Understanding the new distinguisher of alternant codes at degree 2

Axel Lemoine[1,3], Rocco Mora[2], and Jean-Pierre Tillich[1]

[1] Inria Paris, France
{axel.lemoine,jean-pierre.tillich}@inria.fr
[2] CISPA, Germany
rocco.mora@cispa.de
[3] DGA, France

Abstract. Distinguishing Goppa codes or alternant codes from generic linear codes [FGO+11] has been shown to be a first step before being able to attack McEliece cryptosystem based on those codes [BMT24]. Whereas the distinguisher of [FGO+11] is only able to distinguish Goppa codes or alternant codes of rate very close to 1, in [CMT23a] a much more powerful (and more general) distinguisher was proposed. It is based on computing the Hilbert series $\{\mathrm{HF}(d),\ d \in \mathbb{N}\}$ of a Pfaffian modeling. The distinguisher of [FGO+11] can be interpreted as computing $\mathrm{HF}(1)$. Computing $\mathrm{HF}(2)$ still gives a polynomial time distinguisher for alternant or Goppa codes and is apparently able to distinguish Goppa or alternant codes in a much broader regime of rates as the one of [FGO+11]. However, the scope of this distinguisher was unclear. We give here a formula for $\mathrm{HF}(2)$ corresponding to generic alternant codes when the field size q satisfies $q \geqslant r$, where r is the degree of the alternant code. We also show that this expression for $\mathrm{HF}(2)$ provides a lower bound in general. The value of $\mathrm{HF}(2)$ corresponding to random linear codes is known and this yields a precise description of the new regime of rates that can be distinguished by this new method. This shows that the new distinguisher improves significantly upon the one given in [FGO+11].

1 Introduction

McEliece cryptosystem [McE78] is the oldest code-based scheme and it is based on binary Goppa codes, a subfamily of alternant codes. It is believed to be quantum-resistant and its IND-CCA secure variation [ABC+22] is currently a fourth round finalist of the NIST post-quantum competition. For a long time, it was believed that structural attacks aiming at recovering the underlying Goppa structure from an arbitrary generator matrix of the code were much more expensive than message recovery attacks. The latter ignore completely the algebraic structure and aim just at decoding a generic linear code.

In [FGO+11] another approach was tried. Instead of trying to recover directly the algebraic structure from a generator matrix of a Goppa code, a potentially easier problem is solved first, namely that of *distinguishing* a Goppa code from a generic linear code just from the knowledge of a generator matrix of the code. This is a promise problem where either we are given a generator matrix of a Goppa code or one of a random linear code and one must decide in which case we are. It turned out that there is a way to solve this problem in polynomial time for Goppa codes, and more generally for alternant codes, as long as their rate is high enough [FGO+11]. It took a while to transform this distinguisher into an algorithm recovering the algebraic structure of the Goppa or the alternant code. This has recently been (partly) achieved in [BMT24, CMT23b]. Unfortunately, the specific case of *binary* Goppa codes could not be handled by these two papers.

Interestingly enough, [CMT23b] also puts forward a new algebraic object, namely the matrix code of quadratic relations. The point is that this matrix code can be associated to any linear code. However, the matrix code associated to Goppa or alternant codes contains matrices of unusually low rank, namely rank 3 in odd characteristic and rank 2 in even characteristic, which are consequences of structured quadratic relations. Finding such low rank matrices can in principle be achieved by solving the corresponding MinRank problem. Moreover, in characteristic 2, the matrix code is a subspace of skew-symmetric matrices and the MinRank problem can be modeled with a system where the Pfaffians of principal submatrices of order 4 are equated to 0. The polynomials corresponding to these equations define what we call the Pfaffian ideal. The existence of low-rank matrices has been exploited to mount a distinguisher attack and its complexity has been partially analyzed [CMT23b] as we recall below.

This work focuses on characteristic 2 and aims to advance the knowledge of a fundamental object associated with the above-mentioned Pfaffian ideal (and with polynomial ideals in general): its Hilbert function (or series). This Hilbert series $\{\mathrm{HF}(d), d \in \mathbb{N}\}$ turns out to be a very good way to distinguish alternant or Goppa codes from generic linear codes. Whereas $\mathrm{HF}(d)$ never vanishes in the first case, it turns out to be equal to 0 for a large enough degree in the second case. This gives a new distinguisher for Goppa or alternant codes. The Hilbert function associated to a generic linear code can be easily derived by making some assumptions that have been verified experimentally [CMT23b, Conjecture 1] and the smallest degree for which the Hilbert series vanishes can be computed. Interestingly in the case when the co-dimension $n-k$ of the code is of the form $n-k = \mathcal{O}(n^{\alpha})$ when $\alpha < 1$ and n is the codelength, the degree d at which this happens is low enough so that the actual computation of the Hilbert series can be done with a complexity which is smaller than the aforementioned message recovery attacks. Potentially, this also paves the way to key attacks on the McEliece cryptosystem based on such codes of very large rate which are *less complex* than message recovery attacks.

Unfortunately, whereas the Hilbert series $\{\mathrm{HF}_{\mathrm{R}}(d), d \in \mathbb{N}\}$ of a generic linear code is well understood in [CMT23b], the Hilbert series $\{\mathrm{HF}_{\mathrm{A}}(d), d \in \mathbb{N}\}$ that corresponds to an alternant code is much more difficult to analyze. This is a pity, since this would allow to understand precisely the scope of the distinguisher based on the computation of the Hilbert series. The only case, which was understood right now is the Hilbert series at degree 1, $\mathrm{HF}(1)$. It turns out that knowing $\mathrm{HF}(1)$ is equivalent to knowing the dimension of the square of the dual code and the distinguisher of alternant or Goppa codes based on the fact that their $\mathrm{HF}(1)$ differs is actually equivalent to the distinguisher of [FGO$^+$11].

The aim of this work is to understand the value of $\mathrm{HF}_\mathrm{A}(2)$. We will provide here a formula for it together with a proof using a natural conjecture that has been verified experimentally. We also prove that this formula is actually a rigorous lower bound on $\mathrm{HF}_\mathrm{A}(2)$ in general. It turns out that the distinguisher based on $\mathrm{HF}_\mathrm{A}(2) \neq \mathrm{HF}_\mathrm{R}(2)$ works for a much broader set of of parameters than the distinguisher $\mathrm{HF}_\mathrm{A}(1) \neq \mathrm{HF}_\mathrm{R}(1)$ (which is equivalent to the one of [FGO$^+$11]). It also shows that the parameter range for which $\mathrm{HF}_\mathrm{A}(2) \neq \mathrm{HF}_\mathrm{R}(2)$ is much broader than the range of parameters for which $\mathrm{HF}_\mathrm{R}(2) = 0$. This improves for certain parameters the distinguisher of [CMT23b] and could also open the way to key attacks in the regime of parameters for which $\mathrm{HF}_\mathrm{A}(2) \neq \mathrm{HF}_\mathrm{R}(2)$, much in the same way that [FGO$^+$11, MT23] were a first step before the attacks of [BMT24, CMT23b]. On top of that, knowing the Hilbert series precisely is crucial when it comes to solve the Pfaffian system and our work can be viewed as a significant step in this direction.

It is also worthwhile to note that another generalization of the distinguisher of [FGO$^+$11] has been proposed recently in [Ran24] and has lead to a breakthrough result, namely a distinguisher of subexponential complexity of Goppa or alternant codes which works even in the constant rate regime and for any finite characteristic. A crucial ingredient to get this subexponential complexity is shortening the dual of the alternant or Goppa code and then applying the algebraic distinguisher to it. It would be interesting to understand how the HF_A distinguisher behaves at degree 2 when applied to such shortened codes.

2 Preliminaries

General notation. We work in characteristic 2 throughout the paper. We denote by $\mathbb{F}_q$ the finite field of size q which is therefore assumed here to be a power of 2. If we just want to indicate that we deal with an arbitrary field we simply write $\mathbb{F}$.

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 $\boldsymbol{x} = (x_i)_{1 \leqslant i \leqslant n} \in \mathbb{F}^n$, 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 to 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 $(x_i^a y_i^b)_{1 \leqslant i \leqslant n}$.

Reed-Solomon and alternant codes.

Definition 1 (Generalized Reed-Solomon code). *Let $n \leqslant q$ be an integer, $\boldsymbol{x} = (x_1, \ldots, x_n)$ be a vector of pairwise-distinct elements of $\mathbb{F}_q$, and $\boldsymbol{y} \in (\mathbb{F}_q^\times)^n$.*

The Generalized Reed-Solomon (GRS in short) code of dimension r, support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$ is

$$\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y}) \overset{def}{=} \{(y_1 f(x_1),\dots,y_n f(x_n)) \mid f \in \mathbb{F}_q[X]_{<r}\}.$$

Alternant codes are subfield subcodes of GRS codes. It will be convenient here to follow the point of view of [MS86] which defines them in terms of the dual GRS code (which is itself a GRS code [MS86]).

Definition 2 (Alternant code). *Let r, m be two integers, $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ be a support (i.e. an n-tuple of distinct elements of $\mathbb{F}_{q^m}$), and $\boldsymbol{y} \in (\mathbb{F}_{q^m}^{\times})^n$ be a multiplier. The alternant code over $\mathbb{F}_q$ of degree r, support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$ is the subfield subcode over $\mathbb{F}_q$ of $\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{\perp}$:*

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

m is called the extension degree of the alternant code.

We know that [MS86] $\dim_{\mathbb{F}_q} \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) \geqslant n - rm$ and this bound is generally tight. Goppa codes are a particular family of alternant codes. They are defined as

Definition 3 (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 $i \in \{1,\dots,n\}$. 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 $\boldsymbol{y} \overset{def}{=} \left(\frac{1}{\Gamma(x_1)},\dots,\frac{1}{\Gamma(x_n)}\right)$.*

Schur/component-wise product. The family of codes defined above can be conveniently generated by vectors that are component-wise (also called Schur) products of $\boldsymbol{x}$ and $\boldsymbol{y}$. Recall that this product is defined as

Definition 4. *The component-wise product of two vectors $\boldsymbol{a},\boldsymbol{b} \in \mathbb{F}^n$ is defined as*

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

The i-th power of a vector $\boldsymbol{a}$ is defined by $\boldsymbol{a}^i = \underbrace{\boldsymbol{a} \star \cdots \star \boldsymbol{a}}_{i\ times}$. This notation is compatible with the notation $f(\boldsymbol{x})$ introduced above. Sometimes we will drop the star, i.e. $\boldsymbol{y}\boldsymbol{x}^i = \boldsymbol{y} \star \boldsymbol{x}^i$.

Since any polynomial P in $\mathbb{F}[z]$ of degree $< r$ can be written as a linear combination over $\mathbb{F}$ of powers of z of degree $< r$, by using the notation given above we can view a GRS code as

$$\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y}) \overset{\text{def}}{=} \left\langle \boldsymbol{x}^a \boldsymbol{y} \mid 0 \leqslant a < r \right\rangle_{\mathbb{F}_q}.$$

The Schur product is also an essential ingredient for distinguishing GRS codes or alternant codes from random codes. The Schur/component-wise product of codes is defined 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 $\mathscr{C}$.

GRS codes turn out to display a very peculiar property with respect to the square of codes. It is readily seen that $\dim \mathscr{C}^{\star 2} \leqslant \min\left(n, \binom{k+1}{2}\right)$ where k and n are respectively the dimension and length of $\mathscr{C}$. For random codes, the upper-bound is almost always an equality [CCMZ15], whereas the situation for GRS codes is completely different: in this case, we namely have

$$\dim \mathscr{C}^{\star 2} = \min(n, 2k - 1) . \tag{1}$$

The reason of this particular behavior comes from the fact that GRS codes are polynomial evaluation codes. Since the Schur product of two polynomial evaluations of degree $\deg P \leqslant k-1$ and $\deg Q \leqslant k-1$ respectively is itself a polynomial evaluation of degree $\deg(P \cdot Q) = \deg P + \deg Q < 2k - 1$:

$$(y_i P(x_i))_i \star (y_i Q(x_i))_i = (y_i^2 P \cdot Q(x_i))_i,$$

it is readily seen that

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2k-1}(\boldsymbol{x}, \boldsymbol{y} \star \boldsymbol{y}), \tag{2}$$

which explains (1). In a sense, the square code construction "sees" the polynomial structure of the GRS code. Similarly, alternant codes inherit the polynomial structure of the GRS super-code and can also be detected by taking the square of them [COT14] (or their dual code [MT22]).

Quadratic relations over a basis of a code. The aforementioned distinguisher is based on computing the dimension of square codes or on computing related quantities. A new way of approaching the problem of distinguishing such codes has been introduced in [CMT23b] and consists instead in considering *linear relations* between the Schur products of basis elements of the code or the dual code. Higher order relations were studied in [Ran24] and lead to a powerful distinguisher. This new approach may be described using the framework detailed below.

For any integer k, we denote with

$$S_k \overset{\text{def}}{=} \mathbb{F}[x_1, \ldots, x_k] = \bigoplus_{d \geqslant 0} S_k^{(d)}$$

the polynomial ring in k variables over $\mathbb{F}$, graded by degree, where $S_k^{(d)}$ stands for the homogeneous component of degree d. Elements of $S_k^{(2)}$ are referred to as *quadratic forms.* Given a list $\mathcal{V} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ of k vectors of length n over $\mathbb{F}$, there is a natural evaluation map

$$\mathrm{ev}_{\mathcal{V}} : S_k \longrightarrow \mathbb{F}^n$$

defined on each homogeneous component by

$$\mathrm{ev}_{\mathcal{V}}^{(d)} \overset{\text{def}}{=} \mathrm{ev}_{\mathcal{V}|S_k^{(d)}} : \begin{cases} S_k^{(d)} & \longrightarrow \mathbb{F}^n \\ \sum\limits_{i_1 \leqslant \ldots \leqslant i_d} c_{i_1,\ldots i_d} x_{i_1} \ldots x_{i_d} & \longmapsto \sum\limits_{i_1 \leqslant \ldots \leqslant i_d} c_{i_1,\ldots i_d} \boldsymbol{v}_{i_1} \star \ldots \star \boldsymbol{v}_{i_d}, \end{cases}$$

and then extended to S_k by linearity.

Definition 6. *Let $\mathscr{C}$ be an $[n, k]$-linear code over $\mathbb{F}$, and let $\mathcal{V} \overset{def}{=} (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ be a basis of $\mathscr{C}$. The code of quadratic relations of $\mathscr{C}$ with respect to $\mathcal{V}$ is defined as $\mathscr{C}_{rel}(\mathcal{V}) \overset{def}{=} \ker \mathrm{ev}_{\mathcal{V}}^{(2)}$.*

In this setting, the code of quadratic relations is seen as a linear subspace of $S_k^{(2)}$. A quadratic form

$$f = \sum_{i \leqslant j} c_{i,j} x_i x_j \in S_k^{(2)}$$

is associated to a matrix

$$\mathrm{Mat}(f) \overset{\text{def}}{=} \begin{pmatrix} 2c_{1,1} & c_{1,2} & c_{1,3} & \ldots & c_{1,k} \\ c_{1,2} & 2c_{2,2} & c_{2,3} & \ldots & c_{2,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{1,k} & c_{2,k} & c_{3,k} & \ldots & 2c_{k,k} \end{pmatrix},$$

which is skew-symmetric, i.e symmetric with a zero diagonal, when $\mathbb{F}$ has characteristic 2. We may thus define the code of matrices

$$\mathscr{C}_{\mathrm{mat}}(\mathcal{V}) \overset{\text{def}}{=} \{\mathrm{Mat}(f) \mid f \in \mathscr{C}_{rel}(\mathcal{V})\}.$$

This link between quadratic forms and matrices is a powerful tool for analyzing quadratic relations. For instance, the rank of the matrix of a quadratic form may provide insightful information about the "*shortness*" of the form. In the following of this work, we may refer to the ranke of $\mathrm{Mat}(f)$ as the *rank* of the quadratic form f.
We recall that a lot of interesting features of the code of relations remain invariant under a change of basis.

Lemma 1 ([CMT23b], Proposition 4).

$$\dim \mathscr{C}_{mat}(\mathcal{V}) = \dim \mathscr{C}_{rel}(\mathcal{V}).$$

Furthermore, $\dim \mathscr{C}_{rel}(\mathcal{V})$ and the rank distribution of $\mathscr{C}_{mat}(\mathcal{V})$ are invariant under a change of basis.

As a consequence, we sometimes write $\mathscr{C}_{\mathrm{rel}}$ or $\mathscr{C}_{\mathrm{mat}}$ without specifying the basis when we refer to invariants.

3 Codes of relations of a generalized Reed-Solomon code

The key for understanding $\mathrm{HF}_{\mathrm{A}}(2)$ will be to treat the case $m = 1$ first, *i.e.* when the alternant code is actually a generalized Reed-Solomon code.

3.1 Fundamental relations in the canonical basis

The behavior of $\mathscr{C}_{\mathrm{rel}}$ for a GRS code is easily seen using the very structured basis of these codes that we introduce in the following.

Definition 7 (Canonical basis). *$\mathcal{A} = (\boldsymbol{a}_0, \dots, \boldsymbol{a}_{r-1})$, where $\boldsymbol{a}_i = \boldsymbol{x}^i\boldsymbol{y}$ forms a basis of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$, which we call a canonical basis.*

The codewords of a canonical basis $\mathcal{A}$ are subject to very simple quadratic relations, that we will call *fundamental.*

Definition 8 (Fundamental relations). *We define the space of* ***fundamental quadratic forms*** *as*

$$\mathcal{F}_r \overset{def}{=} \left\langle x_i x_j - x_k x_l \mid 0 \leqslant i, j, k, l < r,\ \ i + j = k + l \right\rangle_{\mathbb{F}_q}.$$

It turns out that

Proposition 1. $\dim \mathcal{F}_r = \binom{r-1}{2}$.

Proof. Consider the Veronese embedding

$$\nu : \begin{cases} \mathbb{P}^1 & \longrightarrow \mathbb{P}^{r-1} \\ (x : y) & \longmapsto (y^{r-1} : xy^{r-2} : \dots : x^{r-1}), \end{cases}$$

and define $\mathcal{Y}$ as the image of ν. Clearly the ideal generated by $\mathcal{F}_r$ is a subset of the ideal of $\mathcal{Y}$. Besides, it is well-known (see [Ver82]) that the ideal of $\mathcal{Y}$ is given by the determinental ideal generated by the 2×2 minors of the following $2 \times (r - 1)$ matrix

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{r-2} \\ x_1 & x_2 & \dots & x_{r-1} \end{pmatrix}. \tag{3}$$

Since each of these minors actually belong to $\mathcal{F}_r$, we conclude that the ideal generated $\mathcal{F}_r$ is the same as the above-mentioned determinental ideal, *i.e* the ideal of $\mathcal{Y}$. Their homogeneous component of degree 2 coincide as well, one being given by $\mathcal{F}_r$ exactly, the other one being spanned by the $\binom{r-1}{2}$ minors of size 2×2 of (3). Therefore we only need to show that these minors are linearly independant to prove the proposition. Assuming they are not, there must exist two indices $i < j$ such that the minor

$$\begin{vmatrix} x_i & x_j \\ x_{i+1} & x_{j+1} \end{vmatrix} = x_i x_{j+1} - x_{i+1} x_j$$

is a linear combination of other minors of (3). Now consider the polynomial matrix

$$\begin{pmatrix} x_0 \dots x_{i-1} \; x_{i+1} \dots x_{j-1} \; x_{j+1} \dots x_{r-2} \\ x_1 \dots \; x_i \;\; x_{i+2} \dots \;\; x_j \;\; x_{j+2} \dots x_{r-1} \end{pmatrix},$$

which is nothing but (3) where columns i and j have been removed. Our assumption implies that if the above matrix is of rank < 2, then so is (3). Note that this is the case if and only if the two rows are proportional. For (3), this translates into the x_i's being in geometric progression, but not for the submatrix given above, since its two rows being proportional does not require x_{i+1} to be a multiple of x_i. One may therefore choose a specialization (which may lie in an extension of $\mathbb{F}$) where the rows of the submatrix are proportional without the rows of (3) being proportional. The submatrix would have rank < 2 while (3) would not. This contradicts the minor produced by columns i, j being linearly dependant from the others. □

It is readily seen that whenever $\mathcal{A}$ is a canonical basis of some GRS code, then $\mathcal{F}_r \subseteq \mathscr{C}_{\mathrm{rel}}(\mathcal{A})$. The following proposition gives a condition for the last inclusion to be an equality.

Proposition 2. *If $2r - 1 \leqslant n$, then $\mathscr{C}_{rel}(\mathcal{A}) = \mathcal{F}_r$.*

Proof. We first recall that $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2r-1}(\boldsymbol{x}, \boldsymbol{y}^2)$. We have

$$\begin{aligned} \dim \mathscr{C}_{\mathrm{rel}}(\mathcal{A}) &= \binom{r+1}{2} - \dim \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} \;\; \text{(by Proposition 5 of [CMT23b])} \\ &= \frac{1}{2} r(r+1) - (2r-1) \;\; \text{(by (1))} \\ &= \frac{1}{2}(r^2 - 3r + 2) \\ &= \frac{1}{2}(r-1)(r-2) \\ &= \binom{r-1}{2}. \end{aligned}$$

By Proposition 1, $\mathcal{F}_r$ is a subspace of $\mathscr{C}_{\mathrm{rel}}(\mathcal{A})$ of codimension 0, *i.e* $\mathscr{C}_{\mathrm{rel}}(\mathcal{A}) = \mathcal{F}_r$. □

We are therefore interested in the vector space $\mathcal{F}_r$. One could write a basis of $\mathcal{F}_r$ using the determinental ideal introduced in the proof of Propositon 1. We will use a different method so as to extract a basis from the generators of $\mathcal{F}_r$ which give a nice structure to the matrix space spanned by the matrices of the fundamental quadratic forms. Start with the following decomposition

$$\mathcal{F}_r = \bigoplus_{s=2}^{2r-4} \mathcal{F}_{r,s},$$

where $\mathcal{F}_{r,s} \overset{\text{def}}{=} \langle x_i x_j - x_k x_l \mid 0 \leqslant i,j,k,l < r, \; i+j = k+l = s \rangle_{\mathbb{F}_q}$. The indices of the sum run from 2 to $2r-4$ since $\mathcal{F}_{r,s} = \{0\}$ when s is outside this range.

To write a basis of $\mathcal{F}_r$, it suffices to write a basis of $\mathcal{F}_{r,s}$ for all possible values of s. To this end, our idea is to first choose $k \leqslant l$ as close to $\lfloor \frac{s}{2} \rfloor$ as possible, then choose the lowest i and the greatest j such that $i + j = s$. A basis of $\mathcal{F}_{r,s}$ will then be given by the sequence $(x_{i+t}x_{j-t} - x_k x_l)_{0 \leqslant t < k-i}$. The first bases may be found in the following table.

value of s	Basis of $\mathcal{F}_{r,s}$
2	$x_0x_2 - x_1^2$
3	$x_0x_3 - x_1x_2$
4	$x_0x_4 - x_2^2,\ x_1x_3 - x_2^2$
$\vdots$	$\ldots$

Table 1. Basis of $\mathcal{F}_{r,s}$ for the first values of s.

More formally, we get a basis of $\mathcal{F}_r$ by running Algorithm 1.

Algorithm 1 Generation of a basis $\mathcal{B} = (f_1, \ldots, f_N)$ of $\mathcal{F}_r$

```
Input: an integer $r \geqslant 3$
Output: A basis $(f_1, \ldots, f_N)$ of $\mathcal{F}_r$        $\rhd\ N = \binom{r-1}{2}$.
$\mathcal{B} \leftarrow \varnothing$
$s \leftarrow 2$
while $s \leqslant 2r - 4$ do
    $i \leftarrow \max\{0, s - r + 1\}$
    $j \leftarrow s - i$
    if $s \mod 2 = 0$ then
        $k \leftarrow s/2$
        $l \leftarrow s/2$
    else
        $k \leftarrow \frac{s-1}{2}$
        $l \leftarrow \frac{s+1}{2}$
    $\mathcal{B} \leftarrow \mathcal{B} \cup \{x_{i+t}x_{j-t} - x_k x_l \mid 0 \leqslant t < k - i\}$
    $s \leftarrow s + 1$
return $\mathcal{B}$
```

Theorem 1. *Algorithm 1 generates a basis of $\mathcal{F}_r$.*

Proof. Let $F = \{f_1, \ldots, f_N\}$ be the sequence of quadratic forms returned by Algorithm 1. Let us prove that F generates $\mathcal{F}_r$. Consider a nonzero quadratic form $f = x_i x_j - x_k x_l$ such that $i + j = k + l = s$. Without loss of generality, we may assume $i < j$ and $k \leqslant l$. If $l - k \in \{0, 1\}$, then f actually is an element of

F. Now suppose that $l - k \geqslant 2$, and define k', l' by

$$(k', l') = \begin{cases} \left(\frac{s}{2}, \frac{s}{2}\right) & \text{if } s \mod 2 = 0 \\ \left(\frac{s-1}{2}, \frac{s+1}{2}\right) & \text{otherwise.} \end{cases}$$

We notice that both $g = x_i x_j - x_{k'} x_{l'}$ and $h = x_k x_l - x_{k'} x_{l'}$ belong to F, and that $f = g - h$. Therefore F is a *generating set* of $\mathcal{F}_r$.
Now, for each quadratic form $f = x_i x_j - x_k x_l \in F$, with $i < j$ and $k \leqslant l$, we see that f is *the only* quadratic form in F having $x_i x_j$ among its monomials. This implies that the elements of F are linearly independent. □

Combining Proposition 2 and Theorem 1, we get

Corollary 1. *When $2r - 1 \leqslant n$, Algorithm 1 returns a basis of $\mathscr{C}_{rel}(\mathcal{A})$.*

The reason why we wrote this algorithm instead of simply considering the determinental ideal will be clarified in Remark 2.

3.2 Rank 2 matrices in $\mathscr{C}_{\mathbf{mat}}$

Among the fundamental relations, the ones of the form

$$x_i x_j - x_k^2,$$

when $i + j = 2k$, give a matrix of rank 2 when the base field $\mathbb{F}_q$ of S_r is of characteristic 2. This suggests that there are many quadratic relations of rank 2 in $\mathscr{C}_{\text{mat}}$. We may detect this interesting feature of the matrix code of relations related to a GRS code using an algebraic system.

Implicit modeling of [CMT23b]. To find rank 2 matrices in $\mathscr{C}_{\text{mat}}$, we may adopt the inverse point of view, *i.e* finding matrices belonging to $\mathscr{C}_{\text{mat}}$ inside the variety of skew-symmetric matrices of rank $\leqslant 2$. To describe this variety, we first recall the following fact.

Fact 1 *Let $\boldsymbol{A} = (a_{i,j})_{1 \leqslant i,j \leqslant n}$ be a square matrix in characteristic 2 such that $a_{i,j} = a_{j,i}$ for all i, j, and $a_{i,i} = 0$ for all i. Then the determinant of A can be expressed as the square of a polynomial expression in the coefficients $a_{i,j}$. This polynomial is 0 if n is odd, and has degree $n/2$ otherwise. We denote with $\mathbf{Pf}(\boldsymbol{A})$ this polynomial expression, and call it the Pfaffian of $\boldsymbol{A}$. For example,*

$$\mathbf{Pf}\begin{pmatrix} 0 & a & b & c \\ a & 0 & d & e \\ b & d & 0 & f \\ c & e & f & 0 \end{pmatrix} = af + be + dc.$$

We will now describe the algebraic variety of rank $\leqslant 2$ skew-symmetric matrices in characteristic 2. To begin with, write the generic skew-symmetric matrix

$$\boldsymbol{M} = \begin{pmatrix} 0 & X_{1,2} & \dots & X_{1,r} \\ X_{1,2} & 0 & \dots & X_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ X_{1,r} & X_{2,r} & \dots & 0 \end{pmatrix}.$$

We know that the variety of rank $\leqslant 2$ skew-symmetric matrices in characteristic 2 may be described by the following equations [Wim12]:

$$X_{i,j}X_{k,l} + X_{i,k}X_{j,l} + X_{i,l}X_{j,k} = 0,\ 1 \leqslant i < j < k < l \leqslant r. \tag{4}$$

The left-hand side of Equation (4) is nothing but the Pfaffian of the submatrix of $\boldsymbol{M}$ obtained by taking rows and columns indexed by i, j, k, l. This is why we will call it a Pfaffian of $\boldsymbol{M}$. More generally, if $\boldsymbol{N}$ is any skew-symmetric matrix whose coefficients lie in some polynomial ring, we denote by $\mathbf{Pf}(\boldsymbol{N}, 2)$ the set of polynomials given by the Pfaffians of all submatrices of size 4×4 extracted from $\boldsymbol{N}$ using the same set of indices for rows and columns (such submatrices are sometimes called *principal* submatrices). Adding linear equations expressing the fact that $\boldsymbol{M}$ belongs to $\mathscr{C}_{\text{mat}}$, we obtain the first algebraic modeling of rank $\leqslant 2$ matrices in $\mathscr{C}_{\text{mat}}$:

Modeling 2 (Implicit modeling) *The implicit modeling of rank $\leqslant 2$ matrices in $\mathscr{C}_{mat}$ consists of the ideal I generated by the $\binom{r}{4}$ Pfaffians of the generic skew-symmetric $r \times r$ matrix $\boldsymbol{M}$ and parity-check equations expressing the fact that $\boldsymbol{M}$ belongs to $\mathscr{C}_{mat}$.*

Remark 1. We call this modeling *implicit* because the matrix code is defined through implicit (*i.e* parity-check) equations. In the following section, we will detail another algebraic modeling, called *explicit*, because in this modeling the matrix code is defined by a parametrization.

Explicit modeling. Another strategy is to compute a basis $(\boldsymbol{B}_1, \dots, \boldsymbol{B}_N)$ of $\mathscr{C}_{\text{mat}}$ and solve algebraically the MinRank problem with matrix

$$\boldsymbol{M} \overset{\text{def}}{=} \sum_{i=1}^{N} X_i \boldsymbol{B}_i \tag{5}$$

by writing that all the Pfaffians corresponding to the 4×4 principal minors are zero. For example, when $\mathscr{C}_{\text{mat}}$ is the matrix code of relations of a square-distinguishable GRS code of dimension r with respect to a canonical basis, the matrices $\boldsymbol{B}_i$ may be taken as the matrices of the quadratic forms f_i returned by

Algorithm 1. Here are a few examples of $\boldsymbol{M}$ for small values of r in such a case.

$$\underset{(r=5)}{\boldsymbol{M}} = \begin{pmatrix} 0 & 0 & X_1 & X_2 & X_4 \\ 0 & 0 & X_2 & X_3 & X_5 \\ X_1 & X_2 & 0 & X_5 & X_6 \\ X_2 & X_3 & X_5 & 0 & 0 \\ X_4 & X_5 & X_6 & 0 & 0 \end{pmatrix}, \underset{(r=6)}{\boldsymbol{M}} = \begin{pmatrix} 0 & 0 & X_1 & X_2 & X_4 & X_6 \\ 0 & 0 & X_2 & X_3 & X_5 & X_8 \\ X_1 & X_2 & 0 & X_5 + X_6 & X_7 & X_9 \\ X_2 & X_3 & X_5 + X_6 & 0 & X_9 & X_{10} \\ X_4 & X_5 & X_7 & X_9 & 0 & 0 \\ X_6 & X_8 & X_9 & X_{10} & 0 & 0 \end{pmatrix},$$

$$\underset{(r=8)}{\boldsymbol{M}} = \begin{pmatrix} 0 & 0 & X_1 & X_2 & X_4 & X_6 & X_9 & X_{12} \\ 0 & 0 & X_2 & X_3 & X_5 & X_8 & X_{11} & X_{15} \\ X_1 & X_2 & 0 & X_5 + X_6 & X_7 & X_{10} & X_{14} & X_{17} \\ X_2 & X_3 & X_5 + X_6 & 0 & X_{10} + X_{11} + X_{12} & X_{13} & X_{16} & X_{19} \\ X_4 & X_5 & X_7 & X_{10} + X_{11} + X_{12} & 0 & X_{16} + X_{17} & X_{18} & X_{20} \\ X_6 & X_8 & X_{10} & X_{13} & X_{16} + X_{17} & 0 & X_{20} & X_{21} \\ X_9 & X_{11} & X_{14} & X_{16} & X_{18} & X_{20} & 0 & 0 \\ X_{12} & X_{15} & X_{17} & X_{19} & X_{20} & X_{21} & 0 & 0 \end{pmatrix}.$$

These matrices have a very special shape that is produced on purpose by Algorithm 1:

Remark 2. When $\boldsymbol{M}$ is written using the matrices returned by Algorithm 1,

- the coefficient of $\boldsymbol{M}$ at (i, j) is a single variable, unless $i = j \pm 1$;
- any variable X_i appears in exactly one anti-diagonal of $\boldsymbol{M}$;
- when the coefficient of $\boldsymbol{M}$ at (i, j) is not a single variable (*i.e* $i = j \pm 1$), it actually is nothing but the sum of all variables appearing in the same anti-diagonal defined by $i' + j' = i + j$.

These remarks will be crucial in the proof of Theorem 3 thereafter. Let us now detail the explicit modeling. The matrix $\boldsymbol{M}$ is the generic matrix in $\mathscr{C}_{\text{mat}}$. Since it is skew-symmetric, one may consider its Pfaffians of degree 2, *i.e* the Pfaffians of all 4×4 principal submatrices of $\boldsymbol{M}$, which leads to the following algebraic modeling.

Modeling 3 (Explicit Pfaffian modeling) *The explicit modeling consists of* $\binom{r}{4}$ *equations* $f = 0$ *for* $f \in \mathbf{Pf}(\boldsymbol{M}, 2)$. *More explicitly, writing* $\boldsymbol{M} = (m_{i,j})_{1 \leqslant i,j \leqslant r}$, *the equations are*

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

where each coefficient $m_{i,j}$ *is a polynomial of degree 1.*

We are interested in computing the Hilbert function at degree 2 of the ideal generated by $\mathbf{Pf}(\boldsymbol{M}, 2)$. We recall the concept of Hilbert function.

Definition 9 (Hilbert function). *Let* I *be a homogeneous ideal of a polynomial ring* $\mathbb{F}[\boldsymbol{X}]$. *Writing* $\mathbb{F}[\boldsymbol{X}]_d$ *the (finite dimensional)* $\mathbb{F}$*-vector space spanned by monomials of degree* d *and* $I_d = I \cap \mathbb{F}[\boldsymbol{X}]_d$, *the Hilbert function of* I *is defined as*

$$\mathrm{HF}_{\mathbb{F}[\boldsymbol{X}]/I}(d) \overset{def}{=} \dim_{\mathbb{F}} \mathbb{F}[\boldsymbol{X}]_d / I_d, \ d \in \mathbb{N}.$$

Experimentally, we always find that the elements of $\mathbf{Pf}(\boldsymbol{M},2)$ are linearly independent when $2r-1 \leqslant n$, *i.e* when the matrix $\boldsymbol{M}$ is the generic matrix in the matrix space of fundamental relations. This leads us to state the following as a conjecture.

Conjecture 1. When $2r-1 \leqslant n$, the Hilbert function at degree 2 for the explicit Pfaffian modeling for rank $\leqslant 2$ matrices in $\mathscr{C}_{\mathrm{mat}}$ is given by

$$\mathrm{HF}(2) = \binom{\binom{r-1}{2}+1}{2} - \binom{r}{4} = \frac{1}{12}(r-1)(r-2)(r^2-3r+6).$$

Remark 3. We emphasize that the generic matrix $\boldsymbol{M}$ in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ obtained by taking the matrices of the forms f_i's returned by Algorithm 1 only depends on r. Therefore, Conjecture 1 may be checked easily for all parameters r, q used in cryptography.

We have introduced two algebraic modelings for solving the same problem: finding rank $\leqslant 2$ matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ when $\mathcal{A}$ is a canonical basis of some GRS code. However, since the Hilbert function strongly depends on how the equations are written, one must be careful when changing the modeling. In our case, we can safely do so thanks to the following theorem.

Theorem 2. *Let I (resp. J) be the ideal of the polynomial ring $\boldsymbol{R}$ (resp. $\boldsymbol{S}$) produced by the implicit (resp. explicit) modeling. $\boldsymbol{R}/I$ and $\boldsymbol{S}/J$ both have a structure of graded $\mathbb{F}$-algebra. There exists a map*

$$\Phi : \boldsymbol{R}/I \longrightarrow \boldsymbol{S}/J$$

that defines an isomorphism of graded $\mathbb{F}$-algebras.

This theorem is proved in the appendix. Note that it implies that the Hilbert function of the (implicit or explicit) Pfaffian modeling is also invariant under a change of basis. In the following, we sometimes talk about *the Pfaffian modeling associated with a code* without specifying whether it is implicit or explicit, since we only deal with Hilbert functions.

4 Hilbert function of a Pfaffian ideal associated with a generic alternant code

4.1 The block-diagonal code of relations

In the case of alternant codes, the crux for having rank 2 matrices in $\mathscr{C}_{\mathrm{mat}}$ is to consider [CMT23b] the extension to $\mathbb{F}_{q^m}$ of the *dual* code. Let us then recall the following fact.

Proposition 3 ([BMT24], Proposition 14). *For any code $\mathscr{C} \subseteq \mathbb{F}_q^n \subseteq \mathbb{F}_{q^m}^n$, we denote by $\mathscr{C}_{\mathbb{F}_{q^m}}$ the $\mathbb{F}_{q^m}$-vector space spanned by $\mathscr{C}$. Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})$ be an alternant code of extension degree m. Then*

$$(\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^\perp)_{\mathbb{F}_{q^m}} = \sum_{j=0}^{m-1} \mathbf{GRS}_r(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j}).$$

With the usual assumption that $\dim_{\mathbb{F}_q} \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) = n - rm$*, the above sum becomes a direct sum and the sequence* $\mathcal{A} = (\boldsymbol{a}_0, \dots, \boldsymbol{a}_{r-1}, \boldsymbol{a}_0^q, \dots, \boldsymbol{a}_{r-1}^q, \dots, \boldsymbol{a}_{r-1}^{q^{m-1}})$ *is a basis of* $(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp)_{\mathbb{F}_{q^m}}$*, called the* ***canonical basis****.*

When $r < q+1$, it follows from the analysis of [FGO⁺11] that $\mathscr{C}_{\mathrm{rel}}(\mathcal{A})$ is spanned by

$$x_{rl+a}x_{rl+b} - x_{rl+c}x_{rl+d}$$

for $0 \leqslant l < m$ and $0 \leqslant a, b, c, d < r$ such that $a + b = c + d$. This implies that any matrix $\boldsymbol{A} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ has a block-diagonal structure, *i.e.*

$$\boldsymbol{A} = \boldsymbol{A}_0 \oplus \dots \oplus \boldsymbol{A}_{m-1} \stackrel{\mathrm{def}}{=} \begin{pmatrix} \boldsymbol{A}_0 & \dots & \boldsymbol{0}_r \\ \vdots & \ddots & \vdots \\ \boldsymbol{0}_r & \dots & \boldsymbol{A}_{m-1} \end{pmatrix}$$

where $\boldsymbol{A}_j \in \mathscr{C}_{mat}(\boldsymbol{a}_0^{q^i}, \dots, \boldsymbol{a}_{r-1}^{q^j})$ is the matrix associated with some element of the code of quadratic relations of $\mathbf{GRS}_r(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$ with respect to its canonical basis.

Remark 4. In other words, when $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_0^q, \dots, \mathcal{A}_0^{q^{m-1}})$ where $\mathcal{A}_0 = (\boldsymbol{y}, \dots, \boldsymbol{x}^{r-1}\boldsymbol{y})$, we have $\mathscr{C}_{\mathrm{mat}}(\mathcal{A}) \simeq \mathscr{C}_{\mathrm{mat}}(\mathcal{A}_0)^m$, the isomorphism being given explicitly by

$$\begin{cases} \mathscr{C}_{\mathrm{mat}}(\mathcal{A}_0)^m & \longrightarrow \mathscr{C}_{\mathrm{mat}}(\mathcal{A}) \\ (\boldsymbol{A}_0, \dots, \boldsymbol{A}_{m-1}) & \longmapsto \boldsymbol{A}_0 \oplus \dots \oplus \boldsymbol{A}_{m-1}. \end{cases}$$

4.2 The Hilbert function at degree 2

The authors of [CMT23b] noticed that the Hilbert function of the Pfaffian modeling at degree 1 can be used as a distinguisher that boils down to the one presented in [FGO⁺11]. We recall that a generic alternant code is *square-distinguishable* if it is 1-distinguishable in the sense of [CMT23b]. The Hilbert function at degree 2 can also be used as a distinguisher which seems to work on a larger range of parameters. Our goal here is to find a formula for HF(2) when the code is square-distinguishable, assuming $r < q + 1$. In such a regime, all matrices in the matrix code of relations associated to a canonical basis $\mathcal{A}$ are block-diagonal in the generic alternant case. Therefore, so is the generic matrix $\boldsymbol{M}$ in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$. More precisely, it can be written like

$$\boldsymbol{M} = \begin{pmatrix} \boldsymbol{M}_0 & \dots & \boldsymbol{0}_r \\ \vdots & \ddots & \vdots \\ \boldsymbol{0}_r & \dots & \boldsymbol{M}_{m-1} \end{pmatrix} \in \mathbb{F}_{q^m}[X_i \mid 1 \leqslant i \leqslant mN]^{rm \times rm}, \tag{6}$$

where each $\boldsymbol{M}_i = X_{Ni+1}B_1 + \dots + X_{(N+1)i}B_N$ and where the B_j's stand for the matrices of the quadratic forms f_j's returned by Algorithm 1. For such a block-diagonal structure, computing the Hilbert function at degree 2 becomes doable.

Theorem 3. *Assume that Conjecture 1 holds. Let $\boldsymbol{M}$ be the generic matrix of Equation (6). The Hilbert function HF_A at degree 2 of the ideal generated by $\mathbf{Pf}(\boldsymbol{M}, 2)$ is given by*

$$\mathrm{HF}(2) = \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

Proof. Here we use the explicit modeling for performing the analysis. The theorem is thus about the dimension of the vector space spanned by $\mathbf{Pf}(\boldsymbol{M}, 2)$. We will describe all the nonzero elements of $\mathbf{Pf}(\boldsymbol{M}, 2)$ and inspect their linear dependencies. To do so, we will consider 4 cases. If $1 \leqslant i_1 < \ldots < i_p$, the notation $\boldsymbol{M}[i_1, \ldots, i_p]$ denotes the extracted matrix of $\boldsymbol{M}$ where rows *and* columns $i_1, \ldots, i_p$ have been taken. Let $1 \leqslant i < j < k < l \leqslant rm$.

- *Case 1: the submatrix $\boldsymbol{M}[i,j,k,l]$ is a submatrix of some $\boldsymbol{M}_s$.* The corresponding Pfaffian of $\boldsymbol{M}$ is actually a Pfaffian of $\boldsymbol{M}_s$. Conjecture 1 states that these polynomials are linearly independent. Moreover, the Pfaffians of different blocks $\boldsymbol{M}_s, \boldsymbol{M}_t$ are linearly independent since they are polynomials in different variables.
- *Case 2: the submatrix $\boldsymbol{M}[i,j]$ is a submatrix of some $\boldsymbol{M}_s$ and the submatrix $\boldsymbol{M}[k,l]$ is a submatrix of some $\boldsymbol{M}_t$ with $s < t$, and no coefficient is taken right above/under the diagonal.* In such a case, the submatrix has the form

  $$\boldsymbol{M}[i,j,k,l] = \begin{pmatrix} 0 & X_a & 0 & 0 \\ X_a & 0 & 0 & 0 \\ 0 & 0 & 0 & X_b \\ 0 & 0 & X_b & 0 \end{pmatrix}$$

  with $Ns+1 \leqslant a < (N+1)s$, $Nt+1 \leqslant b < (N+1)t$ and its Pfaffian is X_aX_b. Indeed, the coefficients $m_{i,k}$ and $m_{j,l}$ are 0 because of the block-diagonal structure, and $m_{i,j}$ and $m_{k,l}$ are single variables since $i \neq j \pm 1$ and $k \neq l \pm 1$ (see Section 3).This gives $N \times \binom{m}{2}$ polynomials that are linearly independent. They are also not in the vector space spanned by the polynomials of case 1 since none of the latter polynomials have a monomial in common with the Pfaffians of case 2.
- *Case 3: same as case 2, but some coefficients may be taken right above/under the diagonal.* The thing here is that there is no simple way to express the corresponding coefficients, as they might be sums of variables and not variables alone. However, as we noticed in Section 3, when a coefficient of $\boldsymbol{M}$ is not a single variable, then it is the sum of other coefficients of $\boldsymbol{M}$ that *are* single variables. Each time some coefficient of $\boldsymbol{M}$ is a sum of variables, all variables appearing in the coefficient also appear alone in the same anti-diagonal. In other words, we may have to consider some Pfaffians of the form

  $$\mathbf{Pf}(\boldsymbol{M}[i,j,k,l]) = \mathbf{Pf}\begin{pmatrix} 0 & \alpha & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta \\ 0 & 0 & \beta & 0 \end{pmatrix} = \alpha(X_{sN+1}, \ldots, X_{(s+1)N}) \times \beta(X_{tN+1}, \ldots, X_{(t+1)N})$$

where α, β are degree-1 polynomials of the appropriate variables. We see that the Pfaffian we obtain is a linear combination of the Pfaffians obtained in case 2, hence they do not change the dimension of the Pfaffian ideal at degree 2.

- *Case 4: at least one of the indices i, j, k, l is alone in its range* $[\![sN+1, (s+1)N]\!]$, say i. In this case, the first column of the corresponding submatrix is zero, hence its Pfaffian itself is zero.

The Hilbert function at degree 2 is the number of monomials of degree 2 minus the number of algebraically independent Pfaffians of $\boldsymbol{M}$. Among all monomials of degree 2, we have the monomials $X_a X_b$ where the variables X_a, X_b do not appear in the same submatrix $\boldsymbol{M}_s$. We saw in case 2 that these monomials appear in the Pfaffians of $\boldsymbol{M}$. All the other monomials are of the form $X_a X_b$ where X_a and X_b *do* appear in the same block. For each block $\boldsymbol{M}_s$, the number of monomials $X_a X_b$ minus the number of algebraically independant Pfaffians of $\boldsymbol{M}_s$ is exactly given by $\dfrac{1}{12}(r-1)(r-2)(r^2-3r+6)$, as stated in Conjecture 1. Since there are m blocks, we conclude that

$$HF(2) = \frac{m}{12}(r-1)(r-2)(r^2-3r+6)$$

Which ends the proof. □

Corollary 2. *Let $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ be a* ***generic*** *square-distinguishable alternant code with $r < q+1$. If Conjecture 1 holds, then the Hilbert function at degree 2 associated with the (implicit or explicit) Pfaffian modeling for rank $\leqslant 2$ matrices in $\mathscr{C}_{mat}$ is given by*

$$\mathrm{HF}_A(2) = \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

Proof. With the genericity and square-distinguishability assumptions, the generic matrix in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$ is the one described in Equation (6). Therefore the corollary follows directly from Theorem 3.

Corollary 2 requires Conjecture 1 to hold, and is also limited to the case $r < q+1$. Indeed, equality cannot be claimed in general, because there might exist alternant codes for which additional relations occur. Analogously to previous results on the Hilbert function at degree 1 [MT23], the value provided by Theorem 3 for degree 2 still represents a lower bound.

Corollary 3. *The Hilbert function of the Pfaffian modeling associated with an alternant code of order r and extension degree m satisfies*

$$\mathrm{HF}_A(2) \geqslant \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

Before proving Corollary 3, we need a pair of auxiliary results.

Lemma 2. *Let $\boldsymbol{X} = (X_1, \ldots, X_a)$ and $\boldsymbol{Y} = (Y_1, \ldots, Y_b)$ be two vectors of variables. Let M, N be two $s \times t$ matrices whose entries are linear homogeneous polynomials in $\mathbb{F}[\boldsymbol{X}], \mathbb{F}[\boldsymbol{X}, \boldsymbol{Y}]$ respectively and such that*

$$n_{i,j}(\boldsymbol{X}, \boldsymbol{Y}) = m_{i,j}(\boldsymbol{X}) + l_{i,j}(\boldsymbol{Y}).$$

Let $f(\boldsymbol{Z})$ be a multivariate polynomial function over a field $\mathbb{F}$, where the variables are viewed as the entries $z_{i,j}$ of an $s \times t$ matrix $\boldsymbol{Z}$. Let $\langle Y_i \rangle_i \subset \mathbb{F}[\boldsymbol{X}, \boldsymbol{Y}]$ the ideal generated by $\boldsymbol{Y}$'s variables.

$$f(N) - f(M) \in \langle Y_i \rangle_i$$

Proof. Let $f(\boldsymbol{Z}) = \sum_{\boldsymbol{a} \in A} \alpha_{\boldsymbol{a}} \boldsymbol{Z}^{\boldsymbol{a}}$, where A is a finite subset of $\mathbb{N}^{s \times t}$ and $\alpha_{\boldsymbol{a}} \in \mathbb{F}$ and we define $\boldsymbol{Z}^{\boldsymbol{a}} = \prod_{i,j} z_{i,j}^{a_{i,j}}$. Similarly we write

$$M^{\boldsymbol{a}} \overset{\text{def}}{=} \prod_{i,j} m_{i,j}^{a_{i,j}}$$
$$N^{\boldsymbol{a}} \overset{\text{def}}{=} \prod_{i,j} n_{i,j}^{a_{i,j}}$$

When the input is N, we obtain

$$f(N) = \sum_{\boldsymbol{a} \in A} \alpha_{\boldsymbol{a}} N^{\boldsymbol{a}} = \sum_{\boldsymbol{a} \in A} \alpha_{\boldsymbol{a}} \prod_{i,j} (m_{i,j} + l_{i,j}(\boldsymbol{Y}))^{a_{i,j}}.$$

By expanding the product, we obtain

$$f(N) = \left(\sum_{\boldsymbol{a} \in A} \alpha_{\boldsymbol{a}} M^{\boldsymbol{a}} \right) + g(\boldsymbol{X}, \boldsymbol{Y})$$

where each monomial appearing in g is a multiple of at least a variable y_i. Therefore

$$f(N) - f(M) = g(\boldsymbol{X}, \boldsymbol{Y}) \in \langle Y_i \rangle_i .$$

□

The previous lemma can be used to show that the Hilbert function for the Pfaffian ideal can only increase by letting the underlying matrix code grow.

Lemma 3. *Let $\mathbb{F}$ be a finite field of characteristic 2. Let $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_l \in \mathbb{F}^{s \times t}$ be linearly independent (skew-)symmetric matrices and $\mathscr{C} = \langle \boldsymbol{M}_1, \ldots, \boldsymbol{M}_l \rangle_{\mathbb{F}}, \mathscr{C}' = \langle \boldsymbol{M}_1, \ldots, \boldsymbol{M}_{l'} \rangle_{\mathbb{F}} \subseteq \mathbb{F}^{s \times t}$ with $l' < l$ be two matrix codes. Let $\mathcal{I} \subseteq \mathbb{F}[X_1, \ldots, X_l]$ (resp. $\mathcal{I}' \subseteq \mathbb{F}[X_1, \ldots, X_{l'}]$) be the Pfaffian ideal corresponding to the explicit modeling for $\mathscr{C}$ (resp. $\mathscr{C}'$) expressing that the entries of an element of the matrix code is of rank $\leqslant 2$. Then for all $d \in \mathbb{N}$,*

$$\mathrm{HF}_{\mathbb{F}[X_1, \ldots, X_l]/\mathcal{I}}(d) \geqslant \mathrm{HF}_{\mathbb{F}[X_1, \ldots, X_l']/\mathcal{I}'}(d)$$

Proof. Pfaffians of order 4 are homogeneous polynomial in the matrix entries. Therefore, from Lemma 2, any element P of the Pfaffian ideal $\mathcal{I} \subseteq \mathbb{F}[X_1, \ldots, X_l]$ can be written as an element of $\mathcal{I}' + \langle X_{l'+1}, \cdots, X_l \rangle$, thus $P \subseteq \mathcal{I}' + \langle X_{l'+1}, \cdots, X_l \rangle$, or equivalently

$$\mathbb{F}[X_1, \ldots, X_l]/\mathcal{I} \supseteq \mathbb{F}[X_1, \ldots, X_l]/(\mathcal{I}' + \langle X_{l'+1}, \cdots, X_l \rangle) \simeq \mathbb{F}[X_1, \ldots, X_l']/\mathcal{I}'.$$

By definition of Hilbert series, we obtain

$$\mathrm{HF}_{\mathbb{F}[X_1,\ldots,X_l]/\mathcal{I}}(d) \geqslant \mathrm{HF}_{\mathbb{F}[X_1,\ldots,X_l']/\mathcal{I}'}(d)$$

for any degree d. □

With Lemma 3 at hand, we can finally prove Corollary 3.

Proof (of Corollary 3.). Even without the condition $r < q + 1$ (resp. $r < q - 1$) for the degree of an alternant (resp. Goppa) code and without Conjecture 1, the matrix code $\mathscr{C}$ of relationships still contains the block-diagonal matrix code generated by the matrices corresponding to the fundamental relations. Let $\mathscr{C}'$ be the space spanned by such matrices and for which Theorem 3 provides the value of the Hilbert function at degree 2 as

$$\frac{m}{12}(r-1)(r-2)(r^2 - 3r + 6).$$

Since $\mathscr{C}' \subseteq \mathscr{C}$, from Lemma 3, we derive

$$\mathrm{HF}_{\mathbb{F}[\boldsymbol{X}]/\mathcal{I}}(2) \geqslant \frac{m}{12}(r-1)(r-2)(r^2 - 3r + 6).$$

□

Corollary 3 allows us to state when a generic alternant code is 2-distinguishable. We use here the following definition of d-distinguishability

Definition 10. *An alternant code is d-distinguishable if the associated Hilbert function HF_A satisfies*

$$\mathrm{HF}_A(d) > \mathrm{HF}_R(d)$$

where HF_R is the Hilbert series of a random linear code of the same length and dimension as the alternant code.

Corollary 4. *If $\mathrm{HF}_R(2) < \frac{m}{12}(r-1)(r-2)(r^2-3r+6)$, then an alternant code $\mathscr{A}_r$ is 2-distinguishable.*

In the case $r < q+1$, we experimentally found that the Hilbert function at degree 2 for a generic alternant code was always equal to $\frac{m}{12}(r-1)(r-2)(r^2-3r+6)$.

5 The new distinguisher regime

From [CMT23a], it can be readily deduced that $\mathrm{HF}_{\mathrm{R}}(2)$ corresponding to a random linear code of the same dimension $k = n - rm$ as a generic alternant code of length n, degree r and extension degree m is given by

$$\mathrm{HF}_{\mathrm{R}}(2) = \max\left\{0, \frac{1}{2}\left(k^2 - k(s^2 - s + 1) + \frac{s^4 - s^2}{6}\right)\right\}, \tag{7}$$

where $s \overset{\text{def}}{=} rm$. Indeed, the Hilbert function associated to a linear code of the same dimension $k = n - rm$ as a generic alternant code of length n, degree r and extension degree m is given at degree 2 by $\mathrm{HF}_{\mathrm{R}}(2) = \max\left(0, \binom{k}{2}h(0) - \binom{k}{1}h(1) + \binom{k}{0}h(2)\right)$ where $h(d) \overset{\text{def}}{=} \frac{1}{rm+d-1}\binom{rm+d-1}{d+1}\binom{rm+d-1}{d}$. Moreover, we notice that

$$\begin{aligned} h(2) &= \frac{1}{rm+1}\binom{rm+1}{3}\binom{rm+1}{2} \\ &= \frac{1}{rm+1}\frac{(rm+1)rm(rm-1)}{6}\frac{(rm+1)rm}{2} \\ &= \frac{(rm)^2(rm+1)(rm-1)}{12} \\ &= \frac{s^4 - s^2}{12}, \end{aligned}$$

where $s \overset{\text{def}}{=} rm$. If we plug this expression in the expression we have for $\mathrm{HF}_{\mathrm{R}}(2)$, namely $\mathrm{HF}_{\mathrm{R}}(2) = \max\left(0, \binom{k}{2}h(0) - \binom{k}{1}h(1) + \binom{k}{0}h(2)\right)$ and using the fact that $h(0) = 1$ and $h(1) = \binom{mr}{2}$ we obtain

$$\begin{aligned} \mathrm{HF}_{\mathrm{R}}(2) &= \max\left(0, \frac{k(k-1)}{2} - k\frac{mr(mr-1)}{2} + \frac{s^4 - s^2}{12}\right) \\ &= \max\left(0, \frac{k^2}{2} - k\frac{s^2 - s + 1}{2} + \frac{s^4 - s^2}{12}\right). \end{aligned}$$

Combined with Corollary 4, this implies

Proposition 4. *For a given degree r and extension degree m and assuming that the field size q satisfies $q \geqslant r$, a generic alternant code whose dimension satisfies $k > k_0$ where*

$$k_0 \overset{def}{=} \frac{s^2 - s + 1 - \sqrt{\frac{s^4}{3} + \frac{2H}{3} - 2s^3 + \frac{11}{3}s^2 - 2s + 1}}{2}$$

with $s \overset{def}{=} rm$, $H \overset{def}{=} m(r-1)(r-2)(r^2 - 3r + 6)$ is 2-distinguishable.

Proof. k_0 is defined as the smallest root of the equation (in X)

$$\frac{1}{2}\left(X^2 - X(s^2 - s + 1) + \frac{s^4 - s^2}{6}\right) = \frac{m(r-1)(r-2)(r^2 - 3r + 6)}{12}. \tag{8}$$

Clearly, when the dimension k of an alternant code of degree r and extension degree m is bigger than this k_0, we have $\mathrm{HF}_{\mathrm{R}}(2) < \mathrm{HF}_{\mathrm{A}}(2)$ and it is distinguishable at degree 2. (8) is equivalent to

$$X^2 - X(s^2 - s + 1) + \frac{s^4 - s^2 - H}{6} = 0,$$

where $H \stackrel{\text{def}}{=} m(r-1)(r-2)(r^2-3r+6)$. Therefore

$$\begin{aligned}
k_0 &= \frac{s^2 - s + 1 - \sqrt{\Delta}}{2} \\
\text{where } \Delta &\stackrel{\text{def}}{=} (s^2 - s + 1)^2 - \frac{2}{3}(s^4 - s^2 - H) \\
&= s^4 + s^2 + 1 - 2s^3 + 2s^2 - 2s - \frac{2}{3}s^4 + \frac{2}{3}s^2 + \frac{2}{3}H \\
&= \frac{s^4}{3} + \frac{2}{3}H - 2s^3 + \frac{11}{3}s^2 - 2s + 1.
\end{aligned}$$

□

A natural asymptotic choice of parameters is to let r go to infinity and assume that $m = \mathcal{O}(\log r)$. This is in general the range which is chosen for m, since in order to maximize the decoding capacity one chooses the smallest possible m such that $q^m \geqslant n$. In such a case, it is straightforward to check that

$$k_0 \underset{r\to\infty}{\sim} \frac{1 - \sqrt{\frac{1+\frac{2}{m^3}}{3}}}{2} m^2 r^2.$$

When m also goes to infinity with r, we have

$$k_0 \sim \frac{1 - \sqrt{\frac{1}{3}}}{2} m^2 r^2 \approx 0.21 m^2 r^2.$$

This is much better than the distinguisher of [FGO+11]. In the regime where $q \geqslant r$, it is able to distinguish a generic alternant code from a generic linear code when $n > \binom{mr+1}{2} - \frac{m(r-1)(r-2)}{2}$, that is when $k > \binom{mr+1}{2} - rm - \frac{m(r-1)(r-2)}{2}$. This corresponds to $k > k_1 \stackrel{\text{def}}{=} \binom{mr}{2} - \frac{m(r-1)(r-2)}{2}$ with $k_1 = \frac{1-\frac{1}{m}}{2} m^2 r^2 + o\left(m^2 r^2\right)$ as $r \to \infty$ and if m goes to infinity as well, $k_1 \sim \frac{m^2 r^2}{2}$.

Comparison with the distinguisher given in [Ran24] The syzygy distinguisher given in [Ran24], like the Pfaffian distinguisher we consider here, can be viewed as a broad generalization of the original distinguisher given in [FGO+11]. However it relies on a distinct approach and is the first one that has been shown to be able to distinguish constant rate alternant or Goppa codes with subexponential complexity. This is quite an achievement. It is worthwhile to compare both distinguishers for parameters for which they have roughly the same complexity. Both distinguishers rely on computing the rank of certain matrices. In the case of the distinguisher we consider here, we compute the rank of a matrix of size $a \times b$ where a and b are of order $\mathcal{O}\left((rm)^4\right)$ when n is say of order $(rm)^2$ which will be our assumption to make the comparison. To make a fair comparison between both approaches it makes sense to consider the syzygy distinguisher proposed in [Ran24] without the additional trick of shortening the dual of the alternant/Goppa code, since the Pfaffian distinguisher could also benefit from this trick but it remains to analyze its impact precisely.

The syzygy distinguisher considers the rank of matrices with a number of rows and columns of size $\mathcal{O}\left((rm)^4\right)$ when computing the Betti number $\beta_{p-1,p}$ when $p = 4$. In both cases, computing the distinguisher can be achieved with time complexity $\mathcal{O}\left((rm)^{4\omega+\varepsilon}\right)$ for any $\varepsilon > 0$ where ω is the exponent of matrix multiplication [BCS97, §16.5]. It distinguishes an alternant code from a random code when the Betti number corresponding to the dual of the alternant code is different from the Betti number of the random code. In the parameter regime we consider, namely n of order $(rm)^2$, m of order $\log_q n$ and letting n go to infinity, it turns out by using Theorem 1 of [Ran24] giving a lower bound on the Betti number $\beta_{p-1,p}$ of an alternant code together with [Ran24, Prop. 10] estimating the Betti number $\beta_{p-1,p}$ of a generic linear code, one is able to distinguish up to values of n satisfying $n \geqslant \frac{(rm)^2}{4}(1-o(1))$, which gives in terms of the dimension k of the code $k \geqslant \frac{(rm)^2}{4}(1+o(1))$. This is slightly worse than the Pfaffian distinguisher in this regime of parameters.

6 Concluding Remarks

This work shows that the lower bound $\mathrm{HF}_{\mathrm{A}}(2) > 0$ of [CMT23b, Prop. 18] is very pessimistic and can be significantly improved. Understanding the precise behavior of $\mathrm{HF}_{\mathrm{A}}(d)$ is really desirable not only to assess precisely the power of the Pfaffian distinguisher given in [CMT23b] but should also be very helpful in understanding this distinguisher if instead of applying it to the dual of the alternant or Goppa code we want to distinguish, we apply it to a shortening of this latter code. This paper can be seen as a first step towards this goal. It is tempting to conjecture that similarly to what happened in [Ran24] which resulted in a much improved distinguisher, we should observe the same behavior for the Pfaffian distinguisher. This work also shows that the Pfaffian distinguisher at degree 2 seems a little bit more powerful than the syzygy distinguisher of [Ran24] at degree 4 which has a similar complexity. In light of this result and the fact that the syzygy distinguisher is of subexponential complexity when applied to the right shortened code, this raises the issue whether the same also applies to the Pfaffian distinguisher studied here when applied to the suitable shortened code.

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.

BCS97. Peter Bürgisser, Michael Clausen, and Mohammad Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.

BMT24. Magali Bardet, Rocco Mora, and Jean-Pierre Tillich. Polynomial time key-recovery attack on high rate random alternant codes. *IEEE Trans. Inform. Theory*, 70(6):4492–4511, 2024.

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.

CMT23a. Alain Couvreur, Rocco Mora, and Jean-Pierre Tillich. A new approach based on quadratic forms to attack the McEliece cryptosystem. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part IV*, volume 14441 of *LNCS*, pages 3–38. Springer, 2023.

CMT23b. Alain Couvreur, Rocco Mora, and Jean-Pierre Tillich. A new approach based on quadratic forms to attack the McEliece cryptosystem. *arXiv preprint arXiv:2306.10294*, 2023.

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

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.

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

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.

MT23. Rocco Mora and Jean-Pierre Tillich. On the dimension and structure of the square of the dual of a Goppa code. *Des. Codes Cryptogr.*, 91(4):1351–1372, 2023.

Ran24. Hugues Randriambololona. The syzygy distinguisher. *CoRR*, abs/2407.15740, 2024.

Ver82. Veronese. Behandlung der projectivischen verhältnisse der räume von verschiedenen dimensionen durch das princip des projicirens und schneidens. *Mathematische Annalen*, 19:161–234, 1882.

Wim12. Michael Wimmer. Algorithm923: Efficient numerical computation of the Pfaffian for dense and banded skew-symmetric matrices. *ACM Trans. Math. Software*, 38(4), aug 2012.

A Proof of Theorem 2: a slightly more general version

As we have already mentioned, several equivalent modelings can be applied to find rank $\leqslant 2$ matrices in $\mathscr{C}_{mat}$. However, we are not interested in solving the algebraic system yet, but rather in computing algebraic quantities such as Hilbert functions. It is then mandatory to wonder whether the Hilbert function of all these modelings are the same. The varieties produced by each ideals being isomorphic is not sufficient at all to conclude that their Hilbert series coincide, since this object strongly depends on how the equations defining the variety are written. In this appendix, we will be interested in two different modelings of the same problem and will show that they are *equivalent, i.e* produce the same Hilbert series. The problem in question is to find the intersection between an algebraic variety and a linear subspace. This is formally defined in the following.

Problem 1. Let $f_1, \ldots, f_N$ be homogeneous polynomials in $\mathbb{F}[X_1, \ldots, X_n]$ and $V \subset \mathbb{F}^n$ a linear subspace of $\mathbb{F}^n$. The goal is to compute

$$\boldsymbol{V}(f_1, \ldots, f_N) \cap V = \{\boldsymbol{x} \in V \mid \forall i \in [\![1, N]\!],\ f_i(\boldsymbol{x}) = 0\}.$$

Example 1. The linear MinRank problem, i.e the problem aiming at finding rank $\leqslant r$ matrices in some subspace, can be seen as an instance of Problem 1.

We will be interested in two modelings of Problem 1.

Modeling 4 (Implicit modeling) *Let* $k \overset{def}{=} \dim_{\mathbb{F}}(V)$. *There exists linearly independent linear forms* $L_1, \ldots, L_{n-k}$ *such that*

$$V = \{\boldsymbol{x} \in \mathbb{F}^n \mid \forall i \in [\![1, n-k]\!],\ L_i(\boldsymbol{x}) = 0\}.$$

The implicit algebraic modeling corresponding to Problem 1 is defined by the ideal

$$I \overset{def}{=} (f_1, \ldots, f_N, L_1, \ldots, L_{n-k}).$$

I is an ideal of $\mathbb{F}[X_1, \ldots, X_n]$.

Modeling 5 (Explicit modeling) *Let* $k \overset{def}{=} \dim_{\mathbb{F}}(V)$ *and let* $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ *be an* $\mathbb{F}$*-basis of* V*. The explicit algebraic modeling corresponding to Problem 1, with respect to the basis* $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$*, is defined by the ideal*

$$J \overset{def}{=} (f_1(Y_1\boldsymbol{v}_1 + \ldots + Y_k\boldsymbol{v}_k), \ldots, f_N(Y_1\boldsymbol{v}_1 + \ldots + Y_k\boldsymbol{v}_k)).$$

J is an ideal of $\mathbb{F}[Y_1, \ldots, Y_k]$.

Modeling 4 corresponds to the implicit modeling detailed in Section 3, and Modeling 5 corresponds to the explicit modeling of Section 3. The first thing to notice here is that if $f_1, \ldots, f_N$ are homogeneous (which is required by the specification of Problem 1), then both modelings produce homogeneous ideals. Therefore, both ideals have a structure of graded $\mathbb{F}$-algebra. From now on, we will denote with $\boldsymbol{R}$ (resp. $\boldsymbol{S}$) the polynomial ring in $X_1, \ldots, X_n$ (resp. $Y_1, \ldots, Y_k$) over $\mathbb{F}$. The equivalence between the two modelings is stated by the following.

Theorem 4. *Let $f_1, \dots, f_N \in \boldsymbol{R}$ be homogeneous polynomials, and let $V \subset \mathbb{F}^n$ be a subspace of dimension $k < n$. Let I (resp. J) denote the ideal produced by the implicit (resp. explicit) modeling. There exists a map*

$$\overline{\Phi} : \boldsymbol{R}/I \longrightarrow \boldsymbol{S}/J$$

which defines an isomorphism of graded $\mathbb{F}$-algebras.

This statement clearly implies that the Hilbert functions associated with both modelings are equal, and therefore ensures the validity of Theorem 2.
Note that the change of modelings, from the implicit version to the explicit one, is nothing but a change of variables :

$$(X_1, \dots, X_n) = (Y_1, \dots, Y_k)\boldsymbol{P},$$

where each row of $\boldsymbol{P} \in \mathbb{F}^{k \times n}$ corresponds to the coordinates of a vector of a basis of V. In a more coding-theoretic vocabulary, $\boldsymbol{P}$ is a generator matrix of V. This implies that $\boldsymbol{P}$ is necessarily of rank k. We will assume, without loss of generality, that $\boldsymbol{P}$ is in systematic form, i.e $\boldsymbol{P} = (I_k \mid *)$.

In the following, we will try to construct the isomorphism $\overline{\Phi}$. To begin with, let us introduce the map

$$\Phi : \begin{cases} \boldsymbol{R} & \longrightarrow \boldsymbol{S} \\ f & \longmapsto f\left(\sum_{j=1}^{k} P_{j,1}Y_j, \dots, \sum_{j=1}^{k} P_{j,n}Y_j\right). \end{cases}$$

Applying Φ is actually doing the change of variables. Before proving Theorem 4, we need the following auxiliary results.

Lemma 4. *The map Φ is a surjective morphism of graded $\mathbb{F}$-algebras.*

Proof. It is clear that Φ is a morphism of $\mathbb{F}$-algebras. Furthermore, applying Φ on a polynomial f boils down to composing f with homogeneous polynomials of degree 1, therefore Φ preserves the degree, *i.e* sends homogeneous components onto homogeneous components of same degree. Hence Φ is a morphism of *graded* $\mathbb{F}$-algebras.
Finally, since $\boldsymbol{P}$ is in systematic form, we have $\Phi(X_i) = Y_i$ for all $1 \leqslant i \leqslant k$. Since all generators of $\boldsymbol{S}$ as an $\mathbb{F}$-algebra lie in the image of the $\mathbb{F}$-algebra morphism Φ, we conclude that Φ is surjective. □

Lemma 5. $J = \Phi(I)$.

Proof. Since $J = (\Phi(f_1), \dots, \Phi(f_N))$, we know that any element of J can be written as the image of an element of I by the map Φ, *i.e* $J \subseteq \Phi(I)$. To prove that $\Phi(I)$ is not strictly bigger that J, it only remains to show that $\Phi(L_i) \in J$ for all $i = 1, \dots, n-k$.

Remember that the rows of $\boldsymbol{P}$ are the vectors of a basis of V. Hence, for all $(y_1, \dots, y_k) \in \mathbb{F}^k$, we have

$$\forall 1 \leqslant i \leqslant n-k,\ L_i\left(\sum_{j=1}^{k} y_j \boldsymbol{P}_j\right) = 0,$$

where $\boldsymbol{P}_j$ denotes the j-th row of $\boldsymbol{P}$. In other words, the polynomials $\Phi(L_i)$ are linear forms that vanish over $\mathbb{F}^k$ entirely. This implies that $\Phi(L_i) = 0$ for all $i \in [\![0, n-k]\!]$. As a consequence, we have both $\Phi(f_i) \in J$ and $\Phi(L_i) \in J$ for all i, therefore $\Phi(I) \subseteq J$. □

Now that we know how the image of Φ behaves, it only remains to investigate its kernel.

Lemma 6. $\ker \Phi = (L_1, \dots, L_{n-k})$.

Proof. This fact is not trivial because we cannot assume that $\mathbb{F}$ is algebraically closed[4]. To deal with it, we introduce

$$\overline{V} = \{\boldsymbol{x} \in \overline{\mathbb{F}}^n \mid \forall 1 \leqslant i \leqslant n-k,\ L_i(\boldsymbol{x}) = 0\} = \langle V \rangle_{\overline{F}},$$

where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$. By Hilbert's Nullstellensatz, we have

$$\boldsymbol{I}(\overline{V}) = \sqrt{(L_1, \dots, L_{n-k})} = (L_1, \dots, L_{n-k}),$$

the last equality comes from the fact that all the L_i's have degree 1. Now, let $f \in \ker \Phi$. By definition,

$$f\left(\sum_{j=1}^{k} P_{j,1} Y_j, \dots, \sum_{j=1}^{k} P_{j,n} Y_j\right) = 0.$$

We may apply this polynomial on any element $\boldsymbol{y} \in \overline{\mathbb{F}}^k$, which means that

$$\forall \boldsymbol{x} \in \overline{V},\ f(\boldsymbol{x}) = 0.$$

This implies that $f \in (L_1, \dots, L_{n-k})$, as an ideal of $\overline{\mathbb{F}}[X_1, \dots, X_n]$, but since the coefficients of f lie in $\mathbb{F}$, we have $f \in (L_1, \dots, L_{n-k})$ as an ideal of $\boldsymbol{R}$. We have thus proven that $\ker \Phi \subseteq (L_1, \dots, L_{n-k})$. The other inclusion is already proven in the previous lemma. □

We are now ready to provide a proof of Theorem 4.

Proof (Proof of Theorem 4). Lemma 5 implies that if f is defined modulo an element of I, then $\Phi(f)$ is *well-defined* modulo an element of J. In other words, Φ induces a morphism $\overline{\Phi}$ which is the only one such that the following diagram commutes :

[4] In our case, $\mathbb{F} = \mathbb{F}_q$ is a finite field which is not algebraically closed.

$$\begin{tikzcd}
\boldsymbol{R} \arrow[r, "\mathit{\Phi}"] \arrow[d, "\pi"] & \boldsymbol{S} \arrow[d, "\pi"] \\
\boldsymbol{R}/I \arrow[r, "\overline{\mathit{\Phi}}"] & \boldsymbol{S}/J
\end{tikzcd}$$

On the above diagram, we used the symbol π to write both canonical projections. Since $\mathit{\Phi}$ is a surjective morphism of graded $\mathbb{F}$-algebras, and since $\mathit{\Phi}(I) = J$ (Lemma 5), so is $\overline{\mathit{\Phi}}$. Finally, let us prove that $\mathit{\Phi}$ is injective. Let $f \in \boldsymbol{R}$ such that $\overline{\mathit{\Phi}} \circ \pi(f) = 0$, or equivalently, $\mathit{\Phi}(f) \in J$. Since $J = \mathit{\Phi}(I)$, there exists $g \in I$ such that $\mathit{\Phi}(f) = \mathit{\Phi}(g)$, hence $f - g \in \ker \mathit{\Phi}$. By Lemma 6, we have $\ker \mathit{\Phi} \subseteq I$, which implies that $f \in I$, or equivalently $\pi(f) = 0$.