A Heuristic Subexponential Attack on the McEliece Cryptosystem

Pierre Briaud[1,2], Axel Lemoine[3,4], Hugues Randriambololona[5,6], and Jean-Pierre Tillich[3]

[1] Université de Limoges, XLIM, France
[2] CNRS, France
[3] Inria, France
[4] DGA, France
[5] ANSSI, Laboratoire de cryptographie, France
[6] Télécom Paris, C[2], France

Abstract. We provide a new way of performing an algebraic attack on the McEliece cryptosystem based on binary Goppa codes. It also applies in general to the case where the field over which the Goppa code is defined is of even characteristic. It is based on a new algebraic modeling for finding matrices of rank 2 in the code of quadratic relations related to the Goppa code that is attacked. Such matrices are then used to recover the secret algebraic structure of the code, from which an equivalent secret key can be efficiently derived, leading to a full key-recovery attack. A byproduct of our approach is a new distinguisher for Goppa codes in even characteristic which is as the syzygy distinguisher of [Ran25] subexponential in the security level of the scheme. We demonstrate the effectiveness of our attack on McEliece TII challenges, some of which having been studied in [BLT26], and aimed at having 83,89,119,166, 210 and even 248 bit security respectively and CFS keys with parameters $r = 9$ and $m = 16$, corresponding to a security of 74.9 bits according to [LS12]. This CFS key was not attacked in practice in [BLT26] and took us 14 hours of computation and 24GB of RAM. We make the conjecture that this attack has a complexity which is of the same nature as the distinguisher, namely subexponential in the security level. It should be noted that this attack is at best of complexity of order 2^{454} for NIST level 1 `Classic McEliece` parameters.

1 Introduction

1.1 The McEliece scheme

The McEliece encryption scheme [McE78], proposed only a few months after RSA [RSA78], is the oldest public-key cryptosystem still believed to resist both classical and quantum attacks. Unlike RSA, its security relies in part on the NP-hard problem of decoding a random linear code [BMvT78].

The public key is a linear code $\mathscr{C}$, given by an arbitrary generator matrix $\boldsymbol{G}$. The code is chosen from a family equipped with an efficient decoding algorithm depending on the specific code instance. In its simplest form, encryption is

$$\mathsf{Enc} : \boldsymbol{m} \longmapsto \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}, \tag{1.1}$$

where $\boldsymbol{e}$ is a random error vector whose Hamming weight equals the error-correction capacity of $\mathscr{C}$. Decryption uses the efficient decoding algorithm for $\mathscr{C}$ to remove the error and recover the message $\boldsymbol{m}$.

The private key consists of the parameters defining the decoding algorithm. The underlying assumption is that the public description of the scheme, namely a generator matrix of $\mathscr{C}$, does not reveal these parameters, *i.e.* essentially which code in the family was selected. In the original proposal, McEliece suggested binary Goppa codes because of their strong error-correction capacity and their similarity to random linear codes; for instance, they attain the Gilbert–Varshamov bound [MS77, Ch. 12, §4, Problem 9].

The scheme has withstood extensive cryptanalytic efforts. Message-recovery attacks amount to decoding random linear codes and are widely regarded as the main threat to the scheme. Their complexity has decreased only marginally over time as can be seen from Prange's algorithm in 1962 [Pra62] to nowadays [Dum86, LB88, Ste88, Dum89, CC98, BLP11, MMT11, BJMM12, MO15, BM17, CDMT22, Ess22, EZ23, CDMT24, DEEK24]. Other attacks include combinatorial key-recovery attacks [Gib91, Sen00, Pan25], but their complexity remains far higher than that of message-recovery attacks. One should also mention the optimized implementation of message-recovery attacks in [BLP08], which successfully broke the original McEliece parameters, although it does not threaten the parameters currently recommended in [ABC+22]. The scheme also appears resistant to known quantum attacks [DMR11, Ber10, KT17, Tra24].

This strong resistance to attacks was a major argument during the NIST post-quantum cryptography competition for the IND-CCA secure variant `Classic McEliece` [ABC+22], which reached the final round of the competition. Although it was ultimately not selected by NIST for standardization, it is currently undergoing standardization within ISO.

However, the Goppa codes used in the scheme possess a rich algebraic structure that has motivated numerous algebraic attacks. We now review the results obtained in this direction.

1.2 Algebraic attacks on the McEliece scheme

The algebraic structure of Goppa codes. The efficient decoding algorithms and strong error-correction capability of Goppa codes stem from the fact that such codes are subcodes of a well-known family of algebraic codes with excellent decoding properties, namely generalized Reed–Solomon (GRS) codes.

Definition 1.1 (Generalized Reed–Solomon code). *Let $\boldsymbol{x} = (x_i)_{1\le i\le n} \in \mathbb{F}^n$ be a vector of pairwise distinct elements, let $\boldsymbol{y} = (y_i)_{1\le i\le n}$ be a vector of nonzero elements, and let $r < n$. The* generalized Reed–Solomon code *of dimension r, support $\boldsymbol{x}$, and multiplier $\boldsymbol{y}$ is*

$$\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y}) \stackrel{\text{def}}{=} \{(y_i f(x_i))_{1\le i\le n} \mid f \in \mathbb{F}[X]_{<r}\}.$$

GRS codes cannot be used directly in the McEliece scheme: their alphabet size must grow with the code length, and the resulting cryptosystem was completely broken in [SS92]. However, the situation changes drastically for suitable subcodes. Such subcodes inherit efficient decoding algorithms from the ambient GRS code while apparently resisting the attack of [SS92], even in the case of subfield subcodes. These codes are known as *alternant codes*, of which Goppa codes form a particular family. Unlike GRS codes, alternant codes can have arbitrary length over a fixed finite field $\mathbb{F}_q$. Binary Goppa codes were likely chosen by McEliece because of their particularly strong decoding performance among binary alternant codes.

It is convenient to define alternant codes through duality, using the fact that the dual of a GRS code is again a GRS code (see [MS86, Th.. 4, p. 304]).

Definition 1.2 (Alternant code). *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ be a vector with pairwise distinct elements, let $\boldsymbol{y} \in (\mathbb{F}_{q^m}^\times)^n$, and let $r < n$. The* alternant code *over $\mathbb{F}_q$ of support $\boldsymbol{x}$, multiplier $\boldsymbol{y}$, degree r, and extension degree m is*

$$\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) \stackrel{\text{def}}{=} \left(\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^\perp\right) \cap \mathbb{F}_q^n.$$

The dimension of alternant codes satisfies

$$\dim_{\mathbb{F}_q} \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) \ge n - rm,$$

and equality holds for generic alternant codes. We call alternant codes meeting this bound *proper* alternant codes.

Goppa codes are simply alternant codes with a specific algebraic relation between the support and the multiplier.

Definition 1.3 (Goppa code). *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ be a vector with pairwise distinct elements, let $r < n$, and let $\Gamma \in \mathbb{F}_{q^m}[X]$ be a monic polynomial such that $\Gamma(x_i) \neq 0$ for all i. The* Goppa code *over $\mathbb{F}_q$ of support $\boldsymbol{x}$ and Goppa polynomial Γ is*

$$\mathscr{G}(\boldsymbol{x}, \Gamma) \stackrel{\text{def}}{=} \mathscr{A}_r\left(\boldsymbol{x}, \frac{1}{\Gamma(\boldsymbol{x})}\right), \qquad \text{where } \frac{1}{\Gamma(\boldsymbol{x})} = \left(\frac{1}{\Gamma(x_i)}\right)_{1 \leq i \leq n}.$$

The Goppa distinguishing problem. A natural approach to key-recovery attacks against the McEliece scheme based on Goppa codes is to exploit their underlying algebraic structure. While algebraic attacks [FOPT10, BC18, BB22] have been successful against alternant or Goppa codes endowed with additional symmetries, such as quasi-cyclic or quasi-dyadic versions [BCGO09, MB09, FOPT10], the unstructured Goppa codes proposed in [McE78, ABC+22] appear resistant to such attacks. Nevertheless, in the highly degraded parameter regime considered for the so-called CFS signature scheme based on binary Goppa codes [CFS01], algebraic attacks exhibit a markedly different behavior on binary Goppa codes than on random linear codes, even though they do not break the scheme. This observation led to polynomial-time distinguishers capable of separating binary Goppa codes, and more generally alternant codes, from random codes in the very high-rate regime [FGO+11, FGO+13].

An important feature of this line of research is that the distinguishing problem appears substantially simpler than the problem of breaking the McEliece scheme. As such, it has provided valuable insight into structural properties of Goppa codes that could potentially be exploited in future attacks. Significant progress has recently been made in this direction. Whereas the distinguisher of [FGO+11] only applied to codes of rate extremely close to 1, the works [CMT23, Ran25, HW26] considerably extended the range of parameters for which distinguishing is possible, including codes of constant rate.

Most notably, the breakthrough work [Ran25] achieved, for the first time, key distinguishing in subexponential complexity with respect to the security level λ of the scheme, where 2^λ denotes the complexity of the best known attack against the scheme. For the McEliece cryptosytem based on binary Goppa codes this corresponds to the complexity of the best known generic decoding attack which performs message recovery. For constant rate binary Goppa codes λ is proportional to the number of errors introduced during the encryption (namely the Hamming weight of $\boldsymbol{e}$ in (1.1)).

The square code. The distinguisher introduced in [FGO+11] was later reinterpreted in terms of square codes [MP12], which is now the standard viewpoint. This perspective also led to attacks against certain McEliece variants in specific parameter regimes, namely wild Goppa codes with extension degree 2 [COT14]; see also [FPdP14].

The construction relies on the component-wise product of vectors

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

where $\boldsymbol{a} = (a_i)_{1 \leq i \leq n}$ and $\boldsymbol{b} = (b_i)_{1 \leq i \leq n}$ (we also set $\boldsymbol{a}^2 \stackrel{\text{def}}{=} \boldsymbol{a} \star \boldsymbol{a}$). This induces a product on codes.

Definition 1.4. *Let $\mathscr{C}, \mathscr{D} \subseteq \mathbb{F}_q^n$ be linear codes. Their* component-wise product *is*

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

When $\mathscr{C} = \mathscr{D}$, the code $\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$ is called the square *of $\mathscr{C}$.*

Square codes provide an efficient way to distinguish GRS codes from random linear codes. Indeed, for a random code $\mathscr{C}$ of length n, one typically has

$$\dim \mathscr{C}^{\star 2} = \min\left\{n, \binom{\dim \mathscr{C} + 1}{2}\right\},$$

whereas the polynomial structure of GRS codes implies $\mathbf{GRS}_k(\boldsymbol{x},\boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2k-1}(\boldsymbol{x},\boldsymbol{y}^2)$, and therefore $\dim \mathbf{GRS}_k(\boldsymbol{x},\boldsymbol{y})^{\star 2} = \min(2\dim(\mathbf{GRS}_k(\boldsymbol{x},\boldsymbol{y})) - 1, n)$.

This unusually small square-code dimension persists for the duals of very high-rate alternant and Goppa codes [MP12]. In fact, this characterization is equivalent to the original distinguisher of [FGO+11]; see also [MT22] for a more detailed analysis of the square of dual alternant and Goppa codes.

It is worth noting that this reinterpretation of the distinguisher of [FGO+11], combined with a shortening technique, eventually led to a key-recovery attack [BMT24] against generic alternant codes over $\mathbb{F}_2$ and $\mathbb{F}_3$ in the parameter ranges where the distinguisher applies. Remarkably, this attack completely fails for Goppa codes, despite the fact that they form a more structured subclass of alternant codes.

Matrices of low rank in the code of quadratic relations. Our approach is based on the distinguisher of [CMT23], which applies in characteristic 2 and which we now briefly recall.

It is convenient to work over the extension field $\mathbb{F}_{q^m}$. For a code $\mathscr{C}$ defined over $\mathbb{F}_q$, we denote by $\mathscr{C}_{\mathbb{F}_{q^m}}$ its $\mathbb{F}_{q^m}$-linear span in $\mathbb{F}_{q^m}^n$.

Definition 1.5 (Extension of a code over a field extension). *Let $\mathscr{C}$ be a linear code over $\mathbb{F}_q$. The* extension *of $\mathscr{C}$ to $\mathbb{F}_{q^m}$ is the $\mathbb{F}_{q^m}$-linear code*

$$\mathscr{C}_{\mathbb{F}_{q^m}} \subseteq \mathbb{F}_{q^m}^n$$

generated by $\mathscr{C}$.

If $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})$, $\mathscr{C}^{\perp}_{\mathbb{F}_{q^m}}$ admits the decomposition (see e.g. [BMT24, prop. 14])

$$(\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^{\perp})_{\mathbb{F}_{q^m}} = \sum_{j=0}^{m-1} \mathbf{GRS}_r\left(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j}\right), \tag{1.2}$$

This extended code contains triples of codewords $(\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3)$ satisfying

$$\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \boldsymbol{c}_3^2. \tag{1.3}$$

For example, one may take $\boldsymbol{c}_1 = \boldsymbol{y}$, $\boldsymbol{c}_2 = \boldsymbol{y}\star\boldsymbol{x}^2$, $\boldsymbol{c}_3 = \boldsymbol{y}\star\boldsymbol{x}$. Such triples can be sought by taking an arbitrary basis $\mathcal{B} = (\boldsymbol{b}_1,\dots,\boldsymbol{b}_k)$ of $(\mathscr{C}^{\perp})_{\mathbb{F}_{q^m}}$. One considers the vector space of all $\boldsymbol{c} = (c_{ij})_{1\le i\le j\le k} \in \mathbb{F}_{q^m}^{k(k+1)/2}$ such that

$$\sum_{1\le i\le j\le k} c_{ij}\, \boldsymbol{b}_i \star \boldsymbol{b}_j = 0.$$

This space is called the *code of quadratic relations* of $\mathscr{C}$ with respect to $\mathcal{B}$ and is denoted by $\mathscr{C}_{\mathrm{rel}}(\mathcal{B})$. Elements of $\mathscr{C}_{\mathrm{rel}}(\mathcal{B})$ may be viewed either as quadratic forms

$$Q_{\boldsymbol{c}}(\boldsymbol{x}) = \sum_{1\le i\le j\le k} c_{ij} x_i x_j,$$

or through their associated polar forms. The polar form of $Q_{\boldsymbol{c}}$ is defined via the matrix $\boldsymbol{M}_{\boldsymbol{c}}$ by

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

where $\boldsymbol{x} = (x_1,\dots,x_k)$ and $\boldsymbol{y} = (y_1,\dots,y_k)$. Equivalently this matrix $\boldsymbol{M}_{\boldsymbol{c}} = (m_{ij})_{\substack{1\le i\le k\\ 1\le j\le k}}$ is given by

$$m_{ij} = m_{ji} = c_{ij} \quad (i\neq j), \qquad m_{ii} = 2c_{ii}.$$

The collection of these $\boldsymbol{M}_{\boldsymbol{c}}$ defines the matrix code of quadratic relations introduced in [CMT23].

Definition 1.6 (Matrix code of quadratic relations). *Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}$ with basis $\mathcal{B}=(\boldsymbol{b}_1,\dots,\boldsymbol{b}_k)$. The* matrix code of quadratic relations *associated with $\mathcal{B}$ is*

$$\mathscr{C}_{\mathrm{mat}}(\mathcal{B}) \stackrel{\mathrm{def}}{=} \{\boldsymbol{M}_{\boldsymbol{c}} \mid \boldsymbol{c}\in\mathscr{C}_{\mathrm{rel}}(\mathcal{B})\} \subseteq \mathbf{Sym}_k(\mathbb{F}),$$

where $\mathbf{Sym}_k(\mathbb{F})$ denotes the set of $k\times k$ symmetric matrices with entries in $\mathbb{F}$.

In characteristic 2, the quadratic relation (1.3) gives rise to a polar form of rank 2, which is a highly atypical property for the extension of a code of rate below $\frac{1}{3}$ if such a code is random [CMT23]. This naturally leads to a MinRank problem: finding a rank-2 matrix in the matrix code of quadratic relations.

The work [CMT23] considered a specific algebraic modeling of this problem that contains quadratic and linear equations, referred to as the *Pfaffian modeling*. This modeling has the advantage of being amenable to analysis. Although it did not lead to a key-recovery attack, the authors showed that the associated Macaulay matrices exhibit different rank profiles depending on whether one starts from a random code or from an alternant/Goppa code. This discrepancy yields the distinguisher of [CMT23].

From the distinguisher of [CMT23] to an attack. The work [Mor25] showed that the Pfaffian modeling of [CMT23] can actually lead to key-recovery attacks in certain very specific cases, namely Goppa codes of degree 2 appearing in some of the TII challenges[7]. The main idea is to specialize a suitable number of variables so as to obtain a zero-dimensional variety and then recover enough rank-2 matrices in the matrix code of quadratic relations to mount an attack.

This approach was significantly extended in [BLT26], where the authors successfully attacked the very high-rate Goppa codes used in the CFS signature scheme, as well as several high-rate TII challenges with security levels up to 210 bits. Two main ideas were introduced.

(i) Instead of applying the Pfaffian modeling directly to the dual of the Goppa code, as in [CMT23, Mor25], the authors apply it to a suitable shortening of this code. This substantially decreases the number of variables while preserving the existence of rank-2 matrices in the associated matrix code of quadratic relations.

(ii) The second key idea is to search for squares of linear polynomials in the degree-2 Macaulay matrix and replace them by their square roots. This makes it possible to compute a Gröbner basis while remaining entirely at degree 2, leading to a dramatic speedup in the resolution of the system.

The fact that this improved Gröbner basis computation remains at degree 2 is likely related to the fact that all codes attacked in [BLT26] are 2-*distinguishable* in the sense of [CMT23, Def. 12] (see also [LMT25, Def. 10]). This means that the rank of the degree-2 Macaulay matrix differs from that obtained for a random code of the same parameters. More precisely, denoting by $\mathrm{HF}(2)$ the value at 2 of the Hilbert function of the associated quotient ring, we have $\mathrm{HF}(2)=0$ in the random case, whereas $\mathrm{HF}(2)>0$ in the public-key case.

The analysis of [CMT23] shows that $\mathrm{HF}(2)=0$ for random codes only when the rate satisfies $R=\mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$ with a sufficiently small implied constant. In the attack of [BLT26], this rate corresponds to that of the shortened dual Goppa code. Consequently, the attack only applies when the original Goppa code has rate extremely close to 1, and thus poses no threat to Classic McEliece.

A natural idea is then to continue the Gröbner basis computation to higher degrees and search for squares at degree $d>2$. Experimental evidence suggests that this could extend the attack to parameter ranges beyond those covered by [BLT26], including additional TII challenges. One may even wonder whether this approach could eventually threaten Classic McEliece.

It is tempting to conjecture that the relevant degree is the first degree d for which the Hilbert function $\mathrm{HF}(d)$ differs from that of a random code under the same algebraic modeling, *i.e.* the first degree at which the code becomes distinguishable in the sense of [CMT23]. Using the estimate of [CMT23, Conj. 2], $d\approx c\,\frac{k^2}{n-k}$, where the attack is performed on a shortened dual code of dimension

[7] https://crowdchallenge.tii.ae/mceliece-challenges

k, length n, and $c \approx \frac{1}{4}$, one finds that by using [BLT26, Thm. 3.7], the best possible choice is $k = \Theta\left(\frac{n}{\log n}\right)$. Since the algebraic modeling involves roughly $\binom{k}{2} \sim \frac{k^2}{2}$ variables, the resulting complexity is of order $2^{\Theta(n/\log n)}$. For the constant-rate Goppa codes used in schemes such as Classic McEliece, whose decoding capacity is of order $\Theta(n/\log n)$, this complexity is exponential in the decoding capacity. In particular, it is asymptotically larger than the subexponential distinguishing attack of [Ran25].

A more precise complexity analysis under this conjecture therefore suggests that Classic McEliece remains secure against this approach.

1.3 Contributions

The new approach. As we have just discussed, it does not seem possible to obtain a complexity better than an exponential bound in the security level if we use the natural higher-degree continuation of [BLT26]. However, since alternative distinguishers with subexponential complexity exist (e.g., [Ran25]), it cannot be ruled out that other competitive approaches may still be found.

We give such a competitive distinguisher. Our distinguisher is actually closely related to [CMT23, BLT26] in its overall structure, but we manage to avoid the large number of variables inherent to the Pfaffian modeling that impacted the complexity. To achieve this, we just use another modeling of the same problem that is able to reduce the number of unknowns from $\binom{k}{2} \sim k^2/2$ down to $2(k-2)$. Its equations are bilinear and not merely quadratic, and we thus use standard tools for solving bilinear systems to adapt the distinguishing approach of [CMT23, BLT26]. More precisely, we consider Macaulay matrices indexed by bi-degrees instead of by the total degree. The rank of these Macaulay matrices can be predicted to a sufficient extent, allowing us to identify distinguishing bi-degrees that are of the same order as the degree at which the distinguisher of [CMT23] works. By simply reducing the number of variables and working at this degree, the resulting complexity is subexponential in the security level of the scheme, as in [Ran25].

However contrarily to [Ran25] where the problem of transforming this distinguisher into an attack remains to be found, this is not the case here. This can be expected since it was already not a problem in [BLT26] if we allow exponential cost. More concretely, at the bi-degrees we distinguish, there are degree falls. Experimental evidence seems to point towards the fact that at the corresponding total degree, the approach of [BLT26] still applies. In particular, we obtain equations that are squares at this degree and by replacing them by their square root the Gröbner basis stops at this degree. This allows us to find a rank-2 matrix in the matrix code of quadratic relations. Moreover, we propose here a new way to exploit such a matrix to directly recover the support of the Goppa code. This allows us to break the scheme. We have run experiments on TII challenges to verify this. In other words, if the Gröbner basis computation stops at the degree where we distinguish, this gives on the spot a subexponential attack on the McEliece scheme. Note that this feature is very robust: even if we had to go higher degrees, as long as the degree at which we compute the Gröbner basis would be say twice, or more generally a constant number of times the degree at which we distinguish, we would get a subexponential attack (in the security level). We conjecture that this is indeed the case. Note that this will be for the *first time* a *subexponential attack* on the McEliece cryptosystem based on binary Goppa codes.

The new modeling. Let us introduce now the new modeling we are going to bring in. It relies on a very simple parametrization of skew-symmetric matrices of rank ≤ 2. Indeed, it is easy to verify that any such matrix $\boldsymbol{M} \in \mathbb{F}_q^{k\times k}$ can be written as

$$\boldsymbol{M} = \boldsymbol{x}^\intercal \cdot \boldsymbol{y} + \boldsymbol{y}^\intercal \cdot \boldsymbol{x}, \tag{1.4}$$

for some $\boldsymbol{x} \in \mathbb{F}_q^k$ and some $\boldsymbol{y} \in \mathbb{F}_q^k$. In our case, we may further assume that up to some multiplicative constant, we search for such an $\boldsymbol{M}$ whose bottom right 2×2 block is just the block $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This is equivalent to having $x_{k-1} = y_k = 1$ and $x_k = y_{k-1} = 0$ in (1.4) and thus gives the aforementioned $2(k-2)$ unknowns. We will basically search for a matrix $\boldsymbol{M}$ of this form in

the matrix code $\mathscr{C}_{\mathrm{mat}}$ of quadratic relations (a vector space of $k \times k$ skew-symmetric matrices) by finding some $\boldsymbol{x} = (x_1, \cdots, x_{k-2}, 1, 0)$ and $\boldsymbol{y} = (y_1, \cdots y_{k-2}, 0, 1)$ such that $\boldsymbol{x}^\intercal \cdot \boldsymbol{y} + \boldsymbol{y}^\intercal \cdot \boldsymbol{x}$ belongs to $\mathscr{C}_{\mathrm{mat}}$. Finally, since a linear space of skew-symmetric matrices $\boldsymbol{M} = (m_{ij})_{\substack{1 \le i \le j \\ 1 \le j \le k}}$ in $\mathbb{F}_q^{k \times k}$ of dimension K can be specified by $\binom{k}{2} - K$ linear equations relating the entries $m_{i,j}$ of $\boldsymbol{M}$, we proceed by substituting the above parametrization into these linear constraints. This gives us a polynomial system in the variables x_i and y_i, consisting of $\binom{k}{2} - \dim \mathscr{C}_{\mathrm{mat}}$ equations.

Macaulay matrix approach to derive a distinguisher. Much like known solving algorithms for bilinear equations, we study Macaulay matrices associated to our system which are indexed by bi-degree. Our system deviates from the generic behavior of bilinear systems because the bilinear equations are linear in the quantities $x_i y_j + y_j x_i$. We use this together with estimates of the rank of Macaulay matrices for generic bilinear systems to predict the rank of the Macaulay matrices when applying this modeling to a matrix code $\mathscr{C}_{\mathrm{mat}}$ arising from the random case.

Our rank prediction is sufficient to identify bi-degrees at which we can show that our system has no solutions in the random case (this is equivalent to the vanishing of the Hilbert function in [CMT23]). Since we expect solutions in the Goppa case, this yields a distinguisher at these bi-degrees, even though we do not at all control the rank profile in the Goppa case. We also discuss degree falls, which may allow to distinguish at lower bi-degrees (this corresponds to moments when the HF differs).

This leads to a distinguisher that consists solely of linear algebra, namely Macaulay matrix rank computations and computations to detect degree falls. We show that these computations reduce to determining whether a certain sparse matrix has full rank, which can be significantly sped up by applying Wiedemann's algorithm.

Subexponential complexity. By analyzing this distinguisher for constant-rate Goppa codes, we find that these codes can be distinguished with a complexity that is only subexponential in the error-correction capacity of the Goppa code (which, in the standard definition, is proportional to the security level). We provide an upper bound on the exponent of the distinguisher, which turns out to coincide with the asymptotic complexity of the syzygy distinguisher. On Classic McEliece instances, the distinguisher obtained through our approach has a complexity comparable to that of the syzygy distinguisher, performs worse than the higher-order vanishing distinguisher of [HW26], but performs significantly better than the Pfaffian distinguisher of [CMT23].

A heuristic subexponential attack that has been verified on TII challenges. Apart from the fact that it leads to a distinguisher, this new algebraic modeling can be turned into an attack much in the same way that the distinguisher based on the Pfaffian modeling of [CMT23] has been turned into an attack in [Mor25, BLT26]. This comes from the fact that both modelings aim at the same target which are matrices of rank 2 in the matrix code of quadratic relations. However, this attack seems clearly more efficient than those attacks based on the Pfaffian modeling as can already be guessed from the fact that the associated distinguisher is way more efficient. We have verified this attack both on TII challenges that were treated in [BLT26], namely instances claiming a security of 83, 89, 119, 166 and 210 bits against key attacks and on CFS [CFS01] instances which is a code based signature scheme which can be broken algebraically in the same way because it is also based on binary Goppa codes as in the McEliece scheme. In particular, we have attacked with it a CFS instance with parameters $r = 9$ and $m = 16$ in less than 14 hours and 24 GB of RAM which was not reported as practical in [BLT26]. By doing so, we have also improved the way the rank 2 matrices were used to recover the algebraic structure of the Goppa code in [Mor25, BLT26]. Instead of using the modeling and its algebraic solving for producing a collection of such matrices of rank 2 we actually show that a single matrix of rank 2 is sufficient to derive the secret Goppa structure with it.

Much has to be understood in detail for this new attack. However, it seems that solving occurs at a degree which is the degree at which we distinguish. If this holds, then this gives a subexponential attack on the McEliece cryptosystem. In any case, we do not expect a big difference

between this solving degree and the distinguishing degree, it is why we conjecture this attack to be subexponential.

Impact on the McEliece scheme. If this conjecture is true, this shows that at least asymptotically the message attacks which were always thought to be the only real threat on the McEliece scheme and which are used to estimate the security level are outperformed asymptotically by this new key attack. This does not, for the time being, constitute a threat to Classic McEliece, as can be seen from the fact that even the bit complexity of our distinguisher—which may be regarded as a very crude upper bound on the complexity of the attack—is between 3 and 6 times the security level. Moreover it should be noted that in the case of Classic McEliece, the complexity of these key recovery attacks is much larger than 2^{256} which is larger than the complexity of the best key recovery attack considered in the guide for security reviewers document for `Classic McEliece` `https://classic.mceliece.org/mceliece-security-20221023.pdf`. Note that the reason why we are interested in these distinguishers is not to challenge the security proof of the McEliece cryptosystem, as in [FGO+11], but rather to solve a potentially simpler problem with the aim of making progress on algebraic attacks, in the hope of turning these distinguishers into actual attacks at a later stage. This strategy has proved particularly fruitful. For instance, the early distinguishers of [FGO+11] can in many cases be turned into attacks [BMT24], and new distinguishers have been found [CMT23, Ran25, HW26]. Although their complexity has significantly decreased over time, it still remains far beyond the security level of the schemes currently proposed, with the notable exception of the new distinguisher proposed in [GIJS26]. The question of where this algebraic progress may lead is tantalizing.

Comparison with the previous approaches. In a nutshell, this paper follows the approach of [CMT23, Mor25, BLT26] for attacking the McEliece cryptosystem by searching for rank-2 matrices in the matrix code of quadratic relations. However, these works rely on a Pfaffian modeling to find such matrices. Since this modeling involves a number of unknowns that is quadratic in the code dimension, the resulting distinguishers and attacks cannot achieve subexponential complexity in the security level.

We instead introduce a new parametrized bilinear modeling that drastically reduces the number of unknowns, making it linear in the code length. This reduction is instrumental in obtaining a subexponential attack. Moreover, we can analyze the behavior of Gröbner basis computations for this modeling and predict when they distinguish a random code from a binary Goppa code. This yields a new distinguisher with subexponential complexity, as in [Ran25], but based on a fundamentally different approach from the syzygy distinguisher of [Ran25].

Unlike the distinguisher of [Ran25], however, our approach produces rank-2 matrices that naturally lead to a full attack. In contrast to [Mor25, BLT26], our attack requires only one—or, depending on the rate, very few—rank-2 matrices to recover the algebraic structure of the code. This is achieved by exploiting these matrices more directly than in [Mor25, BLT26]. Finally, as in [BLT26], we use shortening as part of the attack, but, unlike in [BLT26], we obtain a precise characterization of how far the code can be shortened while preserving the conditions required for the attack. This is obtained by bringing in a new notion of multiplicative subcode which is of independent interest for understanding algebraic attacks in this context.

2 Notation

General notation. $[\![a, b]\!]$ indicates the closed integer interval between a and b. $\mathbb{F}_q$ denotes the finite field with q elements. We warn the reader that all what is written applies only if the characteristic of the field is 2. In other words in all what is written from now on, we assume that q is a power of 2. This is used to show that the matrix code of quadratic relations associated to the dual of the Goppa code we attack contains a matrix of rank 2 (see [CMT23]).

Assumption 1. *In the whole article, q stands for a certain power of 2.*

Vector and matrix notation. Vectors are indicated by lowercase bold letters such as $\boldsymbol{x}$ and matrices by uppercase bold letters such as $\boldsymbol{M}$.

Given a function f acting on $\mathbb{F}_q$ and a vector $\boldsymbol{x} = (x_i)_{1\leq i\leq n} \in \mathbb{F}_q^n$, the expression $f(\boldsymbol{x})$ is the component-wise mapping of f on $\boldsymbol{x}$, *i.e.* $f(\boldsymbol{x}) = (f(x_i))_{1\leq i\leq n}$. We will also apply this for functions f acting on $\mathbb{F}_q^n \times \mathbb{F}_q^n$: for instance for two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_q^n$ and two positive integers a and b we denote by $\boldsymbol{x}^a\boldsymbol{y}^b$ the vector $(x_i^a y_i^b)_{1\leq i\leq n}$. 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 $\boldsymbol{A}^{(s)}$ which stands for the entries of $\boldsymbol{A}$ all raised to the power s, *i.e.* the entry (i,j) of $\boldsymbol{A}^{(s)}$ is equal to $a_{i,j}^s$. The scalar product between $\boldsymbol{x} = (x_i)_{1\leq i\leq n} \in \mathbb{F}_q^n$ and $\boldsymbol{y} = (y_i)_{1\leq i\leq n} \in \mathbb{F}_q^n$ is denoted by $\boldsymbol{x}\cdot\boldsymbol{y}$ and is defined by $\boldsymbol{x}\cdot\boldsymbol{y} = \sum_{i=1}^n x_i y_i$.

Ideals. Ideals are indicated by calligraphic $\mathcal{I}$. Given a sequence S of polynomials, $\mathcal{I}(S)$ refers to the polynomial ideal generated by this sequence. Given polynomials $f_1, \ldots, f_m$, we denote by $\mathcal{I}(f_1, \ldots, f_m)$ the ideal generated by them.

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. The *rate* of the code is equal to the ratio $\frac{k}{n}$. Linear codes can be specified compactly by a *generator matrix*, *i.e.* a $k \times n$ matrix $\boldsymbol{G}$ over $\mathbb{F}_q$ whose rows generate the associated k-dimensional linear code $\mathscr{C}$ over $\mathbb{F}_q$ or equivalently

$$\mathscr{C} = \{\boldsymbol{u}\boldsymbol{G} \mid \boldsymbol{u} \in \mathbb{F}_q^k\}.$$

The *dual* of a code $\mathscr{C}$ is defined as $\mathscr{C}^\perp \stackrel{\text{def}}{=} \{\boldsymbol{d} \in \mathbb{F}^n \mid \forall \boldsymbol{c} \in \mathscr{C},\ \boldsymbol{c}\cdot\boldsymbol{d} = 0\}$. We also consider the *shortening* operation which reduces the dimension and length of a code.

Definition 2.1 (Shortening). *Let $\mathscr{C}$ be an $[n,k]$-code and $I \subset \{1, ..., n\}$. The shortening of $\mathscr{C}$ at I is the $[n-|I|, \geq k-|I|]$-linear code given by*

$$\mathbf{Sh}_I(\mathscr{C}) \stackrel{\text{def}}{=} \{(c_j)_{j\neq I} \in \mathbb{F}_q^{n-|I|} \mid \boldsymbol{c} \in \mathscr{C},\ \forall i \in I,\ c_i = 0\}.$$

3 Preliminaries

3.1 Gröbner basis techniques for bilinear systems

Let $R = \mathbb{F}_q[x_1, \cdots x_{n_x}, y_1, \cdots, y_{n_y}]$ be a polynomial ring, let $\boldsymbol{x} = (x_1, \cdots, x_{n_x})$ and let $\boldsymbol{y} = (y_1, \cdots, y_{n_y})$. The bi-degree of a polynomial $f \in R$ is defined by

$$\boldsymbol{d} = (d_x, d_y) \stackrel{\text{def}}{=} \big(\deg_{\boldsymbol{x}}(f), \deg_{\boldsymbol{y}}(f)\big),$$

where $\deg_{\boldsymbol{x}}(f)$ (resp. $\deg_{\boldsymbol{y}}(f)$) is the partial degree of f with respect to $\boldsymbol{x}$ (resp. $\boldsymbol{y}$). Note that a polynomial of bi-degree $\boldsymbol{d}$ does not necessarily contain monomials of bi-degree $\boldsymbol{d}$. We use the partial order on bi-degrees defined by $(d'_x, d'_y) \leq (d_x, d_y)$ if and only if $d'_x \leq d_x$ and $d'_y \leq d_y$. We write $R_{\boldsymbol{d}}$ for the $\mathbb{F}_q$-vector space of bihomogeneous polynomials of bi-degree $\boldsymbol{d}$. These are the polynomials whose monomials all have the same bi-degree $\boldsymbol{d}$. We also define $R_{\leq \boldsymbol{d}} \stackrel{\text{def}}{=} \oplus_{\boldsymbol{d}'\leq\boldsymbol{d}} R_{\boldsymbol{d}'}$. A homogeneous bilinear system corresponds to a bihomogeneous system of bi-degree $(1,1)$. By abuse of terminology, we will also refer to an affine system as bilinear if its equations contain arbitrary monomials of bi-degree $\leq (1,1)$.

We introduce Macaulay matrices indexed by bi-degrees.

Definition 3.1 (Homogeneous Macaulay matrix). *Let $F \in R^m$ be a bihomogeneous system and let $\boldsymbol{d} \in \mathbb{N}^2$. The homogeneous Macaulay matrix of F in bi-degree $\boldsymbol{d}$ is the matrix $\boldsymbol{M}_{\boldsymbol{d}}(F)$ whose columns are indexed by all monomials $\nu \in R_{\boldsymbol{d}}$, rows are indexed by pairs (μ, f) for all monomials $\mu \in R$ and $f \in F$ such that $\mu f \in R_{\boldsymbol{d}}$, and coefficients are given by coef$(\nu, \mu f)$.*

Definition 3.2 (Affine Macaulay matrix). *Let $F \in R^m$ be a polynomial system and let $\boldsymbol{d} \in \mathbb{N}^2$. The affine Macaulay matrix of F in bi-degree $\boldsymbol{d}$ is the matrix $\boldsymbol{M}_{\leq \boldsymbol{d}}(F)$ whose columns are indexed by all monomials $\nu \in R_{\leq \boldsymbol{d}}$, rows are indexed by pairs (μ, f) for all monomials $\mu \in R$ and $f \in F$ such that $\mu f \in R_{\leq \boldsymbol{d}}$, and coefficients are given by coef$(\nu, \mu f)$.*

Such matrices appear in most solving algorithms for bilinear systems following Lazard's approach [Laz83]. A pioneering work in this area is the bihomogeneous adaptation of F5 [Fau02] given in [FSS11, §6.1], which considers several such matrices. In the overdetermined case, an adaptation of the XL algorithm [CKPS00] that solves an affine system F by applying Gaussian elimination or sparse linear algebra on a single $\boldsymbol{M}_{\leq \boldsymbol{d}}(F)$ was later used in [PST20, Beu21, BCV23, NRS25, BFM+25]. Just as with the standard grading, the main difficulty in the analysis is to find bi-degrees $\boldsymbol{d}$ at which such an XL approach can work.

This can be done using Hilbert bi-series. The Hilbert bi-series of a bihomogeneous ideal $\mathcal{I} \subset R$ is defined as

$$\mathrm{HS}_{R/\mathcal{I}}(s,t) = \textstyle\sum_{\boldsymbol{d} \in \mathbb{N}^2} \dim\left(R_{\boldsymbol{d}}/\mathcal{I}_{\boldsymbol{d}}\right) s^{d_x} t^{d_y},$$

where $\mathcal{I}_{\boldsymbol{d}} \stackrel{\text{def}}{=} \mathcal{I} \cap R_{\boldsymbol{d}}$. An explicit formula is known if the ideal $\mathcal{I}$ is generated by a bi-regular sequence [FSS11, Theorem 5.1], but this result does not readily extend to the overdetermined case $M > n_x + n_y$, where M represents the number of equations. In this setting, we note that [PST20, Beu21, NRS25, BFM+25] rely on a conjectured generating series

$$\frac{(1-st)^M}{(1-s)^{n_x}(1-t)^{n_y}} \tag{3.1}$$

to estimate the complexity of XL. This series was recently shown in Julia Sauvage's PhD thesis [Sau26] to coincide with the Hilbert bi-series of what is called a semi-bi-regular system. A sketch of justification can also be found in [PST20].

3.2 A determinant ideal

We introduce the ideal generated by the maximal minors of a $2 \times k$ matrix of variables with a natural bi-grading on the associated polynomial ring R.

Proposition 3.3. *The ideal $\mathcal{I}^{(k)} \stackrel{\text{def}}{=} \langle\, x_i y_j - x_j y_i \mid i,j \in [\![1,k]\!],\ i<j \,\rangle$ generated by all principal minors of the matrix*

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_k \\ y_1 & y_2 & \cdots & y_k \end{pmatrix}$$

has an associated Hilbert bi-series given by

$$\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) = \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^k(1-t)^k}. \tag{3.2}$$

The proof can be found in Appendix B. In this appendix, we also show that the coefficient of $s^a t^b$ in the Taylor expansion of this Hilbert bi-series, denoted by $[s^a t^b](\cdot)$ throughout the paper, admits a compact expression.

Lemma 3.4. *For any bi-degree $\boldsymbol{d} = (a,b) \in \mathbb{N}^2$, we have*

$$\dim(R_{\boldsymbol{d}}/\mathcal{I}^{(k)}_{\boldsymbol{d}}) = \left[s^a t^b\right] \mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) = \tbinom{k+a+b-1}{a+b}.$$

4 A New Modeling

In even characteristic, recall that a skew-symmetric matrix $\boldsymbol{M} = (m_{i,j})_{1 \leq i,j \leq D} \in \mathbb{F}_q^{D \times D}$ is simply a symmetric matrix with all diagonal entries equal to zero. Moreover, this matrix has rank at most two if and only if

$$\forall 1 \leq i \leq j \leq k \leq \ell \leq D,\ m_{i,j}m_{k,\ell} + m_{i,k}m_{j,\ell} + m_{i,\ell}m_{j,k} = 0, \tag{4.1}$$

the left hand-side of (4.1) being referred to as *a Pfaffian* of $\boldsymbol{M}$. This fact naturally leads to the so-called Pfaffian modeling used in [CMT23, BLT26] to build respectively a distinguisher and an attack on the McEliece scheme in some regime. Our work introduces a new way to search for matrices of rank 2 in a vector space of skew-symmetric matrices in characteristic 2, obtained by parameterizing the variety of all such matrices and then plugging this parametrization into linear equations expressing that the matrices we target belong to the desired space.

4.1 The parametrization

Lemma 4.1. *Let $\mathbb{F}_q$ be a field of characteristic 2 and let $\boldsymbol{M}$ be skew-symmetric in $\mathbb{F}_q^{D \times D}$ such that $\mathbf{Rank}(\boldsymbol{M}) \leq 2$. There exist $\boldsymbol{u},\ \boldsymbol{v} \in \mathbb{F}_q^D$ such that*

$$\boldsymbol{M} = \boldsymbol{u}^\intercal \boldsymbol{v} + \boldsymbol{v}^\intercal \boldsymbol{u}.$$

Proof. If $\boldsymbol{M} = 0$ this is trivial by taking $\boldsymbol{u} = \boldsymbol{v} = \boldsymbol{0}$. Otherwise up to scaling we can assume that one entry m_{i_0,j_0} of $\boldsymbol{M}$ is equal to 1, in which case (4.1) specializes to

$$m_{i,j} = m_{i_0,i}m_{j_0,j} + m_{i_0,j}m_{j_0,i}$$

for all $i, j \in [\![1, D]\!]$. It thus suffices to define $\boldsymbol{u},\ \boldsymbol{v} \in \mathbb{F}_q^D$ by $u_t = m_{i_0,t}$ and $v_t = m_{j_0,t}$ for any $t \in [\![1, D]\!]$. □

4.2 The parameterized modeling

We look for a rank-2 skew-symmetric matrix $\boldsymbol{M}$ in the vector space generated by K skew-symmetric matrices $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ of size $D \times D$. We furthermore impose that one entry of $\boldsymbol{M}$ is equal to 1, for instance $m_{D-1,D}$.

Modeling 1 (Parametrized modeling). *The parameterized modeling expressing that a skew-symmetric matrix*

$$\boldsymbol{M} = (m_{i,j})_{\substack{i \in [\![1,D]\!] \\ j \in [\![1,D]\!]}}$$

of size $D \times D$ belongs to the space generated by K skew-symmetric matrices $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ is of rank 2 and satisfies $m_{D-1,D} = 1$ is given by

Unknowns: $\boldsymbol{x} = (x_1, \cdots, x_{D-2}),\ \boldsymbol{y} = (y_1, \cdots, y_{D-2})$

Equations: $M = \binom{D}{2} - K$ *bilinear equations in the unknowns $\boldsymbol{x}$ and $\boldsymbol{y}$ given by*

$$L_\ell(\boldsymbol{N}) = 0,$$

where

$$\boldsymbol{N} \stackrel{\text{def}}{=} (\boldsymbol{x}, 1, 0)^\intercal (\boldsymbol{y}, 0, 1) + (\boldsymbol{y}, 0, 1)^\intercal (\boldsymbol{x}, 1, 0),$$

and where the L_ℓ's are linear relations between the coefficients of any element in the span of $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ for $\ell \in [\![1, \binom{D}{2} - K]\!]$.

Notation 1. *In the following, we denote by F the (affine) bilinear system given by Modeling 1.*

We cannot say at this stage that this modeling approach is more relevant than the Pfaffian approach since we have not yet detailed the complexity of solving Modeling 1. Still, the number of variables is only linear in D, while it is quadratic in D in the Pfaffian modeling. In Appendix E, we provide a more detailed discussion of the relationship between the Pfaffian system and our system; this discussion will not be used afterwards.

A crucial property we will use in the analysis is that the bihomogeneous parts of bi-degree $(1,1)$ in the equations of F are included in the determinantal ideal $\mathcal{I}^{(D-2)}$ of Proposition 3.3, and moreover that without the implicit specialization $x_{D-1}=1$, $x_D=0$, $y_{D-1}=0$, and $y_D=1$, we obtain an ideal included in $\mathcal{I}^{(D)}$.

5 Understanding Shortening with the Multiplicative Subcode

An important ingredient for decreasing the complexity of our distinguisher and our attack is to use shortening. This allows to decrease significantly the dimension of the code and therefore the number of unknowns in the algebraic system while still keeping rank-2 matrices in the associated code of quadratic relations. The issue here is how much we can shorten while still keeping this property. A partial answer was given in [BLT26] where a lower bound on the number of times we can shorten while still keeping rank-2 matrices in the associated code of quadratic relations was given. This lower bound already shows that we can reduce the dimension from $r \cdot m$ to something which is of order $o(r \cdot m)$. The argument which is used there builds upon [Ran25, Cor. 5].

5.1 The multiplicative subcode

We realize here that we can further reduce the code dimension compared to [BLT26] by using an improvement of Corollary 5 of [Ran25]. Such an improvement relies on Remark 1 in the latest eprint version of the paper [Ran24].

Remark 1 in [Ran24] basically says that we can shorten more than predicted in the original paper, with a sketch of an argument mentioning a particular subcode of the dual of the Goppa code. In our case, this code is not only helpful for the same purpose of shortening, but it also allows us to understand a key component of the attacks of [Mor25, BLT26], namely the subcode of the dual of the Goppa code we get by taking the subspace generated by all row spans of the rank-2 matrices we obtain with the Pfaffian modeling (note that this also applies to our modeling). This code has a multiplicative structure and we call it the *multiplicative subcode* (no particular name for it was given in [Ran24]).

Definition 5.1 (Multiplicative subcode of the extended dual of an alternant code). *Let $\mathscr{C}$ be the extension over $\mathbb{F}_{q^m}$ of the dual of an alternant code of length n over $\mathbb{F}_q$ of extension degree m with support $\boldsymbol{x}=(x_1,\cdots,x_n)\in\mathbb{F}_{q^m}^n$. We call $\mathscr{M}^\ell(\mathscr{C})$ its multiplicative subcode of order ℓ defined inductively by*

$$\begin{aligned}\mathscr{M}^0(\mathscr{C}) &\stackrel{\text{def}}{=} \mathscr{C}\\ \mathscr{M}^\ell(\mathscr{C}) &\stackrel{\text{def}}{=} \mathscr{M}^{\ell-1}(\mathscr{C}) \cap \boldsymbol{x} \star \mathscr{M}^{\ell-1}(\mathscr{C}) \quad \text{for } \ell \geq 1.\end{aligned}$$

When $\ell=1$ we will refer to this code simply as the multiplicative subcode *of $\mathscr{C}$ and denote it by $\mathscr{M}(\mathscr{C})$.*

5.2 The main result

The result showing how many times we can shorten is governed by the dimension of the multiplicative subcode of order 2 as shown by

Proposition 5.2. *Let $\mathscr{C} \stackrel{\text{def}}{=} (\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^\perp)_{\mathbb{F}_{q^m}}$ and $s \stackrel{\text{def}}{=} \dim \mathscr{M}^2(\mathscr{C})$. If we shorten $\mathscr{C}$ at $s-1$ positions, the matrix code of quadratic relations $\mathscr{C}_{\text{mat}}$ of the resulting shortened code contains at least one rank-2 matrix.*

5.3 Proof of Proposition 5.2

We decompose the proof into several steps. Before that we introduce some notation. We start from a code $\mathscr{C}$ as in the statement of the proposition and we denote by k its dimension.

In order to understand whether the matrix code $\mathscr{C}_{\mathrm{mat}}$ of $\mathscr{C}_s$ which is $\mathscr{C}$ shortened in s positions $j_1, \cdots, j_s$ contains rank-2 matrices, let us introduce $\mathscr{C}_\ell$ for $\ell \in [\![1, s]\!]$ which is $\mathscr{C}$ shortened in the ℓ positions $j_1, \cdots, j_\ell$. Furthermore, let $(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_k)$ be a basis of $\mathscr{C}$ such that $\langle \boldsymbol{c}_1, \cdots, \boldsymbol{c}_{k-\ell} \rangle_{\mathbb{F}_{q^m}} \subseteq \mathscr{C}_\ell$ for all ℓ in $[\![1, s]\!]$ Finally, in the same vein as [Ran24, Ran25, BLT26], we use the evaluation map

$$\begin{aligned} \mathrm{ev} : \mathcal{R} &\to \mathbb{F}_{q^m}^n \\ f &\mapsto f(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_k) \end{aligned}$$

where $\mathcal{R}$ is the polynomial ring $\mathcal{R} = \mathbb{F}_{q^m}[X_1, \cdots, X_k]$. We denote by $\mathcal{L}$ and $\mathcal{Q}$ the subspaces of linear and quadratic forms of $\mathcal{R}$, respectively. We may identify any element of $\mathcal{L}$ with a codeword of $\mathscr{C}$ and denote by L the one-to-one map that sends an element of $\mathscr{C}$ to $\mathcal{L}$. Finally, we denote by $I_2(\mathscr{C})$ the kernel of ev restricted to $\mathcal{Q}$, with a slight abuse of notation, as this kernel depends on $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k)$, rather than solely on $\mathscr{C}$. This $I_2(\mathscr{C})$ is naturally identified with the code of quadratic relations we are considering.

Step 1: showing that $I_2(\mathscr{C})$ contains all principal minors of a certain $2 \times d$ matrix $\boldsymbol{\Phi} \in \mathcal{L}^{2\times d}$. The first step is as in [Ran24, Ran25] to construct a matrix $\boldsymbol{\Phi}$ of size $2 \times d$ over $\mathcal{R}$, where d is an appropriate integer which is such that any principal minor of this matrix is in $I_2(\mathscr{C})$. The matrix $\boldsymbol{\Phi}$ which is of interest in our case is given in [Ran24, Remark 1] and we make it explicit.

Lemma 5.3. *Let W be the subspace of elements f of $\mathcal{L}$ which are such that $\boldsymbol{x} \star \mathrm{ev}(f)$ belongs to $\mathscr{C}$. We fix a basis $(f_1, \cdots, f_d)$ of W and we let $\boldsymbol{\Phi}$ be the matrix*

$$\boldsymbol{\Phi} \stackrel{\text{def}}{=} \begin{bmatrix} f_1 & f_2 & \cdots & f_d \\ L(\boldsymbol{x} \star \mathrm{ev}(f_1)) & L(\boldsymbol{x} \star \mathrm{ev}(f_2)) & \cdots & L(\boldsymbol{x} \star \mathrm{ev}(f_d)) \end{bmatrix}.$$

Any 2×2 minor of $\boldsymbol{\Phi}$ is in $I_2(\mathscr{C})$.

Proof. We have to prove that for all i and j in $[\![1, d]\!]$, $i \neq j$, ev vanishes on the homogeneous quadratic polynomial (possibly null):

$$f_i L(\boldsymbol{x} \star \mathrm{ev}(f_j)) - f_j L(\boldsymbol{x} \star \mathrm{ev}(f_i)).$$

This follows immediately from the fact that

$$\begin{aligned} \mathrm{ev}\left(f_i L(\boldsymbol{x} \star \mathrm{ev}(f_j)) - f_j L(\boldsymbol{x} \star \mathrm{ev}(f_i))\right) &= \mathrm{ev}(f_i) \star \boldsymbol{x} \star \mathrm{ev}(f_j) - \mathrm{ev}(f_j) \star \boldsymbol{x} \star \mathrm{ev}(f_i) \\ &= \boldsymbol{0}. \end{aligned}$$

□

It will be convenient to introduce from now on the following notation

Notation 2. *We let V be the subspace of $\mathcal{L}^2$ generated by the columns of $\boldsymbol{\Phi}$.*

Step 2: proving the same property for $\mathscr{C}_j$ for a matrix $\boldsymbol{\Phi}_j \in \mathcal{L}^{2\times(d-j)}$. The second ingredient consists in showing that by shortening $\mathscr{C}$ in j positions to obtain a code $\mathscr{C}_j$ we may still define a $2 \times (d-j)$ matrix $\boldsymbol{\Phi}_j$ whose principal minors all belong to $I_2(\mathscr{C}_j)$, for any $j \in [\![1, s]\!]$. This follows almost word by word the discussion in [BLT26, §3.1] that itself is basically nothing but the approach of [Ran25, §3 (shortening)]. Since [BLT26] deals with a slightly different (and shorter) $\boldsymbol{\Phi}$ we still detail the proof. We have similarly to [BLT26, prop. 3.1]

Proposition 5.4. *For $j \in [\![1, s]\!]$, let $\mathcal{R}_j = \mathbb{F}_{q^m}[X_1, \cdots, X_{k-j}]$ and let $V_j \stackrel{\text{def}}{=} V \cap \mathcal{R}_j^2$. We let $\mathbf{\Phi}_j$ be a matrix whose columns generate V_j. All 2×2 minors of $\mathbf{\Phi}_j$ belong to $I_2(\mathscr{C}_j)$.*

Proof. Since $V_j \subseteq V$ and by the multilinearity of the determinant, any 2×2 minor of $\mathbf{\Phi}_j$ is a linear combination of minors of $\mathbf{\Phi}$. Thus the associated homogeneous quadratic polynomial p evaluates to $\mathbf{0}$ by ev. Since it also belongs to $\mathcal{R}_j$ by definition of V_j, we conclude that $p \in I_2(\mathscr{C}_j)$. □

Step 2 is completed by showing that $\dim V_j \geq \dim V - j$. For this we simply slightly adapt [Ran25, Prop. 4] or [BLT26, Lem. 3.2] to our setting.

Lemma 5.5. *We have*

$$\dim V_j \geq \dim V_{j-1} - 1, \ \forall j \in [\![1, s]\!] \tag{5.1}$$
$$\dim V_j \geq \dim V - j \tag{5.2}$$

where $V_0 \stackrel{\text{def}}{=} V$.

The proof is basically identical to that of [BLT26, Lem. 3.2], see [BLT26, §A].

Step 3: showing that some of the principal minors give rank 2 matrices in $\mathscr{C}_{\mathbf{mat}}$ of $\mathscr{C}_{\boldsymbol{s}}$. As explained in [BLT26, §3.1], Lemma 5.5 shows that for any $j \in [\![1, s]\!]$, the matrix $\mathbf{\Phi}_j$ contains at least $d - j$ columns, which gives many quadratic relations which are in $I_2(\mathscr{C}_j)$ by taking all its 2×2 minors. These yield matrices of rank at most 4 in $\mathscr{C}_{\text{mat}}$.

We can actually directly get matrices of rank 2 by following the exact same path as in [BLT26, §3.1], as long as j is sufficiently small. The idea is that for a suitable choice of the basis of V_j determining the columns of $\mathbf{\Phi}_j$, one can find a 2×2 minor of $\mathbf{\Phi}_j$ of the form $\begin{vmatrix} a & b \\ b & c \end{vmatrix}$. For this we consider for $j \in [\![0, s]\!]$ the two subspaces V_j^1 and V_j^2 of $\mathcal{R}_j$ as the projection of V_j on the first entry or on the second entry, *i.e.* $V_j^i = \pi_i(V_j)$ with $\pi_i(x_1, x_2) = x_i$ with $(x_1, x_2) \in \mathcal{R}^2$. Note that we defined $V_0 \stackrel{\text{def}}{=} V$ and we also let $\mathbf{\Phi}_0 = \mathbf{\Phi}$, $\mathcal{R}_0 \stackrel{\text{def}}{=} \mathcal{R}$. To spot 2×2 minors as above where the same entry appears in different rows, the approach of [BLT26] is to look at the intersection $V_j^1 \cap V_j^2$. It is implicitly proved in the proof of Theorem 3.5 in [BLT26] that

Lemma 5.6. *If $\dim\left(V_j^1 \cap V_j^2\right) \geq 1$, then $I_2(\mathscr{C}_j)$ contains at least one quadratic form of bilinear rank 2.*

We give in the appendix a proof of this statement. Then the following lemma shows how this intersection survives after shortening.

Lemma 5.7. *Let $d' \stackrel{\text{def}}{=} \dim V_0^1 \cap V_0^2$. We have for any $j \in [\![0, d']\!]$,*

$$\dim\left(V_j^1 \cap V_j^2\right) \geq d' - j.$$

The proof is in essence nothing but the proof of [BLT26, Lem. 3.3] adapted to our setting. Now what is missing to apply Lemma 5.6 is just a lower bound on d' before shortening. We give it in

Lemma 5.8. *We have*

$$\dim V_0^1 \cap V_0^2 \geq \dim \mathscr{M}^2(\mathscr{C}).$$

Proof. Consider a basis $(\boldsymbol{d}_1, \cdots, \boldsymbol{d}_{d''})$ of $\mathscr{M}^2(\mathscr{C})$ where $d'' \stackrel{\text{def}}{=} \dim \mathscr{M}^2(\mathscr{C})$. Let $f_i \stackrel{\text{def}}{=} L(\boldsymbol{d}_i)$ for $i \in [\![1, d'']\!]$. Since $\boldsymbol{d}_i \in \mathscr{M}^2(\mathscr{C})$ we have that $\boldsymbol{d}_i$, $\boldsymbol{x} \star \boldsymbol{d}_i$ and $\boldsymbol{x}^2 \star \boldsymbol{d}_i$ all belong to $\mathscr{C}$. We may therefore define $g_i \stackrel{\text{def}}{=} L(\boldsymbol{x} \star \boldsymbol{d}_i)$ and $h_i \stackrel{\text{def}}{=} L(\boldsymbol{x}^2 \star \boldsymbol{d}_i)$ for all $i \in [\![1, d'']\!]$. Clearly $\begin{bmatrix} f_i \\ g_i \end{bmatrix}$ and $\begin{bmatrix} g_i \\ h_i \end{bmatrix}$ both belong to $V_0 = V$. This implies that g_i belongs to $V_0^1 \cap V_0^2$ by definition. The g_i's are all independent. This finishes the proof. □

Wrap-up. We are now ready to prove Proposition 5.2.

Proof (of Proposition 5.2). We use Lemma 5.6 to deduce that as long $\dim(V_j^1 \cap V_j^2)$ is positive, $I_2(\mathscr{C})$ contains a quadratic form of bilinear rank 2. By Lemma 5.7 and Lemma 5.8 we know that this quantity is positive for $j < \dim(\mathscr{M}^2)$. □

5.4 Comparison with shortening in [Ran25]

It is insightful to compare how much we can shorten in our case versus how much we can shorten in the case of [Ran25]. It is readily seen from [Ran24, Remark 1] that if we ignore the small defect heuristic of [Ran25, §4] that has only a marginal effect, the syzygy distinguisher of [Ran25] allows to shorten $\dim \mathscr{M} - 1$ times and still works for distinguishing between the random case and the alternant/Goppa case. For our distinguisher we can only shorten $\dim \mathscr{M}^2 - 1$ times. This is smaller since $\mathscr{M}^2 \subset \mathscr{M}$.

6 A New Distinguisher

Our distinguisher follows the framework of [CMT23], except that we replace the Pfaffian modeling with our new parameterized modeling. In this framework, the set of matrices $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ in Modeling 1 corresponds to a basis for the code of quadratic relations $\mathscr{C}_{\mathrm{mat}}$ associated to an $[n,k]$-code $\mathscr{C}$, where the number of rows and columns is $D = k$. In our case, this code $\mathscr{C}$ will be a shortening of the extension over $\mathbb{F}_{q^m}$ of the dual of the Goppa code over $\mathbb{F}_q$ of extension degree m that we consider. First, we may assume that we are outside the square-distinguishable regime, i.e., that $\mathscr{C}^{*2} = \mathbb{F}_q^n$. In this case,

$$K = \dim \mathscr{C}_{\mathrm{mat}} = \binom{k+1}{2} - \dim \mathscr{C}^{*2} = \binom{k+1}{2} - n = \binom{k}{2} - (n-k).$$

If we keep calling M the number of equations in our parameterized modeling F, we thus have:

$$M = \binom{k}{2} - K = n - k.$$

We also assume that we are in the regime where we do not expect a matrix of rank 2 in $\mathscr{C}_{\mathrm{mat}}$ when this space is associated with a random $[n,k]$-code. The corresponding constraint on the parameters is according to [CMT23, Prop. 10]:

Assumption 2. *We assume that*

$$n > 3k - 3.$$

Under Assumption 2, the system F is overdetermined, since the condition amounts to $n - k > 2(k-2) + 1$ which corresponds to $\underbrace{M}_{\#\text{ equations}} > \underbrace{2(k-2)}_{\#\text{ unknowns}} + 1$. A random system with the same ratio between equations and variables has no solution with overwhelming probability, but in our case we can be more certain because of what we said on $\mathscr{C}_{\mathrm{mat}}$. In other words, we are in a case when Modeling 1 applied to a random $[n,k]$-code $\mathscr{C}$ has no solutions.

6.1 Showing that F has no solution in the random case

A natural candidate for distinguishing the two cases via bi-graded Macaulay matrices is a bi-degree at which we can show that F has no solution in the random case, since F does admit a solution in the Goppa case after our shortening. We thus look for the analogue of the vanishing of the Hilbert function in [CMT23].

More precisely, we are interested in bi-degrees $\boldsymbol{d} = (a,b)$ such that the polynomial 1 can be found in the rowspace of $\boldsymbol{M}_{\leq \boldsymbol{d}}(F)$ when F has no solution. To find those bi-degrees, we consider

the homogenized system $F^{\text{hom}} \subset R^{\text{hom}} \stackrel{\text{def}}{=} \mathbb{F}_q[x_1, \cdots, x_{k-2}, y_1, \cdots, y_{k-2}, h_x, h_y]$ that we obtain by replacing the affine equations $x_{k-1} = 1$ and $y_k = 1$ with $x_{k-1} = h_x$ and $y_k = h_y$ respectively, where h_x and h_y are homogenization variables. Note that F^{hom} is still overdetermined under Assumption 2 (since $n - k \geq 2(k-1)$). An important property of this homogenized system for analyzing the behavior of Gröbner basis algorithms is that its equations are linear combinations of the maximal minors of the matrix

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_{k-2} & h_x & 0 \\ y_1 & y_2 & \cdots & y_{k-2} & 0 & h_y \end{pmatrix}.$$

If we let $\mathcal{J}$ be the ideal generated by these maximal minors, this implies that

$$\text{RowSpace}(\boldsymbol{M}_{\boldsymbol{d}}(F)) \subset \mathcal{J}_{\boldsymbol{d}},$$

where we recall that $\mathcal{J}_{\boldsymbol{d}} = \mathcal{J} \cap (R^{\text{hom}})_{\boldsymbol{d}}$. This holds for any bi-degree $\boldsymbol{d}$.

In the random case, when $\mathscr{C}_{\text{mat}}$ does not contain any rank-2 matrix, we expect this inclusion to become an equality for sufficiently large $\boldsymbol{d}$. It is not enough that $\mathscr{C}_{\text{mat}}$ contains no rank-2 matrices that correspond to solutions of F to argue that at some point $\mathcal{J}_{\boldsymbol{d}} = (R^{\text{hom}})_{\boldsymbol{d}}$, since there are other rank-2 matrices that may give solutions to F^{hom} at infinity which do not correspond to solutions of F. As $h_x h_y \in \mathcal{J}$, this equality implies that $h_x^a h_y^b \in \text{RowSpace}(\boldsymbol{M}_{\boldsymbol{d}}(F^{\text{hom}}))$, and thus we will find 1 in the rowspace of $\boldsymbol{M}_{\leq \boldsymbol{d}}(F)$. On the contrary, in the Goppa case, equality cannot happen because we have solutions.

The rank of the matrix $\boldsymbol{M}_{\boldsymbol{d}}(F^{\text{hom}})$ is expected to match the maximal number of equations at this bi-degree for a generic bilinear system, as given by Equation (3.1) with $m = n - k$ and $n_x = n_y = k - 1$,

$$E_{\leq}(a,b) \stackrel{\text{def}}{=} \left[s^a t^b\right] \frac{1}{(1-s)^{k-1}(1-t)^{k-1}} - \frac{(1-st)^{n-k}}{(1-s)^{k-1}(1-t)^{k-1}},$$

as long as this value is smaller than the dimension of $\mathcal{J}_{(a,b)}$. The Hilbert bi-series of $\mathcal{J}$ follows from the same argument as in the proof of Proposition 3.3.

Lemma 6.1. *The ideal $\mathcal{J}$ generated by all principal minors of the matrix*

$$\boldsymbol{Z}_1 \stackrel{\text{def}}{=} \begin{pmatrix} x_1 & x_2 & \cdots & x_{k-2} & h_x & 0 \\ y_1 & y_2 & \cdots & y_{k-2} & 0 & h_y \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} \boldsymbol{Z}_0 & \begin{matrix} h_x \\ 0 \end{matrix} & \begin{matrix} 0 \\ h_y \end{matrix} \end{pmatrix}$$

has an associated Hilbert bi-series given by

$$HS_{R^{hom}/\mathcal{J}}(s,t) = \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^{k-1}(1-t)^{k-1}}.$$

The proof can be found in Appendix B. Overall, we find:

$$D_{\leq}(a,b) \stackrel{\text{def}}{=} \dim \mathcal{J}_{(a,b)} = \left[s^a t^b\right] \frac{1}{(1-s)^{k-1}(1-t)^{k-1}} - \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^{k-1}(1-t)^{k-1}}.$$

We finish with a conjecture on the bi-degrees at which we expect to show that F has no solutions in the random case. We have simplified the relevant inequality $E_{\leq}(a,b) \geq D_{\leq}(a,b)$ by clearing out the common term $\frac{1}{(1-s)^{k-1}(1-t)^{k-1}}$.

Conjecture 1 (Random case). *Let F be Modeling 1 applied to a matrix code $\mathscr{C}_{\text{mat}}$ associated to a random code such that $\mathscr{C}_{\text{mat}}$ does not contain any rank-2 matrix (this requires Assumption 2). As long as*

$$\left[s^a t^b\right] \frac{(1-st)^{n-k}}{(1-s)^{k-1}(1-t)^{k-1}} \leq \left[s^a t^b\right] \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^{k-1}(1-t)^{k-1}}, \tag{6.1}$$

the polynomial 1 can be found in the rowspace of $\boldsymbol{M}_{\leq(a,b)}(F)$. Otherwise, the rank of $\boldsymbol{M}_{\leq(a,b)}(F)$ is equal to $E_{\leq}(a,b)$.

The right-hand side of Equation (6.1) can simplified as follows

$$\begin{aligned}\left[s^a t^b\right](1-s)(1-t)\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) &= \left[s^a t^b\right]\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) + \left[s^{a-1}t^{b-1}\right]\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t)\\ &\quad - \left[s^{a-1}t^{b}\right]\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) - \left[s^{a}t^{b-1}\right]\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t)\\ &= \tbinom{k+a+b-1}{a+b} + \tbinom{k+a+b-3}{a+b-2} - 2\tbinom{k+a+b-2}{a+b-1}\\ &= \tbinom{k+a+b-3}{a+b},\end{aligned}$$

by using Lemma 3.4 in the second line and Pascal's rule in the third line. As long as $a \geq 1$ and $b \geq 1$, we obtain that Equation (6.1) is equivalent to

$$\left[s^a t^b\right]\frac{(1-st)^{n-k}}{(1-s)^{k-1}(1-t)^{k-1}} \leq \binom{k+a+b-3}{a+b}.$$

If Conjecture 1 holds, it is clear that we can distinguish by computing a row echelon form of $\boldsymbol{M}_{\leq(a,b)}(F)$ at a bi-degree (a,b) such that $E_{\leq}(a,b) \geq D_{\leq}(a,b)$. Thus we introduce the following notion.

Definition 6.2 (Consistency bi-degree). *We call (a,b) a consistency bi-degree for code length n and code dimension k if and only if*

$$\left[s^a t^b\right]\frac{(1-st)^{n-k}}{(1-s)^{k-1}(1-t)^{k-1}} \leq \binom{k+a+b-3}{a+b}. \tag{6.2}$$

6.2 Degree falls

We may find *degree falls* in bi-degrees (a,b) which are lower than the consistency bi-degrees predicted by Conjecture 1. This is relevant if we can already distinguish at these lower degrees.

By degree fall polynomials, we refer here to polynomials generated at a given bi-degree whose actual bi-degree is strictly lower, but we do not control if such polynomials are linearly independent when we find them or if they are already in the rowspan of Macaulay matrices at lower bi-degrees. We obtain them from syzygies in the system F^{top}, which consists of the bihomogeneous parts of bi-degree $(1,1)$ in F. We have already said at the end of Section 4 that the equations of F^{top} were included in $\mathcal{I}^{(k-2)}$. In particular, we can use the above reasoning applied to F^{top} instead of F^{hom} and $\mathcal{I}^{(k-2)}$ instead of $\mathcal{J}$ to predict combinatorial syzygies once we reach the maximum possible number of monomials.

Conjecture 2 (Random case). *Under the same hypotheses as in Conjecture 1, we expect degree falls to occur at bi-degree (a,b) whenever*

$$\left[s^a t^b\right]\frac{(1-st)^{n-k}}{(1-s)^{k-2}(1-t)^{k-2}} < \left[s^a t^b\right]\frac{s(1-t)^{k-2} - t(1-s)^{k-2}}{(s-t)(1-s)^{k-2}(1-t)^{k-2}}. \tag{6.3}$$

Motivated by Conjecture 2 we introduce the following notion. Here again we have used Lemma 3.4 to simplify the right-hand side of Equation (6.3).

Definition 6.3 (Critical bi-degree). *We call (a,b) a critical bi-degree for code length n and code dimension k if and only if*

$$\left[s^a t^b\right]\frac{(1-st)^{n-k}}{(1-s)^{k-2}(1-t)^{k-2}} \leq \binom{k+a+b-3}{a+b}. \tag{6.4}$$

Note that there is no clear reason why one should be able to distinguish at a critical bi-degree (a,b), as opposed to at a consistency bi-degree (a,b). We discuss this more in Appendix C. In fact, even in the case of an affine system without any bilinear structure, it is known that the first degree fall is not always a good measure of the complexity of solving it.

What we would do in the most general setting at such a bi-degree (a, b) is to compute degree fall polynomials from vectors in the left kernel of $\boldsymbol{M}_{(a,b)}(F^{\text{top}})$, hoping to get a discrepancy via further computations on these polynomials whose cost does not exceed that of their generation. In particular, we will assume that the linear algebra step on $\boldsymbol{M}_{(a,b)}(F^{\text{top}})$ represents the dominant cost.

Remark 6.4 (Edge cases for Conjectures 1 and 2). Conjectures 1 and 2 must in fact be restricted to bi-degrees (d_x, d_y) such that $\min(d_x, d_y) < d$, where d denotes the degree of regularity of the Pfaffian modeling of [CMT23]. Indeed, by definition of the degree of regularity, there will be a nontrivial intersection between the parity-check equations $\mathcal{L}$ augmented in degree d and the Pfaffian relations $\mathcal{P}$ augmented in the same degree in their modeling, since

$$\langle \mathcal{L} \rangle_d + \langle \mathcal{P} \rangle_d = \mathbb{F}_{q^m}[m_{i,j}]_d.$$

In other words, some Pfaffian equations will belong to $\langle \mathcal{L} \rangle_d$. Now, translating this back to our modeling by substituting $m_{i,j} = x_i y_j + x_j y_i$, these equations vanish, thus yielding as many syzygies as the dimension of this intersection. Note that we do not need to understand what happens for bi-degrees (d_x, d_y) such that $\min(d_x, d_y) \geq d$, since [CMT23] already distinguishes in degree d and thus we cannot obtain better than [CMT23] by considering the associated Macaulay matrices.

6.3 Complexity of the distinguisher

We give upper bounds on the complexity of our distinguisher based on Definition 6.2 or Definition 6.3. In the first case, we perform linear algebra operations on an affine Macaulay matrix $\boldsymbol{M}_{\leq \boldsymbol{d}}(F)$ where $\boldsymbol{d}$ is a consistency bi-degree, while in the second case we work on $\boldsymbol{M}_{\boldsymbol{d}}(F^{\text{top}})$ where $\boldsymbol{d}$ is a critical bi-degree. In both cases, we can either use dense linear algebra or Wiedemann's algorithm [Wie86] taking advantage of the sparsity of the Macaulay matrices.

Our Macaulay matrices are clearly sparse. The only potential issue is that, at the bi-degrees of interest, they are rectangular, with slightly more columns than rows due to the determinantal structure, rather than square. This is in fact not an issue. Indeed, assume that we have a rectangular matrix $\boldsymbol{M}$ of size $A \times B$, for which we want to determine whether it has rank D or rank strictly smaller than a predicted value D, and which is sparse in the sense that it has bounded row weight w_1 and bounded column weight w_2. Then we can simply multiply on the left with a sparse random matrix $\boldsymbol{A}$ of size $D \times A$ and on the right with a sparse random matrix $\boldsymbol{B}$ of size $B \times D$. To check whether $\boldsymbol{M}$ has rank D we check with Wiedemann's algorithm that the square $D \times D$ matrix $\boldsymbol{A} \cdot \boldsymbol{M} \cdot \boldsymbol{B}$ has full rank D. We can choose the row and column weight so that the multiplication by $\boldsymbol{A}$ or $\boldsymbol{B}$ has the same cost as multiplying by $\boldsymbol{M}$. For instance we can choose the row weight of $\boldsymbol{A}$ to be w_2 and its column weight bounded by $\frac{w_2 \times D}{A}$. We proceed similarly with $\boldsymbol{B}$. The cost of Wiedemann's algorithm is then estimated as $\mathcal{O}(D \times N)$, where N is the number of nonzero entries in $\boldsymbol{M}$. This is a standard trick which was used (and its validity verified experimentally) in the case of the Pfaffian distinguisher in [CMT23, §5.4].

Proposition 6.5 gives the complexity of the version of our distinguisher based on the consistency bi-degree.

Proposition 6.5. *Let $\mathcal{D}$ be the set of consistency bi-degrees. The complexity of the distinguisher based on the consistency bi-degree is given by*

$$\mathcal{O}\left(\min_{(a,b)\in\mathcal{D}}\left(\min\left(\binom{k+a-2}{a}^{\omega}\binom{k+b-2}{b}^{\omega}, C_W(a,b)\right)\right)\right),$$

where ω is the exponent of linear algebra and where $C_W(a, b)$ is up to a constant the complexity of the Wiedemann's approach which is given by

$$C_W(a,b) \stackrel{\text{def}}{=} (n-k)k^2\binom{k+a-3}{a-1}\binom{k+b-3}{b-1}\binom{k+a-2}{a}\binom{k+b-2}{b}.$$

Proof. Recall that the ring R involves two blocks of $k-2$ variables. The number of columns in bi-degree $\leq (a,b)$ is equal to

$$\dim R_{\leq(a,b)} = \binom{k+a-2}{a}\binom{k+b-2}{b}.$$

This already yields the complexity of the dense linear algebra approach given at the left-hand side. For the Wiedemann's approach, we upper bound the rank D by this number of columns as well. The number N of non-zero entries in the Macaulay matrix is at most k^2 times the number of equations we generate, *i.e.*

$$(n-k)\dim R_{\leq(a-1,b-1)} = (n-k)\binom{k+a-3}{a-1}\binom{k+b-3}{b-1}.$$

This gives the formula for $C_W(a,b)$. □

Proposition 6.6 corresponds to critical bi-degrees. Here we do not use the Wiedemann's approach because computing the rank of $\boldsymbol{M_d}(F^{\mathrm{top}})$ does not always allow to distinguish.

Proposition 6.6. *Let $\mathcal{D}$ be the set of critical bi-degrees. The complexity of the distinguisher based on the critical bi-degree is given by*

$$\mathcal{O}\left(\min_{(a,b)\in\mathcal{D}}\binom{k+a-3}{a}^{\omega}\binom{k+b-3}{b}^{\omega}\right),$$

where ω is the exponent of linear algebra.

Proof. This follows from

$$\dim R_{(a,b)} = \binom{k+a-3}{a}\binom{k+b-3}{b}.$$

Remark 6.7. For either of the two notions of bi-degree we use, we can of course restrict ourselves to the subset of $\mathcal{D}$ obtained by keeping only the minimal elements with respect to $\leq$ (we get a subset $\mathcal{D}'$ of pairwise incomparable bi-degrees).

6.4 Application to Classic McEliece

We have applied this distinguisher to Classic McEliece and display in Table 6.1 its performance. Its complexity is greater than the complexity of the higher order distinguisher of [HW26], is more or less comparable to the syzygy distinguisher of [Ran25] and is way better than the complexity of the Pfaffian distinguisher of [CMT23] (note however that this distinguisher did not use shortening at that time).

Table 6.1: Complexity of the distinguisher proposed here compared to the complexity distinguishers of [CMT23, Ran25, HW26] on the Classic McEliece parameters. For each distinguisher, s refers to the relevant number of shortened positions. $\log_2 C_{\text{iter}}^{\text{CW}}$ [Ran25] refers to the logarithm of the complexity of the distinguisher of [Ran25] which is computed step by step. It consists in echelonizing at each step a big matrix. The exponent of linear algebra was chosen in [Ran25] to be the Coppersmith-Winograd constant $\omega = 2.373$. $\log_2 C_{\text{iter}}^{\text{CW}}$ [HW26] refers to the same quantity, but this time for the distinguisher of [HW26], where p is the degree at which it succeeds. We give $\log_2 C_{\text{crit}}^{\text{CW}}$ and $\log_2 C_{\text{cons}}^{\text{CW}}$ the complexities of our distinguishers, using respectively the consistency bi-degree and the critical bi-degree, where linear algebra is estimated with the same Coppersmith-Winograd constant $\omega = 2.373$. Since choosing such a constant for linear algebra is questionable we have also given the logarithm of the complexity by using instead Strassen's algorithm which corresponds to the linear algebra exponent $\omega = 2.81$. Finally we add the complexity $C_{\text{cons}}^{\text{Wied}}$ of Wiedemann's algorithm for the distinguisher using the consistency bi-degree. It should be noted that, by design, the number of distinct keys in `Classic McEliece` is at most 2^{256}, while the complexity of our distinguisher is much higher than that of exhaustive key search.

(n, r, m)	$(3488, 64, 12)$	$(4608, 96, 13)$	$(6688, 128, 13)$	$(6960, 119, 13)$	$(8192, 128, 13)$
$\log_2 C_{\text{sparse}}$ [CMT23]	2231	5643	6425	4822	4501
$\log_2 C_{\text{iter}}^{\text{CW}}$ [Ran25]	469	909	982	841	801
s [Ran25]	405	643	930	866	954
r [Ran25]	43	93	94	77	70
$\log_2 C_{\text{KW}}$ [Ran25]	401	772	834	716	683
$\log_2 C_{\text{iter}}^{\text{CW}}$ [HW26]	331	706	818	652	624
s	123	91	175	217	271
p	23	51	57	44	41
$\log_2 C_{\text{cons}}^{\text{CW}}$	515	979	1058	896	853
$\log_2 C_{\text{cons}}^{\text{S}}$	610	1159	1253	1060	1011
$\log_2 C_{\text{cons}}^{\text{Wied}}$	454	847	915	777	742
$(a, b)_{\text{cons}}$	(15,24)	(34,43)	(34,45)	(26,39)	(24,36)
$\log_2 C_{\text{crit}}^{\text{CW}}$	513	976	1057	888	851
$\log_2 C_{\text{crit}}^{\text{S}}$	607	1156	1252	1052	1009
$(a, b)_{\text{crit}}$	(14,25)	(32,45)	(33,46)	(31,33)	(23,37)
s	383	639	895	823	895

7 Asymptotic Behavior

In this section we derive the asymptotic behavior of our distinguisher and show in particular that it has subexponential complexity in the error correction capacity of the Goppa code (which is for constant rate proportional in the security level of the scheme).

7.1 Critical bi-degree of the form $(d, 1)$

The criterion whether a bi-degree of the form $(d, 1)$ or $(1, d)$ is critical or not is much simpler than in the general case and will be sufficient for our purpose. We namely have the following proposition.

Proposition 7.1. *The bi-degree $(d, 1)$ is critical for $[n, k]$ codes when $d \geq \frac{(k-2)^2-n-k+5}{n-2k+3}$.*

Proof. By definition and using the explicit expression of the coefficient of $s^d t$ in $\frac{(1-st)^{n-k}}{(1-s)^{k-2}(1-t)^{k-2}}$, we obtain that the bi-degree $(d, 1)$ is critical if and only if

$$(k-2)\tbinom{k+d-3}{d} - (n-k)\tbinom{k+d-4}{d-1} \leq \tbinom{k+d-2}{d+1}.$$

Expressing all binomials in function of $\binom{k+d-4}{d-1}$ and dividing by this quantity, this is equivalent to

$$(k-2)\tfrac{k+d-3}{d} - (n-k) \leq \tfrac{k+d-2}{d+1}\tfrac{k+d-3}{d}.$$

Clearing out the denominators, we get

$$\begin{aligned}(k+d-2)(k+d-3) &\geq (k-2)(k+d-3)(d+1) - (n-k)d(d+1)\\ (1-(k-2)+(n-k))\,d^2 + \big((2k-5)-(k-2)^2+(n-k)\big)\,d &\geq 0\\ (n-2k+3)\,d^2 + \big(-(k-2)^2+n+k-5\big)\,d &\geq 0.\end{aligned}$$

Since by assumption on the parameters $n > 3k-3$, we have $k < \frac{n+3}{2}$ and we eventually obtain

$$d \geq \tfrac{(k-2)^2-n-k+5}{n-2k+3}.$$

□

For constant $\frac{k}{n}$, the lower bound given by this proposition scales as k^2/n. In Appendix D, we show that the same conclusion holds for the least consistency bi-degree of the form $(d,1)$. This implies that for bi-degrees of this form at least, there is not much difference in terms of asymptotic complexity between relying on the critical bi-degree or on the consistency bi-degree.

7.2 Combining our distinguisher with shortening

A plain use of Proposition 7.1 together with Proposition 6.6 would show that as is also the case for the syzygy distinguisher of [Ran25], our distinguisher has exponential complexity in the codelength to distinguish constant rate codes. Our distinguisher has even a worse behavior since it only works for code rates below $\frac{1}{3}$. There is a way to improve the capacity of distinguishing the code by shortening the code. This changes the picture completely in our case, since this allows to distinguish in subexponential time alternant Goppa codes over $\mathbb{F}_q$ of length n and extension degree m at constant rate in the natural code regime where the codelength n, the alphabet size q and the extension degree m are such that $n = \Theta(q^m)$ at any constant code rate $R \in (0,1)$.

Theorem 7.2. *Assume that we have a family of proper alternant codes $(\mathscr{A}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ whose rates tend to a constant $R \in (0,1)$. Let n_i, r_i, m_i be respectively the length, degree and extension degree of $\mathscr{A}_i$ and assume that $n_i = \Theta(q^{m_i})$ and n_i tends to infinity as i tends to infinity. If Conjecture 1 holds, then we can distinguish the $\mathscr{A}_i$'s from random codes with complexity C upper bounded by*

$$C \leq q^{\frac{\omega(1-R)r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)^3}{R\log_q r_i}(1+o(1))}. \tag{7.1}$$

Remark 7.3. Notice that this is the same complexity as the syzygy distinguisher of [Ran25]. The reason is that basically the dimension of the shortened code we use to distinguish is of the same order in both cases and the degree in which we distinguish are asymptotically equivalent. We use our distinguisher at bi-degrees of type $(d,1)$ because it is easier to analyze asymptotically. The examples of distinguishers for Classic McEliece show that this is not optimal for cryptographic parameters and it might be that we can improve the complexity exponent by a multiplicative constant by using other bi-degrees.

8 Key Recovery Attack against the McEliece Scheme

We have explained how the new parameterized modeling leads to a more efficient distinguisher than the older Pfaffian modeling of [CMT23] and to a faster solving process than what was done in [BLT26] as well. We shall now explain how to use a matrix of rank 2 to recover an equivalent decoding algorithm for the public McEliece key. The attack that we explain here needs only one matrix of rank 2.

Throughout this section, we consider $\mathscr{C} = \mathscr{G}(\boldsymbol{x}, \Gamma)^{\perp}_{\mathbb{F}_{q^m}}$ the extension over $\mathbb{F}_{q^m}$ of the dual of a Goppa code of support $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ and irreducible (or at least square-free) Goppa polynomial Γ of degree r. We assume that a rank-2 matrix $\boldsymbol{M}$ has been computed inside the matrix code of relations of $\mathscr{C}$ with respect a public basis given by the rows of the public generator matrix $\boldsymbol{G}_{\text{pub}}$. As explained in [BLT26, §5.3], the matrix $\boldsymbol{M}$ yields three codewords $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathscr{C}$ such that $\boldsymbol{u} \star \boldsymbol{v} = \boldsymbol{w}^2$ which are obtained as follows:

– $\boldsymbol{u} = \boldsymbol{\lambda}\boldsymbol{G}_{\text{pub}}$, $\boldsymbol{v} = \boldsymbol{\mu}\boldsymbol{G}_{\text{pub}}$ where $(\boldsymbol{\lambda}, \boldsymbol{\mu})$ is a basis of the rowspace of $\boldsymbol{M}$;
– $\boldsymbol{w} = (\boldsymbol{u} \star \boldsymbol{v})^{2^{m-1}}$.

Our attack follows the classical path consisting in recovering an alternative support $\boldsymbol{x}'$ that describes the same code $\mathscr{C}$ (possibly with a different multiplier), and then an efficient decoding algorithm up to r errors for $\mathscr{C}^\perp$.

Algorithm 8.1 Key recovery attack against McEliece

Require: Public generator matrix $\boldsymbol{G}_{\text{pub}}$ of $\mathscr{C} = \mathscr{G}(\boldsymbol{x}, \Gamma)^\perp_{\mathbb{F}_{q^m}}$

Ensure: A support $\boldsymbol{\alpha}$ and multiplier $\boldsymbol{\gamma}$ yielding an equivalent private key $\mathbf{Pct}_I(\mathscr{C}) = \mathscr{A}_{2r}(\boldsymbol{\alpha}, \boldsymbol{\gamma})^\perp_{\mathbb{F}_{q^m}}$ for some $I \subset [\![1, n]\!]$

1: Compute a rank-2 matrix $\boldsymbol{M}$ in the matrix code of relations of $\mathscr{C}$ w.r.t. $\boldsymbol{G}_{\text{pub}}$
2: Let $(\boldsymbol{\lambda}, \boldsymbol{\mu})$ be a basis of the row space of $\boldsymbol{M}$; set $\boldsymbol{u} \leftarrow \boldsymbol{\lambda}\boldsymbol{G}_{\text{pub}}$, $\boldsymbol{v} \leftarrow \boldsymbol{\mu}\boldsymbol{G}_{\text{pub}}$, $\boldsymbol{w} \leftarrow (\boldsymbol{u} \star \boldsymbol{v})^{2^{m-1}}$
3: Set $I \leftarrow \{i \mid u_i = 0 \text{ or } v_i = 0 \text{ or } w_i = 0\}$ and let $\mathscr{C}' \leftarrow \mathbf{Pct}_I(\mathscr{C})$
4: Compute $\boldsymbol{\alpha} \leftarrow \mathbf{Pct}_I(\boldsymbol{u}) \star \mathbf{Pct}_I(\boldsymbol{w})^{-1}$ ▷ support candidate, see §8.1
5: Solve $\boldsymbol{\gamma} \star \mathbf{RS}_{2r}(\boldsymbol{\alpha}) \subset \mathscr{C}'$ for $\boldsymbol{\gamma}$ ▷ see §8.2
6: **return** $(\boldsymbol{\alpha}, \boldsymbol{\gamma})$

8.1 Retrieving a support

Due to the shortening that we have to use in order to retrieve a triple $\boldsymbol{u}, \boldsymbol{v}$ and $\boldsymbol{w}$, there are many positions at which these three vectors are zero simultaneously. In the following, we will need to exclude these positions. This is simply done by puncturing the code $\mathscr{C}$ at all coordinates such that one of the three vectors is zero. However, we also need the corresponding punctured code to have the same dimension as the original one, hence we assume that the number of times we shorten does not exceed the codimension of $\mathscr{C}$. Observe that this is indeed the case for all concrete parameters considered in Section A, and also for Classic McEliece. Thanks to this assumption, the relation $\boldsymbol{u} \star \boldsymbol{v} = \boldsymbol{w}^2$ is equivalent to the existence of a vector $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{u} = \boldsymbol{\alpha} \star \boldsymbol{w}$ and $\boldsymbol{w} = \boldsymbol{\alpha} \star \boldsymbol{v}$, namely $\boldsymbol{\alpha} = \boldsymbol{u} \star \boldsymbol{w}^{-1}$. This vector is a natural candidate for the alternative support $\boldsymbol{x}'$:

Conjecture 3. *The vector $\boldsymbol{\alpha}$ is a valid support for $\mathscr{C}$, i.e. there exists $\boldsymbol{\beta} \in (\mathbb{F}_{q^m}^\times)^n$ such that $\mathscr{C} = \mathscr{A}_r(\boldsymbol{\alpha}, \boldsymbol{\beta})^\perp_{\mathbb{F}_{q^m}}$.*

Let us give some justification for this conjecture. Supported by [CMT23, Prop. 10] which means that there are no rank-2 relations in a random code of rate less than one third,[8] we expect that the existence of the triple $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ in geometric progression cannot happen accidentally but indeed comes from the algebraic structure of $\mathscr{C}$, which means that we expect $\boldsymbol{\alpha}$ to be a rational fraction in the original support $\boldsymbol{x}$, possibly up to conjugation. Moreover, as we have shortened the maximum number of times to compute the triple, we expect that the only remaining such rational fractions are homographies $z \mapsto \frac{az+b}{cz+d}$, $ad - bc \neq 0$, in which case $\boldsymbol{\alpha}$ is indeed a valid support.

Remark 8.1. Asymptotically, the assumption that the dimension of the punctured code is the same as that of the original code might fail in some regimes. Indeed, as $n \to \infty$, we shorten roughly rm times, so the length $\approx n - rm$ of the punctured code will be smaller than rm if $rm > n/2$. This problem is tackled by computing another triple by shortening at a different set of positions. Our task is then to glue the resulting support candidates together. For this, observe that on their overlap, two punctured support vectors are related to each other by a composition of a homography and a power of the Frobenius automorphism. Such a composition is easily recovered as soon as we choose the shortening positions so that the overlap has size at least 3. Repeating this roughly $\frac{rm}{n-rm}$ times, we then recover a long enough support candidate to proceed to the next step.

[8] Note that this rate condition is indeed satisfied on the examples listed above, and that more generally, shortening a lot ensures that we deal with codes of sufficiently small rate.

8.2 Recovering a decoding algorithm

Keeping in mind that $\mathscr{G}(\boldsymbol{x}, \Gamma) = \mathscr{A}_{2r}\left(\boldsymbol{x}, \Gamma(\boldsymbol{x})^{-2}\right)$ [Pat75], our strategy given a candidate support $\boldsymbol{\alpha}$ is to represent $\mathscr{C}$ as a dual alternant code $\mathscr{A}_{2r}\left(\boldsymbol{\alpha}, \boldsymbol{\gamma}\right)^{\perp}_{\mathbb{F}_{q^m}}$. For this, we solve the linear system

$$\boldsymbol{\gamma} \star \mathbf{RS}_{2r}(\boldsymbol{\alpha}) \subset \mathscr{C},$$

which we experimentally observed to have only one solution up to scalar multiplication. Note that this provides a decoding algorithm for $\mathscr{C}$ up to r errors, which is considered an equivalent private key in the McEliece cryptosystem.

8.3 Experimental comparison with the Pfaffian attack [BLT26]

We have compared our solving strategy with the Pfaffian modeling detailed in [BLT26]. Like in [BLT26], we take advantage of the existence of perfect squares in the parameterized modeling in order to eliminate variables.

The first advantage that we note is that the Pfaffian modeling at some degree d is comparable to the parameterized modeling at total degree $2d$, due to the number of monomials that are involved. Therefore, instances solved at odd total degree take special advantage of the parameterized modeling. This is notably the case for square-distinguishable instances, which we solve at total degree 3, *i.e.* bidegree (1,2) and (2,1). For example our `Magma` implementation successfully recovers the structure of a binary Goppa code of parameters $n = 1024, r = 6, m = 10$ in about 30s using less than 1GB of RAM, while the rather optimized C implementation of [BLT26] needs about 300s (most of this time being spent computing the Pfaffians themselves) and 1.5GB of RAM. More interestingly, in less than 14 hours and 24GB of RAM, we were able to recover a CFS private key [CFS01] with parameters $r = 9$ and $m = 16$ using our new modeling at total degree 3 and the key recovery attack, while the Pfaffian modeling was not reported as practical in [BLT26].

Finally, note that under Conjecture 1 the parameterized modeling need not be computed at a specific total degree: echelonizing a Macaulay matrix at the bi-degree given in the conjecture is indeed expected to be sufficient. This makes a crucial difference, especially as the total degree tends to infinity, in which case the number of monomials of bi-degree less than (a, b) becomes negligible compared to the number of monomials of total degree less than $a + b$.

A Distinguishable TII challenges

We give here, for all TII challenges distinguishable at total degree at most 8, the smallest[9] bi-degree (a, b) at which the corresponding code becomes distinguishable. Due to Remark 6.4, we do not include a bi-degree when it corresponds to a case in which [CMT23] already distinguishes at the degree of regularity d, in which case our distinguisher brings no improvement over [CMT23]. Note however that distinguishing in total degree $2d$ still brings an improvement when our bi-degree is smaller than (d, d), since the resulting Macaulay matrix is smaller.

Each table corresponds to bi-degrees of the same total degree. In these tables, λ denotes the security level as estimated by TII; that is, an exhaustive brute-force search is expected to have complexity 2^{λ}. The values n, r, m correspond to the length, degree, extension degree of the corresponding Goppa code and s is the number of times we shorten the code. The value #cols denotes the number of columns in the Macaulay matrix, while C denotes the corresponding linear-algebra complexity, assuming $\omega = 2.81$.

A.1 Consistency bi-degrees (Conjecture 1)

The following tables report the smallest consistency bi-degree and the corresponding complexity of the distinguisher, based on Conjecture 1.

[9] With respect to the lexicographical ordering.

Table A.1: Bi-degrees of total degree 3.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$
44	61	2	6	1	25.58	9.104
48	60	2	6	1	25.58	9.104
58	57	2	6	1	25.58	9.104
63	55	2	6	1	25.58	9.104
65	54	2	6	1	25.58	9.104
68	53	2	6	1	25.58	9.104

Table A.2: Bi-degrees of total degree 4.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
70	255	5	8	11	47.19	16.79	1	3
83	253	5	8	11	47.19	16.79	1	3

Table A.3: Bi-degrees of total degree 5.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
39	28	2	5	1	33.94	12.08	2	3
45	62	3	6	4	40.83	14.53	1	4
50	61	3	6	4	40.83	14.53	1	4
53	60	3	6	4	43.10	15.34	2	3
57	59	3	6	4	43.10	15.34	2	3
60	58	3	6	4	43.10	15.34	2	3
119	508	7	9	19	63.91	22.74	1	4
125	507	7	9	19	63.91	22.74	1	4
166	500	7	9	19	63.91	22.74	1	4
210	491	7	9	19	63.91	22.74	1	4
244	483	7	9	19	63.91	22.74	1	4
248	482	7	9	19	63.91	22.74	1	4

Table A.4: Bi-degrees of total degree 6.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
41	27	2	5	1	35.49	12.63	1	5
43	26	2	5	1	38.04	13.54	2	4
66	56	3	6	4	45.79	16.29	1	5
84	254	6	8	15	66.10	23.52	1	5
91	253	6	8	15	66.10	23.52	1	5
96	512	8	9	23	75.57	26.89	1	5
105	511	8	9	23	75.57	26.89	1	5
113	510	8	9	23	75.57	26.89	1	5
134	507	8	9	23	75.57	26.89	1	5
164	502	8	9	23	75.57	26.89	1	5
172	1020	11	10	38	84.84	30.19	1	5
187	1018	11	10	38	84.84	30.19	1	5
200	495	8	9	23	75.57	26.89	1	5
240	1010	11	10	38	84.84	30.19	1	5
246	1009	11	10	38	84.84	30.19	1	5
252	1008	11	10	38	84.84	30.19	1	5

Table A.5: Bi-degrees of total degree 7.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
72	125	5	7	11	68.59	24.41	2	5
77	124	5	7	11	68.59	24.41	2	5
86	122	5	7	11	68.59	24.41	2	5
90	121	5	7	11	68.59	24.41	2	5
92	254	7	8	19	80.66	28.71	2	5
94	120	5	7	11	70.35	25.04	3	4
110	251	7	8	19	80.66	28.71	2	5
129	509	9	9	28	86.59	30.81	1	6
189	499	9	9	28	90.74	32.29	2	5
204	1017	12	10	43	97.01	34.52	1	6
209	495	9	9	28	90.74	32.29	2	5
211	1016	12	10	43	97.01	34.52	1	6
214	1017	13	10	48	105.0	37.37	3	4
223	492	9	9	28	90.74	32.29	2	5
231	1013	12	10	43	97.01	34.52	1	6
250	1010	12	10	43	97.01	34.52	1	6

Table A.6: Bi-degrees of total degree ≥ 8 for which the distinguisher complexity is lower than the security level.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
138	509	10	9	33	102.2	36.37	2	6
158	506	10	9	33	102.2	36.37	2	6
160	240	7	8	19	88.46	31.48	2	6
171	237	7	8	19	88.46	31.48	2	6
178	235	7	8	19	88.46	31.48	2	6
208	497	10	9	33	102.2	36.37	2	6
212	224	7	8	19	90.96	32.37	3	5
213	496	10	9	33	102.2	36.37	2	6

A.2 Critical bi-degrees (Conjecture 2)

The following tables report the same data where we have replaced the consistency bi-degree with the critical bi-degree of Definition 6.3.

Table A.7: Bi-degrees of total degree 2.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
44	61	2	6	1	18.67	6.644	1	1
48	60	2	6	1	18.67	6.644	1	1
58	57	2	6	1	18.67	6.644	1	1
63	55	2	6	1	18.67	6.644	1	1
65	54	2	6	1	18.67	6.644	1	1
68	53	2	6	1	18.67	6.644	1	1

Table A.8: Bi-degrees of total degree 3.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
39	28	2	5	1	22.96	8.170	1	2
41	27	2	5	1	22.96	8.170	1	2
43	26	2	5	1	22.96	8.170	1	2

Table A.9: Bi-degrees of total degree 4.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
45	62	3	6	4	35.21	12.53	1	3
50	61	3	6	4	35.21	12.53	1	3
53	60	3	6	4	35.21	12.53	1	3
57	59	3	6	4	35.21	12.53	1	3
60	58	3	6	4	35.21	12.53	1	3
66	56	3	6	4	36.57	13.02	2	2
70	255	5	8	11	47.19	16.79	1	3
83	253	5	8	11	47.19	16.79	1	3
89	252	5	8	11	47.19	16.79	1	3

Table A.10: Bi-degrees of total degree 5.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
47	23	2	5	1	31.94	11.37	1	4
84	254	6	8	15	58.10	20.68	1	4
91	253	6	8	15	58.10	20.68	1	4
96	512	8	9	23	68.73	24.46	2	3
105	511	8	9	23	68.73	24.46	2	3
113	510	8	9	23	68.73	24.46	2	3
134	507	8	9	23	68.73	24.46	2	3
164	502	8	9	23	68.73	24.46	2	3
244	483	7	9	19	63.91	22.74	1	4
248	482	7	9	19	63.91	22.74	1	4

Table A.11: Bi-degrees of total degree 6.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
49	21	2	5	1	35.49	12.63	1	5
72	125	5	7	11	61.75	21.98	2	4
77	124	5	7	11	61.75	21.98	2	4
86	122	5	7	11	61.75	21.98	2	4
90	121	5	7	11	61.75	21.98	2	4
129	509	9	9	28	80.95	28.81	2	4
172	1020	11	10	38	84.84	30.19	1	5
174	1021	12	10	43	90.02	32.04	2	4
187	1018	11	10	38	84.84	30.19	1	5
200	495	8	9	23	75.57	26.89	1	5
204	1017	12	10	43	90.02	32.04	2	4
211	1016	12	10	43	90.02	32.04	2	4
240	1010	11	10	38	84.84	30.19	1	5
246	1009	11	10	38	84.84	30.19	1	5
252	1008	11	10	38	84.84	30.19	1	5

Table A.12: Bi-degrees of total degree 7.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
46	63	4	6	7	59.03	21.01	2	5
92	254	7	8	19	76.63	27.27	1	6
110	251	7	8	19	76.63	27.27	1	6
138	509	10	9	33	94.73	33.71	3	4
158	506	10	9	33	94.73	33.71	3	4
160	240	7	8	19	80.66	28.71	2	5
171	237	7	8	19	80.66	28.71	2	5
178	235	7	8	19	82.53	29.37	3	4
214	1017	13	10	48	103.0	36.66	2	5

Table A.13: Bi-degrees of total degree 8.

λ	n	r	m	s	$\log_2 C$	$\log_2 \#\text{cols}$	a	b
51	62	4	6	7	64.11	22.81	2	6
55	61	4	6	7	64.11	22.81	2	6
59	60	4	6	7	64.11	22.81	2	6
85	256	8	8	23	94.24	33.54	3	5
93	255	8	8	23	94.24	33.54	3	5
100	254	8	8	23	94.24	33.54	3	5
208	497	10	9	33	102.2	36.37	2	6
212	224	7	8	19	88.46	31.48	2	6
213	496	10	9	33	102.2	36.37	2	6
220	221	7	8	19	88.46	31.48	2	6

B Omitted Proofs

B.1 Proof of Proposition 3.3

We first recall this proposition.

Proposition B.1. *The ideal* $\mathcal{I}^{(k)} \overset{\text{def}}{=} \langle x_i y_j - x_j y_i | i, j \in [\![1, k]\!],\ i < j \rangle$ *generated by all principal minors of the matrix*

$$\boldsymbol{Z} = \begin{pmatrix} x_1 & x_2 & \cdots & x_k \\ y_1 & y_2 & \cdots & y_k \end{pmatrix}$$

has an associated Hilbert bi-series given by

$$\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) = \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^k(1-t)^k}.$$

Proof. We use the well-known fact that the set of maximal minors of a matrix of variables forms a universal Gröbner basis. Then, note that we have

$$\mathrm{HS}_{R/\mathcal{I}^{(k)}} = \mathrm{HS}_{R/\mathrm{in}_\prec(\mathcal{I}^{(k)})},$$

where $\prec$ is any *graded* monomial order on R and $\mathrm{in}_\prec(\mathcal{I}^{(k)})$ denotes the initial ideal of $\mathcal{I}^{(k)}$ with respect to this order [CLO15, Chapter 9]. For the proof, we may thus choose such an order $\prec$ for which this ideal takes a particularly simple form. Namely, we choose the graded lexicographic order induced by

$$x_1 > x_2 > \cdots > x_k > y_1 > y_2 > \cdots > y_k.$$

For $i < j$, the leading monomial of $x_iy_j - x_jy_i$ with respect to $\prec$ is x_iy_j. As recalled at the beginning of the proof, the maximal minors form a universal Gröbner basis. Hence,

$$\mathrm{in}_\prec(\mathcal{I}^{(k)}) = \langle\, x_iy_j \mid i,j \in [\![1,k]\!],\ i<j \,\rangle\,.$$

We are left with computing the Hilbert series of the quotient by this monomial ideal. We denote a general monomial $\mu \in R$ by $\mu \stackrel{\text{def}}{=} x_1^{a_1}\dots x_k^{a_k}y_1^{b_1}\dots y_k^{b_k}$, and define $A \stackrel{\text{def}}{=} \{i \mid a_i > 0\}$ and $B \stackrel{\text{def}}{=} \{i \mid b_i > 0\}$ to be its supports in the $\boldsymbol{x}$- and $\boldsymbol{y}$-variables, respectively. We have that μ is not divisible by any x_iy_j with $1 \le i < j \le k$ if and only if $\max(B) \le \min(A)$, with the conventions $\min(\emptyset) = +\infty$ and $\max(\emptyset) = 0$. It therefore remains to count the monomials μ such that $\max(B) \le \min(A)$, and we start by counting those for which $\delta \stackrel{\text{def}}{=} \min(A)$ is fixed. They are precisely the monomials that do not involve $x_1,\dots,x_{\delta-1}$, in which x_δ occurs with a positive exponent, and that do not involve $y_{\delta+1},\dots,y_k$. The corresponding bigraded generating series is

$$\underbrace{\frac{s}{1-s}}_{x_\delta}\underbrace{\frac{1}{(1-s)^{k-\delta}}}_{x_{\delta+1},\dots,x_k}\underbrace{\frac{1}{(1-t)^{\delta}}}_{y_1,\dots,y_\delta} = \frac{s}{(1-s)^{k-\delta+1}(1-t)^{\delta}}.$$

Finally, summing over all possible values of $1 \le \delta \le k$ and including the monomials that do not involve any $\boldsymbol{x}$-variable, we obtain

$$\begin{aligned}
\mathrm{HS}_{R/\mathrm{in}_\prec(\mathcal{I}^{(k)})}(s,t) &= \frac{1}{(1-t)^k} + \sum_{\delta=1}^{k} \frac{s}{(1-s)^{k-\delta+1}(1-t)^{\delta}} \\
&= \frac{1}{(1-t)^k} + \frac{s}{(1-s)^{k+1}} \sum_{\delta=1}^{k} \left(\frac{1-s}{1-t}\right)^{\delta} = \frac{1}{(1-t)^k} + \frac{s}{(s-t)(1-s)^k}\left(1 - \left(\frac{1-s}{1-t}\right)^{k}\right) \\
&= \frac{(s-t)(1-s)^k + s(1-t)^k - s(1-s)^k}{(s-t)(1-s)^k(1-t)^k} = \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^k(1-t)^k}.
\end{aligned}$$

We can conclude since again $\mathrm{HS}_{R/\mathcal{I}^{(k)}} = \mathrm{HS}_{R/\mathrm{in}_\prec(\mathcal{I}^{(k)})}$. □

B.2 Proof of Lemma 3.4

We first recall this lemma.

Lemma B.2. *For any bi-degree $\boldsymbol{d} = (a,b) \in \mathbb{N}^2$, we have*

$$\dim(R_{\boldsymbol{d}}/\mathcal{I}^{(k)}_{\boldsymbol{d}}) = \left[s^a t^b\right] \mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) = \binom{k+a+b-1}{a+b}.$$

Proof. Recall from the previous proposition that

$$\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) = \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^k(1-t)^k}.$$

We rewrite this series as

$$\mathrm{HS}_{R/\mathcal{I}^{(k)}}(s,t) = \frac{f(s)-f(t)}{s-t},$$

where $f(x) = \frac{x}{(1-x)^k}$. We are left with finding the coefficients c_n in the Taylor expansion $f(x) = \sum_{n\geq 0} c_n x^n$, since

$$\frac{f(s)-f(t)}{s-t} = \sum_{n\geq 1} c_n \sum_{i=0}^{n-1} s^{n-1-i}t^i.$$

In particular, the coefficient of $s^a t^b$ is equal to c_{a+b+1}. Finally,

$$f(x) = \frac{x}{(1-x)^k} = x\sum_{n\geq 0}\binom{k+n-1}{n}x^n = \sum_{n\geq 1}\binom{k+n-2}{n-1}x^n,$$

hence $c_n = \binom{k+n-2}{n-1}$. □

B.3 Proof of Lemma 6.1

Lemma B.3. *The ideal $\mathcal{J}$ generated by all principal minors of the matrix*

$$\boldsymbol{Z}_1 \overset{\text{def}}{=} \begin{pmatrix} x_1 & x_2 & \cdots & x_{k-2} & h_x & 0 \\ y_1 & y_2 & \cdots & y_{k-2} & 0 & h_y \end{pmatrix} \overset{\text{def}}{=} \begin{pmatrix} \boldsymbol{Z}_0 & \begin{matrix} h_x \\ 0 \end{matrix} & \begin{matrix} 0 \\ h_y \end{matrix} \end{pmatrix}$$

has an associated Hilbert bi-series given by

$$HS_{R^{hom}/\mathcal{J}}(s,t) = \frac{s(1-t)^k - t(1-s)^k}{(s-t)(1-s)^{k-1}(1-t)^{k-1}}.$$

Proof. As in the proof of Proposition 3.3, the maximal minors of $\boldsymbol{Z}_0$ form a universal Gröbner basis. The remaining maximal minors of $\boldsymbol{Z}_1$ are $h_x y_i$ for $1 \leq i \leq k-2$, $x_i h_y$ for $1 \leq i \leq k-2$, and $h_x h_y$. In particular, we can check that the set of maximal minors of $\boldsymbol{Z}_1$ still forms a Gröbner basis by computing S-polynomials. This gives the initial ideal, and we can then proceed with the same counting argument as at the end of the proof of Proposition 3.3 to obtain the Hilbert bi-series. □

B.4 Proof of Lemma 5.6

We first recall this lemma. Before doing so, recall that we showed the existence of a matrix $\boldsymbol{\Phi}$ with entries in $\mathcal{L} \subset \mathcal{R} = \mathbb{F}_{q^m}[X_1, \ldots, X_k]$ such that all its 2×2 minors belong to $I_2(\mathscr{C})$. We then set $V_j = V \cap \mathcal{R}_j^2$, where $\mathcal{R}_j = \mathbb{F}_{q^m}[X_1, \ldots, X_{k-j}]$, and showed that a matrix $\boldsymbol{\Phi}_j$ whose columns generate V_j has the same property as $\boldsymbol{\Phi}$ with respect to the shortened code, namely that all its 2×2 minors belong to $I_2(\mathscr{C}_j)$. At this point, we wanted to find, by reasoning on dimensions, specific 2×2 minors that give relations of rank 2. We had defined $V_j^i = \pi_i(V_j)$ for $i \in \{1,2\}$, where $\pi_i(x_1,x_2) = x_i$ for $(x_1,x_2) \in \mathcal{R}_j^2$.

Lemma 5.6. *If $\dim\left(V_j^1 \cap V_j^2\right) \geq 1$, then $I_2(\mathscr{C}_j)$ contains at least one quadratic form of bilinear rank 2.*

Proof. When Lemma 5.6 applies, there exists a linear form u in $V_j^1 \cap V_j^2$ such that either (i) there exist two pairs of the form $(a,u)^\intercal$ and $(u,b)^\intercal$ in V_j, or (ii) the vector $(u,u)^\intercal$ belongs to V_j. Case (i) implies on the spot that $I_2(\mathscr{C}_j)$ contains a quadratic form of bilinear rank 2 which is nothing but the minor $\begin{vmatrix} a & u \\ u & b \end{vmatrix} = a\times b - u^2$. Indeed, this minor is a combination of minors of $\boldsymbol{\Phi}_j$ and belongs to $I_2(\mathscr{C}_j)$. Case (ii) is ruled out exactly as in [BLT26, Lemma 3.4] which in our case reads as

Lemma B.4. *We have for any $s \in [\![0, d']\!]$ that*

$$\left\{x \in \mathcal{R}_s : \begin{pmatrix} x \\ x \end{pmatrix} \in V_s\right\} = \{0\}.$$

□

B.5 Proof of Theorem 7.2

Let us first recall this theorem

Theorem 7.2. *Assume that we have a family of proper alternant codes $(\mathscr{A}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ whose rates tend to a constant $R \in (0,1)$. Let n_i, r_i, m_i be respectively the length, degree and extension degree of $\mathscr{A}_i$ and assume that $n_i = \Theta\left(q^{m_i}\right)$ and n_i tends to infinity as i tends to infinity. If Conjecture 1 holds, then we can distinguish the $\mathscr{A}_i$'s from random codes with complexity C upper bounded by*

$$C \leq q^{\frac{\omega(1-R)r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)^3}{R \log_q r_i}(1+o(1))}. \tag{7.1}$$

The key point is that we can use our distinguisher to sufficiently shortened codes, as shown by

Lemma B.5. *Assume that we have a family of proper alternant codes $(\mathscr{A}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ whose rates tend to a constant $R \in (0,1)$. Let n_i, r_i, m_i be respectively the length, degree and extension degree of $\mathscr{A}_i$ and assume that $n_i = \Theta\left(q^{m_i}\right)$ and n_i tends to infinity as i tends to infinity. Let $\mathscr{C}_i$ be the extension of $\mathscr{A}^{\perp}$ over $\mathbb{F}_{q^{m_i}}$. There exists a sequence of nonnegative integers $(s_i)_{i=1}^{\infty}$ such at the same time*
(i) the matrix code $\mathscr{C}_{\mathrm{mat}}(\mathscr{D}_i)$ contains a rank-2 matrix where $\mathscr{D}_i$ is $\mathscr{C}_i$ shortened in s_i positions chosen arbitrarily such that the dimension k_i of $\mathscr{D}_i$ is $r_i \cdot m_i - s_i$ for any i and s_i,
(ii) $s_i = r_i\left(\log_q r_i + \mathcal{O}(1)\right)$,
(iii) $k_i = r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)$.

Proof. We use here Theorem 3.5 in [BLT26] which says that if we choose

$$\begin{aligned} s_i &\stackrel{\text{def}}{=} (e_i+1)r_i - 2\frac{q^{e_i+1}-1}{q-1} \quad \text{with} \\ e_i &\stackrel{\text{def}}{=} \left\lceil \log_q \frac{r_i}{2} \right\rceil, \end{aligned}$$

then the matrix code $\mathscr{C}_{\mathrm{mat}}(\mathscr{D}_i)$ contains a rank-2 matrix. This proves (i). Note that $e_i = \log_q r_i + \mathcal{O}(1)$ which implies $s_i = r_i \log_q r_i + \mathcal{O}(r_i)$ and hence proves (ii). To prove (iii), note that

$$\begin{aligned} k_i &= r_i \cdot m_i - s_i \\ &= r_i\left(m_i - \log_q r_i + \mathcal{O}(1)\right). \end{aligned} \tag{B.1}$$

Now, combining $m_i = \log_q n_i + \mathcal{O}(1)$ and $r_i \cdot m_i = (1-R)n_i(1+o(1))$ yields

$$r_i = \frac{(1-R)n_i}{\log_q n_i}(1+o(1)), \tag{B.2}$$

hence

$$\log_q r_i = \log_q n_i - \log_q \log_q n_i + \mathcal{O}(1). \tag{B.3}$$

Taking the logarithm once more also shows that

$$\log_q \log_q r_i = \log_q \log_q n_i + \log_q\left(1 + \frac{\log_q \log_q n_i}{\log_q n_i}\right) = \log_q \log_q n_i + \mathcal{O}(1), \tag{B.4}$$

which leads to

$$\begin{aligned} m_i - \log_q r_i &= \log_q n_i - \log_q n_i + \log_q \log_q n_i + \mathcal{O}(1) \quad \text{(by (B.3))} \\ &= \log_q \log_q n_i + \mathcal{O}(1) \\ &= \log_q \log_q r_i + \mathcal{O}(1) \quad \text{(by (B.4))} \end{aligned}$$

and proves (iii).

We are ready now to prove our theorem.

Proof (of Theorem 7.2). From Proposition 7.1 we can distinguish $\mathscr{A}_i$ from a random code at a bi-degree $(d_i, 1)$ such that $d_i = \frac{(k_i-2)^2-n'_i-k_i+5}{n'_i-2k_i+3} + \mathcal{O}(1)$ where k_i and n'_i are respectively the dimension of $\mathscr{D}_i$ of the extended dual of $\mathscr{A}_i$ shortened in s_i positions introduced in Lemma B.5. Since $k_i = r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)$ and

$$\begin{aligned} n'_i = n_i - s_i &= n_i - r_i(\log_q r_i + \mathcal{O}(1)) \\ &= n_i - r_i(\log_q n_i - \log_q \log_q n_i + \mathcal{O}(1)) \text{ (by (B.3))} \\ &= n_i - r_i m_i - r_i(\log_q \log_q n_i + \mathcal{O}(1)) \text{ (as } m_i = \log_q n_i + \mathcal{O}(1)) \\ &= Rn_i(1 + o(1)), \end{aligned}$$

we obtain

$$\begin{aligned} d_i &= \frac{r_i^2\left(\log_q \log_q r_i + \mathcal{O}(1)\right)^2}{Rn_i}(1 + o(1)) \\ &= \frac{r_i^2\left(\log_q \log_q r_i + \mathcal{O}(1)\right)^2}{R^{\frac{r_i \log_q(r_i)}{(1-R)}}}(1 + o(1)) \text{ (by (B.2) and (B.3))} \\ &= \frac{(1-R)r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)^2}{R\log_q r_i}(1 + o(1)). \end{aligned}$$

Now using Proposition 6.6 the complexity C of computing the distinguisher at bi-degree $(d_i, 1)$ is upper bounded by $\binom{k_i+d_i+\mathcal{O}(1)}{d_i+\mathcal{O}(1)}^\omega$, where ω is the exponent of linear algebra. Since

$$\begin{aligned} \log_q C &\leq \omega \log_q \binom{k_i + d_i + \mathcal{O}(1)}{d_i + \mathcal{O}(1)} \\ &= \omega d_i \log_q \frac{k_i}{d_i} \text{ (by Stirling's formula and using that } d_i = o(k_i)) \\ &= \frac{\omega(1-R)r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)^3}{R\log_q r_i}(1 + o(1)), \end{aligned}$$

where the last equation used that $k_i = r_i\left(\log_q \log_q r_i + \mathcal{O}(1)\right)$. □

C Distinguishing at a Critical Bi-Degree

We can distinguish at critical bi-degrees in some cases. For instance, there can be rare parameter sets for which every critical bi-degree (a, b) is a consistency bi-degree. Otherwise, we can clearly distinguish at a critical bi-degree (a, b) if by chance the rank of $\boldsymbol{M}_{(a,b)}(F^{\text{top}})$ differs between the random case and the Goppa/alternant case. Note that Conjecture 2 does not control this behavior.

If however this rank is the same, then we would collect the same number of degree fall polynomials at this bi-degree (a, b) in both cases. A possibility is that the number of linearly independent ones is not the same, in which case we can also distinguish at this point. If still we cannot distinguish, the natural approach would be to perform higher-degree computation with these degree fall polynomials, namely by multiplying them by variables and use solving techniques inspired from the MutantXL algorithm [BDMM09]. The main issue is that the bilinear adaptation of this approach is not well understood, even in the case of random overdetermined bilinear systems.

D Consistency Bi-Degree of the Form $(d, 1)$

We show here that the least consistency bi-degree of the form $(d, 1)$ is of the order of k^2/n just as the least critical bi-degree of the same form.

By definition and using the explicit expression of the coefficient of $s^d t$ in $\frac{(1-st)^{n-k}}{(1-s)^{k-1}(1-t)^{k-1}}$, the least consistency bi-degree of the form $(d,1)$ corresponds to the smallest integer d such that

$$(k-1)\tbinom{k+d-2}{d} - (n-k)\tbinom{k+d-3}{d-1} \leq \tbinom{k+d-2}{d+1}.$$

As in the proof of Proposition 7.1, we express all binomials in function of $\binom{k+d-2}{d}$ and we divide by this quantity. We obtain

$$(k-1) - (n-k)\tfrac{d}{k+d-2} \leq \tfrac{k-2}{d+1},$$

i.e.

$$(n-2k+1)d^2 + (n-k^2+2k-3)d - (k-2) \geq 0.$$

Let $\Delta(n,k) \stackrel{\text{def}}{=} (n-k^2+2k-3)^2 + 4(n-2k+1)(k-2)$. We retain the positive root

$$\tfrac{k^2-n-2k+\sqrt{\Delta(n,k)}+3}{2(n-2k+1)}.$$

We can finish the computation from there to get the approximation of d we want.

Otherwise, we can more simply observe that $(d,1)$ is greater than or equal to the least critical bi-degree of the same form on the one hand, and on the other hand that $d \leq d_0$, where d_0 is defined as the least integer such that

$$(k-1)\tbinom{k+d_0-2}{d_0} - (n-k)\tbinom{k+d_0-3}{d_0-1} \leq 0.$$

We can conclude since

$$d_0 = \min\left\{d \geq 1 \;\middle|\; d \geq \tfrac{(k-1)(k-2)}{n-2k+1}\right\} = \left\lceil \tfrac{(k-1)(k-2)}{n-2k+1} \right\rceil \sim k^2/n.$$

E Relationship to the Pfaffian Modeling

Let $\boldsymbol{M} = (m_{i,j})$ be a formal $D \times D$ skew-symmetric matrix in characteristic 2. On the one hand, recall that the Pfaffian modeling exploits the fact that this matrix is of rank ≤ 2 if and only if

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

for all $1 \leq i < j < k < l \leq D$. On the other hand, our parametrization is $m_{i,j} = x_i y_j + y_i x_j$, where the unknowns $\boldsymbol{x}$ and $\boldsymbol{y}$ can be stacked in a matrix

$$\boldsymbol{Z} = \begin{pmatrix} x_1 & x_2 & \cdots & x_D \\ y_1 & y_2 & \cdots & y_D \end{pmatrix}.$$

Then clearly, the above $\binom{D}{4}$ quadratic equations correspond to the Plücker relations for the Grassmannian $\mathrm{Gr}(2,D)$, *i.e.*

$$|\boldsymbol{Z}|_{*,\{i,j\}}|\boldsymbol{Z}|_{*,\{k,l\}} + |\boldsymbol{Z}|_{*,\{i,k\}}|\boldsymbol{Z}|_{*,\{j,l\}} + |\boldsymbol{Z}|_{*,\{i,l\}}|\boldsymbol{Z}|_{*,\{j,k\}} = 0,$$

still for all $1 \leq i < j < k < l \leq D$.

We consider here the implicit version of the Pfaffian modeling, where the term "implicit" follows the terminology of [LMT25]. In this version, the $m_{i,j}$'s are the unknowns, and one adds the $\binom{D}{4}$ quadratic equations that form a system Q together with the parity-check equations of $\mathscr{C}_{\mathrm{mat}}$, instead of using a basis. Since Q corresponds to the Plücker relations, such an implicit modeling is nothing more than a set of parity-check equations in the Plücker algebra $\mathbb{F}_q[|\boldsymbol{Z}|_{*,T}] \simeq \mathbb{F}_q[m_{i,j}]/\mathcal{I}(Q)$. In our case, we have bilinear equations, and we multiply them by arbitrary elements in $\mathbb{F}_q[\boldsymbol{Z}]$. While these equations can still be viewed in $\mathbb{F}_q[|\boldsymbol{Z}|_{*,T}]$, those obtained by multiplication are no longer contained in this algebra. They are simply in the ideal $\mathcal{I}^{(D)} \subset \mathbb{F}_q[\boldsymbol{Z}]$ generated by the maximal minors of $\boldsymbol{Z}$ that was defined in Proposition 3.3. The Plücker relations remain relations in this ideal, but we obtain more of them. For instance, in bi-degree $(2,1)$, we have, for all $1 \leq i < j < k \leq D$,

$$x_i|\boldsymbol{Z}|_{*,\{j,k\}} + x_j|\boldsymbol{Z}|_{*,\{i,k\}} + x_k|\boldsymbol{Z}|_{*,\{i,j\}} = 0.$$

We do not need to study all these relations by hand, since they are already captured by the Hilbert bi-series that we used in our analysis.

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.

BB22. Magali Bardet and Manon Bertin. Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography 2022*, volume 13512 of *LNCS*, pages 107–123, Cham, September 2022. Springer International Publishing.

BC18. Élise Barelli and Alain Couvreur. An efficient structural attack on NIST submission DAGS. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology - ASIACRYPT'18*, volume 11272 of *LNCS*, pages 93–118. Springer, December 2018.

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.

BCV23. John B. Baena, Daniel Cabarcas, and Javier Verbel. On the complexity of solving generic overdetermined bilinear systems. *Advances in Mathematics of Communications*, 17(5):1210–1234, 2023.

BDMM09. Johannes A. Buchmann, Jintai Ding, Mohamed Saied Emam Mohamed, and Wael Said Abd Elmageed Mohamed. MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. In *Symmetric Cryptography*, volume 9031 of *Dagstuhl Seminar Proceedings (DagSemProc)*, pages 1–7, 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.

Beu21. Ward Beullens. Improved Cryptanalysis of UOV and Rainbow. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, volume 12696 of *Lecture Notes in Computer Science*, pages 348–373. Springer International Publishing, 2021.

BFM+25. Charles Bouillaguet, Thibauld Feneuil, Jules Maire, Matthieu Rivain, Julia Sauvage, and Damien Vergnaud. Multivariate Commitments and Signatures with Efficient Protocols. Cryptology ePrint Archive, Paper 2025/2035, 2025.

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.

BLP08. Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Attacking and Defending the McEliece Cryptosystem. In *Post-Quantum Cryptography 2008*, volume 5299 of *LNCS*, pages 31–46, 2008.

BLP11. Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Smaller decoding exponents: ball-collision decoding. In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 743–760, 2011.

BLT26. Magali Bardet, Axel Lemoine, and Jean-Pierre Tillich. An attack on the CFS scheme and on TII McEliece challenges. In M. Rosulek N. Heninger, editor, *Advances in Cryptology - CRYPTO2026, 46th Annual International Cryptology Conference, Part IV*, volume 16803 of *LNCS*, pages 380–412, Santa Barbara, CA, USA, August 2026. Springer.

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.

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.

BMvT78. Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, 24(3):384–386, May 1978.

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.

CDMT22. Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Statistical Decoding 2.0: Reducing Decoding to LPN. In *Advances in Cryptology - ASIACRYPT 2022*, LNCS. Springer, 2022.

CDMT24. Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Reduction from sparse LPN to LPN, dual attack 3.0. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *LNCS*, pages 286–315. Springer, 2024. Artifact available at https://artifacts.iacr.org/eurocrypt/2024/a10/.

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.

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.

CLO15. David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics, Springer-Verlag, New York., 2015.

CMT23. 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.

COT14. Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial Time Attack on Wild McEliece over Quadratic Extensions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 17–39. Springer Berlin Heidelberg, 2014.

DEEK24. Léo Ducas, Andre Esser, Simona Etinski, and Elena Kirshanova. Asymptotics and Improvements of Sieving for Codes. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *Lecture Notes in Computer Science*, pages 151–180. Springer, 2024.

DMR11. Hang Dinh, Cris Moore, and Alexander Russell. The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks. In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 761–779. Springer, 2011.

Dum86. Ilya Dumer. On syndrome decoding of linear codes. In *Proceedings of the 9th All-Union Symp. on Redundancy in Information Systems, abstracts of papers (in russian), Part 2*, pages 157–159, Leningrad, 1986.

Dum89. Ilya Dumer. Two decoding algorithms for linear codes. *Probl. Inf. Transm.*, 25(1):17–23, 1989.

Ess22. Andre Esser. Revisiting Nearest-Neighbor-Based Information Set Decoding. Cryptology ePrint Archive, Paper 2022/1328, 2022. https://eprint.iacr.org/2022/1328.

EZ23. Andre Esser and Floyd Zweydinger. New Time-Memory Trade-Offs for Subset Sum - Improving ISD in Theory and Practice. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 360–390. Springer, 2023.

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.

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.

FSS11. Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. *J. Symbolic Comput.*, 46(4):406–437, 2011.

Gib91. J. K. Gibson. Equivalent Goppa Codes and Trapdoors to McEliece's Public Key Cryptosystem. In Donald Davies, editor, *Advances in Cryptology - EUROCRYPT 1991*, volume 547 of *LNCS*, pages 517–521. Springer Berlin / Heidelberg, 1991.

GIJS26. Ashrujit Ghoshal, Yuval Ishai, Aayush Jain, and Nuozhou Sun. Quasipolynomial Cryptanalysis of the McEliece Cryptosystem (or: PIR Meets McEliece). Cryptology ePrint Archive, Paper 2026/1630, 2026.

HW26. Tobias Hemmert and Andreas Wiemers. Distinguishing Goppa codes using higher-order vanishing. In M. Rosulek N. Heninger, editor, *Advances in Cryptology - CRYPTO 2026, 46th Annual International Cryptology Conference, Part IV*, volume 16803 of *LNCS*, pages 191–223, Santa Barbara, CA, USA, August 2026. 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.

LB88. Pil J. Lee and Ernest F. Brickell. An Observation on the Security of McEliece's Public-Key Cryptosystem. In *Advances in Cryptology - EUROCRYPT'88*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

LMT25. Axel Lemoine, Rocco Mora, and Jean-Pierre Tillich. Understanding the new distinguisher of alternant codes at degree 2. *IACR Cryptol. ePrint Arch.*, page 531, 2025.

LS12. Gregory Landais and Nicolas Sendrier. Implementing CFS. In *Progress in Cryptology - INDOCRYPT 2012*, volume 7668 of *LNCS*, pages 474–488. Springer, 2012.

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 42-44.

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.

Mor25. Rocco Mora. On the matrix code of quadratic relationships for a goppa code. *Adv. Math. Commun.*, 19(3):829–852, 2025.

MP12. Irene Márquez-Corbella and Ruud Pellikaan. Error-correcting pairs for a public-key cryptosystem, 2012.

MS77. F. Jessie MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

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.

NRS25. Kai-Chun Ning, Lars Ran, and Simona Samardjiska. Multi-homogeneous XL. Cryptology ePrint Archive, Paper 2025/2060, 2025.

Pan25. Lorenz Panny. On breaking McEliece keys using brute force. Cryptology ePrint Archive, Paper 2025/632, 2025.

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.

PST20. Ray Perlner and Daniel Smith-Tone. Rainbow Band Separation is Better than we Thought. Cryptology ePrint Archive, Paper 2020/702, 2020.

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

Ran25. Hugues Randriambololona. The syzygy distinguisher. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VI*, volume 15606 of *Lecture Notes in Computer Science*, pages 324–354. Springer, 2025.

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.

Sau26. Julia Sauvage. *Security analysis of cryptographic algorithms based on structured polynomial systems.* PhD thesis, Sorbonne Université, 2026.

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

SS92. Vladimir Michilovich Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. Appl.*, 1(4):439–444, 1992.

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.

Tra24. Bénédikt Minh Dang Tran. *Post-Quantum Code-Based Cryptography.* PhD thesis, EPFL, Lausanne, 2024.

Wie86. Douglas Wiedemann. Solving sparse linear equations over finite fields. *IEEE transactions on information theory*, 32(1):54–62, 1986.