THE TANGENT SPACE ATTACK

AXEL LEMOINE

Abstract. We propose a new method for retrieving the algebraic structure of a generic alternant code given an arbitrary generator matrix, provided certain conditions are met. We then discuss how this challenges the security of the McEliece cryptosystem instantiated with this family of codes. The central object of our work is the quadratic hull related to a linear code, defined as the intersection of all quadrics passing through the columns of a given generator or parity-check matrix, where the columns are considered as points in the affine or projective space. The geometric properties of this object reveal important information about the internal algebraic structure of the code. This is particularly evident in the case of generalized Reed-Solomon codes, whose quadratic hull is deeply linked to a well-known algebraic variety called *the rational normal curve*. By utilizing the concept of Weil restriction of affine varieties, we demonstrate that the quadratic hull of a generic dual alternant code inherits many interesting features from the rational normal curve, on account of the fact that alternant codes are subfield-subcodes of generalized Reed-Solomon codes. If the rate of the generic alternant code is sufficiently high, this allows us to construct a polynomial-time algorithm for retrieving the underlying generalized Reed-Solomon code from which the alternant code is defined, which leads to an efficient key-recovery attack against the McEliece cryptosystem when instantiated with this class of codes. Finally, we discuss the generalization of this approach to Algebraic-Geometry codes and Goppa codes.

Introduction

McEliece cryptosystem. The problem of decoding random linear codes, also known as *random decoding problem*, is widely regarded as a difficult problem. It was shown in [BMvT78] that this problem is NP-hard, which may be thought of as *worst-case* hardness. More interestingly, the random decoding problem has also been deeply studied in the *average case*. After decades of research, the best generic decoding algorithm [BM17] remains exponential, which makes the decoding problem a good candidate for asymmetric cryptography. Moreover, it is generally agreed that the decoding problem is quantum resistant, given that the best known quantum decoding algorithm [KT17] also has exponential complexity. Until very recently, the NIST was still considering several code-based cryptosystems [AAB+22, AAB+17, ABC+22] in the fourth round of its post-quantum standardization competition, whose [AAB+17] was eventually declared the winner.

The first code-based public-key cryptosystem was proposed by McEliece back in 1978 [McE78]. The idea is to pick a linear code among a family of codes for which efficient decoding algorithms exist, provided that some secret structure about the code is known. The public key consists of a generator matrix of the code, which appears random, while the private key is represented by an efficient decoding algorithm. To encrypt a message, the sender first encodes it using the public generator matrix, and then deliberately adds a random error vector whose Hamming weight equals the code's decoding capability. Only the owner of the private key can recover the original message using the efficient decoding algorithm.

Key words and phrases. McEliece scheme, Alternant codes, Algebraic-geometry codes, Weil restriction.

The security of the scheme strongly relies on the choice of the family of codes, as the latter has to behave like random codes. Under the hypothesis of *indistinguishability* between the family of codes that is being used and random codes, a rigorous security proof was given in [CFS01]. Under such an assumption, breaking the cryptosystem boils down to decoding a random linear code, whose computational intractability has already been discussed. Many families have been considered for this purpose, for instance generalized Reed-Solomon (GRS) codes by Niederreiter in [Nie86], which were proven insecure for such a use case in [SS92] by Sidelnikov and Shestakov, or algebraic-geometry (AG) codes proposed by Janwa and Moreno in [JM96] and attacked by Couvreur, Márquez-Corbella and Pellikaan in [CMCP14]. Interestingly, the family of binary Goppa codes, originally proposed by McEliece, still looks like a relevant proposition nowadays. Despite the existence of distinguishers against Goppa codes, such as those presented in [FGO$^+$11, CMT23] which both handle high-rate Goppa codes in polynomial time, or [Ran24] which handles constant-rate Goppa codes in sub-exponential — but still high — time, no efficient key-recovery or message-recovery attacks exist against McEliece scheme with *binary* Goppa codes. Most notably, the key recovery attack proposed in [BMT24] could only work for generic alternant codes, while [CMT23] treats the case of codes over a large alphabet and thus excludes the binary case.

Codes and geometry. A generator matrix of a linear code may be thought of as a collection of points in the affine or projective space, each column of the matrix being seen as a point. The *quadratic hull* of a code with respect to such a matrix is defined as the intersection of all quadrics that pass through each of these points. For generalized Reed-Solomon codes whose dimension does not exceed half the length, the quadratic hull turns out to be a rational normal curve. Using Weil restriction and the strong rigidity of the objects that are derived from it, we wish to provide the same kind of results for generic alternant codes.

Our contribution. We propose a new approach for recovering the private structure of a generic alternant code using both algebraic-geometry and Galois theory. Our algorithm has polynomial complexity with respect to the length and dimension of the code, and is able to fully recover the structure of the code provided that the rate of the alternant code is high enough for the square of its dual not to fill the entire ambient space. To achieve this goal, we compute the quadratic hull with respect to the public parity-check matrix of the code. Under some hypotheses, this algebraic variety is the Weil restriction of the affine cone over the rational normal curve, up to an unknown change of basis. Even after this change of basis, this variety keeps an interesting property: its tangent spaces are stabilized by a certain linear operator. One may therefore compute the space of linear operators that stabilize all these tangent spaces, which turns out to have a structure of algebra isomorphic to the extension field over which the underlying GRS code is defined. This enables us to compute another parity-check matrix of the code which directly yields a generator matrix of the underlying GRS code, up to conjugation by the Frobenius automorphism. The final step is to apply [SS92] to recover a support and a multiplier, and thus an efficient decoding algorithm. We eventually study the application of our framework to Goppa codes and algebraic-geometry codes, and investigate some natural generalization of generic alternant codes that are vulnerable to our attack.

Outline of the paper. The first section is dedicated to the basic notions of coding theory that we will need throughout the paper. In Section 2 we set up our key-recovery problem, and explain why this naturally leads to the concept of Weil restriction of ideals and affine algebraic varieties. Section 3 introduces the notion of Weil restriction of scalars, and establishes several results such as Lemma 2 which identifies subspaces having the structure of a Weil restriction, or Theorem 3 which explicitly gives the family of linear automorphisms that preserve this structure.

In this section, we also introduce the notion of Weil-properness, that essentially tells us when this framework can be used to analyze the structure of trace codes. Section 4 provides a polynomial-time algorithm for retrieving an efficient decoding algorithm for the subfield-subcode being used in the McEliece cryptosystem, be it a generic alternant code, the subfield subcode of a generic AG code, or even a Goppa code of sufficiently low degree, but provided that the square of the dual code is not the entire ambient space.

1. Notations and prerequisites

1.1. **Basic notation.**

Fields. Throughout the paper, we work with an extension of finite fields $\mathbb{F}_{q^m}/\mathbb{F}_q$, together with a primitive element $\alpha \in \mathbb{F}_{q^m}$, so that $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. We may sometimes also refer to a generic field as $\mathbb{F}$. The algebraic closure of $\mathbb{F}$ is denoted by $\overline{\mathbb{F}}$.

Vectors and matrices. Codewords, *i.e.* elements of a linear code, are denoted using bold lower-case letters. We use the row-vectors convention for codewords. For geometric points in the affine space, we instead use the column-vectors convention. Matrices are denoted with bold capital letters. If $(\lambda_1, \dots, \lambda_n) \in \mathbb{F}^n$, the notation $\mathrm{Diag}(\lambda_1, \dots, \lambda_n)$ stands for the diagonal matrix with entries given by the λ_i's. We freely use this notation to build block-diagonal matrices as well. Finally, $\mathbf{GL}_k(\mathbb{F})$ denotes the general linear group of size k over $\mathbb{F}$, while $\mathbf{GL}(\mathbb{F}^k)$ denotes the group of linear automorphisms of $\mathbb{F}^k$. We have of course $\mathbf{GL}_k(\mathbb{F}) \simeq \mathbf{GL}(\mathbb{F}^k)$.

Spans and ideals. If E is any subset of an $\mathbb{F}$-vector space, we denote by $\mathrm{Span}_{\mathbb{F}}(E)$ the $\mathbb{F}$-vector subspace spanned by E. Similarly, when A is a subset of a ring $\boldsymbol{R}$, the notation $\langle A \rangle$ stands for the ideal generated by A.

Partial derivatives. Let $\boldsymbol{R} = \mathbb{F}[x_s \mid s \in S]$ be a polynomial ring whose variables are indexed by a finite set S. For $f \in \boldsymbol{R}$, we write $\partial_s f$ for the partial derivative of f with respect to x_s.

Varieties. In this paper, the term *algebraic variety* refers to algebraic subsets of $\mathbb{F}^r$ for some integer r and field $\mathbb{F}$, *i.e.* the zero locus associated to an ideal $I \subset \mathbb{F}[X_1, \dots, X_r]$ in $\mathbb{F}^r$. When we are given such an ideal I, we denote by $V(I)$ its variety, or sometimes $V_{\mathbb{F}}(I)$ when we want to emphasize that the ground field is $\mathbb{F}$. If I is the defining ideal of the variety V, the coordinate ring of V is denoted with $\mathbb{F}[V]$ and defined by $\mathbb{F}[X_0, \dots, X_{r-1}]/I$.

1.2. **Linear codes.**

A linear subspace $\mathscr{C} \subseteq \mathbb{F}^n$ of dimension r is called an $[n,k]_{\mathbb{F}}$-linear code. We may talk about $[n,k]_q$-codes when $\mathbb{F} = \mathbb{F}_q$. A *generator matrix* of $\mathscr{C}$ is a matrix $\boldsymbol{G}$ with coefficients in $\mathbb{F}$ whose row space equals $\mathscr{C}$. An $[n,k]_{\mathbb{F}}$-code $\mathscr{C}$ may as well be defined by a *parity-check matrix* $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$ which is such that

$$\mathscr{C} = \{\boldsymbol{x} \in \mathbb{F}^n \mid \boldsymbol{H}\boldsymbol{x}^\top = 0\}.$$

As $\mathbb{F}^n$ is endowed with the canonical inner product defined by

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}^n,\ \boldsymbol{x} \cdot \boldsymbol{y} \stackrel{\text{def}}{=} \sum_{i=1}^{n} x_i y_i,$$

we may define the *dual* of a code $\mathscr{C}$ as $\mathscr{C}^\perp \stackrel{\text{def}}{=} \{\boldsymbol{y} \in \mathbb{F}^n \mid \forall \boldsymbol{x} \in \mathscr{C},\ \boldsymbol{x} \cdot \boldsymbol{y} = 0\}$. Note that $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$ is a parity-check matrix of $\mathscr{C}$ if and only if it is a generator matrix of $\mathscr{C}^\perp$.

1.3. **Componentwise product of codes.** The space $\mathbb{F}^n$ naturally comes with the canonical product algebra structure. The multiplication law will be denoted with the star notation as follows:

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}^n,\ \boldsymbol{x} \star \boldsymbol{y} \stackrel{\text{def}}{=} (x_1 y_1, \dots, x_n y_n).$$

This immediately gives rise to the notion of product of codes.

Definition 1. *For any $\mathbb{F}$-linear codes $\mathscr{C}, \mathscr{D} \subset \mathbb{F}^n$, we define*

$$\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}.$$

We also write $\mathscr{C}^{\star 2} = \mathscr{C} \star \mathscr{C}$.

Note that the componentwise product of codes is associative and may therefore be iterated. We will thus write $\mathscr{C}^{\star d}$ for $\underbrace{\mathscr{C} \star \dots \star \mathscr{C}}_{d \text{ times}}$.

Let $\boldsymbol{G} \in \mathbb{F}^{r \times n}$ be a generator matrix of $\mathscr{C}$, and let $\boldsymbol{g}_j$ denote the j-th column of $\boldsymbol{G}$ for all $1 \leq j \leq n$. Define $\boldsymbol{R} = \mathbb{F}[X_0, \dots, X_{r-1}]$ together with the natural evaluation map

$$\mathrm{ev}_{\boldsymbol{G}} : \begin{cases} \boldsymbol{R} & \longrightarrow \mathbb{F}^n \\ f & \longmapsto (f(\boldsymbol{g}_1), \dots, f(\boldsymbol{g}_n)). \end{cases} \tag{1}$$

Alternatively, following the convention of [Ran24], $\mathrm{ev}_{\boldsymbol{G}}$ can be defined as the only homomorphism of (graded) $\mathbb{F}$-algebras mapping each variable X_i onto the i-th row $\boldsymbol{r}_i$ of $\boldsymbol{G}$ — here we have $0 \leq i < r$ in order to be consistent with the way we enumerate the variables of $\boldsymbol{R}$. The image of this map, which does not depend on the choice of $\boldsymbol{G}$, was denoted in [Ran24] by $\bigoplus_{d \geq 0} \mathscr{C}^{\star d}$ and referred to as the *homogeneous coordinate ring* of $\mathscr{C}$. On the contrary, the kernel of $\mathrm{ev}_{\boldsymbol{G}}$ formally depends on the choice of $\boldsymbol{G}$ and will be denoted by $I(\boldsymbol{G})$ in this paper. It has a structure of graded ideal, *i.e.*

$$I(\boldsymbol{G}) = \bigoplus_{d \geq 0} I_d(\boldsymbol{G}),$$

where $I_d(\boldsymbol{G})$ is the homogeneous component of degree d of $I(\boldsymbol{G})$, that we will refer to as the vanishing ideal of $\boldsymbol{G}$ at degree d.

Definition 2 (Quadratic hull [Ran19])**.** *We define the algebraic quadratic hull of $\mathscr{C}$ with respect to $\boldsymbol{G}$ as the polynomial ideal generated by $I_2(\boldsymbol{G})$. The algebraic variety induced by the algebraic quadratic hull will be denoted by $V_2(\boldsymbol{G})$ and referred to as the geometric quadratic hull of $\mathscr{C}$ with respect to $\boldsymbol{G}$.*

Remark 1. Hilbert's Nullstellensatz establishes a correspondence between ideals of $\overline{\mathbb{F}}[X_1, \dots, X_r]$ and algebraic subsets of $\overline{\mathbb{F}}^r$, meaning that we can work with either the algebraic or the geometric quadratic hull equivalently. However, most of the time we only have access to the $\mathbb{F}$-rational points of the variety, preventing the Nullstellensatz to hold as $\mathbb{F}$ will always be a finite field in this paper. This will require us to be cautious and to always specify which version of the quadratic hull — algebraic or geometric — we will be working with.

Note that the vector space $I_2(\boldsymbol{G})$ is the very same object as the *code of quadratic relations* introduced in [CMT23], as we have

$$I_2(\boldsymbol{G}) = \left\{ \sum_{i \leq j} c_{i,j} X_i X_j \mid \sum_{i \leq j} c_{i,j} \boldsymbol{r}_i \star \boldsymbol{r}_j = 0 \right\}.$$

Recall that the dimension of $I_2(\boldsymbol{G})$ is related to that of $\mathscr{C}^{\star 2}$ by

$$\dim I_2(\boldsymbol{G}) = \binom{r+1}{2} - \dim \mathscr{C}^{\star 2}, \tag{2}$$

which can be obtained by applying the rank-nullity theorem on the evaluation map $\mathrm{ev}_{\boldsymbol{G}}$ restricted to $\boldsymbol{R}_2$. Although we emphasize the dependence of $I_2(\boldsymbol{G})$ on the choice of generator matrix, many properties of the algebraic or geometric quadratic hull are actually intrinsic. More precisely, the quadratic hull — be it algebraic or geometric — depends only on the code, at least up to some linear transformation.

Proposition 1. *Let $\boldsymbol{G}_1, \boldsymbol{G}_2$ be two $r \times n$ generator matrices of an $\mathbb{F}$-linear code $\mathscr{C}$. Denote by $\boldsymbol{P} \in \mathbf{GL}_r(\mathbb{F})$ the transition matrix so that $\boldsymbol{G}_2 = \boldsymbol{P} \cdot \boldsymbol{G}_1$. Then*

(i) $I_2(\boldsymbol{G}_1) = \left\{ f^{\boldsymbol{P}} \mid f \in I_2(\boldsymbol{G}_2) \right\}$, *where* $f^{\boldsymbol{P}} = f((X_1 \ \dots \ X_r) \cdot \boldsymbol{P}^\top)$;
(ii) $V_2(\boldsymbol{G}_2) = \left\{ \boldsymbol{P} \cdot \boldsymbol{v} \mid \boldsymbol{v} \in V_2(\boldsymbol{G}_1) \right\}$.

Proof. Denote by $\boldsymbol{g}_1, \dots, \boldsymbol{g}_n$ the columns of $\boldsymbol{G}_1$. As the columns of $\boldsymbol{G}_2$ are $\boldsymbol{P} \cdot \boldsymbol{g}_1, \dots, \boldsymbol{P} \cdot \boldsymbol{g}_n$, we see that for any quadratic form $f \in \boldsymbol{R}_2$,

$$\begin{aligned} f \in I_2(\boldsymbol{G}_2) &\iff \forall 1 \le i \le n,\ f(\boldsymbol{P} \cdot \boldsymbol{g}_i) = 0 \\ &\iff \forall 1 \le i \le n,\ f^{\boldsymbol{P}}(\boldsymbol{g}_i) = 0 \\ &\iff f^{\boldsymbol{P}} \in I_2(\boldsymbol{G}_1), \end{aligned}$$

which proves (i). Note that (ii) follows directly from this by definition of the geometric quadratic hull. □

As a result of this proposition, several features such as the dimension of $I_2(\boldsymbol{G})$, the dimension of the geometric quadratic hull or even its smoothness do not depend on the specific generator matrix we are working with. We may sometimes omit the dependence on the generator matrix when we refer to invariant quantities, and write $I_2(\mathscr{C})$ instead of $I_2(\boldsymbol{G})$.

1.4. **GRS codes.** Many codes used in the McEliece scheme are derived from generalized Reed-Solomon codes, which we introduce below.

Definition 3 (GRS codes)**.** *Let $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}^n$ be a vector of pairwise-distinct elements, $\boldsymbol{y} \in (\mathbb{F}^\times)^n$, and let $r \le n$ be an integer. The generalized Reed-Solomon (GRS) code of degree r, support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$ is defined by*

$$\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) = \{ \boldsymbol{y} \star f(\boldsymbol{x}) \mid f \in \mathbb{F}[X],\ \deg f < r \},$$

where $f(\boldsymbol{x}) = (f(x_1), \dots, f(x_n))$.

Remark 2. A generator matrix of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ is given by the following truncated Vandermonde matrix:

$$\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y}) = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ x_1 y_1 & x_2 y_2 & \dots & x_n y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{r-1} y_1 & x_2^{r-1} y_2 & \dots & x_n^{r-1} y_n \end{pmatrix}.$$

A GRS code of degree r has dimension r. It follows from the fact that univariate polynomials of degree at most $r-1$ have at most $r-1$ roots that a GRS code is always MDS, meaning that its minimum distance d is equal to $n - r + 1$ — the highest possible value by Singleton's bound. Furthermore, the Welch-Berlekamp algorithm [WB86] enables to decode these codes up to half their minimum distance in $O(n^3)$ operations in $\mathbb{F}$. These positive features explain why these codes have been so widely studied by researchers and engineers. However, all these nice properties mean that GRS codes are far from looking like random codes. In particular, their behavior with respect to the componentwise product is very peculiar, as we state below without proof.

Proposition 2. $\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2r-1}(\boldsymbol{x},\boldsymbol{y}^{\star 2})$.

Hence, the dimension of the square of a GRS code increases *linearly*. In the random case [CCMZ15], the square of an $[n,k]$-code has dimension $\min\{n, \frac{k(k+1)}{2}\}$ with overwhelming probability, which means a *quadratic* increase. Equation (2) shows that GRS codes having a small square means they have an unexpectedly large algebraic quadratic hull. It is particularly visible when we look at the quadratic hull of $\boldsymbol{V}_r(\boldsymbol{x},\boldsymbol{y})$.

Proposition 3. *If $2r-1 \leq n$, then $I_2(\boldsymbol{V}_r(\boldsymbol{x},\boldsymbol{y}))$ is spanned by the 2×2 minors of*

$$\begin{pmatrix} X_0 & X_1 & \dots & X_{r-2} \\ X_1 & X_2 & \dots & X_{r-1} \end{pmatrix}. \tag{3}$$

Proof. See for instance [LMT25, Propositions 1 & 2]. □

The projective variety defined by the determinantal ideal generated by the minors of (3) is the rational normal curve in $\mathbb{P}^{r-1}$, defined as the image of the Veronese embedding

$$\nu : \begin{cases} \mathbb{P}^1 & \longmapsto \mathbb{P}^{r-1} \\ (u:v) & \longmapsto (v^{r-1} : uv^{r-2} : \dots : u^{r-1}). \end{cases}$$

Remark 3. We may sometimes denote with *a rational normal curve* any curve which is the image of the projective line through a map $(u:v) \mapsto (f_0(u,v) : \dots : f_{r-1}(u,v))$, where $(f_0,\dots,f_{r-1})$ is a basis of the r-dimensional vector space of homogeneous bivariate polynomials of degree $r-1$. Up to projective equivalence, all these curves are actually the same, which is why some authors talk about *the* rational normal curve.

The link between GRS codes and the rational normal curve provides a lot of insightful information about these codes. For example, as suggested in [MMP14], any generator matrix of a GRS code can be seen as a collection of points in the projective space, through which there passes a unique rational normal curve [GH78]. Computing a parametrization of the latter provides an alternative to the Sidelnikov-Shestakov attack.

1.5. **Alternant codes.** The original proposal of McEliece [McE78] suggested implementing the scheme with binary Goppa codes, which are a subclass of the much broader family of alternant codes.

Definition 4 (Alternant code)**.** *Let $\boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ be some support and multiplier, and let $r \geq 2$ be an integer. The alternant code of degree r, support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$ is defined by*

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

In this paper, we study the structure of alternant codes through their dual code. To this end, we need to introduce the trace map associated to the Galois extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ and defined by

$$\mathrm{Tr} : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow \mathbb{F}_q \\ x & \longmapsto \displaystyle\sum_{j=0}^{m-1} x^{q^j}. \end{cases}$$

Applying this map coordinatewise to any codeword is a way to construct a q-ary linear code given a code defined over $\mathbb{F}_{q^m}$.

Definition 5 (Trace code)**.** *Let $\mathscr{C}$ be an $[n,k]_{q^m}$-code. The **trace code** of $\mathscr{C}$ is the $\mathbb{F}_q$-linear code defined by*

$$\mathrm{Tr}(\mathscr{C}) \overset{\text{def}}{=} \{\mathrm{Tr}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathscr{C}\},$$

where $\mathrm{Tr}(\boldsymbol{c}) \overset{\text{def}}{=} (\mathrm{Tr}(c_1),\dots,\mathrm{Tr}(c_n))$.

Another way to construct an $\mathbb{F}_q$-linear code starting from an $\mathbb{F}_{q^m}$-linear code $\mathscr{C}$ consists of merely taking the intersection of $\mathscr{C}$ with the subfield $\mathbb{F}_q^n$, like when we defined alternant codes. The resulting code, denoted by

$$\mathscr{C}_{|\mathbb{F}_q} \stackrel{\text{def}}{=} \mathscr{C} \cap \mathbb{F}_q^n$$

is referred to as the *subfield-subcode* of $\mathscr{C}$. It turns out that those two constructions are dual to each other as stated by Delsarte's theorem.

Theorem 1 ([Del75])**.** $(\mathscr{C}_{|\mathbb{F}_q})^\perp = \mathrm{Tr}\left(\mathscr{C}^\perp\right)$*, or equivalently* $(\mathscr{C}^\perp)_{|\mathbb{F}_q} = \mathrm{Tr}\left(\mathscr{C}\right)^\perp$.

From this, we immediately get that duals of alternant codes are trace codes of GRS codes.

Corollary 1. $\mathscr{A}_r\left(\boldsymbol{x},\boldsymbol{y}\right)^\perp = \mathrm{Tr}\left(\mathbf{GRS}_r\left(\boldsymbol{x},\boldsymbol{y}\right)\right)$.

We may thus study alternant codes as trace codes of GRS codes. In general, for an $\mathbb{F}_{q^m}$-linear code $\mathscr{C}$, the structure of trace code can be used to derive a generator matrix of $\mathrm{Tr}\left(\mathscr{C}\right)$ given a generator matrix of $\mathscr{C}$, which may be really helpful for establishing a link between the structure of $\mathscr{C}$ and that of the trace code. We start with a generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r\times n}$ of $\mathscr{C}$, and let $\mathscr{D} = (\mathscr{C}^\perp)_{|\mathbb{F}_q}$, so that

$$\mathscr{D} = \{\boldsymbol{h} \in \mathbb{F}_q^n \mid \forall \boldsymbol{c} \in \mathscr{C},\ \boldsymbol{c}\cdot\boldsymbol{h} = 0\}.$$

Let us denote with $\boldsymbol{r}_i = (g_{i,1},\ldots,g_{i,n})$ the i-th row of $\boldsymbol{G}$. By linearity of the dot product, the above condition is equivalent to $\boldsymbol{h}\cdot\boldsymbol{r}_i = 0$ for all $0 \le i < r$. Since $\boldsymbol{h}$ has coefficients in $\mathbb{F}_q$, the equation $\boldsymbol{h}\cdot\boldsymbol{r}_i = 0$ yields m equations over $\mathbb{F}_q$. To see this, for all coefficient $g_{i,j}$ of $\boldsymbol{G}$, write $g_{i,j} = g_{i,j,0} + g_{i,j,1}\alpha + \ldots + g_{i,j,m-1}\alpha^{m-1}$, with $g_{i,j,\ell} \in \mathbb{F}_q$, and α being the primitive element in $\mathbb{F}_{q^m}$. Then for any $\boldsymbol{h} \in \mathbb{F}_q^n$,

$$\begin{aligned}
\boldsymbol{h}\cdot\boldsymbol{r}_i = 0 &\iff \sum_{j=1}^{n} h_j g_{i,j} = 0 \\
&\iff \sum_{j=1}^{n}\sum_{\ell=0}^{m-1} \alpha^\ell h_j g_{i,j,\ell} = 0 \\
&\iff \sum_{\ell=0}^{m-1} \alpha^\ell \sum_{j=1}^{n} h_j g_{i,j,\ell} = 0 \\
&\iff \forall\ 0 \le \ell < m,\ \sum_{j=1}^{n} h_j g_{i,j,\ell} = 0.
\end{aligned}$$

As a result, the $rm \times n$ matrix obtained by taking $\boldsymbol{G}$ and replacing each coefficient $g_{i,j}$ by the column-vector of its $\mathbb{F}_q$-coordinates is a parity-check matrix of $\mathscr{D}$, *i.e.* a generator matrix of $\mathscr{D}^\perp$. By Delsarte's theorem, $\mathscr{D}^\perp = \mathrm{Tr}\left(\mathscr{C}\right)$, which means that we have obtained a generator matrix of $\mathrm{Tr}\left(\mathscr{C}\right)$. It is clear from here that $\dim_{\mathbb{F}_q}\mathrm{Tr}\left(\mathscr{C}\right) \le m\cdot\dim_{\mathbb{F}_{q^m}}\mathscr{C}$. Subfield-subcodes or trace codes that reach this bound will be called *proper* codes.

2. The problem of recovering the structure of an alternant code

In the McEliece cryptosystem instantiated with the family of alternant codes, the knowledge of some support and multiplier plays the role of the private key, just as in the case of generalized Reed-Solomon codes. A noisy codeword $\boldsymbol{y} = \boldsymbol{c}+\boldsymbol{e}$ can indeed be interpreted as a noisy codeword of the underlying GRS code of dimension $n-r$. Using a support and a multiplier, one can run the Welch-Berlekamp algorithm and thus recover $\boldsymbol{c}$, provided that the Hamming weight of $\boldsymbol{e}$ is strictly less than $r/2$. This is why any information about the support and the multiplier of the alternant code must again be kept secret. Although several algorithms [CGG+13, MMP14, SS92]

can recover such a support and multiplier in polynomial time in the GRS case, this task appears to be more difficult in the generic alternant case.

2.1. **The key-recovery problem.** We formulate the key-recovery problem in the following manner.

Problem 1. *Given $\boldsymbol{H}_{\text{pub}} \in \mathbb{F}_q^{rm \times n}$ a parity-check matrix of a proper alternant code $\mathscr{A}$, find a support $\boldsymbol{x}$ and a multiplier $\boldsymbol{y}$ such that $\mathscr{A} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$.*

Throughout the rest of the paper, we make use of the natural vector space identification:

$$\Psi_\alpha : \begin{cases} \mathbb{F}_{q^m} & \xrightarrow{\sim} \mathbb{F}_q^m \\ x = \sum_{j<m} x_j \alpha^j & \longmapsto (x_0, \dots, x_{m-1}). \end{cases} \tag{4}$$

By a slight abuse of notation, given a vector $\boldsymbol{v} = (v_0, \dots, v_{r-1}) \in \mathbb{F}_{q^m}^r$, we write $\Psi_\alpha(\boldsymbol{v}) = (\Psi_\alpha(v_0), \dots, \Psi_\alpha(v_{r-1})) \in \mathbb{F}_q^{rm}$. Finally, if $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r \times n}$ is a matrix whose columns are $(\boldsymbol{g}_1, \dots, \boldsymbol{g}_n)$, we denote by $\Psi_\alpha(\boldsymbol{G}) \in \mathbb{F}_q^{rm \times n}$ the matrix whose columns are $(\Psi_\alpha(\boldsymbol{g}_1), \dots, \Psi_\alpha(\boldsymbol{g}_n))$.

We explained in the previous section that whenever $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r \times n}$ is a generator matrix of $\mathscr{C}$, then $\Psi_\alpha(\boldsymbol{G})$ is a parity-check matrix of $\mathscr{C}_{|\mathbb{F}_q}$. In particular, $\boldsymbol{H}_{\text{sec}} \overset{\text{def}}{=} \Psi_\alpha(\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y}))$ is a valid parity-check matrix of the alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$. Moreover, the knowledge of $\boldsymbol{H}_{\text{sec}}$ directly yields the support $\boldsymbol{x}$ and the multiplier $\boldsymbol{y}$, and therefore the private key. If now $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{G})$ for some other generator matrix of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$, then one directly recovers $\boldsymbol{G}$ by reading the columns of $\boldsymbol{H}_{\text{sec}}$, and it only remains to run [SS92] to recover an efficient decoding algorithm. We just described a whole family of easy instances of Problem 1.

In reality, an attacker would not be given $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{G})$ directly. Instead, the public key consists of $\boldsymbol{H}_{\text{pub}} = \boldsymbol{P} \cdot \boldsymbol{H}_{\text{sec}}$ where $\boldsymbol{P}$ is a random $rm \times rm$ nonsigular matrix with entries in $\mathbb{F}_q$. In some sense, the transition matrix $\boldsymbol{P}$ not only shuffles the basis of the underlying GRS code, but also hides the $\mathbb{F}_{q^m}$-linear structure that is visible in $\boldsymbol{H}_{\text{sec}}$, preventing an attacker from being able to directly recover a generator matrix of the GRS code. However, Proposition 1 tells us that if we look at the quadratic hull of $\boldsymbol{H}_{\text{pub}}$, it has a good chance to share strong properties with that of $\boldsymbol{H}_{\text{sec}}$. This leads us to investigate the state of the art about the algebraic quadratic hull of an alternant code.

2.2. **The quadratic hull of an alternant code.** The dimension of the space of quadratic forms vanishing at all columns of a given parity-check matrix of an alternant code was first studied in [FGO+10]. Equivalently by Equation (2) one can study the dimension of the square of the dual code, as it was first noticed in [MP12] and fully investigated in [MT21].

Theorem 2 ([MT21], Theorem 19)**.** *Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ be a proper dual alternant code. Then*

$$\dim I_2(\mathscr{C}) \geq \frac{m}{2}(r-1)\left((2e_{\mathscr{A}}+1)r - 2\frac{q^{e_{\mathscr{A}}+1}-1}{q-1}\right), \tag{5}$$

where $e_{\mathscr{A}} = \lfloor \log_q(r-1) \rfloor$.

Note that we did not specify any generator matrix in the above statement, as the result is independent of such a choice. Even though the above result is an inequality, it turns out that one can confidently predict when equality holds.

Heuristic 1 ([FGO+10])**.** *Assume that $\boldsymbol{x}$ and $\boldsymbol{y}$ are chosen independently at random. Then equality is reached in Inequality (5) as soon as the right-hand side exceeds $\binom{rm+1}{2} - n$.*

This is the high-rate regime corresponding to the so called *square-distinguishability* of (duals of) alternant codes. In general, we say that alternant codes are square-distinguishable when the square of their dual code has dimension lower than $\min\{n, \binom{rm+1}{2}\}$, *i.e.* when the dimension of the square of the dual code is unexpectedly low compared to what we would obtain from a random code having the same parameters.

When we further assume that $r \leq q$, we see that $e_{\mathscr{A}} = 0$ and the dimension of $I_2(\mathscr{C})$ simplifies as

$$\dim I_2(\mathscr{C}) = m\binom{r-1}{2},$$

which means that in such a case, the dimension of the vanishing ideal at degree 2 of an alternant code is exactly m times that of the underlying GRS code, which suggests a link between the algebraic quadratic hull of the dual of an alternant code and that of the underlying GRS code. We use the geometric framework to explain this. Let $\mathcal{Y}$ be the geometric quadratic hull of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ with respect to $\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y})$. Recall that $\mathcal{Y}$, when seen as a projective variety, is the rational normal curve and its defining ideal is generated by the 2×2 minors of (3). A point $P = (p_0 : \ldots : p_{r-1}) \in \mathbb{P}^{r-1}(\mathbb{F}_{q^m})$ belongs to $\mathcal{Y}$ if and only if the vector $(p_0, \ldots, p_{r-1})$ satisfies these homogeneous quadratic equations. As we will explain in the following section, this condition boils down to the whole vector of coordinates $\Psi_\alpha(p_0, \ldots, p_{r-1}) \in \mathbb{F}_q^{rm}$ satisfying m quadratic relations over $\mathbb{F}_q$. In other words, any quadratic equation satisfied by the columns of $\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y})$ yields m quadratic equations satisfied by the columns of the parity-check matrix $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y}))$ of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$. This phenomenon highlights a link between the quadratic hull of an $\mathbb{F}_{q^m}$-linear code and that of its trace code. This is the concept of *affine Weil restriction*, to which the following section is dedicated.

3. Affine Weil restriction

The idea of Weil restriction is to construct a variety defined over $\mathbb{F}_q$ given a variety defined over $\mathbb{F}_{q^m}$ by splitting the variables of the defining equations according to their $\mathbb{F}_q$-coordinates. An algebraic variety $V \subset \mathbb{F}_{q^m}^r$ would thus give rise to a variety $W \stackrel{\text{def}}{=} \Psi_\alpha(V) \subset \mathbb{F}_q^{rm}$. Weil restriction is the process through which we obtain the defining ideal of W given the defining ideal of V.

3.1. **Definition and first properties.** Let $\boldsymbol{R} = \mathbb{F}_{q^m}[X_0, \ldots, X_{r-1}]$ be the polynomial ring over $\mathbb{F}_{q^m}$ in $r \geq 2$ variables. Besides, consider the two polynomial rings

$$\boldsymbol{S} = \mathbb{F}_q[x_{i,j} \mid 0 \leq i < r,\ 0 \leq j < m],$$

and

$$\boldsymbol{S} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} = \mathbb{F}_{q^m}[x_{i,j} \mid 0 \leq i < r,\ 0 \leq j < m].$$

This last ring, of which $\boldsymbol{S}$ is a subring, enables us to define the following as a homomorphism of graded $\mathbb{F}_{q^m}$-algebras:

$$\Phi : \begin{cases} \boldsymbol{R} & \longrightarrow \boldsymbol{S} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} \\ X_i & \longmapsto \sum_{j=1}^{r} \alpha^j x_{i,j}. \end{cases} \tag{6}$$

Applying Φ corresponds to splitting each variable X_i according to its $\mathbb{F}_q$-coordinates. The resulting polynomial has coefficients in $\mathbb{F}_{q^m}$, so we may again gather its $\mathbb{F}_q$-coordinates. In other words, for any $f \in \boldsymbol{R}$, there are unique $\Phi_1(f), \ldots, \Phi_m(f) \in \boldsymbol{S}$ such that

$$\Phi(f) = \sum_{j=0}^{m-1} \alpha^j \Phi_j(f).$$

In particular, each map $\Phi_j : \boldsymbol{R} \to \boldsymbol{S}$ is an $\mathbb{F}_q$-linear map.

Definition 6 (Weil restriction)**.** *The Weil restriction of an ideal $I \subset \boldsymbol{R}$ is defined by*

$$\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I) \overset{\text{def}}{=} \langle \Phi_j(f) \mid f \in I,\ 0 \leq j < m \rangle \subset \boldsymbol{S}.$$

The main property at the core of Weil restriction is the correspondence between rational points.

Proposition 4. *Let $I \subset \boldsymbol{R}$ be an ideal, and let $J = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I)$. Then*

$$V_{\mathbb{F}_q}(J) = \Psi_\alpha(V_{\mathbb{F}_{q^m}}(I)).$$

Proof. Let $P \in \mathbb{F}_{q^m}^r$. The following equivalences hold:

$$\begin{aligned}
\forall f \in I,\ f(P) = 0 &\iff \forall f \in I,\ \Phi(f)(\Psi_\alpha(P)) = 0 \\
&\iff \forall f \in I,\ \forall 0 \leq j < m,\ \Phi_j(f)(\Psi_\alpha(P)) = 0 \text{ By identification} \\
&\iff \forall g \in J,\ g(\Psi_\alpha(P)) = 0,
\end{aligned}$$

Hence $P \in V_{\mathbb{F}_{q^m}}(I) \iff \Psi_\alpha(P) \in V_{\mathbb{F}_q}(J)$, and thus $\Psi_\alpha(V_{\mathbb{F}_{q^m}}(I)) \subseteq V_{\mathbb{F}_q}(J)$. By taking $Q \in \mathbb{F}_q^{rm}$ and reading the above equivalences backwards with $\Psi_\alpha^{-1}(Q)$ playing the role of P, we obtain the converse inclusion. □

Weil restriction can be defined as a functor from the category of varieties defined over $\mathbb{F}_{q^m}$ to that of varieties defined over $\mathbb{F}_q$. This means that we can define the Weil restriction of a morphism $f : V_1 \to V_2$ as well, where $V_1 \subset \mathbb{F}_{q^m}^r$ and $V_2 \subset \mathbb{F}_{q^m}^s$ are algebraic varieties. We will restrict ourselves to the case where f is defined by a collection of polynomials $(f_1, \ldots, f_s)$, with each $f_i \in \mathbb{F}_{q^m}[V_1]$. In such a case, one can take any representative of each f_i in $\boldsymbol{R}$ and apply the map Φ, hence getting polynomials $\Phi_0(f_i), \ldots, \Phi_{m-1}(f_i) \in \boldsymbol{S}$.

Proposition 5. *The collection of polynomials $(\Phi_0(f_1), \ldots, \Phi_{m-1}(f_1), \ldots, \Phi_0(f_s), \ldots, \Phi_{m-1}(f_s))$ is a well-defined rational function $W_1 \to W_2$, where $W_i \overset{\text{def}}{=} \Psi_\alpha(V_i)$, $i \in \{1, 2\}$. We refer to it as the Weil restriction of f.*

Proof. Let $I \subset \boldsymbol{R}$ be the ideal defining V_1. By definition of Weil restriction, if $g \in I$, then all the $\Phi_j(g)$'s belong to $J \overset{\text{def}}{=} \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I)$. As a consequence, if $f \in \mathbb{F}_{q^m}[V_1]$ is defined up to an element of I, then all the $\Phi_j(f)$'s are well-defined up to an element of J. This proves that the collection of polynomials given in the proposition define a rational function $W_1 \to W_2$. □

Remark 4. This is again the good notion for Weil restriction, as we can easily see that the following

$$\begin{array}{ccc}
V_1 & \xrightarrow{\quad f \quad} & V_2 \\
{\scriptstyle \Psi_\alpha}\downarrow & & \downarrow{\scriptstyle \Psi_\alpha} \\
W_1 & \xrightarrow[\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f)]{} & W_2
\end{array}$$

is a commutative diagram.

We now investigate the case of $\mathbb{F}_{q^m}$-linear maps, as it will be central in the following. First, let us introduce the matrix $\boldsymbol{J} \in \mathbb{F}_q^{m \times m}$ defined as the matrix of the $\mathbb{F}_q$-linear map

$$\mu_\alpha : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow \mathbb{F}_{q^m} \\ x & \longmapsto \alpha x, \end{cases}$$

with respect to the monomial basis $(1, \alpha, \ldots, \alpha^{m-1})$ of $\mathbb{F}_{q^m}$. Note that $\boldsymbol{J}$ is nothing but the companion matrix of the minimal polynomial Π_α of α over $\mathbb{F}_q$. Given any field element $x = x_0 + x_1\alpha + \ldots + x_{m-1}\alpha^{m-1}$, the matrix $x_0\boldsymbol{I}_m + x_1\boldsymbol{J} + \ldots + x_{m-1}\boldsymbol{J}^{m-1}$ is the matrix of the

multiplication by x in the monomial basis $(1, \alpha, \ldots, \alpha^{m-1})$. We denote it by $\mathrm{Mat}_\alpha(x)$. All in all, the map

$$\mathrm{Mat}_\alpha : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow \mathbb{F}_q[\boldsymbol{J}] \\ x & \longmapsto \mathrm{Mat}_\alpha(x) \end{cases}$$

defines an isomorphism of $\mathbb{F}_q$-algebras. These matrices are the natural way of seeing multiplications in terms of $\mathbb{F}_q$-coordinates, as

$$\forall x, y \in \mathbb{F}_{q^m},\ \Psi_\alpha(xy) = \mathrm{Mat}_\alpha(x) \cdot \Psi_\alpha(y). \tag{7}$$

Furthermore, one can identify the image of Mat_α using the following criterion.

Proposition 6. *Let $\boldsymbol{B} \in \mathbb{F}_q^{m\times m}$. Then $\boldsymbol{B} \in \mathbb{F}_q[\boldsymbol{J}]$ if and only if $\boldsymbol{BJ} = \boldsymbol{JB}$.*

Proof. It is clear that a polynomial in $\boldsymbol{J}$ commutes with $\boldsymbol{J}$. Conversely, let $\boldsymbol{B} \in \mathbb{F}_q^{m\times m}$ and assume that $\boldsymbol{B}$ and $\boldsymbol{J}$ commute. The minimal polynomial $\Pi_{\boldsymbol{J}}$ of $\boldsymbol{J}$ over $\mathbb{F}_q$ is that of α, and is therefore irreducible of degree m. As $\mathbb{F}_{q^m}/\mathbb{F}_q$ is a Galois extension, $\Pi_{\boldsymbol{J}}$ splits into linear factors over $\mathbb{F}_{q^m}$. More precisely,

$$\Pi_{\boldsymbol{J}} = \prod_{j=0}^{m-1} (X - \alpha^{q^j}).$$

This implies that $\boldsymbol{J}$ is diagonalizable over $\mathbb{F}_{q^m}$, and there exists $\boldsymbol{P} \in \mathbf{GL}_m(\mathbb{F}_{q^m})$ such that

$$\boldsymbol{PJP}^{-1} = \Delta_\alpha \overset{\text{def}}{=} \mathrm{Diag}(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}),$$

the diagonal entries being pairwise distinct. Since $\boldsymbol{B}$ commutes with $\boldsymbol{J}$, we see that $\boldsymbol{PBP}^{-1}$ commutes with Δ_α and consequently stabilizes its eigenspaces. As the latter are lines, we conclude that $\boldsymbol{PBP}^{-1}$ is also a diagonal matrix and there exists $(\beta_1, \ldots, \beta_m) \in \mathbb{F}_{q^m}^m$ such that $\boldsymbol{PBP}^{-1} = \mathrm{Diag}(\beta_1, \ldots, \beta_m)$. Now let $f \in \mathbb{F}_{q^m}[X]$ be an interpolating polynomial such that $f(\alpha^{q^j}) = \beta_j$ for all j. We see that

$$f(\boldsymbol{PJP}^{-1}) = \boldsymbol{P}f(\boldsymbol{J})\boldsymbol{P}^{-1} = \mathrm{Diag}(f(\alpha), \ldots, f(\alpha^{q^{m-1}})) = \mathrm{Diag}(\beta_1, \ldots, \beta_m) = \boldsymbol{PBP}^{-1}.$$

Thus, $\boldsymbol{B} = f(\boldsymbol{J})$. By writing $f = f_0 + \alpha f_1 + \ldots + \alpha^{m-1} f_{m-1}$, with $f_j \in \mathbb{F}_q[X]$, and then proceeding through identification (which is possible as both $\boldsymbol{B}$ and $\boldsymbol{J}$ lie in $\mathbb{F}_q^{m\times m}$) we see that $\boldsymbol{B} = f_0(\boldsymbol{J})$ which ends the proof. □

Equation (7) essentially states that $\mathrm{Mat}_\alpha(x)$ is the matrix of the Weil restriction of the multiplication map associated to x. This can be naturally generalized to higher dimensions. More specifically, we define below the Weil restriction of a matrix.

Definition 7. *Let*

$$\boldsymbol{B} = (a_{i,j})_{\substack{1\le i\le s \\ 1\le j\le r}} \in \mathbb{F}_{q^m}^{s\times r}$$

be a matrix. We denote by $\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B})$ the matrix of the Weil restriction of the map $\boldsymbol{v} \mapsto \boldsymbol{Bv}$ in the canonical basis, i.e.

$$\forall \boldsymbol{v} \in \mathbb{F}_{q^m}^r,\ \Psi_\alpha(\boldsymbol{B} \cdot \boldsymbol{v}) = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B}) \cdot \Psi_\alpha(\boldsymbol{v}).$$

Remark 5. By applying Equation (7) coefficient-wise, we see that

$$\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B}) = \begin{pmatrix} \mathrm{Mat}_\alpha(a_{1,1}) & \ldots & \mathrm{Mat}_\alpha(a_{1,r}) \\ \vdots & \ddots & \vdots \\ \mathrm{Mat}_\alpha(a_{s,1}) & \ldots & \mathrm{Mat}_\alpha(a_{s,r}) \end{pmatrix} \in \mathbb{F}_q^{sm\times rm}.$$

For any non-negative integer k, let $\boldsymbol{J}_k = \mathrm{Diag}(\boldsymbol{J}, \dots, \boldsymbol{J})$. Note that $\boldsymbol{J}_k$ is the Weil restriction of the homothety of $\mathbb{F}_{q^m}^k$ defined by α, *i.e.* the scalar multiplication by α. Matrices of the form $\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B})$ can be identified in $\mathbb{F}_q^{sm \times rm}$ using the following algebraic criterion, which may be thought of as a generalization of Proposition 6.

Proposition 7. *Let $\boldsymbol{A} \in \mathbb{F}_q^{sm \times rm}$. The following are equivalent:*

(i) $\boldsymbol{A}\boldsymbol{J}_r = \boldsymbol{J}_s\boldsymbol{A}$;
(ii) there exists $\boldsymbol{B} \in \mathbb{F}_{q^m}^{s \times r}$ *such that* $\boldsymbol{A} = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B})$.

Proof. The existence of $\boldsymbol{B} \in \mathbb{F}_{q^m}^{s \times r}$ such that $\boldsymbol{A} = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B})$ is equivalent to each block $\boldsymbol{A}_{i,j} \in \mathbb{F}_q^{m \times m}$ being in the image of Mat_α, which by Proposition 6 boils down to the $\boldsymbol{A}_{i,j}$'s commuting with $\boldsymbol{J}$. Gathering these commutativity conditions is exactly equivalent to (i). □

3.2. **Weil-properness.** We now have introduced the necessary framework for stating as a proposition the link between the quadratic hull of an alternant code and that of the underlying GRS code.

Proposition 8. *Let $\mathscr{C} \subset \mathbb{F}_{q^m}^n$ be a proper code. Let $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r \times n}$ be a generator matrix of $\mathscr{C}$ and let $\boldsymbol{H}_{\mathrm{sec}} = \Psi_\alpha(\boldsymbol{G})$, which is the secret parity-check matrix of $\mathrm{Tr}(\mathscr{C})$. Then*

$$\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\langle I_2(\boldsymbol{G})\rangle) \subseteq \langle I_2(\boldsymbol{H}_{\mathrm{sec}})\rangle, \tag{8}$$

and

$$V_2(\boldsymbol{H}_{\mathrm{sec}}) \subseteq \Psi_\alpha(V_2(\boldsymbol{G})). \tag{9}$$

Proof. By Proposition 4, for any polynomial $f \in I_2(\boldsymbol{G})$, the $\Phi_j(f)$'s all vanish at the columns of $\boldsymbol{H}_{\mathrm{sec}}$. As a consequence,

$$\mathrm{Span}_{\mathbb{F}_q}\{\Phi_j(f) \mid f \in I_2(\boldsymbol{G}),\ 0 \leq j < m\} \subseteq I_2(\boldsymbol{H}_{\mathrm{sec}}),$$

which is a refinement of (8). Taking the varieties reverses the inclusion, which leads to (9) by Proposition 4. □

The above proposition only states inclusions, while equalities will be needed in the following.

Definition 8 (Weil-properness)**.** *A linear code $\mathscr{D} = \mathrm{Tr}(\mathscr{C})$ is said to be* ***Weil-proper*** *if and only if Inclusion (8) is an equality.*

Determining whether a linear code is Weil-proper may sometimes be done by just measuring the dimension of its vanishing ideal at degree 2. For alternant codes, we have the following result.

Proposition 9. *Under Heuristic 1, when $r \leq q$, a generic q-ary alternant code of degree r achieving equality in (5) is Weil-proper.*

For the proof of Proposition 9 we will need the following lemma. The proof of the lemma is quite technical and not really relevant here, which is why we decided to move it to the appendix.

Lemma 1. *Let $I \subset \boldsymbol{R}$ be a homogeneous ideal. If $(f_1, \dots, f_N)$ is a minimal set of generators for I, then the sequence $(\Phi_j(f_i))_{i,j}$ is a minimal set of generators of $\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I)$.*

In case of Weil-properness, it is indeed clear that if $(f_1, \dots, f_N)$ is a basis of $I_2(\boldsymbol{G})$, then $(\Phi_j(f_i))_{i,j}$ generates $I_2(\Psi_\alpha(\boldsymbol{G}))$. What is much less clear however is that there are no linear dependencies between the $\Phi_j(f_i)$'s over $\mathbb{F}_q$.

Corollary 2. *Let $\mathscr{D} = \mathrm{Tr}(\mathscr{C})$. Then $\mathscr{D}$ is Weil-proper if, and only if*

$$\dim_{\mathbb{F}_q} I_2(\mathscr{D}) = m \dim_{\mathbb{F}_{q^m}} I_2(\mathscr{C}).$$

Proof. By Proposition 8 and Lemma 1, the Weil restriction of $I_2(\mathscr{C})$ is an $m \dim_{\mathbb{F}_{q^m}} I_2(\mathscr{C})$-dimensional subspace of $I_2(\mathscr{D})$. Equality therefore holds if and only if $I_2(\mathscr{D})$ has dimension $m \dim_{\mathbb{F}_{q^m}} I_2(\mathscr{C})$. □

Gathering all these results enables us to prove Proposition 9 under Heuristic 1.

Proof of Proposition 9. When $r \leq q$, the vanishing ideal at degree 2 of a generic alternant code in the square-distinguishable regime equals m times the dimension of the vanishing ideal at degree 2 of the underlying GRS code. By Corollary 2 we get that such an alternant code is Weil-proper. □

Lemma 1 also allows us to derive a necessary condition for a code to be Weil proper in general in terms of regime of parameters.

Corollary 3. *Let $\mathscr{D} = \mathrm{Tr}(\mathscr{C})$ be a proper linear code, i.e. $\dim_{\mathbb{F}_q} \mathscr{D} = rm$ where $r = \dim_{\mathbb{F}_{q^m}} \mathscr{C}$. If $\mathscr{D}$ is Weil proper, then*

$$n \geq \binom{rm+1}{2} - m \dim_{\mathbb{F}_{q^m}} I_2(\mathscr{C}).$$

Proof. By Corollary 2, we have

$$\binom{rm+1}{2} - m \dim_{\mathbb{F}_{q^m}} I_2(\mathscr{C}) = \binom{rm+1}{2} - \dim_{\mathbb{F}_q} I_2(\mathscr{D}) = \dim \mathscr{D}^{\star 2} \leq n.$$

□

In the regime where an alternant code is Weil-proper, the Weil restriction structure of the quadratic hull may be visible even if we only have access to $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{P} \cdot \boldsymbol{H}_{\mathrm{sec}}$, thanks to Proposition 1. Our goal is to determine which properties of $I_2(\boldsymbol{H}_{\mathrm{sec}})$, related to its Weil restriction structure, are preserved by linear transformation and therefore still detectable in $I_2(\boldsymbol{H}_{\mathrm{pub}})$. This naturally leads to the problem of distinguishing affine varieties that are the Weil restriction of a smaller variety over a larger field.

3.3. **Distinguishing Weil restrictions.** Our strategy for finding a criterion that distinguishes Weil restrictions from other varieties consists in first looking at the case of vector subspaces, and then generalizing to algebraic varieties using tangent spaces.

Let $V \subset \mathbb{F}_{q^m}^r$ be some vector subspace. Intuitively, $\Psi_\alpha(V)$ not only lists the points of V in terms of $\mathbb{F}_q$-coordinates, but also somehow reflects the $\mathbb{F}_{q^m}$-linearity of V. More formally, the fact that if $\boldsymbol{v} \in V$, then $\alpha \cdot \boldsymbol{v} \in V$ must be visible in W. Indeed, as $\boldsymbol{J}_r$ is the Weil restriction of the scalar multiplication by α, we see that

$$\alpha \cdot \boldsymbol{v} \in V \iff \boldsymbol{J}_r \cdot \Psi_\alpha(\boldsymbol{v}) \in W. \tag{10}$$

The following proposition states that this can be used to identify Weil restriction of vector spaces.

Lemma 2. *Let $W \subset \mathbb{F}_q^{rm}$ be a vector subspace. The following are equivalent:*

(i) W is $\boldsymbol{J}_r$-invariant, i.e. $\forall \boldsymbol{x} \in W,\ \boldsymbol{J}_r \boldsymbol{x} \in W$;
(ii) There exists some subspace $V \subset \mathbb{F}_{q^m}^r$ such that $W = \Psi_\alpha(V)$.

Proof. Let $W \subset \mathbb{F}_q^{rm}$ be a vector subspace, and set $V = \Psi_\alpha^{-1}(W)$, which is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}^r$ a priori. It suffices to prove that W is $\boldsymbol{J}_r$-invariant if and only if V is an $\mathbb{F}_{q^m}$-vector subspace of $\mathbb{F}_{q^m}^r$. Since V is already an $\mathbb{F}_q$-vector space, it is an $\mathbb{F}_{q^m}$-vector space if, and only if

$$\forall \boldsymbol{v} \in V,\ \alpha \boldsymbol{v} \in V,$$

which by Equivalence (10) is equivalent to

$$\forall \boldsymbol{v} \in V,\ \boldsymbol{J}_r \Psi_\alpha(\boldsymbol{v}) \in W.$$

Finally, since Ψ_α is a bijection between V and W, we see that V is an $\mathbb{F}_{q^m}$-vector subspace if and only if

$$\forall \boldsymbol{w} \in W,\ \boldsymbol{J}_r \boldsymbol{w} \in W,$$

which proves the proposition. □

Remark 6. Lemma 2 is actually a well-known result from the theory of matrix rank-metric codes. More precisely, given a k-dimensional $\mathbb{F}_{q^m}$-linear code $\mathscr{C} \subset \mathbb{F}_{q^m}^n$ endowed with the rank-metric, one can build a code $\mathscr{C}_{\mathrm{mat}}$ from a basis $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_k\}$ of $\mathscr{C}$ by defining

$$\mathscr{C}_{\mathrm{mat}} = \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{M}_{1,0}, \dots, \boldsymbol{M}_{1,m-1}, \dots, \boldsymbol{M}_{k,0}, \dots, \boldsymbol{M}_{k,m-1}\},$$

where $\boldsymbol{M}_{i,j} = (\Psi_\alpha(\alpha^j v_{i,1}) | \dots | \Psi_\alpha(\alpha^j v_{i,n})) \in \mathbb{F}_q^{m \times n}$, with $\boldsymbol{v}_i = (v_{i,1}, \dots, v_{i,n})$. As $\mathscr{C}$ is an $\mathbb{F}_{q^m}$-linear code, we have

$$\forall \boldsymbol{M} \in \mathscr{C}_{\mathrm{mat}},\ \boldsymbol{J}\boldsymbol{M} \in \mathscr{C}_{\mathrm{mat}}.$$

More generally, an $\mathbb{F}_q$-vector subspace $\mathscr{M} \subset \mathbb{F}_q^{m \times n}$ is $\mathbb{F}_{q^m}$-linear, *i.e.* built using the above process, if and only if $\boldsymbol{J}\boldsymbol{M} \in \mathscr{M}$ for all $\boldsymbol{M} \in \mathscr{M}$.

Definition 9 (Stabilizer)**.** *For any vector space $W \subset \mathbb{F}_q^{rm}$, we denote by* $\mathrm{St}(W)$ *the set of matrices $\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm}$ such that $\boldsymbol{A} \cdot W \subseteq W$. Note that* $\mathrm{St}(W)$ *is a subalgebra of the $\mathbb{F}_q$-algebra $\mathbb{F}_q^{rm \times rm}$.*

Remark 7. Lemma 2 amounts to say that a subspace W is a Weil restriction if and only if we have $\mathbb{F}_q[\boldsymbol{J}_r] \subset \mathrm{St}(W)$.

Distinguishing Weil restrictions is therefore a solved problem when it comes to vector subspaces. In order to generalize our approach for algebraic varieties, we need some linear data associated to varieties. This is exactly the role played by tangent spaces.

Definition 10. *Let $P \in V \overset{\mathrm{def}}{=} V_{\mathbb{F}_{q^m}}(I)$ where $I \subset \boldsymbol{R}$ is an ideal. The tangent space of V at P is defined by*

$$T_P V = \left\{ \boldsymbol{h} \in \mathbb{F}_{q^m}^r \mid \forall f \in I,\ \sum_{i=0}^{r-1} h_i \partial_i f(P) = 0 \right\}.$$

As I is finitely generated, $T_P V$ may be computed as the kernel of the Jacobian matrix of a list of generators.

A vector subspace of $\mathbb{F}_q^{rm}$ is a Weil restriction if and only if it is globally invariant under the action of $\boldsymbol{J}_r$. When a variety W is the Weil restriction of some other variety V, then one can expect that its tangent spaces are also the Weil restriction of some vector subspace of $\mathbb{F}_{q^m}^r$. This would enable us to use our criterion to determine whether a variety is a Weil restriction. It turns out that it is true, thanks to the commutativity between Weil restrictions and tangent spaces.

Proposition 10. *Let $V = V_{\mathbb{F}_{q^m}}(I) \subset \mathbb{F}_{q^m}^r$ be an algebraic variety of defining ideal $I \subset \boldsymbol{R}$. Let $W = \Psi_\alpha(V)$, $P \in V$ and $Q = \Psi_\alpha(P)$. Then*

$$T_Q W = \Psi_\alpha(T_P V).$$

Proof. First, notice that by the rules of derivation, we have

$$\partial_{ij} \Phi(f) = \alpha^j \Phi(\partial_i f), \tag{11}$$

for all $f \in \boldsymbol{R}$ and indices $0 \leq i < r, 0 \leq j < m$. Now, let $\boldsymbol{h} = (h_{i,j}) \in \mathbb{F}_q^{rm}$. We have

$$\begin{aligned}
\boldsymbol{h} \in \Psi_\alpha(T_P V) &\iff \forall f \in I,\ \sum_{i=0}^{r-1} \left(\sum_{j=0}^{m-1} h_{i,j} \alpha^j \right) \partial_i f(P) = 0 \\
&\iff \forall f \in I,\ \sum_{i=0}^{r-1} \sum_{j=0}^{m-1} h_{i,j} \alpha^j \Phi(\partial_i f)(Q) = 0 \text{ Since } \partial_i f(P) = \Phi(\partial_i f)(Q) \\
&\iff \forall f \in I,\ \sum_{i=0}^{r-1} \sum_{j=0}^{m-1} h_{i,j} \partial_{ij} \Phi(f)(Q) = 0 \text{ By Equation (11)} \\
&\iff \forall f \in I,\ \forall 0 \leq \ell < m,\ \sum_{i=0}^{r-1} h_{i,j} \partial_{ij} \Phi_\ell(f)(Q) = 0 \\
&\iff \boldsymbol{h} \in T_Q W.
\end{aligned}$$

□

This gives us a necessary condition for an algebraic variety to be a Weil restriction.

Corollary 4. *Let $W \subset \mathbb{F}_q^{rm}$ be an algebraic variety. If there exists an algebraic variety $V \subset \mathbb{F}_{q^m}^r$ such that $W = \Psi_\alpha(V)$, then for all $Q \in W$, the tangent space $T_Q W \subset \mathbb{F}_q^{rm}$ is $\boldsymbol{J}_r$-invariant.*

Back to linear codes, we obtain the following corollary.

Corollary 5. *Let $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y}))$ be the secret parity-check matrix of a Weil-proper alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$. For all $P \in V_{\text{sec}} \overset{\text{def}}{=} V_2(\boldsymbol{H}_{\text{sec}})$, the tangent space $T_P V_{\text{sec}}$ is $\boldsymbol{J}_r$-invariant.*

3.4. **Weil-preserving transformations.** Corollary 5 establishes a distinguishing property for the quadratic hull of a Weil-proper alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ with respect to a secret parity-check matrix $\boldsymbol{H}_{\text{sec}}$, *i.e.* of the form $\Psi_\alpha(\boldsymbol{G})$ where $\boldsymbol{G}$ is a generator matrix of the underlying GRS code. Again, denote by $\boldsymbol{H}_{\text{pub}}$ the corresponding public key, which is related to the private key by the relation $\boldsymbol{H}_{\text{pub}} = \boldsymbol{P}\boldsymbol{H}_{\text{sec}}$ for some secret nonsingular $rm \times rm$ matrix $\boldsymbol{P}$, which is nothing but a change of basis. We get the following proposition given how a change of basis acts on linear maps.

Proposition 11. *If $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ is Weil-proper, then for all $Q \in V_{\text{pub}} \overset{\text{def}}{=} V_2(\boldsymbol{H}_{\text{pub}})$, the tangent space $T_Q V_{\text{pub}}$ is globally invariant under the action of $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}$.*

Proof. We know from Proposition 1 that $V_{\text{pub}} = \boldsymbol{P} \cdot V_{\text{sec}}$, which implies that $T_Q V_{\text{pub}} = \boldsymbol{P} \cdot T_{\boldsymbol{P}^{-1}Q} V_{\text{sec}}$. Since $T_{\boldsymbol{P}^{-1}Q} V_{\text{sec}}$ is $\boldsymbol{J}_r$-invariant, $T_Q V_{\text{pub}}$ is $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}$-invariant. □

All tangent spaces of the public variety V_{pub} share the property of being invariant under the very same linear operator. This will be the first cornerstone of our attack, which we will detail in the following section. The second core idea behind the attack consists in finding another transition matrix than $\boldsymbol{P}$ that directly leaks a generator matrix of the underlying GRS code — or, as we will see, one of its conjugates. Such a transition matrix would also map the variety $V_{\text{sec}} \overset{\text{def}}{=} V_2(\boldsymbol{H}_{\text{sec}})$ onto another algebraic variety, itself being linked to the quadratic hull of a GRS code through Weil restriction. We then see that the set of such transition matrices are exactly those that map Weil restrictions onto other Weil restrictions. The following theorem is an exhaustive description of such linear transformations.

Weil restrictions of invertible $r \times r$ matrices over $\mathbb{F}_{q^m}$ are natural candidates for such transition matrices. If $\boldsymbol{A} = \text{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B})$, then $\boldsymbol{A}$ indeed maps a Weil restriction $W = \Psi_\alpha(V)$ onto that of

$\boldsymbol{B} \cdot V$. Another type of transformations mapping Weil restrictions onto Weil restrictions is given by the Frobenius automorphism. Let $\boldsymbol{\Theta}$ be the matrix of the Frobenius automorphism $\theta : x \mapsto x^q$ in the monomial basis $(1, \alpha, \dots, \alpha^{m-1})$, and define $\boldsymbol{\Theta}_r = \mathrm{Diag}(\boldsymbol{\Theta}, \dots, \boldsymbol{\Theta}) \in \mathbb{F}_q^{rm \times rm}$. Then $\boldsymbol{\Theta}_r$ maps $W = \Psi_\alpha(V)$ onto the Weil restriction of $V^q = \{(v_1^q, \dots, v_r^q) \mid \boldsymbol{v} \in V\}$, which is also an algebraic variety. The following theorem essentially states that these two examples generate all possible matrices mapping Weil restrictions onto Weil restrictions.

Theorem 3. *Let $\mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$ be the set of invertible $rm \times rm$ matrices over $\mathbb{F}_q$ that map Weil restrictions of subvarieties of $\mathbb{F}_{q^m}^r$ onto Weil restrictions of subvarieties of $\mathbb{F}_{q^m}^r$. Then*

$$\mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r) = \{\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B}) \cdot \boldsymbol{\Theta}_r^j \mid \boldsymbol{B} \in \mathbf{GL}_r(\mathbb{F}_{q^m}),\ 0 \leq j < m\}.$$

The goal of the attack will be to find a matrix $\boldsymbol{Q}$ such that $\boldsymbol{QP} \in \mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$, so that the columns of $\boldsymbol{QH}_{\mathrm{pub}} = \boldsymbol{QPH}_{\mathrm{sec}}$ belong to the Weil restriction of some rational normal curve. Before proving Theorem 3, we need to give two auxiliary results. The first gives a better description of the action of the Frobenius automorphism in terms of $\mathbb{F}_q$-coordinates. The matrix $\boldsymbol{\Theta}$ represents the Frobenius map in the following way:

$$\forall x \in \mathbb{F}_{q^m},\ \Psi_\alpha(x^q) = \boldsymbol{\Theta} \cdot \Psi_\alpha(x).$$

Meanwhile, the element $x \in \mathbb{F}_{q^m}$ is also identified with the matrix $\mathrm{Mat}_\alpha(x)$. Since Mat_α is a field isomorphism, we have

$$\forall x \in \mathbb{F}_{q^m},\ \mathrm{Mat}_\alpha(x^q) = \mathrm{Mat}_\alpha(x)^q.$$

There is a way of expressing the above property using the matrix $\boldsymbol{\Theta}$ as stated in our first lemma.

Lemma 3. *For all $x \in \mathbb{F}_{q^m}$, $\mathrm{Mat}_\alpha(x)^q = \boldsymbol{\Theta} \cdot \mathrm{Mat}_\alpha(x) \cdot \boldsymbol{\Theta}^{-1}$.*

Proof. Let $x \in \mathbb{F}_{q^m}$. For all $y \in \mathbb{F}_{q^m}$, we have

$$\begin{aligned}
\boldsymbol{\Theta} \cdot \mathrm{Mat}_\alpha(x) \cdot \Psi_\alpha(y) &= \boldsymbol{\Theta} \cdot \Psi_\alpha(xy) \\
&= \Psi_\alpha((xy)^q) \\
&= \Psi_\alpha(x^q y^q) \\
&= \mathrm{Mat}_\alpha(x^q) \cdot \Psi_\alpha(y^q) \\
&= \mathrm{Mat}_\alpha(x)^q \cdot \boldsymbol{\Theta} \cdot \Psi_\alpha(y),
\end{aligned}$$

and this holds for any choice of $y \in \mathbb{F}_{q^m}$. As a result, $\boldsymbol{\Theta} \cdot \mathrm{Mat}_\alpha(x) = \mathrm{Mat}_\alpha(x)^q \cdot \boldsymbol{\Theta}$. □

Remark 8. Lemma 3 can be summed up in one sentence, essentially saying that conjugation by the matrix $\boldsymbol{\Theta}$ and Galois conjugation by the Frobenius automorphism boil down to the very same operation.

Lemma 2 states that vector subspaces that are the Weil restriction of another vector space are stabilized by $\boldsymbol{J}_r$, and therefore by any polynomial in $\boldsymbol{J}_r$. Such a matrix is nothing but the Weil restriction of an $\mathbb{F}_{q^m}$-homothety. The second ingredient in the proof of Theorem 3 is the converse: a matrix that stabilizes all vector subspaces that are a Weil restriction is a polynomial in $\boldsymbol{J}_r$.

Lemma 4. *Let $\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm}$. If $\boldsymbol{A}$ stabilizes all vector subspaces of $\mathbb{F}_q^{rm}$ that are the Weil restriction of a subspace of $\mathbb{F}_{q^m}^r$, then $\boldsymbol{A} \in \mathbb{F}_q[\boldsymbol{J}_r]$.*

Proof. Let us introduce the $\mathbb{F}_q$-linear endomorphism a of $\mathbb{F}_{q^m}^r$ represented by the matrix $\boldsymbol{A}$, *i.e.* a is defined by

$$\forall \boldsymbol{v} \in \mathbb{F}_{q^m}^r,\ a(\boldsymbol{v}) = \Psi_\alpha^{-1}(\boldsymbol{A} \cdot \Psi_\alpha(\boldsymbol{v})).$$

Since $\boldsymbol{A}$ stabilizes vector subspaces that are Weil restrictions, it stabilizes in particular Weil restrictions of $\mathbb{F}_{q^m}$-lines. Equivalently, the $\mathbb{F}_q$-linear endomorphism a maps any vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^r$ onto some $\lambda_{\boldsymbol{v}}\boldsymbol{v}$, with $\lambda_{\boldsymbol{v}} \in \mathbb{F}_{q^m}$. If now we take two vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_{q^m}^r$, then by $\mathbb{F}_q$-linearity we have

$$a(\boldsymbol{u}+\boldsymbol{v}) = \lambda_{\boldsymbol{u}+\boldsymbol{v}}(\boldsymbol{u}+\boldsymbol{v}) = a(\boldsymbol{u}) + a(\boldsymbol{v}) = \lambda_{\boldsymbol{u}}\boldsymbol{u} + \lambda_{\boldsymbol{v}}\boldsymbol{v}.$$

As $r \geq 2$, we can take $\boldsymbol{u}$ and $\boldsymbol{v}$ linearly independent over $\mathbb{F}_{q^m}$, which then implies

$$\lambda_{\boldsymbol{u}+\boldsymbol{v}} = \lambda_{\boldsymbol{u}} = \lambda_{\boldsymbol{v}}.$$

Finally, by noticing that the same reasoning holds if we replace $\boldsymbol{v}$ with $\beta\boldsymbol{v}$ for some nonzero $\beta \in \mathbb{F}_{q^m}$, we conclude that $\lambda_{\beta\boldsymbol{v}} = \lambda_{\boldsymbol{v}}$. All in all, there exists a *unique* $\lambda \in \mathbb{F}_{q^m}$ such that

$$\forall \boldsymbol{v} \in \mathbb{F}_{q^m}^r,\ a(\boldsymbol{v}) = \lambda\boldsymbol{v},$$

which indeed means that a is an $\mathbb{F}_{q^m}$-linear homothety. In terms of matrices, this implies that $\boldsymbol{A} = f(\boldsymbol{J}_r)$, the polynomial $f \in \mathbb{F}_q[X]$ being the one that determines λ. □

Remark 9. The assumption $r \geq 2$ that we made at the very beginning of this section is mandatory here, not only for the proof to work but also for the result to hold. If indeed $r = 1$, then the only $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^r$ are $\{0\}$ and $\mathbb{F}_{q^m}$, whose Weil restriction are respectively $\{0\}$ and $\mathbb{F}_q^m$. All matrices $\boldsymbol{A} \in \mathbb{F}_q^{m\times m}$ stabilize these spaces, and therefore the implication stated by Lemma 4 is untrue in this case.

We are now ready to prove Theorem 3.

Proof of Theorem 3. Clearly any matrix $\boldsymbol{A}$ of the form $\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B}) \cdot \boldsymbol{\Theta}^j$ is the Weil restriction of some $\mathbb{F}_q$-linear automorphism $a = b \circ \theta^j$. Therefore, if $W = \Psi_\alpha(V)$, then $\boldsymbol{A}$ maps W onto the Weil restriction of $b(V^{q^j})$.

Now let $\boldsymbol{A} \in \mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$. We aim to show that there exists some integer j such that $\boldsymbol{A}\boldsymbol{\Theta}^j$ is the Weil restriction of an $\mathbb{F}_{q^m}$-linear automorphism of $\mathbb{F}_{q^m}^r$. Firstly, notice that since $\boldsymbol{A}$ is a bijection as a linear map, any linear Weil restriction can be seen as the preimage through $\boldsymbol{A}$ of another linear Weil restriction, and as such is stabilized by both $\boldsymbol{J}_r$ and $\boldsymbol{A}^{-1}\boldsymbol{J}_r\boldsymbol{A}$. By Lemma 4, we conclude that $\boldsymbol{A}^{-1}\boldsymbol{J}_r\boldsymbol{A}$ is a polynomial in $\boldsymbol{J}_r$. Furthermore, conjugation by the matrix $\boldsymbol{A}^{-1}$ is an automorphism of the $\mathbb{F}_q$-algebra $\mathbb{F}_q^{rm\times rm}$, which means that it induces an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_q[\boldsymbol{J}_r] \simeq \mathbb{F}_{q^m}$. In other words, conjugation by $\boldsymbol{A}^{-1}$ defines an element of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle\theta\rangle$. This means that $\boldsymbol{A}^{-1}\boldsymbol{J}_r\boldsymbol{A}$ is actually an $\mathbb{F}_q$-conjugate of $\boldsymbol{J}_r$, *i.e.* of the form $\boldsymbol{J}_r^{q^j}$ for some integer j. Equivalently by Lemma 3, there is an integer j such that

$$\boldsymbol{A}^{-1}\boldsymbol{J}_r\boldsymbol{A} = \boldsymbol{\Theta}^j\boldsymbol{J}_r\boldsymbol{\Theta}^{-j},$$

which implies $\boldsymbol{A}\boldsymbol{\Theta}^j$ commutes with $\boldsymbol{J}_r$. By Proposition 7, $\boldsymbol{A}\boldsymbol{\Theta}^j = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{B})$ for some $\boldsymbol{B} \in \mathbf{GL}_r(\mathbb{F}_{q^m})$, which proves the theorem. □

Corollary 6. *Let $\boldsymbol{A} \in \mathbf{GL}_{rm}(\mathbb{F}_q)$. Then $\boldsymbol{A} \in \mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$ if, and only if there exists some integer j such that $\boldsymbol{A}\boldsymbol{J}_r\boldsymbol{A}^{-1} = \boldsymbol{J}_r^{q^j}$.*

Proof. Write $\boldsymbol{A} = \boldsymbol{A}_0\boldsymbol{\Theta}^j$ for some integer j. Since $\boldsymbol{A}_0$ commutes with $\boldsymbol{J}_r$ by Proposition 7, we see that

$$\boldsymbol{A}^{-1}\boldsymbol{J}_r\boldsymbol{A} = \boldsymbol{\Theta}^{-j}\boldsymbol{A}_0^{-1}\boldsymbol{J}_r\boldsymbol{A}_0\boldsymbol{\Theta}^j = \boldsymbol{\Theta}^{-j}\boldsymbol{J}_r\boldsymbol{\Theta}^j = \boldsymbol{J}_r^{q^{m-j}},$$

the last equality coming from Lemma 3. Raising the above equality to the power q^j gives

$$\boldsymbol{A}\boldsymbol{J}_r\boldsymbol{A}^{-1} = \boldsymbol{J}_r^{q^j},$$

as required. The converse can be obtained in the same way by reading the above backwards. □

Proposition 12. *$\mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$ is a subgroup of $\mathbf{GL}_{rm}(\mathbb{F}_q)$, and its group structure is given by*

$$\mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r) \simeq \mathbf{GL}_r(\mathbb{F}_{q^m}) \rtimes \mathbb{Z}/m\mathbb{Z}.$$

Proof. We identify $\mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$ with the set of $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}^r$ of the form $b \circ \theta^j$ for $b \in \mathbf{GL}(\mathbb{F}_{q^m}^r)$ and $0 \leq j < m$. Then for any $c \in \mathbf{GL}(\mathbb{F}_{q^m}^r)$ and $0 \leq k < m$, we see that

$$(c \circ \theta^k) \circ (b \circ \theta^j) = (c \circ b^{(q^k)}) \circ \theta^{k+j},$$

where $b^{(q^k)}$ is the $\mathbb{F}_{q^m}$-automorphism whose matrix in the canonical basis is that of b where all coefficients have been raised to the power q^k. This is indeed a semi-direct product group structure between $\mathbf{GL}(\mathbb{F}_{q^m}^r) \simeq \mathbf{GL}_r(\mathbb{F}_{q^m})$ and $\langle\theta\rangle \simeq \mathbb{Z}/m\mathbb{Z}$. □

4. An attack against generic square-distinguishable alternant codes

Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ be a generic q-ary alternant code of extension degree m. We assume that we are in the square-distinguishable regime, *i.e.* that the right-hand side of Inequality (5) is greater than $n - \binom{rm+1}{2}$, so that Inequality (5) is an equality by Heuristic 1. In the following, we denote by $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y}))$ the secret parity-check matrix of $\mathscr{C}$, where $\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y})$ is the Vandermonde generator matrix of Remark 2. The public key is another parity-check matrix $\boldsymbol{H}_{\text{pub}} = \boldsymbol{P}\boldsymbol{H}_{\text{sec}}$, where $\boldsymbol{P}$ is a secret $rm \times rm$ nonsingular q-ary matrix. We also denote by V_{sec} (resp. V_{pub}) the geometric quadratic hull of $\boldsymbol{H}_{\text{sec}}$ (resp. $\boldsymbol{H}_{\text{pub}}$). By Proposition 1, we have $V_{\text{pub}} = \boldsymbol{P} \cdot V_{\text{sec}}$. We aim to recover the private key, which is an efficient decoding algorithm for $\mathscr{C}$. Our global approach follows a quite natural strategy consisting in retrieving some support $\boldsymbol{x}'$ and multiplier $\boldsymbol{y}'$.

4.1. Case $r \leq q$.

In the regime where $r \leq q$, Proposition 9 ensures that $\mathscr{C}$ is a Weil-proper alternant code. By Proposition 11, *all* the tangent spaces of V_{pub} are stabilized by $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}$. These tangent spaces have dimension $2m$, as they are the image through $\boldsymbol{P}$ of the tangent spaces of V_{sec}, themselves being the Weil restrictions of the tangent spaces of the quadratic hull of $\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y})$ by Proposition 10, which we know have dimension 2 as tangent spaces of the affine cone over a projective curve. Intuitively, there should not be much more matrices stabilizing all tangent spaces of V_{sec} than those that stabilize all Weil restrictions. Although this statement is likely to be provable, we state the following result as a heuristic.

Heuristic 2. *Generally, we have*

$$\bigcap_{Q \in V_{\text{pub}}} \mathrm{St}(T_Q V_{\text{pub}}) = \mathbb{F}_q[\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}].$$

Experimentally, taking the intersection over only

$$N \stackrel{\text{def}}{=} \left\lceil \frac{1}{\rho(1-\rho)} \right\rceil$$

points, where $\rho = \dfrac{2}{r}$, suffices to get $\mathbb{F}_q[\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}]$.

Let $\mathcal{A} \stackrel{\text{def}}{=} \mathbb{F}_q[\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}]$. In order to compute $\mathcal{A}$ in practice, one has to compute sufficiently many tangent spaces and then compute the space of matrices that stabilize all of them. Computing tangent spaces of V_{pub} can be done in polynomial time by merely computing the right kernel of the Jacobian matrix of a basis of the vanishing ideal at degree 2. Recall that computing rational points of V_{pub} is free, as we already have n points given by the columns of $\boldsymbol{H}_{\text{pub}}$. Finally, computing the stabilizing algebra of all those tangent spaces can be done by simply solving a linear system of $2m \times (rm - 2m)$ equations. Indeed, let $\boldsymbol{A} = (a_{i,j})$ be an $rm \times rm$ matrix whose entries are unknowns. Let $T = T_{\boldsymbol{g}} V_{\text{pub}}$ be the tangent space of V_{pub} at some point $\boldsymbol{g}$, that we

may assume to be a column of $\boldsymbol{H}_{\text{pub}}$. Then T can be seen as a linear code, and as such we can compute a generator matrix $\boldsymbol{G}$ and a parity-check matrix $\boldsymbol{H}$ of T. Then $\boldsymbol{A}$ stabilizes T if and only if for any $\boldsymbol{h} \in T$, the vector $\boldsymbol{Ah}$ is orthogonal to the rows of $\boldsymbol{H}$. By linearity, the matrix $\boldsymbol{A}$ stabilizes T if and only if for any row $\boldsymbol{r}$ of $\boldsymbol{G}$, we have $\boldsymbol{HAr}^\top = 0$. All in all, the equations over the $a_{i,j}$'s expressing the fact that $\boldsymbol{A}$ stabilizes T are the coefficients of $\boldsymbol{HAG}^\top$, which is indeed an $(rm - 2m) \times 2m$ matrix. Gathering these equations in a list for sufficiently many tangent spaces, we get a system of equations whose solution space is the intersection of the stabilizers of all these tangent spaces. For the system to be overdetermined, we need to compute at least

$$\left\lceil \frac{(rm)^2}{2m(rm-2m)} \right\rceil = \left\lceil \frac{1}{\rho(1-\rho)} \right\rceil$$

tangent spaces, which explains Heuristic 2. Step by step, we give a full algorithm for recovering $\mathcal{A}$.

Algorithm 1 Computing $\mathcal{A} = \mathbb{F}_q[\boldsymbol{PJ}_r\boldsymbol{P}^{-1}]$

1: **Input:** $\boldsymbol{H}_{\text{pub}} = (\boldsymbol{g}_1|\dots|\boldsymbol{g}_n)$ the public parity-check matrix of $\mathscr{C}$
2: **Output:** $\boldsymbol{A}_1, \dots, \boldsymbol{A}_m$ an $\mathbb{F}_q$-basis of $\mathcal{A}$
3: Compute a basis $\mathcal{F} = (f_1, \dots, f_N)$ of $I_2(\boldsymbol{H}_{\text{pub}})$
4: Compute the Jacobian matrix $\mathbf{Jac}(\mathcal{F}) = (\partial_{jk} f_i)_{i;j,k} \in \boldsymbol{S}_1^{N \times rm}$
5: $\boldsymbol{A} \leftarrow (a_{i,j})$ ▷ Its entries are unknowns, or formal variables $a_{i,j}$
6: $\mathcal{S} \leftarrow \varnothing$ ▷ A set of linear equations over the $a_{i,j}$'s defining the stabilizers
7: $i \leftarrow 0$
8: **while** $\#\mathcal{S} < (rm)^2$ **do** ▷ While there are more unknowns than equations
9: Compute $T_i \overset{\text{def}}{=} T_{\boldsymbol{g}_i} V$ as the right kernel of $\mathbf{Jac}(\mathcal{F})(\boldsymbol{g}_i)$
10: Compute a generator matrix $\boldsymbol{G}_i$ and a parity-check matrix $\boldsymbol{H}_i$ of T_i
11: Add to $\mathcal{S}$ the coefficients of $\boldsymbol{H}_i\boldsymbol{A}\boldsymbol{G}_i^\top$
12: $i \leftarrow i + 1$
13: Compute $\boldsymbol{A}_1, \dots, \boldsymbol{A}_m$ a basis of the solution space of $\mathcal{S}$
14: **return** $\boldsymbol{A}_1, \dots, \boldsymbol{A}_m$

Theorem 4. *Assuming Heuristic 2 is true, Algorithm 1 returns a basis of $\mathcal{A}$ in $O\left(rn^\omega\right)$ operations in $\mathbb{F}_q$, where ω is the exponent of linear algebra.*

Proof. Step 3 amounts to computing the left kernel of the matrix whose rows are $\boldsymbol{r}_i \star \boldsymbol{r}_j$, $i \leq j$, where $\boldsymbol{r}_i$ stands for the i-th row of $\boldsymbol{G}_{\text{pub}}$. This is a $\binom{rm+1}{2} \times n$ matrix. As we assume to be in a regime where there are no elements in $I_2(\boldsymbol{G}_{\text{pub}})$ whose existence is forced by dimension, we have $\binom{rm+1}{2} = O(n)$ and the cost of Step 3 is therefore $O(n^\omega)$.
The cost of Step 4 is negligible compared to that of Step 9. Evaluating $\mathbf{Jac}(\mathcal{F})$ at $\boldsymbol{g}_i$ is also negligible compared to computing the right-kernel of the resulting matrix, which costs $O(n^\omega)$ or even less since $\dim I_2(\boldsymbol{G}_{\text{pub}})$ is typically significantly inferior to n. Step 11 adds $2m \times (rm - 2m)$ equations to the set $\mathcal{S}$. The number of times we need to go through the loop to have $\#\mathcal{S} \geq (rm)^2$ is therefore

$$\frac{(rm)^2}{2m(rm-2m)} = \frac{r^2}{2(r-2)} < r.$$

We conclude that we need to go through the loop $O(r)$ times to complete $\mathcal{S}$. Once this is done, Heuristic 2 ensures that the matrices that satisfy all equations of $\mathcal{S}$ are in $\mathcal{A}$. Solving the system costs $O((rm)^{2\omega}) = O(n^\omega)$ operations in $\mathbb{F}_q$. The overall complexity is therefore $O(rn^\omega)$, as we compute the right-kernel of the Jacobian matrix $O(r)$ times. □

Remark 10. Essentially, we need to compute sufficiently many equations so that the linear system $\mathcal{S}$ is overdetermined. Experimentally, having $\mathcal{S}$ overdetermined always suffices to have the solutions space reduced to $\mathcal{A}$. If it is not the case, we just need to add a few more equations by computing some additional tangent spaces. We expect the number of potential additional steps to be negligible, so that it does not change the total complexity of Algorithm 1.

Using Algorithm 1, we get access to $\mathcal{A}$. The next step is to use the field structure of $\mathcal{A}$, which is ensured by the following.

Proposition 13. $\mathcal{A} \simeq \mathbb{F}_{q^m}$.

Proof. We already have $\mathbb{F}_q[\boldsymbol{J}_r] \simeq \mathbb{F}_q[\boldsymbol{J}] \simeq \mathbb{F}_{q^m}$, the last isomorphism being Mat_α. Now, define

$$C_{\boldsymbol{P}} : \begin{cases} \mathbb{F}_q^{rm \times rm} & \longrightarrow \mathbb{F}_q^{rm \times rm} \\ \boldsymbol{A} & \longmapsto \boldsymbol{P}\boldsymbol{A}\boldsymbol{P}^{-1}, \end{cases}$$

which we refer to as *the conjugation map of* $\boldsymbol{P}$, and which is known to be an automorphism of the $\mathbb{F}_q$-algebra $\mathbb{F}_q^{rm \times rm}$. Therefore, $\mathcal{A} = C_{\boldsymbol{P}}(\mathbb{F}_q[\boldsymbol{J}_r])$ inherits the field structure of $\mathbb{F}_q[\boldsymbol{J}_r]$, from which we conclude $\mathcal{A} \simeq \mathbb{F}_{q^m}$. □

Conjugation by the matrix $\boldsymbol{P}$ defines an isomorphism from $\mathbb{F}_q[\boldsymbol{J}_r]$ to $\mathcal{A}$. Even if we know both $\mathcal{A}$ and $\boldsymbol{J}_r$, we still do not have access to $\boldsymbol{P}$ nor its conjugation map, and not even to the restriction of the latter to $\mathbb{F}_q[\boldsymbol{J}_r]$. What we can do, however, is draw $\boldsymbol{A} \in \mathcal{A}$ uniformly at random until we get a generator of $\mathcal{A}$, *i.e.* an element of degree m. There should not be many trials necessary to get such a matrix $\boldsymbol{A}$. Indeed, it suffices to find a generator of the multiplicative group $\mathcal{A}^\times$, which has the following proportion in $\mathcal{A}$:

$$\pi = \prod_p \left(1 - \frac{1}{p}\right),$$

where the product is taken over all prime divisors p of $q^m - 1$. The probability to need more than t trials to get a generator is thus $(1-\pi)^t$, which tends towards zero exponentially fast.

Let $\Pi_{\boldsymbol{A}}$ be the minimal polynomial of such a matrix $\boldsymbol{A}$ over $\mathbb{F}_q$. This polynomial is irreducible of degree m over $\mathbb{F}_q$. Since $\mathbb{F}_{q^m}/\mathbb{F}_q$ is Galois, it splits into linear factors over $\mathbb{F}_{q^m}$:

$$\Pi_{\boldsymbol{A}} = \prod_{j=0}^{m-1} (X - \zeta^{q^j}),$$

where $\zeta \in \mathbb{F}_{q^m}$ is therefore a primitive element. As such, there exists some polynomial $f \in \mathbb{F}_q[X]$ of degree at most $m-1$ such that $f(\zeta) = \alpha$. Applying f on $\boldsymbol{A}$, we get a matrix with the same minimal polynomial as $\boldsymbol{J}_r$, which enables us to assume that $\Pi_{\boldsymbol{A}} = \Pi_\alpha$ in the following.

Lemma 5. *There exists an integer* $0 \leq j < m$ *such that* $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1} = \boldsymbol{A}^{q^j}$.

Proof. The conjugation map $C_{\boldsymbol{P}}$ preserves minimal polynomials, therefore $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}$ has the same minimal polynomial as $\boldsymbol{J}_r$, which is also that of $\boldsymbol{A}$. As a result, $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}$ is a Galois conjugate of $\boldsymbol{A}$, *i.e.* of the form $\boldsymbol{A}^{q^j}$ for some j. □

On the other hand, one can compute some matrix $\boldsymbol{Q}$ satisfying $\boldsymbol{J}_r = \boldsymbol{Q}\boldsymbol{A}\boldsymbol{Q}^{-1}$, the existence of which is proven below.

Lemma 6. *There exists* $\boldsymbol{Q} \in \mathbf{GL}_{rm}(\mathbb{F}_q)$ *such that* $\boldsymbol{J}_r = \boldsymbol{Q}\boldsymbol{A}\boldsymbol{Q}^{-1}$.

Proof. The two matrices share the same *irreducible* minimal polynomial, which implies that their Jordan normal form is the same. They are therefore similar over $\mathbb{F}_{q^m}$. As both of them have coefficients in $\mathbb{F}_q$, they are in fact similar over $\mathbb{F}_q$. □

The matrix $\boldsymbol{Q}$ of the previous lemma is exactly the one that we were looking for, as stated below.

Theorem 5. *One can compute $\boldsymbol{Q} \in \mathbf{GL}_{rm}(\mathbb{F}_q)$ such that $\boldsymbol{QP} \in \mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$.*

Proof. Let $\boldsymbol{Q}$ be the matrix of Lemma 6. From Lemma 5 and 6, we get

$$\begin{cases} \boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1} = \boldsymbol{A}^{q^j} \\ \boldsymbol{J}_r = \boldsymbol{Q}\boldsymbol{A}\boldsymbol{Q}^{-1}, \end{cases}$$

from which we get $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1} = \boldsymbol{Q}^{-1}\boldsymbol{J}_r^{q^j}\boldsymbol{Q}$, or equivalently $(\boldsymbol{QP})\boldsymbol{J}_r(\boldsymbol{QP})^{-1} = \boldsymbol{J}_r^{q^j}$. By Theorem 3, this means $\boldsymbol{QP} \in \mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$. □

It only remains to explain why this solves our problem.

Proposition 14. *Let $\boldsymbol{G}' = \Psi_\alpha^{-1}(\boldsymbol{Q}\boldsymbol{H}_{\mathrm{pub}})$. Then $\boldsymbol{G}'$ is a generator matrix of $\mathbf{GRS}(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$.*

Proof. As $\boldsymbol{QP} \in \mathscr{G}(\mathbb{F}_{q^m}/\mathbb{F}_q; r)$, it preserves Weil restrictions. More precisely, there is some $\boldsymbol{B} \in \mathbf{GL}_r(\mathbb{F}_{q^m})$ such that $\boldsymbol{Q} \cdot V_{\mathrm{pub}} = \boldsymbol{QP} \cdot V_{\mathrm{sec}}$ is the Weil restriction $\boldsymbol{B} \cdot \mathcal{Y}^{q^j}$, where $\mathcal{Y}$ is the geometric quadratic hull of $\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y})$. This means that the columns of $\boldsymbol{G}'$ are points of $\boldsymbol{B} \cdot \mathcal{Y}^{q^j}$. In other words, there exist polynomials $f_1, \dots, f_r \in \mathbb{F}_{q^m}[X]$ of degree at most $r-1$ such that

$$\boldsymbol{G}' = \begin{pmatrix} y_1^{q^j} f_1(x_1^{q^j}) & \dots & y_n^{q^j} f_1(x_n^{q^j}) \\ \vdots & \ddots & \vdots \\ y_1^{q^j} f_r(x_1^{q^j}) & \dots & y_n^{q^j} f_r(x_n^{q^j}) \end{pmatrix},$$

which means that the row space of $\boldsymbol{G}'$ is a subspace of $\mathbf{GRS}(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$. Since $\boldsymbol{Q}\boldsymbol{H}_{\mathrm{pub}}$ has rank rm, $\boldsymbol{G}'$ has rank r and is therefore a generator matrix of $\mathbf{GRS}(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$. □

The Sidelnikov-Shestakov attack then suffices to recover a support $\boldsymbol{x}'$ and a multiplier $\boldsymbol{y}'$ in $O(n^\omega)$ operations in $\mathbb{F}_{q^m}$. The whole algorithm is detailed below.

Algorithm 2 Recovering a support $\boldsymbol{x}'$ and a multiplier $\boldsymbol{y}'$ for $\mathscr{C}$

Input: $\boldsymbol{H}_{\mathrm{pub}}$ the public parity-check matrix of $\mathscr{C}$
Output: $\boldsymbol{x}', \boldsymbol{y}'$ such that $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}', \boldsymbol{y}')$.
Compute $\mathcal{A}$ using Algorithm 1
Compute $\boldsymbol{A} \in \mathcal{A}$ such that $\Pi_{\boldsymbol{A}} = \Pi_\alpha$
Compute $\boldsymbol{Q} \in \mathbf{GL}_{rm}(\mathbb{F}_q)$ such that $\boldsymbol{J}_r = \boldsymbol{Q}\boldsymbol{A}\boldsymbol{Q}^{-1}$
Compute $\boldsymbol{G}' = \Psi_\alpha^{-1}(\boldsymbol{Q}\boldsymbol{H}_{\mathrm{pub}})$ and let $\mathscr{D} = \{\boldsymbol{m}\boldsymbol{G}' \mid \boldsymbol{m} \in \mathbb{F}_{q^m}^r\}$
Apply [SS92] on $\mathscr{D}$ to get $\boldsymbol{x}', \boldsymbol{y}'$ such that $\mathscr{D} = \mathbf{GRS}_r(\boldsymbol{x}', \boldsymbol{y}')$
Return $\boldsymbol{x}', \boldsymbol{y}'$.

Theorem 6. *Provided that $m = O(\log r)$, Algorithm 2 returns a support $\boldsymbol{x}'$ and a multiplier $\boldsymbol{y}'$ such that $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}', \boldsymbol{y}')$ at a cost of $O(rn^\omega)$ operations in $\mathbb{F}_q$.*

Proof. Firstly, let us prove that $\boldsymbol{x}', \boldsymbol{y}'$ returned by Algorithm 2 are indeed valid support and multiplier. By Proposition 14, we have

$$\mathbf{GRS}_r(\boldsymbol{x}', \boldsymbol{y}') = \mathbf{GRS}(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$$

for some integer $0 \leq j < m$. The GRS codes generated by $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{x}', \boldsymbol{y}'$ respectively are therefore equal up to Galois conjugation, the latter being erased by the trace map. As a consequence,

the two GRS codes have the same trace codes. By duality, $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{x}', \boldsymbol{y}'$ generate the same alternant code.

Let us now derive the complexity of Algorithm 2. Step 3 requires $O(rn^\omega)$ operations in $\mathbb{F}_q$ by Theorem 4. Step 4 requires computing matrices $\boldsymbol{A} \in \mathcal{A}$ at random $O(1)$ times, then computing the minimal polynomial and checking its degree. Computing the minimal polynomial of $\boldsymbol{A}$ requires $O((rm)^\omega)$ operations in $\mathbb{F}_q$, so Step 4 is negligible. Computing the similarity matrix $\boldsymbol{Q}$ requires computing the Jordan normal form of $\boldsymbol{A}$ and checking whether it is equal to that of $\boldsymbol{J}_r$ (which can be precomputed). This step requires $O((rm)^\omega)$ operations (possibly in $\mathbb{F}_{q^m}$) and is again negligible. The only remaining costly operation is Step 7 which is known to require $O(n^\omega)$ operations in $\mathbb{F}_{q^m}$, which boils down to $O(mn^\omega)$ operations on $\mathbb{F}_q$. Since $m = O(\log r)$ — which is the natural asymptotic regime in McEliece cryptosystem — we conclude that the overall complexity is bounded by that of Algorithm 1. □

We provide a `SageMath` implementation of our attack, which is available here.

4.2. **Case $r > q$.** The attack described in the previous section requires the alternant code to be generic, square-distinguishable, and of degree $r \leq q$. If we run the exact same algorithm with a generic square-distinguishable alternant code of degree $r > q$ in input, then it turns out that the algorithm does return valid support $\boldsymbol{x}'$ and multiplier $\boldsymbol{y}'$. Although we will not provide a proof of this, we will try to give a partial explanation. To this end we introduce two results.

Theorem 7 (Weil's theorem)**.** *Let $I \subset \boldsymbol{R}$ be an ideal and $J = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I) \subset \boldsymbol{S}$, where $\boldsymbol{R}$ and $\boldsymbol{S}$ are the polynomial rings defined in Section 3. There exists an isomorphism of graded $\mathbb{F}_{q^m}$-algebras*

$$(\boldsymbol{S}/J) \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} \simeq \bigotimes_{j=0}^{m-1} \boldsymbol{R}/I^{q^j}, \tag{12}$$

where $I^{q^j} = \{f^{(q^j)} \mid f \in I\}$, the notation $f^{(q^j)}$ referring to f where the automorphism θ^j has been applied on the coefficients — the degree is preserved.

Proof. This result is [CCG23, Theorem 2.8] in the case of finite fields. □

This means that we can work equivalently with the Weil restriction or the ideal obtained by extension of scalars. Note that this theorem somehow looks like the following result from coding theory.

Proposition 15 ([BMT24])**.** *Let $\mathscr{C} \subset \mathbb{F}_{q^m}^n$ be a proper code. Then*

$$\mathrm{Tr}\left(\mathscr{C}\right)_{\mathbb{F}_{q^m}} = \bigoplus_{j=0}^{m-1} \mathscr{C}^{q^j},$$

where $\mathrm{Tr}\left(\mathscr{C}\right)_{\mathbb{F}_{q^m}}$ denotes the $\mathbb{F}_{q^m}$-linear code spanned by $\mathrm{Tr}\left(\mathscr{C}\right)$.

To understand why Algorithm 2 still works in the case $r > q$, we can therefore study the quadratic hull of

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

A natural choice for the generator matrix of this code is the matrix whose columns consist of the following list:

$$\begin{aligned}\mathcal{B} = \{&\boldsymbol{y}, \boldsymbol{x}\boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1}\boldsymbol{y}\\ &\boldsymbol{y}^q, (\boldsymbol{x}\boldsymbol{y})^q, \ldots, (\boldsymbol{x}^{r-1}\boldsymbol{y})^q\\ &\ldots\\ &\boldsymbol{y}^{q^{m-1}}, (\boldsymbol{x}\boldsymbol{y})^{q^{m-1}}, \ldots, (\boldsymbol{x}^{r-1}\boldsymbol{y})^{q^{m-1}}\},\end{aligned}$$

which was first introduced in [CMT23] and referred to as *the canonical basis*. For more convenience, we will analyze the quadratic hull of $\mathscr{C}_{\mathbb{F}_{q^m}}$ in the polynomial ring

$$\boldsymbol{R} = \mathbb{F}_{q^m}[X_{i,u} \mid 0 \leq i < r,\ 0 \leq u < m],$$

the evaluation map sending $X_{i,u}$ onto $(\boldsymbol{x}^i \star \boldsymbol{y})^{q^u}$. As recalled in [CMT23], the work that was done in [FGO+11] shows that, heuristically, the algebraic quadratic hull related to this basis $\mathcal{B}$ is generated by the equations of the form

$$f_{i,j,k,\ell,u,v} = X_{i,u}X_{j,v} - X_{k,u}X_{\ell,v},$$

for all $0 \leq u, v < m$ and $0 \leq i, j, k, \ell < r$ such that $iq^u + jq^v = kq^u + \ell q^v$. Denoting by $\mathcal{Y}$ the affine cone over the rational normal curve, we see that these equations define a subvariety of

$$\mathcal{Y} \times \mathcal{Y}^q \times \ldots \times \mathcal{Y}^{q^{m-1}},$$

which is the variety obtained by extension of scalars of the quadratic hull of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ by Weil's theorem. We see that the defining ideal of this product variety is generated by the $f_{i,j,k,\ell,u,v}$'s with $u = v$. Furthermore, it is the expected quadratic hull of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp_{\mathbb{F}_{q^m}}$ when $r \leq q$, *i.e.* when we have Weil-properness. On the other hand, the crossed equations $f_{i,j,k,\ell,u,v}$ where $u \neq v$ might be interpreted as field equations. We indeed see the following experimentally.

Heuristic 3. *Let $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y}))$. When $r > q$, the algebraic quadratic hull of $\boldsymbol{H}_{\text{sec}}$ is the Weil restriction of $\langle I_2(\boldsymbol{V}_r(\boldsymbol{x}, \boldsymbol{y})) \cup \{X_i^{q^m} - X_i \mid 0 \leq i < r\}\rangle$.*

The variety of which the algebraic quadratic hull of $\boldsymbol{H}_{\text{pub}}$ is the Weil restriction is thus the one-dimensional variety given by the lines passing through the points of the cone over the rational normal curve. The Weil restriction of a line is an m-dimensional vector-space, and therefore the arguments of Heuristic 2 still hold in this case. In fact, Weil-properness is not a necessary condition for the attack to succeed. What we need is to have a quadratic hull presenting some algebraic structure over $\mathbb{F}_{q^m}$, so that we get access to sufficiently many vector spaces that are stabilized by $\boldsymbol{P}\boldsymbol{J}_r\boldsymbol{P}^{-1}$. All in all, our attack breaks McEliece scheme with generic square-distinguishable alternant codes, regardless of how q compares to r. Our `SageMath` implementation generates such a generic alternant code, and recovers a support and a multiplier as soon as we are in the square-distinguishable regime.

4.3. **What about Goppa codes ?** In both [ABC+22] and [McE78], McEliece cryptosystem is described with the family of binary Goppa codes.

Definition 11 (Goppa code)**.** *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ be a support and $\Gamma \in \mathbb{F}_{q^m}[X]$ be a polynomial of degree r such that $\Gamma(x_i) \neq 0$ for all i. The Goppa code of support $\boldsymbol{x}$ and Goppa polynomial Γ is defined by*

$$\mathscr{G}(\boldsymbol{x}, \Gamma) = \mathscr{A}_r\left(\boldsymbol{x}, \Gamma(\boldsymbol{x})^{-1}\right).$$

A result analogous to Theorem 2 exists also for Goppa codes.

Theorem 8 ([MT21]). *Let $\mathscr{C} = \mathscr{G}(\boldsymbol{x}, \Gamma)^\perp$ be a proper dual Goppa code. If $r < q-1$, then*

$$\dim I_2(\mathscr{C}) \geq m\binom{r-1}{2}.$$

When $r \geq q-1$, we have the following bound:

$$\dim I_2(\mathscr{C}) \geq \frac{m}{2} r\left((2e_{\mathscr{G}}+1)r - 2(q-1)q^{e_{\mathscr{G}}-1} - 1\right), \tag{13}$$

where $e_{\mathscr{G}} = \left\lceil \log_q\left(\frac{r}{(q-1)^2}\right)\right\rceil + 1.$

Like in the alternant case, these bounds are tight in the following sense.

Heuristic 4 ([FGO+11]). *As soon as the right-hand side of the inequalities of Theorem 8 exceed $\binom{rm+1}{2} - n$, these inequalities are equalities.*

As a direct consequence, we see that Goppa codes essentially behave like alternant codes when $r < q-1$, which means that Algorithm 2 returns valid support and multiplier in such a case. When $r \geq q-1$ however, even the previous argument of Heuristic 3 may not apply. This is indeed what we see in practice.

Heuristic 5. *Let $\boldsymbol{H}$ be any parity-check matrix of a degree-r Goppa code $\mathscr{G}(\boldsymbol{x}, \Gamma)$. If $r \geq q-1$, then the dimension of the geometric quadratic hull of $\boldsymbol{H}$ is equal to 1.*

This is unfortunate, as no algebraic structure over $\mathbb{F}_{q^m}$ is visible in the quadratic hull of such Goppa codes. In particular, binary Goppa codes, be they square-distinguishable or not, are again out of reach. We present in the following table a comparison between our attack and the current state of the art.

Target	Paper	$r(\geq 3)$	q	complexity
generic square dist. alternant	[BMT24]	any	$q \in \{2,3\}$	rn^ω
generic square dist. alternant	[CMT23]	$< q+1$	any	$n^{\omega+2}$
generic square dist. alternant	[CMT23] + [BMT24]	any	any	$n^{\omega+2}$
generic square dist. alternant	this paper	any	any	rn^ω
square dist. Goppa	[CMT23]	$< q-1$	any	$n^{\omega+2}$
square dist. Goppa	this paper	$< q-1$	any	rn^ω

FIGURE 1. Comparison

4.4. **Generalization to Algebraic-Geometry codes.** Algebraic-Geometry (AG) codes, first introduced by Goppa in [Gop81], are a natural generalization of GRS codes. They have been proposed by Janwa and Moreno in [JM96] for McEliece cryptosystem, but this proposition was eventually proven insecure in [CMCP14]. However, the security of McEliece with subfield subcodes of AG codes, often referred to as SSAG codes, remains unknown in general. In this last subsection, we aim to show that our algorithm can be applied to attack SSAG codes as well, provided that certain conditions are met.

We first need to recall some notions. In the following, $\mathcal{X}$ denotes a smooth, projective and absolutely irreducible algebraic curve defined over $\mathbb{F}_{q^m}$. We denote by g the genus of $\mathcal{X}$. We also denote by $\mathbb{F}_{q^m}(\mathcal{X})$ the function field of $\mathcal{X}$ with field of constants $\mathbb{F}_{q^m}$. Recall that $\mathrm{Div}(\mathcal{X})$ stands for the divisor group of $\mathcal{X}$, *i.e.* the free abelian group generated by the points of $\mathcal{X}$ over the algebraic closure of $\mathbb{F}_{q^m}$. A divisor $D \in \mathrm{Div}(\mathcal{X})$ therefore takes the form

$$D = \sum_{P \in \mathcal{X}} n_P \cdot (P),$$

where all but finitely many n_P's are zero. We write

$$\mathrm{supp}(D) = \{P \in \mathcal{X} \mid n_P \neq 0\},$$

and call it the support of D. The degree of D is defined by $\deg D = \sum_{P\in\mathcal{X}} n_P \in \mathbb{Z}$. We say that D is an *effective* divisor, and write $D \geq 0$, when $\forall P \in \mathcal{X},\ n_P \geq 0$. The divisor D is said to be defined over $\mathbb{F}_{q^m}$ when

$$D^{q^m} \stackrel{\text{def}}{=} \sum_{P\in\mathcal{X}} n_P(P^{q^m}) = D,$$

where P^{q^m} is the point of $\mathcal{X}$ with all coordinates being those of P to the power q^m — this is indeed a point of $\mathcal{X}$ as $\mathcal{X}$ is defined over $\mathbb{F}_{q^m}$. The subgroup of divisors defined over $\mathbb{F}_{q^m}$ will be referred to as $\mathrm{Div}_{\mathbb{F}_{q^m}}(\mathcal{X})$. Note that the points of a divisor defined over $\mathbb{F}_{q^m}$ need not have their coordinates in $\mathbb{F}_{q^m}$. This remark is particularly relevant when we look at principal divisors, which are divisors associated to nonzero rational functions in the following manner. For $f \in \mathbb{F}_{q^m}(\mathcal{X})^\times$ such a nonzero rational function and $P \in \mathcal{X}$, we write $\mathrm{ord}_P(f)$ the valuation of f at P. The principal divisor associated to f is defined by

$$(f) = \sum_{P\in\mathcal{X}} \mathrm{ord}_P(f) \cdot (P).$$

Although the zeros and poles of f may not lie in $\mathcal{X}(\mathbb{F}_{q^m})$, the whole divisor (f) is globally invariant under the Frobenius automorphism and is therefore defined over $\mathbb{F}_{q^m}$. Furthermore, the following holds.

Theorem 9 ([Sil09], Proposition 3.1 (b))**.** *For all $f \in \mathbb{F}_{q^m}(\mathcal{X})^\times$, we have $\deg(f) = 0$.*

Finally, we denote by $\mathcal{L}(D)$ the Riemann-Roch space of D, which is defined by

$$\mathcal{L}(D) = \{f \in \mathbb{F}_{q^m}(\mathcal{X})^\times \mid (f) + D \geq 0\} \cup \{0\}.$$

As stated by the famous Riemann-Roch theorem, this space is a finite dimensional $\mathbb{F}_{q^m}$-vector space whose dimension $\ell(D)$ is related to the degree of D. We give the special case of Riemann-Roch theorem for divisors of sufficiently high degree.

Theorem 10 (Riemann-Roch)**.** *If $\deg D > 2g - 2$, then $\ell(D) = \deg D + 1 - g$.*

Proof. See [Sil09, Corollary 5.5 (c)]. □

We have introduced all the necessary material to define algebraic-geometry codes.

Definition 12. *Let $\mathcal{P} = (P_1, \ldots, P_n) \in \mathcal{X}(\mathbb{F}_{q^m})^n$ be a tuple of pairwise distinct $\mathbb{F}_{q^m}$-rational points of $\mathcal{X}$, and let $D \in \mathrm{Div}_{\mathbb{F}_{q^m}}(\mathcal{X})$ be such that $\mathrm{supp}(D) \cap \{P_1, \ldots, P_n\} = \varnothing$. The algebraic-geometry code of support $\mathcal{P}$ and divisor D is defined by*

$$\mathscr{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(D)\}.$$

Remark 11. When $\mathcal{X} = \mathbb{P}^1$ and $D = (r+1)P_\infty$ where $P_\infty = (1:0)$, the above definition gives Reed-Solomon codes. See [Sti09, Proposition 2.3.5] for further details.

Let $r = \ell(D) - 1$ and $(f_0, \ldots, f_r)$ be a basis of $\mathcal{L}(D)$. Since $\mathcal{X}$ is a smooth curve, the rational function $\phi_D = (f_0, \ldots, f_r)$ defines a morphism $\mathcal{X} \to \mathbb{P}^r$. If $\deg D > 2g$, then ϕ_D defines an isomorphism between $\mathcal{X}$ and $\mathcal{Y} = \phi_D(\mathcal{X})$. Moreover, like in the case of GRS codes, the following matrix

$$V(\mathcal{P}, \phi_D) = \begin{pmatrix} f_0(P_1) & f_0(P_2) & \ldots & f_0(P_n) \\ f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_r(P_1) & f_r(P_2) & \ldots & f_r(P_n) \end{pmatrix}$$

is a generator matrix of $\mathscr{C} \overset{\text{def}}{=} \mathscr{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D)$, and each column defines a point on $\mathcal{Y}$. From the work of [MMP14], we know that if $\deg D > 2g+1$, then the quadratic hull of this matrix is equal to $\mathcal{Y}$, which implies that the quadratic hull of $\mathrm{Tr}\,(\mathscr{C})$ is a subvariety of $\Psi_\alpha(\mathcal{Y})$. In order to adapt our attack to SSAG codes, we need to understand when such a code is Weil-proper. Extensive computations in our `SageMath` implementation available here have led us to the following quite natural conjecture. We have investigated Weil-properness of *generic* one point AG codes, *i.e.* codes of the form

$$\mathscr{C} = \{\boldsymbol{c} \star \boldsymbol{y} \mid \boldsymbol{c} \in \mathscr{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, r \cdot (P_\infty))\} \tag{14}$$

where $\boldsymbol{y} \in (\mathbb{F}_{q^m}^\times)^n$ is chosen uniformly at random.

Heuristic 6 (Weil-properness of one point generic AG codes)**.** *Let $\mathscr{D} = \mathrm{Tr}\,(\mathscr{C})$ where $\mathscr{C}$ is as in Equation (14). We make the two following assumptions:*

(i) $2g + 2 \leq r \leq q$*;*

(ii) $n > \binom{(r+1-g)m+1}{2} - m \dim_{\mathbb{F}_{q^m}} I_2(\mathscr{C})$.

Then $\mathscr{D}$ is Weil-proper.

In such a case, one can compute the tangent spaces of the quadratic hull of the public generator matrix of $\mathscr{D}$. The assumption $2g + 2 \leq r$ ensures that the quadratic hull of $\mathscr{C}$ is a projective variety of dimension 1, therefore the underlying ideal has dimension 2, which means that the quadratic hull of $\mathscr{D}$ has dimension $2m$. All in all, Algorithm 2 eventually retrieves a generator matrix of $\mathscr{C}$, and then [CMCP14] recovers an efficient decoding algorithm. This class of AG codes is therefore vulnerable to our attack.

Like in the case of alternant codes, the attack still succeeds when we no longer have the assumption $r \leq q$.

Heuristic 7. *Let $\boldsymbol{H}_{\text{sec}} = \Psi_\alpha(\boldsymbol{G})$ be the secret generator matrix of $\mathscr{D}$, where $\boldsymbol{G}$ is a generator matrix of $\mathscr{C}$. We still assume $2g + 2 \leq r$, as well as (ii) of the previous heuristic, but now we also assume $r > q$. Then the algebraic quadratic hull of $\boldsymbol{H}_{\text{sec}}$ is equal to the Weil restriction of $\langle I_2(\boldsymbol{G}) \cup \{X_i^{q^m} - X_i \mid 0 \leq i \leq r - g\}\rangle$.*

Our `SageMath` implementation also provides Algorithm 2 in the case of generic one point AG codes, regardless of how r compares to q.

5. Conclusion and open problems

The geometric analysis of linear codes using the quadratic hull seems to be a prolific approach. Using Weil restriction, we have been able to write an algorithm that recovers the structure of a trace code, provided that the original code has a nontrivial quadratic hull and assuming Weil-properness. This notion turns out to be more powerful than what we actually need for our attack to succeed. We eventually described a polynomial-time attack against the McEliece cryptosystem instantiated with generic alternant codes, generic one-point SSAG codes, or even Goppa codes of sufficiently low degree.

For future work, better understanding what happens when the degree of the alternant code gives rise to field equations even in the high-rate regime will be crucial to see whether we can adapt our framework to the case of binary Goppa codes. It is also still unclear whether other families of codes are vulnerable to our attack.

Acknowledgements

This work was in part funded by the *Direction Générale de l'Armement* (DGA). The author would also like to thank Jean-Pierre Tillich for his advice and feedback, as well as Alain Couvreur for his insightful discussions.

References

[AAB+17] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, and Gilles Zémor. HQC, November 2017. NIST Round 1 submission for Post-Quantum Cryptography.

[AAB+22] Carlos Aguilar Melchor, Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim Güneysu, Rafael Misoczki, Edoardo Persichetti, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, and Gilles Zémor. BIKE. Round 4 Submission to the NIST Post-Quantum Cryptography Call, v. 5.1, October 2022.

[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.

[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.

[CCG23] Alessio Caminata, Michela Ceria, and Elisa Gorla. The complexity of solving weil restriction systems. *Journal of Algebra*, 621:116–133, 2023.

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

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

[CGG+13] Alain Couvreur, Philippe Gaborit, Valérie Gautier, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes. In *International Workshop on Coding and Cryptography - WCC 2013*, pages 181–193, Bergen, Norway, April 2013.

[CMCP14] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2014*, pages 1446–1450, June 2014.

[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.

[Del75] Philippe Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 21(5):575–576, 1975.

[Eis06] D. Eisenbud. *The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra*. Graduate Texts in Mathematics. Springer New York, 2006.

[FGO+10] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high rate McEliece cryptosystems. IACR Cryptology ePrint Archive, Report2010/331, 2010. http://eprint.iacr.org/.

[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.

[GH78] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Pure and Applied Mathematics. A Wiley-Interscience Publication. John Wiley & Sons, New York, 1978.

[Gop81] Valerii D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981. In Russian.

[JM96] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Des. Codes Cryptogr.*, 8(3):293–307, 1996.

[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.

[LMT25] Axel Lemoine, Rocco Mora, and Jean-Pierre Tillich. Understanding the new distinguisher of alternant codes at degree 2. Cryptology ePrint Archive, Paper 2025/531, 2025.

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

[MMP14] Irene Márquez–Corbella, Edgar Martínez–Moro, and Ruud Pellikaan. On the unique representation of very strong algebraic geometry codes. *Des. Codes Cryptogr.*, 70(1–2):215–230, 2014.

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

[MT21] Rocco Mora and Jean-Pierre Tillich. On the dimension and structure of the square of the dual of a Goppa code. preprint, 2021.

[Nie86] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[Ran19] Hugues Randriambololona. The quadratic hull of a code and the geometric view on multiplication algorithms. *CoRR*, abs/1912.06627, 2019.

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

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2009.

[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.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[WB86] Lloyd R Welch and Elwyn R Berlekamp. Error correction for algebraic block codes, December 1986. US Patent 4,633,470.

6. Appendix

6.1. **Graded free resolutions.** The proof of Lemma 1 involves the notion of minimal graded free resolution of finitely generated graded modules over polynomial rings. Let us define

$$\boldsymbol{R} = \mathbb{F}_{q^m}[X_0, \dots, X_{r-1}] \text{ and } \boldsymbol{S} = \mathbb{F}_q[x_{i,j} \mid 0 \leq i < r,\ 0 \leq j < m].$$

Both $\boldsymbol{R}$ and $\boldsymbol{S}$ have a structure of graded rings. More precisely, we can write

$$\boldsymbol{R} = \bigoplus_{d\in\mathbb{N}} \boldsymbol{R}_d \text{ and } \boldsymbol{S} = \bigoplus_{d\in\mathbb{N}} \boldsymbol{S}_d,$$

where $\boldsymbol{R}_d$ and $\boldsymbol{S}_d$ refer to the vector space spanned by monomials of degree d, and we have $\boldsymbol{R}_a\boldsymbol{R}_b \subset \boldsymbol{R}_{a+b}$ for all $a, b \in \mathbb{N}$ — and likewise for $\boldsymbol{S}$. In the same manner, if M is a module over $\boldsymbol{R}$, we say that M is a graded $\boldsymbol{R}$-module if one can write $M = \bigoplus_{d\in\mathbb{Z}} M_d$ and if

$$\forall a \in \mathbb{N},\ \forall b \in \mathbb{Z},\ \boldsymbol{R}_a M_b \subset M_{a+b}.$$

Definition 13. *Let M be a finitely generated $\boldsymbol{R}$-module. A free resolution of M is an exact sequence*

$$\dots \to \mathbb{F}_{i+1} \to \mathbb{F}_i \to \dots \to \mathbb{F}_0 \to M \to 0,$$

where each $\mathbb{F}_i$ is a free $\boldsymbol{R}$-module. We write $\mathbb{F}_\bullet \to M \to 0$ for conciseness. If moreover each $\mathbb{F}_i$ is a graded free $\boldsymbol{R}$-module, and if the maps $\mathbb{F}_{i+1} \to \mathbb{F}_i$ and $\mathbb{F}_0 \to M$ preserve the degree, then we say that $\mathbb{F}_\bullet \to M \to 0$ is a graded free resolution of M.

6.2. **Minimal resolutions.** Let M be a finitely generated $\boldsymbol{R}$-module. If $(x_1, \dots, x_n) \in M^n$ is a minimal set of generators of M, then we have a natural map

$$\mathbb{F}_0 = \boldsymbol{R}^n \twoheadrightarrow M.$$

One can repeat this process inductively by setting $M_1 = \ker(\mathbb{F}_0 \to M)$ and let $\mathbb{F}_1$ be the free module over a minimal set of generators of M_1, and so on. This is the notion of minimality of a free resolution, that we define more formally below.

Definition 14. *Let $\mathbb{F}_\bullet \to M \to 0$ be a free resolution of the finitely generated graded $\boldsymbol{R}$-module M. Define the sequence of $\boldsymbol{R}$-modules $(M_i)_{i\in\mathbb{N}}$ by $M_0 = M$ and $M_{i+1} = \ker(F_i \to M_i)$. We say that the resolution is minimal if for any $i \in \mathbb{N}$, the cardinality of a minimal set of generators of M_i equals the rank of the free module $\mathbb{F}_i$.*

If N is any graded $\boldsymbol{R}$-module, then for any integer j we denote by $N(j)$ the graded $\boldsymbol{R}$-module whose degree d component is defined by the degree $d + j$ component of N:

$$\forall d \in \mathbb{Z},\ N(j)_d = N_{d+j}.$$

We now assume that M is a graded $\boldsymbol{R}$-module. By taking into account the degree of the elements of a minimal set of generators of M, we get a degree-preserving natural surjective map

$$\mathbb{F}_0 = \bigoplus_{j\in\mathbb{N}} \boldsymbol{R}(-j)^{\beta_{0,j}} \twoheadrightarrow M,$$

where $\beta_{0,j}$ is therefore the number of elements of degree j in a minimal set of generators of M. Repeating this construction inductively, we obtain a minimal graded free resolution of M. The fact that the numbers of generators of a certain degree in a minimal set of generators does not depend on the choice of generators is a consequence of the following result.

Theorem 11 ([Eis06], Theorem 1.6)**.** *If $\mathbb{F}_\bullet$ and $\mathbb{G}_\bullet$ are minimal graded free resolutions of M, then there is a graded isomorphism of complexes $\mathbb{F}_\bullet \to \mathbb{G}_\bullet$ inducing the identity map on M.*

We can therefore talk about *the* minimal graded free resolution of the finitely generated graded $\boldsymbol{R}$-module M. For any integer $j \in \mathbb{N}$, we can write

$$\mathbb{F}_i = \bigoplus_{j \in \mathbb{N}} \boldsymbol{R}(-j)^{\beta_{i,j}},$$

and the $\beta_{i,j} \in \mathbb{N}$ are called the *graded Betti numbers* of M.

6.3. **Minimal set of generators of a Weil restriction.** A homogeneous ideal $I \subset \boldsymbol{R}$ is a graded $\boldsymbol{R}$-module. Since $\boldsymbol{R}$ is a noetherian ring by Hilbert's basis theorem, we know that I is finitely generated. As a result we can apply the framework that we introduced above on the finitely generated graded module $\boldsymbol{R}/I$. Furthermore, if $J = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I)$, then J is also a finitely generated graded $\boldsymbol{S}$-module, and as such we can also consider the minimal graded free resolution of $\boldsymbol{S}/J$. The Betti numbers of $\boldsymbol{R}/I$ and $\boldsymbol{S}/J$ are related by the following formula.

Proposition 16. *Let $(\beta_{i,j})_{i,j}$ and $(\gamma_{i,j})_{i,j}$ be the graded Betti numbers of $\boldsymbol{R}/I$ and $\boldsymbol{S}/J$ respectively. Then for all i and j, we have*

$$\gamma_{i,j} = \sum_{\substack{i_1+\ldots+i_m=i \\ j_1+\ldots+j_m=j}} \prod_{s=1}^{m} \beta_{i_s,j_s}. \tag{15}$$

Proof. Let $\mathbb{F}_\bullet$ be a minimal graded free resolution of $\boldsymbol{R}/I$. By [CCG23, Theorem 3.3], we have a minimal graded free resolution

$$\mathbb{G}_\bullet \overset{\text{def}}{=} \mathbb{F}_\bullet^{\otimes m} \longrightarrow (\boldsymbol{S}/J) \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} \longrightarrow 0. \tag{16}$$

We thus have for all $i \in \mathbb{N}$,

$$\mathbb{G}_i = \bigoplus_{i_1+\ldots+i_m=i} \mathbb{F}_{i_1} \otimes \ldots \otimes \mathbb{F}_{i_m}.$$

Expanding each $\mathbb{F}_{i_s}$ as $\bigoplus_{j_s} \boldsymbol{R}(-j_s)^{\beta_{i_s,j_s}}$ gives

$$\begin{aligned}
\mathbb{G}_i &= \bigoplus_{i_1+\ldots+i_m=i} \bigotimes_{s=1}^{m} \left(\bigoplus_{j_s} \boldsymbol{R}(-j_s)^{\beta_{i_s,j_s}} \right) \\
&= \bigoplus_{i_1+\ldots+i_m=i} \bigoplus_{j_1,\ldots,j_m} \boldsymbol{R}(-j_1)^{\beta_{i_1,j_1}} \otimes \ldots \otimes \boldsymbol{R}(-j_m)^{\beta_{i_m,j_m}} \\
&= \bigoplus_{i_1+\ldots+i_m=i} \bigoplus_{j_1,\ldots,j_m} \boldsymbol{R}(-j_1-\ldots-j_m)^{\beta_{i_1,j_1} \times \ldots \times \beta_{i_m,j_m}}.
\end{aligned}$$

Since the map $\Phi : \boldsymbol{R} \to \boldsymbol{S} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ is an injective homomorphism of graded $\mathbb{F}_{q^m}$-algebras, we get that the Betti numbers of $\boldsymbol{S}/J$ and $(\boldsymbol{S}/J) \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ are the same. Identifying the component of degree j of $\mathbb{G}_i$ eventually gives the desired formula. □

Focusing on $i = 1$ gives the number of generators in a minimal set of generators of the ideals I and J respectively. The leads us to a proof of Lemma 1, that we recall below.

Lemma 1. *Let $I \subset \boldsymbol{R}$ be a homogeneous ideal. If $(f_1, \ldots, f_N)$ is a minimal set of generators for I, then the sequence $(\Phi_j(f_i))_{i,j}$ is a minimal set of generators of* $\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I)$.

Proof. Retaking the notations of Proposition 16, it suffices to show that

$$\forall j \in \mathbb{N},\ \gamma_{1,j} = m\beta_{1,j}.$$

Let $j \in \mathbb{N}$. In Equation (15), every index i_s must be equal to zero but one, which must be equal to one. As $\mathbb{F}_0 = \boldsymbol{R}$, we see that for each integer j_s, the Betti number β_{0,j_s} equals 1 if and only if

$j_s = 0$, and 0 otherwise. Therefore, in the product of Equation (15), we only have Betti numbers of the form $\beta_{0,0}$ and one of the form β_{1,j_s}, and that j_s must be equal to j. All in all, we get

$$\gamma_{1,j} = \sum_{s=1}^{m} \beta_{0,0} \times \ldots \times \underbrace{\beta_{1,j}}_{\text{position } s} \times \ldots \times \beta_{0,0} = m\beta_{1,j}$$

as required. □

Inria Paris, France

DGA, France
Email address: axel.lemoine@inria.fr