On the dimension and structure of the square of the dual of alternant codes and Goppa codes

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

[1] Inria, 2 rue Simone Iff, 75012 Paris, France
rocco.mora@inria.fr,jean-pierre.tillich@inria.fr
[2] Sorbonne Universités, UPMC Univ Paris 06

Abstract. The Goppa Code Distinguishing (GD) problem asks to distinguish efficiently a generator matrix of a Goppa code from a randomly drawn one. We revisit a distinguisher for alternant and Goppa codes through a new approach, namely by studying the dimension of square codes. We provide here a rigorous upper bound for the dimension of the square of the dual of an alternant or Goppa code, while the previous approach only provided algebraic explanations based on heuristics. Moreover, for Goppa codes, our proof extends to the non-binary case as well, thus providing an algebraic explanation for the distinguisher which was missing up to now. All the upper bounds are tight and match experimental evidence. Our work also introduces new algebraic results about products of trace codes in general and of dual of alternant and Goppa codes in particular, clarifying their square code structure. This might be of interest for cryptanalysis purposes.

1 Introduction

The McEliece scheme.

The McEliece encryption scheme [18], which dates back to 1978, is a code-based cryptosystem built upon the family of binary Goppa codes. It is equipped with very fast encryption and decryption algorithms and has very small ciphertexts. It is also widely viewed as a viable quantum safe cryptosystem, since the best quantum algorithm for breaking it [12] has exponential complexity and the corresponding exponent barely improves the exponent of the best classical algorithm [3] by about 40 percent. *Classic McEliece* [2] is currently the only code-based finalist at the third round of the NIST Post-Quantum Cryptography Standardization Process. This competition aims to replace classical public-key cryptography with quantum-secure alternatives and NIST has expressed the opinion that Classic McEliece could be ready for standardization at the end of the third round.

Over the years, the attempts to attack McEliece scheme moved in two main directions. One hand, we have *message-recovery attacks*. They consist in inverting the McEliece encryption without finding a trapdoor and make use of general decoding algorithms. Despite considerable improvements [22,4,16,1,17,3], all

these algorithms have exponential complexity. The parameters of McEliece-like schemes have then been intentionally chosen to thwart this attack, which is considered as the main threat to the scheme. Despite all these efforts, the original McEliece cryptosystem [18] based on binary Goppa codes remains, after more than forty years, unbroken, be it by a classical or a quantum computer. It is now the oldest public-key cryptosystem with this feature.

The other way to attack the cryptosystem is by seeking to recover the private key. For a long time it was widely believed that even a simpler task which is just to distinguish efficiently a generator matrix of a Goppa code from a randomly drawn generator matrix with non negligible probability was unfeasible. This is the so called *Goppa Code Distinguishing (GD) problem* as introduced in [6]. The nice feature of this problem is that it is possible to devise a security proof for the McEliece scheme based solely on the intractability of this problem and decoding a generic linear code [21]. The belief about GD problem hardness was basically justified by the fact that Goppa codes behave like random codes in many aspects.

A distinguisher for high rate.

However, this belief was severely questioned in [10,11] which gave a polynomial time algorithm that distinguishes between Goppa codes (or more generally alternant codes) and random ones from their generator matrices at least for very high rate codes. It is based on the kernel of a linear system related to an algebraic system encoding the key-recovery problem for McEliece cryptosystem. Indeed, it was shown to have an unexpectedly high dimension. This distinguisher was later on given another interpretation in [15], where it was proved that this dimension is related to the dimension of the square of the dual of the public code.

The algebraic explanations given in [11] do not represent however a rigorous proof of the dimension of the kernel sought, but they rely on heuristic considerations. Indeed, while a set of vectors is proposed as candidate for the kernel basis, its elements are neither proved to be independent nor a set of generators. Moreover, in the case of Goppa codes, even if a general formula for the dimension of the kernel was provided which matches the experimental evidence, an algebraic explanation was only provided in the case of binary Goppa codes with square free Goppa polynomials. This explanation crucially relies on the fact that binary Goppa codes are in this case also Goppa codes of a higher degree (with a Goppa polynomial being the square of the original polynomial). Clearly, this approach does not generalize to non binary Goppa codes.

Our contribution

In the present article, we revisit the distinguisher for random alternant codes and Goppa codes. We do so by exploiting the link given by [15]. Indeed we provide a rigorous upper bound on the dimension of the square code of the dual of an alternant or a Goppa code that coincides with the experiments. By using [15], this also gives a lower bound on the dimension of the kernel of the matrix considered in [11]. Together with results about the typical dimension

of the square of random codes [5], this provides the first rigorous analysis of the approach pioneered in [10], because the typical dimension of the square of a random code is way larger than this upper-bound on the dimension of the square of the dual of a Goppa or alternant code.

A distinguisher can sometimes be turned into an attack. In the code-based cryptography setting, this is for instance the case for GRS codes. The uncommon dimension of the square of a GRS code leads to a successful key-recovery for several proposed variants of McEliece cryptosystem built upon this family of codes for any rate [7]. Despite the strong relation between generalized Reed-Solomon codes and alternant codes, the same attacks cannot be carried over from the former to the latter, because of the additional subfield subcode structure. A similar idea has been successfully exploited for Wild Goppa codes though [8]. But in this case, the distinguisher is based on considerations of square of Goppa codes themselves, which only applies to a very restricted class of parameters. Indeed the attack can only work for extensions of degree $m = 2$ and there is no way to go beyond it, because for $m > 2$ the square code fills the whole space. In our case, our distinguisher is based on squaring the *dual* of a Goppa code (or an alternant code) and works for *any* field extension degree.

However, the fact that the dual of a Goppa code is the trace of a generalized Reed-Solomon code rather than the subfield subcode of a generalized Reed-Solomon code seems to complicate significantly the attempts to turn this distinguisher into an attack. But again, having now a much better algebraic (and rigorous) explanation of why the distinguisher works, together with new algebraic results about products involved in the square of the dual of the Goppa code gives a much better understanding of the square code structure. This is clearly desirable and needed if we want to mount a key recovery attack based on these square code considerations. The hope is that this will ultimately lead to being able to attack McEliece schemes based on very high rate Goppa codes. As explained earlier, this will still not threaten the codes used in the aforementioned NIST competition, but this would break the 20 years old signature scheme [6] that is based on very high rate Goppa codes.

2 Notation and prerequisites

In this section we fix notation used throughout the article. We also recall basic definitions, component-wise products, square codes and some algebraic codes derived from generalized Reed-Solomon codes.

Let $\mathbb{F}$ be a generic finite field, $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ the finite fields with q and q^m elements respectively, where q denotes a prime power, and m is a positive integer. Given $v_1, \ldots, v_k \in \mathbb{F}^n$, we denote with $\langle v_1, \ldots, v_k \rangle_{\mathbb{F}}$ the subspace of vectors in $\mathbb{F}^n$ spanned by $\{v_1, \ldots, v_k\}$. An $[n, k]$-code over $\mathbb{F}$ is a linear subspace of vectors in $\mathbb{F}^n$ of dimension k. The positive integer n is called the *code length*.

We will also use for a function f acting on $\mathbb{F}$ and a vector $x = (x_i)_{1 \leqslant i \leqslant n}$ in $\mathbb{F}^n$ by $f(x)$ the vector $(f(x_i))_{1 \leqslant i \leqslant n}$. A useful linear map from $\mathbb{F}_{q^m}$ to its subfield $\mathbb{F}_q$ is the *trace* operator $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined as $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = \sum_{i=0}^{m-1} x^{q^i}$.

The definition extends to vectors $x \in \mathbb{F}_{q^m}^n$ so that the trace acts component-wise $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x_1), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x_n))$.

2.1 Reed-Solomon, alternant and Goppa codes

We first recall the definitions of some well-known classes of algebraic codes.

Definition 1. *Let $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$ be a vector of pairwise distinct entries and $y = (y_1, \ldots, y_n) \in \mathbb{F}^n$ a vector of nonzero entries. The $[n, r]$ generalized Reed-Solomon (GRS) code with support x and multiplier y is*

$$\mathbf{GRS}_r(x, y) \stackrel{def}{=} \{(y_1 P(x_1), \ldots, y_n P(x_n)) \mid P \in \mathbb{F}[z], \deg P < r\}.$$

The dual of a GRS code is also a GRS code, where the support and the multiplier are related to the ones of the primal code.

Proposition 1. *[14, Theorem 4, p. 304] The dual of a GRS code is a GRS code*

$$\mathbf{GRS}_r(x, y)^\perp = \mathbf{GRS}_{n-r}(x, y^\perp),$$

with $y^\perp \stackrel{def}{=} \left(\frac{1}{\pi'_x(x_1)y_1}, \ldots, \frac{1}{\pi'_x(x_n)y_n}\right)$, and π'_x is the derivative of $\pi_x \stackrel{def}{=} \prod_{i=1}^n (z - x_i)$.

An *alternant code* can be defined as the subfield subcode of a GRS code:

Definition 2. *Let $n \leq q^m$, for some positive integer m. Let $\mathbf{GRS}_r(x, y)$ be the GRS code over $\mathbb{F}_{q^m}$ of dimension r with support $x \in \mathbb{F}_{q^m}^n$ and multiplier $y \in (\mathbb{F}_{q^m}^*)^n$. The alternant code with support x and multiplier y and degree r over $\mathbb{F}_q$ is*

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

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

Note that from Delsarte's theorem [9] and by duality,

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

The dimension of an alternant code of order r built upon an extension field of degree m has therefore dimension at least $n - rm$. There exists a subclass of alternant codes which is particularly attractive for cryptographic purposes:

Definition 3. *Let $x \in \mathbb{F}_{q^m}^n$ be a support vector and $\Gamma \in \mathbb{F}_{q^m}[z]$ a polynomial of degree r such that $\Gamma(x_i) \neq 0$ for all $i \in \{1, \ldots, n\}$. The Goppa code of degree r, support x and Goppa polynomial Γ is defined as $\mathscr{G}(x, \Gamma) \stackrel{def}{=} \mathscr{A}_r(x, y)$, where $y \stackrel{def}{=} \left(\frac{1}{\Gamma(x_1)}, \ldots, \frac{1}{\Gamma(x_n)}\right)$.*

Square of codes

GRS codes turn out to display a very peculiar property with respect to the component-wise/Schur product of codes which is defined from the component-wise/Schur product of vectors $a \star b \stackrel{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$ by

Definition 4. *The component-wise product of codes $\mathscr{C}, \mathscr{D}$ over $\mathbb{F}$ with the same length n is defined as $\mathscr{C} \star \mathscr{D} \stackrel{def}{=} \langle c \star d \mid c \in \mathscr{C}, d \in \mathscr{D} \rangle_{\mathbb{F}}$. If $\mathscr{C} = \mathscr{D}$, we call $\mathscr{C}^{\star 2} \stackrel{def}{=} \mathscr{C} \star \mathscr{C}$ the square code of $\mathscr{C}$.*

It is easy to verify the following folklore result (see for instance [5])

Proposition 2. *Let $\mathscr{C}$ be a linear code over $\mathbb{F}$ of dimension k and length n. Then $\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} \leq \min\left(n, \binom{k+1}{2}\right)$.*

For a random linear code $\mathscr{C}$ whose square does not fill the full space, the dimension of its square code is exactly $\binom{k+1}{2}$ with high probability, where k is the dimension of $\mathscr{C}$. On the other hand GRS codes behave very differently (and can therefore be distinguished from random codes by this tool) as shown by

Proposition 3. *Let $\mathbf{GRS}_k(x, y)$ be a GRS code with support x, multiplier y and dimension k. We have $\mathbf{GRS}_k(x, y)^{\star 2} = \mathbf{GRS}_{2k-1}(x, y^2)$. Hence, if $k \leq \frac{n+1}{2}$,*

$$\dim_{\mathbb{F}_{q^m}} (\mathbf{GRS}_k(x, y))^{\star 2} = 2k - 1.$$

Note that the square code dimension is here $2k - 1$, i.e. it is linear in k and not quadratic. Since the dual of a Reed-Solomon code is again a Reed-Solomon code, it turns out that this algebraic class is distinguishable for any rate. For other families, a square code-based distinguisher may occur only for certain rates. For instance Goppa codes (and more in general alternant codes) are distinguishable whenever the rate is high enough as we will now recall. Again this is related to such square code considerations as we will now explain.

The distinguisher of Goppa/alternant codes of [10,11] and its relationship with square code considerations

The dual of an alternant (or Goppa) code can also be distinguished from random codes when the primal code has a high enough rate, using the square code tool. The different behavior was already observed in [10]. Here however, the distinguisher was presented in terms of the kernel dimension D of a linear system obtained by linearizing in the proper way the algebraic system that encodes the key-recovery problem for McEliece cryptosystem endowed with alternant or Goppa codes. Indeed let $P = (p_{ij})_{i,j}$ be a generator matrix of an $[n, k]$ alternant (or Goppa) code $\mathscr{C}$ in systematic form, i.e. with its first k columns that form an identity block and consider the following linear system

$$\mathscr{L}_p = \left\{ \sum_{k+1 \leq j < j' \leq n} p_{ij} p_{ij'} Z_{jj'} = 0 \mid 1 \leq i \leq k \right\}.$$

The dimension D of the solution space of this system turns out to be much smaller in the case of high rate Goppa or alternant codes than for random codes. A formula for D coinciding with experimental evidence was given in [11] together with a convincing algebraic explanation for alternant and binary Goppa codes.

It has been proved in [15] that such D is related to the dimension of the square of the dual code $\mathscr{C}^\perp$. Indeed, from [15, Proposition 1],

$$\dim_{\mathbb{F}} \left(\mathscr{C}^\perp\right)^{\star 2} = \binom{\dim_{\mathbb{F}}(\mathscr{C}^\perp)+1}{2} - D. \tag{2}$$

The formula for D given in [11] predicts with (2) for a generic alternant code $\mathbb{F}_q$ of length n and extension degree m that

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(x,y)^\perp)^{\star 2} = \min\left\{n, \binom{rm+1}{2} - \frac{m}{2}(r-1)\left((2e_{\mathscr{A}}+1)r - 2\frac{q^{e_{\mathscr{A}}}-1}{q-1}\right)\right\}, \tag{3}$$

whereas for a generic Goppa code $\mathscr{G}(x,\Gamma)$ of length n over $\mathbb{F}_q$ with Goppa polynomial $\Gamma(X) \in \mathbb{F}_{q^m}[X]$ of degree r:

$$\dim(\mathscr{G}(x,\Gamma)^\perp)^{\star 2} = \min\left\{n, \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2)\right\}, \quad \text{if } r < q-1 \tag{4}$$

$$\dim(\mathscr{G}(x,\Gamma)^\perp)^{\star 2} = \min\left\{n, \binom{rm+1}{2} - \frac{m}{2}r\left((2e_{\mathscr{G}}+1)r - 2(q-1)q^{e_{\mathscr{G}}-1} - 1\right)\right\}, \quad \text{otherwise,} \tag{5}$$

where $e_{\mathscr{A}}$ and $e_{\mathscr{G}}$ are respectively defined by

$$e_{\mathscr{A}} \stackrel{\text{def}}{=} \max\{i \in \mathbb{N} \mid r \geq q^i + 1\} = \lfloor \log_q(r-1) \rfloor$$
$$e_{\mathscr{G}} \stackrel{\text{def}}{=} \min\{i \in \mathbb{N} \mid r \leq (q-1)^2 q^i\} + 1 = \left\lceil \log_q\left(\frac{r}{(q-1)^2}\right)\right\rceil + 1.$$

As shown in [11], these formulas agree with extensive experimental evidence.

3 Our results

Note: Full proofs are given in the full version of the paper [19].

3.1 A general result about square of trace codes

Part of our results about the abnormally small dimension of the square of the dual of alternant or Goppa codes will use a general result about square of trace codes (recall that the dual of an alternant code is the trace of a GRS code). For this we will use (and prove)

Proposition 4. *Let $\mathscr{C}$ and $\mathscr{D}$ be two linear codes over $\mathbb{F}_{q^m}$ with the same length n. Then $\mathrm{Tr}(\mathscr{C}) \star \mathrm{Tr}(\mathscr{D}) \subseteq \sum_{i=0}^{m-1} \mathrm{Tr}\left(\mathscr{C} \star \mathscr{D}^{q^i}\right)$, where $\mathscr{D}^{q^i} \stackrel{def}{=} \{d^{q^i} \mid d \in \mathscr{D}\}$. When $\mathscr{C} = \mathscr{D}$ this can be refined to give*

$$\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) = \mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^{m-u}}\right) \tag{6}$$

$$(\mathrm{Tr}(\mathscr{C}))^{\star 2} \subseteq \sum_{u=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) \tag{7}$$

$$\dim_{\mathbb{F}_q}\left(\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^{m/2}}\right)\right) \leqslant m\frac{(\dim_{\mathbb{F}_{q^m}}(\mathscr{C}))^2}{2} \quad \textit{if } m \textit{ is even.} \tag{8}$$

From Proposition 3 we know that square codes of GRS codes have an abnormally small dimension. A natural question is whether or not this implies that the square of the trace of a GRS code has itself a small dimension. More generally, this raises the following fundamental issue: if the dimension of a square code $\mathscr{C}^{\star 2}$ over $\mathbb{F}_{q^m}$ is smaller than what we expect from a random code, namely that $\dim\left(\mathscr{C}^{\star 2}\right) < \binom{\dim \mathscr{C}+1}{2}$ (if $\binom{\dim \mathscr{C}+1}{2}$ is smaller than the code length) then does this property survive for the trace code:

$$\dim\left(\mathrm{Tr}(\mathscr{C})\right)^{\star 2} < \binom{\dim \mathrm{Tr}(\mathscr{C}) + 1}{2}?$$

This is related to open questions raised in [20, C.4]. This is indeed the case up to some extent, due to the following proposition:

Proposition 5. *Let $\mathscr{C}$ be an $\mathbb{F}_{q^m}$-linear code. We have*

$$\dim_{\mathbb{F}_q}\left(\mathrm{Tr}(\mathscr{C})\right)^{\star 2} \leqslant m \cdot \dim_{\mathbb{F}_{q^m}} \mathscr{C}^{\star 2} + \binom{m}{2}\left(\dim_{\mathbb{F}_{q^m}} \mathscr{C}\right)^2. \tag{9}$$

3.2 Alternant case with $e_{\mathscr{A}} = 0$ and Goppa case with $e_{\mathscr{G}} = 0$

It is straightforward to use Proposition 5 together with Proposition 3 to derive an upper bound on the dimension of the square of the dual of an alternant or Goppa code which is valid for all parameters and is tight when $e_{\mathscr{A}} = 0$ for random alternant codes and when $r < q - 1$ for Goppa codes.

Theorem 1. *Let $\mathscr{A}_r(x, y)$ be an alternant code over $\mathbb{F}_q$. Then*

$$\dim_{\mathbb{F}_q}\left(\mathscr{A}_r(x, y)^{\perp}\right)^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2). \tag{10}$$

Remark 1. Note that $\mathscr{A}_r(x, y)^{\perp}$ is (typically) of dimension rm. Therefore the term $\binom{rm+1}{2}$ represents the dimension we expect from the square of a random code of the same dimension (if $\binom{rm+1}{2}$ is smaller than the codelength). Therefore the term $\frac{m}{2}(r-1)(r-2)$ can be interpreted as the defect of the dimension when compared to the random case.

3.3 Alternant case with $e_{\mathscr{A}} > 0$

In this case, there are new linear relationships arising for alternant codes (hence also for Goppa codes) of high enough order r. More precisely, the threshold value for which new relations are guaranteed is $r \geq q+1$, i.e. $e_{\mathscr{A}} > 0$. The reason we have a refinement of the upper bound of Theorem 1 for values of r for which $e_{\mathscr{A}} > 0$ is that now in Proposition 4 for $\mathscr{C} \stackrel{\text{def}}{=} \mathbf{GRS}_r(x,y)$ (which is the relevant quantity here since $\mathrm{Tr}(\mathscr{C}) = \mathscr{A}_r(x,y)^\perp$) we get terms of the form $\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right)$ which have a smaller dimension than the generic upper bound mr^2. This is due to the fact that these $\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right)$ will actually be duals of alternant codes for small values of u as shown by the following lemma

Lemma 1. *Let $\mathscr{C} \stackrel{def}{=} \mathbf{GRS}_r(x,y)$ and $f \stackrel{def}{=} \lfloor \log_q(r) \rfloor$. We have*

$$\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) \subseteq \mathscr{A}_{(r-1)(1+q^u)+1}(x, y^{1+q^u})^\perp \text{ for all integers } u \geqslant 0, \quad (11)$$

$$\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) = \mathscr{A}_{(r-1)(1+q^u)+1}(x, y^{1+q^u})^\perp \text{ for all } u \text{ in } \{0, \cdots, f\}. \quad (12)$$

From this, we readily derive that

Theorem 2. *Let $\mathscr{A}_r(x,y)$ be an alternant code over $\mathbb{F}_q$. Then*

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(x,y)^\perp)^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2}(r-1)\left((2e_{\mathscr{A}}+1)r - 2\frac{q^{e_{\mathscr{A}}+1}-1}{q-1}\right). \quad (13)$$

3.4 Goppa case with $r \geq q-1$

In the previous subsections, we used linear relationships within the individual $\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right)$ subspaces, showing that they are spanned by less than $r^2 m$ vectors if r is large enough. We will see that the dimension of some $\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right)$ is even smaller in the Goppa case with $r \geq q-1$ (see (15) below). Moreover, they are no more disjoint, i.e. $\dim_{\mathbb{F}_q}\left(\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) \cap \mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^v}\right)\right) > 0$ for some $0 \leq u < v \leq e_{\mathscr{G}}$ as shown by

Theorem 3. *Let $\mathscr{C} \stackrel{def}{=} \mathbf{GRS}_r(x,y)$, where $y_i = \frac{1}{\Gamma(x_i)}$ and Γ is a polynomial of degree r and $f \stackrel{def}{=} \lfloor \log_q(r) \rfloor$. Let us define for any positive integer v*

$$\mathscr{B}_v \stackrel{def}{=} \mathscr{A}_{r(q^v - q^{v-1}+1)}(x, y^{q^v+1})^\perp, \quad \text{and} \quad \mathscr{B}_0 \stackrel{def}{=} \mathscr{A}_{2r-1}(x, y^2)^\perp. \quad (14)$$

Then

$$\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^v}\right) \subseteq \mathscr{B}_v \quad \text{for all positive integers } v, \quad (15)$$

$$\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) = \mathscr{B}_u \quad \text{for } 0 \leqslant u \leqslant f, \quad (16)$$

$$\mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}\right) \subseteq \mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^q\right) \subseteq \cdots \subseteq \mathrm{Tr}\left(\mathscr{C} \star \mathscr{C}^{q^u}\right) \quad \text{for } 0 \leqslant u \leqslant f. \quad (17)$$

An easy corollary of this theorem is that

Corollary 1. *Let $\mathscr{G}(x, \Gamma)$ be a Goppa code of order $r \geq q-1$ over $\mathbb{F}_q$. Then*

$$\dim_{\mathbb{F}_q}(\mathscr{G}(x,\Gamma)^{\perp})^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2} r\left((2e_{\mathscr{G}}+1)r - 2(q-1)q^{e_{\mathscr{G}}-1} - 1\right).$$

Remark 2. One might wonder how the quantity $e_{\mathscr{G}}$ arises in the previous corollary. Indeed, it does not appear in the previous lemmas. Actually Theorem 3 is used to prove that for e in $\{0, \cdots, \lfloor m/2 \rfloor\}$ we have

$$\dim_{\mathbb{F}_q}(\mathscr{G}(x,\Gamma)^{\perp})^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2} r\left((2e)r - 2(q-1)q^{e-1} - 1\right).$$

The point is that the choice $e = e_{\mathscr{G}}$ minimizes the upper-bound.

4 Conclusion

In this article we revisited the distinguisher for random alternant and Goppa codes presented for the first time in [11] through a different approach, namely using squares of codes. With this simple but powerful tool we were able (i) to provide explicitly the linear relationships determining the distinguisher in a more straightforward way, (ii) to rigorously prove a tight upper bound for the dimension of the square of the dual of an alternant or Goppa code, while [11] only provides an algebraic explanation which does not however represent neither an upper or a lower bound. Our proof is also valid in the case of non-binary Goppa case, for which the conjectured distinguisher is only demonstrated experimentally in [11]. By doing this we got an unifying explanation for the behavior of all Goppa codes, which does not make use of specific features of the binary case. Finally, we illustrated an interesting property of the structure of the square of the dual of any Goppa code, relating it to the dual of another alternant code. This connection could be of help for a potential key-recovery attack.

References

1. Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in $2^{n/20}$: How 1+1 = 0 improves information set decoding. In: Advances in Cryptology - EUROCRYPT 2012. LNCS, Springer (2012)
2. Bernstein, D.J., Chou, T., Lange, T., von Maurich, I., Mizoczki, R., Niederhagen, R., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Wen, W.: Classic McEliece: conservative code-based cryptography. `https://classic.mceliece.org` (Mar 2019), second round submission to the NIST post-quantum cryptography call
3. Both, L., May, A.: Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{2/21n}$ and McEliece Security. In: WCC Workshop on Coding and Cryptography (Sep 2017), `http://wcc2017.suai.ru/Proceedings{_}WCC2017.zip`

4. Canteaut, A., Chabaud, F.: A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Trans. Inform. Theory **44**(1), 367–378 (1998). https://doi.org/10.1109/18.651067, http://dx.doi.org/10.1109/18.651067
5. Cascudo, I., Cramer, R., Mirandola, D., Zémor, G.: Squares of random linear codes. IEEE Trans. Inform. Theory **61**(3), 1159–1173 (3 2015). https://doi.org/10.1109/TIT.2015.2393251
6. Courtois, N., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: Advances in Cryptology - ASIACRYPT 2001. LNCS, vol. 2248, pp. 157–174. Springer, Gold Coast, Australia (2001)
7. Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J.P.: Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Des. Codes Cryptogr. (2), 641–666 (2014)
8. Couvreur, A., Otmani, A., Tillich, J.P.: Polynomial time attack on wild McEliece over quadratic extensions. IEEE Trans. Inform. Theory **63**(1), 404–427 (1 2017)
9. Delsarte, P.: On subfield subcodes of modified Reed-Solomon codes. IEEE Trans. Inform. Theory **21**(5), 575–576 (1975)
10. Faugère, J.C., Gauthier, V., Otmani, A., Perret, L., Tillich, J.P.: A distinguisher for high rate McEliece cryptosystems. In: Proc. IEEE Inf. Theory Workshop-ITW 2011. pp. 282–286. Paraty, Brasil (Oct 2011)
11. Faugère, J.C., Gauthier, V., Otmani, A., Perret, L., Tillich, J.P.: A distinguisher for high rate McEliece cryptosystems. IEEE Trans. Inform. Theory **59**(10), 6830–6844 (Oct 2013)
12. Kachigar, G., Tillich, J.P.: Quantum information set decoding algorithms. In: Post-Quantum Cryptography 2017. LNCS, vol. 10346, pp. 69–89. Springer, Utrecht, The Netherlands (Jun 2017)
13. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North–Holland, Amsterdam, fifth edn. (1986)
14. Márquez-Corbella, I., Pellikaan, R.: 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
15. May, A., Meurer, A., Thomae, E.: Decoding random linear codes in $O(2^{0.054n})$. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology - ASIACRYPT 2011. LNCS, vol. 7073, pp. 107–124. Springer (2011)
16. May, A., Ozerov, I.: On computing nearest neighbors with applications to decoding of binary linear codes. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015. LNCS, vol. 9056, pp. 203–228. Springer (2015)
17. McEliece, R.J.: A Public-Key System Based on Algebraic Coding Theory, pp. 114–116. Jet Propulsion Lab (1978), dSN Progress Report 44
18. Mora, R., Tillich, J.P.: On the dimension and structure of the square of the dual of a goppa code. preprint (2021), http://arxiv.org/abs/2111.13038
19. Randriambololona, H.: On products and powers of linear codes under componentwise multiplication. In: Algorithmic arithmetic, geometry, and coding theory, Contemp. Math., vol. 637, pp. 3–78. Amer. Math. Soc., Providence, RI (2015). https://doi.org/10.1090/conm/637/12749
20. Sendrier, N.: On the use of structured codes in code based cryptography. In: S. Nikova, B. Preneel, L.S. (ed.) Coding Theory and Cryptography III. pp. 59–68. The Royal Flemish Academy of Belgium for Science and the Arts (2010)
21. Stern, J.: A method for finding codewords of small weight. In: Cohen, G.D., Wolfmann, J. (eds.) Coding Theory and Applications. LNCS, vol. 388, pp. 106–113. Springer (1988)