrm{Mac_d}(\mathcal{F}^h|_{\mathbf{b}})^h\right) = [w^d]H_{k,m,q}(w),$$

was always met, so it follows that $\mathcal{F}|_{\mathbf{b}}$ was q-semi-regular in all the instances considered in the experiments. Next, it was always the case that

$$\mathsf{corank}\left(\mathrm{L}^k_{D,d}(\mathcal{F})\right) = [w^D z^d]\frac{H_{k,m,q}(wz)\cdot M_{n-k,q}(w)}{(1-z)(1-w)}.$$

Notice that when $\mathrm{L}^k_{D,d}(\mathcal{F})$ has no rows, we have

$$\begin{aligned}\mathsf{corank}\left(\mathrm{L}^k_{D,d}(\mathcal{F})\right) &= \mathsf{ncols}\left(\mathrm{L}^k_{D,d}(\mathcal{F})\right)\\ &= \mathsf{ncols}\left(\mathrm{Mac_D}(\mathcal{F})\right) - \mathsf{ncols}\left(\mathrm{M}^k_{D,d}(\mathcal{F})\right).\end{aligned}$$

Thus, according to our experiments, we claim that a sequence $\mathcal{F}$ of quadratic polynomials that is chosen uniformly at random from $\mathbb{F}_q[\mathbf{x},\mathbf{y}]^m$, has a probability close to 1 of being q-semi-regular. That is also the case for the specialized sequence $\mathcal{F}|_{\mathbf{b}}$, when $\mathbf{b}$ is a vector chosen uniformly at random from $\mathbb{F}_q^{n-k}$.

5.2 Testing accuracy of predictions for $\mathsf{corank}\left(\mathrm{Mac_D}(\mathcal{F})\right)$

Here we present our experimental results to test Assumption 1. For a given tuple of integer parameters (q,k,m,D), where q is a prime power, we perform the following experiment:

1. Sample uniformly an affine quadratic $\mathcal{F}\in\mathbb{F}_q[\mathbf{x}]^m$.
2. Check if $\mathsf{corank}\left(\mathrm{Mac_D}(\mathcal{F})\right) = [z^D]\left[\frac{H_{k,m,q}(z)}{1-z}\right]_+$.

In only 52 out of 5085 instances that were considered, the corank of $\mathrm{Mac_D}(\mathcal{F})$ was not the predicted value $[z^D]\left[\frac{H_{k,m,q}(z)}{1-z}\right]_+$. That is, Assumption 1 is satisfied in 99% of all the instances that were run in our experiments.

5.3 Testing effectiveness of Crossbred on admissible parameters

In this section, we show our experimental results performed to test the effectiveness of Crossbred (Algorithm 1) to find solutions of quadratic systems over finite fields, when the algorithm is instantiated on admissible parameters. In particular, we have to experimentally verify Assumption 2.

For a given triple of integer parameters (q,n,m) and admissible parameters (D,d,k), i.e., it holds that $[w^D z^d]S_{k,q}(w,z)\geq 0$ and $[z^D]\left[\frac{H_{k,m,q}(z)}{1-z}\right]_+ = 0$, we perform the following experiment:

1. Sample uniformly a quadratic $\mathcal{F}\in\mathbb{F}_q[\mathbf{x},\mathbf{y}]^m$.

2. Compute a basis $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_s\}$ of $\mathsf{ker}(\mathrm{M}^k_{D,d}(\mathcal{F}))$.
3. Compute $\mathcal{P} = \{p_1, \ldots, p_s\}$, where p_i is the polynomial corresponding to $\mathbf{v}_i \cdot \mathrm{Mac}^k_{D,d}(\mathcal{F})$ and $p_i \neq 0$.
4. Compute $\mathcal{P}|_{\mathbf{b}}$ and $\mathcal{F}|_{\mathbf{b}}$ for a random $\mathbf{b} \in \mathbb{F}_q^{n-k}$.
5. Compute the corank of $\mathrm{M}_{\mathbf{b}} := \mathrm{Mac}_{\mathrm{d}}(\mathcal{P}|_{\mathbf{b}} \cup \mathcal{F}|_{\mathbf{b}})$.

We divide all the instances considered into two groups, group **G1** in which the chosen $\mathbf{b}$ is part of a solution of $\mathcal{F}$, and group **G2** in which the chosen $\mathbf{b}$ is not part of any solution of $\mathcal{F}$. For each set of parameters (q, n, m, D, d, k), we count the number of times $\mathsf{corank}(\mathrm{M}_{\mathbf{b}})$ is equal to zero, and the number of times it is not. Notice that $\mathsf{corank}(\mathrm{M}_{\mathbf{b}}) = 0$ if and only if $\mathsf{rank}(\mathrm{M}_{\mathbf{b}}) = [z^d]M_{k,q}(z)/(1-z)$. In our experiments for **G1** we obtained that $\mathsf{corank}(\mathrm{M}_{\mathbf{b}}) > 0$ in all the instances considered for admissible parameters. Moreover, $\mathsf{corank}(\mathrm{M}_{\mathbf{b}}) = 1$ in 1013 out of 1015 and 1260 out of 1275 instances of admissible parameters for $q = 16$ and $q = 3$, respectively; and $\mathsf{corank}(\mathrm{M}_{\mathbf{b}}) = 2$ in the remaining cases. That is, there was unique solution in 99% of the instances considered in **G1**. For group **G2** we found that $\mathsf{corank}(\mathrm{M}_{\mathbf{b}}) > 0$ (and equal to 1) in only 10 out of 1015 and 29 out of 1275 instances of admissible parameters for $q = 16$ and $q = 3$, respectively. These experimental results show us that when the algorithm is instantiated on admissible parameters, Assumption 2 is satisfied 100% of the times when $\mathbf{b}$ is part of a solution of $\mathcal{F}$, and 98% of the times when $\mathbf{b}$ is not part of any solution of $\mathcal{F}$; which gives us a very high effectiveness for Crossbred in those cases.

6 Implications to Cryptography

In Section 4, we show that one additional condition has to be introduced over a triple of parameters (D, d, k) for Crossbred to work, see Definition 5. This implies that for some instance of MQ, the set of admissible parameters is a proper subset of the set estimated in previous works and therefore the complexity of Crossbred was underestimated.

MQ parameters (q, n, m)	Old optimal (D, d, k)	Old Estimate	New optimal (D, d, k)	New Estimate
(256, 43, 43)	(24, 4, 31)	153.2	(23, 5, 32)	153.5
(16, 63, 63)	(22, 3, 33)	166.1	(22, 3, 33)	166.1
(256, 71, 71)	(30, 19, 63)	247.3	(30, 19, 63)	247.3
(256, 95, 95)	(30, 26, 83)	334.6	(30, 22, 80)	338.6

Table 1. New estimates for the complexity of the Crossbred algorithm to perform a forgery attack against the UOV signature scheme.

As an example, Table 1 shows the complexity estimates of Crossbred against the instances of the MQ problem required to perform direct forgery attack

against the UOV signature scheme, as specified in [BCD+23]. The Old optimal set of parameters is taken from the set of parameters satisfying only condition i) in Definition 5 and represents the optimal according to the state of the art. The New optimal set is taken from the set of admissible parameters according to Definition 5. Both complexity estimates are computed as the logarithm of the number of multiplications over $\mathbb{F}_q$ in Crossbred, when it is instantiated with parameters (D, d, k). We observe that for the first three instances the estimated complexity barely changes, but for the last instance it was underestimated by a factor of 16.

References

Bar04. Magali Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes cor- recteurs et à la cryptographie.* PhD thesis, Université de Paris 6 - Pierre et Marie Curie, 2004.

BBSV22. Stefano Barbero, Emanuele Bellini, Carlo Sanna, and Javier Verbel. Practical complexities of probabilistic algorithms for solving Boolean polynomial systems. *Discrete Appl. Math.*, 309:13–31, 2022.

BCD+23. Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang. UOV: Specifications, 2023. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/UOV-spec-web.pdf.

Beu22. Ward Beullens. MAYO: Practical post-quantum signatures from oil-and-vinegar maps. In Riham AlTawy and Andreas Hülsing, editors, *SAC 2021*, volume 13203 of *LNCS*, pages 355–376. Springer, Heidelberg, September / October 2022.

BFR23. Ryad Benadjila, Thibauld Feneuil, and Matthieu Rivain. MQ on my mind: Post-quantum signatures from the non-structured multivariate quadratic problem. Cryptology ePrint Archive, Paper 2023/1719, 2023. https://eprint.iacr.org/2023/1719.

BFSS13. Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Pierre-Jean Spaenlehauer. On the complexity of solving quadratic Boolean systems. *Journal of Complexity*, 29(1):53–75, 2013.

BFSY05. Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *MEGA 2005 - 8th International Symposium on Effective Methods in Algebraic Geometry*, pages 1–17, 2005.

BMSV22. Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel. An estimator for the hardness of the MQ problem. In Lejla Batina and Joan Daemen, editors, *AFRICACRYPT 22*, volume 2022 of *LNCS*, pages 323–347. Springer Nature, July 2022.

CHR+16. Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. From 5-pass MQ-based identification to MQ-based signatures. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 135–165. Springer, Heidelberg, December 2016.

CHR+20. Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. MQDSS specifications, 2020. http://mqdss.org/specification.html.

CSD. Information Technology Laboratory Computer Security Division. Round 1 additional signatures - post-quantum cryptography: Digital signature schemes: Csrc.

Dua23. João Diogo Duarte. On the complexity and admissible parameters of the crossbred algorithm in $\mathbb{F}_{q\geq 2}$. Cryptology ePrint Archive, Paper 2023/1664, 2023. https://eprint.iacr.org/2023/1664.

DY09. Jintai Ding and Bo-Yin Yang. *Multivariate Public Key Cryptography*, pages 193–241. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

GJ90. Michael R. Garey and David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., USA, 1990.

JV18. Antoine Joux and Vanessa Vitse. A crossbred algorithm for solving Boolean polynomial systems. In Jerzy Kaczorowski, Josef Pieprzyk, and Jacek Pomykała, editors, *Number-Theoretic Methods in Cryptology*, pages 3–21, Cham, 2018. Springer International Publishing.

Kal95. Erich Kaltofen. Analysis of coppersmith's block wiedemann algorithm for the parallel solution of sparse linear systems. *Mathematics of Computation*, 64(210):777–806, 1995.

KPG99. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. *EUROCRYPT 1999. LNCS*, 1592:206–222, 1999.

Nak23. Shuhei Nakamura. Admissible parameter sets and complexity estimation of crossbred algorithm. Cryptology ePrint Archive, Paper 2023/1687, 2023. https://eprint.iacr.org/2023/1687.

tea23. The FLINT team. *FLINT: Fast Library for Number Theory*, 2023. Version 3.0.0, https://flintlib.org.

YC04. Bo-Yin Yang and Jiun-Ming Chen. Theoretical analysis of XL over small fields. In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *Information Security and Privacy*, pages 277–288, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

YCBC07. Bo-Yin Yang, Owen Chia-Hsin Chen, Daniel J. Bernstein, and Jiun-Ming Chen. Analysis of QUAD. In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 290–308. Springer, Heidelberg, March 2007.

YDH+15. Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai. MQ challenge: Hardness evaluation of solving multivariate quadratic problems. In *NIST Workshop on Cybersecurity in a Post-Quantum World*, 2015. Washington, D.C. https://www.mqchallenge.org.