A new approach based on quadratic forms to attack the McEliece cryptosystem

Alain Couvreur[1], Rocco Mora[2], and Jean-Pierre Tillich[2]

[1] Inria Saclay, LIX, CNRS UMR 7161, École Polytechnique, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau Cedex
[2] Inria Paris, 2 rue Simone Iff, 75012 Paris, France
{alain.couvreur,rocco.mora,jean-pierre.tillich}@inria.fr

Abstract. We bring in here a novel algebraic approach for attacking the McEliece cryptosystem which is right now at the 4-th round of the NIST competition. It consists in introducing a subspace of matrices representing quadratic forms. Those are associated with quadratic relationships for the component-wise product in the dual of the Goppa (or alternant) code of the cryptosystem. Depending on the characteristic of the field over which the code is defined, this space of matrices consists only of symmetric matrices (odd characteristic) or skew-symmetric matrices (characteristic 2). It turns out that this matrix space contains unusually low-rank matrices (rank 3 matrices in odd characteristic, rank 2 matrices for characteristic 2) which reveal the secret polynomial structure of the code. Finding such matrices can then be used to recover the secret key of the scheme. We devise a dedicated approach in characteristic 2 consisting in using a Gröbner basis modeling that a skew-symmetric matrix is of rank 2. This allows to analyze the complexity of solving the corresponding algebraic system with Gröbner bases techniques. This computation behaves differently when applied to the skew-symmetric matrix space associated with a random code rather than with a Goppa or an alternant code. This gives a distinguisher of the latter code family. We give a bound on its complexity which turns out to interpolate nicely between polynomial and exponential depending on the code parameters. A distinguisher for alternant/Goppa codes was already known [FGO$^+$11]. It is of polynomial complexity but works only in a narrow parameter regime. This new distinguisher is also polynomial for the parameter regime necessary for [FGO$^+$11] but contrarily to the previous one is able to operate for virtually all code parameters relevant to cryptography. Moreover, we use this matrix space to find a polynomial time attack of the McEliece cryptosystem provided that the Goppa code is distinguishable by the method of [FGO$^+$11] and its degree is less than $q - 1$, where q is the alphabet size of the code.

1 Introduction

The McEliece Cryptosytem

The McEliece encryption scheme [McE78], which is only a few months older than RSA [RSA78], is a code-based cryptosystem built upon the family of binary

Goppa codes. It is equipped with very fast encryption and decryption algorithms and has very small ciphertexts but large public key size. Contrarily to RSA which is broken by quantum computers [Sho94], it is also widely viewed as a viable quantum-safe cryptosystem. A variation of this public key cryptosystem intended to be IND-CCA secure and an associated key exchange protocol [ABC$^+$22] is one of the three code-based remaining candidates in the fourth round of the NIST post-quantum competition on post-quantum cryptography. Its main selling point for being standardized is that it is the oldest public key cryptosystem which has resisted all possible attacks be they classical or quantum so far, this despite very significant efforts to break it.

The consensus right now about this cryptosystem is that key-recovery attacks that would be able to exploit the underlying algebraic structure are way more expensive than message-recovery attacks that use decoding algorithms for generic linear codes. Because of this reason, the parameters of the McEliece are chosen according to the latest algorithms for decoding a linear code. This is also actually another selling point for this cryptosystem, since despite significant efforts on improving the algorithms for decoding linear codes, all the classical algorithms for performing this task are of exponential complexity and this exponent has basically only decreased by less than 20 percent for most parameters of interest after more than 60 years of research [Pra62, Ste88, Dum89, CC98, MMT11, BJMM12, MO15, BM17]. The situation is even more stable when it comes to quantum algorithms [Ber10, KT17].

Key Recovery Attacks

The best key recovery attack has not changed for many years. It was given in [LS01] and consists in checking all Goppa polynomials and all possible supports with the help of [Sen00]. Its complexity is also exponential with an exponent which is much bigger than the one obtained for message recovery attacks. There has been some progress on this issue, not on the original McEliece cryptosystem, but on variations of it. This concerns very high rate binary Goppa codes for devising signature schemes [CFS01], non-binary Goppa codes over large alphabets [BLP10, BLP11], or more structured versions of the McEliece system, based on quasi-cyclic alternant codes [BCGO09, CBB$^+$17] (a family of algebraic codes containing Goppa codes retaining the essential algebraic features of Goppa codes) or on quasi-dyadic Goppa codes such as [MB09, BLM11, BBB$^+$17].

The quasi-cyclic or quasi-dyadic alternant/Goppa codes have been attacked in [FOPT10, GUL09] by providing a suitable algebraic modeling for the secret key and then solving the algebraic system with Gröbner bases techniques. This algebraic modeling tries to recover the underlying polynomial structure of these codes coming from the underlying generalized Reed-Solomon structure by using just an arbitrary generator matrix of the alternant or Goppa code which is given by the public key of the scheme. This is basically the secret key of the scheme. It allows to decode the alternant or Goppa code and therefore all possible ciphertexts. Recall that a generalized Reed-Solomon code is defined by

Definition 1 (Generalized Reed-Solomon (GRS) code). *Let $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}^n$ be a vector of pairwise distinct entries and $\boldsymbol{y} = (y_1, \dots, y_n) \in \mathbb{F}^n$ a vector of nonzero entries, where $\mathbb{F}$ is a finite field. The generalized Reed-Solomon (GRS) code over $\mathbb{F}$ of dimension k with support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$ is*

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \overset{def}{=} \{(y_1 P(x_1), \dots, y_n P(x_n)) \mid P \in \mathbb{F}[z], \deg P < k\}.$$

Alternant codes are defined as subfield subcodes of GRS codes, meaning that an alternant code $\mathscr{A}$ of length n is defined over some field $\mathbb{F}_q$ whereas the underlying GRS code $\mathscr{C}$ is defined over an extension field $\mathbb{F}_{q^m}$ of degree m. The alternant code is defined in this case as the set of codewords of the GRS code whose entries all belong to the subfield $\mathbb{F}_q$, *i.e*

$$\mathscr{A} = \mathscr{C} \cap \mathbb{F}_q^n.$$

Rather than trying to recover the polynomial structure of the underlying GRS code, these algebraic attacks actually recover the polynomial structure of the *dual code.* Recall that the dual code of a linear code is defined by

Definition 2 (dual code). *The dual $\mathscr{C}^\perp$ of a linear code $\mathscr{C}$ of length n over $\mathbb{F}_q$ is the subspace of $\mathbb{F}_q^n$ defined by $\mathscr{C}^\perp \overset{def}{=} \{\boldsymbol{d} \in \mathbb{F}_q^n : \boldsymbol{d} \cdot \boldsymbol{c} = 0, \ \forall \boldsymbol{c} \in \mathscr{C}\}$, where $\boldsymbol{d} \cdot \boldsymbol{c} = \sum_{i=1}^n c_i d_i$ with $\boldsymbol{c} = (c_i)_{1 \leqslant i \leqslant n}$ and $\boldsymbol{d} = (d_i)_{1 \leqslant i \leqslant n}$.*

The dual code of an alternant code has also a polynomial structure owing to the fact that the dual of a GRS code is actually a GRS code:

Proposition 1. *[MS86, Theorem 4, p. 304] Let $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ be a GRS code of length n. Its dual is also a GRS code. In particular $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp = \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}^\perp)$, with $\boldsymbol{y}^\perp \overset{def}{=} \left(\frac{1}{\pi'_{\boldsymbol{x}}(x_1) y_1}, \dots, \frac{1}{\pi'_{\boldsymbol{x}}(x_n) y_n}\right)$, where $\pi_{\boldsymbol{x}}(z) \overset{def}{=} \prod_{i=1}^n (z - x_i)$ and $\pi'_{\boldsymbol{x}}$ is its derivative.*

It is actually the dual of the underlying GRS code which serves to define the multiplier and the support of an alternant code as shown by

Definition 3 (alternant code). *Let $n \leqslant q^m$, for some positive integer m. Let $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ be the GRS code over $\mathbb{F}_{q^m}$ of dimension r with support $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ and multiplier $\boldsymbol{y} \in (\mathbb{F}_{q^m}^*)^n$. The alternant code with support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$, degree r over $\mathbb{F}_q$ is*

$$\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) \overset{def}{=} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp \cap \mathbb{F}_q^n = \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}^\perp) \cap \mathbb{F}_q^n.$$

The integer m is called extension degree of the alternant code.

It is much more convenient to recover with an algebraic modeling the support and the multiplier of the dual of the underlying GRS code because *any* codeword $\boldsymbol{c} = (c_i)_{1 \leqslant i \leqslant n}$ of the alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ is readily seen to be orthogonal to any codeword $\boldsymbol{d}$ of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$, *i.e.* $\boldsymbol{c} \cdot \boldsymbol{d} = 0$. The algebraic modeling of [FOPT10] is based on such equations where the unknowns are the entries of $\boldsymbol{x}$ and $\boldsymbol{y}$. Goppa codes can be recovered from this approach too, since they are particular alternant codes

Definition 4 (Goppa code). *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ be a support vector and $\Gamma \in \mathbb{F}_{q^m}[z]$ a polynomial of degree r such that $\Gamma(x_i) \neq 0$ for all $i \in \{1, \ldots, n\}$. The Goppa code of degree r with support $\boldsymbol{x}$ and Goppa polynomial Γ is defined as $\mathscr{G}(\boldsymbol{x}, \Gamma) \overset{def}{=} \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$, where $\boldsymbol{y} \overset{def}{=} \left(\frac{1}{\Gamma(x_1)}, \ldots, \frac{1}{\Gamma(x_n)}\right)$.*

This approach worked because the quasi cyclic/dyadic structure allowed to reduce drastically the number of unknowns of the algebraic system when compared to the original McEliece cryptosystem. A variant of this algebraic modeling was introduced in [FPdP14] to attack certain parameters of the variant of the McEliece cryptosystem [BLP10, BLP11] based on wild Goppa codes/wild Goppa codes incognito. It only involves equations on the multiplier $\boldsymbol{y}$ of the Goppa code induced by the wild Goppa structure. The McEliece cryptosystem based on plain binary Goppa codes seems immune to both approaches. The first one because the degree and the number of variables of the resulting system are most certainly too big to make such an approach likely to succeed if not at the cost of a very high exponential complexity (but this has to be confirmed by a rigorous analysis which is hard to perform because Gröbner bases techniques perform here very differently from a generic system). The second one because this modeling does not apply to binary Goppa codes. In particular, it needs a very small extension degree and a code alphabet size that are prime powers rather than prime.

It was also found that Gröbner bases techniques when applied to the algebraic system [FOPT10] behaved very differently when the system corresponds to a Goppa code instead of a random linear code of the same length and dimension. This approach led to [FGO$^+$11] that gave a way to distinguish high-rate Goppa codes from random codes. It is based on the kernel of a linear system related to the aforementioned algebraic system. It was shown there to have an unexpectedly high dimension when instantiated with Goppa codes or the more general family of alternant codes rather than with random linear codes. Another interpretation was later on given to this distinguisher in [MP12], where it was proved that the kernel dimension is related to the dimension of the square of the dual of the Goppa code. Very recently, [MT22] revisited [FGO$^+$11] and gave rigorous bounds for the dimensions of the square codes of Goppa or alternant codes and a better insight into the algebraic structure of these squares. Recall here that the component-wise/Schur product/square of codes is defined from the component-wise/Schur product of vectors $\boldsymbol{a} = (a_i)_{1 \leqslant i \leqslant n}$ and $\boldsymbol{b} = (b_i)_{1 \leqslant i \leqslant n}$

$$\boldsymbol{a} \star \boldsymbol{b} \overset{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$$

by

Definition 5. *The component-wise product of codes $\mathscr{C}, \mathscr{D}$ over $\mathbb{F}$ with the same length n is defined as*

$$\mathscr{C} \star \mathscr{D} \overset{def}{=} \langle \boldsymbol{c} \star \boldsymbol{d} \mid \boldsymbol{c} \in \mathscr{C}, \boldsymbol{d} \in \mathscr{D} \rangle_{\mathbb{F}}.$$

If $\mathscr{C} = \mathscr{D}$, we call $\mathscr{C}^{\star 2} \overset{def}{=} \mathscr{C} \star \mathscr{C}$ the square code of $\mathscr{C}$.

The reason why Goppa codes behave differently from random codes for this product is essentially because the underlying GRS code behaves very abnormally with respect to the component-wise product. Indeed,

Proposition 2. *[CGG+14] Let $\mathbf{GRS}_k(\boldsymbol{x},\boldsymbol{y})$ be a GRS code with support $\boldsymbol{x}$, multiplier $\boldsymbol{y}$ and dimension k. We have $\mathbf{GRS}_k(\boldsymbol{x},\boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2k-1}(\boldsymbol{x},\boldsymbol{y}\star\boldsymbol{y})$. Hence, if $k \leqslant \frac{n+1}{2}$, $\dim_{\mathbb{F}_{q^m}}(\mathbf{GRS}_k(\boldsymbol{x},\boldsymbol{y}))^{\star 2} = 2k-1$.*

On the other hand, random linear codes behave very differently, because they attain with probability close to 1 [CCMZ15] the general upper bound on the dimension given by $\dim_{\mathbb{F}} \mathscr{C}^{\star 2} \leqslant \min\left(n, \binom{\dim_{\mathbb{F}} \mathscr{C}+1}{2}\right)$. In other words, the dimension of the square of a random linear code scales quadratically as long as the dimension is $k = \mathcal{O}(\sqrt{n})$ and attains after this the full dimension n, whereas the dimension of the square of a GRS code of dimension k increases only linearly in k. This peculiar property of GRS codes survives in a disguised form in the square of the dual of an alternant/Goppa code as shown by [MT22].

This tool was also instrumental in another breakthrough in this area, namely that for the first time a polynomial attack [COT14] was found on the McEliece scheme when instantiated with Goppa codes. This was done by using square code considerations. However, this attack required very special parameters to be carried out: (i) the extension degree should be 2, (ii) the Goppa code should be a wild Goppa code. It is insightful to remark that this attack exploits the unusually low dimension of the square of wild Goppa codes when their dimension is low enough whereas the distinguisher of [FGO+11] actually uses the small dimension of the square of the *dual* of a Goppa or alternant code. The dual of such codes has a much more involved structure, in particular it loses a lot of the nice polynomial structure of the Goppa code (this was essential in the attack performed in [COT14]). This is probably the reason why for a long time the distinguisher of [FGO+11] has not turned into an actual attack. However, recently in [BMT23] it has been found out that in certain cases (i) very small field size $q = 2$ or $q = 3$ over which the code is defined, (ii) being a *generic alternant code* rather than being in the special case of Goppa code, (iii) being in the region of parameters where the distinguisher of [FGO+11] applies, then this distinguisher can actually be turned into a polynomial-time attack. Note that this paper also made some crucial improvements in the algebraic modeling of [FOPT10] (in particular by adding low-degree equations that take into account that the multiplier and support of the alternant/Goppa code should satisfy certain constraints).

A new approach

A first idea: abnormal quadratic relations in the extended dual alternant/Goppa code. We devise in this submission two radically new attacks on the McEliece cryptosystem when it is based on alternant or Goppa codes. Both exploit the structure of the extension over a larger field of the dual of an alternant/Goppa code. The extension of a code over a field extension is given by

Definition 6 (extension of a code over a field extension). *Let $\mathscr{C}$ be a linear code over $\mathbb{F}_q$. We denote by $\mathscr{C}_{\mathbb{F}_{q^m}}$ the $\mathbb{F}_{q^m}$-linear span of $\mathscr{C}$ in $\mathbb{F}_{q^m}^n$.*

It turns out that the extension of the dual of an alternant code contains actually GRS codes as shown by

Proposition 3. *[BMT23] Let $\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})$ be an alternant code over $\mathbb{F}_q$. Then $\left(\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^\perp\right)_{\mathbb{F}_{q^m}} = \sum_{j=0}^{m-1} \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^j)} = \sum_{j=0}^{m-1} \mathbf{GRS}_r(\boldsymbol{x}^{q^j},\boldsymbol{y}^{q^j})$.*

Observe now that a GRS code contains non-zero codewords $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$ satisfying a very peculiar property, namely

$$\boldsymbol{c}_1 \star \boldsymbol{c}_3 = \boldsymbol{c}_2^{\star 2}. \tag{1}$$

This comes by choosing $\boldsymbol{c}_1 = \boldsymbol{y}\boldsymbol{x}^a = (y_i x_i^a)_{1 \leqslant i \leqslant n}$, $\boldsymbol{c}_2 = \boldsymbol{y}\boldsymbol{x}^b = (y_i x_i^b)_{1 \leqslant i \leqslant n}$ and $\boldsymbol{c}_3 = \boldsymbol{y}\boldsymbol{x}^c = (y_i x_i^c)_{1 \leqslant i \leqslant n}$ for any a, b, c in $[\![0, r-1]\!]$ satisfying $b = \frac{a+c}{2}$. Such a relation is unlikely to hold in a random linear code of dimension k, unless it is of rate k/n close to 1. Therefore the dual code of our alternant or Goppa code contains very peculiar codewords. The issue is now how to find them?

A new concept: the code of quadratic relationships. Equation (1) can be viewed as a quadratic relation between codewords. There is a natural object that can be brought in that encodes in a natural way quadratic relations

Definition 7 (Code of quadratic relations). *Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}$ and let $\mathcal{V} = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\}$ be a basis of $\mathscr{C}$. The **code of relationships between the Schur's products with respect to $\mathcal{V}$** is*

$$\mathscr{C}_{rel}(\mathcal{V}) \overset{def}{=} \{\boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k} \mid \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j = 0\} \subseteq \mathbb{F}^{\binom{k+1}{2}}.$$

Such an element $\boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k}$ of $\mathscr{C}_{\mathrm{rel}}(\mathcal{V})$ defines a quadratic form as

$$Q_{\boldsymbol{c}}(x_1, \cdots, x_k) = \sum_{i \leqslant j} c_{i,j} x_i x_j.$$

When a basis $\mathcal{V}$ containing the aforementioned $\boldsymbol{c}_i$ is chosen, this means that there exists a codeword in $\mathscr{C}_{\mathrm{rel}}(\mathcal{V})$ whose associated quadratic form is of the form $x_i x_j - x_\ell^2$ (for $\boldsymbol{v}_i = \boldsymbol{c}_1$, $\boldsymbol{v}_j = \boldsymbol{c}_3$, $\boldsymbol{v}_\ell = \boldsymbol{c}_2$). In other words, this quadratic form is of rank 3 (in odd characteristic). To find such abnormal codewords it is convenient to represent the elements of $\mathscr{C}_{\mathrm{rel}}(\mathcal{V})$ as matrices corresponding to the bilinear map given by the polar form of the quadratic form, i.e. the matrix $\boldsymbol{M}_{\boldsymbol{c}}$ corresponding to $\boldsymbol{c} \in \mathscr{C}_{\mathrm{rel}}(\mathcal{V})$ that satisfies for all $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_{q^m}^k$

$$\boldsymbol{x}\boldsymbol{M}_{\boldsymbol{c}}\boldsymbol{y}^\intercal = Q_{\boldsymbol{c}}(\boldsymbol{x}+\boldsymbol{y}) - Q_{\boldsymbol{c}}(\boldsymbol{x}) - Q_{\boldsymbol{c}}(\boldsymbol{y}). \tag{2}$$

This definition allows to have a matrix definition of the quadratic form which works both in odd characteristic and characteristic 2 and which satisfies the crucial relation (3) when the basis is changed. Note that $\boldsymbol{M}_{\boldsymbol{c}}$ is symmetric in odd characteristic, whereas it is skew-symmetric in characteristic 2.

Definition 8 (Matrix code of relationships). *Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}$ and let $\mathcal{V} = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\}$ be a basis of $\mathscr{C}$. The* ***matrix code of relationships between the Schur's products with respect to*** *$\mathcal{V}$ is*

$$\mathscr{C}_{mat}(\mathcal{V}) \overset{def}{=} \{\boldsymbol{M_c} = (m_{i,j})_{\substack{1 \leqslant i \leqslant k \\ 1 \leqslant j \leqslant k}} \mid \boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k} \in \mathscr{C}_{rel}(\mathcal{V})\} \subseteq \mathbf{Sym}(k, \mathbb{F}),$$

where $\boldsymbol{M_c}$ is defined as $\begin{cases} m_{i,j} \overset{def}{=} m_{j,i} \overset{def}{=} c_{i,j}, & 1 \leqslant i < j \leqslant k, \\ m_{i,i} \overset{def}{=} 2c_{i,i}, & 1 \leqslant i \leqslant k. \end{cases}$

The previous discussion shows that if $\mathcal{V}$ contains the triple $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$, then there exists a matrix of rank 3 in the matrix code of relationships in odd characteristic. Note that the matrix is of rank 2 in characteristic 2 since the polar form corresponding to the quadratic form $Q(\boldsymbol{x}) = x_i x_j - x_\ell^2$ is given by $(x_i + y_i)(x_j + y_j) - (x_\ell + y_\ell)^2 - x_i x_j + x_\ell^2 - y_i y_j + y_\ell^2 = x_i y_j + x_j y_i$.

Now the point is that even if we do not have a basis containing the $\boldsymbol{c}_i$'s, there are still rank 3 (or 2) matrices in the matrix code of relationships. This holds because a change of basis basically amounts to a congruent matrix code. Indeed if $\mathcal{A}$ and $\mathcal{B}$ are two different bases of the same code, there exists (see Proposition 4) an invertible $\boldsymbol{P} \in \mathbb{F}^{k \times k}$ such that

$$\mathscr{C}_{\text{mat}}(\mathcal{A}) = \boldsymbol{P}^\intercal \mathscr{C}_{\text{mat}}(\mathcal{B}) \boldsymbol{P}. \tag{3}$$

Therefore for any choice of basis, there exists a rank 3 matrix in the corresponding matrix code of relationships. Finding such matrices can be viewed as a MinRank problem for rank 3 with symmetric matrices

Problem 1 (Symmetric MinRank problem for rank r). Let $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ be K symmetric matrices in $\mathbb{F}^{N \times N}$. Find an $\boldsymbol{M} \in \langle \boldsymbol{M}_1, \cdots, \boldsymbol{M}_K \rangle_{\mathbb{F}}$ of rank r.

Of course, the dimension of the matrix code could be so large that there are rank 3 (or 2) matrices which are here by chance and which are not induced by these unusual quadratic relations between codewords of the GRS code. We will study this problem and will give in Section 4 bounds on the parameters of the problem which rule out this possibility. Basically, the parameters that we will encounter for breaking McEliece-type systems will avoid this phenomenon.

A dedicated algebraic approach for finding rank 2 in a skew-symmetric matrix code. There are many methods which can be used to solve the MinRank problem, be they combinatorial [GC00], based on an algebraic modeling and solving them with Gröbner basis or XL type techniques, such as [KS99, FLP08, FSEDS10, VBC+19, BBC+20] or hybrid methods [BBB+22]. Basically all of them can be adapted to the symmetric MinRank problem. One of the most attractive methods for solving the problem for the parameters we have is the Support Minors approach introduced in [BBC+20]. Unfortunately due to the symmetric of skew-symmetric form of the matrix space, solving the corresponding system with the proposed XL type approach behaves very differently from a generic matrix space and its complexity seems very delicate to predict. For this reason, we have devised another way of solving the corresponding MinRank problem in characteristic 2 by taking advantage that we know a Gröbner basis for the algebraic system expressing that a skew-symmetric matrix is of rank $\leqslant 2$ by using the nullity of all minors of size greater than 2. This allows us to understand the complexity of solving the corresponding algebraic system consisting in adding to this Gröbner basis the linear equations expressing that the skew-symmetric matrix should also belong to the matrix code of relationships. It turns out that the Gröbner basis computation behaves differently when applied to the skew-symmetric matrix space associated with a random code rather than with a Goppa or an alternant code. This clearly yields a way to distinguish a Goppa code or more generally an alternant code from a random code. Contrarily to the distinguisher that has been devised in [FGO$^+$11] which works only for a very restricted set of parameters, this new distinguisher basically works for virtually all code parameters relevant to cryptography. This very simple observation can be made rigorous and we can give a bound on the degree at which the Gröbner basis computation sees a difference. From this, we can derive a bound on the complexity of the distinguisher. Interestingly enough, this complexity stays polynomial for the regime of parameters where [FGO$^+$11] works and scales smoothly between polynomial and exponential in between.

A new attack exploiting rank defective matrices in the matrix code of relationships. There is another way to exploit this matrix code which consists in observing that for a restricted set of code parameters (i) the degree r of the alternant code is less than $q+1$ or $q-1$ in the Goppa case, (ii) the code is distinguishable with the method of [FGO$^+$11], a rank defective matrix in the matrix code of relationships leaks information on the secret polynomial structure of the code. This can be used to mount a simple attack by just (i) looking for such matrices by picking enough random elements in the matrix code and verifying if they are rank defective (ii) and then exploiting the information gathered here to recover the support and multiplier of the alternant/Goppa code.

Summary of the contributions. In a nutshell, our contributions are

- We introduce a new concept, namely the matrix code of quadratic relationships which can be derived from the extended dual of the Goppa/alternant code for which we want to recover its polynomial structure. This is a subspace of symmetric or skew-symmetric matrices depending on the field characteristic over which the code is defined which has the particular feature of containing very low-rank matrices (rank 3 in odd characteristic, rank 2 in characteristic 2) which are related to the secret key of the corresponding McEliece cryptosystem.
- We devise a dedicated algebraic approach for finding these low-rank matrices in characteristic 2 when this subspace of matrices is formed by skew-symmetric matrices. It takes advantage of the fact that we know a Gröbner

basis for the algebraic system expressing the fact that a skew-symmetric matrix is of rank $\leqslant 2$ based on the nullity of all minors of size greater than 2. This system can be solved with the help of Gröbner bases techniques. It turns out that the solving process behaves differently when applied to the matrix code of quadratic relationships associated with a random linear code rather than with a Goppa or an alternant code. This gives a way to distinguish a Goppa code or more generally an alternant code from a random code which contrarily to the distinguisher of [FGO$^+$11, FGO$^+$13] works for virtually all code parameters relevant to cryptography (recall that the latter works only for very high rate Goppa or alternant codes). Moreover, the complexity of this system solving can be analyzed and an upper bound on the complexity of the distinguisher can be given. It is polynomial in the same regime of parameters when the distinguisher of [FGO$^+$11] works and scales nicely between this polynomial regime and an exponential regime depending on the code parameters. This can be considered as a breakthrough in this area.

- Rank defective elements in this matrix space also reveal something about the hidden polynomial structure of the Goppa or alternant code in a certain parameter regime, namely when (i) the degree r of the alternant code is less than $q+1$ or $q-1$ in the Goppa case, (ii) the code is distinguishable with the method of [FGO$^+$11]. We use this to give a polynomial-time attack in such a case by just looking for rank defective elements with a random search. This complements nicely the polynomial attack which has been found in [BMT23] which also needs that the code is distinguishable with [FGO$^+$11], but works in the reverse parameter regime $r \geqslant q+1$ (and has also additional restrictions, code alphabet size either binary or ternary and it does not work for Goppa codes). Note that in conjunction with the filtration of [BMT23], this new attack works for *any* distinguishable generic alternant code. This gives yet another example of a case when the distinguisher of [FGO$^+$11] turns into an actual attack of the scheme.

2 Notation and preliminaries

2.1 Notation

General notation $[\![a, b]\!]$ indicates the closed integer interval between a and b. We will make use of two notations for finite fields, $\mathbb{F}_q$ denotes the finite field with q elements, but sometimes we do not indicate the size of it when it is not important to do so and simply write $\mathbb{F}$. Instead, a generic field (not necessarily finite) is denoted by $\mathbb{K}$ and its algebraic closure by $\overline{\mathbb{K}}$.

Vector and matrix notation. Vectors are indicated by lowercase bold letters $\boldsymbol{x}$ and matrices by uppercase bold letters $\boldsymbol{M}$. Given a function f acting on $\mathbb{F}$ and a vector $\boldsymbol{x} = (x_i)_{1 \leqslant i \leqslant n} \in \mathbb{F}$, the expression $f(\boldsymbol{x})$ is the component-wise mapping of f on $\boldsymbol{x}$, i.e. $f(\boldsymbol{x}) = (f(x_i))_{1 \leqslant i \leqslant n}$. We will even apply this with functions f

acting on $\mathbb{F} \times \mathbb{F}$: for instance for two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}^n$ and two positive integers a and b we denote by $\boldsymbol{x}^a\boldsymbol{y}^b$ the vector $(x_i^a y_i^b)_{1 \leqslant i \leqslant n}$. We will use the same operation over matrices, but in order to avoid confusion with the matrix product, we use for a matrix $\boldsymbol{A} = (a_{i,j})_{i,j}$ the notation $\boldsymbol{A}^{(q)}$ which stands for the entries of $\boldsymbol{A}$ all raised to the power q, i.e. the entry (i,j) of $\boldsymbol{A}^{(q)}$ is equal to $a_{i,j}^q$. The scalar product between $\boldsymbol{x} = (x_i)_{1 \leqslant i \leqslant n} \in \mathbb{F}^n$ and $\boldsymbol{y} = (y_i)_{1 \leqslant i \leqslant n} \in \mathbb{F}^n$ is denoted by $\boldsymbol{x} \cdot \boldsymbol{y}$ and is defined by $\boldsymbol{x} \cdot \boldsymbol{y} = \sum_{i=1}^n x_i y_i$.

Symmetric and skew-symmetric matrices. The set of $k \times k$ symmetric matrices over $\mathbb{F}$ is denoted by $\mathbf{Sym}(k, \mathbb{F})$, whereas the corresponding set of skew-symmetric matrices is denoted by $\mathbf{Skew}(k, \mathbb{F}_q)$. The number of symmetric matrices of size t and rank r is denoted by $N(t,r)$ whereas the number of skew-symmetric matrices of the same size and rank is denoted by $N_0(t,r)$ (the finite field over which the matrix is defined will be clear from the context).

Vector spaces. Vector spaces are indicated by $\mathscr{C}$. For two vector spaces $\mathscr{C}$ and $\mathscr{D}$, the notation $\mathscr{C} \oplus \mathscr{D}$ means that the two vector spaces are in direct sum, i.e. that $\mathscr{C} \cap \mathscr{D} = \{0\}$. The $\mathbb{F}$-linear space generated by $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m \in \mathbb{F}^n$ is denoted by $\langle\, \boldsymbol{x}_1, \dots, \boldsymbol{x}_m \,\rangle_{\mathbb{F}}$.

Codes. A linear code $\mathscr{C}$ of length n and dimension k over $\mathbb{F}_q$ is a k dimensional subspace of $\mathbb{F}_q^n$. We refer to it as an $[n,k]$-code.

Ideals. Ideals are indicated by calligraphic $\mathcal{I}$. Given a sequence S of polynomials, $\mathcal{I}(S)$ refers to the polynomial ideal generated by such sequence. Given the polynomials $f_1, \dots, f_m$, we denote by $\langle f_1, \dots, f_m \rangle$ the ideal generated by them. The variety associated with a polynomial ideal $\mathcal{I} \subseteq \mathbb{K}[x_1, \dots, x_n]$ is indicated by $\boldsymbol{V}(\mathcal{I})$ and defined as $\boldsymbol{V}(\mathcal{I}) = \{\boldsymbol{a} \in \overline{\mathbb{K}}^n \mid \forall f \in \mathcal{I},\ f(\boldsymbol{a}) = 0\}$.

2.2 Distinguishable Alternant or Goppa Code

We will frequently use here the term *distinguishable alternant/Goppa* (in the sense of [FGO+11]) code. They are defined as

Definition 9 (distinguishable alternant/Goppa code). *A (generic) alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ of length n over $\mathbb{F}_q$ and extension degree m is said to be distinguishable iff*

$$n > \binom{rm+1}{2} - \frac{m}{2}(r-1)\left((2e_{\mathscr{A}}+1)r - 2\frac{q^{e_{\mathscr{A}}+1}-1}{q-1}\right) \tag{4}$$

where $e_{\mathscr{A}} \overset{def}{=} \max\{i \in \mathbb{N} \mid r \geqslant q^i + 1\} = \left\lfloor \log_q(r-1) \right\rfloor$.
A Goppa code $\mathscr{G}(\boldsymbol{x}, \Gamma)$ *of the same parameters is said to be distinguishable iff*

$$n > \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2), \qquad \textit{if } r < q-1 \tag{5}$$

$$n > \binom{rm+1}{2} - \frac{m}{2} r\left((2e_{\mathscr{G}}+1)r - 2(q-1)q^{e_{\mathscr{G}}-1} - 1\right), \qquad \textit{else,} \tag{6}$$

where $e_{\mathscr{G}} \overset{def}{=} \min\{i \in \mathbb{N} \mid r \leqslant (q-1)^2 q^i\} + 1 = \left\lceil \log_q\left(\frac{r}{(q-1)^2}\right)\right\rceil + 1$.

This definition is basically due to the fact that there is a way to distinguish such codes from random codes in this case [FGO$^+$11]. For our purpose, it is better to use the point of view of [MT22] and to notice that they are distinguishable because the computation of the dimension of the square of the dual code leads to a result which is different from n and $\binom{rm+1}{2}$ (which is the expected dimension of the square of a dual code of dimension rm). This is shown by

Theorem 1 *[MT22] For an alternant code* $\mathbb{F}_q$ *of length* n *and extension degree* m *we have*

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp})^{\star 2} \leqslant \min\left\{n, \binom{rm+1}{2} - \frac{m}{2}(r-1)\left((2e_{\mathscr{A}}+1)r - 2\frac{q^{e_{\mathscr{A}}+1}-1}{q-1}\right)\right\}. \tag{7}$$

where $e_{\mathscr{A}} \overset{def}{=} \max\{i \in \mathbb{N} \mid r \geqslant q^i + 1\} = \left\lfloor \log_q(r-1) \right\rfloor$.
For a Goppa code $\mathscr{G}(\boldsymbol{x}, \Gamma)$ *of length* n *over* $\mathbb{F}_q$ *with Goppa polynomial* $\Gamma(X) \in \mathbb{F}_{q^m}[X]$ *of degree* r *we have*

$$\dim(\mathscr{G}(\boldsymbol{x}, \Gamma)^{\perp})^{\star 2} \leqslant \min\left\{n, \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2)\right\}, \quad \textit{if } r < q-1 \tag{8}$$

$$\dim(\mathscr{G}(\boldsymbol{x}, \Gamma)^{\perp})^{\star 2} \leqslant \min\left\{n, \binom{rm+1}{2} - \frac{m}{2} r\left((2e_{\mathscr{G}}+1)r - 2(q-1)q^{e_{\mathscr{G}}-1} - 1\right)\right\}, \quad \textit{else,} \tag{9}$$

where $e_{\mathscr{G}} \overset{def}{=} \min\{i \in \mathbb{N} \mid r \leqslant (q-1)^2 q^i\} + 1 = \left\lceil \log_q\left(\frac{r}{(q-1)^2}\right)\right\rceil + 1$.

3 Invariants of the Matrix Code of Quadratic Relations

3.1 Changing the basis

The fundamental objects that we have introduced, namely the code of relationships $\mathscr{C}_{\text{rel}}(\mathcal{V})$ and the corresponding matrix code $\mathscr{C}_{\text{mat}}(\mathcal{V})$ both depend on the basis $\mathcal{V}$ which is chosen. However, all these matrix codes are isometric for the rank metric, namely the metric d between matrices given by

$$d(\boldsymbol{X}, \boldsymbol{Y}) \overset{\text{def}}{=} \mathbf{Rank}(\boldsymbol{X} - \boldsymbol{Y}).$$

This holds because of the following result

Proposition 4. *Let $\mathcal{A}$ and $\mathcal{B}$ be two bases of a same $[n,k]$ $\mathbb{F}$-linear code $\mathscr{C}$, with $\mathbb{F}$. Then $\mathscr{C}_{mat}(\mathcal{A})$ and $\mathscr{C}_{mat}(\mathcal{B})$ are isometric matrix codes, i.e. there exists $\boldsymbol{P} \in \mathbf{GL}_k(\mathbb{F})$ such that*

$$\mathscr{C}_{mat}(\mathcal{A}) = \boldsymbol{P}^{\mathsf{T}} \mathscr{C}_{mat}(\mathcal{B}) \boldsymbol{P}. \tag{10}$$

The matrix $\boldsymbol{P}$ coincides with the change of basis matrix between $\mathcal{A}$ and $\mathcal{B}$.

This Proposition is proved in Appendix §3. This result implies that there are several fundamental quantities which stay invariant when considering different bases, such as for instance

- the distribution of ranks $\{n_i, 0 \leqslant i \leqslant k\}$ where n_i is the number of matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{V})$ of rank i;
- the dimension of $\mathscr{C}_{\mathrm{mat}}(\mathcal{V})$.

We will sometime avoid specifying the basis, and simply write $\mathscr{C}_{\mathrm{mat}}$, when referring to invariants for the code.

3.2 Dimension

We can be a little bit more specific concerning the dimension. In general, two different bases of a same code provide different codes of relationships. The corresponding dimension, instead, is an invariant:

Proposition 5. *Let $\mathscr{C} \subseteq \mathbb{F}^n$ be an $[n,k]$ linear code with ordered basis $\mathcal{V}$. Then*

$$\begin{aligned}
\dim_{\mathbb{F}} \mathscr{C}_{rel}(\mathcal{V}) &= \binom{k+1}{2} - \dim_{\mathbb{F}} \mathscr{C}^{\star 2} \\
\dim_{\mathbb{F}} \mathscr{C}_{mat}(\mathcal{V}) &= \dim_{\mathbb{F}} \mathscr{C}_{rel}(\mathcal{V}) \quad \textit{(in odd characteristic)} \\
\dim_{\mathbb{F}} \mathscr{C}_{mat}(\mathcal{V}) &\leqslant \dim_{\mathbb{F}} \mathscr{C}_{rel}(\mathcal{V}) \quad \textit{(characteristic } 2\textit{)} \\
&= \dim_{\mathbb{F}_{q^m}} \mathbf{Pct}_D\left(\mathscr{C}_{rel}(\mathcal{V})\right),
\end{aligned}$$

where $D = \{(i,i) \mid i \in [\![1,k]\!]\}$ and $\mathbf{Pct}_D\left(\mathscr{C}_{rel}(\mathcal{V})\right)$ denotes the code punctured over the set D.

Proof. The first point directly follows by applying the rank-nullity theorem with respect to the map $T\colon \mathbb{F}^{\binom{k+1}{2}} \to \mathbb{F}^n$, $T(\boldsymbol{c}) = \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j$:

$$\binom{k+1}{2} = \dim_{\mathbb{F}} \mathbb{F}^{\binom{k+1}{2}} = \dim_{\mathbb{F}} \operatorname{Im}(T) + \dim_{\mathbb{F}} \ker(T) = \dim_{\mathbb{F}} \mathscr{C}^{\star 2} + \dim_{\mathbb{F}} \mathscr{C}_{\mathrm{rel}}(\mathcal{V}).$$

For the second point, it is enough to observe that any entry of $\boldsymbol{c} \in \mathscr{C}_{\mathrm{rel}}(\mathcal{V})$ corresponds to an entry in the lower triangular part of $\boldsymbol{M_c} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{V})$ and that 2 is coprime with the field characteristic. The third point follows a similar reasoning, but this time coordinates of $\boldsymbol{c}$ indexed by elements in D always correspond to zero entries in $\boldsymbol{M_c}$. □

In characteristic 2, since for a code $\mathscr{C}$ of dimension larger than 1, the set D defined in the proposition above is such that

$$|D| = k = \dim_{\mathbb{F}} \mathscr{C} < \dim_{\mathbb{F}} \mathscr{C}^{\star 2} = \binom{k+1}{2} - \dim_{\mathbb{F}} \mathscr{C}_{\mathrm{rel}}(\mathcal{V}),$$

we expect $\dim_{\mathbb{F}} \mathscr{C}_{\mathrm{rel}}(\mathcal{V}) = \dim_{\mathbb{F}} \mathbf{Pct}_D\left(\mathscr{C}_{\mathrm{rel}}(\mathcal{V})\right)$. Therefore the next assumption is reasonable and experimentally supported:

Assumption 1 *Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}$ (of even characteristic) and let $\mathcal{V}$ be a basis of $\mathscr{C}$. Then*

$$\dim_{\mathbb{F}_{q^m}} \mathscr{C}_{mat}(\mathcal{V}) = \dim_{\mathbb{F}_{q^m}} \mathscr{C}_{rel}(\mathcal{V}) = \binom{k+1}{2} - \dim_{\mathbb{F}} \mathscr{C}^{\star 2}.$$

4 Low-rank matrices in $\mathscr{C}_{\mathbf{mat}}$

4.1 Low-rank matrices from quadratic relations in [FGO+13]

By Proposition 4, all the matrix codes $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ are isometric for any choice of basis $\mathcal{B}$. We will be interested here in showing that the matrix code of quadratic relations associated to the extension over $\mathbb{F}_{q^m}$ of the dual of an alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ defined over $\mathbb{F}_q$ contains many low rank matrices. This is due to the fact that this code contains the GRS codes $\mathbf{GRS}_r(\boldsymbol{x}^{q^i}, \boldsymbol{y}^{q^i})$ for all $i \in [\![0, m-1]\!]$ (Proposition 3). This will be clear if we choose the basis appropriately. We can namely choose the ordered basis

$$\mathcal{A} = (\boldsymbol{y}, \boldsymbol{x}\boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1}\boldsymbol{y}, \ldots, \boldsymbol{y}^{q^{m-1}}, (\boldsymbol{x}\boldsymbol{y})^{q^{m-1}}, \ldots, (\boldsymbol{x}^{r-1}\boldsymbol{y})^{q^{m-1}}). \tag{11}$$

We call this the *canonical basis*. It will be convenient to denote the r first basis elements by $\boldsymbol{a}_0 \overset{\text{def}}{=} \boldsymbol{y}$, $\boldsymbol{a}_1 \overset{\text{def}}{=} \boldsymbol{x}\boldsymbol{y}, \ldots, \boldsymbol{a}_{r-1} \overset{\text{def}}{=} \boldsymbol{x}^{r-1}\boldsymbol{y}$ and view the basis as

$$\mathcal{A} = (\boldsymbol{a}_0, \cdots, \boldsymbol{a}_{r-1}, \boldsymbol{a}_0^q, \cdots, \boldsymbol{a}_{r-1}^q, \cdots, \boldsymbol{a}_0^{q^{m-1}}, \cdots, \boldsymbol{a}_{r-1}^{q^{m-1}}).$$

There are simple quadratic relations between the $\boldsymbol{a}_i^{q^j}$ owing to the trivial algebraic relations introduced in [FGO+13]: $(\boldsymbol{x}^a\boldsymbol{y})^{q^l} \star (\boldsymbol{x}^b\boldsymbol{y})^{q^u} = (\boldsymbol{x}^c\boldsymbol{y})^{q^l} \star (\boldsymbol{x}^d\boldsymbol{y})^{q^u}$ if $aq^l + bq^u = cq^l + dq^u$. This amounts to the quadratic relation between the basis elements

$$\boldsymbol{a}_a^{q^l} \star \boldsymbol{a}_b^{q^u} - \boldsymbol{a}_c^{q^l} \star \boldsymbol{a}_d^{q^u} = 0. \tag{12}$$

It is readily seen that matrix of $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ corresponding to this quadratic relationship is of rank 4 with the exception of the case $c = d$ and $l = u$ where it is of rank 3 (odd characteristic) or rank 2 (characteristic 2). Indeed, if we reorder the basis $\mathcal{B}$ such that it starts with $\boldsymbol{a}_a^{q^l}, \boldsymbol{a}_b^{q^l}, \boldsymbol{a}_c^{q^l}$, then it is readily seen that the matrix $\boldsymbol{M} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ corresponding to (12) has only zeros with the exception of the first 3×3 block $\boldsymbol{M}'$ which is given by

$$\boldsymbol{M}' = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -2 \end{bmatrix} \text{ (odd characteristic)}, \quad \boldsymbol{M}' = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ (characteristic 2)}.$$

This leads to the following fact

Fact 1 *Consider the alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ of extension degree m and let $\mathscr{C}_{mat}(\mathcal{A})$ be the corresponding matrix code associated to the basis choice* (11)*. Let $l \in [\![0, m-1]\!]$ and a, b, c in $[\![0, r-1]\!]$ be such that $a+b = 2c$. Then the matrix of $\mathscr{C}_{mat}(\mathcal{A})$ corresponding to the quadratic relation $\boldsymbol{a}_a^{q^l} \star \boldsymbol{a}_b^{q^l} - \left(\boldsymbol{a}_c^{q^l}\right)^{\star 2} = 0$ is of rank* 3 *in odd characteristic and of rank* 2 *in characteristic* 2*.*

This already shows that there are many rank 2 or 3 matrices in $\mathscr{C}_{\mathrm{mat}}$ corresponding to an alternant code. But it will turn out that there are even more matrices and that there are subsets of these matrices which form a vector space of matrices. Moreover, depending on the fact that the alternant code has a Goppa structure we will have even more low rank matrices as we show below. We namely have in characteristic 2

Proposition 6. *Let $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ be an alternant code of extension degree m and order r over a field of characteristic* 2*. Then $\mathscr{C}_{mat}$ contains $\left\lfloor \frac{r-1}{2} \right\rfloor$-dimensional subspaces of rank-($\leqslant 2$) matrices. If $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ is a binary Goppa code with a square-free Goppa polynomial, then $\mathscr{C}_{mat}$ contains $(r-1)$-dimensional subspaces of rank-($\leqslant 2$) matrices.*

This proposition is proved in Appendix §C.1. We can also give a lower bound on the number of such matrices as shown by

Proposition 7. *Let $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ be an alternant code in characteristic* 2 *and extension degree m. The matrix code of quadratic relationships $\mathscr{C}_{mat}$ contains at least $\Omega(m(q^{m(r-2)})$ matrices of rank 2.*

In the particular case of binary Goppa codes associated to a square-free polynomial (i.e. the standard choice in a McEliece cryptosystem) we have

Proposition 8. *Let $\mathscr{G}(\boldsymbol{x}, \Gamma)$ be a binary Goppa code of extension degree m with Γ a square-free polynomial of degree r. Then $\mathscr{C}_{mat}$ contains at least*

$$m \frac{(q^{mr}-1)(q^{m(r-1)}-1)}{q^{2m}-1}$$

matrices of rank 2.

These propositions are proved in Appendix §C.1. It also turns out that for the "canonical" choice mentioned above (namely when choosing the basis $\mathcal{A}$ given in (11)) under certain circumstances, $\mathscr{C}_{\mathrm{mat}}$ contains the subspace of block diagonal skew symmetric matrices with blocks of size r

Proposition 9. *Let $\mathscr{G}(\boldsymbol{x}, \Gamma)$ be a binary $[n, n-rm]$ Goppa code with Γ a square-free polynomial of degree r and let $\mathcal{A}$ be the canonical basis of $\mathscr{G}(\boldsymbol{x}, \Gamma)^{\perp}_{\mathbb{F}_{q^m}}$ given in* (11) *with $\boldsymbol{y} = \frac{1}{\Gamma(\boldsymbol{x})}$. Then $\mathscr{C}_{mat}(\mathcal{A})$ contains the space of block-diagonal skew-symmetric matrices with $r \times r$ blocks.*

4.2 The random case

We have described in the previous subsection a family of matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ with a small rank. In particular, we found rank 3 matrices for odd characteristic and rank 2 matrices for even characteristic. In the case of binary Goppa codes with square-free Goppa polynomial, the subspace generated by such rank 2 matrices is even bigger. Since the two codes $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ and $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ have the same weight distribution, the same number of low-rank matrices must exist for $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ as well. We may wonder if such low-rank matrices exist in the matrix code of relationships $\mathscr{C}_{\mathrm{mat}}(\mathcal{R})$ of an $[n, rm]$ random $\mathbb{F}_{q^m}$-linear code $\mathscr{R}$ with basis $\mathcal{R}$. This can be determined by computing the Gilbert-Varshamov distance d_{GV} for spaces of symmetric (resp. skew-symmetric) matrices, which is the smallest d such that

$$|\mathscr{C}_{\mathrm{mat}}(\mathcal{R})||B_d^{(\mathbf{Sym})}| \geqslant |\mathbf{Sym}(rm, \mathbb{F}_{q^m})|, \tag{13}$$

$$|\mathscr{C}_{\mathrm{mat}}(\mathcal{R})||B_d^{(\mathbf{Skew})}| \geqslant |\mathbf{Skew}(rm, \mathbb{F}_{q^m})|, \tag{14}$$

where $B_d^{(\mathbf{Sym})}$ (resp. $B_d^{(\mathbf{Skew})}$) is the ball of symmetric (resp. skew-symmetric) matrices of radius d (with respect to the rank metric). The rationale of this definition is that it can be proved that for a random linear code $\mathscr{C}$ the probability of having a non zero matrix of rank $\leqslant d$ in $\mathscr{C}$ is upper-bounded by the ratio $\frac{|\mathscr{C}||B_d^{(\mathbf{Sym})}|}{|\mathbf{Sym}(rm,\mathbb{F}_{q^m})|}$ in the symmetric case. A similar bound holds in the skew-symmetric case. In a low-rank scenario, more precisely when $\binom{rm+1}{2} \leqslant n$, the code $\mathscr{C}_{\mathrm{mat}}(\mathcal{R})$ is expected to be trivial. This corresponds indeed to the distinguishable regime. We will then assume $\binom{rm+1}{2} > n$.

Proposition 10. *Let $\mathscr{R} \subset \mathbb{F}_{q^m}^n$ be a random code of dimension rm with basis $\mathcal{R}$ and let $\binom{rm+1}{2} > n$. Under the assumption that $\mathscr{C}_{mat}(\mathcal{R})$ behaves as a random linear code concerning the rank weight distribution, it contains matrices or rank $\leqslant d$ with non-negligible probability iff*

$$n \leqslant drm - \binom{d}{2} \qquad \textit{(symmetric case)}$$

$$n \leqslant (2\lfloor d/2\rfloor + 1)rm - \binom{2\lfloor d/2\rfloor + 1}{2} \qquad \textit{(skew-symmetric case)}$$

This proposition is proved in §C.2. In particular, we expect rank-3 symmetric matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{R})$ for

$$n \leqslant 3rm - 3 \tag{15}$$

and rank-2 skew-symmetric matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{R})$ in characteristic 2 for

$$n \leqslant (2\lfloor 2/2\rfloor + 1)rm - \binom{2\lfloor 2/2\rfloor + 1}{2} = 3rm - 3$$

as well. We observe that for all security levels of Classic McEliece [ABC+22], the code rate is such that $n = \alpha rm$ with $\alpha \in (3.5, 5)$. This means that any algorithm that finds low-rank matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{R})$ represents a distinguisher between Goppa codes (and more in general alternant codes) and random linear codes for Classic McEliece rates.

5 A New Distinguisher of Alternant and Goppa Codes in Characteristic 2

We are going to focus here on the particular case of characteristic 2 where we want to find rank 2 matrices in the matrix code of quadratic relations. We are going to consider a particular algebraic modeling for finding matrices of this kind for which we can estimate the running time of Gröbner bases algorithms for solving it. We will show that the behavior of the Gröbner basis computation is quite different when applied to the matrix code corresponding to an alternant (or a Goppa) code rather than to the matrix code corresponding to a random code of the same dimension and length as the alternant/Goppa code. This provides clearly a distinguisher of an alternant or Goppa code whose complexity can be estimated. It turns out that this algorithm is of polynomial complexity for the code parameters where the original distinguisher of [FGO$^+$11] works (it actually computes equivalent quantities), but contrarily to the distinguisher given in [FGO$^+$11] it works for distinguishing most codes of cryptographic interest at the cost of being of exponential complexity when the code rate is constant (but it scales from polynomial to subexponential and then to exponential in between).

5.1 A modeling coming from the Pfaffian ideal.

We are first going to give an algebraic modelling expressing that a skew-symmetric matrix $\boldsymbol{M}$ with arbitrary entries is of rank $\leqslant 2$ coming by expressing the fact that all minors of size 4 should be zero which implies that $\boldsymbol{M}$ should be of rank $\leqslant 2$, because any skew-symmetric matrix is of even rank and can therefore not be of rank 3. In other words, let us consider the generic skew-symmetric matrix $\boldsymbol{M} = (m_{i,j})_{i,j} \in \mathbf{Skew}(s, \mathbb{F}_{q^m})$, whose entries $m_{i,j}$ with $1 \leqslant i < j \leqslant s$ are independent variables. Let $\boldsymbol{m} = (m_{i,j})_{1 \leqslant i < j \leqslant s}$. We will write sometimes $m_{j,i}$ with $i < j$, this must just be seen as an alias for $m_{i,j}$ and not as another variable. We denote by $\mathbf{Minors}(\boldsymbol{M}, d)$ the set of all minors of $\boldsymbol{M}$ of size d. The set of specializations of $\boldsymbol{M}$ that provide rank 2 matrices is the variety of the determinantal ideal generated by $\mathbf{Minors}(\boldsymbol{M}, 3)$. Since there do not exist rank 3 matrices in $\mathbf{Sym}(s, \mathbb{F}_{q^m})$, the ideal generated by each possible 4×4 minor of $\boldsymbol{M}$ leads to the same variety:

$$\boldsymbol{V}(\mathcal{I}(\mathbf{Minors}(\boldsymbol{M}, 3))) = \boldsymbol{V}(\mathcal{I}(\mathbf{Minors}(\boldsymbol{M}, 4))).$$

The homogeneous ideal $\mathcal{I}(\mathbf{Minors}(\boldsymbol{M}, 2l))$ is not radical. The determinant of a generic skew-symmetric matrix of size $2l \times 2l$ is the square of a polynomial of degree l, called *Pfaffian*. It is well-known that the radical ideal is generated by the square roots of a subset of minors, namely those corresponding to a submatrix with the same subset for row and column indexes. Note that such matrices are skew-symmetric as well, and thus their determinant is the square of a Pfaffian polynomial. In particular, we define

Definition 10 (Pfaffian ideal for rank 2). *The Pfaffian ideal of rank 2 for $\boldsymbol{M}$ in characteristic 2 is*

$$\mathcal{P}_2(\boldsymbol{M}) \overset{def}{=} \langle m_{i,j}m_{k,l} + m_{i,k}m_{j,l} + m_{i,l}m_{j,k} \mid 1 \leqslant i < j < k < l \leqslant s \rangle, \qquad (16)$$

Remark 1. Note that in the definition of the Pfaffian ideal (16), the 4-tuple (i, j, k, l) is given by distinct values. Indeed, as already shown, if two indexes are equal then

$$m_{i,j}m_{k,l} + m_{i,k}m_{j,l} + m_{i,l}m_{j,k} = 0$$

identically, thus these equations do not have to be considered.

We have

Proposition 11. *[HT92, Theorem 5.1] The basis* $\{m_{i,j}m_{k,l}+m_{i,k}m_{j,l}+m_{i,l}m_{j,k} \mid 1 \leqslant i < j < k < l \leqslant s\}$ *is a Gröbner basis of* $\mathcal{P}_2(\boldsymbol{M})$ *with respect to a suitable order.*

Another straightforward result is that

Proposition 12. *We have* $\boldsymbol{V}(\mathcal{P}_2(\boldsymbol{M})) = \boldsymbol{V}(\mathcal{I}(\mathbf{Minors}(\boldsymbol{M}, 4)))$.

Proof. One can verify that for any $f \in \mathbf{Minors}(\boldsymbol{M}, 4)$, $f \in \mathcal{P}_2(\boldsymbol{M})$ and for any f in the basis of $\mathcal{P}_2(\boldsymbol{M})$, $f \in \sqrt{\mathcal{I}(\mathbf{Minors}(\boldsymbol{M}, 4))}$. By Hilbert's Nullstellensatz, the thesis follows.

Our modeling takes advantage of the deep knowledge we have about this ideal. We express now the fact that a matrix $\boldsymbol{M}$ of size s belongs to some matrix code $\mathscr{C}_{\text{mat}}$ associated to an $[n, k]$ code (which implies that $s = n - k$) by $t \overset{\text{def}}{=} \binom{s}{2} - \dim \mathscr{C}_{\text{mat}}$ linear equations $L_1 = 0, \cdots, L_t = 0$ linking the $m_{i,j}$'s. The algebraic modeling we use to express that an element $\boldsymbol{M}$ of $\mathscr{C}_{\text{mat}}$ is of rank $\leqslant 2$ uses these t equations and the Gröbner basis of the Pfaffian ideal. In other words we have the following algebraic modeling

Modeling 1 ($\boldsymbol{M} \in \mathscr{C}_{\textbf{mat}}$, Rank($\boldsymbol{M}$) $\leqslant 2$)

- $\binom{s}{4}$ *quadratic equations* $m_{i,j}m_{k,l} + m_{i,k}m_{j,l} + m_{i,l}m_{j,k} = 0$ *where* $1 \leqslant i < j < k < l \leqslant s$
- $t \overset{def}{=} \binom{s}{2} - \dim \mathscr{C}_{mat}$ *linear equations* $L_1 = 0, \cdots, L_t = 0$ *linking the* m_{ij}*'s expressing the fact that* $\boldsymbol{M}$ *belongs to* $\mathscr{C}_{mat}$.

5.2 Gröbner bases and Hilbert series

We will be interested in computing the Hilbert series of the ideal corresponding to Modeling 1 because it will turn out to behave differently depending on the code we use for defining the associated matrix code $\mathscr{C}_{\text{mat}}$. This will lead to a distinguisher of alternant or Goppa codes. Given a homogeneous ideal $\mathcal{I} \in \mathbb{K}[\boldsymbol{z}]$, $\boldsymbol{z} = (z_1, \ldots, z_n)$, the Hilbert function of the ring $R = \mathbb{K}[\boldsymbol{z}]/\mathcal{I}$ is defined as

$$HF_R(d) \overset{\text{def}}{=} \dim_{\mathbb{K}}(R) = \dim_{\mathbb{K}}(\mathbb{K}[\boldsymbol{z}]_d) - \dim_{\mathbb{K}}(\mathcal{I}_d),$$

where $\mathbb{K}[\boldsymbol{z}]_d = \{f \in \mathbb{K}[\boldsymbol{z}] \mid \deg(f) = d\}$ and $\mathcal{I}_d = \mathcal{I} \cap \mathbb{K}[\boldsymbol{z}]_d$. Then the Hilbert series of R is the formal series

$$HS_R(t) \overset{\text{def}}{=} \sum_{d \geqslant 0} HF_R(d)t^d.$$

Computing individual terms $HF_R(d)$ as we will be interested here can be done by computing the rank of the Macaulay matrix at degree d by taking m generators of the ideal $\mathcal{I}$ (see Appendix §A) and its cost is upper-bounded by

Proposition 13. *Let $F = \{f_1, \dots, f_m\} \subset \mathbb{K}[z_1, \dots, z_n]$ be a homogeneous system. Let $\mathcal{I}$ be the corrresponding ideal. The term $HF_R(d)$ of degree d of the Hilbert function of $R = \mathbb{K}[\boldsymbol{z}]/\mathcal{I}$ can be computed in time bounded by*

$$\mathcal{O}\left(md\binom{n+d-1}{d}^{\omega}\right),$$

where ω is the linear algebra exponent.

Fortunately, the Hilbert function for our Pfaffian ideal is known. We define the quotient ring

$$R(\boldsymbol{M}) = \mathbb{F}_{q^m}[\boldsymbol{m}]/\mathcal{P}_2(\boldsymbol{M}).$$

The Hilbert function (or equivalently the Hilbert series) of $R(\boldsymbol{M})$ is well-known:

Proposition 14. *[GK04, (from) Theorem 1] Let $\boldsymbol{M} = (m_{i,j})_{i,j}$ be the generic $s \times s$ skew-symmetric matrix over $\mathbb{F}$. Then* $\dim \boldsymbol{V}(\mathcal{P}_2(\boldsymbol{M})) = 2s - 3$ *and*

$$HF_{R(\boldsymbol{M})}(d) = \binom{s+d-2}{d}^2 - \binom{s+d-2}{d+1}\binom{s+d-2}{d-1},$$

$$HS_{R(\boldsymbol{M})}(z) = \frac{\sum_{d=0}^{s-3}\left(\binom{s-2}{d}^2 - \binom{s-3}{d-1}\binom{s-1}{d+1}\right)z^d}{(1-z)^{2s-3}}.$$

Modeling 1 adds linear equations to it expressing the fact that the matrix should also be in the matrix code of quadratic relationships. There is one handy tool that allows to compute the Hilbert series obtained by enriching with polynomials an ideal whose Hilbert series is known.

Proposition 15. *[Bar04, Lemma 3.3.2] As long as there are not reductions to 0 in the F5 algorithm, the Hilbert function $HF_{\mathbb{K}[\boldsymbol{x}]/\langle f_1,\dots,f_m\rangle}(d)$ satisfies the following recursive formula:*

$$HF_{\mathbb{K}[\boldsymbol{x}]/\langle f_1,\dots,f_m\rangle}(d) = HF_{\mathbb{K}[\boldsymbol{x}]/\langle f_1,\dots,f_{m-1}\rangle}(d) - HF_{\mathbb{K}[\boldsymbol{x}]/\langle f_1,\dots,f_{m-1}\rangle}(d-d_m)$$

where $d_m = \deg(f_m)$.

Essentially, reductions to 0 in F5 correspond to "non generic" reductions to 0 and experimentally we have not observed this behavior for Modeling 1 when we add the linear equations expressing that $\boldsymbol{M}$ belongs to $\mathscr{C}_{\text{mat}}$ to the Pfaffian ideal when $\mathscr{C}_{\text{mat}}$ is the matrix code of relationships associated to a random linear code.

5.3 Analysis of the Hilbert series for the Pfaffian ideal

We will from now on consider that the matrix code $\mathscr{C}_{\text{mat}}$ of quadratic relations is associated to a code $\mathscr{C}$ over $\mathbb{F}_{q^m}$ of parameters $[n, mr]$ which are the same as those of the extended dual code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}_{\mathbb{F}_{q^m}}$ of an alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}$ of length n over $\mathbb{F}_q$ and extension degree m which we assume to be of generic dimension $k = n - mr$. We will from now on also assume that the $[n, mr]$ code $\mathscr{C}$ we consider satisfies

$$\dim \mathscr{C}^{\star 2} = n. \tag{17}$$

This corresponds to the generic case of a random code as soon as $\binom{rm+1}{2} \geqslant n$ and to duals of alternant codes/Goppa codes that are not distinguishable. We also assume that we are in the generic case where Assumption 1 holds, that we namely have

$$\dim_{\mathbb{F}_{q^m}} \mathscr{C}_{\text{mat}}(\mathcal{V}) = \binom{mr+1}{2} - \dim_{\mathbb{F}} \mathscr{C}^{\star 2} = \binom{mr}{2} + mr - n = \binom{mr}{2} - k$$

where k is given above and corresponds to the dimension of the alternant code we are interested in. Notice that k is also the cardinality of the set of independent linear equations expressing in Modeling 1 that the $rm \times rm$ $\boldsymbol{M}$ belongs to $\mathscr{C}_{\text{mat}}$ since $\binom{rm}{2} - \dim \mathscr{C}_{\text{mat}} = k$. We also let from now on $s = rm$. We are going to show now that the Hilbert function of the ring $\mathbb{F}_{q^m}[\boldsymbol{m}]/(\mathcal{P}(\boldsymbol{M}) + \langle L_i \rangle_i)$ differs starting from some degree $\bar{d}$ depending on how the linear relationships L_i's are defined (coming from $\mathscr{C}_{\text{mat}}$ associated to a random $\mathscr{C}$ or to the extended dual of an alternant or Goppa code). We will assume that the parameters of our matrix code are such that we do not expect a matrix or rank 2 when $\mathscr{C}$ is random, which according to Proposition 10 holds as soon as $n > 3rm - 3$, *i.e* essentially for $k/n > 2/3$.

Random case We assume that we are in scenario where there are no reductions to 0 in F5 and that we can apply Proposition 15

$$\begin{aligned} HF_{\mathbb{K}[\boldsymbol{z}]/(\mathcal{I}+\langle L_1,\dots,L_\ell\rangle)}(d) &= HF_{\mathbb{K}[\boldsymbol{z}]/(\mathcal{I}+\langle L_1,\dots,L_{\ell-1}\rangle)}(d) - HF_{\mathbb{K}[\boldsymbol{z}]/(\mathcal{I}+\langle L_1,\dots,L_{\ell-1}\rangle)}(d-1) \\ &= \dots \\ &= HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d) - \sum_{i=0}^{\ell-1} HF_{\mathbb{K}[\boldsymbol{z}]/(\mathcal{I}+\langle L_1,\dots,L_i\rangle)}(d-1), \end{aligned}$$

which, by induction, leads to

$$HF_{\mathbb{K}[\boldsymbol{z}]/(\mathcal{I}+\langle L_1,\dots,L_\ell\rangle)}(d) = \sum_{i=0}^{d} (-1)^i \binom{\ell}{i} HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d-i).$$

This holds as long as there are no reductions to 0 in F5, when there are we expect that the Hilbert series at this degree is zero, which means that the induction formula should be

$$HF_{\mathbb{K}[\boldsymbol{z}]/(\mathcal{I}+\langle f\rangle)}(d) = \max(HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d) - HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d-\bar{d}), 0).$$

This leads to the following conjecture, experimentally supported.

Conjecture 1 (Random case) *Let $L_1, \dots, L_k$ be the k linear relationships relative to the matrix code $\mathscr{C}_{mat}$ associated to a random $[n,s]$-code as above. Let $\mathcal{P}_2^+(\boldsymbol{M}) \overset{def}{=} \mathcal{P}(\boldsymbol{M}) + \langle L_1, \dots, L_k \rangle$. If, for any $d' < d$, $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d') > 0$ then*

$$\begin{aligned} HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) &= \max(0, \sum_{i=0}^{d} (-1)^i \binom{k}{i} HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2(\boldsymbol{M})}(d-i)) \\ &= \max(0, \sum_{i=0}^{d} (-1)^i \binom{k}{i} \left(\binom{s+d-i-2}{d-i}^2 - \binom{s+d-i-2}{d-i-1}\binom{s+d-i-2}{d-i+1} \right)). \end{aligned}$$

Otherwise $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) = 0$.

Because we assume that Modeling 1 has only zero for solution in the random case there exist a d such that $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) = 0$. Experiments (see Appendix §D.1) lead to conjecture the following behavior:

Conjecture 2 *Let $\mathscr{C}_{mat}$ be the matrix code of relationships originated by a random $[n,s]$ code as above. Let $\mathcal{P}_2^+(\boldsymbol{M})$ the corresponding Pfaffian ideal and $d_0 = \min\{d : HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) = 0\}$. Then*

$$d_0 \sim c\frac{s^2}{k}$$

for a constant c equal or close to $\frac{1}{4}$.

Alternant/Goppa case. In the alternant/Goppa case however the Hilbert series never vanishes because the variety of solutions has always positive dimension. We can even lower its dimension by a rather large quantity.

Proposition 16. *Let $\mathscr{C}_{mat}$ be the matrix code of quadratic relationships corresponding to the extended dual of an $[n, n-rm]$ binary Goppa code over a field of even characteristic. Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the corresponding Pfaffian ideal. Then $\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M})) \geqslant 2r-3$.*

Proof. We recall from Proposition 14 that the dimension of the variety of the generic Pfaffian ideal $\mathcal{P}_2(\boldsymbol{M})$ is $2s-3$, where s is the matrix size. The result follows from the construction given in Section 4, for counting the number of rank 2 matrices, where we have shown that $\mathscr{C}_{\text{mat}}(\mathcal{A})$ contains a subspace of matrices that are isomorphic to the full space of skew-symmetric matrices of size r. This allows to lower bound $\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M}))$ in terms of $\dim \boldsymbol{V}(\mathcal{P}_2(\boldsymbol{N}))$, where $\boldsymbol{N}$ is the generic skew-symmetric matrix of size $r \times r$. More precisely,

$$\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M})) \geqslant \dim \boldsymbol{V}(\mathcal{P}_2(\boldsymbol{N})) = 2r-3.$$

□

More in general, we can upper bound the dimension of the variety using the following proposition, whose proof is given in Appendix §D.2.

Proposition 17. *Let $\mathscr{C}_{mat}$ be the matrix code of quadratic relationships corresponding to the extended dual of an $[n, n-rm]$ alternant code over a field of even characteristic. Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the corresponding Pfaffian ideal. Then* $\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M})) \geqslant r-2$.

Remark 2. Equalities in the two previous propositions were met in the experiments we performed. Note that, comparing with Proposition 6, the Pfaffian ideal contains subspaces of dimension roughly half the dimensio □n of the variety.

Now, as a consequence of the variety not being trivial, we have

Proposition 18. *Let $\mathscr{C}_{mat}$ be the matrix code of quadratic relationships corresponding to the extended dual of an $[n, n-rm]$ alternant code. Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the corresponding Pfaffian ideal. For all $d \in \mathbb{N}$, $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) > 0$.*

Proof. Assume by contradiction that $\exists d \in \mathbb{N}$ such that $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) = 0$. Therefore

$$\dim_{\mathbb{F}_{q^m}} (\mathcal{P}_2^+(\boldsymbol{M}))_d = \dim_{\mathbb{F}_{q^m}} \mathbb{F}_{q^m}[\boldsymbol{m}]_d,$$

i.e. all the monomials of degree d belong to $\mathcal{P}_2^+(\boldsymbol{M})$, in particular all the monomials $m_{i,j}^d$. This implies that the only element in the variety of $\mathcal{P}_2^+(\boldsymbol{M})$ is the zero matrix (with some multiplicity). This is in contradiction with the existence of rank 2 matrices in $\mathscr{C}_{\text{mat}}$ that must therefore be solutions of the Pfaffian system. □

Computing the Hilbert function up to some degree d provides a distinguisher as soon as it assumes a different value depending on whether it refers to random or alternant/Goppa codes. Thanks to Proposition 18, this will happen at the latest at the degree of regularity d_0 corresponding to a random code.

An extension of the distinguisher of [FGO$^+$11]. Note that in general

$$HF_{\mathbb{F}_{q^m}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(1) = \dim_{\mathbb{F}_{q^m}} \mathscr{C}_{\text{mat}}(\mathcal{B}).$$

Hence, a different evaluation of the Hilbert function in degree 1 witnesses an unusually large dimension of $\mathscr{C}_{\text{mat}}(\mathcal{B})$ and consequently an atypically small dimension of the square code. Indeed, this corresponds to the distinguisher from [FGO$^+$11]. The next example shows that we can improve upon the distinguisher of [FGO$^+$11] for some parameters already considering degree $d = 2$. Note that the evaluation of the Hilbert function in degree 2 can be obtained by just computing the rank of the initial Pfaffian system. This already is the first improvement on the distinguisher [FGO$^+$11] in approximately 10 years. Examples where we can distinguish both Goppa and generic alternant codes are given in Table 1 whereas examples where we distinguish only Goppa codes are given in Table 2.

$HF_{\mathbb{F}_{q^m}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(2)$	$256 \geqslant n \geqslant 77$	$n = 76$	$n = 75$	$n = 74$	$n = 73$	...
Random code	0	10	71	133	196	...
Alternant code	**20**	**20**	71	133	196	...
Goppa code	**80**	**80**	**80**	133	196	...

Table 1. Hilbert function at degree 2 with respect to random, alternant and Goppa codes with parameters $q = 4, m = 4, r = 4$. The evaluations in bold correspond to distinguishable lengths.

$HF_{\mathbb{F}_{q^m}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(2)$	$n = 64$	$n = 63$	$n = 62$	$n = 61$	$n = 60$	$n = 59$	$n = 58$	...
Random code	2718	2826	2935	3045	3156	3268	3381	...
Alternant code	2718	2826	2935	3045	3156	3268	3381	...
Goppa code	**2971**	**2971**	**2971**	**3048**	**3158**	**3269**	3381	...

Table 2. Hilbert function at degree 2 with respect to random, alternant and Goppa codes with parameters $q = 2, m = 6, r = 3$. The evaluations in bold correspond to distinguishable lengths.

This distinguisher can be further improved if one understands better the structure of the matrix code corresponding to alternant/Goppa codes. Indeed, it may happen that for some $d < d_0$, although for a random code $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) > 0$, still the Hilbert function assumes a different value (a larger one) than for an alternant/Goppa code. Tables 1 and 2 show this behavior for some specific lengths. In other words, for now we are just exploiting the fact that, in the case of an alternant/Goppa code, $HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) > 0$ for all $d \in \mathbb{N}$. The next theorem improves the lower bound above in the case of binary square-free Goppa code, *i.e.* those used in McEliece's schemes.

Theorem 2 *Let $\mathscr{G}(\boldsymbol{x}, \Gamma)$ be a non distinguishable binary $[n, k = n - rm]$ Goppa code with Γ a square-free polynomial of degree r and extension degree m. Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the corresponding Pfaffian ideal. Then, for all $d > 0$,*

$$HF_{\mathbb{F}_{2^m}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) \geqslant m\left(\binom{r+d-2}{d}^2 - \binom{r+d-2}{d+1}\binom{r+d-2}{d-1}\right).$$

The proof is given in Appendix §D. Theorem 2 has some theoretical interest, because it shows that the distinguisher can be further improved by analyzing the matrix code of relationships obtained from a Goppa code.

6 An attack on distinguishable random alternant codes, without the use of Gröbner bases

We are going to present now a polynomial time attack on distinguishable generic alternant code defined over $\mathbb{F}_q$ as soon as the degree r satisfies $r < q+1$ by using this new notion of the matrix code of quadratic relations. We also recall that a distinguishable alternant code must have degree $r \geqslant 3$. If we combine this together with the filtration technique of [BMT23] which allows to compute from a (distinguishable) alternant code of degree r satisfying $r \geqslant q+1$ an alternant code with the same support but of degree $r-1$ we obtain an attack on all distinguishable generic alternant codes. This is a big improvement on the attack presented in [BMT23] which needed two conditions to hold (1) a distinguishable alternant code (2) q is either 2 or 3. Moreover [BMT23] could not handle the subcase where the alternant code is actually a Goppa code, whereas our new attack is able to treat this case at least in the case $r < q-1$. We present in Table 3 a summary of the attacks. In other words, all distinguishable generic alternant codes can now be attacked. The reason why for the time being the distinguishable Goppa codes are out of reach, is that the filtration technique of [BMT23] for reducing the degree of the code does not work for the special case of Goppa codes.

Table 3. Summary of the attacks against *distinguishable* codes . The column q corresponds to the restrictions on q for the attack to work and the column r has the same meaning for the parameter r.

code	technique/paper	$r(\geqslant 3)$	q
(generic) distinguishable alternant code	[BMT23]	any	$\in \{2,3\}$
(generic) distinguishable alternant code	this paper	$< q+1$	any
(generic) distinguishable alternant code	this paper + filtration techn. of [BMT23]	any	any
distinguishable Goppa codes	this paper	$< q-1$	any

Thus, from now on, we will consider an alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_q^n$ of extension degree m which is such that $r < q+1$. For generic alternant codes, this corresponds to the distinguisher case with $e = 0$. If instead the alternant code is also Goppa, then we restrict ourselves to the case of $r < q-1$. We will show now how to recover $\boldsymbol{x}$ and $\boldsymbol{y}$ from the knowledge of a generator matrix of this code by making use of the matrix code of quadratic relations associated to the extended dual code over $\mathbb{F}_{q^m}$.

The idea

We first present the underlying idea by picking the canonical basis $\mathcal{A}$ (11) and the parity-check matrix $\boldsymbol{H}_{\mathcal{A}}$ of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})_{\mathbb{F}_{q^m}}$ whose rows correspond to the elements of $\mathcal{A}$ in that same order. Recall that this basis can be written as

$$\mathcal{A} = (\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{a}_1^q, \cdots, \boldsymbol{a}_r^q, \cdots, \boldsymbol{a}_1^{q^{m-1}}, \cdots, \boldsymbol{a}_r^{q^{m-1}}).$$

We also assume q is odd for now. The crucial point is that, with the assumption of a distinguishable generic alternant code (resp. Goppa code) with $r < q+1$ (resp. $r < q-1$), the analysis provided in [FGO$^+$11] implies that the matrix code is generated by *all and only* relations of the kind

$$\boldsymbol{y}^{q^l}\boldsymbol{x}^{aq^l} \star \boldsymbol{y}^{q^l}\boldsymbol{x}^{bq^l} = \boldsymbol{y}^{q^l}\boldsymbol{x}^{cq^l} \star \boldsymbol{y}^{q^l}\boldsymbol{x}^{dq^l}$$

where l is arbitrary in $[\![0, m-1]\!]$ and a, b, c, d in $[\![0, r-1]\!]$ such that $a+b = c+d$. This corresponds to the quadratic relation

$$\boldsymbol{a}_{a+1}^{q^l} \star \boldsymbol{a}_{b+1}^{q^l} - \boldsymbol{a}_{c+1}^{q^l} \star \boldsymbol{a}_{d+1}^{q^l} = 0.$$

The related code of relationships $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ has therefore a block diagonal structure with blocks of size r, *i.e.*, for each element in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$, the entries outside the m diagonal blocks of size $r \times r$ are 0. Thus, an element $\boldsymbol{A}$ of $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ has the following block shape:

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_{0,0} & & & \\ & \boldsymbol{A}_{1,1} & & \boldsymbol{0} \\ \boldsymbol{0} & & \ddots & \\ & & & \boldsymbol{A}_{m-1,m-1} \end{bmatrix} \tag{18}$$

where the diagonal blocks $\boldsymbol{A}_{i,i}$ are symmetric and of size r. Clearly $\mathbf{Rank}(\boldsymbol{A}_{i,i}) \leqslant r$ and, because of the block diagonal shape, $\mathbf{Rank}(\boldsymbol{A}) = \sum_i \mathbf{Rank}(\boldsymbol{A}_{i,i})$. Now assume that $\boldsymbol{A}$ happens to be minimally rank defective, i.e.

$$\mathbf{Rank}(\boldsymbol{A}) = rm - 1.$$

It means that for exactly one index $j \in [\![0, m-1]\!]$, $\mathbf{Rank}(\boldsymbol{A}_{j,j}) = r - 1$, and for all $i \in [\![0, m-1]\!] \backslash \{j\}$, $\mathbf{Rank}(\boldsymbol{A}_{i,i}) = r$. We consider the left kernel of (the map corresponding to) the matrix $\boldsymbol{A}$, simply denoted by $\ker(\boldsymbol{A})$. Note that, if we identify row vectors with column vectors, left and right kernels are the same in this case, as $\boldsymbol{A}$ is symmetric. Since $\mathbf{Rank}(\boldsymbol{A}) = rm-1$, we have $\dim(\ker(\boldsymbol{A})) = 1$. Let $\boldsymbol{v} = (\boldsymbol{v}_0, \dots, \boldsymbol{v}_{m-1}) \in \mathbb{F}_{q^m}^{rm}$ be a generator of $\ker(\boldsymbol{A})$, with $\boldsymbol{v}_i \in \mathbb{F}_{q^m}^r$. Because of the block diagonal structure of $\boldsymbol{A}$, $\boldsymbol{v}$ must satisfy

$$\boldsymbol{v} = (\boldsymbol{0}_r, \dots, \boldsymbol{0}_r, \boldsymbol{v}_j, \boldsymbol{0}_r, \dots, \boldsymbol{0}_r).$$

In other words, the computation of this nullspace provides information about the position of the vectors generating a single GRS code $\mathbf{GRS}_r(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$. The key idea is that if enough of such vectors are found, a basis of the corresponding GRS code can be retrieved.

6.1 Choosing $\mathcal{B}$ with a special shape

Consider an ordered basis

$$\mathcal{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_r, \boldsymbol{b}_1^q, \dots, \boldsymbol{b}_r^q, \dots, \boldsymbol{b}_1^{q^{m-1}}, \dots, \boldsymbol{b}_r^{q^{m-1}}) \tag{19}$$

of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})_{\mathbb{F}_{q^m}}^\perp$. Such a basis can be computed by drawing $\boldsymbol{b}_1, \dots, \boldsymbol{b}_r \in \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})_{\mathbb{F}_{q^m}}^\perp$ at random, applying the Frobenius map $m-1$ times and checking if the obtained family generates $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})_{\mathbb{F}_{q^m}}^\perp$, or equivalently if its dimension is rm. If not, draw another r-tuple $\boldsymbol{b}_1, \dots, \boldsymbol{b}_r$ at random until the construction provides a basis. We remark that even sampling a basis as in (19) does not provide a basis with the same properties of $\mathcal{A}$, *i.e.* $(\boldsymbol{b}_1, \dots, \boldsymbol{b}_r)$ is not an ordered basis of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$, except with negligible probability. When $\mathcal{B}$ is chosen as in (19), the transition matrix $\boldsymbol{P}$ has a special shape.

Lemma 1. *The matrix* $\boldsymbol{P}$ *is blockwise Dickson. That is to say, there exist* $\boldsymbol{P}_0, \dots, \boldsymbol{P}_{m-1} \in \mathbb{F}_{q^m}^{r \times r}$ *such that*

$$\boldsymbol{P} = \begin{pmatrix} \boldsymbol{P}_0 & \boldsymbol{P}_1 & \cdots & \boldsymbol{P}_{m-1} \\ \boldsymbol{P}_{m-1}^{(q)} & \boldsymbol{P}_0^{(q)} & \cdots & \boldsymbol{P}_{m-2}^{(q)} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{P}_1^{(q^{m-1})} & \boldsymbol{P}_2^{(q^{m-1})} & \cdots & \boldsymbol{P}_0^{(q^{m-1})} \end{pmatrix}. \tag{20}$$

Proof. This is a direct consequence of the structure of the bases $\mathcal{A}$ and $\mathcal{B}$. □

Let $\boldsymbol{S} \in \mathbf{GL}_{mr}(\mathbb{F}_{q^m})$ be the right r-cyclic shift matrix, *i.e.*

$$\boldsymbol{S} \overset{\text{def}}{=} \begin{pmatrix} & \boldsymbol{I}_r & & & \\ & & \boldsymbol{I}_r & & \boldsymbol{0} \\ & & \boldsymbol{0} & \ddots & \\ & & & & \boldsymbol{I}_r \\ \boldsymbol{I}_r & & & & \end{pmatrix}. \tag{21}$$

Note that $\boldsymbol{S}^{-1} = \boldsymbol{S}^\intercal$ is the left r-cyclic shift matrix. The block-wise Dickson structure of $\boldsymbol{P}$ can be re-interpreted as follows:

Proposition 19. *Let* $\boldsymbol{S}$ *be defined as in* (21) *and* $\boldsymbol{P}$ *satisfy the blockwise Dickson structure of* (20)*. Then* $\boldsymbol{P} = \boldsymbol{S}^\intercal \boldsymbol{P}^{(q)} \boldsymbol{S}$.

Proof. Direct computation. □

The following result will also be used frequently in what follows

Proposition 20. *Whenever a basis* $\mathcal{B}$ *has the form given in* (19)*,* $\mathscr{C}_{mat}(\mathcal{B})$ *is stable by the operation*

$$\boldsymbol{M} \longmapsto \boldsymbol{S}^\intercal \boldsymbol{M}^{(q)} \boldsymbol{S}.$$

The proof is given in §E of the appendix. Note that $\boldsymbol{S}^{(q^i)} = \boldsymbol{S}$ for any i. Therefore, by applying i times the map $\boldsymbol{M} \longmapsto \boldsymbol{S}^\intercal \boldsymbol{M}^{(q)} \boldsymbol{S}$, we obtain $\boldsymbol{M} \longmapsto (\boldsymbol{S}^\intercal)^i \boldsymbol{M}^{(q^i)} (\boldsymbol{S})^i$. We say that $\boldsymbol{M}$ and $(\boldsymbol{S}^\intercal)^i \boldsymbol{M}^{(q^i)} (\boldsymbol{S})^i$ are *blockwise Dickson shift* of the other.

6.2 The full algorithm with respect to a public basis $\mathcal{B}$

Algorithm 1 provides a sketch of the attack in the case of odd chacteristic field size. We will then justify why this algorithm is supposed to work with non-negligible probability, elaborate on some subroutines (as sampling matrices of rank $rm - 1$) and adapt it to the even characteristic case. We now show the structure of the attack, given a public basis $\mathcal{B}$. In this case, it becomes crucial to choose a basis of the following form

$$\mathcal{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_r, \boldsymbol{b}_1^q, \dots, \boldsymbol{b}_r^q, \dots, \boldsymbol{b}_1^{q^{m-1}}, \dots, \boldsymbol{b}_r^{q^{m-1}}).$$

Algorithm 1 Sketch of the attack for odd characteristic

```
1: Choose a basis $\mathcal{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_r, \boldsymbol{b}_1^q, \dots, \boldsymbol{b}_r^q, \dots, \boldsymbol{b}_1^{q^{m-1}}, \dots, \boldsymbol{b}_r^{q^{m-1}})$ for $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}_{\mathbb{F}_{q^m}}$.
2: $\mathscr{S}_{aux} \leftarrow \{0\}$
3: repeat
4:     Sample $\boldsymbol{B} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of rank $rm - 1$ at random
5:     $\boldsymbol{v} \leftarrow$ generator of $\ker(\boldsymbol{B})$
6:     $\mathscr{S}_{aux} \leftarrow \mathscr{S}_{aux} + \left\langle \boldsymbol{v}, \boldsymbol{v}^q \boldsymbol{S}, \dots, \boldsymbol{v}^{q^{m-1}} \boldsymbol{S}^{m-1} \right\rangle_{\mathbb{F}_{q^m}}$
7: until $\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} = (r-1)m$    ▷ At that point $\mathscr{S}_{aux}$ is a subspace of kernel
   elements of matrices of $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of rank $rm - 1$.
8: Sample $\boldsymbol{B}_1 \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of rank $rm - 1$ at random
9: $\boldsymbol{u}_1 \leftarrow$ generator of $\ker(\boldsymbol{B}_1)$
10: $\mathscr{V} \leftarrow \langle \boldsymbol{u}_1 \rangle$
11: for $j \in [\![2, r]\!]$ do
12:     Sample $\boldsymbol{B}_j \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of rank $rm - 1$ at random
13:     $\boldsymbol{u}_j \leftarrow$ generator of $\ker(\boldsymbol{B}_j)$
14:     repeat
15:         $\boldsymbol{u}_j \leftarrow \boldsymbol{u}_j^q \boldsymbol{S}$
16:     until $\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \langle \boldsymbol{u}_1, \boldsymbol{u}_j \rangle = (r-1)m + 1$
17:     $\mathscr{V} \leftarrow \mathscr{V} + \langle \boldsymbol{u}_j \rangle$
18: $\mathscr{D} \leftarrow \mathscr{V}^{\perp}$
19: $\mathscr{G} \leftarrow \mathscr{D}$
20: for $j \in [\![1, m-2]\!]$ do
21:     $\mathscr{D} \leftarrow \mathscr{D}^{(q)} \boldsymbol{S}$
22:     $\mathscr{G} \leftarrow \mathscr{G} \cap \mathscr{D}$
23: Apply the Sidelnikov-Shestakov attack on $\mathscr{G} \cdot \boldsymbol{H}_{\mathcal{B}}$
```

How to compute such a basis has already been explained in a previous section. The correctness of the whole algorithm follows on the spot from the following propositions whose proofs can be found in the appendix. The first one explains why when we have one kernel element in Algorithm 1 at line 6 we can find $m-1$ other ones.

Proposition 21. *Let $\boldsymbol{v}$ be in the kernel of a matrix $\boldsymbol{B}$ in $\mathscr{C}_{mat}(\mathcal{B})$ of rank $rm-1$. Then $\boldsymbol{v}^q \boldsymbol{S}, \dots, \boldsymbol{v}^{q^{m-1}} \boldsymbol{S}^{m-1}$ are $m-1$ elements that are also kernel elements of matrices in $\mathscr{C}_{mat}(\mathcal{B})$ of rank $rm-1$ which are respectively $\boldsymbol{S}^{\mathsf{T}} \boldsymbol{B}^{(q)} \boldsymbol{S}, \cdots, (\boldsymbol{S}^{\mathsf{T}})^{m-1} \boldsymbol{B}^{(q^{m-1})} \boldsymbol{S}^{m-1}$.*

Then we are going to give a description of the space $\mathscr{V}$ produced in line 17. Basically this a vector space of elments that correspond to a same GRS code, in the following sense.

Definition 11. *Let $\mathcal{A}, \mathcal{B}$ be the two basis introduced before and $\boldsymbol{P}$ the change of basis, i.e. $\boldsymbol{H}_{\mathcal{B}} = \boldsymbol{P} \boldsymbol{H}_{\mathcal{A}}$. Let $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{F}_{q^m}^{rm}$ be two vectors such that*

$$\boldsymbol{u}_t (\boldsymbol{P}^{-1})^{\mathsf{T}} \boldsymbol{P}^{-1} \boldsymbol{H}_{\mathcal{B}} \in \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{q^{j_t}}$$

*for some values $j_t \in [\![0, m-1]\!]$. We say that $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ **correspond to the same GRS code with respect to the basis** $\mathcal{B}$ if and only if $j_1 = j_2$.*

Two vectors $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ obtained by computing the nullspaces or rank $rm-1$ matrices can correspond or not to the same GRS code. In any case, from them, we can easily exhibit two vectors corresponding to the same GRS code by choosing among their shifts $\boldsymbol{v}^{q^i}\boldsymbol{S}^i$. More precisely, we have

Proposition 22. *Let $\mathcal{A}, \mathcal{B}$ be the two basis introduced before and $\boldsymbol{P}$ the change of basis, i.e. $\boldsymbol{H}_{\mathcal{B}} = \boldsymbol{P}\boldsymbol{H}_{\mathcal{A}}$. Let $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{F}_{q^m}^{rm}$ be two vectors such that*

$$\boldsymbol{u}_t(\boldsymbol{P}^{-1})^{\intercal}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} \in \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^{j_t})}$$

for some values $j_t \in [\![0, m-1]\!]$. There exists a unique $l \in [\![0, m-1]\!]$ such that $\boldsymbol{u}_1$ and $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ correspond to the same GRS code.

To detect which shift of $\boldsymbol{u}_2$ corresponds to the same GRS code of $\boldsymbol{u}_1$, we rely on the following proposition.

Proposition 23. *Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{r-1}, \boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{F}_{q^m}^{rm}$ be the generators of the kernels of $\boldsymbol{B}_1, \dots, \boldsymbol{B}_{r-1}, \boldsymbol{B}', \boldsymbol{B}'' \in \mathscr{C}_{mat}(\mathcal{B})$ respectively, for randomly sampled matrices of rank $rm-1$. Define*

$$\mathscr{S}_{aux} \overset{def}{=} \left\langle \boldsymbol{v}_j^{q^l}\boldsymbol{S}^l \mid j \in [\![1, r-1]\!], l \in [\![0, m-1]\!] \right\rangle_{\mathbb{F}_{q^m}}.$$

If the following conditions are satisfied:

- *$\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} = (r-1)m$ (i.e. the $(r-1)m$ vectors that generate $\mathscr{S}_{aux}$ are linearly independent;*
- *$\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \langle \boldsymbol{u}_t \rangle_{\mathbb{F}_{q^m}} = (r-1)m+1, \quad t = 1, 2;$*

then the two following statements are equivalent:

1. *$\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \left\langle \boldsymbol{u}_1, \boldsymbol{u}_2^{q^l}\boldsymbol{S}^l \right\rangle_{\mathbb{F}_{q^m}} = (r-1)m+1;$*
2. *$\boldsymbol{u}_1$ and $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ correspond to the same GRS code with respect to $\mathcal{B}$.*

We are therefore able to construct a space of dimension r whose elements all correspond to a same GRS code. Then we use

Proposition 24. *Let $\mathscr{V}_j$ be the $[rm, r]$ linear code generated by r linearly independent vectors corresponding to the same GRS code $\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^j)}$ with respect to $\mathcal{B}$. Then the linear space $\mathscr{V}_j^{\perp}$ orthogonal to $\mathscr{V}_j$ is such that*

$$\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}} = \sum_{i \in [\![0,m-1]\!]\setminus\{j\}} \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^i)}. \tag{22}$$

Given $\mathscr{V}_j^{\perp}$, the other codes $\mathscr{V}_i^{\perp}\boldsymbol{H}_{\mathcal{B}}$ that are sums of $m-1$ GRS codes can be obtained according to the the following chain of equalities

$$\sum_{i \in [\![0,m-1]\!]\setminus\{j+l \mod m\}} \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^i)}$$

$$= \left(\sum_{i \in [\![0,m-1]\!]\setminus\{j\}} \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^i)} \right)^{(q^l)} = (\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}})^{(q^l)} = (\mathscr{V}_j^{\perp})^{(q^l)}\boldsymbol{H}_{\mathcal{B}}^{(q^l)} = (\mathscr{V}_j^{\perp})^{(q^l)}\boldsymbol{S}\boldsymbol{H}_{\mathcal{B}}.$$

After this, we are ready to compute a basis of a GRS code.

Proposition 25. *Let $\mathscr{V}_j^{\perp}$ be a linear space satisfying Equation* (22)*, for all $j \in [\![0, m-1]\!]$. Then with the standard assumption that all $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^j)}$ are in direct sum, we obtain, for any $j \in [\![0, m-1]\!]$,*

$$\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^j)} = \bigcap_{i \in [\![0, m-1]\!] \setminus \{j\}} \mathscr{V}_i^{\perp} \boldsymbol{H}_{\mathcal{B}}.$$

Remark 3. In the q odd case, the only exception to what was said until now occurs for $r = 3$. In this case a non-full rank diagonal block $\boldsymbol{B}_{j,j}$ becomes the null block, because there are no matrices of rank 1 or 2. In this case, the kernel of a rank $r(m-1) = 3m-3$ matrix is a three-dimensional subspace, which immediately provides the subspace $\mathscr{V}_j$ from which to recover the associated GRS codes.

How to sample matrices in $\mathscr{C}_{\mathbf{mat}}(\boldsymbol{\mathcal{B}})$ of rank $rm - 1$

This is the most costly part of the algorithm. We first address the case of odd characteristic, as the case of even characteristic needs an ad hoc discussion. It is not too difficult to estimate that the density of rank $rm-1$ matrices inside $\mathscr{C}_{\mathrm{mat}}(B)$ is of order q^{-m} (see E.7) and therefore it is desirable to have a better technique than just a brute force approach. We proceed instead as follows. We take two matrices $\boldsymbol{D}_1, \boldsymbol{D}_2$ at random in $\mathscr{C}_{\mathrm{mat}}(\mathcal{D})$ and solve over $\mathbb{F}_{q^m}$ the equation

$$\det(w\boldsymbol{D}_1 + \boldsymbol{D}_2) = 0.$$

The determinant $\det(w\boldsymbol{D}_1 + \boldsymbol{D}_2)$ is a univariate polynomial of degree rm and since w is taken over $\mathbb{F}_{q^m}$ we can expect to have solutions with non-negligible probability. A root w_0 of $\det(w\boldsymbol{D}_1 + \boldsymbol{D}_2)$ determines a matrix $w_0\boldsymbol{D}_1 + \boldsymbol{D}_2$ whose rank is strictly smaller than rm but not necessarily equal to $rm-1$. However, the rank $rm-1$ is by far the most likely outcome. Repeating the process enough times ($\Theta(1)$ times on average) then provides a matrix of rank $rm-1$.

6.3 Even characteristic

This case is treated in the appendix.

7 Conclusion

A general methodology for studying the key security of the McEliece cryptosystem. Trying to find an attack on the key of the McEliece scheme based on Goppa codes, has turned out over the years to be a formidable problem. The progress on this issue has basically been non existent for many years and it was for a long time judged that the McEliece scheme is immune against this kind of attacks. This changed a little bit when many variants of the original

McEliece came out, either by turning to a slightly larger class of codes namely the alternant codes which retain the main algebraic structure of the Goppa code and/or adding additional structure on it [BCGO09, BBB$^+$17], changing the alphabet [BLP10, BLP11], or going to extreme parameters [CFS01]. This has lead to devise many tools to attack these variants such as algebraic modeling to recover the alternant stucture of a Goppa code which is basically enough to recover its structure [FOPT10], using square code considerations [COT14], or trying to solve a simpler problem which is to distinguish these algebraic codes from random codes [FGO$^+$11, FGO$^+$13, MT22]. We actually believe that in order to make further progress on this very hard problem, it is desirable to move away now from studying particular schemes proposed in the literature, by exploring and developing systematically tools for solving this problem and study the region of parameters (alphabet size q, code length n, degree r of the code, extension degree m) where these methods work. We suggest the following research plan

- Studying the slightly more general problem of attacking alternant codes might be the right way to go because it retains the essential algebraic features of Goppa codes and it allows to find attacks that might not work in the subcase of Goppa codes where the additional structure can be a nuisance. An example which is particularly enlightening here is the recent work [BMT23] (attack on generic alternant codes in a certain parameter regime which amazingly does not work in the particular case of Goppa codes where the additional structure prevents the attack to work).
- A particularly fruitful research thread is to study potentially the easier problem of finding a distinguisher for alternant/Goppa codes first.
- Turn later on this distinguisher into an attack (such as [BMT23] for the distinguisher of [FGO$^+$11]).

This is the research plan we have followed to some extent here.

A distinguisher in odd characteristic. It is clear that any algebraic modeling for solving the symmetric MinRank problem for rank 3 could be used to attack the problem in odd characteristic. The Support Minors modeling of [BBC$^+$20] would be for instance a good candidate for this. The difficulty is here to predict the complexity of system solving, since the fact that the matrices are symmetric gives many new linear dependencies that do not happen in the generic MinRank case. This is clearly a promising open problem.

Turning the distinguisher of §5 into an attack. The Pfaffian modeling for the distinguisher can be used in principle to attack the key-recovery problem as well. This problem is strictly harder than just distinguishing because of the algebraic structure in the code $\mathscr{C}_{\text{mat}}(\mathcal{A})$ that is much stronger than in $\mathscr{C}_{\text{mat}}(\mathcal{R})$ (random case). In particular, rank 2 matrices are found at a potentially larger degree than $\bar{d}$ at which the Hilbert function in the random case becomes 0. The fact that the solution space is very large, in particular it contains a rather large vector space (see Section 4), suggests though that we can safely specialize a rather large number of variables to speed up the system solving. Once a rank 2 matrix is found, the attack is not finished yet, but it is tempting to conjecture that the main bottleneck is to find such a matrix first and that for some of the tools developed in the attack given in Section 6 might be used to finish the job.

Indeed, since rank 2 matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ are identically zero outside the main block diagonal, we can consider a matrix subcode spanned by many of them, obtained by solving the Pfaffian system with different specializations. This subcode will have a block diagonal shape and that is why the attack of the last section is expected to apply on such subspace.

References

[ABC$^+$22] Martin Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Mizoczki, Ruben Niederhagen, Edoardo Persichetti, Kenneth Paterson, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wang Wen. Classic McEliece (merger of Classic McEliece and NTS-KEM). `https://classic.mceliece.org`, November 2022. Fourth round finalist of the NIST post-quantum cryptography call.

[Bar04] Magali Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Paris VI, December 2004. http://tel.archives-ouvertes.fr/tel-00449609/en/.

[BBB$^+$17] Gustavo Banegas, Paulo S.L.M Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti, and Jefferson E. Ricardini. DAGS : Key encapsulation for dyadic GS codes. `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/DAGS.zip`, November 2017. First round submission to the NIST post-quantum cryptography call.

[BBB$^+$22] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. Revisiting algebraic attacks on minrank and on the rank decoding problem, 2022.

[BBC$^+$20] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. 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*, pages 507–536, 2020.

[BCGO09] Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani. Reducing key length of the McEliece cryptosystem. In Bart Preneel, editor, *Progress in Cryptology - AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 77–97, Gammarth, Tunisia, June 21-25 2009.

[Ber10] Daniel J. Bernstein. Grover vs. McEliece. In Nicolas Sendrier, editor, *Post-Quantum Cryptography 2010*, volume 6061 of *LNCS*, pages 73–80. Springer, 2010.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

[BLM11] Paulo Barreto, Richard Lindner, and Rafael Misoczki. Monoidic codes in cryptography. In *Post-Quantum Cryptography 2011*, volume 7071 of *LNCS*, pages 179–199. Springer, 2011.

[BLP10] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Wild McEliece. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *LNCS*, pages 143–158, 2010.

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Wild McEliece Incognito. In Bo-Yin Yang, editor, *Post-Quantum Cryptography 2011*, volume 7071 of *LNCS*, pages 244–254. Springer Berlin Heidelberg, 2011.

[BM17] Leif Both and Alexander May. Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{2/21n}$ and McEliece Security. In *WCC Workshop on Coding and Cryptography*, September 2017.

[BMT23] Magali Bardet, Rocco Mora, and Jean-Pierre Tillich. Polynomial time key-recovery attack on high rate random alternant codes. *CoRR*, abs/2304.14757, 2023.

[CBB$^+$17] Alain Couvreur, Magali Bardet, Élise Barelli, Olivier Blazy, Rodolfo Canto Torres, Phillipe Gaborit, Ayoub Otmani, Nicolas Sendrier, and Jean-Pierre Tillich. BIG QUAKE. `https://bigquake.inria.fr`, November 2017. NIST Round 1 submission for Post-Quantum Cryptography.

[CC98] Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Trans. Inform. Theory*, 44(1):367–378, 1998.

[CCMZ15] Igniacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of random linear codes. *IEEE Trans. Inform. Theory*, 61(3):1159–1173, 3 2015.

[CCNY12] Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang. Solving quadratic equations with xl on parallel architectures. In *Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14*, pages 356–373. Springer, 2012.

[CFS01] Nicolas Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 157–174, Gold Coast, Australia, 2001. Springer.

[CGG$^+$14] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. *Des. Codes Cryptogr.*, 73(2):641–666, 2014.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, pages 392–407, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[COT14] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. New identities relating wild Goppa codes. *Finite Fields Appl.*, 29:178–197, 2014.

[Dum89] Il'ya Dumer. Two decoding algorithms for linear codes. *Probl. Inf. Transm.*, 25(1):17–23, 1989.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero: F5. In *Proceedings ISSAC'02*, pages 75–83. ACM press, 2002.

[FGO$^+$11] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high rate McEliece cryptosystems. In *Proc. IEEE Inf. Theory Workshop- ITW 2011*, pages 282–286, Paraty, Brasil, October 2011.

[FGO$^+$13] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high rate McEliece cryptosystems. *IEEE Trans. Inform. Theory*, 59(10):6830–6844, October 2013.

[FLP08] Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. Cryptanalysis of Minrank. In David Wagner, editor, *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *LNCS*, pages 280–296, 2008.

[FOPT10] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 279–298, 2010.

[FPdP14] Jean-Charles Faugère, Ludovic Perret, and Frédéric de Portzamparc. Algebraic attack against variants of McEliece with Goppa polynomial of a special form. In *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 21–41, Kaoshiung, Taiwan, R.O.C., December 2014. Springer.

[FSEDS10] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In *International Symposium on Symbolic and Algebraic Computation, ISSAC 2010, Munich, Germany, July 25-28, 2010*, pages 257–264, 2010.

[GC00] Louis Goubin and Nicolas Courtois. Cryptanalysis of the TTM cryptosystem. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 44–57. Springer, 2000.

[GK04] Sudhir R Ghorpade and Christian Krattenthaler. The hilbert series of pfaffian rings. In *Algebra, Arithmetic and Geometry with Applications: Papers from Shreeram S. Abhyankar's 70th Birthday Conference*, pages 337–356. Springer, 2004.

[GUL09] Valérie Gauthier-Umaña and Gregor Leander. Practical key recovery attacks on two McEliece variants, 2009. IACR Cryptology ePrint Archive, Report2009/509.

[HT92] Jürgen Herzog and Ngô Viêt Trung. Gröbner bases and multiplicity of determinantal and pfaffian ideals. *Advances in Mathematics*, 96(1):1–37, 1992.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in Cryptology - CRYPTO'99*, volume 1666 of *LNCS*, pages 19–30, Santa Barbara, California, USA, August 1999. Springer.

[KT17] Ghazal Kachigar and Jean-Pierre Tillich. Quantum information set decoding algorithms. In *Post-Quantum Cryptography 2017*, volume 10346 of *LNCS*, pages 69–89, Utrecht, The Netherlands, June 2017. Springer.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra*, volume 162 of *LNCS*, pages 146–156, Berlin, 1983. Springer. Proceedings Eurocal'83, London, 1983.

[LS01] Pierre Loidreau and Nicolas Sendrier. Weak keys in the McEliece public-key cryptosystem. *IEEE Trans. Inform. Theory*, 47(3):1207–1211, 2001.

[Mac94] Francis Sowerby Macaulay. *The algebraic theory of modular systems*, volume 19. Cambridge University Press, 1994.

[Mas69] James L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inform. Theory*, 15(1):122–127, 1969.

[MB09] Rafael Misoczki and Paulo Barreto. Compact McEliece keys from Goppa codes. In *Selected Areas in Cryptography*, Calgary, Canada, August 13-14 2009.

[McE78] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $O(2^{0.054n})$. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[MO15] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[MP12] Irene Márquez-Corbella and Ruud Pellikaan. Error-correcting pairs for a public-key cryptosystem. CBC 2012, Code-based Cryptography Workshop, 2012. Available on `http://www.win.tue.nl/~ruudp/paper/59.pdf`.

[MS86] Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North–Holland, Amsterdam, fifth edition, 1986.

[MT22] Rocco Mora and Jean-Pierre Tillich. On the dimension and structure of the square of the dual of a Goppa code. In *WCC 2022 - Workshop on Coding Theory and Cryptography*, 2022.

[Pat75] N. Patterson. The algebraic decoding of Goppa codes. *IEEE Trans. Inform. Theory*, 21(2):203–207, 1975.

[Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[Sen00] Nicolas Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. *IEEE Trans. Inform. Theory*, 46(4):1193–1203, 2000.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In S. Goldwasser, editor, *FOCS*, pages 124–134, 1994.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.

[VBC$^+$19] Javier Verbel, John Baena, Daniel Cabarcas, Ray Perlner, and Daniel Smith-Tone. On the complexity of “superdetermined” Minrank instances. In *Post-Quantum Cryptography 2019*, volume 11505 of *LNCS*, pages 167–186, Chongqing, China, May 2019. Springer.

A Gröbner bases and Computing the Hilbert Series

Gröbner basis techniques are the main tool at hand to solve multivariate polynomial systems and therefore to perform algebraic cryptanalysis. One crucial notion for this kind of computation and for the complexity analysis is the Macaulay matrix [Mac94]. We give the definition that is relevant in the homogeneous case.

Definition 12 (Macaulay Matrix [Mac94]). *Let* $F = \{f_1, \dots, f_m\} \subset \mathbb{K}[\boldsymbol{x}]$ *be a homogeneous system such that* $\deg(f_i) = d_i$. *Let* d *be a positive integer. The (homogeneous) Macaulay matrix* $Mac(F, d)$ *of* F *in degree* d *is a matrix whose rows are each indexed by a polynomial* $m_j f_i$*, for any* $f_i \in F$ *and any monomial* m_j *of degree* $d - d_i$*, and whose columns are indexed by all the monomials of degree* *d. The entry corresponding to the row indexed by $m_j f_i$ and column indexed by m_l is the coefficient of m_l in $m_j f_i$. In particular, if $m_j f_i = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \boldsymbol{x}^\alpha$ and $m_l = \boldsymbol{x}^\beta$, then the corresponding entry of $Mac(F, d)$ is a_β:*

$$Mac(F, d) = \begin{array}{c} \\ m_j f_i \end{array} \begin{array}{c} m_l \\ \begin{bmatrix} & \vdots & \\ \cdots & a_\beta & \cdots \\ & \vdots & \end{bmatrix} \end{array}.$$

A Gröbner basis can be computed using linear algebra, in particular [Laz83] showed that it is enough to perform Gaussian elimination on a Macaulay matrix in degree equal to the degree of regularity d_{reg}. Several algorithms and variants are linear-algebra based, for instance F4 [Fau99], F5 [Fau02] or XL [CKPS00]. Differently from methods not exploiting the Macaulay matrix construction, this approach allows to derive complexity estimates for this task. Computing the Hilbert series can also be done with these methods and this is the only result we need here, which is

Proposition 13. *Let $F = \{f_1, \ldots, f_m\} \subset \mathbb{K}[z_1, \ldots, z_n]$ be a homogeneous system. Let $\mathcal{I}$ be the corrresponding ideal. The term $HF_R(d)$ of degree d of the Hilbert function of $R = \mathbb{K}[\boldsymbol{z}]/\mathcal{I}$ can be computed in time bounded by*

$$\mathcal{O}\left(md\binom{n+d-1}{d}^\omega\right),$$

where ω is the linear algebra exponent.

We also remark that these methods can take advantage of algorithms that benefit from matrix sparsity [CCNY12].

B Proof related to Section 3

Let us recall the proposition we prove.

Proposition 4. *Let $\mathcal{A}$ and $\mathcal{B}$ be two bases of a same $[n, k]$ $\mathbb{F}$-linear code $\mathscr{C}$, with $\mathbb{F}$. Then $\mathscr{C}_{mat}(\mathcal{A})$ and $\mathscr{C}_{mat}(\mathcal{B})$ are isometric matrix codes, i.e. there exists $\boldsymbol{P} \in \mathbf{GL}_k(\mathbb{F})$ such that*

$$\mathscr{C}_{mat}(\mathcal{A}) = \boldsymbol{P}^\intercal \mathscr{C}_{mat}(\mathcal{B}) \boldsymbol{P}. \tag{10}$$

The matrix $\boldsymbol{P}$ coincides with the change of basis matrix between $\mathcal{A}$ and $\mathcal{B}$.

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be related as $\boldsymbol{H}_\mathcal{B} = \boldsymbol{P}\boldsymbol{H}_\mathcal{A}$. where $\boldsymbol{H}_\mathcal{A}$, resp. $\boldsymbol{H}_\mathcal{B}$ is a matrix whose rows are the basis elements of $\mathcal{A}$, resp. $\mathcal{B}$. It will be helpful to view an element $\boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k}$ of $\mathscr{C}_{\text{rel}}$ as a matrix $\boldsymbol{C} = (C_{i,j})_{\substack{1 \leqslant i \leqslant k \\ 1 \leqslant j \leqslant k}}$ where $C_{ij} = c_{ij}$ for $i \leqslant j$ and $C_{ij} = 0$ otherwise. We can write the matrix $\boldsymbol{M_c}$ of $\mathscr{C}_{\text{mat}}$ corresponding to $\boldsymbol{c}$ as $\boldsymbol{M_c} = \boldsymbol{C} + \boldsymbol{C}^\intercal$. Consider an element $\boldsymbol{M} \in \mathscr{C}_{\text{mat}}(\mathcal{B})$. By definition of $\mathscr{C}_{\text{mat}}(\mathcal{B})$ there is an element $\boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k}$ of $\mathscr{C}_{\text{rel}}(\mathcal{B})$ such that

$\boldsymbol{M} = \boldsymbol{M_c}$. Consider the matrix $\boldsymbol{C}$ corresponding to $\boldsymbol{c}$ that we just introduced. By definition of $\mathscr{C}_{\mathrm{rel}}(\mathcal{B})$ we have

$$\sum_{1 \leqslant i \leqslant j \leqslant k} c_{i,j} \boldsymbol{b}_i \star \boldsymbol{b}_j = 0. \tag{23}$$

We have for all i in $[\![1,k]\!]$: $\boldsymbol{b}_i = \sum_{s=1}^{k} p_{is} \boldsymbol{a}_s$, where $p_{i,j}$ denotes the entry (i,j) of $\boldsymbol{P}$. Therefore

$$\begin{aligned}
\sum_{1 \leqslant i \leqslant j \leqslant k} c_{i,j} \boldsymbol{b}_i \star \boldsymbol{b}_j &= \sum_{1 \leqslant i \leqslant j \leqslant k} c_{i,j} \left(\sum_{s \in [\![1,k]\!]} p_{i,s} \boldsymbol{a}_s \right) \star \left(\sum_{t \in [\![1,k]\!]} p_{j,t} \boldsymbol{a}_t \right) \\
&= \sum_{s,t \in [\![1,k]\!]} \left(\sum_{1 \leqslant i \leqslant j \leqslant k} p_{i,s} p_{j,t} c_{i,j} \right) \boldsymbol{a}_s \star \boldsymbol{a}_t \\
&= \sum_{1 \leqslant s < t \leqslant k} \left(\sum_{1 \leqslant i \leqslant j \leqslant k} (p_{i,s} p_{j,t} + p_{i,t} p_{j,s}) c_{i,j} \right) \boldsymbol{a}_s \star \boldsymbol{a}_t \\
&\quad + \sum_{s \in [\![1,k]\!]} \left(\sum_{1 \leqslant i \leqslant j \leqslant k} p_{i,s} p_{j,s} c_{i,j} \right) \boldsymbol{a}_s \star \boldsymbol{a}_s
\end{aligned}$$

Let $\boldsymbol{D} = (d_{s,t})_{\substack{1 \leqslant s \leqslant k \\ 1 \leqslant t \leqslant k}}$ where

$$\begin{aligned}
d_{s,t} &\stackrel{\text{def}}{=} \sum_{1 \leqslant i \leqslant j \leqslant k} (p_{i,s} p_{j,t} + p_{i,t} p_{j,s}) c_{i,j} \quad \text{for } 1 \leqslant s < t \leqslant k \\
d_{s,s} &\stackrel{\text{def}}{=} \sum_{1 \leqslant i \leqslant j \leqslant k} p_{i,s} p_{j,s} c_{i,j} \quad \text{for } s \in [\![1,k]\!] \\
d_{s,t} &\stackrel{\text{def}}{=} 0 \quad \text{otherwise.}
\end{aligned}$$

$\boldsymbol{d} \stackrel{\text{def}}{=} (d_{i,j})_{1 \leqslant i \leqslant j \leqslant k}$ is because of (23) an element of $\mathscr{C}_{\mathrm{rel}}(\mathcal{A})$. Now from the definition of $\boldsymbol{D}$ is clear that we have $\boldsymbol{D} + \boldsymbol{D}^{\mathsf{T}} = \boldsymbol{P}^{\mathsf{T}} \left(\boldsymbol{C} + \boldsymbol{C}^{\mathsf{T}} \right) \boldsymbol{P}$. In other words, the matrix $\boldsymbol{M_d}$ in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ corresponding to $\boldsymbol{d}$ satisfies

$$\begin{aligned}
\boldsymbol{M_d} &= \boldsymbol{D} + \boldsymbol{D}^{\mathsf{T}} \\
&= \boldsymbol{P}^{\mathsf{T}} \left(\boldsymbol{C} + \boldsymbol{C}^{\mathsf{T}} \right) \boldsymbol{P} \\
&= \boldsymbol{P}^{\mathsf{T}} \boldsymbol{M_c} \boldsymbol{P}.
\end{aligned}$$

This holds for any $\boldsymbol{c}$ in $\mathscr{C}_{\mathrm{rel}}(\mathcal{B})$. This leads to $\boldsymbol{P}^{\mathsf{T}} \mathscr{C}_{\mathrm{mat}}(\mathcal{B}) \boldsymbol{P} \subseteq \mathscr{C}_{\mathrm{mat}}(\mathcal{A})$. Since $\boldsymbol{P}$ is invertible, this implies $\mathscr{C}_{\mathrm{mat}}(\mathcal{A}) = \boldsymbol{P}^{\mathsf{T}} \mathscr{C}_{\mathrm{mat}}(\mathcal{B}) \boldsymbol{P}$. □

C Proofs of some results given in Section 4

C.1 Proofs of the results given in §4.1

For all the proofs given here we recall that we have fixed the basis

$$\mathcal{A} \stackrel{\text{def}}{=} \{ \boldsymbol{y}, \boldsymbol{xy}, \ldots, \boldsymbol{x}^{r-1} \boldsymbol{y}, \ldots, \boldsymbol{y}^{q^{m-1}}, (\boldsymbol{xy})^{q^{m-1}}, \ldots, (\boldsymbol{x}^{r-1} \boldsymbol{y})^{q^{m-1}} \}.$$

We will also consider the following block form of the matrices $\boldsymbol{M} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$:

$$\boldsymbol{M}_{\boldsymbol{c}} = \begin{pmatrix} \boldsymbol{M}_{0,0} & \boldsymbol{M}_{0,1} \dots & \boldsymbol{M}_{0,m-1} \\ \boldsymbol{M}_{1,0} & \ddots & \\ \vdots & & \vdots \\ \boldsymbol{M}_{m-1,0} & \dots & \boldsymbol{M}_{m-1,m-1} \end{pmatrix},$$

with $\boldsymbol{M}_{l,u} = (m_{i,j}^{(l,u)})_{\substack{0 \leqslant i \leqslant r-1 \\ 0 \leqslant j \leqslant r-1}} \in \mathbb{F}_{q^m}^{r \times r}$.

We are first going to prove Proposition 9 which is given by

Proposition 9. *Let $\mathscr{G}(\boldsymbol{x}, \Gamma)$ be a binary $[n, n-rm]$ Goppa code with Γ a square-free polynomial of degree r and let $\mathcal{A}$ be the canonical basis of $\mathscr{G}(\boldsymbol{x}, \Gamma)_{\mathbb{F}_{q^m}}^{\perp}$ given in* (11) *with $\boldsymbol{y} = \frac{1}{\Gamma(\boldsymbol{x})}$. Then $\mathscr{C}_{mat}(\mathcal{A})$ contains the space of block-diagonal skew-symmetric matrices with $r \times r$ blocks.*

Proof. Recall from [Pat75] that, if $\mathscr{G}(\boldsymbol{x}, \Gamma) = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ and Γ is a square-free polynomial of degree r, then

$$\mathscr{G}(\boldsymbol{x}, \Gamma) = \mathscr{G}(\boldsymbol{x}, \Gamma^2) = \mathscr{A}_{2r}(\boldsymbol{x}, \boldsymbol{y}^2).$$

Thus

$$\boldsymbol{x}^{i2^l} \boldsymbol{y}^{2^{(l+1 \mod m)}} \in \mathscr{G}(\boldsymbol{x}, \Gamma)_{\mathbb{F}_{q^m}}^{\perp},$$

for all $i \in [\![0, 2r-1]\!], l \in [\![0, m-1]\!]$. Consequently each equation

$$(\boldsymbol{x}^a \boldsymbol{y})^{2^l} (\boldsymbol{x}^b \boldsymbol{y})^{2^l} = (\boldsymbol{x}^{a+b} \boldsymbol{y}^2)^{2^{l-1}} (\boldsymbol{x}^{a+b} \boldsymbol{y}^2)^{2^{l-1}}, \tag{24}$$

with $l \in [\![1, m]\!], 0 \leqslant b < a < r$ corresponds to a codeword $\boldsymbol{c}$ in $\mathscr{C}_{\mathrm{rel}}(\mathcal{A})$. Let us fix (a, b, l). Since $(\boldsymbol{x}^{a+b} \boldsymbol{y}^2)^{2^{l-1}} (\boldsymbol{x}^{a+b} \boldsymbol{y}^2)^{2^{l-1}}$ is a square and the field characteristic is 2, the matrix $\boldsymbol{M} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ corresponding to the relation (24) is such that

$$\boldsymbol{M}_{l,u} = \boldsymbol{0}_{r \times r}, \quad \text{if } l \neq u$$

and

$$m_{i,j}^{(l,l)} = \begin{cases} 1 & \text{if } (i,j) \in \{(a,b), (b,a)\} \\ 0 & \text{otherwise} \end{cases}.$$

Hence

$$\mathbf{Rank}(\boldsymbol{M}) = \mathbf{Rank}(\boldsymbol{M}_{l,l}) = 2.$$

It is trivial to check that the set of matrices obtained by any possible choice of a, b and l generates the space of all block-diagonal skew-symmetric matrices with $r \times r$ blocks. *qed*

Let us prove Proposition 6 that we recall here

Proposition 6. *Let $\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})$ be an alternant code of extension degree m and order r over a field of characteristic 2. Then $\mathscr{C}_{mat}$ contains $\left\lfloor \frac{r-1}{2} \right\rfloor$-dimensional subspaces of rank-($\leqslant 2$) matrices. If $\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})$ is a binary Goppa code with a square-free Goppa polynomial, then $\mathscr{C}_{mat}$ contains $(r-1)$-dimensional subspaces of rank-($\leqslant 2$) matrices.*

Proof. Let us consider the matrix subspace originated by choosing all the matrices corresponding to (12) for a fixed $l = u$ and such that $c = d$, $a + b = 2c$, a and b are even and one between them equals a fixed even value j (alternatively one can choose a, b both odd and one equal to an odd j). Any matrix $\boldsymbol{M}$ in this subspace is zero outside the union of the $(lr + j + 1)$-th column and the $(lr + j + 1)$-th row. Its rank is therefore upper bounded by 2. In other words, any such matrix $\boldsymbol{M}$ has the following shape

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{0} & & & \\ & \ddots & & \mathbf{0} \\ & & \boldsymbol{M}_{l,l} & \\ & \mathbf{0} & & \ddots \\ & & & \mathbf{0} \end{bmatrix}, \quad \text{with} \quad \boldsymbol{M}_{l,l} = \left[\begin{array}{cccccccc} \mathbf{0} & & * & & \mathbf{0} & & & \\ & & 0 & & & & & \\ * & 0 & 0 & 0 & * & 0 & * & 0 \\ & & 0 & & & & & \\ & & * & & & & & \\ \mathbf{0} & & 0 & & \mathbf{0} & & & \\ & & * & & & & & \\ & & 0 & & & & & \end{array}\right] \begin{array}{l} \\ \\ \leftarrow (j+1)\text{-th row} \\ \\ \\ \\ \\ \\ \end{array}, \tag{25}$$

where all the $*$'s in the $(j+1)$-th row of $\boldsymbol{M}_{l,l}$ can be chosen independently. Thus, the subspace dimension is $\left\lfloor \frac{r-1}{2} \right\rfloor$, because each of the $\left\lfloor \frac{r+1}{2} \right\rfloor$ odd entries of the $(j+1)$-th column of $\boldsymbol{M}_{l,l}$ is a $*$, with the exception of the $(j+1, j+1)$ entry, which is 0.

If $\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})$ is a Goppa code $\mathscr{G}(\boldsymbol{x},\Gamma)$, we consider instead the matrix subspace originated by choosing all the matrices corresponding to (24) for a fixed l and such that one between a or b equals a fixed value j. Any matrix $\boldsymbol{M}$ in this subspace is null outside the union of the $(lr+j+1)$-th column and the $(lr+j+1)$-th row. Its rank is therefore upper bounded by 2. In other words, any such matrix $\boldsymbol{M}$ has the following shape

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{0} & & & \\ & \ddots & & \mathbf{0} \\ & & \boldsymbol{M}_{l,l} & \\ & \mathbf{0} & & \ddots \\ & & & \mathbf{0} \end{bmatrix}, \quad \text{with} \quad \boldsymbol{M}_{l,l} = \left[\begin{array}{cccccccc} \mathbf{0} & & * & & \mathbf{0} & & & \\ & & * & & & & & \\ * & * & 0 & * & * & * & * & * \\ & & * & & & & & \\ & & * & & & & & \\ \mathbf{0} & & * & & \mathbf{0} & & & \\ & & * & & & & & \\ & & * & & & & & \end{array}\right] \begin{array}{l} \\ \\ \leftarrow (j+1)\text{-th row} \\ \\ \\ \\ \\ \\ \end{array}, \tag{26}$$

where all the $*$'s in the $(j+1)$-th row of $\boldsymbol{M}_{l,l}$ can be chosen independently. Thus, the subspace dimension is $r - 1$, because each of the r entries of the $(j + 1)$-th column of $\boldsymbol{M}_{l,l}$ is a $*$, with the exception of the $(j+1, j+1)$ entry, which is 0. □

We will prove now Proposition 7 that we recall here

Proposition 7. *Let $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ be an alternant code in characteristic* 2 *and extension degree m. The matrix code of quadratic relationships $\mathscr{C}_{mat}$ contains at least $\Omega(m(q^{m(r-2)})$ matrices of rank 2.*

Proof. It directly follows from Lemmas 2 and 3 that we will give below. □

To understand what is going on in this case, it is insightful to have a look at some examples first. Let us fix a value $l = u \in \llbracket 0, m-1 \rrbracket$ and consider the subspace of $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ spanned by all the matrices corresponding to a quadratic relation

$$(\boldsymbol{x}^a\boldsymbol{y})^{q^l} \star (\boldsymbol{x}^b\boldsymbol{y})^{q^l} = (\boldsymbol{x}^c\boldsymbol{y})^{q^l} \star (\boldsymbol{x}^c\boldsymbol{y})^{q^l},$$

for any possible choice of $r-1 \geqslant a > c \geqslant d > b \geqslant 0$. It follows from the analysis of the distinguisher in [FGO$^+$13] and [MT22] that this space has dimension $\binom{r-1}{2}$. Let $\boldsymbol{M}_{l,l}(\boldsymbol{u})$ be the generic diagonal block matrix of such subspace, where $\boldsymbol{u} = (u_1, \ldots, u_{\binom{r-1}{2}})$ is the vector of coefficients with respect to the basis. We give examples for some small values of r.

Example 1. – For $r = 3$:

$$\boldsymbol{M}_{l,l}(\boldsymbol{u}) = \begin{bmatrix} 0 & 0 & u_1 \\ 0 & 0 & 0 \\ u_1 & 0 & 0 \end{bmatrix}.$$

– For $r = 4$:

$$\boldsymbol{M}_{l,l}(\boldsymbol{u}) = \begin{bmatrix} 0 & 0 & u_1 & u_2 \\ 0 & 0 & u_2 & u_3 \\ u_1 & u_2 & 0 & 0 \\ u_2 & u_3 & 0 & 0 \end{bmatrix}.$$

– For $r = 5$:

$$\boldsymbol{M}_{l,l}(\boldsymbol{u}) = \begin{bmatrix} 0 & 0 & u_1 & u_2 & u_4 \\ 0 & 0 & u_2 & u_3 & u_5 \\ u_1 & u_2 & 0 & u_5 & u_6 \\ u_2 & u_3 & u_5 & 0 & 0 \\ u_4 & u_5 & u_6 & 0 & 0 \end{bmatrix}.$$

– For $r = 6$:

$$\boldsymbol{M}_{l,l}(\boldsymbol{u}) = \begin{bmatrix} 0 & 0 & u_1 & u_2 & u_4 & u_7 \\ 0 & 0 & u_2 & u_3 & u_5 + u_7 & u_8 \\ u_1 & u_2 & 0 & u_5 & u_6 & u_9 \\ u_2 & u_3 & u_5 & 0 & u_9 & u_{10} \\ u_4 & u_5 + u_7 & u_6 & u_9 & 0 & 0 \\ u_7 & u_8 & u_9 & u_{10} & 0 & 0 \end{bmatrix}.$$

Size $r \times r$	3	4	5	6	7	8
n. of rank 2 matrices	$q^m - 1$	$q^{2m} - 1$	$2q^{3m} - q^{2m} - 1$	$2q^{4m} - q^{2m} - 1$	$3q^{5m} - q^{4m} - q^{2m} - 1$	$3q^{6m} - q^{5m} - q^{2m} - 1$

Table 4. Number of rank-2 block matrices

Table 4 illustrates the experimental number of rank 2 matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ such that $\mathbf{Rank}(M_{1,1}) = 2$ and all the other blocks are null, for small values of r and over the field $\mathbb{F}_{q^m}$.

Table 4 suggests that these blocks have a number of rank 2 specializations that roughly grows as $\left\lfloor \frac{r-1}{2} \right\rfloor (q^m)^{r-2}$. We are now going to show the shape of a number of rank-2 matrices in the order of $(q^m)^{r-2}$. Despite not being all the rank-2 matrices, this is interesting in order to determine the dimension of the variety corresponding to a determinantal ideal, which indeed can be proved to be at least $r-2$. The explanation can be split into odd and even matrix sizes.

From the matrices $\boldsymbol{M}_{l,l}(\boldsymbol{u})$ with odd size $r \times r$, by specializing some of the $\boldsymbol{u}$ variables and selecting some row/column indexes, we can determine submatrices of size $\lceil r/2 \rceil \times \lceil r/2 \rceil$ that are skew-symmetric but without any other additional relation. Again, we first give examples for some small values of r.

Example 2. – For $r = 3$, the submatrix obtained by taking row/column indexes in $\{1, 3\}$ is

$$\begin{bmatrix} 0 & u_1 \\ u_1 & 0 \end{bmatrix}.$$

– For $r = 5$, the submatrix obtained by taking row/column indexes in $\{1, 3, 5\}$ is

$$\begin{bmatrix} 0 & u_1 & u_4 \\ u_1 & 0 & u_6 \\ u_4 & u_6 & 0 \end{bmatrix}.$$

More generally, it is enough to build the $\lceil r/2 \rceil \times \lceil r/2 \rceil = \frac{r+1}{2} \times \frac{r+1}{2}$ submatrix selecting the odd row/column indexes. By specializing all the u_i's not appearing in the submatrix, this gives a lower bound on the number of matrices of rank 2. In particular

Lemma 2. *The number of choices of* $\boldsymbol{u}$ *for which* $\boldsymbol{M}_{l,l}(\boldsymbol{u})$ *(r odd) has rank 2 is lower bounded by* $N_0\left(\frac{r+1}{2}, 2\right)$.

Since

$$N_0\left(\frac{r+1}{2}, 2\right) = (q^m)^{2\frac{r+1}{2}-3} + o((q^m)^{2\frac{r+1}{2}-3}) = q^{m(r-2)} + o(q^{m(r-2)}),$$

and we have m blocks, we expect that the number of solutions is at least in the order of $mq^{m(r-2)}$. Analogously for $\boldsymbol{M}_{l,l}(\boldsymbol{u})$ matrices with even size, we do not construct generic skew-symmetric submatrices but we provide specializations of $\boldsymbol{M}_{l,l}(\boldsymbol{u})$ related to such submatrices. We first give the examples for some small values of r.

Example 3. – For $r = 4$:

$$\begin{bmatrix} 0 & 0 & u_1 & \lambda u_1 \\ 0 & 0 & \lambda u_1 & \lambda^2 u_1 \\ u_1 & \lambda u_1 & 0 & 0 \\ \lambda u_1 & \lambda^2 u_1 & 0 & 0 \end{bmatrix}.$$

– For $r = 6$:

$$\begin{bmatrix} 0 & 0 & u_1 & \lambda u_1 & u_4 & \lambda u_4 \\ 0 & 0 & \lambda u_1 & \lambda^2 u_1 & \lambda u_4 & \lambda^2 u_4 \\ u_1 & \lambda u_1 & 0 & 0 & u_6 & \lambda u_6 \\ \lambda u_1 & \lambda^2 u_1 & 0 & 0 & \lambda u_6 & \lambda^2 u_6 \\ u_4 & \lambda u_4 & u_6 & \lambda u_6 & 0 & 0 \\ \lambda u_4 & \lambda^2 u_4 & \lambda u_6 & \lambda^2 u_6 & 0 & 0 \end{bmatrix}.$$

More generally we can replace each entry u_i of a generic anti-symmetric matrix of size $\frac{r}{2} \times \frac{r}{2}$ with the 2×2 block $\begin{bmatrix} u_i & \lambda u_i \\ \lambda u_i & \lambda^2 u_i \end{bmatrix}$ and each null element of the diagonal with the null 2×2 block. It is clear that if the starting $\frac{r}{2} \times \frac{r}{2}$ matrix has rank 2, then the same occurs for the $r \times r$ block matrix. Moreover, the variable λ adds one degree of freedom. Hence we have

Lemma 3. *The number of choices for u_i's such that the specialized $r \times r$ matrix $W^{(\boldsymbol{u})}$ (r even) has rank 2 is lower bounded by $q^m \cdot N_0(\frac{r}{2}, 2)$.*

Since

$$q^m \cdot N_0\left(\frac{r}{2}, 2\right) = (q^m) \cdot (q^m)^{2\frac{r}{2}-3} + o((q^m) \cdot (q^m)^{2\frac{r}{2}-3}) = q^{m(r-2)} + o(q^{m(r-2)}),$$

and we have m blocks, we have proved that the number of rank-2 matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ is again at least in the order of $mq^{m(r-2)}$.

We are now going to prove a refinement of this counting for binary Goppa codes

Proposition 8. *Let $\mathscr{G}(\boldsymbol{x}, \Gamma)$ be a binary Goppa code of extension degree m with Γ a square-free polynomial of degree r. Then $\mathscr{C}_{mat}$ contains at least*

$$m\frac{(q^{mr} - 1)(q^{m(r-1)} - 1)}{q^{2m} - 1}$$

matrices of rank 2.

Proof. We have seen that each choice of (a, b, l) from (24) leads to a different matrix $\boldsymbol{M}$ in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ which is null outside the diagonal block $\boldsymbol{M}_{l,l}$ and such that $\mathbf{Rank}(\boldsymbol{M}) = \mathbf{Rank}(\boldsymbol{M}_{l,l}) = 2$. Furthermore, the block submatrix $\boldsymbol{M}_{l,l}$ is such that only one element below the diagonal is nonzero, *i.e.* the entry $(a+1, b+1)$. Hence the set over all possible choices of (a, b, l) of these matrices generates the full subspace of skew-symmetric block diagonal matrices. Therefore, by counting the rank-2 matrices in this subspace, the number of rank-2 matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ can be lower bounded by

$$mN_0(r,2) = m\frac{(q^{mr}-1)(q^{m(r-1)}-1)}{q^{2m}-1}.$$

□

C.2 Proof of Proposition 10

Let us first recall this proposition.

Proposition 10. *Let $\mathscr{R} \subset \mathbb{F}_{q^m}^n$ be a random code of dimension rm with basis $\mathcal{R}$ and let $\binom{rm+1}{2} > n$. Under the assumption that $\mathscr{C}_{mat}(\mathcal{R})$ behaves as a random linear code concerning the rank weight distribution, it contains matrices or rank $\leqslant d$ with non-negligible probability iff*

$$n \leqslant drm - \binom{d}{2} \qquad \textit{(symmetric case)}$$

$$n \leqslant (2\lfloor d/2\rfloor + 1)rm - \binom{2\lfloor d/2\rfloor + 1}{2} \qquad \textit{(skew-symmetric case)}$$

For this proof, we will need the following results giving the number of symmetric/skew-symmetric matrices of a given rank. The number of symmetric matrices over a finite field of a given rank can be found in [Mas69].

Proposition 26. *[Mas69, Theorem 2] Let $N(t,r)$ denote the number of symmetric matrices of size $t \times t$, rank r, with entries in $\mathbb{F}_q$. Then*

$$N(t,2s) = \prod_{i=1}^{s} \frac{q^{2i}}{q^{2i}-1} \prod_{i=0}^{2s-1}(q^{t-i}-1), \quad 2s \leqslant t$$

$$N(t,2s+1) = \prod_{i=1}^{s} \frac{q^{2i}}{q^{2i}-1} \prod_{i=0}^{2s}(q^{t-i}-1), \quad 2s+1 \leqslant t.$$

When the field characteristic is 2, the number of skew-symmetric matrices has also been computed.

Proposition 27. *[Mas69, Theorem 3] Let $N_0(t,r)$ denote the number of symmetric matrices of size $t \times t$, rank r, with entries in $\mathbb{F}_q$, $q = 2^n$, and 0 on the main diagonal. Then*

$$N_0(t,2s) = \prod_{i=1}^{s} \frac{q^{2i-2}}{q^{2i}-1} \prod_{i=0}^{2s-1}(q^{t-i}-1), \quad 2s \leqslant t$$

$$N_0(t,2s+1) = 0.$$

Remark 4. Proposition 27 implies that skew-symmetric matrices defined over a field of characteristic 2 have always even rank.

We are ready now to give a proof of Proposition 10.

Proof (of Proposition 10). For a random code $\mathscr{R}$ with basis $\mathcal{R}$, $\dim(\mathscr{C}_{\text{mat}}(\mathcal{R})) = \binom{rm+1}{2} - n$ is expected with probability $1 - o(1)$ when $\binom{rm+1}{2} > n$ [CCMZ15]. From Propositions 26,27 we have respectively

$$\begin{aligned}
|B_d^{(\mathbf{Sym})}| \sim & N(rm, d) \\
= & \prod_{i=1}^{\lfloor d/2 \rfloor} \frac{(q^m)^{2i}}{(q^m)^{2i} - 1} \prod_{i=0}^{d-1} ((q^m)^{rm-i} - 1) \\
\sim & \prod_{i=0}^{d-1} (q^m)^{rm-i} \\
= & (q^m)^{drm - \binom{d}{2}}.
\end{aligned}$$

and (in characteristic 2)

$$\begin{aligned}
|B_d^{(\mathbf{Skew})}| \sim & N_0(rm, 2\lfloor d/2 \rfloor) \\
= & \prod_{i=1}^{\lfloor d/2 \rfloor} \frac{(q^m)^{2i-2}}{(q^m)^{2i} - 1} \prod_{i=0}^{2\lfloor d/2 \rfloor - 1} ((q^m)^{rm-i} - 1) \\
\sim & (q^m)^{-2\lfloor d/2 \rfloor} \prod_{i=0}^{d-1} (q^m)^{rm-i} \\
= & (q^m)^{2\lfloor d/2 \rfloor rm - \binom{2\lfloor d/2 \rfloor + 1}{2}}.
\end{aligned}$$

Therefore, from Gilbert-Varshamov bounds (13),(14) we get that rank-d matrices belong to $\mathscr{C}_{\text{mat}}(\mathcal{R})$ with non negligible probability iff

- (for symmetric matrices)

$$\begin{aligned}
& (q^m)^{\binom{rm+1}{2} - n} (q^m)^{drm - \binom{d}{2}} \geqslant (q^m)^{\binom{rm+1}{2}} \\
\iff & \binom{rm+1}{2} - n + drm - \binom{d}{2} \geqslant \binom{rm+1}{2} \\
\iff & n \leqslant drm - \binom{d}{2}.
\end{aligned}$$

- (for skew-symmetric matrices in characteristic 2)

$$\begin{aligned}
& (q^m)^{\binom{rm+1}{2} - n} (q^m)^{2\lfloor d/2 \rfloor - \binom{2\lfloor d/2 \rfloor + 1}{2}} \geqslant (q^m)^{\binom{rm}{2}} \\
\iff & \binom{rm+1}{2} - n + 2\lfloor d/2 \rfloor rm - \binom{2\lfloor d/2 \rfloor + 1}{2} \geqslant \binom{rm}{2} \\
\iff & n \leqslant (2\lfloor d/2 \rfloor + 1) rm - \binom{2\lfloor d/2 \rfloor + 1}{2}.
\end{aligned}$$

□

D Proofs and experimental evidence corresponding to Section 5

D.1 Experiments about the Hilbert function convergence

In Conjecture 2, we claimed that $d_0 \sim c\frac{s^2}{k}$ for some constant c. We experimentally verified this in the following way. We define $k = \lfloor \beta s^\alpha \rfloor$ for several positive values of β and $\alpha \in (1, 2)$. We start from a value $s = 2^i$ such that the parameters are above Gilbert-Varshamov bound and not distinguishable and then we let s double each time and update k accordingly. The ratio $\frac{d_0 k}{s^2}$ is eventually a decreasing function and seems to converge to $c = \frac{1}{4}$ (or something very close to it) from above, even though with a different speed depending on α. In particular, let us choose $\beta = 1$ and let us test the convergence for different vaules of α in Table 5.

α	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9
$\frac{d_0 k}{s^2} < 0.28$ starting from	$s = 2^{18}$	$s = 2^{14}$	$s = 2^{14}$	$s = 2^{15}$	$s = 2^{18}$	$s = 2^{24}$	$s = 2^{36}$	$s = 2^{72}$
$\frac{d_0 k}{s^2} < 0.255$ starting from		$s = 2^{21}$	$s = 2^{20}$	$s = 2^{23}$	$s = 2^{29}$	$s = 2^{38}$	$s = 2^{57}$	$s = 2^{114}$
$\frac{d_0 k}{s^2} < 0.252$ starting from			$s = 2^{23}$	$s = 2^{28}$	$s = 2^{34}$	$s = 2^{45}$	$s = 2^{67}$	$s = 2^{133}$
$\frac{d_0 k}{s^2} < 0.251$ starting from					$s = 2^{37}$	$s = 2^{50}$		

Table 5. Experiments for the convergence of the Hilbert function

D.2 Proof of Proposition 2

Let us first recall the Proposition.

Proposition 17. *Let $\mathscr{C}_{mat}$ be the matrix code of quadratic relationships corresponding to the extended dual of an $[n, n - rm]$ alternant code over a field of even characteristic. Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the corresponding Pfaffian ideal. Then* $\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M})) \geqslant r - 2$.

Proof. We recall from Proposition 14 that the dimension of the variety of the generic Pfaffian ideal $\mathcal{P}_2(\boldsymbol{M})$ is $2s - 3$, where s is the matrix size. The result follows from the construction given in Appendix §C.1, for estimating the number of rank 2 matrices, where we have shown that $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ contains subspaces of matrices that are isomorphic to the full space of skew-symmetric matrices for some smaller size. This allows to lower bound $\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M}))$ in terms of $\dim \boldsymbol{V}(\mathcal{P}_2(\boldsymbol{N}))$, where $\boldsymbol{N}$ is the generic skew-symmetric matrix of smaller size. More precisely:

- if r is odd: let $\boldsymbol{N}$ be the generic skew-symmetric matrix of size $\frac{r+1}{2} \times \frac{r+1}{2}$. Then the construction explained before Lemma 2 in Appendix §C.1 implies that
$$\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M})) \geqslant \dim \boldsymbol{V}(\mathcal{P}_2(\boldsymbol{N})) = 2\frac{r+1}{2} - 3 = r - 2;$$

– if r is even: this is the most subtle case, because we do not construct generic skew-symmetric matrices. Let $\boldsymbol{N}$ be the generic skew-symmetric matrix of size $\frac{r}{2} \times \frac{r}{2}$ and $\boldsymbol{N}'$ be the skew-symmetric matrix of size $r \times r$ with indeterminates given as in the construction explained before Lemma 3 in Appendix §C.1. We identify $n_{i,j} = n'_{2i-1,2j-1}$ and define the function $f(i) = \begin{cases} 0 & i \text{ odd} \\ 1 & i \text{ even} \end{cases}$. Using the ideintification above, we can rewrite the generators of the Pfaffian ideal for $\boldsymbol{N}'$ in function of $n_{i,j}$'s and λ. If i, j, k, l are such that there are not two consecutive indexes with the smallest being odd, then

$$\begin{aligned} & n'_{i,j}n'_{k,l} + n'_{i,k}n'_{j,l} + n'_{i,l}n'_{j,k} \\ =& \lambda^{f(i)+f(j)} n_{\lceil \frac{i}{2} \rceil, \lceil \frac{j}{2} \rceil} \lambda^{f(k)+f(l)} n_{\lceil \frac{k}{2} \rceil, \lceil \frac{l}{2} \rceil} + \lambda^{f(i)+f(k)} n_{\lceil \frac{i}{2} \rceil, \lceil \frac{k}{2} \rceil} \lambda^{f(j)+f(l)} n_{\lceil \frac{j}{2} \rceil, \lceil \frac{l}{2} \rceil} \\ & + \lambda^{f(i)+f(l)} n_{\lceil \frac{i}{2} \rceil, \lceil \frac{l}{2} \rceil} \lambda^{f(j)+f(k)} n_{\lceil \frac{j}{2} \rceil, \lceil \frac{k}{2} \rceil} \\ =& \lambda^{f(i)+f(j)+f(k)+f(l)} (n_{\lceil \frac{i}{2} \rceil, \lceil \frac{j}{2} \rceil} n_{\lceil \frac{k}{2} \rceil, \lceil \frac{l}{2} \rceil} + n_{\lceil \frac{i}{2} \rceil, \lceil \frac{k}{2} \rceil} n_{\lceil \frac{j}{2} \rceil, \lceil \frac{l}{2} \rceil} + n_{\lceil \frac{i}{2} \rceil, \lceil \frac{l}{2} \rceil} n_{\lceil \frac{j}{2} \rceil, \lceil \frac{k}{2} \rceil}). \end{aligned}$$

Otherwise, if for instance $j = i+1$, i odd, then

$$n'_{i,j}n'_{k,l} + n'_{i,k}n'_{j,l} + n'_{i,l}n'_{j,k} = 0 \cdot n'_{k,l} + n'_{i,k}(\lambda n'_{i,l}) + n'_{i,l}(\lambda n'_{i,k}) = 0$$

Therefore $\mathcal{P}_2(\boldsymbol{N}') = \mathcal{P}_2(\boldsymbol{N})$ seen as ideals in $\mathbb{F}_{q^m}[(n_{i,j})_{i,j}, \lambda]$. Hence

$$\dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{M})) \geqslant \dim \boldsymbol{V}(\mathcal{P}_2^+(\boldsymbol{N})') = 1 + \dim \boldsymbol{V}(\mathcal{P}_2(\boldsymbol{N})) = 1 + 2\frac{r}{2} - 3 = r - 2,$$

where the summand 1 corresponds to the free parameter λ used in the construction.

□

D.3 Proof of Theorem 2

Let us first recall the Theorem.

Theorem 2 *Let $\mathscr{G}(\boldsymbol{x}, \Gamma)$ be a non distinguishable binary $[n, k = n - rm]$ Goppa code with Γ a square-free polynomial of degree r and extension degree m. Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the corresponding Pfaffian ideal. Then, for all $d > 0$,*

$$HF_{\mathbb{F}_{2^m}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) \geqslant m \left(\binom{r+d-2}{d}^2 - \binom{r+d-2}{d+1}\binom{r+d-2}{d-1} \right).$$

Proof. For our convenience we denote $R \overset{\text{def}}{=} \mathbb{F}_{2^m}[\boldsymbol{m}]$. Define $\boldsymbol{m}^{(l)} \overset{\text{def}}{=} (m_{i,j})_{lr+1 \leqslant i < j \leqslant (l+1)r}$ and $\boldsymbol{m}^{(\setminus l)}$ the sequence of monomials that are in $\boldsymbol{m}$ but not in $\boldsymbol{m}^{(l)}$, for all $l \in [\![0, m-1]\!]$. Moreover, we define the sequence of variables $\boldsymbol{m}^{(out)}$ that are not in any of the $\boldsymbol{m}^{(l)}$'s. We consider the corresponding polynomial rings $R_l \overset{\text{def}}{=}$

$\mathbb{F}_{2^m}[\boldsymbol{m}^{(l)}]$, $R_{\backslash l} \overset{\text{def}}{=} \mathbb{F}_{2^m}[\boldsymbol{m}^{(\backslash l)}]$ and $R_{out} \overset{\text{def}}{=} \mathbb{F}_{2^m}[\boldsymbol{m}^{(out)}]$ and, with some abuse of notation, the monomial ideals over $\mathbb{F}_{2^m}[\boldsymbol{m}]$ generated by these sequences of variables: $\mathcal{I}^{(l)} = \mathcal{I}(\boldsymbol{m}^{(l)}), \mathcal{I}^{(\backslash l)} = \mathcal{I}(\boldsymbol{m}^{(\backslash l)}), \mathcal{I}^{(out)} = \mathcal{I}(\boldsymbol{m}^{(out)})$. Finally, we define the monomial ideal $\mathcal{I}^{(quad)}$ generated by all possible quadratic monomials with two unknowns belonging to two different diagonal blocks. We recall from Proposition 9 that each skew-symmetric block diagonal matrix belongs to $\mathscr{C}_{\text{mat}}(\mathcal{A})$. Therefore, the homogeneous linear relationships L_i's such that $\mathcal{P}_2^+(\boldsymbol{M}) = \mathcal{P}_2(\boldsymbol{M}) + \langle L_i \rangle_i$ can be chosen in such a way that only the variables in $\boldsymbol{m}^{(out)}$ can appear in them, *i.e.* $L_j \in \mathcal{I}^{(out)}$.

Let us take an element in the basis of $\mathcal{P}_2(\boldsymbol{M})$ as in (16):

$$Q_{a,b,c,d} = m_{a,b}m_{c,d} + m_{a,c}m_{b,d} + m_{a,d}m_{b,c}.$$

We analyze two cases:

- If there exists $l \in [\![0, m-1]\!]$ such that $lr + 1 \leqslant a < b < c < d \leqslant (l+1)r$, then $Q_{a,b,c,d} \in \mathcal{P}_2(\boldsymbol{M}_{l,l})$, *i.e.* the Pfaffian ideal corresponding to the $(l+1)$-th diagonal block submatrix.
- Otherwise, the monomials $m_{a,b}m_{c,d}, m_{a,c}m_{b,d}$ and $m_{a,d}m_{b,c}$ belong to either $\mathcal{I}^{(out)}$ or $\mathcal{I}^{(quad)}$.

In both cases we obtain

$$Q_{a,b,c,d} \in \left(\sum_{i=0}^{m-1} \mathcal{P}_2(\boldsymbol{M}_{l,l}) \right) + \mathcal{I}^{(out)} + \mathcal{I}^{(quad)}.$$

Hence

$$\mathcal{P}_2^+(\boldsymbol{M}) = \mathcal{P}_2(\boldsymbol{M}) + \langle L_1, \ldots, L_k \rangle \subseteq \left(\sum_{l=0}^{m-1} \mathcal{P}_2(\boldsymbol{M}_{l,l}) \right) + \mathcal{I}^{(out)} + \mathcal{I}^{(quad)}.$$

One can readily verify that, for any $l \in [\![0, m-1]\!]$, the monomial ideal $\mathcal{I}^{(\backslash l)}$ contains:

- $\mathcal{I}^{(out)}$;
- $\mathcal{I}^{(quad)}$;
- $\mathcal{P}_2(\boldsymbol{M}_{l',l'})$, for all $l' \in [\![0, m-1]\!] \backslash \{l\}$.

This results in

$$\left(\sum_{l=0}^{m-1} \mathcal{P}_2(\boldsymbol{M}_{l,l}) \right) + \mathcal{I}^{(out)} + \mathcal{I}^{(quad)} \subseteq \bigcap_{l \in [\![0,m-1]\!]} \left(\mathcal{P}_2(\boldsymbol{M}_{l,l}) + \mathcal{I}^{(\backslash l)} \right).$$

Note now that, for any $\bar{l} \in [\![1, m-1]\!]$,

$$\bigcap_{l \in [\![0,\bar{l}-1]\!]} \left(\mathcal{P}_2(\boldsymbol{M}_{l,l}) + \mathcal{I}^{(\backslash l)} \right) + \mathcal{P}_2(\boldsymbol{M}_{\bar{l},\bar{l}}) + \mathcal{I}^{(\backslash \bar{l})} = \langle \boldsymbol{m} \rangle \qquad (27)$$

and

$$HS_{R/\langle \boldsymbol{m} \rangle}(z) = HS_{\mathbb{F}_{2^m}}(z) = 1.$$

By applying recursively relation (27) on the quotient rings, we obtain

$$\begin{aligned}
HF_{R/\mathcal{P}_2^+(\boldsymbol{M})}(d) \geqslant & HF_{R/\bigcap_{l \in [\![0,m-1]\!]}\left(\mathcal{P}_2(\boldsymbol{M}_{l,l})+\mathcal{I}^{(\backslash l)}\right)}(d) \\
= & HF_{R/\bigcap_{l \in [\![0,m-2]\!]}\left(\mathcal{P}_2(\boldsymbol{M}_{l,l})+\mathcal{I}^{(\backslash l)}\right)}(d) + HF_{R/\left(\mathcal{P}_2(\boldsymbol{M}_{m-1,m-1})+\mathcal{I}^{(\backslash m-1)}\right)}(d) - HF_{\mathbb{F}_{2^m}}(d) \\
= & HF_{R/\bigcap_{l \in [\![0,m-3]\!]}\left(\mathcal{P}_2(\boldsymbol{M}_{l,l})+\mathcal{I}^{(\backslash l)}\right)}(d) + HF_{R/\left(\mathcal{P}_2(\boldsymbol{M}_{m-2,m-2})+\mathcal{I}^{(\backslash m-2)}\right)}(d) \\
& + HF_{R/\left(\mathcal{P}_2(\boldsymbol{M}_{m-1,m-1})+\mathcal{I}^{(\backslash m-1)}\right)}(d) - 2HF_{\mathbb{F}_{2^m}}(d) \\
= & \dots \\
= & \sum_{l=0}^{m-1} HF_{R/\left(\mathcal{P}_2(\boldsymbol{M}_{l,l})+\mathcal{I}^{(\backslash l)}\right)}(d) - (m-1)HF_{\mathbb{F}_{2^m}}(d) \\
= & \sum_{l=0}^{m-1} HF_{R_l/\mathcal{P}_2(\boldsymbol{M}_{l,l})}(d) - (m-1)HF_{\mathbb{F}_{2^m}}(d) \\
= & \begin{cases} m-(m-1) = 1 & \text{if } d = 0 \\ m\left(\binom{r+d-2}{d}^2 - \binom{r+d-2}{d+1}\binom{r+d-2}{d-1}\right) & \text{if } d > 0 \end{cases}.
\end{aligned}$$

□

E Proofs for some of the Results of Section 6

E.1 Proof of Proposition 20

Let us recall first the proposition

Proposition 20. *Whenever a basis $\mathcal{B}$ has the form given in* (19)*, $\mathscr{C}_{mat}(\mathcal{B})$ is stable by the operation*

$$\boldsymbol{M} \longmapsto \boldsymbol{S}^\intercal \boldsymbol{M}^{(q)} \boldsymbol{S}.$$

Proof. Let $\boldsymbol{B} = (b_{i,j})_{i,j} \in \mathscr{C}_{\text{mat}}(\mathcal{B}) \subseteq \mathbb{F}_{q^m}^{rm \times rm}$. Then, by definition,

$$\sum_{i<j} 2b_{i,j}\boldsymbol{b}_i \star \boldsymbol{b}_j + \sum_i b_{i,i}\boldsymbol{b}_i \star \boldsymbol{b}_i = 0.$$

Then, by applying the Frobenius map $z \mapsto z^q$ component-wise,

$$0 = \sum_{i<j} 2^q b_{i,j}^q \boldsymbol{b}_i^q \star \boldsymbol{b}_j^q + \sum_i b_{i,i}^q \boldsymbol{b}_i^q \star \boldsymbol{b}_i^q = \sum_{i<j} 2b_{i,j}^q \boldsymbol{b}_i^q \star \boldsymbol{b}_j^q + \sum_i b_{i,i}^q \boldsymbol{b}_i^q \star \boldsymbol{b}_i^q.$$

From now on, the indexes are considered modulo rm. The structure of the basis $\mathcal{B}$ yields

$$\sum_{i<j} 2b_{i,j}^q \boldsymbol{b}_{i+r}^q \star \boldsymbol{b}_{j+r}^q + \sum_i b_{i,i}^q \boldsymbol{b}_{i+r}^q \star \boldsymbol{b}_{i+r}^q = 0$$

and hence

$$\sum_{i<j} 2b^q_{i-r,j-r}\boldsymbol{b}^q_i \star \boldsymbol{b}^q_j + \sum_i b^q_{i-r,i-r}\boldsymbol{b}^q_i \star \boldsymbol{b}^q_i = 0$$

The matrix $(b^q_{i-r,j-r})_{i,j}$ is nothing but $\boldsymbol{S}^\intercal \boldsymbol{B}^{(q)}\boldsymbol{S}$ and hence $\boldsymbol{S}^\intercal \boldsymbol{B}^{(q)}\boldsymbol{S} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$. □

E.2 Proof of Proposition 21

Let us recall this proposition

Proposition 21. *Let $\boldsymbol{v}$ be in the kernel of a matrix $\boldsymbol{B}$ in $\mathscr{C}_{mat}(\mathcal{B})$ of rank $rm-1$. Then $\boldsymbol{v}^q\boldsymbol{S}, \dots, \boldsymbol{v}^{q^{m-1}}\boldsymbol{S}^{m-1}$ are $m-1$ elements that are also kernel elements of matrices in $\mathscr{C}_{mat}(\mathcal{B})$ of rank $rm-1$ which are respectively $\boldsymbol{S}^\intercal\boldsymbol{B}^{(q)}\boldsymbol{S}, \cdots,$ $(\boldsymbol{S}^\intercal)^{m-1}\boldsymbol{B}^{(q^{m-1})}\boldsymbol{S}^{m-1}$.*

Proof. Given $\boldsymbol{B} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$, it follows from Proposition 20 that

$$(\boldsymbol{S}^\intercal)^i\boldsymbol{B}^{(q^i)}(\boldsymbol{S})^i \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B}), \quad \text{for any } i \in [\![0, m-1]\!]$$

and all these matrices have the same rank, namely $rm-1$. Moreover, if $\boldsymbol{v}$ generates the nullspace of $\boldsymbol{B}$, then $\boldsymbol{v}^{q^i}\boldsymbol{S}^i$ is in the kernel of $(\boldsymbol{S}^\intercal)^i\boldsymbol{B}^{(q^i)}\boldsymbol{S}^i$ since

$$\begin{aligned}&(\boldsymbol{v}^{q^i}\boldsymbol{S}^i)\cdot(\boldsymbol{S}^\intercal)^i\boldsymbol{B}^{(q^i)}\boldsymbol{S}^i\\ =&\boldsymbol{v}^{q^i}\boldsymbol{B}^{(q^i)}\boldsymbol{S}^i\\ =&(\boldsymbol{v}\boldsymbol{B})^{(q^i)}\boldsymbol{S}^i\\ =&0.\end{aligned}$$

□

E.3 Proof of Proposition 22

The proposition states that

Proposition 22. *Let $\mathcal{A}, \mathcal{B}$ be the two basis introduced before and $\boldsymbol{P}$ the change of basis, i.e. $\boldsymbol{H}_{\mathcal{B}} = \boldsymbol{P}\boldsymbol{H}_{\mathcal{A}}$. Let $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{F}_{q^m}^{rm}$ be two vectors such that*

$$\boldsymbol{u}_t(\boldsymbol{P}^{-1})^\intercal\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} \in \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^{j_t})}$$

for some values $j_t \in [\![0, m-1]\!]$. There exists a unique $l \in [\![0, m-1]\!]$ such that $\boldsymbol{u}_1$ and $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ correspond to the same GRS code.

Proof. Let $\boldsymbol{B} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ such that $\boldsymbol{u}_2$ generates $\ker(\boldsymbol{B})$. By Proposition 21, we know that $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ generates the kernel of $(\boldsymbol{S}^\intercal)^l\boldsymbol{B}^{(q^l)}\boldsymbol{S}^l$. We get

$$\begin{aligned}
0 =& \boldsymbol{u}_2^{q^l}\boldsymbol{B}^{(q^l)}\\
=& \boldsymbol{u}_2^{q^l}(\boldsymbol{P}^{(q^l)^\intercal})^{-1}\boldsymbol{A}^{(q^l)}(\boldsymbol{P}^{(q^l)})^{-1}\\
=& \boldsymbol{u}_2^{q^l}(\boldsymbol{P}^{(q^l)^\intercal})^{-1}(\boldsymbol{S}^l(\boldsymbol{S}^\intercal)^l)\boldsymbol{A}^{(q^l)}(\boldsymbol{S}^l(\boldsymbol{S}^\intercal)^l)(\boldsymbol{P}^{(q^l)})^{-1}\\
=& (\boldsymbol{u}_2^{q^l}(\boldsymbol{P}^{(q^l)^\intercal})^{-1}\boldsymbol{S}^l)((\boldsymbol{S}^\intercal)^l\boldsymbol{A}^{(q^l)}\boldsymbol{S}^l)(\boldsymbol{S}^\intercal)^l(\boldsymbol{P}^{(q^l)})^{-1}\\
=& (\boldsymbol{u}_2^{q^l}((\boldsymbol{S}^\intercal)^l\boldsymbol{P}^{(q^l)^\intercal})^{-1})((\boldsymbol{S}^\intercal)^l\boldsymbol{A}^{(q^l)}\boldsymbol{S}^l)(\boldsymbol{S}^\intercal)^l(\boldsymbol{P}^{(q^l)})^{-1} \quad \text{by Proposition 19}\\
=& (\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l\boldsymbol{P}^{\intercal-1})((\boldsymbol{S}^\intercal)^l\boldsymbol{A}^{(q^l)}\boldsymbol{S}^l)(\boldsymbol{S}^\intercal)^l(\boldsymbol{P}^{(q^l)})^{-1},
\end{aligned}$$

which implies

$$(\boldsymbol{u}_2^{q^l}\boldsymbol{S})\boldsymbol{P}^{\intercal-1}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} = (\boldsymbol{u}_2^{q^l}\boldsymbol{S}\boldsymbol{P}^{\intercal-1})\boldsymbol{H}_{\mathcal{A}} \in \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^{j_2+l})},$$

since the diagonal block of rank $r-1$ in $(\boldsymbol{S}^\intercal)^l\boldsymbol{A}^{(q^l)}\boldsymbol{S}^l$ is the one indexed by $j_2+l \mod m$. Therefore, $\boldsymbol{u}_1$ and $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ correspond to the same GRS code with respect to $\mathcal{B}$ for the unique value $l \in [\![0, m-1]\!]$ such that $j_1 = j_2 + l \mod m$. □

E.4 Proof of Proposition 23

This proposition says that

Proposition 23. *Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{r-1}, \boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{F}_{q^m}^{rm}$ be the generators of the kernels of $\boldsymbol{B}_1, \ldots, \boldsymbol{B}_{r-1}, \boldsymbol{B}', \boldsymbol{B}'' \in \mathscr{C}_{mat}(\mathcal{B})$ respectively, for randomly sampled matrices of rank $rm-1$. Define*

$$\mathscr{S}_{aux} \overset{def}{=} \left\langle \boldsymbol{v}_j^{q^l}\boldsymbol{S}^l \mid j \in [\![1, r-1]\!], l \in [\![0, m-1]\!] \right\rangle_{\mathbb{F}_{q^m}}.$$

If the following conditions are satisfied:

- $\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} = (r-1)m$ *(i.e. the $(r-1)m$ vectors that generate $\mathscr{S}_{aux}$ are linearly independent;*
- $\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \langle \boldsymbol{u}_t \rangle_{\mathbb{F}_{q^m}} = (r-1)m + 1, \quad t = 1, 2;$

then the two following statements are equivalent:

1. $\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \left\langle \boldsymbol{u}_1, \boldsymbol{u}_2^{q^l}\boldsymbol{S}^l \right\rangle_{\mathbb{F}_{q^m}} = (r-1)m + 1;$
2. *$\boldsymbol{u}_1$ and $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ correspond to the same GRS code with respect to $\mathcal{B}$.*

Proof. Let $j \in [\![0, r-1]\!]$. For each $i \in [\![0, m-1]\!]$, there exists a unique $\boldsymbol{v}_j^{(q^l)}\boldsymbol{S}^l$, $l \in [\![0, m-1]\!]$, such that

$$\boldsymbol{v}_j^{q^l}\boldsymbol{S}^l(\boldsymbol{P}^{-1})^\intercal\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} \subseteq \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^i)}.$$

As this holds for all $j \in [\![0, r-1]\!]$, we obtain that

$$\mathscr{S}_{aux}(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} = \sum_{i=0}^{m-1} \mathscr{G}_i,$$

where $\mathscr{G}_i$ is an $[n, r-1]$ linear code contained into $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$. From the standard assumption that all the codes $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$'s are in direct sum, we get $\mathscr{S}_{aux}(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} = \bigoplus_{i=0}^{m-1} \mathscr{G}_i$. Analogously for $\boldsymbol{u}_t$, $t = 1, 2$, we have

$$\boldsymbol{u}_t(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} \in \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_t})}.$$

The condition $\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \langle \boldsymbol{u}_t \rangle_{\mathbb{F}_{q^m}} = (r-1)m+1 = \dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + 1$ implies that

$$\left(\mathscr{S}_{aux} + \langle \boldsymbol{u}_t \rangle_{\mathbb{F}_{q^m}}\right)(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} = \left(\bigoplus_{i \in [\![0, m-1]\!] \setminus \{i_t\}} \mathscr{G}_i\right) \oplus \mathscr{G}'_{i_t},$$

with $\mathscr{G}'_{i_t} \subseteq \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_t})}$. But

$$\dim_{\mathbb{F}_{q^m}} \mathscr{G}'_{i_t} = \dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \langle \boldsymbol{u}_t \rangle_{\mathbb{F}_{q^m}} - \dim_{\mathbb{F}_{q^m}} \bigoplus_{i \in [\![0, m-1]\!] \setminus \{i_t\}} \mathscr{G}_i = (r-1)m+1-(r-1)(m-1) = r,$$

hence $\mathscr{G}'_{i_t} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_t})}$. Note that, with the same argument,

$$\begin{aligned}&\left(\mathscr{S}_{aux} + \left\langle \boldsymbol{u}_2^{q^l}\boldsymbol{S}^l \right\rangle_{\mathbb{F}_{q^m}}\right)(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}}\\ &= \left(\bigoplus_{i \in [\![0, m-1]\!] \setminus \{(i_2+l) \mod m\}} \mathscr{G}_i\right) \oplus \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_2+l})}.\end{aligned}$$

We can conclude that

$$\begin{aligned}&\left(\mathscr{S}_{aux} + \left\langle \boldsymbol{u}_1, \boldsymbol{u}_2^{q^l}\boldsymbol{S}^l \right\rangle_{\mathbb{F}_{q^m}}\right)(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}}\\ &= \left(\bigoplus_{i \in [\![0, m-1]\!] \setminus \{i_1, (i_2+l) \mod m\}} \mathscr{G}_i\right) \oplus \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_1})} \oplus \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_2+l})}.\end{aligned}$$

Hence

$$\dim_{\mathbb{F}_{q^m}} \mathscr{S}_{aux} + \left\langle \boldsymbol{u}_1, \boldsymbol{u}_2^{q^l}\boldsymbol{S}^l \right\rangle_{\mathbb{F}_{q^m}} = \begin{cases}(r-1)m+1 & \text{if } i_1 = i_2 + l \mod m\\ (r-1)m+2 & \text{otherwise}\end{cases}.$$

and the first case is equivalent to say that

$$\left\langle \boldsymbol{u}_1, \boldsymbol{u}_2^{q^l}\boldsymbol{S}^l \right\rangle_{\mathbb{F}_{q^m}}(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} \subseteq \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^{i_1})},$$

i.e. $\boldsymbol{u}_1$ and $\boldsymbol{u}_2^{q^l}\boldsymbol{S}^l$ correspond to the same GRS code with respect to $\mathcal{B}$. □

E.5 Proof of Proposition 24

Let us recall this proposition

Proposition 24. *Let $\mathscr{V}_j$ be the $[rm, r]$ linear code generated by r linearly independent vectors corresponding to the same GRS code $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^j)}$ with respect to $\mathcal{B}$. Then the linear space $\mathscr{V}_j^{\perp}$ orthogonal to $\mathscr{V}_j$ is such that*

$$\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}} = \sum_{i \in [\![0,m-1]\!]\setminus\{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}. \tag{22}$$

Proof. Since $\dim_{\mathbb{F}_{q^m}}(\mathscr{V}_j) = r$ and each of its elements correspond to the j-th GRS code, a generator matrix of $\mathscr{V}_j(\boldsymbol{P}^{-1})^{\intercal}$ is

$$[\mathbf{0}_{r\times r} \mid \cdots \mid \mathbf{0}_{r\times r} \mid \underbrace{\boldsymbol{I}_r}_{j\text{-th block}} \mid \mathbf{0}_{r\times r} \mid \cdots \mid \mathbf{0}_{r\times r}].$$

Let us pick $\boldsymbol{v}^{\perp} \in \mathscr{V}_j^{\perp}$. For any $\boldsymbol{v} \in \mathscr{V}_j$, we can write

$$\begin{aligned}0 =&\langle \boldsymbol{v}, \boldsymbol{v}^{\perp}\rangle\\ =&\langle \boldsymbol{v}\boldsymbol{I}_{rm}, \boldsymbol{v}^{\perp}\rangle\\ =&\langle \boldsymbol{v}(\boldsymbol{P}^{\intercal})^{-1}\boldsymbol{P}^{\intercal}, \boldsymbol{v}^{\perp}\rangle\\ =&\langle \boldsymbol{v}(\boldsymbol{P}^{-1})^{\intercal}, \boldsymbol{v}^{\perp}\boldsymbol{P}\rangle.\end{aligned}$$

Therefore $\boldsymbol{v}^{\perp}\boldsymbol{P}$ is zero on the j-th block. Hence

$$\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}} = (\mathscr{V}_j^{\perp}\boldsymbol{P})\boldsymbol{H}_{\mathcal{A}} \subseteq \sum_{i \in [\![0,m-1]\!]\setminus\{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)},$$

and since $\dim_{\mathbb{F}_{q^m}}(\mathscr{V}_j^{\perp}) = rm - \dim_{\mathbb{F}_{q^m}} \mathscr{V}_j = (r-1)m$,

$$\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}} = \sum_{i \in [\![0,m-1]\!]\setminus\{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}.$$

□

E.6 Proof of Proposition 25

Let us recall this proposition

Proposition 25. *Let $\mathscr{V}_j^{\perp}$ be a linear space satisfying Equation (22), for all $j \in [\![0, m-1]\!]$. Then with the standard assumption that all $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^j)}$ are in direct sum, we obtain, for any $j \in [\![0, m-1]\!]$,*

$$\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^j)} = \bigcap_{i \in [\![0,m-1]\!]\setminus\{j\}} \mathscr{V}_i^{\perp}\boldsymbol{H}_{\mathcal{B}}.$$

Proof. Since $\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^j)} \subset \mathscr{V}_i^{\perp}$ for all $i \neq j$, it follows that

$$\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{(q^j)} \subseteq \bigcap_{i\in[\![0,m-1]\!]\setminus\{j\}} \mathscr{V}_i^{\perp}\boldsymbol{H}_{\mathcal{B}}.$$

On the other hand, since the GRS codes are in direct sum, we get

$$\dim_{\mathbb{F}_{q^m}} \bigcap_{i\in[\![0,m-1]\!]\setminus\{j\}} \mathscr{V}_i^{\perp} = r(m-1) - r(m-2) = r,$$

which leads to the equality. □

E.7 Estimate of matrices of rank $rm-1$ in $\mathscr{C}_{\mathbf{mat}}(\boldsymbol{\mathcal{B}})$

We start by recalling that $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ and $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ have the same weight distribution, thus it is convenient to consider the block diagonal structure of $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$. Let us also define the matrix space containing all possible block diagonal (with m blocks of size $r \times r$) symmetric matrices $\mathscr{D} \subset \mathbf{Sym}(rm, \mathbb{F}_{q^m})$. The ratio of rank $rm-1$ matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{D})$ is given by

$$\frac{N(r,r-1)\cdot N(r,r)^{m-1}}{(q^m)^{m\binom{r+1}{2}}},$$

where N is defined as in Proposition **??**. Note that, for $q^m \to \infty$,

$$N(t,s) \to \prod_{i=0}^{s-1}(q^m)^{t-i} = (q^m)^{\sum_{i=0}^{s-1} t-i} = (q^m)^{\binom{t+1}{2}-\binom{t-s+1}{2}} = (q^m)^{ts-s^2/2+s/2}.$$

Hence the ratio above tends to

$$\frac{N(r,r-1)N(r,r)^{m-1}}{(q^m)^{m\binom{r+1}{2}}} \to \frac{(q^m)^{r(r-1)-(r-1)^2/2+(r-1)/2}(q^m)^{(m-1)(r^2-r^2/2+r/2)}}{(q^m)^{m\binom{r+1}{2}}} = \frac{1}{q^m}.$$

The ratios of matrices of a given rank in $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ is not the same as for $\mathscr{C}_{\mathrm{mat}}(\mathcal{D})$, and a more detailed analysis would be useful to derive the exact probability of sampling matrices of rank $rm-1$. However, we expect the distribution not to deviate too much from this behavior. We provide in Table 6 the number of different diagonal blocks in $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of a given rank in for small values of q^m (odd case) and r. Note that the total number is given by $(q^m)^{\binom{r-1}{2}}$.

E.8 Characteristic 2

Recall that skew-symmetric matrices in characteristic 2 can only have even rank. This immediately invalidates the search arguments explained before: either rank rm or $rm-1$ do not exist in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ and $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$. The same constraint occurs for the $r \times r$ diagonal blocks with respect to the canonical basis $\mathcal{A}$, on which we focus now. However, the previous strategy can be adapted to even characteristic by

r	q^m	[rank 0, rank 1, ..., rank r]
3	3	[1, 0, 0, 2]
3	5	[1, 0, 0, 4]
3	7	[1, 0, 0, 6]
3	9	[1, 0, 0, 8]
3	11	[1, 0, 0, 10]
4	3	[1, 0, 0, 8, 18]
4	5	[1, 0, 0, 24, 100]
4	7	[1, 0, 0, 48, 294]
4	9	[1, 0, 0, 80, 648]
4	11	[1, 0, 0, 120, 1210]
5	3	[1, 0, 0, 44, 378, 306]
5	5	[1, 0, 0, 224, 5500, 9900]
5	7	[1, 0, 0, 636, 30870, 86142]
5	9	[1, 0, 0, 1376, 110808, 419256]
5	11	[1, 0, 0, 2540, 306130, 1462890]
6	3	[1, 0, 0, 152, 4374, 18072, 36450]
6	5	[1, 0, 0, 1224, 157500, 1919400, 7687500]
7	3	[1, 0, 0, 638, 55566, 587502, 4754538, 8950662]

Table 6. Experimental number of different diagonal blocks in $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of a given rank (q^m odd case).

limiting the search to even-rank matrices. Indeed, in our setting, the maximum rank achievable in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ is $2\left\lfloor \frac{r}{2} \right\rfloor m$, because for each $r \times r$ diagonal block the rank is at most the largest even integer bounded by r, *i.e.* $2\left\lfloor \frac{r}{2} \right\rfloor$. Consequently, the second largest rank achievable by a matrix in $\boldsymbol{A} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ with the block diagonal structure as in (18) is

$$2\left\lfloor \frac{r}{2} \right\rfloor m - 2.$$

- In the case where r is even, $2\left\lfloor \frac{r}{2} \right\rfloor m - 2 = rm - 2$, and $\boldsymbol{A}$ as in (18) is such that there exists a unique $j \in [\![1, m]\!]$ for which $\mathbf{Rank}(\boldsymbol{A}_{j,j}) = r - 2$ and $\mathbf{Rank}(\boldsymbol{A}_{j,j}) = r$ otherwise. Indeed, the parity constraint on the skew-symmetric matrices prohibits having two diagonal blocks of rank $r - 1$. This time, the nullspace of $\boldsymbol{A}$ is generated by two linearly independent vectors $\boldsymbol{u}$ and $\boldsymbol{v}$, and these vectors are zero outside the same j-th length-r blocks:

  $$\boldsymbol{v} = (\mathbf{0}, \dots, \mathbf{0}, \boldsymbol{v}_i, \mathbf{0}, \dots, \mathbf{0})$$

  and

  $$\boldsymbol{u} = (\mathbf{0}, \dots, \mathbf{0}, \boldsymbol{u}_i, \mathbf{0}, \dots, \mathbf{0}).$$

  With similar arguments to the q odd case, it is therefore possible to retrieve a basis of a GRS code $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{q^j}$. We only need to give an estimate of the ratio of rank $rm - 2$ matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$, to ensure that we can find them with non-negligible probability.

We consider the $rm \times rm$ matrix space $\mathscr{D} \subset \mathbf{Skew}(rm, \mathbb{F}_{q^m})$ containing all possible block diagonal (with m blocks of size $r \times r$) skew-symmetric matrices. The ratio of rank $rm-2$ matrices in $\mathscr{D}$ is given by

$$\frac{N_0(r, r-2) \cdot N_0(r,r)^{m-1}}{(q^m)^{m\binom{r}{2}}}. \tag{28}$$

Note that for $q \to \infty$,

$$N_0(t, 2s) \to \prod_{i=0}^{s} \frac{1}{q^2} \prod_{i=0}^{2s-1} (q^m)^{t-i} = (q^m)^{-2s+\sum_{i=0}^{2s-1} t-i} = (q^m)^{\binom{t+1}{2}-\binom{t-2s+1}{2}-2s} = (q^m)^{s(2t-2s-1)}.$$

Hence the ratio above tends to

$$\frac{N_0(r, r-2) \cdot N_0(r,r)^{m-1}}{(q^m)^{m\binom{r}{2}}} \to \frac{(q^m)^{\frac{(r+1)(r-2)}{2}}(q^m)^{(m-1)\binom{r}{2}}}{(q^m)^{m\binom{r}{2}}} = \frac{1}{q^m},$$

i.e. the same as for rank $rm-1$ matrices in the q odd case. The approach for finding matrices of rank $rm-1$ described above is therefore expected to work with high probability in this case as well.

Remark 5. In the case of a binary Goppa code with a square-free Goppa polynomial, we have shown in Proposition 9 that $\mathscr{C}_{\text{mat}}(\mathcal{A})$ contains the space of block-diagonal skew-symmetric matrices with $r \times r$ blocks. Under the condition that $r < q-1$, these matrices generates $\mathscr{C}_{\text{mat}}(\mathcal{A})$, *i.e.* $\mathscr{C}_{\text{mat}}(\mathcal{A}) = \mathscr{D}$. Therefore, in this special case, (28) provides the exact ratio of rank $rm-2$ matrices in $\mathscr{C}_{\text{mat}}(\mathcal{A})$ (or $\mathscr{C}_{\text{mat}}(\mathcal{B})$).

Similarly to what done for the q odd case, we provide in Table 7 the number of different diagonal blocks in $\mathscr{C}_{\text{mat}}(\mathcal{B})$ (when the latter is not originated by a binary Goppa code with square-free polynomial) of a given rank in for small values of q^m (even case) and r (even case). The total number is given by $(q^m)^{\binom{r-1}{2}}$, as before.

r	q^m	[rank 0, rank 1, ..., rank r]
4	2	[1, 0, 3, 0, 4]
4	4	[1, 0, 15, 0, 48]
4	8	[1, 0, 63, 0, 448]
6	2	[1, 0, 27, 0, 612, 0, 384]
6	4	[1, 0, 495, 0, 286224, 0, 761856]
8	2	[1, 0, 171, 0, 51348, 0, 1181376, 0, 864256]

Table 7. Experimental number of different diagonal blocks in $\mathscr{C}_{\text{mat}}(\mathcal{B})$ of a given rank (q^m even, r even case).

Remark 6. In all instances where a filtration has been initially applied, $r = q$ is even, therefore they fall in this case.

The case q even and r even requires only small changes in Algorithm 1. At lines 5,9 and 13, the vectors $\boldsymbol{v}$, $\boldsymbol{u}_1$ and $\boldsymbol{u}_j$ respectively are defined as generators of kernels of rank $rm - 1$ matrices. However, the nullspace of a square matrix of rank $rm - 2$ and size rm is generated by two linearly independent elements. In this case, it suffices to define such vectors as any non-zero element in the kernel and the algorithm still works correctly. It is even possible to exploit the knowledge that two linearly independent generators of a kernel correspond to the same GRS code and roughly halve the number of matrices of rank $rm - 2$ that need to be sampled.

- In the case where r is even, $2\left\lfloor \frac{r}{2} \right\rfloor m - 2 = (r-1)m - 2$ and a similar computation shows that the ratio of rank $r(m-1) - 2$ matrices in $\mathscr{D}$ is given by
$$\frac{N_0(r, r-3) \cdot N_0(r, r-1)^{m-1}}{(q^m)^{m\binom{r}{2}}} \tag{29}$$
and, for $q \to \infty$,
$$\frac{N_0(r, r-3) \cdot N_0(r, r-1)^{m-1}}{(q^m)^{m\binom{r}{2}}} \to \frac{(q^m)^{\frac{(r+2)(r-3)}{2}} (q^m)^{(m-1)\binom{r}{2}}}{(q^m)^{m\binom{r}{2}}} = \frac{1}{(q^m)^3}.$$

Remark 7. Similarly to the r even case, for binary Goppa codes with square-free Goppa polynomials, (29) provides the exact ratio of rank $(r-1)m - 2$ matrices in $\mathscr{C}_{\text{mat}}(\mathcal{A})$ (or $\mathscr{C}_{\text{mat}}(\mathcal{B})$).

We provide in Table 8 the number of different diagonal blocks in $\mathscr{C}_{\text{mat}}(\mathcal{B})$ (when the latter is not originated by a binary Goppa code with square-free polynomial) of a given rank in for small values of q^m (even case) and r (odd case). The total number is given by $(q^m)^{\binom{r-1}{2}}$, as before.

r	q^m	[rank 0, rank 1, ..., rank r]
3	2	[1, 0, 1, 0]
3	4	[1, 0, 3, 0]
3	8	[1, 0, 7, 0]
5	2	[1, 0, 11, 0, 52, 0]
5	4	[1, 0, 111, 0, 3984, 0]
5	8	[1, 0, 959, 0, 261184, 0]
7	2	[1, 0, 75, 0, 5748, 0, 26944, 0]

Table 8. Experimental number of different diagonal blocks in $\mathscr{C}_{\text{mat}}(\mathcal{B})$ of a given rank (q^m even, r odd case).

Rank $rm - 3$ matrices are therefore less probable to be sampled. This issue can be overcome at an asymptotic cost of a factor q^{3m}. Furthermore, a

Gröbner basis approach leads in practice to an even better complexity. More specifically, we can generalize the argument for the previous cases by sampling at random $\boldsymbol{B}_1, \boldsymbol{B}_2, \boldsymbol{B}_3, \boldsymbol{B}_4 \in \mathscr{C}_{\text{mat}}(\mathcal{B})$ and solving the trivariate affine polynomial $\det(w_1\boldsymbol{B}_1 + w_2\boldsymbol{B}_2 + w_3\boldsymbol{B}_3 + \boldsymbol{B}_4)$ with Gröbner basis techniques. As the number of variables is small and constant, this approach seems to be much more efficient than brute force. However, there is another more problematic issue. The nullspace of a matrix $\boldsymbol{A} \in \mathscr{C}_{\text{mat}}(\mathcal{A})$ has in this case dimension $rm - ((r-1)m - 2) = m + 2$ and its generators are not all zero outside a length-r block. Therefore the strategy explained before does not apply directly here. We treat this case in E.9.

E.9 The attack for q even and r odd

As already mentioned, the case where q is even and r is odd raises the additional problem that the nullspace of a matrix $\boldsymbol{A} \in \mathscr{C}_{\text{mat}}(\mathcal{A})$ of rank $(r-1)m-2$ is not zero outside a length-r block. The key idea to adapt the attack is that such nullspace is still "unbalanced" with respect to the m blocks. Indeed, let us consider $\boldsymbol{B} = (\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{A}(\boldsymbol{P}^{-1}) \in \mathscr{C}_{\text{mat}}(\mathcal{B})$ of rank $(r-1)m-2$. Since $\mathbf{Rank}(\boldsymbol{B}) = \mathbf{Rank}(\boldsymbol{A}) = \sum_{l=0}^{m-1} \mathbf{Rank}(\boldsymbol{A}_{l,l})$ and for any l, $\mathbf{Rank}(\boldsymbol{A}_{l,l}) \leqslant r-1$ and it is even, we have that

$$\exists! l \in [\![0, m-1]\!] \text{ s.t. } \mathbf{Rank}(\boldsymbol{A}_{l,l}) = r-3 \wedge \forall i \in [\![0, m-1]\!] \backslash \{l\},\ \mathbf{Rank}(\boldsymbol{A}_{i,i}) = r-1.$$

Therefore, the kernel can be written as

$$\ker \boldsymbol{B} = \langle \boldsymbol{v}_0, \dots, \boldsymbol{v}_{l-1}, \boldsymbol{v}_{l,1}, \boldsymbol{v}_{l,2}, \boldsymbol{v}_{l,3}, \boldsymbol{v}_{l+1}, \dots, \boldsymbol{v}_{m-1} \rangle$$

so that for all $i \in \{1, 2, 3\}$

$$\boldsymbol{v}_{l,i}(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} = \boldsymbol{v}_{l,i}(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{H}_{\mathcal{A}} \in \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^l)},$$

and for all $j \in [\![0, m-1]\!] \backslash \{l\}$

$$\boldsymbol{v}_j(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{P}^{-1}\boldsymbol{H}_{\mathcal{B}} = \boldsymbol{v}_j(\boldsymbol{P}^{-1})^{\mathsf{T}}\boldsymbol{H}_{\mathcal{A}} \in \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^j)}.$$

We do not know how to identify such vectors, though. Assume, however, that we are able to determine different matrices $\boldsymbol{B}_1, \dots, \boldsymbol{B}_s$ of rank $(r-1)m-2$ in $\mathscr{C}_{\text{mat}}(\mathcal{B})$ such that their counterparts in $\mathscr{C}_{\text{mat}}(\mathcal{A})$ have the rank-$(r-3)$ block indexed by the same $j \in [\![0, m-1]\!]$, for some value $s < r$ that we are going to determine later. We will see how to achieve this in E.10. We define the $[rm, \leqslant s(m-1) + \min(3s, r)]$ linear code $\mathscr{V}_j \overset{\text{def}}{=} \sum_{i=1}^{s} \ker \boldsymbol{B}_i$. This construction can be seen as an adaptation of the definition given in Proposition 24, where $\mathscr{V}_j$ is spanned by r vectors, each generating the nullspace of a matrix of rank $rm-1$. If the matrices $\boldsymbol{B}_i$'s have been sampled independently, as is the case, we expect, with a non-negligible probability, that a generator matrix of the code $\mathscr{V}_j(\boldsymbol{P}^{-1})^{\mathsf{T}}$

is the block diagonal matrix

$$\begin{bmatrix} \boldsymbol{G}_{0,0} & & & \\ & \boldsymbol{G}_{1,1} & & \mathbf{0} \\ \mathbf{0} & & \ddots & \\ & & & \boldsymbol{G}_{m-1,m-1} \end{bmatrix}$$

where $\boldsymbol{G}_{j,j}$ has $\min(3s, r)$ rows while $\boldsymbol{G}_{i,i}$ has s rows (and they all have r columns). This is equivalent to say that $\dim_{\mathbb{F}_{q^m}} \mathscr{V}_j = s(m+2)$. Hence, by sampling $s \geqslant \lceil r/3 \rceil$, we ensure $\boldsymbol{G}_{j,j} = \boldsymbol{I}_r$ with non-negligible probability. From now on, we then assume that $\dim_{\mathbb{F}_{q^m}} \mathscr{V}_j = s(m-1) + r$. We define the $[rm, (r-s)(m-1)]$ dual code $\mathscr{V}_j^{\perp}$ and, by repeating the computation made in the proof of Proposition 24, we get that, for any $\boldsymbol{v}^{\perp} \in \mathscr{V}_j^{\perp}$, $\boldsymbol{v}^{\perp}\boldsymbol{P}$ is zero on the j-th block. However, this time we can only assert that

$$\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}} = (\mathscr{V}_j^{\perp}\boldsymbol{P})\boldsymbol{H}_{\mathcal{A}} \subseteq \sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$$

with $\dim_{\mathbb{F}_{q^m}}(\mathscr{V}_j^{\perp}\boldsymbol{H}_{\mathcal{B}}) = \dim_{\mathbb{F}_{q^m}}(\mathscr{V}_j^{\perp}) = (r-s)(m-1)$. In order to obtain the code $\sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$ it is then enough to repeat the process and analogously compute other linear codes $\mathscr{V}_j', \mathscr{V}_j'', \dots$ such that $(\mathscr{V}_j')^{\perp}\boldsymbol{H}_{\mathcal{B}} \subseteq \sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$ as well (by sampling each time different matrices of rank $(r-1)m-2$). Since all these codes are constructed independently, we expect at some point

$$(\mathscr{V}_j + \mathscr{V}_j' + \mathscr{V}_j'' + \dots)^{\perp}\boldsymbol{H}_{\mathcal{B}} = \sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}.$$

Since $(\mathscr{V}_j + \mathscr{V}_j' + \mathscr{V}_j'' + \dots)^{\perp}\boldsymbol{H}_{\mathcal{B}} \subseteq \sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$, one can put $\dim_{\mathbb{F}_{q^m}}(\mathscr{V}_j + \mathscr{V}_j' + \dots)^{\perp} = (r-1)m$ as an exit condition for the construction of such codes.

Remark 8. A good choice for s is $\frac{r-1}{2}$. In this way, $\boldsymbol{G}_{j,j} = \boldsymbol{I}_r$ with very high probability and at the same time, since $2(rm - s(m-1) - \min(3s, r)) \geqslant 2(r-s)(m-1) \geqslant r(m-1)$, computing just two codes $\mathscr{V}_j$ and $\mathscr{V}_j'$ is typically enough to recover $\sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$.

Once the codes $\sum_{i \in \llbracket 1,m \rrbracket \setminus \{j\}} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{(q^i)}$ have been retrieved for any $j \in \llbracket 0, m-1 \rrbracket$, a GRS block code can be obtained from intersections as done previously according to Proposition 25.

E.10 Computing $\mathscr{V}_j$

In this technical subsection, we tackle the problem of determining, given two matrices $\boldsymbol{B}_1, \boldsymbol{B}_2 \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ of rank $(r-1)m-2$, which blockwise Dickson shift of $\boldsymbol{P}^{\intercal}\boldsymbol{B}_2\boldsymbol{P}$ has the diagonal block of rank $r-3$ for the same index l as $\boldsymbol{B}_1$. This represents the basic step to produce elements in $\mathscr{V}_j$ in this case.

Remark 9. Note that, in the q odd case, this would be equivalent to determining which shift of $\boldsymbol{v}_2$ corresponds to the same GRS code of $\boldsymbol{v}_1$ where $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are the generators of the kernels of two matrices $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ respectively of rank $rm-1$. In the case we examine now, however, the dimension of the nullspace is larger than 1 and not all its elements belong to the same GRS code. This explains why we need to move to the matrix formalism. Analogously, in the q odd case, vectors corresponding to the same GRS code were identified by making use of an auxiliary linear code $\mathscr{S}_{aux}$ spanned by kernel generators of a set of matrices. We will see that here we directly employ a set of auxiliary matrices $\boldsymbol{B}_{aux,i}$'s instead.

Analogously to what shown in Proposition 21, we still have that if $\boldsymbol{vB} = 0$, then

$$(\boldsymbol{v}^{q^i}\boldsymbol{S}^i)\cdot(\boldsymbol{S}^\intercal)^i\boldsymbol{B}^{(q^i)}\boldsymbol{S}^i = (\boldsymbol{vB})^{(q^i)}\boldsymbol{S}^i = 0,$$

therefore the nullspaces of blockwise Dickson shift matrices can be easily computed from the others. Let r_1, r_2 be the unique integers such that $r = r_1(m+2)+r_2$ with $r_2 \in \llbracket 1, m+2 \rrbracket$. We split the analysis into different cases:

- **Case** $4 \leqslant r_2 \leqslant m+2$**.** Let $\boldsymbol{B}_1, \boldsymbol{B}_2 \in \mathscr{C}_{\text{mat}}(\mathcal{B})$ of rank $(r-1)m-2$. Let us first consider the case $r_1 = 0$. Consider the linear code

$$\left(\sum_{i=0}^{r-4}\ker\left((\boldsymbol{S}^\intercal)^i\boldsymbol{B}_2^{(q^i)}\boldsymbol{S}^i\right)\right).$$

A generator matrix of $\left(\sum_{i=0}^{r-4}\ker\left((\boldsymbol{S}^\intercal)^i\boldsymbol{B}_2^{(q^i)}\boldsymbol{S}^i\right)\right)(\boldsymbol{P}^{-1})^\intercal$ can be written as

$$\begin{bmatrix} \boldsymbol{G}_{0,0} & & & \\ & \boldsymbol{G}_{1,1} & & \mathbf{0} \\ \mathbf{0} & & \ddots & \\ & & & \boldsymbol{G}_{m-1,m-1} \end{bmatrix} \tag{30}$$

where $r-3$ cyclically consecutive diagonal blocks have $r-1$ rows while the others have $r-3$ rows (and they all have r columns). A generator matrix of $\ker(\boldsymbol{B}_1)(\boldsymbol{P}^{-1})^\intercal$ is instead given by

$$\begin{bmatrix} \boldsymbol{v}_1 & \mathbf{0} & \mathbf{0} \\ & \ddots & \\ & \boldsymbol{v}_{l,1} & \\ \mathbf{0} & \boldsymbol{v}_{l,2} & \mathbf{0} \\ & \boldsymbol{v}_{l,3} & \\ & & \ddots \\ \mathbf{0} & \mathbf{0} & \boldsymbol{v}_m \end{bmatrix} \tag{31}$$

for some $l \in \llbracket 0, m-1 \rrbracket$. If $\mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-1$, then

$$\begin{aligned}\dim_{\mathbb{F}_{q^m}}\left(\ker(\boldsymbol{B}_1) + \sum_{i=0}^{r-4} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)\right) &= \dim_{\mathbb{F}_{q^m}}\left(\left(\ker(\boldsymbol{B}_1) + \sum_{i=0}^{r-4} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)\right)(\boldsymbol{P}^{-1})^\intercal\right)\\ &\leqslant (r-4)((r-1)+1) + (r) + (m-r+3)((r-3)+1)\\ &= rm + 2r - 2m - 6.\end{aligned}$$

On the other hand, if $\mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-3$, then we expect with good probability that the dimension of $\ker(\boldsymbol{B}_1) + \sum_{i=0}^{r-4} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)$ attains

$$\begin{aligned}&(r-3)((r-1)+1) + (m-r+2)((r-3)+1) + ((r-3)+3)\\ =&rm + 2r - 2m - 4.\end{aligned}$$

Therefore, by computing the dimension of $\ker(\boldsymbol{B}_1) + \sum_{i=0}^{r-4} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)$ we determine whether the rank-$(r-3)$ block of $\boldsymbol{B}_1$ corresponds to a rank-$(r-3)$ block of some of the $\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)$'s for some $i \in \llbracket 0, r-4 \rrbracket$. By replacing $\llbracket 0, r-4 \rrbracket$ with other subsets of $\llbracket 0, m-1 \rrbracket$ of cardinality $r-3$ and repeating the process, we finally detect the sought $\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)$. In the case where $r_1 > 0$, we need to sample independent rank-$((r-1)m-2)$ matrices $\boldsymbol{B}_{aux,1}, \dots, \boldsymbol{B}_{aux,r_1} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{B})$. In this case a generator matrix of

$$\left(\sum_{j=1}^{r_1} \sum_{i=0}^{m-1} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_{aux,j}^{(q^i)} \boldsymbol{S}^i\right) + \sum_{i=0}^{r_2-4} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)\right)(\boldsymbol{P}^{-1})^\intercal$$

is with non-negligible probability as in (**??**), where $r_2 - 3$ cyclically consecutive diagonal blocks have $r_1(m+2) + r_2 - 1 = r - 1$ rows while the others have $r_1(m+2) + r_2 - 3 = r - 3$ rows (and they all have r columns). Hence, the computation of

$$\dim_{\mathbb{F}_{q^m}} \ker(\boldsymbol{B}_1) + \sum_{j=1}^{r_1} \sum_{i=0}^{m-1} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_{aux,j}^{(q^i)} \boldsymbol{S}^i\right) + \sum_{i=0}^{r_2-4} \ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)$$

$$\begin{cases} \leqslant & (r_2-4)((r-1)+1) + (r) + (m-r_2+3)((r-3)+1)\\ & = rm + 2r_2 - 2m - 6 \quad \text{if } \mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-1,\\ = & (r_2-3)((r-1)+1) + (m-r_2+2)((r-3)+1) + ((r-3)+3)\\ & = rm + 2r_2 - 2m - 4 \quad \text{otherwise (with high probability)}\end{cases}$$

reveals again whether the rank-$(r-3)$ block of $\boldsymbol{B}_1$ corresponds or not to one of the rank-$(r-3)$ blocks of the $\ker\left((\boldsymbol{S}^\intercal)^i \boldsymbol{B}_2^{(q^i)} \boldsymbol{S}^i\right)$'s.

- **Case** $r_2 = 1$ **and** $r_1 \geqslant 1$**.** The reasoning is very similar to the one in the previous case. An analogous computation shows that

$$\dim_{\mathbb{F}_{q^m}} \ker(\boldsymbol{B}_1) + \sum_{j=1}^{r_1-1}\sum_{i=0}^{m-1} \ker\left((\boldsymbol{S}^{\intercal})^i \boldsymbol{B}_{aux,j}^{(q^i)}\boldsymbol{S}^i\right) + \sum_{i=0}^{m-2}\ker\left((\boldsymbol{S}^{\intercal})^i\boldsymbol{B}_2^{(q^i)}\boldsymbol{S}^i\right)$$
$$\begin{cases} \leqslant & (m-2)((r-2)+1)+(r)+((r-4)+1) \\ & = rm-m-1 \quad \text{if } \mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-2, \\ = & (m-1)((r-2)+1)+((r-4)+3) \\ & = rm-m \quad \text{otherwise (with high probability)} \end{cases},$$

for the index $l \in [\![0, m-1]\!]$ such that a generator matrix of $\ker(\boldsymbol{B}_1)(\boldsymbol{P}^{-1})^{\intercal}$ is as in (31) and a generator matrix of $\left(\sum_{j=1}^{r_1-1}\sum_{i=0}^{m-1}\ker\left((\boldsymbol{S}^{\intercal})^i\boldsymbol{B}_{aux,j}^{(q^i)}\boldsymbol{S}^i\right) + \sum_{i=0}^{m-2}\ker\left((\boldsymbol{S}^{\intercal})^i\boldsymbol{B}_2^{(q^i)}\boldsymbol{S}^i\right)\right)(\boldsymbol{P}^{-1})^{\intercal}$ is as in (30), with $m-1$ cyclically consecutive diagonal blocks having $r-2$ rows while the other having $r-4$ rows (and they all have r columns). Hence we can distinguish the case $\mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-2$ from $\mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-4$.

- **Case** $r_2 = 2$ **and** $r_1 \geqslant 1$**.** In this case, we take two consecutive blockwise Dickson shifts of $\boldsymbol{B}_1$, *i.e.* $\boldsymbol{B}_1$ and $\boldsymbol{S}^{\intercal}\boldsymbol{B}_1^{(q)}\boldsymbol{S}$. Therefore a generator matrix of $\left(\ker(\boldsymbol{B}_1) + \ker(\boldsymbol{S}^{\intercal}\boldsymbol{B}_1^{(q)}\boldsymbol{S})\right)(\boldsymbol{P}^{-1})^{\intercal}$ is given by either

$$\begin{bmatrix} \boldsymbol{V}_{0,0} & & & \\ & \boldsymbol{V}_{1,1} & & \mathbf{0} \\ \mathbf{0} & & \ddots & \\ & & & \boldsymbol{V}_{m-1,m-1} \end{bmatrix}$$

where 2 cyclically consecutive diagonal blocks have 4 rows while the others have 2 rows (and they all have r columns). Let us say that the two blocks with 4 rows are indexed by l and $l+1 \mod m$, for some $l \in [\![0, m-1]\!]$. Then we get

$$\dim_{\mathbb{F}_{q^m}} \ker(\boldsymbol{B}_1) + \ker(\boldsymbol{S}^{\intercal}\boldsymbol{B}_1^{(q)}\boldsymbol{S}) + \sum_{j=1}^{r_1-1}\sum_{i=0}^{m-1} \ker\left((\boldsymbol{S}^{\intercal})^i \boldsymbol{B}_{aux,j}^{(q^i)}\boldsymbol{S}^i\right) + \sum_{i=0}^{m-2}\ker\left((\boldsymbol{S}^{\intercal})^i\boldsymbol{B}_2^{(q^i)}\boldsymbol{S}^i\right)$$
$$\begin{cases} \leqslant & (m-3)((r-3)+2)+(2r)+((r-5)+2) \\ & = rm-m \quad \text{if } \mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-3 \wedge \mathbf{Rank}(\boldsymbol{G}_{l+1 \mod m, l+1 \mod m}) = r-3, \\ = & (m-2)((r-3)+2)+(r)+((r-5)+3+1) \\ & = rm-m+1 \quad \text{otherwise (with high probability)} \end{cases}$$

where a generator matrix of $\left(\sum_{j=1}^{r_1-1}\sum_{i=0}^{m-1}\ker\left((\boldsymbol{S}^{\intercal})^i\boldsymbol{B}_{aux,j}^{(q^i)}\boldsymbol{S}^i\right) + \sum_{i=0}^{m-2}\ker\left((\boldsymbol{S}^{\intercal})^i\boldsymbol{B}_2^{(q^i)}\boldsymbol{S}^i\right)\right)(\boldsymbol{P}^{-1})^{\intercal}$ is as in (30), with $m-1$ cyclically consecutive diagonal blocks having $r-3$ rows while the other having $r-5$ rows (and they all have r columns). Hence we can distinguish the case $\mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-3 \wedge \mathbf{Rank}(\boldsymbol{G}_{l+1 \mod m, l+1 \mod m}) = r-3$ from $\mathbf{Rank}(\boldsymbol{G}_{l,l}) = r-5 \vee \mathbf{Rank}(\boldsymbol{G}_{l+1 \mod m, l+1 \mod m}) = r-5$. Repeating the process at most m times for different pairs of consecutive diagonal block shifts of $\boldsymbol{B}_1$, solves our problem.

- **Case** $r_2 = 3$**.** If $r_1 = 0$, the kernel of a single matrix $\boldsymbol{B}$ already defines $\mathscr{V}_j$ (note that we can choose $s = \lceil \frac{r}{3} \rceil = \frac{r-1}{2} = 1$). Otherwise, let $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ such that generator matrices of $\ker(\boldsymbol{B}_1)(\boldsymbol{P}^{-1})^{\mathsf{T}}$ and $\ker(\boldsymbol{B}_2)(\boldsymbol{P}^{-1})^{\mathsf{T}}$ respectively are given by

$$\begin{bmatrix} \boldsymbol{v}_1 & \mathbf{0} & \mathbf{0} \\ & \ddots & \\ & \boldsymbol{v}_{l_1,1} & \\ \mathbf{0} & \boldsymbol{v}_{l_1,2} & \mathbf{0} \\ & \boldsymbol{v}_{l_2,3} & \\ & & \ddots \\ \mathbf{0} & \mathbf{0} & \boldsymbol{v}_m \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \boldsymbol{u}_1 & \mathbf{0} & \mathbf{0} \\ & \ddots & \\ & \boldsymbol{u}_{l_2,1} & \\ \mathbf{0} & \boldsymbol{u}_{l_2,2} & \mathbf{0} \\ & \boldsymbol{u}_{l_2,3} & \\ & & \ddots \\ \mathbf{0} & \mathbf{0} & \boldsymbol{u}_m \end{bmatrix}. \tag{32}$$

A generator matrix of $\left(\sum_{j=1}^{r_1}\sum_{i=0}^{m-1} \ker\left((\boldsymbol{S}^{\mathsf{T}})^i \boldsymbol{B}_{aux,j}^{(q^i)} \boldsymbol{S}^i\right)\right)(\boldsymbol{P}^{-1})^{\mathsf{T}}$ is expected to be as in (30), with all the block have $r-3$ rows (and r columns). Therefore

$$\dim_{\mathbb{F}_{q^m}} \ker(\boldsymbol{B}_1) + \ker((\boldsymbol{S}^{\mathsf{T}})^l \boldsymbol{B}_2^{(q^l)} (\boldsymbol{S})^l) + \sum_{j=1}^{r_1}\sum_{i=0}^{m-1} \ker\left((\boldsymbol{S}^{\mathsf{T}})^i \boldsymbol{B}_{aux,j}^{(q^i)} \boldsymbol{S}^i\right)$$

$$\left\{\begin{array}{ll} \leqslant & (m-1)((r-3)+2)+(r) \\ & = rm-m+1 \quad \text{if } l_1 = l_2 + l \mod m, \\ = & (m-2)((r-3)+2)+(2r)+((r-5)+3+1) \\ & = rm-m+2 \quad \text{otherwise (with high probability)} \end{array}\right.$$

Repeating the process at most m times for different values of l solves our problem.