Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem

Magali Bardet[1,2], Pierre Briaud[1,3], Maxime Bros[4], Philippe Gaborit[4], and Jean-Pierre Tillich[1]

[1] Inria, 2 rue Simone Iff, 75012 Paris, France
[2] LITIS, University of Rouen Normandie, France
[3] Sorbonne Universités, UPMC Univ Paris 06
pierre.briaud@inria.fr
[4] Univ. Limoges, CNRS, XLIM, UMR 7252, F-87000 Limoges, France
maxime.bros@unilim.fr

Abstract. The Rank Decoding problem (RD) is at the core of rank-based cryptography. Cryptosystems such as ROLLO and RQC, which made it to the second round of the NIST Post-Quantum Standardization Process, as well as the Durandal signature scheme, rely on it or its variants. This problem can also be seen as a structured version of MinRank, which is ubiquitous in multivariate cryptography. Recently, [15,16] proposed attacks based on two new algebraic modelings, namely the MaxMinors modeling which is specific to RD and the Support-Minors modeling which applies to MinRank in general. Both improved significantly the complexity of algebraic attacks on these two problems. In the case of RD and contrarily to what was believed up to now, these new attacks were shown to be able to outperform combinatorial attacks and this even for very small field sizes.

However, we prove here that the analysis performed in [16] for one of these attacks which consists in mixing the MaxMinors modeling with the Support-Minors modeling to solve RD is too optimistic and leads to underestimate the overall complexity. This is done by exhibiting linear dependencies between these equations and by considering an $\mathbb{F}_{q^m}$ version of these modelings which turns out to be instrumental for getting a better understanding of both systems. Moreover, by working over $\mathbb{F}_{q^m}$ rather than over $\mathbb{F}_q$, we are able to drastically reduce the number of variables in the system and we (i) still keep enough algebraic equations to be able to solve the system, (ii) are able to analyze rigorously the complexity of our approach. This new approach may improve the older MaxMinors approach on RD from [15,16] for certain parameters. We also introduce a new hybrid approach on the Support-Minors system whose impact is much more general since it applies to any MinRank problem. This technique improves significantly the complexity of the Support-Minors approach for small to moderate field sizes.

Keywords: Post-quantum cryptography · NIST-PQC candidates · rank metric code-based cryptography · algebraic attack.

1 Introduction

Rank Metric Code-based Cryptography. Code-based cryptography using the rank metric, rank-based cryptography for short, started 30 years ago with the GPT cryptosystem [32] based on Gabidulin codes [31]. These codes can be viewed as analogues of Reed-Solomon codes in the rank metric, where polynomials are replaced by linearized polynomials. However this proposal and its variants were attacked with the Overbeck attack [46], much in the same way as McEliece schemes based on Reed-Solomon codes (or variants of them) have been attacked in [48,28].

Still, these attacks really exploited the strong algebraic structure of Gabidulin codes and did not rule out obtaining a secure version of the McEliece cryptosystem for the rank metric as we will see. One of the nice features of this metric is that it allows to exploit, in a much better way than the Hamming metric, codes which are linear over a very large extension field $\mathbb{F}_{q^m}$. Indeed, assume that we could come up with a code family which is able to decode a linear number of errors in the code length n and which would remain secure when used in a McEliece scheme. In the Hamming metric, the best algorithms for solving the decoding problem for a generic linear code are exponential in this regime in n, whereas they are exponential in $m \cdot n$ in the case of the rank metric. This would give cryptosystems with much smaller keysize in the rank metric case, which somehow mitigates the main drawback of the original McEliece proposal that is its large keysize. This dependency of the complexity exponent in the two parameters m and n also allows for much finer tuning of the parameters of such schemes.

A very significant step in this direction was made with the Low Rank Parity Check codes (LRPC) that were introduced in [34]. This type of codes made it possible to build McEliece schemes that can be viewed as the rank metric analogue of NTRU [40] in the Euclidean metric or of the MDPC cryptosystem in the Hamming metric [44], where the trapdoor is given by small weight vectors which allow efficient decoding. Contrarily to the GPT cryptosystem, this gives a cryptosystem whose security really relies on decoding an unstructured linear code and on distinguishing codes with moderate weight codewords from random linear codes. It can be argued that this second problem is similar in nature to the first one and so we have in a sense a cryptosystem whose security relies solely on the difficulty of generic decoding in the rank metric. This approach led to the design of several cryptosystems: [34,36,6,7], and in 2019, four rank-based schemes of this form [1,2,6,7] made it to the Second Round of the NIST Post-Quantum Standardization Process and were later merged into [8,4].

At the time of these submissions, the combinatorial attacks [45,35,11] were thought to be the most effective against these cryptosystems, especially for small q. However, it turned out later that algebraic attacks [15,16] could be improved a great deal and may be able to outperform the combinatorial attacks. This is the reason why these candidates were not kept for the Third Round, even if NIST still encourages further research on rank-based cryptography [5]. A first motivation is that these schemes still offer an interesting gain in terms of public-key size due to the algebraic structure. Another one is that the use of rank metric for wider cryptographic applications remains to be explored, and a first challenging task would already be the design of a competitive code-based signature scheme. Early attempts [10] based on the hash-and-sign paradigm and on structural masking where broken [29]. More recently, a promising approach, namely Durandal, adapting the Schnorr-Lyubashevsky framework to the rank metric, was proposed [9]. Its security proof relies on the hardness of two problems: the first one is the decoding problem in the rank metric with multiple instances sharing the same support (the so-called RSL problem), while the second one is a new assumption called the Product Spaces Subspaces Indistinguishability problem. The RSL problem was introduced in [33] and also studied in [14]. It may become instrumental to build more efficient rank-based primitives as shown by the recent work [43,21]. Finally, a third type of approach is to rely on the famous Stern's ZK identification protocol [49], which is turned into a signature scheme thanks to the Fiat-Shamir transform. The advantage of this technique is that it only relies on the hardness of decoding a random linear code: first, the security is well understood, and second one can use a seed to generate the public key. This method has already inspired a long sequence of optimizations and adaptations to the rank metric setting, see for instance [37,17,18].

Rank Decoding and MinRank Problems. Codes used in rank metric cryptography are linear codes over an extension field $\mathbb{F}_{q^m}$ of degree m of $\mathbb{F}_q$. An $\mathbb{F}_{q^m}$-linear code of length n is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$, but its codewords can also be viewed as matrices in $\mathbb{F}_q^{m \times n}$. Indeed, if $(\beta_1, \dots, \beta_m)$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$, the word $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$ corresponds to the matrix $\mathrm{Mat}(\boldsymbol{x}) = (X_{ij})_{i,j} \in \mathbb{F}_q^{m \times n}$, where $x_j = \beta_1 X_{1j} + \cdots + \beta_m X_{mj}$ for $j \in \{1..n\}$. The weight of $\boldsymbol{x}$ is then defined by using the underlying rank metric on $\mathbb{F}_q^{m \times n}$, namely $|\boldsymbol{x}| := \mathrm{rk}\,(\mathrm{Mat}\,(\boldsymbol{x}))$, and it is also equal to the dimension of the support $\mathrm{Supp}(\boldsymbol{x}) := \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q}$. Similarly to the Hamming metric, the main source of computational hardness for rank-based cryptosystems is a decoding problem. It is the decoding problem in rank metric restricted to $\mathbb{F}_{q^m}$-linear codes, namely

Problem 1 ((m, n, k, r) Rank Decoding problem (RD)).
The Rank Decoding problem of parameters (m, n, k, r) is given by

Input: an $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C}$ of $\mathbb{F}_{q^m}^n$, an integer $r \in \mathbb{N}$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{y} - \boldsymbol{c}| \le r$ for some $\boldsymbol{c} \in \mathcal{C}$.

Output: $\boldsymbol{c} \in \mathcal{C}$ and an error $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ and $|\boldsymbol{e}| \le r$.

Given $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ a parity-check matrix of an $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$, the syndrome version, denoted by RSD for Rank Syndrome Decoding, asks to find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal$ and $|\boldsymbol{e}| \le r$, and it is equivalent to RD. Even if RD is not known to be NP-complete, there is a randomized reduction from RD to an NP-complete problem [38], namely to decoding in the Hamming metric. An RD instance can also be viewed as a structured instance of the following inhomogeneous MinRank problem.

Problem 2 (Inhomogeneous (m, n, K, r) MinRank problem).
The MinRank problem with parameters (m, n, K, r) is given by
Input: an integer $r \in \mathbb{N}$ and $K + 1$ matrices $\boldsymbol{M}_0, \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$.
Output: field elements $x_1, x_2, \ldots, x_K \in \mathbb{F}_q$

$$\mathrm{rk}\left(\boldsymbol{M}_0 + \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

More precisely, there exists a reduction from RD to the MinRank problem [30]. The latter was defined and proven NP-complete in [23], and it is now ubiquitous in multivariate cryptography [41,47,24,51,19,50,13,20]. In the cryptographically relevant regime, the current best known algorithms to solve it are algebraic attacks which all have exponential complexity.

Solving RD. First, note that owing to the aforementioned reduction [30], all the methods for solving MinRank can be applied to the RD problem. However, a plain MinRank solver would not be the most suitable as it forgets the $\mathbb{F}_{q^m}$-linear structure inherent to RD. In particular, the first attacks specific to the RD problem were of combinatorial nature [25]. They were significantly improved in [45] and further refined in [35,12]. These works can be viewed as the continuation of the former Goubin's kernel attack on generic MinRank [39], which consists of first guessing sufficiently many vectors in the kernel of the rank r matrix and then solving a linear system. The considerable difference in the case of RD is that the success probability of this guess can be greatly increased thanks to the $\mathbb{F}_{q^m}$-linearity. Another way to solve RD is provided by algebraic attacks which are not plain MinRank attacks [42,35]. These techniques were considered to be less efficient than the combinatorial ones for a long time, especially for small values of q. In particular, the parameters of the rank based NIST submissions [6,7,2] were chosen according to the best combinatorial attacks. However, a breakthrough paper [15] showed how the $\mathbb{F}_{q^m}$-linear structure of the problem could be used to devise a dedicated and more efficient algebraic attack based on the so-called MaxMinors modeling. This was further improved in [16], which also introduced another algebraic modeling, the so-called Support-Minors modeling. Support-Minors is a generic MinRank modeling but it can be combined with MaxMinors in order to solve the RD problem. In particular, this thread of work contributed to significantly break the proposed parameters for ROLLO and RQC, and these rank-based schemes have not passed the Second Round of the NIST PQC competition.

The MaxMinors modeling [15,16]. The attack introduced in [15] relies on the following observations

- a vector $\boldsymbol{u} \in \mathbb{F}_{q^m}^n$ is of rank r iff its entries generate a subspace of $\mathbb{F}_{q^m}$ of dimension r, say $\langle s_1, \cdots, s_r \rangle_{\mathbb{F}_q}$. In such a case, there exists $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that
$$\boldsymbol{u} = (s_1, \cdots, s_r)\boldsymbol{C}.$$

– Let $(\boldsymbol{c}, \boldsymbol{e})$ be the solution to RD. There exists $s_1, \cdots, s_r \in \mathbb{F}_{q^m}$ and $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{y} - \boldsymbol{c} = (s_1, \cdots, s_r)\boldsymbol{C}$, because $\boldsymbol{y} - \boldsymbol{c} = \boldsymbol{e}$ is of rank $\leq r$. If we bring in a parity check matrix $\boldsymbol{H}_{\boldsymbol{y}} \in \mathbb{F}_{q^m}^{(n-k-1)\times n}$ of the extended code $\mathcal{C} + \langle \boldsymbol{y} \rangle$ then we have

$$(s_1, \cdots, s_r)\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}} = 0.$$

This implies that the $r \times (n-k-1)$ matrix $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}}$ is not of full rank and that all its maximal minors are equal to 0. By using the Cauchy-Binet formula (3), each of these maximal minors can be expressed as a linear combination of the maximal minors c_T of the matrix $\boldsymbol{C}$. Here c_T denotes the maximal minor equal to the determinant of the square submatrix of $\boldsymbol{C}$ whose column indexes belong to $T \subset \{1..n\}$, $\#T = r$. Overall, the relevant system is a linear system in $\binom{n}{r}$ unknowns, the c_T's, and $m\binom{n-k-1}{r}$ linear equations. This last m factor in the number of equations comes from the fact that initially there are $\binom{n-k-1}{r}$ minors equal to 0, hence $\binom{n-k-1}{r}$ linear equations with coefficients in $\mathbb{F}_{q^m}$ whereas the c_T's belong to $\mathbb{F}_q$. We denote this modeling by MM-$\mathbb{F}_{q^m}$, and from there it is easy to derive a second system MM-$\mathbb{F}_q$ which contains m times more linear equations over $\mathbb{F}_q$.

The precise definition of the two modelings follows. The notation for Modeling 2 are defined in Section 2.

Modeling 1 (MM-$\mathbb{F}_{q^m}$)

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}}) = \left\{ P_J := \left|\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}}\right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\} \tag{MM-$\mathbb{F}_{q^m}$}$$

Unknowns: $\binom{n}{r}$ *variables* $c_T := |\boldsymbol{C}|_{*,T} \in \mathbb{F}_q$, $T \subset \{1..n-k+1\}$, $\#T = r$,
Equations: $\binom{n-k-1}{r}$ *equations* $P_J = 0$, $J \subset \{1..n-k-1\}$, $\#J = r$ *viewed as linear equations over* $\mathbb{F}_{q^m}$ *in the* c_T*'s.*

Modeling 2 (MM-$\mathbb{F}_q$)

$$\begin{aligned} &\text{Unfold}(\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}})) = \\ &\{P_{i,J} := \text{Tr}(\beta_i^\star P_J) \mod I_q : J \subset \{1..n-k-1\},\ \#J = r,\ i \in \{1..m\}\} \end{aligned} \tag{MM-$\mathbb{F}_q$}$$

Unknowns: $\binom{n}{r}$ *variables* $c_T := |\boldsymbol{C}|_{*,T} \in \mathbb{F}_q$, $T \subset \{1..n\}$, $\#T = r$,
Equations: $m\binom{n-k-1}{r}$ *equations* $P_{i,J} = 0$*, which are linear over* $\mathbb{F}_q$ *in the* c_T*'s. Here* I_q *is the ideal generated by all the field equations* $c_T^q - c_T$*'s.*

If $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$, the value of the c_T's may be found by solving the linear system MM-$\mathbb{F}_q$. This is the so-called <u>overdetermined</u> case in [16]. Otherwise, in the <u>underdetermined</u> case, one can adopt a form of hybrid approach by adding random linear constraints on the variables to obtain another linear system that can be solved.

The Support-Minors modeling [16]. An alternative method in the underdetermined case is to rely on the Support-Minors modeling which was introduced in [16]. The Support-Minors modeling is a generic MinRank modeling which is not specific to the RD problem and which can be quite effective in a certain parameter range. In particular, it turned out to be instrumental for breaking the third round or alternate third round multivariate finalists Rainbow and GeMSS of the NIST competition [19,20,50,13]. Applied to the specific RD case, Support-Minors can be explained as follows. First, rewrite $\boldsymbol{y} - \boldsymbol{c} = (s_1, \cdots, s_r)\boldsymbol{C}$ in a matrix form. On the one hand, the matrix $\mathrm{Mat}\left((s_1, \cdots, s_r)\boldsymbol{C}\right)$ is readily seen to be equal to $\boldsymbol{SC}$ where $\boldsymbol{S} := \mathrm{Mat}\left(s_1, \cdots, s_r\right)$ and therefore we have

$$\mathrm{Mat}\left(\boldsymbol{y} + \boldsymbol{xG}\right) = \boldsymbol{SC}, \tag{1}$$

where $\boldsymbol{G}$ is a generator matrix of $\mathcal{C}$, $\boldsymbol{x} = (x_1, \cdots, x_k) \in \mathbb{F}_{q^m}^k$ and $-\boldsymbol{c} = \boldsymbol{xG}$. On the other hand, Equation (1) implies that any row $\boldsymbol{r}_i$ of $\mathrm{Mat}\left(\boldsymbol{y} + \boldsymbol{xG}\right)$ is in the row space of $\boldsymbol{C}$ and therefore all the maximal minors of the matrix $\begin{pmatrix} \boldsymbol{r}_i \\ \boldsymbol{C} \end{pmatrix}$ are equal to 0. Also, it is straightforward to check that row $\boldsymbol{r}_i$ in $\mathrm{Mat}\left(\boldsymbol{y} + \boldsymbol{xG}\right)$ is a vector whose components are linear forms in the $x_{i,j}$'s which are the entries of $\mathrm{Mat}\left(\boldsymbol{x}\right)$. By performing Laplace expansion of any such maximal minor with respect to the first row, this minor can be written as a bilinear polynomial in the $x_{i,j}$'s on the one hand and the maximal minors c_T of $\boldsymbol{C}$ on the other hand. This gives a bilinear system SM-$\mathbb{F}_q$, which as explained above, is not specific to the RD problem: we obtain a similar system for generic MinRank whose x_i variables (coefficients in the rank $\leq r$ linear combination) play the role of our $x_{i,j}$'s. Following the terminology of [16], we call these $x_{i,j}$ variables <u>linear</u> variables and the c_T's the <u>minor</u> variables.

Modeling 3 (SM-$\mathbb{F}_q$) *Applied to an RD instance, the SM Modeling from [16] is the system*

$$\left\{ Q_{i,I} := \left| \begin{pmatrix} \boldsymbol{r}_i \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1, i \in \{1..m\}, \boldsymbol{r}_i = \mathrm{Mat}(\boldsymbol{y} + \boldsymbol{xG})_{i,*} \right\} \tag{SM-$\mathbb{F}_q$}$$

Unknowns: $\binom{n}{r}$ *variables* $c_T \in \mathbb{F}_q$, $k \cdot m$ *variables* $x_{j,j'} \in \mathbb{F}_q$, $j \in \{1..m\}$, $j' \in \{1..k\}$,
Equations: $m\binom{n}{r+1}$ *equations* $Q_{i,I} = 0$ *which are affine bilinear polynomials over* $\mathbb{F}_q$ *in the* $x_{j,j'}$*'s and in the* c_T*'s.*

If there are more linearly independent equations than bilinear monomials, the system may be solved by linearization (i.e. by replacing the monomials by single variables and then obtaining the values of these variables from solving the resulting linear system). Otherwise, the authors propose a dedicated technique to solve at higher degree by multiplying the SM-$\mathbb{F}_q$ equations by monomials of degree $b-1$ in the linear variables to obtain equations of degree b in the linear variables and degree 1 in the c_T's . This amounts to constructing the bi-degree

$(b,1)$ Macaulay matrix $\boldsymbol{M}_b(\text{SM-}\mathbb{F}_q)$ whose columns are indexed by the $\mathcal{M}_b$ bi-degree $(b,1)$ monomials and then to finding a non-trivial element in the right kernel of this matrix. This approach works if the rank of $\boldsymbol{M}_b(\text{SM-}\mathbb{F}_q)$ is $|\mathcal{M}_b|-1$, so that the solution space is one-dimensional and allows to recover the original solution to the MinRank problem. The complexity of the attack is then dominated by the one of solving the system at bi-degree $(b,1)$, and for this it can be beneficial to use the Wiedemann algorithm as the Macaulay matrix is sparse enough for large values of b.

Solving RD by combining MaxMinors and Support-Minors. Recall that in the particular RD case we obtained two algebraic systems involving the same c_T variables, namely the MaxMinors system MM-$\mathbb{F}_q$ and the Support-Minors system SM-$\mathbb{F}_q$. This suggests to combine both modelings by multiplying the MaxMinors equations by degree b monomials in the linear variables and the Support-Minors equations by degree $b-1$ monomials in the linear variables to get equations of bi-degree $(b,1)$. In [16], it was implicitly assumed that the MaxMinors and the Support-Minors systems behave independently at higher degree, namely $\text{rk}(\boldsymbol{M}_b(\text{SMM-}\mathbb{F}_q)) = \text{rk}(\boldsymbol{M}_b(\text{MM-}\mathbb{F}_q)) + \text{rk}(\boldsymbol{M}_b(\text{SM-}\mathbb{F}_q))$ when this number is smaller than $\mathcal{M}_b$ which is the number of bi-degree $(b,1)$ monomials. Here $\boldsymbol{M}_b(\text{MM-}\mathbb{F}_q)$ and $\boldsymbol{M}_b(\text{SMM-}\mathbb{F}_q)$ respectively denote the Macaulay matrices of the MaxMinors system multiplied by the monomials of degree b in the linear variables and the vertical join of $\boldsymbol{M}_b(\text{MM-}\mathbb{F}_q)$ and $\boldsymbol{M}_b(\text{SM-}\mathbb{F}_q)$. While it is trivial to estimate $\text{rk}(\boldsymbol{M}_b(\text{MM-}\mathbb{F}_q))$ as the MaxMinors equations MM-$\mathbb{F}_q$ are linear in the other block of variables, note that the value obtained in [16] for $\text{rk}(\boldsymbol{M}_b(\text{SM-}\mathbb{F}_q))$ is based on much more involved combinatorial arguments and remains conjectural.

Contributions. Most of our work concerns the aforementioned combined approach on the Rank Decoding Problem but some of our results will also apply to the Support-Minors strategy of [16] on non-structured MinRank instances.

First, in this combined RD approach, we show that the implicitly assumed relation $\text{rk}(\boldsymbol{M}_b(\text{SMM-}\mathbb{F}_q)) = \text{rk}(\boldsymbol{M}_b(\text{MM-}\mathbb{F}_q)) + \text{rk}(\boldsymbol{M}_b(\text{SM-}\mathbb{F}_q))$ does not hold. Indeed, there are linear dependencies between the two systems: in particular, we will prove that the MaxMinors equations and some multiples are included in the vector space generated by the Support-Minors equations. We will prove this by considering the "$\mathbb{F}_{q^m}$-version" of both systems. For MaxMinors, this is nothing but the original MaxMinors system MM-$\mathbb{F}_{q^m}$ with coefficients over $\mathbb{F}_{q^m}$. For the $\mathbb{F}_{q^m}$-Support-Minors modeling, this $\mathbb{F}_{q^m}$-version comes from a slight variation of the argument used in [16] for obtaining the Support-Minors modeling. Instead of considering the matrix version of

$$\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G} = (s_1, \cdots, s_r)\boldsymbol{C}, \tag{2}$$

we can directly use this equation to argue that the vector $\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G}$ is in the row space of $\boldsymbol{C}$, which in turn implies that all the maximal minors of the matrix

$\begin{pmatrix} \boldsymbol{y} + \boldsymbol{x}\boldsymbol{G} \\ \boldsymbol{C} \end{pmatrix}$ are equal to 0. By performing Laplace expansion of these minors according to the first row, we obtain in this way $\binom{n}{r+1}$ equations which are bilinear in the entries x_i of $\boldsymbol{x}$ (we still call them the linear variables) and in the maximal minors c_T of $\boldsymbol{C}$:

Modeling 4 (SM-$\mathbb{F}_{q^m}$)

$$\left\{ Q_I := \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\} \qquad (\text{SM-}\mathbb{F}_{q^m})$$

Unknowns: $\binom{n}{r}$ *variables* $c_T \in \mathbb{F}_q$, k *variables* $x_1, \ldots, x_k \in \mathbb{F}_{q^m}$,
Equations: $\binom{n}{r+1}$ *equations* $Q_I = 0$ *for* $I \subset \{1..n\}$, $\#I = r+1$, *viewed as affine bilinear equations over* $\mathbb{F}_{q^m}$ *in the* x_i*'s on the one hand and in the* c_T*'s on the other hand.*

This SM-$\mathbb{F}_{q^m}$ system presents the advantage of being much more compact than the original Support-Minors modeling: the number of linear variables is divided by m (but the unknowns are now in $\mathbb{F}_{q^m}$) and the number of equations is also divided by m. Also, this reduced system will be very handy to study the aforementioned linear dependencies, see Section 3:

(i) it is readily seen that the Support-Minors equations are the result of the Unfold operation applied to these SM-$\mathbb{F}_{q^m}$ equations;
(ii) it is easier to exhibit linear dependencies between the equations in MM-$\mathbb{F}_{q^m}$ and SM-$\mathbb{F}_{q^m}$, which in turn yield linear dependencies between the MaxMinors and the Support-Minors equations over $\mathbb{F}_q$.

This is not the only advantage in considering SM-$\mathbb{F}_{q^m}$ instead of the original Support-Minors equations. It will namely be easier to understand the linear dependencies in the SM-$\mathbb{F}_{q^m}$ equations themselves (which also exist as we will show). Moreover, the very fact that the number of linear variables has shrunk a great deal suggests that instead of using the linearization strategy followed in [16], it might be much more favorable to

(i) use the linear equations linking the minor variables c_T from unfolding MM-$\mathbb{F}_{q^m}$ (the MM-$\mathbb{F}_q$ linear system) equations to substitute for some of them in SM-$\mathbb{F}_{q^m}$ and decrease the number of minor variables in it to obtain a new bilinear system SM-$\mathbb{F}_{q^m}^+$;
(ii) multiply these equations by monomials of degree $b-1$ in the linear variables x_i to obtain a new bi-degree $(b, 1)$ system with a reduced number of bi-degree $(b, 1)$ monomials and choose b large enough so that the linearizing strategy is able to recover the values of these bi-degree $(b, 1)$ monomials.

We call this the "attack over $\mathbb{F}_{q^m}$"and we describe it in Section 4.

Modeling 5 (SM-$\mathbb{F}_{q^m}^+$ over $\mathbb{F}_{q^m}$)

$$\textit{SM-}\mathbb{F}_{q^m}^+ := \textit{SM-}\mathbb{F}_{q^m} \mod (\textit{MM-}\mathbb{F}_q) \qquad (\text{SM-}\mathbb{F}_{q^m}^+)$$

Unknowns: $\binom{n}{r} - m\binom{n-k-1}{r}$ *variables* $c_T \in \mathbb{F}_q$*,* k *unknowns* $x_1, \cdots, x_k$ *in* $\mathbb{F}_{q^m}$*.*
Equations: $\binom{n}{r+1} - \binom{n-k-1}{r+1} - (k+1)\binom{n-k-1}{r}$ *equations of the form* $\widetilde{Q_I} = 0$ *with* $I \subset \{1..n\}$*,* $\#I = r+1$*,* $\#(I \cap \{1..k+1\} \geq 2)$*, where* $\widetilde{Q_I} = \mathrm{NF}(Q_I, \langle P_{i,J} \rangle)$ *is the* Q_I *equation with* c_T *variables removed using MM-*$\mathbb{F}_q$*.*

Second, we show how this "attack over $\mathbb{F}_{q^m}$" and more generally any Support-Minors based MinRank attack may benefit from a hybrid approach similar to the one presented in [16, §4.3] on MaxMinors. There, it was used to decrease the number of minor variables. However, we will show that in our case where we consider systems with minor and linear variables, this hybrid technique has the additional benefit of decreasing the number of linear variables. Roughly speaking, our approach is to associate to a given instance of MinRank (resp. RD) $q^{a \cdot r}$ new MinRank instances (resp. RD instances) with (apparently) the same parameters, for which we know that one of them has its rank r matrix $\boldsymbol{M}$ equal to zero on a fixed set of $a \geq 0$ columns. On any of these instances and by starting from the initial modeling, we hope to find a solution of this particular form by (i) writing that $\binom{n}{r} - \binom{n-a}{r}$ minors c_T should be equal to 0, namely all those that involve one of these a columns (ii) writing $a \cdot m$ linear relations between the linear variables which correspond to the $a \cdot m$ zero entries of $\boldsymbol{M}$. All in all, we may attack a MinRank problem of parameters (m, n, K, r) by performing $q^{a \cdot r}$ attacks on smaller instances with parameters $(m, n-a, K-a \cdot m, r)$ and such that only one of them has a solution. This is much more efficient than the straightforward hybrid approach suggested in [16, §5.5] which consists in fixing a few linear variables and which results only at best in a marginal gain in the complexity. Here, the gain in complexity is much more significant as shown in Subsection 6.1. On a deeper level, our approach also allows to interpolate between the former combinatorial attacks [39] and the algebraic attacks (in particular the plain Support-Minors attack).

2 Notation and preliminaries

Vectors are denoted by lower case boldface letters such as $\boldsymbol{x}$, $\boldsymbol{e}$ and matrices by upper case letters $\boldsymbol{G}$, $\boldsymbol{M}$. The all-zero vector of length ℓ is denoted by $\mathbf{0}_\ell$. The j-th coordinate of a vector $\boldsymbol{x}$ is denoted by x_j and the submatrix of a matrix $\boldsymbol{M}$ formed from the rows in I and columns in J is denoted by $\boldsymbol{M}_{I,J}$. When I (resp. J) consists of all the rows (resp. columns), we may use the notation $\boldsymbol{M}_{*,J}$ (resp. $\boldsymbol{M}_{I,*}$). Similarly, we simplify $\boldsymbol{M}_{i,*} = \boldsymbol{M}_{\{i\},*}$ (resp. $\boldsymbol{M}_{*,j} = \boldsymbol{M}_{*,\{j\}}$) for the i-th row of $\boldsymbol{M}$ (resp. j-th column of $\boldsymbol{M}$) and $\boldsymbol{M}_{i,j} = \boldsymbol{M}_{\{i\},\{j\}}$ for the entry in row i and column j. Finally, $|\boldsymbol{M}|$ is the determinant of a matrix $\boldsymbol{M}$, $|\boldsymbol{M}|_{I,J}$ is the determinant of the submatrix $\boldsymbol{M}_{I,J}$ and $|\boldsymbol{M}|_{*,J}$ the one of $\boldsymbol{M}_{*,J}$.

We will intensively use the Cauchy-Binet formula that expresses the determinant of the product of two matrices $A \in \mathbb{K}^{r \times n}$ and $B \in \mathbb{K}^{n \times r}$ as

$$|AB| = \textstyle\sum_{T \subset \{1..n\}, \#T = r} |A|_{*,T} \, |B|_{T,*}. \tag{3}$$

The notation $\{1..n\}$ stands for the set of integers from 1 to n, and for any subset $J \subset \{k+1..n\}$, we denote by $J-k$ the set $J-k = \{j-k : j \in J\} \subset \{1..n-k\}$.

For q a prime power and $m \geq 1$ an integer, let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_{q^m}$ be the extension of $\mathbb{F}_q$ of degree m. For $x \in \mathbb{F}_{q^m}$ and $0 \leq \ell \leq m-1$, we write $x^{[\ell]} := x^{q^\ell}$ for the ℓ-th Frobenius iterate of x, and this notation is extended to matrices component by component, namely $\boldsymbol{M}^{[\ell]} := \left(\boldsymbol{M}_{i,j}{}^{[\ell]}\right)_{i,j}$. We also make use of the trace operator which is the $\mathbb{F}_q$-linear mapping from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined by

$$\operatorname{Tr}(x) := x + x^q + \cdots + x^{q^{m-1}} = \sum_{\ell=0}^{m-1} x^{[\ell]}.$$

In the whole paper, we consider a fixed basis $\boldsymbol{\beta} := (\beta_1, \ldots, \beta_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The dual basis $\boldsymbol{\beta}^\star := (\beta_1^\star, \ldots, \beta_m^\star)$ of $\boldsymbol{\beta}$ is defined by

$$\operatorname{Tr}(\beta_i \beta_j^\star) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}.$$

Note that for any decomposition in $\boldsymbol{\beta}$ of the form $x = \sum_{i=1}^m x_i \beta_i \in \mathbb{F}_{q^m}$ and any $i \in \{1, \cdots, m\}$, we can recover

$$\operatorname{Tr}(\beta_i^\star x) = x_i. \tag{4}$$

For a vector $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{F}_{q^m}^n$ we denote by $\operatorname{Tr}(\boldsymbol{x})$ the vector $(\operatorname{Tr}(x_i))_{1 \leq i \leq n}$ where the trace is applied componentwise, and for any matrix $\boldsymbol{M} \in \mathbb{F}_{q^m}^{b \times c}$ we denote by $\operatorname{Tr}(\boldsymbol{M}) = (\operatorname{Tr}(\boldsymbol{M}_{i,j}))_{i,j}$. It will be helpful to notice that, thanks to the linearity of Tr over $\mathbb{F}_q$,

$$\operatorname{Tr}(\beta_i^\star \boldsymbol{x}) = \operatorname{Mat}(\boldsymbol{x})_{i,*} \qquad \forall i \in \{1, \cdots, m\}, \tag{5}$$

$$\operatorname{Tr}(\boldsymbol{C}\boldsymbol{M}) = \boldsymbol{C} \operatorname{Tr}(\boldsymbol{M}) \qquad \text{if } \boldsymbol{C} \in \mathbb{F}_q^{a \times b}, \boldsymbol{M} \in \mathbb{F}_{q^m}^{b \times c}. \tag{6}$$

When looking for solutions of a polynomial system in $\mathbb{F}_q$ with coefficients in $\mathbb{F}_{q^m}$, it will be helpful to notice that for $f(\boldsymbol{z}) \in \mathbb{F}_{q^m}[z_1, \cdots, z_N]$ and $\boldsymbol{x} = (x_1, \cdots, x_N) \in \mathbb{F}_q^N$, we have:

$$f(x_1, \cdots, x_N) = 0 \Longleftrightarrow \forall i \in \{1, \cdots, m\},\ \operatorname{Tr}(\beta_i^\star f(\boldsymbol{x})) = 0. \tag{7}$$

This motivates to define the "unfolding" operation which associates to an algebraic system $\mathcal{F} := \{f_1, \ldots, f_M\} \subset \mathbb{F}_{q^m}[z_1, \ldots, z_N]$ with coefficients in $\mathbb{F}_{q^m}$ an equivalent algebraic system over $\mathbb{F}_q$ which defines the same variety over $\mathbb{F}_q$. We call it the associated unfolded system:

$$\operatorname{Unfold}(\{f_1, \ldots, f_M\}) := \{\operatorname{Tr}(\beta_i^\star f_j) \mod I_q : 1 \leq i \leq m, 1 \leq j \leq M\} \in \mathbb{F}_q[\boldsymbol{z}]^{M \cdot m}, \tag{8}$$

where we reduce the polynomials modulo the field equations, i.e. $I_q := \langle z_1^q - z_1, \ldots, z_N^q - z_N \rangle$. For one single polynomial $f(\boldsymbol{z}) = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^N} a_{\boldsymbol{\alpha}} \boldsymbol{z}^{\boldsymbol{\alpha}} \in \mathbb{F}_{q^m}[\boldsymbol{z}]$, this reduction process reads

$$\mathrm{Tr}(\beta_i^\star f(\boldsymbol{z})) \mod I_q = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^N} \mathrm{Tr}(\beta_i^\star a_{\boldsymbol{\alpha}}) \boldsymbol{z}^{\boldsymbol{\alpha}} \in \mathbb{F}_q[\boldsymbol{z}]. \tag{9}$$

In other words, this results in applying the function $x \mapsto \mathrm{Tr}(\beta_i^\star x)$ to each coefficient of the polynomial. It is clear that the solutions to $\mathcal{F}$ in $\mathbb{F}_q^N$ are exactly the solutions to Unfold($\mathcal{F}$) in $\mathbb{F}_q^N$ and that any solution to Unfold($\mathcal{F}$) in any extension field of $\mathbb{F}_q$ is a solution to $\mathcal{F}$. However, note that it may be the case that $\mathcal{F}$ has more solutions than Unfold($\mathcal{F}$) in some extension field. [5]

For the different results in the paper, we consider a particular monomial ordering on our two sets of variables $x_1, \ldots, x_k$ and c_T's for any subset T of size r. The c_T's are ordered lexicographically according to T: $c_{T'} > c_T$ if $t'_j = t_j$ for $j < j_0$ and $t'_{j_0} > t_{j_0}$ where $T = \{t_1 < \cdots < t_r\}$ and $T' = \{t'_1 < \cdots < t'_r\}$. We then choose a grevlex monomial ordering $x_1 > \cdots > x_k > c_T$. Finally, we denote by LT(f) the leading term of a polynomial f with respect to this term order.

3 MaxMinors and Support-Minors systems for RD instances

In this section, we analyse the two RD modelings over $\mathbb{F}_{q^m}$ which take advantage of the underlying extension field structure, namely the MaxMinors (MM-$\mathbb{F}_{q^m}$) and the Support-Minors (SM-$\mathbb{F}_{q^m}$) systems.

The (MM-$\mathbb{F}_{q^m}$) system was already described in [15,16] and recalled in the introduction. The particular form of the MM-$\mathbb{F}_{q^m}$ equations P_J as linear equations comes from the fact that these P_J's can be expressed in terms of the maximal minors of $\boldsymbol{C}$ by using the Cauchy-Binet formula (3). Actually, we also use implicitly the Plücker coordinates associated to the vector space generated by the rows of $\boldsymbol{C}$ by defining new variables $c_T = |\boldsymbol{C}|_{*,T}$, see [22, p.6]. For $N = \binom{n}{r} - 1$ and $P^N(\mathbb{F}_q) = P(\mathbb{F}_q^{N+1})$ the projective space, the Plücker map is defined by

$$\begin{aligned} p : \{\mathcal{W} \subset \mathbb{F}_q^n : \dim(\mathcal{W}) = r\} &\to \mathbb{P}^N(\mathbb{F}_q) \\ \boldsymbol{C} &\mapsto (c_T)_{T \subset \{1..n\}, \#T = r} \end{aligned}$$

where $\boldsymbol{C}$ is any matrix whose rows generate the vector space $\mathcal{W}$. The benefit of introducing such coordinates to describe a vector space $\mathcal{W}$ is that it has unique Plücker coordinates associated to it. On the contrary, this is not the case if one uses the matrix representation of such a vector space: indeed, if the

[5] For instance in $\mathbb{F}_{q^2}$, $f = \beta_1 z_1 + \beta_2 z_2$ admits all multiples of $(\beta_2/\beta_1, 1)$ as solution, whereas Unfold(f) $= \{z_1, z_2\}$ admits only $(0,0)$ as a solution in the algebraic closure of $\mathbb{F}_{q^2}$.

rows of $\boldsymbol{C}$ generate $\mathcal{W}$, then the rows of $\boldsymbol{AC}$ also generate $\mathcal{W}$ for any invertible $\boldsymbol{A} \in GL(r, \mathbb{F}_q)$. For our algebraic system, this brings the benefit of reducing the number of solutions: there are several solutions $\boldsymbol{C}$ to the initial equation (2) but there are unique Plücker coordinates. As already pointed out in [16], it is also extremely beneficial for the computation to replace polynomials $|\boldsymbol{C}|_{*,T}$ with $r!$ terms of degree r in the entries of $\boldsymbol{C}$ by single variables c_T's in $\mathbb{F}_q$. Our second set of equations, namely the (SM-$\mathbb{F}_{q^m}$) system, was also described in the introduction. The particular bilinear shape of these polynomials in the linear and in the minor variables follows by applying Laplace expansion along the first row $\boldsymbol{xG}+\boldsymbol{y}$ of $\begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix}$. Recall also that these minor variables c_T are searched over $\mathbb{F}_q$ while the linear variables x_j are searched over $\mathbb{F}_{q^m}$. In particular, as the MM-$\mathbb{F}_{q^m}$ equations are over $\mathbb{F}_{q^m}$ but linear in these c_T variables, it is possible to generate m times more linear equations in the same variables by forming the unfolded system MM-$\mathbb{F}_q$ = Unfold(MM-$\mathbb{F}_{q^m}$) as already explained in Section 2. While these MM-$\mathbb{F}_{q^m}$ equations are proven to be linearly independent in [16], it is only conjectured that the resulting MM-$\mathbb{F}_q$ equations are linearly independent with overwhelming probability.

In Section 3.1, we show that the two systems over $\mathbb{F}_{q^m}$ described above are not independent: the MM-$\mathbb{F}_{q^m}$ equations are actually included in SM-$\mathbb{F}_{q^m}$; thus, adding the MM-$\mathbb{F}_q$ equations to the SM-$\mathbb{F}_q$ system does not help to solve RD in the underdetermined case as stated in [16]. Also, SM-$\mathbb{F}_{q^m}$ is an interesting modeling in itself to attack the RD problem as it consists of more compact equations over the extension field $\mathbb{F}_{q^m}$. Moreover, we are able to formally prove the linear independence of these equations and more generally the exact dimension of the vector space generated by them at each bi-degree $(b, 1)$ for any $b \geq 1$, which is clearly the key quantity to evaluate the cost such an attack.

However, we show that it is not possible to solve the system by using only these equations over $\mathbb{F}_{q^m}$, even at high bi-degree $(b, 1)$. Finally, note that it is also possible to unfold the SM-$\mathbb{F}_{q^m}$ equations over $\mathbb{F}_q$ but at the cost of multiplying the number of linear variables by a factor m as we also need to express each $x_j = \sum_{i=1}^{m} x_{i,j}\beta_i$ in $\mathbb{F}_{q^m}$ as m times more variables over $\mathbb{F}_q$. In Section 3.2, we show that the result of this operation is nothing more than the system (SM-$\mathbb{F}_q$) which is the Support Minors Modeling of [16] applied to an RD instance, namely SM-$\mathbb{F}_q$ = Unfold(SM-$\mathbb{F}_{q^m}$). In Proposition 5, we also give a proof for the number of linearly independent equations in SM-$\mathbb{F}_q$ that are not in MM-$\mathbb{F}_q$ and which can be seen as the extra information brought by Support-Minors.

For the sake of clarity, most of the proofs are postponed in Appendix A.

3.1 MaxMinors and Support-Minors modelings over $\mathbb{F}_{q^m}$.

In what follows, we always consider RD instances with a unique solution and whose rank weight is exactly r instead of $\leq r$ (we may assume this as trying all the weights smaller than r adds at most a polynomial factor in the total complexity). Let $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ be a full-rank generator matrix of a linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_{q^m}$, and let $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$ be the received word affected by an error of weight r. With our assumption, the decoding problem amounts to finding the unique codeword $\boldsymbol{xG}$ such that the weight of $\boldsymbol{xG}+\boldsymbol{y}$ is r.

In this section, we analyze the link between the SM-$\mathbb{F}_{q^m}$ equations and the MM-$\mathbb{F}_{q^m}$ equations. To this end, we first separate the equations into different sets by defining for nonnegative integers $s,\ i \in \{1..k\}$:

$$\begin{aligned}
\mathcal{Q}_s &= \{Q_I : I \subset \{1..n\},\ \#I = r+1,\ \#(I \cap \{1..k+1\}) = s\},\\
\mathcal{Q}_{\geq s} &= \{Q_I : I \subset \{1..n\},\ \#I = r+1,\ \#(I \cap \{1..k+1\}) \geq s\},\\
\mathcal{P} &= \{P_J : J \subset \{1..n-k-1\},\ \#J = r\},\\
x_i\mathcal{P} &:= \{x_i P : P \in \mathcal{P}\}.
\end{aligned}$$

We are going to prove the following relations, where $\langle \cdot \rangle_{\mathbb{F}_q}$ means the vector space generated over $\mathbb{F}_q$:

$$\begin{aligned}
\mathcal{Q}_0 &\subset \langle \mathcal{Q}_1, \mathcal{Q}_{\geq 2}\rangle_{\mathbb{F}_q} && \text{(Proposition 1)}\\
\langle \mathcal{P}, x_i\mathcal{P} : i \in \{1..k\}, \mathcal{Q}_{\geq 2}\rangle_{\mathbb{F}_q} &= \langle \mathcal{Q}_1, \mathcal{Q}_{\geq 2}\rangle_{\mathbb{F}_q} && \text{(Proposition 3)}\\
\mathcal{P}, x_i\mathcal{P} : i \in \{1..k\}, \mathcal{Q}_{\geq 2} &\text{ are linearly independent over } \mathbb{F}_q && \text{(Proposition 2)}
\end{aligned}$$

The consequence is that if we linearize the (affine) SM-$\mathbb{F}_{q^m}$ system, we get several reductions to zero and also $\binom{n-k-1}{r}$ degree falls[6] that give the P_J's equations. If we then eliminate c_T variables using those linear equations, we get new reductions to zero which correspond to the $x_i P_J$'s. More generally, Proposition 4 tackles the augmented bi-degree $(b, 1)$ case by giving the number of linearly independent Q_I equations for any $b \geq 1$ and without any particular assumption. For all these propositions, it will be helpful to notice that

Fact 1 *Without loss of generality (up to a permutation of coordinates), we can assume that $\boldsymbol{G}$ is in systematic form, i.e. $\boldsymbol{G} = \begin{pmatrix}\boldsymbol{I}_k & *\end{pmatrix}$, that $\boldsymbol{y} = \begin{pmatrix}\boldsymbol{0}_k & 1 & *\end{pmatrix}$ (by adding a suitable codeword and multiplying $\boldsymbol{y}$ by a suitable constant) and that $\boldsymbol{H_y} = \begin{pmatrix}* & \boldsymbol{I}_{n-k-1}\end{pmatrix}$. Then, $\boldsymbol{H} := \begin{pmatrix}\boldsymbol{H_y}\\ \boldsymbol{h}\end{pmatrix}$ is a parity-check matrix for $\mathcal{C}$ for a vector $\boldsymbol{h} = \begin{pmatrix}* & 1 & \boldsymbol{0}_{n-k-1}\end{pmatrix}$ lying in the dual $\mathcal{C}^\perp$. We have $\boldsymbol{yh}^\intercal = 1$.*

Proof. Up to a permutation of the coordinates, we can assume that $\boldsymbol{G}$ is in systematic form $\boldsymbol{G} = \begin{pmatrix}\boldsymbol{I}_k & *\end{pmatrix}$, and up to the addition of an element in $\mathcal{C}$ that $\boldsymbol{y} = (\boldsymbol{0}_k\ *)$. As $\boldsymbol{y}$ contains an error of weight r, it is non-zero, so that up to a permutation of the coordinates of the code and up to the multiplication by a constant in $\mathbb{F}_{q^m}$, we assume that $\boldsymbol{y}$ has the given shape $\boldsymbol{y} = \begin{pmatrix}\boldsymbol{0}_k & 1 & *\end{pmatrix}$. Now, if $\widetilde{\boldsymbol{G}_{\boldsymbol{y}}} = \begin{pmatrix}\boldsymbol{I}_{k+1} & \boldsymbol{A}\end{pmatrix}$ is a generator matrix of $\mathcal{C}_{\boldsymbol{y}}$ in systematic form, then $\boldsymbol{H_y} := \begin{pmatrix}-\boldsymbol{A}^\intercal & \boldsymbol{I}_{n-k-1}\end{pmatrix}$ is suitable. By considering an $\boldsymbol{h}$ linearly independent from the rows of $\boldsymbol{H_y}$ and such that $\boldsymbol{yh}^\intercal \neq 0$, any linear combination between $\boldsymbol{h}$

[6] for affine systems, degree falls correspond to linear combinations between polynomials of a given degree that yield polynomials of smaller degree.

and the rows of $\boldsymbol{H_y}$ still satisfies the same properties. Therefore, we may assume that $\boldsymbol{h} = \left(* \ \boldsymbol{0}_{n-k-1}\right)$, and moreover we have $\boldsymbol{y}\boldsymbol{h}^\mathsf{T} = h_{k+1} \neq 0$. Thus, the vector $h_{k+1}^{-1}\boldsymbol{h}$ is indeed of the form $\left(* \ 1 \ \boldsymbol{0}_{n-k-1}\right)$. □

Proposition 1. *The equations in $\mathcal{Q}_0$ can be obtained as linear combinations between the equations in $\mathcal{Q}_{\geq 1}$:*

$$Q_{T+k+1} = -\sum_{Q_I \in \mathcal{Q}_{\geq 1}} |\boldsymbol{H_y}|_{T,I}\, Q_I, \quad \forall T \subset \{1..n-k-1\},\ \#T = r+1. \tag{10}$$

Proof. This comes from the relations $\left|\begin{pmatrix} \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H_y}^\mathsf{T}\right|_{*,T} = 0$, see Appendix A.1 for details. □

Proposition 2. *The equations in $\mathcal{P} \cup \mathcal{Q}_{\geq 2}$ are linearly independent. Moreover, each variable c_{J+k+1} for any $J \subset \{1..n-k-1\}$, $\#J = r$ appears only as the leading term of P_J and does not appear in any of the equations in $\mathcal{Q}_{\geq 2}$ nor in $P_{J'}$ with $J' \neq J$.*

Proof. See Appendix A.2. □

Proposition 3. *The equations in $\mathcal{Q}_1$ reduce to the equations*

$$\mathcal{P} \cup \bigcup_{j=1}^{k} x_j \mathcal{P}$$

modulo the equations in $\mathcal{Q}_{\geq 2}$. More precisely, for any $J \subset \{1..n-k-1\}$, $\#J = r$ and $j \in \{1..k\}$ we have

$$P_J = Q_{\{k+1\}\cup(J+k+1)} + \sum_{Q_I \in \mathcal{Q}_{\geq 2}} (-1)^r \,|\boldsymbol{H}|_{J\cup\{n-k\},I}\, Q_I$$

$$x_j P_J = Q_{\{j\}\cup(J+k+1)} + \sum_{Q_I \in \mathcal{Q}_{\geq 2}, j \in I} (-1)^{1+\mathrm{Pos}(j,I)} \,|\boldsymbol{H_y}|_{J,I\setminus\{j\}}\, Q_I$$

where $\mathrm{Pos}(i_u, I) = u$ *for* $I = \{i_1, \cdots, i_{r+1}\}$ *such that* $i_1 < \cdots < i_{r+1}$.

Proof. This comes from the relations $P_J = (-1)^r \left|\begin{pmatrix} \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \begin{pmatrix} \boldsymbol{H_y} \\ \boldsymbol{h} \end{pmatrix}^\mathsf{T}\right|_{*,J\cup\{n-k\}}$ and $x_j P_J = (-1)^r \left|\begin{pmatrix} \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \begin{pmatrix} \boldsymbol{H_y} \\ \boldsymbol{e}_j \end{pmatrix}^\mathsf{T}\right|_{*,J\cup\{n-k\}}$ with $\boldsymbol{e}_j$ the j-th canonical basis vector in $\mathbb{F}_q^n$, see Appendix A.2 for details. □

To conclude this section, we have shown that the equations P_J and $\mathcal{Q}_{\geq 2}$ are linearly independent and that the equations in $\mathcal{Q}_0$ and $\mathcal{Q}_1$ are redundant to the system. Moreover, each P_J equation can be used to eliminate the variable

c_{J+k+1} from the system, so that solving $\mathcal{P} \cup \mathcal{Q}_{\geq 2}$ amounts to solve $\mathcal{Q}_{\geq 2}$ and this last system that does not contain the variables c_{J+k+1}. Similarly to [16], a natural approach is now to linearize at higher bi-degree $(b, 1)$ after multiplying the equations by linear variables. Here, we are able to describe precisely the $\mathbb{F}_{q^m}$-vector space generated by the equations $\mathcal{Q}_{\geq 2}$ augmented at bi-degree $(b, 1)$ (see Appendix A.4 for the proof).

Proposition 4. *For any $b \geq 1$, the $\mathbb{F}_{q^m}$-vector space generated by the equations $\mathcal{Q}_{\geq 2}$ augmented at bi-degree $(b, 1)$ by multiplying by monomials of degree $b-1$ in the x_i variables has dimension*

$$\mathcal{N}_b^{\mathbb{F}_{q^m}} := \sum_{i=1}^{k} \binom{n-i}{r} \binom{k+b-1-i}{b-1} - \binom{n-k-1}{r} \binom{k+b-1}{b}, \tag{11}$$

and there are

$$\mathcal{M}_b^{\mathbb{F}_{q^m}} := \binom{k+b-1}{b} \left(\binom{n}{r} - \binom{n-k-1}{r} \right) \tag{12}$$

monomials of degree $(b, 1)$. We have $\mathcal{N}_b^{\mathbb{F}_{q^m}} < \mathcal{M}_b^{\mathbb{F}_{q^m}} - 1$ for any $b \geq 1$.

As a consequence, we see that the system $Q_{\geq 2}$ always has more monomials than equations and cannot be solved in this way at any degree b. The reason is that our initial sets of equations are with coefficients in $\mathbb{F}_{q^m}$ and do not take into account the fact that the c_T's are searched in $\mathbb{F}_q$ (the overall system is not zero-dimensional). This will lead us to propose in Section 4 a mixed modeling by using together equations over $\mathbb{F}_{q^m}$ and over $\mathbb{F}_q$. Prior to that, we come back to the analysis of these $\mathbb{F}_q$ equations in the next section.

3.2 MaxMinors and Support-Minors modelings over $\mathbb{F}_q$.

Here we consider the unfolded systems obtained by expressing all equations of MM-$\mathbb{F}_{q^m}$ (resp. SM-$\mathbb{F}_{q^m}$) in the fixed basis $\boldsymbol{\beta} := (\beta_1, \ldots, \beta_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and taking each component, as described in Section 2. For the P_J's, this unfolding process yields by definition the original (MM-$\mathbb{F}_q$) system $\{P_{i,J}\}_{i,J}$ [16] containing m times more equations than MM-$\mathbb{F}_{q^m}$ and in the same variables. For the Q_I's, as the linear variables x_j lie in the extension field $\mathbb{F}_{q^m}$, we express each x_j in the basis $\boldsymbol{\beta}$ as $x_j = \sum_{i=1}^{m} \beta_i x_{i,j}$, yielding m times more linear variables $x_{i,j}$'s. The same unfolding technique is then applied to obtain a system $\{Q_{i,I}\}_{i,I}$, and Proposition 6 will show that it exactly corresponds to the (SM-$\mathbb{F}_q$) system defined in the introduction.

Following previous work (e.g. [15,16]), we assume that the MM-$\mathbb{F}_q$ equations $P_{i,J}$ are generically as linearly independent as possible. The following Assumption 1 was also validated experimentally with overwhelming probability for a random code $\mathcal{C}$.

Assumption 1 *The $m\binom{n-k-1}{r}$ linear equations $P_{i,J}$ in the $\binom{n}{r}$ variables c_T generate an $\mathbb{F}_q$-vector space of dimension* $\min\left(m\binom{n-k-1}{r}, \binom{n}{r} - 1\right)$.

Remark 1. If we consider only one P_J equation and if we denote by $\boldsymbol{v}_J$ the vector of minors of $(\boldsymbol{H}_{\boldsymbol{y}})_{*,J}$ of size r and by $\boldsymbol{\mu}$ the vector of minors of $\boldsymbol{C}$ of size r, then $P_J = \boldsymbol{v}_J\boldsymbol{\mu}^{\mathsf{T}}$ and the rank of the system $\{P_{i,J} : 1 \leq i \leq m\}$ is exactly the rank of $\boldsymbol{v}_J$ in rank metric. More generally, the number of linearly independent equations in $\{P_{i,J}\}_{i,J}$ is the co-dimension of the subfield subcode of the code generated by the matrix $\left(\boldsymbol{v}_J\right)_{J\subset\{1..n-k-1\},\#J=r}$.

On the contrary, we are able to prove this result for the SM-$\mathbb{F}_q$ equations on a specific RD instance. Note that such a statement is not proven for the SM equations on a random MinRank instance, so in a way this $\mathbb{F}_{q^m}$-linear structure enables one to remove this implicit assumption of [16] in the RD case.

Proposition 5. *The equations in* $\mathrm{Unfold}(\mathcal{Q}_{\geq 2})$ *satisfy* $\mathrm{LT}(Q_{i,I}) = x_{i,i_1}c_{I\setminus\{i_1\}}$ *with* $i_1 = \min(I) \leq k$*. In particular, they are all linearly independent over* $\mathbb{F}_q$*.*

Finally, we show that the equations from SM-$\mathbb{F}_q$ are the unfolded equations obtained from SM-$\mathbb{F}_{q^m}$. To this end, it may be helpful to give more details about this modeling than those given in the introduction. Let $(\boldsymbol{y}, \mathcal{C}, r)$ an RD instance where $\mathcal{C}$ is a code of generator matrix $\boldsymbol{G}$ and let

$$\begin{aligned}\boldsymbol{M}_0 &:= \mathrm{Mat}(\boldsymbol{y})\\ \boldsymbol{M}_{\ell,j} &:= \mathrm{Mat}(\beta_\ell \boldsymbol{G}_{j,*}) \ \text{ for } \ell \in \{1..m\},\ j \in \{1..k\}\end{aligned}$$

As observed in [16], this RD problem is equivalent to a MinRank instance with rank r, $K = km$ and matrices

$$(\boldsymbol{M}_0, \boldsymbol{M}_{1,1}, \ldots, \boldsymbol{M}_{i,j}, \ldots, \boldsymbol{M}_{m,k}) \in \mathbb{F}_q^{m\times n}.$$

There, the Support-Minors modeling is to say that all the maximal minors of the matrices $\begin{pmatrix}\boldsymbol{r}_i\\ \boldsymbol{C}\end{pmatrix}$ are equal to 0 for all $i \in \{1..m\}$ and where $\boldsymbol{r}_i$ is the i-th row in the solution to the MinRank problem, namely

$$\boldsymbol{r}_i = \mathrm{Mat}\left(\boldsymbol{y} + \sum_{\ell=1}^{m}\sum_{j=1}^{k} x_{\ell,j}\beta_\ell \boldsymbol{G}_{j,*}\right)_{i,*} = \mathrm{Tr}(\beta_i^\star(\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G})),$$

$$\text{where } \ \mathrm{rk}\left(\boldsymbol{M}_0 + \sum_{\ell=1}^{m}\sum_{j=1}^{k} x_{\ell,j}\boldsymbol{M}_{\ell,j}\right) \leq r,$$

and where the second equality follows from (5). We then obtain

Proposition 6. *For any* $i \in \{1..m\}$ *and any* $I \subset \{1..n\}$, $\#I = r+1$*, we have*

$$Q_{i,I} := \left|\begin{pmatrix}\boldsymbol{r}_i\\ \boldsymbol{C}\end{pmatrix}\right|_{*,I} = \mathrm{Tr}\left(\beta_i^\star Q_I\right) \mod I_q,$$

where I_q *is the ideal generated by all the field equations* $x_{\ell,j}^q - x_{\ell,j}$ *and* $c_T^q - c_T$*.*

Proof. The proposition basically follows from the linearity of the trace and the determinant with respect to its first row and from (9):

$$\begin{aligned}\mathrm{Tr}\left(\beta_i^\star \left|\begin{pmatrix}\boldsymbol{y}+\boldsymbol{x}\boldsymbol{G}\\ \boldsymbol{C}\end{pmatrix}\right|_{*,I}\right) \mod I_q = &\quad \mathrm{Tr}\left(\left|\begin{pmatrix}\beta_i^\star\left(\boldsymbol{y}+\boldsymbol{x}\boldsymbol{G}\right)\\ \boldsymbol{C}\end{pmatrix}\right|_{*,I}\right) \mod I_q \\ = &\quad \left|\begin{pmatrix}\mathrm{Tr}\left(\beta_i^\star\left(\boldsymbol{y}+\boldsymbol{x}\boldsymbol{G}\right)\right)\\ \boldsymbol{C}\end{pmatrix}\right|_{*,I} = \left|\begin{pmatrix}\boldsymbol{r}_i\\ \boldsymbol{C}\end{pmatrix}\right|_{*,I}.\end{aligned}$$

□

4 Algebraic approach to solve RD by combining SM-$\mathbb{F}_{q^m}$ and MM-$\mathbb{F}_q$

From the material presented in the previous section, we conclude that the $P_{i,J}$ equations over $\mathbb{F}_q$ (i.e. MM-$\mathbb{F}_q$) are necessary to solve the system: without them we cannot solve RD since the previously considered ideal without these equations was not zero-dimensional. However, we also noticed that the SM-$\mathbb{F}_q$ equations over the small field involve a large number of linear variables compared to SM-$\mathbb{F}_{q^m}$. This leads us to propose a new Modeling 5 to attack RD, which relies on solving SM-$\mathbb{F}_{q^m}$ together with MM-$\mathbb{F}_q$. In this way, we take advantage of all the $m\binom{n-k-1}{r}$ linear equations we can get in the c_T's from MM-$\mathbb{F}_q$ while keeping only k linear variables x_i's over $\mathbb{F}_{q^m}$ from SM-$\mathbb{F}_{q^m}$. This increased compactness makes that even if this system were to be solved at higher degree than SM-$\mathbb{F}_q$, it may perform better from a complexity point of view.

Let $\mathrm{NF}(f, \langle P_{i,J}\rangle)$ be the normal form function that associates to any polynomial f the unique polynomial $\widetilde{f} = f \mod \langle P_{i,J}\rangle$ such that no c_T leading term of a polynomial in the $\langle P_{i,J}\rangle$ ideal appears in $\widetilde{f}$. Modeling 5 is the system (SM-$\mathbb{F}_{q^m}^+$) over $\mathbb{F}_{q^m}$ which consists of the equations in $\mathcal{Q}_{\geq 2}$ in which the equations $P_{i,J}$'s are used to remove c_T variables, i.e. $\{\widetilde{Q_I},\ Q_I \in \mathcal{Q}_{\geq 2}\}$ where

$$\widetilde{Q_I} := \mathrm{NF}(Q_I, \langle P_{i,J}\rangle).$$

Then, we solve Modeling 5 using the same technique as in [16] by multiplying the equations by all possible monomials of degree $b-1$ in the x_i's. Once again, the complexity analysis requires to estimate the dimension of the $\mathbb{F}_{q^m}$-vector space generated by the resulting bi-degree $(b,1)$ equations. According to Proposition 4, there are $\mathcal{N}_b^{\mathbb{F}_{q^m}}$ such equations but we provide in this section new syzygies brought by the elimination of the c_T variables using the linear equations $P_{i,J}$. We call $\mathcal{N}_{b,syz}^{\mathbb{F}_q}$ the number of those new syzygies, so that the estimated dimension is $\mathcal{N}_b^{\mathbb{F}_{q^m}} - \mathcal{N}_{b,syz}^{\mathbb{F}_q}$. The final cost follows by comparing this number to the number of monomials $\mathcal{M}_b^{\mathbb{F}_q}$.

Proposition 7. *For any $b \geq 1$, the number of linearly independent equations at bi-degree $(b,1)$ in SM-$\mathbb{F}_{q^m}^+$ is generically*

$$\mathcal{N}_b^{\mathbb{F}_q} = \mathcal{N}_b^{\mathbb{F}_{q^m}} - \mathcal{N}_{b,syz}^{\mathbb{F}_q},$$

with the exact value (from Proposition 4)

$$\mathcal{N}_b^{\mathbb{F}_{q^m}} = \sum_{i=1}^{k} \binom{n-i}{r}\binom{k+b-1-i}{b-1} - \binom{n-k-1}{r}\binom{k+b-1}{b} \tag{23}$$

and the conjectured value, valid as long as $\mathcal{N}_b^{\mathbb{F}_q} < \mathcal{M}_b^{\mathbb{F}_q}$:

$$\mathcal{N}_{b,syz}^{\mathbb{F}_q} = (m-1)\sum_{i=1}^{b}(-1)^{i+1}\binom{k+b-i-1}{b-i}\binom{n-k-1}{r+i}. \tag{13}$$

The number of monomials is

$$\mathcal{M}_b^{\mathbb{F}_q} = \binom{k+b-1}{b}\left(\binom{n}{r} - m\binom{n-k-1}{r}\right), \tag{14}$$

so that we can solve SM-$\mathbb{F}_{q^m}^{+}$ by linearization at bi-degree $(b,1)$ whenever

$$\mathcal{N}_b^{\mathbb{F}_q} \geq \mathcal{M}_b^{\mathbb{F}_q} - 1.$$

In this case, the final cost in $\mathbb{F}_q$ operations is given by

$$\mathcal{O}\left(m^2 \mathcal{N}_b^{\mathbb{F}_q} {\mathcal{M}_b^{\mathbb{F}_q}}^{\omega-1}\right),$$

where ω is the linear algebra constant and where the m^2 factor comes from expressing each $\mathbb{F}_{q^m}$ operation involved in terms of $\mathbb{F}_q$ operations.

Note that it is always possible, whenever the ratio between equations and variables is much larger than 1, to drop excess equations by taking punctured codes much in the same way as in [16, §4.2].

Analysis of the syzygies in Modeling 5. Contrary to Section 3, we are not able to give a proof for the number of linearly independent syzygies due to the $P_{i,J}$'s. This comes from the fact that now, for some large enough b, we can solve the system, implying that the equations are not linearly independent at this degree anymore (hence we cannot give a general proof of independence). Also, we may find specific instances for which our conjecture fails. Still, we can analyse the generic behaviour on random instances. Here, we describe generic syzygies coming from the $\mathbb{F}_{q^m}$ structure and we use them to count precisely the number of equations and monomials at each bi-degree $(b,1)$ to determine the success of a solving strategy by linearization in the generic case.

We start by giving a generalization of Proposition 1, that provides an explanation for the relations between the $\widetilde{Q}_I$ equations starting at bi-degree $(1,1)$.

Proposition 8. *For any $T \subset \{1..n-k-1\}$, $\#T = r+1$ and $1 \leq i \leq m$, we obtain a relation between the $\widetilde{Q}_I$ equations given by*

$$\mathrm{Tr}(\beta_i^\star)\widetilde{Q}_{T+k+1} + \sum_{\substack{I \subset \{1..n\} \\ \#I = r+1 \\ I \cap \{k+1..n\} \subsetneq T+k+1}} \mathrm{Tr}(\beta_i^\star \, |\boldsymbol{H}_{\boldsymbol{y}}|_{T,I})\widetilde{Q}_I = 0. \tag{15}$$

Note that the coefficients of any of these relations belong to $\mathbb{F}_q$.

Proof. This comes from the fact that, for any $0 \leq \ell \leq m-1$:

$$\Gamma_{\ell,T} := \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} (\boldsymbol{H_y}^{[\ell]})^{\mathsf{T}} \right|_{*,T} = 0 \mod \langle P_{i,J} \rangle.$$

Further details as well as the link between $P_J^{[\ell]}$ and $P_{i,J}$ are postponed in Appendix A.5. $\square$

Proposition 8 gives (at most) $m\binom{n-k-1}{r+1}$ syzygies at bi-degree $(1,1)$ which include the relations from Proposition 1 (the $\ell = 0$ case in the proof).

At degree $b = 2$, those relations multiplied by all linear variables generate new relations, but they are not independent anymore: indeed, for $1 \leq \ell \leq m-1$ and any $T_2 \subset \{1..n-k-1\},\ \#T_2 = r+2$ the following minor gives $(m-1)\binom{n-k-1}{r+2}$ relations between the $\mathcal{N}_{1,syz}^{\mathbb{F}_q}$ syzygies at bi-degree $(1,1)$:

$$\left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} (\boldsymbol{H}_{\boldsymbol{y}}^{[\ell]})^{\mathsf{T}} \right|_{*,T_2} = 0,$$

More generally, a similar inclusion-exclusion combinatorial argument as those used to derive [16, Heuristic 2] leads to the following Conjecture 1, that was verified experimentally for $b = 2,\ b = 3$ and $b = 4$.

Conjecture 1 *For $b \geq 1$, the number of independent syzygies is expected to be equal to*

$$\mathcal{N}_{b,syz}^{\mathbb{F}_q} = (m-1) \sum_{i=1}^{b} (-1)^{i+1} \binom{k+b-i-1}{b-i} \binom{n-k-1}{r+i}.$$

5 Hybrid technique on minor variables

In algebraic cryptanalysis, "hybrid approach" usually refers to a generic method to possibly decrease the complexity of an algebraic attack by (a) choosing a subset of unknowns, (b) specializing them to some value, (c) solving the new system with less unknowns and (d) finally trying all possible specializations of those unknowns. The point is that in certain cases, the complexity gain in solving the new system supersedes the loss in complexity coming from exhaustive search. In [16], an indirect approach is followed on the MaxMinors modeling. Instead of performing a naive exhaustive search on random minor variables, the authors proceed by fixing $a \geq 0$ columns in $\boldsymbol{C}$. It can readily be seen that this provides $N := \binom{n}{r} - \binom{n-a}{r}$ linear polynomials involving the c_T's. These equations can in turn be used to reduce the number of c_T variables by the same amount and this costs only to test $q^{a \cdot r}$ different choices instead of trying q^N choices if we had performed the naive exhaustive search of N variables.

Here, we obtain a much more precise understanding of this approach by viewing it as a rerandomizing trick. This was somehow already sketched in [35,

§5.2] for the RD problem (see the proof of Proposition 3 there), but we show that it is more general and it actually applies to any MinRank problem. For simplicity and to adopt the same convention as in [15,16] (see for instance the discussion in [15, Algo 1] for RD), let us assume that the r leftmost columns in the rank r matrix $\boldsymbol{M}$ we are looking for are linearly independent, for instance $\boldsymbol{M} = \boldsymbol{S}\left(\boldsymbol{I}_r\ \boldsymbol{C}'\right)$ with $\boldsymbol{S}$ full-rank. Our approach to solve the initial MinRank problem $(\boldsymbol{M}_0, \ldots, \boldsymbol{M}_K)$ is by further assuming that the last $a \geq 0$ columns in the low-rank solution matrix are zero, i.e. $\boldsymbol{M}_{*,\{n-a+1,n\}} = \boldsymbol{0}_{m\times a}$. Clearly, this does not hold in general. Still, we may multiply this instance to the right by each of the $q^{a\cdot r}$ invertible matrices of the set

$$\mathcal{P} := \left\{ \boldsymbol{P}_{\boldsymbol{A}} = \begin{pmatrix} \boldsymbol{I}_r & \boldsymbol{0}_{r\times(n-a-r)} & -\boldsymbol{A} \\ \boldsymbol{0}_{(n-a-r)\times r} & \boldsymbol{I}_{n-a-r} & \boldsymbol{0}_{(n-a-r)\times r} \\ \boldsymbol{0}_{a\times r} & \boldsymbol{0}_{a\times(n-a-r)} & \boldsymbol{I}_a \end{pmatrix},\ \boldsymbol{A} \in \mathbb{F}_q^{r\times a} \right\}, \tag{16}$$

and eventually exactly one of the resulting $(\boldsymbol{M}_0\boldsymbol{P}_{\boldsymbol{A}}, \ldots, \boldsymbol{M}_K\boldsymbol{P}_{\boldsymbol{A}})$ instances will satisfy this property and then lead to the desired solution. The point is that (i) multiplying by invertible matrices (on the left or the right) preserves the rank (i.e. is an isometry for the rank distance) and therefore $\boldsymbol{M}\boldsymbol{P}_{\boldsymbol{A}}$ is also of rank r, (ii) multiplying by matrices of this form amounts to leave the $(n-a)$ first columns unchanged but adds to the last a columns of $\boldsymbol{M}$ all possible linear combinations of the r first ones. One of them has to 0 because by assumption, the r first columns form a basis of the column space of $\boldsymbol{M}$.

5.1 Generic MinRank instances

First, note that multiplying the initial instance by $\boldsymbol{P}_{\boldsymbol{A}} \in \mathcal{P}$ from Equation (16) has the nice property of keeping the matrices unchanged in their first $n-a$ columns, namely $\boldsymbol{Q}_i := \boldsymbol{M}_i\boldsymbol{P}_{\boldsymbol{A}} := \left(\boldsymbol{L}_i\ \boldsymbol{R}_i\right)$ where $\boldsymbol{L}_i := (\boldsymbol{M}_i)_{*,\{1..n-a\}}$ and $\boldsymbol{R}_i := \boldsymbol{M}_i(\boldsymbol{P}_{\boldsymbol{A}})_{*,\{n-a+1..n\}}$. Also, recall that we target a rank r solution $\boldsymbol{Q} = \boldsymbol{Q}_0 + \sum_{i=1}^{K} x_i\boldsymbol{Q}_i$ such that $\boldsymbol{Q}_{*,\{n-a+1..n\}} = \boldsymbol{0}_{m\times a}$. The solution vector $\boldsymbol{x} := (1, x_1, \ldots, x_K)$ then satisfies

$$\begin{aligned} \operatorname{rk}\left(\boldsymbol{L}_0 + \sum_{i=1}^{K} x_i\boldsymbol{L}_i\right) &= r, \\ \boldsymbol{R}_0 + \sum_{i=1}^{K} x_i\boldsymbol{R}_i &= \boldsymbol{0}_{m\times a}. \end{aligned} \tag{17}$$

We may then solve the $(m, n-a, K, r)$ MinRank instance $(\boldsymbol{L}_0, \ldots, \boldsymbol{L}_K)$ with the help of the linear relations given by Equation (17). This trivially gives a second MinRank problem of parameters $(m, n-a, K-a\cdot m, r)$ by considering a basis of the kernel of (17), see for instance [20, §4 p.11] for a similar discussion. There, the initial MinRank problem and the linear relations which are added highly depend on the structure of the Rainbow scheme so that the resulting instance is not random. On our side, as we deal with generic MinRank problems in this section, we do not expect abnormal behavior for our final $(m, n-a, K-a\cdot m, r)$ instance.

5.2 RD instances

Of course, we may apply the same technique to the RD problem by viewing it as a particular MinRank problem. In this $\mathbb{F}_{q^m}$-linear setting, the RD instance becomes itself another (reduced) RD instance. This can be verified as follows. First of all, the specific form of the solution, i.e. $\boldsymbol{M}_{*,\{n-a+1,n\}} = \mathbf{0}_{m\times a}$, translates into an error $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}_{\check{J}} = \mathbf{0}$, where $J := \{n-a+1..n\}$ and $\check{J} := \{1..n\} \setminus J = \{1..n-a\}$. Also, recall that the underlying MinRank instance over $\mathbb{F}_q$ is of the form

$$\mathrm{rk}\left(\boldsymbol{M}_0 + \sum_{\ell=1}^{m}\sum_{j=1}^{k} x_{\ell,j}\boldsymbol{M}_{\ell,j}\right) = r,$$

where $\boldsymbol{M}_0 := \mathrm{Mat}(\boldsymbol{y})$ and where $\boldsymbol{M}_{\ell,j} := \mathrm{Mat}(\beta_\ell \boldsymbol{G}_{j,*})$. Once again, multiplying all these matrices by $\boldsymbol{P}_{\boldsymbol{A}}$ does not affect the first $n-a$ columns. At the vector level, this implies that the first $n-a$ components of $\boldsymbol{y}\boldsymbol{P}_{\boldsymbol{A}} \in \mathbb{F}_{q^m}^n$ and of any $\boldsymbol{c}\boldsymbol{P}_{\boldsymbol{A}},\ \boldsymbol{c} \in \mathcal{C}$ are exactly the same as before. We aim at solving the RD instance $(\boldsymbol{y}^{\boldsymbol{A}} := \boldsymbol{y}\boldsymbol{P}_{\boldsymbol{A}}, \mathcal{C}^{\boldsymbol{A}} := \mathcal{C}\boldsymbol{P}_{\boldsymbol{A}}, r)$ with the extra assumption on the error $\boldsymbol{e}^{\boldsymbol{A}}$. In other words, we target a solution $(\boldsymbol{c}^{\boldsymbol{A}}, \boldsymbol{e}^{\boldsymbol{A}})$ such that $(\boldsymbol{y}^{\boldsymbol{A}} - \boldsymbol{c}^{\boldsymbol{A}})_J = \mathbf{0}$. For such a solution, with a very mild condition on the shortened code at J we obtain a reduction to an RD instance with smaller parameters, namely

Proposition 9. *Assume that $(\boldsymbol{y}^{\boldsymbol{A}} - \boldsymbol{c}^{\boldsymbol{A}})_J = \mathbf{0}$. Let $\mathcal{C}'$ be the code $\mathcal{C}^{\boldsymbol{A}}$ shortened at J, namely $\mathcal{C}^{'} = \{\boldsymbol{c}_{\check{J}} :\ \boldsymbol{c} \in \mathcal{C}^{\boldsymbol{A}},\ \boldsymbol{c}_J = \mathbf{0}\}$. Assume that $\mathcal{C}'$ is of dimension $k-a$, then by Gaussian elimination on a generator matrix $\boldsymbol{G}^{\boldsymbol{A}}$ of $\mathcal{C}^{\boldsymbol{A}}$ we can obtain a generator matrix of $\mathcal{C}^{\boldsymbol{A}}$ of the form*

$$\boldsymbol{G}" = \begin{pmatrix} \boldsymbol{G}' & \mathbf{0}^{(k-a)\times a} \\ \boldsymbol{B} & \boldsymbol{I}_a \end{pmatrix}.$$

For $j \in J$, let $\boldsymbol{c}^j$ be the unique row of $\boldsymbol{G}"$ which contains a 1 in column j. Define $\boldsymbol{y}' = \boldsymbol{y}"_{\check{J}}$ where $\boldsymbol{y}" := \boldsymbol{y}^{\boldsymbol{A}} - \sum_{j\in J}(\boldsymbol{y}^{\boldsymbol{A}})_j \boldsymbol{c}^j$. Then $(\boldsymbol{y}', \mathcal{C}', r)$ is a valid instance of an RD problem of parameters $(m, n-a, k-a, r)$.

Proof. The first point is just standard linear algebra. For the second point, notice that if we express the solution $\boldsymbol{c}^{\boldsymbol{A}}$ of the RD problem associated to the instance $(\boldsymbol{y}^{\boldsymbol{A}}, \mathcal{C}^{\boldsymbol{A}}, r)$ as a sum

$$\boldsymbol{c}^{\boldsymbol{A}} = \boldsymbol{c}^{"} + \sum_{j\in J} x_j \boldsymbol{c}^j$$

where $\boldsymbol{c}^{"}$ is generated by the first $k-a$ rows of $\boldsymbol{G}"$, we necessarily have $x_j = (\boldsymbol{y}^{\boldsymbol{A}})_j$ because the coordinates of $\boldsymbol{c}^{"}$ are zero on J and $\boldsymbol{y}^{\boldsymbol{A}}_J = \boldsymbol{c}^{\boldsymbol{A}}_J$ by assumption. Therefore

$$\boldsymbol{y}^{\boldsymbol{A}} - \boldsymbol{c}^{\boldsymbol{A}} = \boldsymbol{y}^{\boldsymbol{A}} - \boldsymbol{c}" - \sum_{j\in J}(\boldsymbol{y}^{\boldsymbol{A}})_j \boldsymbol{c}^j = \boldsymbol{y}" - \boldsymbol{c}".$$

Therefore $\boldsymbol{y}" - \boldsymbol{c}"$ is of rank weight r and the proposition follows from this remark and the fact that $\boldsymbol{c}"_{\check{J}}$ belongs obviously to $\mathcal{C}'$.

The condition on the dimension of the shortened holds under very mild conditions. For instance, we have

Lemma 1. *Provided that $k \leq n - a$ and under the assumption that the matrix $\boldsymbol{U}^{\boldsymbol{A}} \in \mathbb{F}_{q^m}^{k \times a}$ defined by $\boldsymbol{U}^{\boldsymbol{A}} := -\boldsymbol{G}_{*,\{1..r\}}\boldsymbol{A} + \boldsymbol{G}_{*,J}$ is full-rank, the code $\mathcal{C}^{\boldsymbol{A}'}$ has dimension $k - a$.*

Proof. Provided that $k \leq n - a$, the matrix $\boldsymbol{G}^{\boldsymbol{A}} \in \mathbb{F}_{q^m}^{k \times n}$ defined by $\boldsymbol{G}^{\boldsymbol{A}} := \boldsymbol{G}\boldsymbol{P}_{\boldsymbol{A}} = \left(\boldsymbol{I}_k \; \boldsymbol{T} \; \boldsymbol{U}^{\boldsymbol{A}}\right)$, where $\boldsymbol{T} := \boldsymbol{G}_{*,\{k+1..n-a\}}$ and $\boldsymbol{U}^{\boldsymbol{A}} := -\boldsymbol{G}_{*,\{1..r\}}\boldsymbol{A} + \boldsymbol{G}_{*,J}$ is a generating matrix for $\mathcal{C}^{\boldsymbol{A}}$ in systematic form. In particular, a systematic parity-check matrix for this code is given by $\boldsymbol{H}^{\boldsymbol{A}} := \begin{pmatrix} -\boldsymbol{T}^\top & \\ -(\boldsymbol{U}^{\boldsymbol{A}})^\top & \boldsymbol{I}_{n-k} \end{pmatrix}$. We obtain the parity check matrix for $\mathcal{C}^{\boldsymbol{A}'}$ by deleting the columns of $\boldsymbol{H}^{\boldsymbol{A}}$ whose index is in J, namely

$$\boldsymbol{H}^{\boldsymbol{A}'} := \begin{pmatrix} -\boldsymbol{T}^\top & \boldsymbol{I}_{n-k-a} \\ -(\boldsymbol{U}^{\boldsymbol{A}})^\top & \boldsymbol{0}_{a \times (n-k-a)} \end{pmatrix}.$$

From there we have that $\operatorname{rk}(\boldsymbol{H}^{\boldsymbol{A}'}) = n - k - a + \operatorname{rk}(\boldsymbol{U}^{\boldsymbol{A}})$, which finishes the proof by using the assumption on $\operatorname{rk}(\boldsymbol{U}^{\boldsymbol{A}})$. $\square$

Using Lemma 1, we are then left with solving an RD instance of parameters $(m, n - a, k - a, r)$.

5.3 Complexity of the hybrid technique

In the MaxMinors case, the original purpose of fixing columns in $\boldsymbol{C}$ was to end up with an overdefined linear system. Here, fixing $a \geq 0$ columns still yields a bilinear modeling which is solved at some bi-degree $(b, 1)$, where $b \geq 1$ is now a function of a. Therefore, the cost of the hybrid technique is estimated by solving a minimization problem over $a \geq 0$. Let $T_{\text{SM,plain},(m,n,K,r)}$ the cost of the standard Support-Minors approach of [16] on a generic MinRank problem of parameters (m, n, K, r). Under the assumption stated at the end of Section 5.1 that the resulting MinRank instances of parameters $(m, n - a, K - a \cdot m, r)$ behave as random, we have

Proposition 10. *The time complexity of the proposed Support-Minors hybrid technique on a generic MinRank problem of parameters (m, n, K, r) is given by*

$$T_{SM,hybrid,(m,n,K,r)} = \min_{a \geq 0} \left(q^{a \cdot r} \cdot T_{SM,plain,(m,n-a,K-a \cdot m,r)}\right).$$

We may obtain a similar statement in the RD case, where we consider any algebraic algorithm $\mathcal{A}$ to solve RD which involves linear and minor variables.

Proposition 11. *The time complexity of the proposed hybrid technique applied to an algebraic algorithm $\mathcal{A}$ to solve an RD problem of parameters (m, n, K, r) is given by*

$$T_{\mathcal{A},hybrid,(m,n,k,r)} = \min_{a \geq 0} \left(q^{a \cdot r} \cdot T_{\mathcal{A},plain,(m,n-a,k-a,r)}\right).$$

In particular, the new SM-$\mathbb{F}_{q^m}^+$ approach presented in this paper is compatible with the hybrid technique. The overall complexity may be easily computed by combining Proposition 7 to obtain $T_{\text{SM-}\mathbb{F}_{q^m}^+,\text{plain},\cdot}$ with Proposition 10.

6 Estimated costs on MinRank and RD instances.

Finally, we provide the bit complexity of the attacks described in this paper on some parameter sets. First, we apply the hybrid technique described in Section 5 to the Support-Minors modeling on generic MinRank instances (see Proposition 10). The same technique is then used on the SM-$\mathbb{F}_{q^m}^+$ system from Section 4 to attack RD instances (see Proposition 7 and Proposition 11). In both cases, these attacks are compared to former attacks on MinRank and RD.

6.1 MinRank instances

For plain MinRank, we notice that the approach of Section 5 on Support-Minors may allow to reach smaller complexities than the ones obtained with the specialization technique of [16] by fixing linear variables, especially for instances with larger q. As an illustration, we present some parameter sets in Table 1. The first one comes from [**?**, Table 24.7.1, D] and the following ones are obtained by increasing the value of q from 2 to 64 but by keeping the same (m, n, K, r). Note that for $q = 64$ and also for even larger values which are not presented here, the Support-Minors attack starts beating the best combinatorial attack, and the greater q, the bigger the gap.

Table 1. Comparison between the Support-Minors approach of [16] (specialization of K_{hyb} linear variables) in column "SM 20" and the approach of Section 5 in column "SM 22". The "comb" column refers to the complexity of the best combinatorial attack (see [26, §4.2] for a broader description of these attacks).

(q, m, n, K, r)	SM 20	b	K_{hyb}	SM 22	b	a	comb
$(2, 19, 19, 81, 10)$	**115**	1	66	**75**	1	4	45
$(4, 19, 19, 81, 10)$	**180**	2	62	**115**	1	4	90
$(8, 19, 19, 81, 10)$	**219**	11	34	**155**	1	4	135
$(16, 19, 19, 81, 10)$	**253**	11	34	**195**	1	4	180
$(64, 19, 19, 81, 10)$	**321**	11	34	**256**	1	4	270

6.2 RD instances

Recall that the cost of the best combinatorial attack of [12] in $\mathbb{F}_q$ operations is

$$\mathcal{O}\left((n-k)^{\omega} m^{\omega} q^{r\left\lceil \frac{(k+1)m}{n} \right\rceil - m}\right), \tag{18}$$

where ω is the linear algebra constant taken equal to 2.81. Also, cryptographically relevant RD instances are such that $r = \mathcal{O}(\sqrt{n})$ or such that the weight r is closer to the Gilbert-Varshamov bound, and we selected parameter sets corresponding to these two situations. The $r = \mathcal{O}(\sqrt{n})$ regime is for instance the one encountered in the NIST submissions ROLLO and RQC. In Table 2, we give the binary logarithm of the complexity of our attack "over $\mathbb{F}_{q^m}$" on ROLLO-I parameters and we also keep track of the optimum values of a_b and b. This cost is compared to the one of the combinatorial attack of [12] ("comb") and to the one of the MaxMinors attack ("MM."). A more recent trend for rank-based proposals is now to consider a different regime where the weight r is chosen closer to the rank Gilbert-Varshamow bound $d_{\mathrm{RGV}} = \mathcal{O}(n)$, see for instance [43,21]. A main motivation for this choice is that algebraic attacks may become less efficient than combinatorial attacks in this case. Note also that in the scheme of [43] which uses LRPC codes, choosing d of the same order somehow increases the rank of the moderate weight codewords in the masked LRPC code and therefore may allow to gain confidence in the indistinguishability assumption. In Table 3, the same comparison as in Table 2 is performed on RD instances with parameters $(m = 2k, n = 2k, k, r \sim d_{\mathrm{RGV}})$. In this very particular case (constant q, fixed rate 1/2 and $m = n$), one may adopt the approximation $d_{\mathrm{RGV}}(m, n, k, q) \sim n(1 - \sqrt{1/2})$ when $n \to +\infty$. Finally, Figure 1 contains a broader comparison between the same attacks for fixed (m, n, k) but for various values of weight.

Table 2. Comparison between known attacks on the new ROLLO-I parameters in [16] and [3] after the 2021-04-21 update. The "*"-symbol means that the best attack is obtained on the derived code from key attack with parameters $(m, n, k, r) = (m, 2k - \lfloor \frac{k}{d} \rfloor, k - \lfloor \frac{k}{d} \rfloor, d)$, where d refers to the rank of the moderate weight codewords in the masked LRPC code. Otherwise, the attack is on an RD problem with parameters $(m, 2k, k, r)$. The struck out numbers are the underestimated values from [16, Table 3].

Instance	q	k	m	r	d	pk size (B)	DFR	MM-$\mathbb{F}_q$	a	p	SM-$\mathbb{F}_{q^m}^+$	b	a	comb
new2ROLLO-I-128	2	83	73	7	8	757	-27	233	18	0	~~180~~ 233	1	15	**222**
new2ROLLO-I-192	2	97	89	8	8	1057	-33	258*	17	0	~~197*~~ **256***	1	14	292*
new2ROLLO-I-256	2	113	103	9	9	1454	-33	408*	30	1	~~283*~~ 403*	1	27	**385***
ROLLO-I-128-spe	2	83	67	7	8	693	-28	240	19	0	247	1	17	**206**
ROLLO-I-192-spe	2	97	79	8	8	958	-34	274*	19	0	278*	1	17	**262***
ROLLO-I-256-spe	2	113	97	9	9	1371	-33	417*	31	0	419*	2	27	**364***

References

1. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Zémor, G.: Ouroboros-R. First round submission

Table 3. Comparison between known attacks on RD instances of parameters $(m, 2k, k, r)$ where r is close to d_{RGV}, namely $r = \left\lceil n(1-\sqrt{1/2})\right\rceil$. The "difference" column contains the difference between the bit complexity of the best algebraic attack (either MM-$\mathbb{F}_q$ or SM-$\mathbb{F}_{q^m}^{+}$) and the one of the combinatorial attack of [12]. Note that this value is always positive for these parameters.

	algebraic						comb	Difference
$(n,k,r\sim d_{\mathrm{RGV}})$	MM-$\mathbb{F}_q$	a	p	SM-$\mathbb{F}_{q^m}^{+}$	a	b	[12]	Δ
$(50, 25, 15)$	395	22	2	387	k	1	**369**	18
$(80, 40, 24)$	979	36	0	973	k	1	**937**	36
$(100, 50, 30)$	1515	46	2	1514	k	1	**1465**	49
$(150, 75, 44)$	3310	71	7	3304	70	2	**3232**	72
$(200, 100, 59)$	5884	95	1	5916	k	1	**5800**	84
$(300, 150, 88)$	13147	145	9	13217	k	1	**13032**	115
$(500, 250, 147)$	36554	244	3	36768	k	1	**36445**	109
$(1000, 500, 293)$	145995	494	35	146520	k	1	**145847**	148

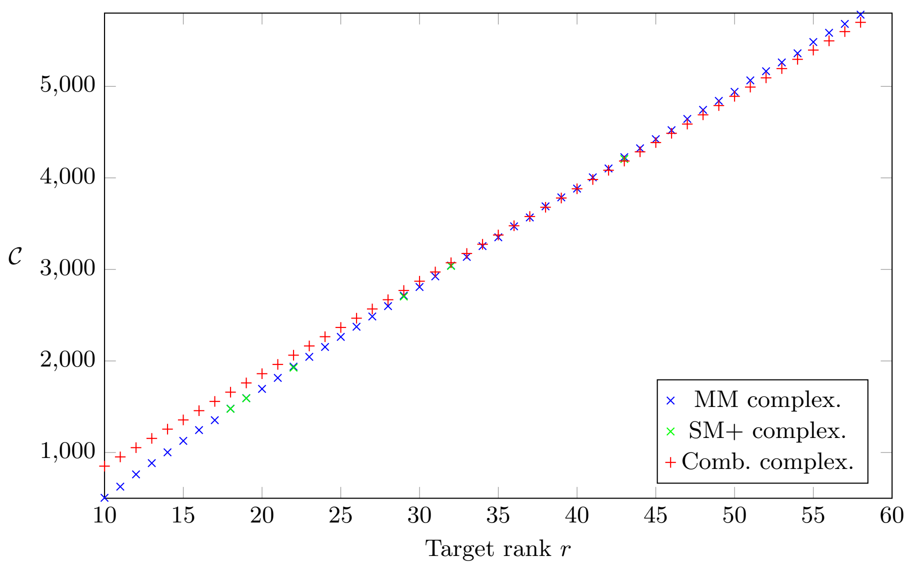

Fig. 1. Comparison between the theoretical complexities $\mathcal{C}$ of MM-$\mathbb{F}_q$/SM-$\mathbb{F}_{q^m}^{+}$ (the best one, hybrid and punctured version) and of the combinatorial attack for RD instances with fixed $(m, n, k) = (200, 200, 100)$ and various values of r. The rank Gilbert-Varshamov bound is $d_{\mathrm{RGV}}(m, n, k, q = 2?) = 58$.

to the NIST post-quantum cryptography call (Nov 2017), https://pqc-ouroborosr.org

2. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G.: Rank quasi cyclic (RQC). First round submission to the NIST post-quantum cryptography call (Nov 2017), https://pqc-rqc.org
3. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bros, M.,

Couvreur, A., Deneuville, J.C., Gaborit, P., Zémor, G., Hauteville, A.: Rank quasi cyclic (RQC). Second Round submission to NIST Post-Quantum Cryptography call (Apr 2020), https://pqc-rqc.org
4. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G., Couvreur, A., Hauteville, A.: Rank quasi cyclic (RQC). Second round submission to the NIST post-quantum cryptography call (Apr 2019), https://pqc-rqc.org
5. Alagic, G., Jacob, A., Daniel, A., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D.: Status report on the second round of the NIST post-quantum cryptography standardization process. Tech. Rep. NISTIR 8309, NIST (Jul 2020). https://doi.org/10.6028/NIST.IR.8309, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf
6. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.P., Zémor, G.: LAKE – Low rAnk parity check codes Key Exchange. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/LAKE.zip
7. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.P., Zémor, G.: LOCKER – LOw rank parity ChecK codes EncRyption. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/LOCKER.zip
8. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.P., Zémor, G., Aguilar Melchor, C., Bettaieb, S., Bidoux, L., Magali, B., Otmani, A.: ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER). Second round submission to the NIST post-quantum cryptography call (Mar 2019), https://pqc-rollo.org
9. Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: a rank metric based signature scheme. In: Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III. LNCS, vol. 11478, pp. 728–758. Springer (2019). https://doi.org/10.1007/978-3-030-17659-4_25, https://doi.org/10.1007/978-3-030-17659-4_25
10. Aragon, N., Gaborit, P., Hauteville, A., Ruatta, O., Zémor, G.: Ranksign – a signature proposal for the NIST's call. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/RankSign.zip
11. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.P.: Improvement of Generic Attacks on the Rank Syndrome Decoding Problem (Oct 2017), https://hal.archives-ouvertes.fr/hal-01618464, working paper or preprint
12. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.P.: A new algorithm for solving the rank syndrome decoding problem. In: 2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018. pp. 2421–2425. IEEE (2018). https://doi.org/10.1109/ISIT.2018.8437464
13. Baena, J., Briaud, P., Cabarcas, D., Perlner, R.A., Smith-Tone, D., Verbel, J.A.: Improving support-minors rank attacks: applications to GeMSS and Rainbow. IACR Cryptol. ePrint Arch., accepted for publication in CRYPTO 2022 p. 1677 (2021), https://eprint.iacr.org/2021/1677

14. Bardet, M., Briaud, P.: "an algebraic approach to the rank support learning problem". In: Cheon, J.H., Tillich, J.P. (eds.) Post-Quantum Cryptography. lncs, Springer International Publishing (2021)
15. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.: An algebraic attack on rank metric code-based cryptosystems. In: Advances in Cryptology - EUROCRYPT 2020 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020. Proceedings (2020), http://arxiv.org/abs/1910.00810
16. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.P., Verbel, J.: Improvements of algebraic attacks for solving the rank decoding and minrank problems. In: Advances in Cryptology - ASIACRYPT 2020, International Conference on the Theory and Application of Cryptology and Information Security, 2020. Proceedings. pp. 507–536 (2020), https://arxiv.org/abs/2002.08322v4
17. Bellini, E., Caullery, F., Gaborit, P., Manzano, M., Mateu, V.: Improved Veron identification and signature schemes in the rank metric. In: Proc. IEEE Int. Symposium Inf. Theory - ISIT 2019. vol. abs/1903.10212, pp. 1872–1876. IEEE, Paris, France (Jul 2019)
18. Bellini, E., Gaborit, P., Hasikos, A., Mateu, V.: Enhancing code based zero-knowledge proofs using rank metric. In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12579, pp. 570–592. Springer (2020). https://doi.org/10.1007/978-3-030-65411-5_28, https://doi.org/10.1007/978-3-030-65411-5_28
19. Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021. Lecture Notes in Computer Science, vol. 12696, pp. 348–373. Springer International Publishing (2021). https://doi.org/10.1007/978-3-030-77870-5_13
20. Beullens, W.: Breaking Rainbow takes a weekend on a laptop. IACR Cryptol. ePrint Arch. (2022), https://eprint.iacr.org/2022/214
21. Bidoux, L., Briaud, P., Bros, M., Gaborit, P.: Rqc revisited and more cryptanalysis for rank-based cryptography. ArXiv **abs/2207.01410** (2022)
22. Bruns, W., Vetter, U.: Determinantal Rings, lncs, vol. 1327. Springer (1988)
23. Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. J. Comput. System Sci. **58**(3), 572–596 (Jun 1999)
24. Cabarcas, D., Smith-Tone, D., Verbel, J.: Key recovery attack for ZHFE. In: Post-Quantum Cryptography 2017. LNCS, vol. 10346, pp. 289–308. Utrecht, The Netherlands (Jun 2017). https://doi.org/10.1007/978-3-319-59879-6_17, https://doi.org/10.1007/978-3-319-59879-6_17
25. Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Advances in Cryptology - ASIACRYPT 1996. LNCS, vol. 1163, pp. 368–381. Springer, Kyongju, Korea (Nov 1996)
26. Courtois, N.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology - ASIACRYPT 2001. LNCS, vol. 2248, pp. 402–421. Springer, Gold Coast, Australia (2001)
27. Courtois, N.: La sécurité des primitives cryptographiques basées sur des problèmes algébriques multivariables mq, ip, minrank, hfe (2001)
28. Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J.P.: Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Des. Codes Cryptogr. **73**(2), 641–666 (2014)

29. Debris-Alazard, T., Tillich, J.P.: A polynomial attack on a NIST proposal: Ranksign, a code-based signature in rank metric. preprint (Apr 2018), https://eprint.iacr.org/2018/339.pdf, IACR Cryptology ePrint Archive
30. Faugère, J.C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of Minrank. In: Wagner, D. (ed.) Advances in Cryptology - CRYPTO 2008. LNCS, vol. 5157, pp. 280–296 (2008)
31. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)
32. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their applications to cryptography. In: Advances in Cryptology - EUROCRYPT'91. pp. 482–489. No. 547 in LNCS, Brighton (Apr 1991)
33. Gaborit, P., Hauteville, A., Phan, D.H., Tillich, J.P.: Identity-based encryption from rank metric. In: Advances in Cryptology - CRYPTO (2017), https://doi.org/10.1007/978-3-319-63697-9_7
34. Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography WCC'2013. Bergen, Norway (2013), www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf
35. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inform. Theory **62**(2), 1006–1019 (2016)
36. Gaborit, P., Ruatta, O., Schrek, J., Zémor, G.: New results for rank-based cryptography. In: Progress in Cryptology - AFRICACRYPT 2014. LNCS, vol. 8469, pp. 1–12 (2014)
37. Gaborit, P., Schrek, J., Zémor, G.: Full cryptanalysis of the chen identification protocol. In: Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings. pp. 35–50 (2011). https://doi.org/10.1007/978-3-642-25405-5_3
38. Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Inform. Theory **62(12)**, 7245–7252 (2016)
39. Goubin, L., Courtois, N.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) Advances in Cryptology - ASIACRYPT 2000. LNCS, vol. 1976, pp. 44–57. Springer (2000)
40. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Buhler, J. (ed.) Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings. LNCS, vol. 1423, pp. 267–288. Springer (1998)
41. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Advances in Cryptology - CRYPTO'99. LNCS, vol. 1666, pp. 19–30. Springer, Santa Barbara, California, USA (Aug 1999). https://doi.org/10.1007/3-540-48405-1
42. Levy-dit-Vehel, F., Perret, L.: Algebraic decoding of rank metric codes. Talk at the Special Semester on Gröbner Bases - Workshop D1 pp. 1–19 (2006), https://ricamwww.ricam.oeaw.ac.at/specsem/srs/groeb/download/Levy.pdf
43. Melchor, C.A., Aragon, N., Dyseryn, V., Gaborit, P., Z'emor, G.: Lrpc codes with multiple syndromes: near ideal-size kems without ideals. ArXiv **abs/2206.11961** (2022)
44. Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.L.M.: MDPC-McEliece: New McEliece variants from moderate density parity-check codes (2012). https://doi.org/10.1109/ISIT.2013.6620590, http://eprint.iacr.org/2012/409

45. Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission **38**(3), 237–246 (2002). https://doi.org/10.1023/A:1020369320078
46. Overbeck, R.: A new structural attack for GPT and variants. In: Mycrypt. LNCS, vol. 3715, pp. 50–63 (2005)
47. Petzoldt, A., Chen, M., Yang, B., Tao, C., Ding, J.: Design principles for HFEv-based multivariate signature schemes. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I. LNCS, vol. 9452, pp. 311–334. Springer (2015). https://doi.org/10.1007/978-3-662-48797-6_14, https://doi.org/10.1007/978-3-662-48797-6_14
48. Sidelnikov, V.M., Shestakov, S.: On the insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl. **1**(4), 439–444 (1992)
49. Stern, J.: A new identification scheme based on syndrome decoding. In: Stinson, D. (ed.) Advances in Cryptology - CRYPTO'93. LNCS, vol. 773, pp. 13–21. Springer (1993)
50. Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all HFE signature variants. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 70–93. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_4, https://doi.org/10.1007/978-3-030-84242-0_4
51. Verbel, J., Baena, J., Cabarcas, D., Perlner, R., Smith-Tone, D.: On the complexity of "superdetermined" Minrank instances. In: Post-Quantum Cryptography 2019. LNCS, vol. 11505, pp. 167–186. Springer, Chongqing, China (May 2019). https://doi.org/10.1007/978-3-030-25510-7_10, https://doi.org/10.1007/978-3-030-25510-7_10

A Missing proofs from Section 3

It will be helpful to notice that Fact 1 implies

Lemma 2. *Let $T \subset \{1..n-k-1\}$, then*

$$|\boldsymbol{H_y}|_{T,T+k+1} = 1 \tag{19}$$

$$|\boldsymbol{H_y}|_{T,I} = 0 \;\; \textit{if } I \cap \{k+2,\cdots,n\} \not\subseteq T+k+1 \tag{20}$$

Proof. This follows immediately from the fact that $\boldsymbol{H_y}$ is in systematic form in its $n-k-1$ last coordinates (i.e. for the positions $j \in \{k+2,\cdots,n\}$): $\boldsymbol{H}_y = \begin{pmatrix} * \; \boldsymbol{I}_{n-k-1} \end{pmatrix}$. Indeed $|\boldsymbol{H_y}|_{T,T+k+1} = |\boldsymbol{I}_s| = 1$ where $s = \#T$. The other minor is 0 since it contains a column which is 0. □

A.1 Proof of Proposition 1

Let us recall this proposition.

Proposition 1. *The equations in $\mathcal{Q}_0$ can be obtained as linear combinations between the equations in $\mathcal{Q}_{\geq 1}$:*

$$Q_{T+k+1} = -\sum_{Q_I \in \mathcal{Q}_{\geq 1}} |\boldsymbol{H_y}|_{T,I} \, Q_I, \quad \forall T \subset \{1..n-k-1\}, \ \#T = r+1. \tag{21}$$

Proof. We first observe that Q in $\mathcal{Q}_0$ is of the formQ_{T+k+1} with $T \subset \{1..n-k-1\}$, $\#T = r+1$. By definition we have $(\boldsymbol{xG}+\boldsymbol{y})\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}} = 0$ and hence by using the Cauchy-Binet formula (3) we obtain

$$0 = \left| \begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}} \right|_{*,T} = \sum_{\substack{I \subset \{1..n\} \\ \#I = r+1}} |\boldsymbol{H_y}|_{T,I} \, Q_I.$$

We then use Lemma 2: $|\boldsymbol{H_y}|_{T,T+k+1} = 1$, and $|\boldsymbol{H_y}|_{T,I} = 0$ if $I \subset \{k+2..n\}$, $I \neq T+k+1$. The previous equation expresses $Q_{T+k+1} \in \mathcal{Q}_0$ in terms of the Q_I's in $Q_{\geq 1}$, namely $Q_{T+k+1} = -\sum_{Q_I \in \mathcal{Q}_{\geq 1}} |\boldsymbol{H_y}|_{T,I} \, Q_I$. □

A.2 Proofs of Propositions 2 and 3

For the proofs of Propositions 3 and 2, we consider a particular grevlex monomial ordering on the variables $x_1 > \cdots > x_k > c_T$ with the c_T's ordered lexicographically according to T: $c_{T'} > c_T$ if $t'_j = t_j$ for $j < j_0$ and $t'_{j_0} > t_{j_0}$ where $T = \{t_1 < \cdots < t_r\}$ and $T' = \{t'_1 < \cdots < t'_r\}$. We denote by $\mathrm{LT}(f)$ the leading term of a polynomial f with respect to this term order.

We will also make use of the following lemma.

Lemma 3. *Let Q_I be an equation in $\mathcal{Q}_{\geq 2}$. We have*

$$\begin{aligned} \mathrm{LT}(Q_I) &= x_{i_1} c_{I_1} \\ Q_I &= x_{i_1} c_{I_1} \underbrace{-\boldsymbol{xG}_{*,i_2} c_{I_2} + \cdots + (-1)^r \boldsymbol{xG}_{*,i_{r+1}} c_{I_{r+1}}}_{\text{smaller terms of degree 2}} \\ &\quad \underbrace{-y_{i_2} c_{I_2} + \cdots + (-1)^r y_{i_{r+1}} c_{I_{r+1}}}_{\text{smaller terms of degree 1}} \end{aligned}$$

where $I = \{i_1 < \cdots < i_{r+1}\}$ and $I_1 := I \setminus \{i_1\}$. The leading terms of such Q_I's are all different and the variables $\{c_{J+k+1}\}_{J \subset \{1..n-k-1\}}$ do not appear in Q_I.

Proof. Since Q_I is in $\mathcal{Q}_{\geq 2}$ we know that $i_1 \leq k$. We have

$$Q_I = \left| \begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} = \sum_{i_u \in I} (-1)^{1+u} (\boldsymbol{xG}_{*,i_u} + y_{i_u}) c_{I \setminus \{i_u\}}.$$

Taking $\boldsymbol{G}$ and $\boldsymbol{y}$ as in Fact 1, for any $i_u \in I^- = I \cap \{1..k\}$ (and at least $i_1 \in I^-$ by assumption), we have $\boldsymbol{xG}_{*,i_u} + \boldsymbol{y}_{i_u} = x_{i_u}$. Let $I_u = I \setminus \{i_u\}$ for $1 \leq u \leq r+1$, then for the chosen ordering we have $I_1 > I_2 > \cdots > I_{r+1}$. The ordered terms in Q_I are then

$$Q_I = x_{i_1} c_{I_1} \underbrace{-\boldsymbol{x}\boldsymbol{G}_{*,i_2} c_{I_2} + \cdots + (-1)^r \boldsymbol{x}\boldsymbol{G}_{*,i_{r+1}} c_{I_{r+1}}}_{\text{smaller terms of degree 2}}$$
$$\underbrace{-y_{i_2} c_{I_2} + \cdots + (-1)^r y_{i_{r+1}} c_{I_{r+1}}}_{\text{smaller terms of degree 1}}$$

so that $\mathrm{LT}(Q_I) = x_{i_1} c_{I_1}$ and these leading terms are different for all the equations. For the last point, we observe that $\{i_1 < i_2\} \subset \{1..k+1\}$. This implies that for any $i_u \in I$, the set $I \setminus \{i_u\}$ contains at least one of i_1, i_2 so that it is not included in $\{k+2..n\}$, from which it follows that the variables $\{c_{J+k+1}\}_{J \subset \{1..n-k-1\}}$ do not appear in Q_I. ◻

We are ready now to prove Proposition 2:

Proposition 2. *The equations in $\mathcal{P} \cup \mathcal{Q}_{\geq 2}$ are linearly independent. Moreover, each variable c_{J+k+1} for any $J \subset \{1..n-k-1\}$, $\#J = r$ appears only as the leading term of P_J and does not appear in any of the equations in $\mathcal{Q}_{\geq 2}$ nor in $P_{J'}$ with $J' \neq J$.*

Proof. Lemma 2 already proves that the equations in $\mathcal{Q}_{\geq 2}$ are linearly independent. Consider now a $P_J \in \mathcal{P}$. Here $J \subset \{1..n-k-1\}$, $\#J = r$. By using the special shape of $\boldsymbol{H}_{\boldsymbol{y}}$ we have

$$\begin{aligned} P_J = \left|\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}}\right|_{*,J} &= \sum_{\substack{T \subset \{1..n\} \\ \#T = r}} c_T \left|\boldsymbol{H}_{\boldsymbol{y}}\right|_{J,T} = \sum_{\substack{T \subset \{1..n\}, \#T = r, \\ T \cap \{k+2..n\} \subset J+k+1}} c_T \left|\boldsymbol{H}_{\boldsymbol{y}}\right|_{J,T} \\ &= c_{J+k+1} + \sum_{\substack{T \subset \{1..n\}, \#T = r, \\ T \cap \{k+2..n\} \subset J+k+1, T \cap \{1..k+1\} \neq \emptyset}} c_T \left|\boldsymbol{H}_{\boldsymbol{y}}\right|_{J,T} \end{aligned}$$

We used here again Lemma 2. Note that the c_T's in the sum are all smaller than c_{J+k+1}, so that c_{J+k+1} is the leading term of P_J and does not appear in any other $P_{J'}$. This shows that the polynomials in $\mathcal{P} \cup \mathcal{Q}_{\geq 2}$ are linearly independent, as they have distinct leading terms, and concludes the proof of Proposition 2. ◻

Let us now recall Proposition 3 before proving it.

Proposition 3. *The equations in $\mathcal{Q}_1$ reduce to the equations*

$$\mathcal{P} \cup \bigcup_{j=1}^{k} x_j \mathcal{P}$$

modulo the equations in $\mathcal{Q}_{\geq 2}$*. More precisely, for any* $J \subset \{1..n-k-1\},\ \#J = r$ *and* $j \in \{1..k\}$ *we have*

$$P_J = Q_{\{k+1\}\cup(J+k+1)} + \sum_{Q_I \in \mathcal{Q}_{\geq 2}} (-1)^r \left|\boldsymbol{H}\right|_{J\cup\{n-k\},I} Q_I$$
$$x_j P_J = Q_{\{j\}\cup(J+k+1)} + \sum_{Q_I \in \mathcal{Q}_{\geq 2}, j\in I} (-1)^{1+\mathrm{Pos}(j,I)} \left|\boldsymbol{H_y}\right|_{J,I\setminus\{j\}} Q_I$$

where $\mathrm{Pos}(i_u, I) = u$ *for* $I = \{i_1, \cdots, i_{r+1}\}$ *such that* $i_1 < \cdots < i_{r+1}$*.*

Proof. Consider $\left|\begin{pmatrix}\boldsymbol{xG}+\boldsymbol{y}\\ \boldsymbol{C}\end{pmatrix}\boldsymbol{H}^\intercal\right|_{*,J\cup\{n-k\}}$. On one hand, we have with the Cauchy-Binet formula

$$\left|\begin{pmatrix}\boldsymbol{xG}+\boldsymbol{y}\\ \boldsymbol{C}\end{pmatrix}\boldsymbol{H}^\intercal\right|_{*,J\cup\{n-k\}} = \sum_{I\subset\{1..n\},\#I=r+1} \left|\boldsymbol{H}\right|_{J\cup\{n-k\},I} Q_I. \tag{22}$$

On the other hand, we use the particular shapes for $\boldsymbol{H}$, $\boldsymbol{y}$ and $\boldsymbol{h}$ given in Fact 1:

$$\begin{aligned}\boldsymbol{H} &= \begin{pmatrix}\boldsymbol{H_y}\\ \boldsymbol{h}\end{pmatrix}\\ \boldsymbol{y} &= \begin{pmatrix}\boldsymbol{0}_k & 1 & *\end{pmatrix}\\ \boldsymbol{h} &= \begin{pmatrix}* & 1 & \boldsymbol{0}_{n-k-1}\end{pmatrix}\end{aligned}$$

and obtain

$$\begin{pmatrix}\boldsymbol{xG}+\boldsymbol{y}\\ \boldsymbol{C}\end{pmatrix}\boldsymbol{H}^\intercal = \begin{pmatrix}\boldsymbol{yH}^\intercal\\ \boldsymbol{CH}^\intercal\end{pmatrix} = \begin{pmatrix}\boldsymbol{yH_y}^\intercal & \boldsymbol{yh}^\intercal\\ \boldsymbol{CH_y}^\intercal & \boldsymbol{Ch}^\intercal\end{pmatrix} = \begin{pmatrix}\boldsymbol{0}_{n-k-1} & 1\\ \boldsymbol{CH_y}^\intercal & \boldsymbol{Ch}^\intercal\end{pmatrix},$$

so that for any $J \subset \{1..n-k-1\},\ \#J = r$ we get

$$\left|\begin{pmatrix}\boldsymbol{xG}+\boldsymbol{y}\\ \boldsymbol{C}\end{pmatrix}\boldsymbol{H}^\intercal\right|_{*,J\cup\{n-k\}} = \left|\begin{pmatrix}\boldsymbol{0} & 1\\ \boldsymbol{CH_y}^\intercal & \boldsymbol{Ch}^\intercal\end{pmatrix}\right|_{*,J\cup\{n-k\}} = (-1)^r \left|\boldsymbol{CH_y}^\intercal\right|_{*,J} = (-1)^r P_J.$$

By using

$$\left|\boldsymbol{H}\right|_{J\cup\{n-k\},I} = \begin{cases}0 & \text{if } I\cap\{k+2..n\} \not\subset J+k+1\\ (-1)^r & \text{if } I = \{k+1\}\cup(J+k+1),\end{cases}$$

we then have $P_J = \underbrace{Q_{\{k+1\}\cup(J+k+1)}}_{\in\mathcal{Q}_1} + (-1)^r \sum_{Q_I\in\mathcal{Q}_{\geq 2}} \left|\boldsymbol{H}\right|_{J\cup\{n-k\},I} Q_I$.

This gives a one-to-one correspondence between equations P_J and equations $Q_{\{k+1\}\cup J+k+1} \in \mathcal{Q}_1$. It remains to show that the $Q_{\{i_1\}\cup J+k+1} \in \mathcal{Q}_1$ with $i_1 \leq k$ reduce to $x_{i_1} P_J$ modulo $\mathcal{Q}_{\geq 2}$.

If $\boldsymbol{g}_{i_1} := \boldsymbol{G}_{\{i_1\},*}$, we consider $\boldsymbol{H}_{i_1}$ a parity-check matrix of the code $\mathcal{C}_{i_1} := \langle \boldsymbol{y}, \boldsymbol{g}_1, \dots, \boldsymbol{g}_{i_1-1}, \boldsymbol{g}_{i_1+1}, \dots, \boldsymbol{g}_k \rangle$ such that $\boldsymbol{H}_{i_1}^\intercal = \begin{pmatrix} \boldsymbol{H}_{\boldsymbol{y}}^\intercal & \boldsymbol{e}_{i_1}{}^\intercal \end{pmatrix}$ and where $\boldsymbol{e}_{i_1}$ is the i_1-th canonical basis vector in $\mathbb{F}_q^n$. Since $\boldsymbol{g}_{i_1}\boldsymbol{e}_{i_1}^\intercal = 1$, we have

$$\begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H}_{i_1}^\intercal = \begin{pmatrix} x_{i_1}\boldsymbol{g}_{i_1}\boldsymbol{H}_{i_1}^\intercal \\ \boldsymbol{C}\boldsymbol{H}_{i_1}^\intercal \end{pmatrix} = \begin{pmatrix} \boldsymbol{0} & x_{i_1} \\ \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\intercal & \boldsymbol{C}\boldsymbol{e}_{i_1}{}^\intercal \end{pmatrix}.$$

For $J \subset \{1..n-k-1\},\ \#J = r$, one obtains

$$\left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H}_{i_1}^\intercal \right|_{*,J\cup\{n-k\}} = \left| \begin{pmatrix} \boldsymbol{0} & x_{i_1} \\ \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\intercal & \boldsymbol{C}\boldsymbol{h}_{i_1}^\intercal \end{pmatrix} \right|_{*,J\cup\{n-k\}}$$

$$= \sum_{I\subset\{1..n\},\#I=r+1} |\boldsymbol{H}_{i_1}|_{J\cup\{n-k\},I}\, Q_I = (-1)^r x_{i_1} \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\intercal \right|_{*,J} = (-1)^r x_{i_1} P_J.$$

By Laplace expansion along the last row, we have $|\boldsymbol{H}_{i_1}|_{J\cup\{n-k\},I} = 0$ if $i_1 \notin I$ and $|\boldsymbol{H}_{i_1}|_{J\cup\{n-k\},I} = (-1)^{r+1+\mathrm{Pos}(i_1,I)} |\boldsymbol{H}_{\boldsymbol{y}}|_{J,I\setminus\{i_1\}}$ if $i_1 \in I$, where $\mathrm{Pos}(i_1, I)$ denotes the position of i_1 in the ordered set I (1 if it is the first element). We deduce from this that

$$\begin{aligned} x_{i_1} P_J &= \sum_{I\subset\{1..n\},\#I=r+1,i_1\in I} (-1)^{1+\mathrm{Pos}(i_1,I)} |\boldsymbol{H}_{\boldsymbol{y}}|_{J,I\setminus\{i_1\}}\, Q_I \\ &= Q_{\{i_1\}\cup(J+k+1)} + \sum_{Q_I\in\mathcal{Q}_{\geq 2},i_1\in I} (-1)^{1+\mathrm{Pos}(i_1,I)} |\boldsymbol{H}_{\boldsymbol{y}}|_{J,I\setminus\{i_1\}}\, Q_I. \end{aligned}$$

Note that by the previous results, $\mathrm{LT}(Q_{\{i_1\}+J+k+1}) = x_{i_1} c_{J+k+1}$ so that all equations in $\mathcal{P} \cup \bigcup_{j=1}^k x_j \mathcal{P} \cup \mathcal{Q}_{\geq 2}$ are linearly independent.

A.3 Proof of Proposition 5

Proposition 5 is obvious using the previous material, by identifying the leadings terms of the polynomials. Let us first recall it.

Proposition 5. *The equations in* $\mathrm{Unfold}(\mathcal{Q}_{\geq 2})$ *satisfy* $\mathrm{LT}(Q_{i,I}) = x_{i,i_1} c_{I\setminus\{i_1\}}$ *with* $i_1 = \min(I) \leq k$. *In particular, they are all linearly independent over* $\mathbb{F}_q$.

Proof. For $Q_I \in \mathcal{Q}_{\geq 2}$ and $1 \leq i \leq m$, the leading term of Q_I is $x_{i_1} c_{I\setminus\{i_1\}} = \sum_{\ell=1}^m \beta_\ell x_{\ell,i_1} c_{I\setminus\{i_1\}}$ and the other monomials involve smaller c_T's, hence $\mathrm{LT}(Q_{i,I}) = x_{i,i_1} c_{I\setminus\{i_1\}}$. ☐

A.4 Proof of Proposition 4

Let us first recall this proposition.

Proposition 4. *For any $b \geq 1$, the $\mathbb{F}_{q^m}$-vector space generated by the equations $\mathcal{Q}_{\geq 2}$ augmented at bi-degree $(b, 1)$ by multiplying by monomials of degree $b-1$ in the x_i variables has dimension*

$$\mathcal{N}_b^{\mathbb{F}_{q^m}} := \sum_{i=1}^{k} \binom{n-i}{r}\binom{k+b-1-i}{b-1} - \binom{n-k-1}{r}\binom{k+b-1}{b}, \tag{23}$$

and there are

$$\mathcal{M}_b^{\mathbb{F}_{q^m}} := \binom{k+b-1}{b}\left(\binom{n}{r} - \binom{n-k-1}{r}\right) \tag{24}$$

monomials of degree $(b, 1)$. We have $\mathcal{N}_b^{\mathbb{F}_{q^m}} < \mathcal{M}_b^{\mathbb{F}_{q^m}} - 1$ for any $b \geq 1$.

Proof. To prove Proposition 4, we describe a basis of the $\mathbb{F}_{q^m}$-vector space generated by the equations $\mathcal{Q}_{\geq 2}$ augmented at bi-degree $(b, 1)$:

$$\mathcal{B}_b = \left\{ {x_{i_1}}^{\alpha_{i_1}} \cdots {x_k}^{\alpha_k} Q_I : I = \{i_1 < i_2 < \cdots < i_{r+1}\}, i_2 \leq k+1, \sum_{j \geq i_1} \alpha_j = b-1 \right\} \tag{25}$$

The set $\mathcal{B}_b$ clearly contains linearly independent equations, since their leading terms are all different:

$$\mathrm{LT}({x_{i_1}}^{\alpha_{i_1}} \cdots {x_k}^{\alpha_k} Q_I) = {x_{i_1}}^{\alpha_{i_1}+1} \cdots {x_k}^{\alpha_k} c_{I \setminus \{i_1\}}.$$

The number of polynomials in $\mathcal{B}_b$ is the number of sets I and $(\alpha_{i_1}, \ldots, \alpha_k)$:

$$\mathcal{N}_b = \sum_{i_1=1}^{k} \sum_{i_2=i_1+1}^{k+1} \binom{n-i_2}{r-1}\binom{k-i_1+1+b-2}{b-1}$$

which gives Eq. (23), considering the identities $\sum_{i_2=i_1+1}^{k+1} \binom{n-i_2}{r-1} = \binom{n-i_1}{r} - \binom{n-k-1}{r}$ and $\sum_{i_1=1}^{k} \binom{k-i_1+1+b-2}{b-1} = \binom{k+b-1}{b}$. The number of monomials comes from the fact that the variables c_{J+k+1} do not appear in $\mathcal{Q}_{\geq 2}$. The inequality $\mathcal{N}_b < \mathcal{M}_b - 1$ is easy to derive using previous identities and $\binom{n-i_1}{r} < \binom{n-1}{r}$ for all $i_1 \geq 1$.

We will now show that the polynomials $x_j Q_I$ for $1 \leq j < i_1$, $Q_I \in \mathcal{Q}_{\geq 2}$ reduce to zero modulo $\mathcal{B}_2$, which is sufficient to conclude the proof. The number of such polynomials is equal to the number of sets $K = \{k_1 < k_2 < \cdots < k_{r+2}\} \subset \{1..n\}$ such that $k_3 \leq k+1$, and we are going to construct the same number of independent syzygies between the polynomials at bi-degree $(2, 1)$. Indeed, for any such K, we have the relation

$$\left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,K} = 0. \tag{26}$$

By Laplace expansion along the first row, one obtains

$$0 = x_{k_1} Q_{\{k_2,\dots,k_{r+2}\}} - \sum_{u=2}^{r+2} (-1)^u \left(\sum_{j=1}^{k} x_j \boldsymbol{G}_{j,k_u} + y_{k_u} \right) Q_{K\setminus\{k_u\}}.$$

Since $|K \cap \{1..k+1\}| \geq 3$, we obtain syzygies between the relevant Q_I, say those such that $|I \cap \{1..k+1\}| \geq 2$. We will now show that those syzygies are linearly independent. To this end, we order the Q_I's according to a grevlex order on the subsets I as for the c_T variables. The largest Q_I is $Q_{\{n-r,\dots,n\}}$, the smallest one is $Q_{\{1..r+1\}}$. The syzygy associated to K is given by

$$\mathcal{G}^K := \left(\underbrace{0}_{I \not\subset K}, \underbrace{(-1)^{1+u} \sum_{j=1}^{k} x_j \boldsymbol{G}_{j,k_u} + \boldsymbol{y}_{k_u}}_{K \setminus I = \{k_u\}} \right)_{I \subset \{1..n\}, \#I = r+1}.$$

The largest set I such that the coefficient in front of Q_I in $\mathcal{G}^K$ is non-zero is $I = K_1 = K \setminus \{k_1\}$ and this coefficient is x_{k_1}. The syzygies which have the same leading position Q_{K_1} as $\mathcal{G}^K$ are the $\mathcal{G}^{K_1 \cup \{j\}}$ for $1 \leq j < k_1$. Finally, the highest degree part in the coefficient in front of Q_{K_1} in $\mathcal{G}^{K_1 \cup \{j\}}$ is x_j, which shows that all the $\mathcal{G}^{K_1 \cup \{j\}}$ are linearly independent for $1 \leq j \leq k_1$. □

A.5 Proof of Proposition 8

Let us recall this proposition.

Proposition 8. *For any $T \subset \{1..n-k-1\}$, $\#T = r+1$ and $1 \leq i \leq m$, we obtain a relation between the $\widetilde{Q}_I$ equations given by*

$$\mathrm{Tr}(\beta_i^\star) \widetilde{Q}_{T+k+1} + \sum_{\substack{I \subset \{1..n\} \\ \#I = r+1 \\ I \cap \{k+1..n\} \subsetneq T+k+1}} \mathrm{Tr}(\beta_i^\star \, |\boldsymbol{H}_{\boldsymbol{y}}|_{T,I}) \widetilde{Q}_I = 0. \tag{27}$$

Note that the coefficients of any of these relations belong to $\mathbb{F}_q$.

Proof. For this purpose, we introduce the ℓ-th Frobenius iterate of the P_J's, that has the advantage to satisfy the relation $\left|\boldsymbol{M}^{[\ell]}\right| = |\boldsymbol{M}|^{[\ell]}$ for any square matrix $\boldsymbol{M}$. This is equivalent to using the unfolded equations $P_{i,J}$ thanks to the following relation: for any $J \subset \{1..n-k-1\}, \#J = r$ we have

$$\langle P_{i,J} : 1 \leq i \leq m \rangle_{\mathbb{F}_{q^m}} = \langle P_J^{[\ell]} : 0 \leq \ell \leq m-1 \rangle_{\mathbb{F}_{q^m}}.$$

We have $P_{i,J} = \mathrm{Tr}(\beta_i^\star P_J) = \sum_{\ell=0}^{m-1} (\beta_i^\star)^{[\ell]} P_J^{[\ell]}$ and $P_J^{[\ell]} = \sum_{i=1}^{m} \beta_i^{[\ell]} P_{i,J}$.

For fixed $0 \leq \ell \leq m-1$ and $T \subset \{1..n-k-1\}, \#T = r+1$, we consider the minor

$$\mathit{\Gamma}_{\ell,T} := \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} (\boldsymbol{H}_{\boldsymbol{y}}{}^{[\ell]})^\intercal \right|_{*,T}.$$

By Laplace expansion along the first row, this minor can be viewed as a combination with coefficients in $\mathbb{F}_{q^m}[x_i]$ between maximal minors of $\boldsymbol{C}({\boldsymbol{H}_{\boldsymbol{y}}}^{[\ell]})^{\mathsf{T}}_{*,T}$, and these minors are exactly the ${P_J}^{[\ell]}$'s for $J \subset T$. The normal form of $\mathit{\Gamma}_{\ell,T}$ with respect to $\langle P_{i,J}\rangle = \langle P_J^{[\ell]}\rangle$ is then 0. Also, using the Cauchy-Binet formula, each minor is a linear combination of the Q_I's, given by

$$\tilde{Q}_{T+k+1} + \sum_{\substack{I\subset\{1..n\},\#I=r+1,\\ I\cap\{k+1..n\}\subsetneq T+k+1}} \tilde{Q}_I \left|{\boldsymbol{H}_{\boldsymbol{y}}}^{[\ell]}\right|_{T,I} = 0.$$

To conclude the proof, we use the fact that the set of previous equations for all $0 \leq \ell \leq m-1$ generate the same vector space over $\mathbb{F}_{q^m}$ as the set of equations

$$\mathrm{Tr}(\beta_i^\star)\tilde{Q}_{T+k+1} + \sum_{\substack{I\subset\{1..n\}\\ \#I=r+1\\ I\cap\{k+1..n\}\subsetneq T+k+1}} \mathrm{Tr}(\beta_i^\star\left|\boldsymbol{H}_{\boldsymbol{y}}\right|_{T,I})\tilde{Q}_I = 0,$$

for all $1 \leq i \leq m$. □