



HAL
open science

Goppa-like AG codes from $C_{a,b}$ curves and their behaviour under squaring their dual

Sabira El Khalfaoui, Mathieu Lhotel, Jade Nardi

► To cite this version:

Sabira El Khalfaoui, Mathieu Lhotel, Jade Nardi. Goppa-like AG codes from $C_{a,b}$ curves and their behaviour under squaring their dual. *IEEE Transactions on Information Theory*, 2024, 70 (5). hal-04234627v2

HAL Id: hal-04234627

<https://univ-rennes.hal.science/hal-04234627v2>

Submitted on 29 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

GOPPA-LIKE AG CODES FROM $C_{a,b}$ CURVES AND THEIR BEHAVIOUR UNDER SQUARING THEIR DUAL

SABIRA EL KHALFAOUI, MATHIEU LHOTEL, AND JADE NARDI

ABSTRACT. In this paper, we introduce a family of codes that can be used in a McEliece cryptosystem, called *Goppa-like AG codes*. These codes generalize classical Goppa codes and can be constructed from any curve of genus $g \geq 0$. Focusing on codes from $C_{a,b}$ curves, we study the behaviour of the dimension of the square of their dual to determine their resistance to distinguisher attacks similar to the one for alternant and Goppa codes developed by Mora and Tillich [MT23]. We also propose numerical experiments to measure the sharpness of our bound.

INTRODUCTION

McEliece cryptosystem. The McEliece cryptosystem is one of the last code-based candidates for standardization of post-quantum cryptographic to the NIST competition since the third round. It guarantees the smallest ciphertexts among all the candidates, but it suffers from the largest public keys. Over the past forty years, there were many attempts in replacing the family of binary Goppa codes by other structured families of codes in order to reduce the key size.

The security of the McEliece cryptosystem is based on two assumptions: (i) in average, it is hard to decode t errors for codes having the same parameters as the codes used as keys and (ii) it is difficult to distinguish codes used as public keys from arbitrary ones. When proposing another family of codes, one must ensure that both of the hardness assumptions are still valid. Algebraic geometry (AG) codes appear to be good candidates for the McEliece cryptosystem, since they are evaluation codes built from algebraic curves (GRS codes are a typical example of AG codes on a genus zero curve). Moreover, they also come with an efficient decoding algorithm (see the survey of Høholdt and Pellikaan [HP95]). In 1996, Janwa and Moreno [JM96] proposed to use AG codes, concatenation or subfield subcode of these codes in the McEliece cryptosystem. As for concatenated ones, they were broken by Sendrier [Sen94]. For AG codes, Faure and Minder proposed an attack in [FM08, Min07, Fau09] for codes of genus at most 2. The scheme based on AG codes has been completely broken by Couvreur, Marquez-Corbella and Pellikaan [CMCP17], who proposed a filtration-based attack on AG codes for any genus, enabling decoding just by handling the public key and without knowledge of the curve and/or the divisor. However, the authors underlined that subfield subcodes of AG codes (SSAG codes in short) are resistant to this filtration attack. Moreover, some of these codes have a good designed minimum distance, such as Cartier codes [Cou14]. This resistance to structural attacks, as well as their good parameters, motivated several works on SSAG codes. Barelli [Bar18] studied the security of quasi-cyclic SSAG codes designed from cyclic covers of the projective line and of plane curves. Recently, Zhao and Chen [ZC22] analysed the parameters and the decoding performance of one-point elliptic subfield subcodes, showing that in the binary case, decoding results on these codes outperform the similar rate in the case of BCH codes. Also, the authors in [PJ14, KN21] focus on one-point Hermitian codes, and manage to compute the exact dimension of their subfield subcodes, in order to get a better estimate for the key size when using them in the McEliece cryptosystem.

Subfield subcodes of AG codes. Let \mathbb{F}_{q^m} be a finite extension of \mathbb{F}_q . Let \mathcal{C} be an AG code, *i.e.* $\mathcal{C} := C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G) \subseteq \mathbb{F}_{q^m}^n$ where \mathcal{X} is an algebraic curve defined over \mathbb{F}_{q^m} , $\mathcal{P} \subseteq \mathcal{X}(\mathbb{F}_{q^m})$ and $G \in \text{Div}(\mathcal{X})$. The subfield subcode of \mathcal{C} over \mathbb{F}_q is defined by

$$C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q} := \mathcal{C} \cap \mathbb{F}_q^n.$$

In this paper, we introduce a specific class of SSAG codes, namely Goppa-like AG codes. The idea of this construction is to introduce some randomness into the family of SSAG codes drawn as private key by mimicking the role of the Goppa polynomial in the case of classical Goppa codes. Given an effective divisor $D \in \text{Div}(\mathcal{X})$ on the curve, we consider SSAG codes associated to divisors

Date: August 7, 2023.

2020 Mathematics Subject Classification. 11T71, 14G50, 14H05, 11G20.

Key words and phrases. AG codes, Subfield subcodes, $C_{a,b}$ curves, Goppa-like AG codes, Trace codes, Schur product.

of the form $D + (g)$, for a large family of functions $g \in \mathbb{F}_q^m(\mathcal{X})$ on the curve. A Goppa-like AG code is then defined as the subfield subcode over \mathbb{F}_q of $C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g))^{\perp}$. In the genus zero case, this construction gives codes which are Hamming equivalent to classical Goppa codes. With a good choice of the curve and divisor, it is possible to encode and decode these codes in a timely manner; this generalization has the potential to significantly improve on the original McEliece proposal. This encourages the present study of structural attacks on Goppa-like AG codes.

Distinguisher attack. Our starting point is the paper by Mora and Tillich [MT23], which benefited from the trace structure of the dual code of a subfield subcode to provide a sharp bound for the dimension of the square of the dual of alternant codes. This gives a distinguisher for these codes: whoever with a generator matrix (or a parity check matrix) of such a code can calculate this dimension in polynomial time and notice that it is significantly smaller than expected. Informally they give a bound of the form

$$\dim \left((\text{GRS}_r(\mathbf{x}, \mathbf{y})|_{\mathbb{F}_q})^{\perp} \right)^{*2} \leq D - \delta$$

where $D = \dim_{\mathbb{F}_q} \left((C|_{\mathbb{F}_q})^{\perp} \right)^{*2} = \binom{mr+1}{2}$ is the expected value for a random r -dimensional code C and $\delta > 0$ (see §1.1 for formal definitions). Mora and Tillich's techniques rely on two features of GRS codes. First, their behaviour with respect to the Schur product is well known. In the particular case of Goppa codes, where the multiplier has the form $\mathbf{y} = (g(x_1)^{-1}, g(x_2)^{-1}, \dots, g(x_n)^{-1})$ for some degree r polynomial g , they managed to get an even sharper upper bound by performing Euclidean division by powers of g .

As Goppa-like AG codes extend Goppa codes, it is natural to wonder if one can derive a structural attack on these codes from Mora and Tillich's attack. The genus \mathfrak{g} of the curve plays a significant role in the parameters of AG codes. The greater the genus, the more \mathbb{F}_q -points the curve \mathcal{X} may have and so the longer the code can be. But the parameters $[n, k, d]$ of an AG code satisfy $n - \mathfrak{g} + 1 \leq k + d \leq n + 1$, which means that an AG code is \mathfrak{g} -far from optimality. Also, the correction capacity naturally suffers from a big genus: the naive correction algorithm can correct up to $\frac{d-1-\mathfrak{g}}{2}$ errors. Only refined techniques, based on error locating arrays [CP20], manage to remove the term related to the genus. Therefore, caution should be exercised when it comes to the impact of the genus on the properties of AG codes. Even if Mora and Tillich's attack does not threaten the Goppa codes used in the NIST competition, SSAG-based propositions may be vulnerable to a similar structural attack.

Contributions of this paper. In the present work, we are interested in the case of one-point Goppa-like AG codes from $C_{a,b}$ curves, a class of curves introduced in [Miu93]. These curves have been extensively studied and they are especially interesting to design AG codes. As we know explicit monomial basis of the AG code associated to any multiple of its unique point at infinity, it allows us to efficiently encode one-point codes [BRS21]. Furthermore, they remain quite general: for examples, elliptic curves, Kummer or Artin-Schreier curves are $C_{a,b}$ curves. It is also natural to wonder how the genus affects the distinguisher: in particular, we give a sufficient condition in terms of the minimal degree our divisor has to satisfy in order to mount the distinguisher. This bound is increasing with the genus of the curve, and coincides with the one given in [MT23] in the case of classical Goppa codes. Consequently, when the genus gets higher, we are not able to distinguish codes associated to low degree divisors. In the worst cases, we might not be able to distinguish anything.

AG codes, as generalizations of GRS codes, have exactly the same behaviour with respect to the Schur product. Moreover, some well-chosen AG codes are defined by the evaluation of *multivariate* polynomials. In this case, we prove that performing division algorithms via Gröbner bases enables us to estimate the dimension of the square of the dual of Goppa-like AG codes. Even better, computations tend to show that the bound we obtain on the dimension is sharp whenever the one-point Goppa-like AG code seems random (*i.e.* the function g is sufficiently random). The counterpart is, as it was the case in [MT23] for classical Goppa codes, that we can only distinguish high rate codes. More precisely, our maximum distinguishable rate is roughly the same as in [MT23]. A comparison of their results and ours is carried out in the case of Goppa-like AG codes defined over an elliptic curve. However, as previously discussed, if the genus becomes too large, the distinguisher may become ineffective: in particular, we show that Goppa-like AG codes constructed from the Hermitian curve resist our distinguisher, which is encouraging if we intend to base the McEliece cryptosystem on such class of codes.

However, as it is already the case for the distinguisher of classical Goppa codes [MT23], it seems complicated to turn this distinguisher into an efficient structural attack. But, having an algebraic

explanation of the structure of the square of the dual of one-point Goppa-like AG codes is still desirable if we want to perform an attack using square code considerations. It also provides a rigorous method for selecting initial parameters that ensure the security of our cryptosystem.

Application of Goppa-like AG codes to the McEliece cryptosystem. For a McEliece cryptosystem based on a family of $[n, k]_q$ linear codes, the public key has size $k(n - k)\lceil \log_2(q) \rceil$, whenever the generator matrix \mathbf{G} of the public code is given in systematic form. The choice of such codes should not be limited to the binary case: Peters [Pet09] showed that for $q > 2$, the subfield subcode construction over \mathbb{F}_q can improve the key size while maintaining the same level of security against a decoding attack.

Information-set decoding (ISD) algorithm, introduced by Prange [Pra62], is the best known algorithm for decoding a random-looking code without any knowledge of its structure. Let us denote by t the error capability of the family of codes we consider. Given a $(n - k) \times n$ parity check matrix \mathbf{H} and a column vector \mathbf{s} of length $n - k$ obtained through \mathbf{H} , the total complexity of finding the row vector $\mathbf{e} \in \mathbb{F}_q^n$ of weight t and satisfying $\mathbf{s} = \mathbf{H}\mathbf{e}^T$ is given by

$$C_{\text{Prange}} = \frac{\binom{n}{t}}{\binom{n-k}{t}} C_{\text{partial Gauss}}$$

where $C_{\text{partial Gauss}}$ is the cost of the partial Gauss–Jordan elimination. We neglect it since the Gaussian elimination is exponentially faster than the collision search.

In this work, we also investigate Goppa-like AG codes over finite fields with different characteristics by analysing the computational cost of the ISD algorithm for parameters relevant to post-quantum cryptography. In Table 1, we provide parameters of Goppa-like AG codes from the Hermitian curve (for g random) that resist the distinguisher given in this paper and that improve key sizes compared to binary Goppa codes. We also compare to the subfield subcodes of one-point Hermitian codes (HSS) [NEK21, Tables 2 and 3], which corresponds to the case where the function g is zero. In this table, s denotes the degree of the one-point divisor $D = sP_\infty$.

	Variant	q	m	n	s	k	t	Security $\log_2(C_{\text{Prange}})$	Key size (Megabytes)
Category 1	Classical	2	12	3 488	–	2 720	64	143	261
	HSS	11	2	1 331	1 174	927	78	142	140
	GLH			1 331	242	955	67	128	155
				1 289	248	901	70	128	151
		13		1 366 [†]	426	668	136	142	216
Category 3	Classical	2	13	4 608	–	3 360	96	185	524
	HSS	13	2	2 197	2 039	1 735	79	185	401
	GLH			2 197	346	1 659	96	204	413
				1 731 [†]	438	1 009	142	192	337
Category 5	Classical	2	13	6 688	–	5 024	128	263	1 045
	HSS	13	2	2 197	1 861	1 398	168	263	559
	GLH	13		2 197	506	1 339	176	256	531
		16		2 467 [†]	570	1 565	166	256	706
	Classical	2	13	8 192	–	6 528	128	300	1 358
	HSS	16	2	4 096	3 874	3 422	111	300	1 153
	GLH			4 096	478	3 378	120	314	1 213
				2 704 [†]	674	1 594	218	300	885

TABLE 1. Comparison between binary Goppa codes (*Classical* [BCC⁺22]), one-point Hermitian subfield subcodes (*HSS* [NEK21]) and Goppa-like Hermitian codes (*GLH*) in the McEliece cryptosystem.

Note that the Goppa-like Hermitian codes given in Table 1 have length at most q^3 . By considering shorter codes, we get smaller keys and better correction capability t , at the expense of the security. For practical use in the McEliece cryptosystem, we need to ensure that for each function g selected, we are able to construct the associated Goppa-like AG code. This is why we must

choose $q^3 - n$ larger than s , so that we can always select n \mathbb{F}_q -points \mathcal{P} outside the zero locus of g and define the evaluation code $C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g))$ properly. If this condition is fulfilled, the length given in Table 1 is followed by a symbol \dagger . At each level of security, we can guarantee this property, sometimes by working over larger alphabets and thus deteriorating the parameters.

In general, Goppa-like Hermitian codes offer significant advantages over classical binary Goppa codes in terms of key size optimization, error correction capability, and potential post-quantum security.

Outline of the paper. The paper is organized as follows. Section 1 is dedicated to basic definitions about linear codes, subfield subcodes and trace codes, AG codes and $C_{a,b}$ curves. In Section 2, we introduce the notion of Goppa-like AG codes and we give a first bound for the dimension of the square of their dual. In Section 3, we refine the bound for Goppa-like AG codes from $C_{a,b}$ curves, associated to one-point divisors. Section 4 concludes this paper with a discussion about this bound on elliptic curves and on the Hermitian curve.

1. PRELIMINARIES

1.1. Linear codes, subfield subcodes and trace codes. In this section, we briefly introduce some notation and basic definitions for linear codes, subfield subcodes, and trace codes. Furthermore, we present significant results that employ component-wise product and the trace map. For further details about linear codes, we refer the reader to [MS86].

Let \mathbb{F}_{q^m} be a finite extension of the field \mathbb{F}_q with q elements, where $m \geq 1$. A *linear code* \mathcal{C} over \mathbb{F}_{q^m} is a vector subspace of $\mathbb{F}_{q^m}^n$. The integer n is called its *length* and we denote by k its *dimension* and by d its *minimum distance*. We say that \mathcal{C} is a $[n, k, d]_{q^m}$ code or that it has parameters $[n, k, d]_{q^m}$ (we may omit the minimum distance in this notation). Given a linear code of length n , its dual code \mathcal{C}^\perp is defined by

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}_{q^m}^n \mid \mathbf{c} \cdot \mathbf{x} = 0, \text{ for all } \mathbf{c} \in \mathcal{C} \},$$

where \cdot denotes the usual scalar product. It is easy to verify that if \mathcal{C} is an $[n, k]_{q^m}$ code, then \mathcal{C}^\perp is a $[n, n - k]_{q^m}$ code. A generator matrix \mathbf{G} of an $[n, k]_{q^m}$ linear code \mathcal{C} is a $k \times n$ matrix over \mathbb{F}_{q^m} whose rows are a basis of \mathcal{C} as a vector space, while a parity check matrix \mathbf{H} of \mathcal{C} is a $(n - k) \times n$ generator matrix of its dual. For a linear code with length n and dimension k , its rate is defined by the ratio $R := \frac{k}{n}$. The Schur product of two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^n$ is defined as

$$\mathbf{a} \star \mathbf{b} := (a_1 b_1, \dots, a_n b_n).$$

It can be extended to codes in the following way: If \mathcal{C} and \mathcal{D} are two codes over \mathbb{F}_{q^m} with same length n , their Schur product is defined as the following component-wise product:

$$\mathcal{C} \star \mathcal{D} := \text{Span}(\mathbf{c} \star \mathbf{d} \mid \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{D}).$$

Moreover, if $\mathcal{C} = \mathcal{D}$, we call $\mathcal{C}^{\star 2} := \mathcal{C} \star \mathcal{C}$ the square of \mathcal{C} . The following lemma gives a first estimation of the dimension of Schur product of codes.

Lemma 1.1 ([MT23, Proposition 10]). *Let \mathcal{C} and \mathcal{D} be two linear codes over \mathbb{F}_{q^m} with same length n and respective dimension $k_{\mathcal{C}}$ and $k_{\mathcal{D}}$. We have*

- (1) $\dim_{\mathbb{F}_{q^m}}(\mathcal{C} \star \mathcal{D}) \leq \min\{k_{\mathcal{C}}k_{\mathcal{D}}, n\}$;
- (2) $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}^{\star 2}) \leq \min\left(n, \binom{k_{\mathcal{C}} + 1}{2}\right)$.

In particular, by [CCMZ15, Theorem 2.3], if \mathcal{C} is sufficiently random and $\mathcal{C}^{\star 2}$ does not fill the full space, we expect to have

$$\dim_{\mathbb{F}_{q^m}}(\mathcal{C}^{\star 2}) = \binom{k_{\mathcal{C}} + 1}{2}.$$

Given a linear code \mathcal{C} over \mathbb{F}_{q^m} , there exist two constructions of codes on the subfield \mathbb{F}_q , namely its subfield subcode and its trace code. The *subfield subcode* of \mathcal{C} , denoted by $\mathcal{C}|_{\mathbb{F}_q}$, is the linear code over \mathbb{F}_q defined by

$$\mathcal{C}|_{\mathbb{F}_q} = \mathcal{C} \cap \mathbb{F}_q^n.$$

Again, if \mathcal{C} is a $[n, k, d]_{q^m}$ code, then $\mathcal{C}|_{\mathbb{F}_q}$ is a $[n, \geq n - m(n - k), \geq d]_q$ code. Let $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ be the trace operator on \mathbb{F}_{q^m} with respect to \mathbb{F}_q , i.e. defined by

$$\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \dots + x^{q^{m-1}},$$

for any $x \in \mathbb{F}_{q^m}$. We can extend this definition to any vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$ by

$$\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\mathbf{c}) = (\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \dots, \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n)).$$

To make the notation less cumbersome, we shall write $\text{Tr}(\cdot)$ instead of $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\cdot)$ in the following.

Given a linear code \mathcal{C} of length n and dimension k over \mathbb{F}_{q^m} , its *trace code* over \mathbb{F}_q is the image under the trace operator, that is $\text{Tr}(\mathcal{C})$. It is a linear code of length n over \mathbb{F}_q , whose dimension satisfies

$$(1) \quad \dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C}) \leq \min\{mk, n\}.$$

Subfield subcodes and trace codes are related by the duality operator, as stated by Delsarte's theorem.

Theorem 1.2 ([Del75, Delsarte's theorem]). *Let \mathcal{C} be a linear code of length n over \mathbb{F}_{q^m} . Then*

$$(\mathcal{C} \cap \mathbb{F}_q^n)^\perp = \text{Tr}(\mathcal{C}^\perp).$$

1.2. AG and SSAG codes.

1.2.1. Definitions. Let \mathcal{X} be a smooth and irreducible projective curve over \mathbb{F}_{q^m} of genus \mathfrak{g} . A *divisor* on \mathcal{X} over \mathbb{F}_{q^m} is a formal sum of places over \mathbb{F}_{q^m} , *i.e.* of the form $G = \sum \nu_P(G)P$, where $\nu_P(G)$ are integers which are all zero except for a finite number of places P . We denote by $\text{Div}(\mathcal{X})$ the set of \mathbb{F}_{q^m} -divisors on \mathcal{X} (we omit the dependence on \mathbb{F}_{q^m}). Given $G \in \text{Div}(\mathcal{X})$, we define its *support* $\text{Supp}(G)$ as the finite set of places P such that $\nu_P(G)$ is non-zero and its *degree* as $\deg(G) = \sum \nu_P(G) \deg(P)$. We say that a divisor $G \in \text{Div}(\mathcal{X})$ is *effective* if for all $P \in \text{Supp}(G)$, we have $\nu_P(G) \geq 0$, in which case we write $G \geq 0$. This permits to define an order on the group of divisors by setting $G_1 \geq G_2$ if and only if $G_1 - G_2 \geq 0$.

A non-zero function $f \in \mathbb{F}_{q^m}(\mathcal{X})$ defines a divisor, called *principal*, denoted by $(f) = \sum \nu_P(f)P$. The *Riemann–Roch space* of a divisor G is defined as the \mathbb{F}_{q^m} vector space

$$\mathcal{L}(G) := \{f \in \mathbb{F}_{q^m}(\mathcal{X}) \mid (f) + G \geq 0\} \cup \{0\},$$

of dimension $\ell(G)$. Let $\mathcal{P} \subseteq \mathbb{F}_{q^m}(\mathcal{X})$ be a set of n distinct rational points such that $\text{Supp}(G) \cap \mathcal{P} = \emptyset$. By numbering the points in $\mathcal{P} = \{P_1, \dots, P_n\}$, we define an evaluation map

$$(2) \quad \text{ev}_{\mathcal{P}} : \begin{cases} \mathcal{L}(G) & \rightarrow \mathbb{F}_{q^m}^n \\ f & \mapsto (f(P_1), \dots, f(P_n)) \end{cases}$$

We can consider the AG code

$$\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G) := \{\text{ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}(G)\},$$

which is a $[n, k \geq \ell(G)]_{\mathbb{F}_{q^m}}$ code. If $n > \deg(G)$, then its dimension is exactly equal to $\ell(G)$ and its minimum distance is bounded from below by the *designed distance* $d^* = n - \deg(G)$.

From the Riemann–Roch theorem, we have

$$\ell(G) \geq \deg(G) + 1 - \mathfrak{g},$$

with equality if $\deg(G) \geq 2\mathfrak{g} - 1$.

The dual of an AG code can be described as a residue code (see [Sti09] for more details), *i.e.*

$$C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)^\perp = C_{\Omega}(\mathcal{X}, \mathcal{P}, G).$$

Residue and evaluation codes are connected by the following result.

Proposition 1.3 ([Sti09, Proposition 2.2.10]). *Let $C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)$ be an AG code defined on a curve \mathcal{X} . Then*

$$C_{\Omega}(\mathcal{X}, \mathcal{P}, G) = C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G^\perp),$$

with $G^\perp = D_{\mathcal{P}} - G + W$, where $D_{\mathcal{P}} = \sum_{P \in \mathcal{P}} P$ and $W = (\omega)$ is a canonical divisor such that for all $P \in \mathcal{P}$, $\nu_P(\omega) = -1$ and $\text{Res}_{\omega}(P) = 1$.

In general, it is hard to find the true dimension of the subfield subcode of an AG code, but a trivial estimate can be derived from Delsarte's theorem (Theorem 1.2):

$$(3) \quad \dim_{\mathbb{F}_q} C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q} \geq n - m \dim_{\mathbb{F}_{q^m}} C_{\Omega}(\mathcal{X}, \mathcal{P}, G).$$

The minimum distance of the SSAG code $C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q}$ is at least the one of the AG code $C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)$ above. It is thus bounded from below by the designed distance $d^* = n - \deg(G)$.

In particular cases, the structure of AG codes may provide sharper bounds on the dimension of their subfield subcodes and trace codes.

Theorem 1.4 ([Sti09, Theorem 9.1.6]). *With notation as above, let G_1 be any divisor such that*

$$(4) \quad G \geq qG_1 \text{ and } G \geq G_1.$$

Then

$$\dim_{\mathbb{F}_q} \text{Tr}(C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)) \leq \begin{cases} m(\ell(G) - \ell(G_1)) + 1 & \text{if } G_1 \geq 0, \\ m(\ell(G) - \ell(G_1)) & \text{if } G_1 \not\geq 0, \end{cases}$$

and

$$\dim_{\mathbb{F}_q} C_{\Omega}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q} \geq \begin{cases} n - 1 - m(\ell(G) - \ell(G_1)) & \text{if } G_1 \geq 0, \\ n - m(\ell(G) - \ell(G_1)) & \text{if } G_1 \not\geq 0. \end{cases}$$

Remark 1.5. The biggest divisor (with respect to the degree) satisfying the conditions in Equation (4) is given by

$$(5) \quad \left\lfloor \frac{G}{q} \right\rfloor := \sum_{P \in \text{Supp}(G^+)} \left\lfloor \frac{\nu_P(G^+)}{q} \right\rfloor P + \sum_{P \in \text{Supp}(G^-)} \nu_P(G^-) P,$$

where G^+ and G^- are effective divisors such that $G = G^+ - G^-$.

With additional hypotheses on G and $\left\lfloor \frac{G}{q} \right\rfloor$, [LC16, Theorem 1] gives an exact formula for such a code.

Regarding the parameters of subfield subcodes of differential codes, Wirtz [Wir88] improved the bound on their the minimum distance.

Theorem 1.6 ([Wir88, Theorem 2]). *Take the same notation as in Theorem 1.4 and assume $\deg(G_1) > 2g - 2$. Set $U := \{P \in \text{Supp}(G) \mid \nu_P(G) \geq 0 \text{ and } \nu_P(G) \equiv q - 1 \pmod{q}\}$ and $G_U = \sum_{P \in U} P$. Then*

$$\dim_{\mathbb{F}_q} C_{\Omega}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q} = \dim_{\mathbb{F}_q} C_{\Omega}(\mathcal{X}, \mathcal{P}, G + G_U)|_{\mathbb{F}_q},$$

hence the minimum distance of $C_{\Omega}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q}$ satisfies

$$d(C_{\Omega}(\mathcal{X}, \mathcal{P}, G)|_{\mathbb{F}_q}) \geq \deg(G) + \deg(G_U) - 2g + 2.$$

1.2.2. First estimation of the dimension of the square of the trace of an AG code. In this paper, we aim to bound the dimension of the square of the dual of an SSAG code. From Delsarte's theorem, this is equivalent to study the square of the trace of the corresponding AG code. This is possible thanks to the following result from [MT23], which is valid for any linear code.

Proposition 1.7 ([MT23, Proposition 15]). *Let \mathcal{C} be a linear code over \mathbb{F}_{q^m} . Then we have*

$$(6) \quad \text{Tr}(\mathcal{C})^{*2} := ((\mathcal{C}^{\perp}|_{\mathbb{F}_q})^{\perp})^{*2} \subseteq \sum_{i=0}^{\lfloor m/2 \rfloor} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}),$$

where $\mathcal{C}^{q^i} = \{(c_1^{q^i}, \dots, c_n^{q^i}) \mid \mathbf{c} \in \mathcal{C}\}$. Moreover, if m is even,

$$(7) \quad \dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^{\frac{m}{2}}}) \leq \frac{m}{2} (\dim_{\mathbb{F}_{q^m}} \mathcal{C})^2.$$

From this result, we can deduce an upper bound for the dimension of the square of the dual of any linear code.

Corollary 1.8 ([MT23, Corollary 16]). *Let \mathcal{C} be any \mathbb{F}_{q^m} -linear code. Then*

$$(8) \quad \dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C})^{*2} \leq m \cdot \dim_{\mathbb{F}_{q^m}}(\mathcal{C}^{*2}) + \binom{m}{2} (\dim_{\mathbb{F}_{q^m}}(\mathcal{C}))^2.$$

Furthermore, if $\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C}) = m \cdot \dim_{\mathbb{F}_{q^m}}(\mathcal{C})$, then

$$\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C})^{*2} - \binom{\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C}) + 1}{2} \leq m \left(\dim_{\mathbb{F}_{q^m}} \mathcal{C}^{*2} - \binom{\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) + 1}{2} \right).$$

The above corollary implies that if the dimension of a square code is smaller than that of a random code, namely

$$\dim_{\mathbb{F}_{q^m}}(\mathcal{C}^{*2}) < \binom{\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) + 1}{2},$$

then this property is retained for the trace code, i.e.

$$\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C})^{*2} < \binom{\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C}) + 1}{2}.$$

This is especially true for Reed–Solomon codes (see [MT23, Proposition 11]) and more generally for AG codes.

Proposition 1.9 ([Mum70, Theorem 6]). *Let F, G be two divisors on \mathcal{X} such that $\deg(G) \geq 2\mathfrak{g} + 1$ and $\deg(F) \geq 2\mathfrak{g}$. Then*

$$\mathcal{L}(F) \cdot \mathcal{L}(G) = \mathcal{L}(F + G),$$

where $\mathcal{L}(F) \cdot \mathcal{L}(G) := \text{Span}(f \cdot g : (f, g) \in \mathcal{L}(F) \times \mathcal{L}(G))$.

If $\text{Supp}(F) \cap \mathcal{P} = \text{Supp}(G) \cap \mathcal{P} = \emptyset$, then denoting all the evaluation maps defined in Equation (2) by $\text{ev}_{\mathcal{P}}$ (regardless of their domain), we have

$$(9) \quad \forall (f, g) \in \mathcal{L}(F) \times \mathcal{L}(G), \text{ev}_{\mathcal{P}}(f) \star \text{ev}_{\mathcal{P}}(g) = \text{ev}_{\mathcal{P}}(f \cdot g).$$

As a consequence, for associated AG codes, we have

$$C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, F) \star C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G) \subseteq C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, F + G).$$

Regarding the Schur square, it implies that

$$C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)^{\star 2} \subseteq C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, 2G),$$

with equality if $\deg(G) \geq 2\mathfrak{g} + 1$. If $\deg(G) \geq \mathfrak{g}$, applying the Riemann–Roch theorem to the divisors G and $2G$ thus gives

$$(10) \quad \begin{aligned} \dim_{\mathbb{F}_{q^m}} C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)^{\star 2} &\leq \dim_{\mathbb{F}_{q^m}} C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, 2G) \\ &= 2 \deg(G) + 1 - \mathfrak{g} \\ &\leq \deg(G) + \dim_{\mathbb{F}_{q^m}} C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G), \end{aligned}$$

which is much smaller than the expected dimension given in Lemma 1.1 (2). Combined with Equation (6), we get a first upper bound on the dimension of the square of the trace of an AG code.

Corollary 1.10. *Let $\mathcal{C} := C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)$ be a k -dimensional AG code on \mathcal{X} associated with a degree $s \geq \mathfrak{g}$ divisor. Then*

$$\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C})^{\star 2} = \dim_{\mathbb{F}_q} ((\mathcal{C}^\perp|_{\mathbb{F}_q})^\perp)^{\star 2} \leq \binom{mk+1}{2} - \frac{m}{2}(k(k-1) - 2s).$$

Proof. From Proposition 1.9 and Equation (10), we have $\dim_{\mathbb{F}_{q^m}} \mathcal{C}^{\star 2} \leq 2s + 1 - \mathfrak{g} \leq k + s$. Thus, Equation (8) leads to

$$\begin{aligned} \dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C})^{\star 2} &\leq m(k+s) + \binom{m}{2} k^2 = (2k+2s+mk^2-k^2) \frac{m}{2} \\ &= (k(mk+1) - k^2 + k + 2s) \frac{m}{2} \\ &= \binom{mk+1}{2} - \frac{m}{2}(k(k-1) - 2s). \end{aligned}$$

□

Remark 1.11. For $\mathcal{X} = \mathbb{P}^1$, we recover [MT23, Theorem 17].

According to the above corollary, the dimension of the square of the dual of an SSAG code is less than the expected value for random codes (which is $\binom{mk+1}{2}$), due to the algebraic structure of AG codes. However, this bound does not fully benefit from this rich structure, notably the following property.

Lemma 1.12. *Let $\mathcal{C} := C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)$ be a k -dimensional AG code on \mathcal{X} . For every $i \geq 0$, we have*

$$\mathcal{C} \star \mathcal{C}^{q^i} \subseteq C_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, (q^i + 1)G)$$

Proof. Fix $i \geq 0$ and let $f_1, f_2 \in \mathcal{L}(G)$. Then the product $f_1 f_2^{q^i}$ belongs to $\mathcal{L}((q^i + 1)G)$ as

$$(f_1 f_2^{q^i}) + (q^i + 1)G = ((f_1) + G) + q^i((f_2) + G) \geq 0.$$

This proves the inclusion of spaces

$$\mathcal{L}(G) \cdot \mathcal{L}(G)^{q^i} \subseteq \mathcal{L}((q^i + 1)G),$$

hence the inclusion of the associated codes. □

Remark 1.13. The property above for $i = 0$ follows from Proposition 1.9. To the best of our knowledge, there is no sufficient criterion for the equality when $i \geq 1$ in the literature. Given a basis $\{f_1, \dots, f_k\}$ of the Riemann–Roch space $\mathcal{L}(G)$, the vector space $\mathcal{L}(G) \cdot \mathcal{L}(G)^{q^i}$ is spanned by the set $\left\{f_u f_v^{q^i} \mid 1 \leq u \leq v \leq k\right\}$. From our experiments, it may happen that the cardinality of this family is larger than $\ell((q^i + 1)G)$ without the equality holding, which means that these generators may be linearly dependent in $\mathcal{L}((q^i + 1)G)$ and do not form a basis of $\mathcal{L}(G) \cdot \mathcal{L}(G)^{q^i}$.

Thanks to Lemma 1.12, it will be possible to better handle the terms $\text{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$ in Equation (6). Our aim for the rest of the paper is to improve the bound of Corollary 1.10 in some specific cases.

1.3. $C_{a,b}$ curves. Throughout this paper, we will be dealing with algebraic geometry codes defined over a $C_{a,b}$ curve. This section is dedicated to some properties on this well-studied class of curves. For further details, we refer to [Miu93].

Definition 1.14. Let a, b be coprime positive integers. A $C_{a,b}$ curve over \mathbb{F}_{q^m} is a curve $\mathcal{X}_{a,b}$ having an irreducible, affine and non-singular plane model with equation

$$(11) \quad f_{a,b}(x, y) = \alpha_{0a}y^a + \alpha_{b0}x^b + \sum \alpha_{ij}x^i y^j = 0,$$

where $f_{a,b} \in \mathbb{F}_{q^m}[X, Y]$ with $\alpha_{0a}, \alpha_{b0} \neq 0$, and the sum is taken over all couples $(i, j) \in \{0, \dots, b\} \times \{0, \dots, a\}$ such that $ai + bj < ab$.

Any curve $\mathcal{X}_{a,b}$ defined as in Equation (11) has a unique point at infinity, denoted by P_∞ . Moreover, as a plane curve, its genus is given by

$$\mathfrak{g}_{a,b} := \frac{(a-1)(b-1)}{2}.$$

1.3.1. The point at infinity P_∞ and the ring \mathcal{S} . We will consider codes obtained by evaluating functions on $\mathcal{X}_{a,b}$ which are regular everywhere, except maybe at the unique point at infinity P_∞ . These functions then belong to the coordinate ring of the affine curve $\mathcal{X}_{a,b} \setminus \{P_\infty\}$, which we denote by \mathcal{S} . We have

$$(12) \quad \mathcal{S} = \bigcup_{s \geq 0} \mathcal{L}(sP_\infty),$$

where each Riemann–Roch space $\mathcal{L}(sP_\infty)$ has an explicit basis as follows:

$$(13) \quad \mathcal{L}(sP_\infty) = \text{Span}\left(x^i y^j \mid 0 \leq i, 0 \leq j \leq a-1 \text{ and } ai + bj \leq s\right).$$

In summary, any function that is regular on all $\mathcal{X}_{a,b}$ except maybe at P_∞ is a bivariate polynomial in the functions x and y .

Definition 1.15 (Weighted degree). Given a monomial of the form $x^i y^j \in \mathcal{S}$, we define its weighted degree by

$$\deg_{a,b}(x^i y^j) := ai + bj.$$

From this degree, we can define a monomial order \prec over $\mathcal{S} \simeq \mathbb{F}_{q^m}[x, y]$ as follows: $x^u y^v \prec x^{u'} y^{v'}$ if

$$(14) \quad \deg_{a,b}(x^u y^v) < \deg_{a,b}(x^{u'} y^{v'}) \text{ or } \left(\deg_{a,b}(x^u y^v) = \deg_{a,b}(x^{u'} y^{v'}) \text{ and } u < u'\right).$$

Any function $f \in \mathcal{S}$ can be written in the form

$$f = c \cdot x^\beta y^\alpha + f'(x, y),$$

with $c \neq 0$, $\alpha \leq a-1$ and $f' \in \mathcal{S}$ such that any monomial $x^i y^j$ of f' satisfies $ai + bj < \deg_{a,b}(x^\beta y^\alpha)$ and $j \leq a-1$. The leading monomial of f with respect to the monomial order \prec is thus defined by $\text{LM}(f) := x^\beta y^\alpha$. This extends the definition of weighted degree to any such function by setting

$$\deg_{a,b}(f) := \deg_{a,b}(\text{LM}(f)).$$

It is easy to check that for any $f \in \mathcal{S}$, its weighted degree $\deg_{a,b}(f)$ is equal to the smallest integer s such that f belongs to the Riemann–Roch space $\mathcal{L}(sP_\infty)$. This way, any function in $\mathcal{L}(sP_\infty)$ can be seen as a polynomial in x and y such that $\deg_{a,b}(f) \leq s$.

Remark 1.16. For every $f \in \mathcal{S}$, we have $\deg_{a,b}(f) = -v_{P_\infty}(f)$.

2. GOPPA-LIKE AG CODES

2.1. Definition, parameters and context in the literature. Let D be an effective divisor of positive degree s on a smooth and irreducible projective curve \mathcal{X} over \mathbb{F}_{q^m} . Take a rational function $g \in \mathbb{F}_{q^m}(\mathcal{X})$ such that $g \notin \mathcal{L}(D)$. Given a set of \mathbb{F}_{q^m} -points $\mathcal{P} \in \mathcal{X}(\mathbb{F}_{q^m})$ such that $\mathcal{P} \cap \text{Supp}(g) = \emptyset$ and $\mathcal{P} \cap \text{Supp}(D) = \emptyset$, we consider the AG code

$$\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g)) = \{ \text{ev}_{\mathcal{P}}(fg^{-1}) \mid f \in \mathcal{L}(D) \}.$$

From now on, we set $G = D + (g)$. Note that we have $\deg(G) = \deg(D)$.

Definition 2.1. The Goppa-like AG code associated to \mathcal{C} is defined as the subfield subcode of its dual code, *i.e.*

$$\Gamma(\mathcal{P}, D, g) := \mathcal{C}^{\perp}|_{\mathbb{F}_q}.$$

Such a code has length $n = \#\mathcal{P}$. As stated in [JM96, Theorem 1], its dimension satisfies

$$\dim_{\mathbb{F}_q} \Gamma(\mathcal{P}, D, g) \geq n - m \dim_{\mathbb{F}_{q^m}} \mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g)) = n - m(\deg(D) - \mathfrak{g} + 1)$$

if $2\mathfrak{g} - 2 < \deg(D) < n$. Its minimum distance is bounded from below by $\deg(D) - 2\mathfrak{g} + 2$.

Remark 2.2. These estimations on the dimension and the minimum distance may be improved by Theorems 1.4 and 1.6. Regarding the dimension, it is worth noting that, since $g \notin \mathcal{L}(D)$, the divisor G is not effective. Hence, any divisor G_1 satisfying the conditions of Equation (4) is also non-effective, which means that

$$\dim_{\mathbb{F}_q} \Gamma(\mathcal{P}, D, g) \geq n - m(\ell(G) - \ell(G_1)).$$

Without additional conditions on the divisor D and the function g , the divisor G_U for $G = D + (g)$ defined in Theorem 1.6 is zero. Generally, we cannot expect for a better bound for the minimum distance.

2.1.1. Why the terminology Goppa-like? In [JM96], Janwa and Moreno define *Goppa codes* on smooth and irreducible projective curves. Compared to their definition, Definition 2.1 introduces a function g which defines a multiplier for the AG code over \mathbb{F}_{q^m} that is algebraically related to the support \mathcal{P} .

Introducing this function g facilitates the use of SSAG codes as public keys for the McEliece cryptosystem. Given a correcting error capability t , we can fix a divisor D whose degree satisfies $\deg(D) \geq 2t + 2\mathfrak{g} + 1$. Then the family of codes in which the public key is picked can be defined by running a family of functions g outside $\mathcal{L}(D)$.

We prefer the terminology *Goppa-like AG codes* instead of simply Goppa codes for two reasons. First, AG codes were historically called *geometric Goppa codes*. Our terminology involving both the words ‘‘Goppa’’ and ‘‘AG’’ removes this possible ambiguity. Second, we want to emphasize the use of a different curve than the projective line \mathbb{P}^1 , like we differentiate AG codes from Reed–Solomon codes.

This denomination is obviously motivated by the fact that here, the rational function g plays the role of the Goppa polynomial. As described in [Sti09, Example 9.1.8], Goppa codes are nothing but Goppa-like AG codes from the projective line $\mathcal{X} = \mathbb{P}^1$. In fact, given $r \geq 0$, the Generalized Reed–Solomon (GRS) code of degree r , support $\mathbf{x} \in \mathbb{F}_{q^m}^n$ and multiplier $\mathbf{y} \in (\mathbb{F}_{q^m}^*)^n$ is defined as

$$\text{GRS}_r(\mathbf{x}, \mathbf{y}) = \{ (y_1 f(x_1), y_2 f(x_2), \dots, y_n f(x_n)) \mid f \in \mathbb{F}_{q^m}[X] \text{ such that } \deg(f) < r \}.$$

Take a univariate polynomial g of degree r such that $g(x_i) \neq 0$ for every $i \in \{1, \dots, n\}$. Then the Goppa code of order r and support $\mathbf{x} \in \mathbb{F}_{q^m}^n$ is defined as

$$(15) \quad \Gamma_r(\mathbf{x}, g) = \text{GRS}_r(\mathbf{x}, \mathbf{y})^{\perp}|_{\mathbb{F}_q},$$

where $\mathbf{y} = (g(x_1)^{-1}, g(x_2)^{-1}, \dots, g(x_n)^{-1})$. Represent the \mathbb{F}_{q^m} -points of \mathbb{P}^1 by the couples $\mathbb{P}^1(\mathbb{F}_{q^m}) = \{ [1 : x] \mid x \in \mathbb{F}_{q^m} \} \cup \{ P_{\infty} \}$ for $P_{\infty} = [0 : 1]$. Take $\mathcal{P} = \{ [1 : x_1], [1 : x_2], \dots, [1 : x_n] \}$ and $D = (r - 1)P_{\infty}$. Finally, the polynomial g can be seen as a function on \mathbb{P}^1 which lies in $\mathcal{L}(rP_{\infty})$ but not in $\mathcal{L}((r - 1)P_{\infty})$. Then both constructions match: $\Gamma_r(\mathbf{x}, g) = \Gamma(\mathcal{P}, D, g)$.

2.1.2. Relation with Cartier codes. Cartier codes [Cou14] are also defined as a geometric realization of Goppa codes, since well-known properties of Goppa codes naturally extend to them. For instance, Theorem 1.6 holds for Cartier code without assumption on the degree of the divisor.

The link with Goppa-like AG codes is the following: by definition, a Cartier code is a subcode of the subfield subcode of a residue code (see [Cou14, Proposition 4.3]), which actually means that for an appropriate choice of divisor, a Cartier code is a subcode of the corresponding Goppa-like AG code. Moreover, [Cou14, Theorem 5.1] provides a sufficient condition for both constructions to be equal. More precisely, let us consider a Goppa-like AG code $\Gamma(\mathcal{P}, D, g)$ and set $G := D + (g)$.

Then the Cartier code $\text{Car}_q(\mathcal{P}, G)$ (see [Cou14, Definition 4.2]) satisfies $\text{Car}_q(\mathcal{P}, G) \subseteq \Gamma(\mathcal{P}, D, g)$, and

$$\dim_{\mathbb{F}_q}(\Gamma(\mathcal{P}, D, g)/\text{Car}_q(\mathcal{P}, G)) \leq m \cdot i(G_1),$$

where G_1 is any divisor such that

$$(4) \quad G \geq qG_1 \text{ and } G \geq G_1.$$

Here $i(G_1)$ stands for the index of speciality of G_1 (see [Sti09, Definition 1.6.10]). By the Riemann–Roch theorem, if $\deg(G_1) > 2\mathfrak{g} - 2$, then $i(G_1) = 0$. Thus, using Remark 1.5, the Cartier code $\text{Car}_q(\mathcal{P}, G)$ coincides with the Goppa-like AG code $\Gamma(\mathcal{P}, D, g)$ whenever $\deg\left(\left[\frac{G}{q}\right]\right) > 2\mathfrak{g} - 2$.

Example 2.3. Let $q = 3$ and $m = 4$. We consider the elliptic curve defined over \mathbb{F}_{q^m} by the equation

$$E : y^2 = x^3 + 2x + 1.$$

As usual, we denote by P_∞ the unique point at infinity on E . We take D as a one-point divisor supported by P_∞ , *i.e.* $D = 7P_\infty$. We consider two choices of function $g \in \mathcal{L}(8P_\infty) \setminus \mathcal{L}(7P_\infty)$:

- (1) First, let $g_1 = x^4$. In this case, g has 2 zeroes (say P_1 and P_2), which are those of x . More precisely, the divisor of g_1 is given by

$$(g_1) = 4(P_1 + P_2) - 8P_\infty.$$

Hence, if we set $G = D + (g_1)$, the divisor $\left[\frac{G}{q}\right] = P_1 + P_2 - P_\infty$ has degree $1 > 2g(E) - 2 = 0$, meaning that the codes $\Gamma(\mathcal{P}, D, g_1)$ and $\text{Car}_3(\mathcal{P}, G)$ are equal over \mathbb{F}_3 .

- (2) Second, take $g_2 = x^4 + xy$. This time, we can verify that g_2 has 8 distinct rational zeroes, say R_1, \dots, R_8 , *i.e.*

$$(g_2) = R_1 + \dots + R_8 - 8P_\infty.$$

Consequently, we easily check that $\deg\left(\left[\frac{G}{q}\right]\right) = -1 \leq 2g(E) - 2$. Some computations realized on Magma show that the codes $\Gamma(\mathcal{P}, D, g_2)$ and $\text{Car}_3(\mathcal{P}, G)$ are not equal in this case.

Magma results are summarized in Table 2, where $\mathcal{P} = E(\mathbb{F}_{q^m}) \setminus \text{Supp}(g)$.

n	$\deg(D)$	Choice of g	$\deg\left(\left[\frac{D+(g)}{q}\right]\right)$	$\dim_{\mathbb{F}_3}(\Gamma(\mathcal{P}, D, g))$	$\dim_{\mathbb{F}_3}(\text{Car}_3(\mathcal{P}, G))$
88	7	$g = x^4$	1	64	
82		$g = x^4 + xy$	-1	50	54

TABLE 2. Comparison of Cartier and Goppa-like constructions

2.2. On the dimension of the square of the dual of a Goppa-like AG code. In this section, we aim to generalize the properties found by the authors of [MT23] in Section 6, in the context of Goppa-like AG codes. Let us consider the AG code

$$\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g))$$

as defined in Section 2.1. Applying Equation (6) yields

$$(16) \quad \text{Tr}(\mathcal{C})^{*2} = (\Gamma(\mathcal{P}, D, g)^\perp)^{*2} \subseteq \sum_{i=0}^{\lfloor m/2 \rfloor} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}).$$

Below, we discuss how to improve the upper bound given in Corollary 1.10, which is valid for all subfield subcodes of AG codes. The idea is to use the specific algebraic structure of our code inherited from the choice of its divisor. In fact, notice that the code \mathcal{C} is monomially equivalent to $\mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D)$. More precisely, using the equality $\mathcal{L}(D + (g)) = g^{-1} \cdot \mathcal{L}(D)$, we can easily deduce the following result.

Lemma 2.4. *Suppose $s \geq \mathfrak{g}$. Then for all $i \geq 0$, we have*

$$\dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \leq m(s(q^i + 1) + 1 - \mathfrak{g}).$$

Proof. From Lemma 1.12, we deduce that

$$\dim_{\mathbb{F}_{q^m}} \mathcal{C} \star \mathcal{C}^{q^i} \leq \dim_{\mathbb{F}_{q^m}} \mathcal{L}((q^i + 1)G) = \dim_{\mathbb{F}_{q^m}} \mathcal{L}((q^i + 1)D) = s(q^i + 1) + 1 - \mathfrak{g},$$

the last equality coming from the Riemann–Roch theorem (since $\deg((q^i + 1)D) = (q^i + 1)s \geq 2\mathfrak{g} - 1$). The result follows from the usual upper bound on the dimension of the trace of a code. \square

Remark 2.5. At first glance, it seems that we could have benefited from Theorem 1.4 to get a sharper bound in the previous lemma. Indeed, for every $i \geq 1$, we have

$$\left\lfloor \frac{(q^i + 1)G}{q} \right\rfloor = q^{i-1}G^+ - (q^i + 1)G^-,$$

writing $G = G^+ - G^-$ with $G^+, G^- \geq 0$. However, in the context of Goppa-like AG codes, we have $G = D + (g)$ where $g \notin \mathcal{L}(D)$, hence $G^- \neq 0$. Without further hypotheses on the divisor D and the function g , the degree of the divisor $\left\lfloor \frac{(q^i+1)G}{q} \right\rfloor$ may be too low to bound the dimension of its Riemann–Roch space from below via the Riemann–Roch theorem.

This simple lemma yields an upper bound on the dimension of the square of the dual of Goppa-like codes.

Proposition 2.6. *Let $\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g))$ be an AG code as above, and suppose $s \geq \mathfrak{g}$. Set $k := \dim_{\mathbb{F}_q} \mathcal{C}$ and $e_0 := \min \left(\lfloor \frac{m}{2} \rfloor, \left\lfloor \log_q \left(\frac{k^2}{s} \right) \right\rfloor \right)$. Then*

$$\dim_{\mathbb{F}_q} (\Gamma(\mathcal{P}, D, g)^\perp)^{\star 2} \leq \binom{mk + 1}{2} - \frac{m}{2} \left(k(k-1)(2e_0 + 1) - 2s \left(\frac{q^{e_0+1} - 1}{q-1} \right) \right).$$

Proof. For any $e \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$, Proposition 1.7 implies that

$$\begin{aligned} \dim_{\mathbb{F}_q} (\Gamma(\mathcal{P}, D, g)^\perp)^{\star 2} &\leq \sum_{i=0}^{\lfloor m/2 \rfloor} \dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \\ &\leq \sum_{i=0}^e m(s(q^i + 1) + 1 - \mathfrak{g}) + \sum_{i=e+1}^{\lfloor m/2 \rfloor} \dim_{\mathbb{F}_q} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \quad (\text{by Lemma 2.4}) \\ &\leq \sum_{i=0}^e m(sq^i + k) + \left(\frac{m-1}{2} - e \right) mk^2 \quad (\text{by the Riemann–Roch theorem}) \\ &\leq \frac{m}{2} \left(2k(e+1) + 2s \left(\frac{q^{e+1} - 1}{q-1} \right) + k^2(m-1) - 2ek^2 \right) \\ &\leq \binom{mk + 1}{2} - \frac{m}{2} \left(k(k-1)(2e+1) - 2s \left(\frac{q^{e+1} - 1}{q-1} \right) \right). \end{aligned}$$

Notice that at the third line, we can replace $\lfloor \frac{m}{2} \rfloor$ with $\frac{m-1}{2}$ while bounding the second part of the sum thanks to Equation (7). To get the best bound, we maximize the expression

$$\frac{m}{2} \left(k(k-1)(2e+1) - 2s \left(\frac{q^{e+1} - 1}{q-1} \right) \right)$$

with respect to e . Removing the constant parts, this is equivalent to find the maximum of the function

$$F(e) = ek^2 - s \frac{q^{e+1}}{q-1}$$

over $\{0, \dots, \lfloor \frac{m}{2} \rfloor\}$ in the discrete domain of non-negative integers. We compute the discrete derivative:

$$\begin{aligned} \Delta F(e) = F(e+1) - F(e) &= (e+1)k^2 - s \frac{q^{e+2}}{q-1} - \left(ek^2 - s \frac{q^{e+1}}{q-1} \right) \\ &= k^2 - sq^{e+1}. \end{aligned}$$

This function is decreasing with e , and the smallest value for which $\Delta F(e) \leq 0$ corresponds to its maximum. It is the smallest value of e such that $k^2 \leq sq^{e+1}$, *i.e.*

$$e_0 := \left\lfloor \log_q \left(\frac{k^2}{s} \right) \right\rfloor.$$

□

Remark 2.7. For $\mathcal{X} = \mathbb{P}^1$, Proposition 2.6 boils down to [MT23, Theorem 19] with $k = s + 1$.

2.2.1. Sharpness of the bound. Definition 2.1 of a Goppa-like AG code $\Gamma(\mathcal{P}, D, g) := \mathcal{C}^\perp|_{\mathbb{F}_q}$ requires very few hypotheses. Besides the conditions on the supports of D and (g) , which guarantee that the code is well-defined, we only ask for the function g not to belong to the Riemann–Roch space $\mathcal{L}(D)$. This assumption is enforced to make sure that the dimension of $\text{Tr}(\mathcal{C})^{*2}$ is not abnormally small compared to the expected value given in Corollary 1.8, and thus to make Goppa-like AG codes resistant to a distinguisher based on the square of their dual.

First, if the function g lied in $\mathcal{L}(D)$ (or more generally if the vector of the evaluations $(g(P))_{P \in \mathcal{P}}$ belonged to $\mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D)$), then the code $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, D + (g))$ would contain the evaluation of the constant function $1 = \frac{g}{g}$, *i.e.* the unit vector $(1, \dots, 1)$. In this case, the vector $(1, \dots, 1)$ would belong to \mathcal{C}^{q^i} for every $i \in \{0, \dots, \lfloor m/2 \rfloor\}$ and each term in the sum on the right hand-side would contain a copy of $\text{Tr}(\mathcal{C})$. This non-trivial intersection between the codes $\text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i})$ would contribute with a negative term in the above bound. Secondly, if g belonged to $\mathcal{L}(D)$, then $D + (g)$ would be effective. This would imply the inclusion $\mathcal{L}((q^i + 1)D) \subset \mathcal{L}((q^{i+1} + 1)D)$ for every $i \geq 0$. Therefore, in the proof of Proposition 2.6, when bounding from above the dimension of the sum by the sum of the dimensions of the trace codes, we would have no chance to get a sharp bound.

Unfortunately, the condition $g \notin \mathcal{L}(D)$ does not guarantee that the bound given in Proposition 2.6 is reached. In the following proposition, we detail one situation in which we cannot hope for equality.

Proposition 2.8. *Using the same notation as above, set $\mathcal{C}_1 = \mathcal{C}_{\mathcal{L}}\left(\mathcal{X}, \mathcal{P}, \left[\frac{D+(g)}{q}\right]\right)$ (see Equation (5) for the definition of $\left[\frac{G}{q}\right]$, given G). If $\dim \mathcal{C}_1 \geq 1$, then the bound given in Proposition 2.6 is not reached.*

Proof. Any non-zero codeword $\mathbf{c} \in \mathcal{C}_1 \subset \mathcal{C}$ satisfies $\mathbf{c}^q \in \mathcal{C}$. As \mathbf{c} lies in $\mathbb{F}_{q^m}^n$, we have $\mathbf{c}^{q^m} = \mathbf{c} \in \mathcal{C}^{q^{m-1}}$. Therefore, we have $\mathcal{C}_1 \subseteq \mathcal{C}^q \cap \mathcal{C}^{q^{m-1}}$, and for every $i \in \{1, \dots, \lfloor \frac{m}{2} \rfloor\}$, we have $\mathcal{C}_1^{q^i} \subseteq \mathcal{C}^{q^i} \cap \mathcal{C}^{q^{i-1}}$. By taking the star product with \mathcal{C} , we have $\mathcal{C} \star \mathcal{C}_1^{q^i} \subseteq (\mathcal{C} \star \mathcal{C}^{q^i}) \cap (\mathcal{C} \star \mathcal{C}^{q^{i-1}})$, hence

$$\text{Tr}(\mathcal{C} \star \mathcal{C}_1^{q^i}) \subseteq \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \cap \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^{i-1}}).$$

As a result, each pair of consecutive terms in the sum $\sum_{i=0}^{\lfloor m/2 \rfloor} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i})$ has non-trivial intersection. However, using [Tia19, Theorem 2], equality with the upper bound only occurs if

$$\bigcap_{0 \leq j \leq \lfloor m/2 \rfloor} \left(\sum_{\substack{0 \leq i \leq \lfloor m/2 \rfloor \\ i \neq j}} \text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \right) = \{0\}.$$

□

Remark 2.9. In [FGO⁺13], the authors predict that the bound given in Proposition 2.6 is sharp for "generic" alternant codes (*i.e.* Goppa-like AG codes constructed on the projective line). A consequence of Proposition 2.8 is that a way to be "non-generic" is to have $\mathcal{C}_1 \neq \{0\}$. We illustrate this in Example 2.10.

As noted in Remark 2.5, when picking the function g at random, the code \mathcal{C}_1 is likely to be reduced to zero. Regarding classical Goppa codes (defined in Equation (15)) used for the McEliece cryptosystem, it is common to ask for the degree r polynomial g to have only simple roots. In this case, we have $\left[\frac{(r-1)P_\infty + (g)}{q}\right] = -P_\infty$ and the code \mathcal{C}_1 defined in Proposition 2.8 is always zero. The situation of Example 2.10 thus never occurs.

As recalled in Section 2.1, Goppa-like AG codes coincide with Cartier code as soon as

$$\deg\left(\left[\frac{D + (g)}{q}\right]\right) > 2\mathfrak{g} - 2.$$

In this case, the code \mathcal{C}_1 has dimension at least \mathfrak{g} . This means that when the Goppa-like code is also a Cartier code on a curve \mathcal{X} with positive genus $\mathfrak{g} > 0$, the dimension of the square of its dual cannot meet the bound given in Proposition 2.6.

Example 2.10. Let $q = 5$ and $m = 4$. Let P_∞ be the point at infinity on the projective line $\mathcal{X} = \mathbb{P}^1$ over \mathbb{F}_{q^m} . Using Magma, we compare the bound given in Proposition 2.6 with the true dimension of the corresponding code. In Table 3 below, we take $\mathcal{P} = \mathbb{P}^1(\mathbb{F}_{q^m}) \setminus \text{Supp}(g)$, $D = sP_\infty$ and P_0 stands for the zero of x in the rational function field $\mathbb{F}_{q^m}(x)$.

n	$s = \deg(D)$	Choice of g	$\frac{D+(g)}{q}$	$\dim_{\mathbb{F}_q} \mathcal{C}_1$	$\dim_{\mathbb{F}_q} (\Gamma(\mathcal{P}, D, g)^\perp)^{*2}$	Bound in Prop 2.6
624	9	$g = x^{10}$	$2P_0 - P_\infty$	2	255	496
	10	$g = x^{11}$			295	570

TABLE 3. Illustration of Proposition 2.6

3. ONE-POINT GOPPA-LIKE AG CODE ON $C_{a,b}$ -CURVES

Example 2.10 illustrates how far the bound provided by Proposition 2.6 can be from the actual dimension when dealing with one-point AG codes. This phenomenon has been carefully studied on $\mathcal{X} = \mathbb{P}^1$ by Mora and Tillich [MT23]. In this section, we will generalize their results. We give a whole framework in which we can improve this bound on $C_{a,b}$ curves.

3.1. Framework: one-point Goppa-like AG codes on $C_{a,b}$ curves. Below, we define a specific class of Goppa-like AG codes on a $C_{a,b}$ curve, associated to a divisor which is equivalent to the one-point divisor sP_∞ . Throughout the rest of the paper, we fix a $C_{a,b}$ curve $\mathcal{X}_{a,b}$ as defined in Definition 1.14.

Definition 3.1. Let $s' > s$ be two integers such that there exists a function $g \in \mathcal{L}(s'P_\infty)$ with $\deg_{a,b}(g) = s'$. Given a set of points $\mathcal{P} \subset \mathcal{X}_{a,b}(\mathbb{F}_{q^m})$ such that $\mathcal{P} \cap \text{Supp}(g) = \emptyset$, we define the one-point Goppa-like AG code associated to \mathcal{P} , s and g as

$$\Gamma(\mathcal{P}, sP_\infty, g) := \mathcal{C}_{\mathcal{L}}(\mathcal{X}_{a,b}, \mathcal{P}, (sP_\infty + (g))^\perp)_{\mathbb{F}_q}.$$

This definition might be restrictive, but it is reasonable as these codes can be encoded quickly thanks to the nice basis of $\mathcal{L}(sP_\infty)$ (see Equation (13)), which is desirable if we aim to build a McEliece cryptosystem based on this family of codes. Moreover, this property will be key in the upcoming sections as it allows a better understanding of the square of the dual of any one-point Goppa-like AG code, under some condition on s and s' .

In the next sections, we generalize the result given in [MT23] in the case of classical Goppa codes, by defining a weighted Euclidean division on the ring \mathcal{S} (see Equation (12)), whose elements are seen as bivariate polynomials.

3.2. Weighted Euclidean division. The following proposition generalizes the classical Euclidean division of univariate polynomials in the case of functions in \mathcal{S} with respect to the weighted degree $\deg_{a,b}$. Before that, we need the following definition.

Definition 3.2. For any function $h \in \mathcal{S}$ with leading monomial $\text{LM}(h) = x^\beta y^\alpha$ and $\alpha < a$, we define over \mathbb{F}_{q^m} the space

$$\mathcal{R}(h) := \text{Span}(x^u y^v \mid u \leq \beta + b - 1 \text{ and } v \leq a - 1 \text{ not both } u \geq \beta \text{ and } v \geq \alpha).$$

Note that the dimension of $\mathcal{R}(h)$ is equal to $\deg_{a,b}(h)$.

Proposition 3.3. Fix a nonzero function $g \in \mathcal{S}$. Then for any function $f \in \mathcal{S}$, there exist $f_1, f_2 \in \mathcal{S}$ such that

$$f = f_1 g + f_2 \text{ with } f_2 \in \mathcal{R}(g).$$

Moreover, we have $\deg_{a,b}(f_2) \leq \deg_{a,b}(f)$.

Proof. Since $f \in \mathcal{S}$, we can see f as a bivariate polynomial in x and y (see Equation 12). In the polynomial ring $\mathbb{F}_{q^m}[x, y]$, we perform the division of f by a Gröbner basis of the ideal generated by the equation $f_{a,b}$ of the curve $\mathcal{X}_{a,b}$ and the polynomial g with respect to the monomial order \prec defined in Equation (14). The fact that f_2 lies in $\mathcal{R}(g)$ follows from [GH00, Proposition 4].

Finally, if we had $\deg_{a,b}(f) < \deg_{a,b}(f_2)$ with $f = f_1 g + f_2$, this would mean that $\text{LM}(f_2) = -\text{LM}(f_1 g) = \lambda x^u y^v$ for some $\lambda \in \mathbb{F}_{q^m}^*$ with both $u \geq \beta$ and $v \geq \alpha$, which is not possible by definition of $\mathcal{R}(g)$. \square

3.3. Study of the codes $\text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i})$. In this paragraph, we will use the weighted Euclidean division above to better control the elements in $\text{Tr}(\mathcal{C} \star \mathcal{C}^{q^i})$ for $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(\mathcal{X}_{a,b}, \mathcal{P}, sP_\infty + (g))$, where we fixed $s' > s \geq 0$, $g \in \mathcal{S}$ with $\deg_{a,b}(g) = s'$ and a set of points $\mathcal{P} \subset \mathcal{X}_{a,b}(\mathbb{F}_{q^m})$ such that $\mathcal{P} \cap \text{Supp}(g) = \emptyset$.

Before diving into technical proofs, let us fix some notation that we will use in the rest of the paper. We extend the evaluation map defined in Equation (2) on all the ring \mathcal{S} :

$$\text{ev}_{\mathcal{P}} : \begin{cases} \mathcal{S} & \rightarrow \mathbb{F}_{q^m}^n \\ f & \mapsto (f(P_1), \dots, f(P_n)) \end{cases}$$

Now, $\text{ev}_{\mathcal{P}}$ is an algebra homomorphism, where $\mathbb{F}_{q^m}^n$ is endowed with the product \star , *i.e.* $\text{ev}_{\mathcal{P}}(f) \star \text{ev}_{\mathcal{P}}(f') := \text{ev}_{\mathcal{P}}(f \cdot f')$ for any $f, f' \in \mathcal{S}$.

For two functions $f, f' \in \mathcal{S}$, we will write $f \equiv_{\mathcal{P}} f'$ if $\text{ev}_{\mathcal{P}}(f) = \text{ev}_{\mathcal{P}}(f')$.

We also extend the trace operator on \mathcal{S} by defining $\text{Tr}(f) = f + f^q + \dots + f^{q^{m-1}}$ for every $f \in \mathcal{S}$. Since the map $\text{ev}_{\mathcal{P}}$ is an algebra homomorphism, we have $\text{ev}_{\mathcal{P}}(\text{Tr}(f)) = \text{Tr}(\text{ev}_{\mathcal{P}}(f))$. Moreover, for any function $f \in \mathcal{S}$, we have

$$(17) \quad \text{Tr}(f^q) \equiv_{\mathcal{P}} \text{Tr}(f).$$

Lemma 3.4. *Take $i \geq 1$. Let $f \in \mathcal{S}$ such that $\deg_{a,b}(f) < s'(q^i + 1)$. Then there exists $f' \in \mathcal{R}(g^{q^i - q^{i-1} + 1})$ such that the vectors $\text{Tr}\left(\frac{f}{g^{q^i + 1}}\right) \equiv_{\mathcal{P}} \text{Tr}\left(\frac{f'}{g^{q^i + 1}}\right)$.*

Proof. By Proposition 3.3, we can write $f = f_1 g^{q^i - q^{i-1} + 1} + f_2$ with $f_2 \in \mathcal{R}(g^{q^i - q^{i-1} + 1})$ and $\deg_{a,b}(f_2) \leq \deg_{a,b}(f)$. Therefore, using Equation (17), we get

$$\begin{aligned} \text{Tr}\left(\frac{f}{g^{q^i + 1}}\right) &= \text{Tr}\left(\frac{f_1 g^{q^i - q^{i-1} + 1}}{g^{q^i + 1}}\right) + \text{Tr}\left(\frac{f_2}{g^{q^i + 1}}\right) \\ &\equiv_{\mathcal{P}} \text{Tr}\left(\frac{f_1^q g}{g^{q^i + 1}}\right) + \text{Tr}\left(\frac{f_2}{g^{q^i + 1}}\right). \end{aligned}$$

By definition, the second term has the expected form. Let us examine the first term. If $f_1 = 0$, we are done. Otherwise, the definition of f_1 gives $\deg_{a,b}(f_1) = \deg_{a,b}(f) - s'(q^i - q^{i-1} + 1)$, and

$$\begin{aligned} \deg_{a,b}(f_1^q g) &= q \deg_{a,b}(f_1) + s' \\ &= q \deg_{a,b}(f) - s'(q-1)(q^i + 1). \end{aligned}$$

Then $\deg_{a,b}(f_1^q g) < \deg_{a,b}(f)$ if and only if $\deg_{a,b}(f) < s'(q^i + 1)$, which holds by definition of f .

Repeating the division process on $f_1^q g$, as the weighted degree decreases, we can find a function $f' \in \mathcal{R}(g^{q^i - q^{i-1} + 1})$ such that $\text{Tr}\left(\frac{f}{g^{q^i + 1}}\right) \equiv_{\mathcal{P}} \text{Tr}\left(\frac{f'}{g^{q^i + 1}}\right)$. \square

Definition 3.5. For any $1 \leq i \leq \lfloor \frac{m}{2} \rfloor$, we define

$$\mathcal{T}_i(s, g) := \left\{ \text{ev}_{\mathcal{P}} \left(\text{Tr}\left(\frac{f}{g^{q^i + 1}}\right) \right) \mid f \in \mathcal{R}(g^{q^i - q^{i-1} + 1}) \cap \mathcal{L}(s(q^i + 1)P_{\infty}) \right\}$$

and we set

$$\mathcal{T}_0(s, g) := \left\{ \text{ev}_{\mathcal{P}} \left(\text{Tr}\left(\frac{f}{g^2}\right) \right) \mid f \in \mathcal{L}(2sP_{\infty}) \right\}.$$

The vector spaces $\mathcal{T}_i(s, g)$ have been designed so that we have

$$(18) \quad \text{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right) \subseteq \mathcal{T}_i(s, g)$$

for all $i \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$. Indeed, it is straightforward for $i = 0$ and it follows from Lemma 3.4 for $i \geq 1$, noticing that $f \in \mathcal{L}(sP_{\infty}) \cdot \mathcal{L}(sP_{\infty})^{q^i} \subseteq \mathcal{L}(s(q^i + 1)P_{\infty})$.

We will benefit from these inclusions to improve the bound given in Proposition 2.6, provided that we can efficiently compute the dimension of the trace codes $\mathcal{T}_i(s, g)$. This is studied in the next section.

3.4. Upper bound in Goppa-like case. In the proposition below, we study the intersection

$$(19) \quad M_i(s, g) := \mathcal{R}(g^{q^i - q^{i-1} + 1}) \cap \mathcal{L}(s(q^i + 1)P_{\infty})$$

for every $i \in \{1, \dots, \lfloor m/2 \rfloor\}$ in order to better grasp the trace codes $\mathcal{T}_i(s, g)$'s introduced in Definition 3.5. First we set some notation: fix $i \in \{1, \dots, \lfloor m/2 \rfloor\}$ and write $\text{LM}(g) = x^{\beta} y^{\alpha}$ with $a\beta + b\alpha = s'$. By reducing modulo the equation $f_{a,b}$ of $\mathcal{X}_{a,b}$, we can write $g^{q^i - q^{i-1} + 1}$ such that its leading monomial with respect to the monomial order \prec is

$$(20) \quad \text{LM}\left(g^{q^i - q^{i-1} + 1}\right) = x^{\beta_i} y^{\alpha_i}$$

where $\alpha_i \in \{0, \dots, a-1\}$ is the remainder of the Euclidean division of $\alpha(q^i - q^{i-1} + 1)$ by a and

$$(21) \quad \beta_i = \beta(q^i - q^{i-1} + 1) + b \frac{\alpha(q^i - q^{i-1} + 1) - \alpha_i}{a} = \frac{s'(q^i - q^{i-1} + 1) - b\alpha_i}{a}.$$

Depending on the weighted degree s' of g , we can compute the exact dimension of the vector space $M_i(s, g)$ defined in Equation (19).

Proposition 3.6. (1) *If $s'(q^i - q^{i-1} + 1) > s(q^i + 1) + a$, then $M_i(s, g) = \mathcal{L}(s(q^i + 1)P_\infty)$;*

(2) *If $s'(q^i - q^{i-1} + 1) \leq s(q^i + 1) + 1 - 2\mathbf{g}_{a,b}$, then $M_i(s, g) = \mathcal{R}(g^{q^i - q^{i-1} + 1})$;*

(3) *If there exists $v^* \in \{1, \dots, \alpha_i - 1\}$ such that*

$$s(q^i + 1) + a - b(a + v^* - \alpha_i) < s'(q^i - q^{i-1} + 1) \leq s(q^i + 1) + a - b(a + v^* - 1 - \alpha_i),$$

we have

$$\dim_{\mathbb{F}_{q^m}}(M_i(s, g)) = \sum_{v=v^*}^{a-1} \left\lfloor \frac{s(q^i + 1) - bv}{a} \right\rfloor + v^*(\beta_i + b) + a - v^*.$$

(4) *Otherwise, there exists $v^* \in \{\alpha_i + 1, \dots, a\}$ such that*

$$s(q^i + 1) + a - b(v^* - \alpha_i) < s'(q^i - q^{i-1} + 1) \leq s(q^i + 1) + a - b(v^* - 1 - \alpha_i),$$

in which case

$$\dim_{\mathbb{F}_{q^m}}(M_i(s, g)) = \sum_{v=v^*}^{a-1} \left\lfloor \frac{s(q^i + 1) - bv}{a} \right\rfloor + v^*\beta_i + \alpha_i b + a - v^*.$$

Proof. Using the notation above, we can write

$$\begin{aligned} \mathcal{R}(g^{q^i - q^{i-1} + 1}) &:= \text{Span}_{\mathbb{F}_{q^m}} \{x^u y^v \mid u \leq \beta_i + b - 1, v \leq a - 1 \text{ not both } u \geq \beta_i \text{ and } v \geq \alpha_i\} \\ &= \text{Span} \left(\begin{array}{c} 1, x, \dots, x^{\beta_i + b - 1}, \\ \dots \\ y^{\alpha_i - 1}, y^{\alpha_i - 1}x, \dots, y^{\alpha_i - 1}x^{\beta_i + b - 1}, \\ y^{\alpha_i}, y^{\alpha_i}x, \dots, y^{\alpha_i}x^{\beta_i - 1}, \\ \dots \\ y^{a-1}, y^{a-1}x, \dots, y^{a-1}x^{\beta_i - 1} \end{array} \right) \end{aligned}$$

Next, we define for any $v \in \{0, \dots, a-1\}$:

$$\ell_v^i := \max \{u \geq 0 \mid x^u y^v \in \mathcal{L}(s(q^i + 1)P_\infty)\} = \left\lfloor \frac{s(q^i + 1) - bv}{a} \right\rfloor,$$

implying

$$\mathcal{L}(s(q^i + 1)P_\infty) = \text{Span} \left(\begin{array}{c} 1, x, \dots, x^{\ell_0^i}, \\ y, yx, \dots, yx^{\ell_1^i}, \\ \dots \\ y^{a-1}, y^{a-1}x, \dots, y^{a-1}x^{\ell_{a-1}^i} \end{array} \right).$$

We thus have a description of a basis of both spaces $\mathcal{R}(g^{q^i - q^{i-1} + 1})$ and $\mathcal{L}(s(q^i + 1)P_\infty)$, leading to an exact formula for the dimension of their intersection $M_i(s, g)$ for any value of i :

$$(22) \quad \dim_{\mathbb{F}_{q^m}} M_i(s, g) = \sum_{v=0}^{\alpha_i - 1} \min(\beta_i + b, \ell_v^i + 1) + \sum_{v=\alpha_i}^{a-1} \min(\beta_i, \ell_v^i + 1).$$

It remains to compute the corresponding minima with respect to v :

(i) If $0 \leq v \leq \alpha_i - 1$, by using Equation (21), we get

$$\beta_i + b \leq \ell_v^i + 1 \iff s'(q^i - q^{i-1} + 1) \leq F(v) := s(q^i + 1) + a - b(a + v - \alpha_i).$$

(ii) Otherwise, $\alpha_i \leq v \leq a - 1$ and

$$\beta_i \leq \ell_v^i + 1 \iff s'(q^i - q^{i-1} + 1) \leq G(v) := s(q^i + 1) + a - b(v - \alpha_i).$$

Note that both F and G are decreasing with v , and we easily check that $F(0) = G(a)$. Thus, we have the following sequence of integers

$$F(\alpha_i - 1) \leq \dots \leq F(0) = G(a) \leq G(a - 1) \leq \dots \leq G(\alpha_i).$$

Depending on the value of s' , there are a few cases to consider:

- $s'(q^i - q^{i-1} + 1) > G(\alpha_i)$, in which case $M_i(s, g) = \mathcal{L}(s(q^i + 1)P_\infty)$;
- $s'(q^i - q^{i-1} + 1) \leq F(\alpha_i - 1)$, and $M_i(s, g) = \mathcal{R}(g^{q^i - q^{i-1} + 1})$;

- There exists $v^* \in \{1, \dots, \alpha_i - 1\}$ such that $F(v^*) < s'(q^i - q^{i-1} + 1) \leq F(v^* - 1)$;
- There exists $v^* \in \{\alpha_i, \dots, a\}$ such that $G(v^*) < s'(q^i - q^{i-1} + 1) \leq G(v^* - 1)$.

The formulas for the dimension of $M_i(s, g)$ follows from the above computations and (22). \square

Note that (1) corresponds to the case where $\mathcal{T}_i(s, g) = \text{Tr}\left(g^{-(q^i+1)} \cdot \mathcal{L}(s(q^i+1)P_\infty)\right)$, which will produce the same bound as the one given in Proposition 2.6. Instead, we focus on (2), since in this case, we can show some inclusion relations between the $\mathcal{T}_i(s, g)$'s.

Proposition 3.7. *Let $i^* \in \{0, \dots, \lfloor \frac{m}{2} \rfloor - 1\}$ be the smallest integer such that*

$$(23) \quad sq^{i^*} \geq (s' - s)(q^{i^*+1} - q^{i^*} + 1) + 2\mathfrak{g}_{a,b} - 1.$$

Then

$$\mathcal{T}_{i^*}(s, g) \subseteq \mathcal{T}_{i^*+1}(s, g) \subseteq \dots \subseteq \mathcal{T}_{\lfloor \frac{m}{2} \rfloor}(s, g).$$

Proof. From Proposition 3.6 (2), we know that (23) implies

$$M_{i^*+1}(s, g) = \mathcal{R}(g^{q^{i^*+1} - q^{i^*} + 1}).$$

Since the function

$$i \mapsto \frac{s(q^i + 1) + 1 - 2\mathfrak{g}_{a,b}}{q^i - q^{i-1} + 1}$$

is increasing with i , we also have

$$(24) \quad M_i(s, g) = \mathcal{R}(g^{q^i - q^{i-1} + 1}), \forall i \in \{i^*, \dots, \lfloor \frac{m}{2} \rfloor + 1\}.$$

We now prove the inclusions between the \mathcal{T}_i 's, assuming first that $i^* \neq 0$ (since the definition of \mathcal{T}_0 is a bit different). Let $i \in \{i^*, \dots, \lfloor \frac{m}{2} \rfloor - 1\}$, and recall that

$$\mathcal{T}_i(s, g) := \left\{ \text{ev}_{\mathcal{P}} \left(\text{Tr} \left(\frac{f}{g^{q^i+1}} \right) \right) \mid f \in \mathcal{R} \left(g^{q^i - q^{i-1} + 1} \right) \cap \mathcal{L}(s(q^i+1)P_\infty) \right\}.$$

Given $\text{ev}_{\mathcal{P}} \left(\text{Tr} \left(\frac{f}{g^{q^{i+1}+1}} \right) \right)$ in $\mathcal{T}_i(s, g)$, we want to show that it belongs to $\mathcal{T}_{i+1}(s, g)$. Applying Proposition 3.3 by replacing f with $fg^{q^{i+1}-q^i}$ and g by $g^{q^{i+1}-q^i+1}$, we obtain

$$(25) \quad fg^{q^{i+1}-q^i} = f_1g^{q^{i+1}-q^i+1} + f_2,$$

with $f_2 \in \mathcal{R}(g^{q^{i+1}-q^i+1}) = M_i(s, g)$ (using (24)) and $\deg_{a,b}(f_2) \leq \deg_{a,b}(fg^{q^{i+1}-q^i})$. Next, we write

$$\begin{aligned} \text{Tr} \left(\frac{f}{g^{q^i+1}} \right) &= \text{Tr} \left(\frac{fg^{q^{i+1}-q^i}}{g^{q^i+1}} \right) \\ &= \text{Tr} \left(\frac{f_1g^{q^{i+1}-q^i+1}}{g^{q^i+1}} \right) + \text{Tr} \left(\frac{f_2}{g^{q^i+1}} \right) \\ &\equiv_{\mathcal{P}} \text{Tr} \left(\frac{f_1g^q}{g^{q^i+1}} \right) + \text{Tr} \left(\frac{f_2}{g^{q^i+1}} \right). \end{aligned}$$

By assumption, we immediately have that $\text{ev}_{\mathcal{P}} \left(\text{Tr} \left(\frac{f_2}{g^{q^i+1}} \right) \right) \in \mathcal{T}_{i+1}(s, g)$. If $f_1 = 0$, we are done. Otherwise, we have from (25):

$$\deg_{a,b}(f_1) = \deg_{a,b}(fg^{q^{i+1}-q^i}) - \deg_{a,b}(g^{q^{i+1}-q^i+1}) = \deg_{a,b}(f) - s'.$$

Thus

$$\begin{aligned} \deg_{a,b}(f_1g^q) < \deg_{a,b}(fg^{q^{i+1}-q^i}) &\iff q \deg_{a,b}(f) + (1-q)s' < \deg_{a,b}(f) + s'(q^{i+1} - q^i) \\ &\iff \deg_{a,b}(f) < s'(q^i + 1), \end{aligned}$$

which is true since in particular $f \in \mathcal{L}(s(q^i+1)P_\infty)$ and $s < s'$. Since the weighted degree decreases, we can repeat the division process until eventually we obtain a quotient f_1 equal to zero, which proves that $\mathcal{T}_i(s, g) \subseteq \mathcal{T}_{i+1}(s, g)$.

In the case $i^* = 0$, we also have to prove that $\mathcal{T}_0(s, g) \subseteq \mathcal{T}_1(s, g)$, which differs from the other cases due to the definition of \mathcal{T}_0 . Let $\text{ev}_{\mathcal{P}} \left(\text{Tr} \left(\frac{f}{g^2} \right) \right) \in \mathcal{T}_0(s, g)$, for some $f \in \mathcal{L}(2sP_\infty)$. Using Proposition 3.3, this time replacing f with fg^{q-1} and g with g^{q+1} yields

$$fg^{q-1} = f_1g^q + f_2,$$

with $f_2 \in \mathcal{R}(g^q) = M_1(s, g)$ (using (24) again). Thus, we can write

$$\mathrm{Tr}\left(\frac{f}{g^2}\right) = \mathrm{Tr}\left(\frac{f_1^q g}{g^{q+1}}\right) + \mathrm{Tr}\left(\frac{f_2}{g^{q+1}}\right),$$

with $\mathrm{ev}_{\mathcal{P}}\left(\mathrm{Tr}\left(\frac{f_2}{g^{q+1}}\right)\right) \in \mathcal{T}_1(s, g)$. Since $\deg_{a,b}(f_1) = \deg_{a,b}(fg^{q-1}) - \deg_{a,b}(g^q) = \deg_{a,b}(f) - s'$, we have

$$\begin{aligned} \deg_{a,b}(f_1^q g) < \deg_{a,b}(fg^{q-1}) &\iff q \deg_{a,b}(f) + (1-q)s' < \deg_{a,b}(f) + s'(q-1) \\ &\iff (q-1) \deg_{a,b}(f) < 2s'(q-1) \\ &\iff \deg_{a,b}(f) < 2s', \end{aligned}$$

which holds since $s < s'$ and $f \in \mathcal{L}(2sP_\infty)$. Repeating the division process until we find a quotient equal to zero shows that $\mathcal{T}_0(s, g) \subseteq \mathcal{T}_1(s, g)$. The other inclusions hold as in the case $i^* \geq 1$. \square

Combining (18) with both the above propositions lead to a better understanding of the dimension of the square of the dual of one-point Goppa-like AG codes.

Corollary 3.8. *With the same notation as in Proposition 3.7, set $k := \dim_{\mathbb{F}_q} C_{\mathcal{L}}(\mathcal{X}_{a,b}, \mathcal{P}, sP_\infty + (g))$. Then, for all $e \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$, the dimension of $\Gamma(\mathcal{P}, sP_\infty, g)^\perp$ is bounded from above by*

$$\dim_{\mathbb{F}_q} (\Gamma(\mathcal{P}, sP_\infty, g)^\perp)^{\star 2} \leq \left(\frac{m-1}{2} - e\right) mk^2 + \dim_{\mathbb{F}_q} \left(\sum_{i=0}^e \mathcal{T}_i(s, g)\right).$$

Moreover, if $i^* \leq e \leq \lfloor \frac{m}{2} \rfloor$ is the integer satisfying Equation (23), we have

$$\begin{aligned} \dim_{\mathbb{F}_q} \Gamma(\mathcal{P}, sP_\infty, g)^\perp \star 2 &\leq \left(\frac{m-1}{2} - e\right) mk^2 + ms'(q^e - q^{e-1} + 1) \\ &\quad + \dim_{\mathbb{F}_q} \left(\sum_{i=0}^{i^*-1} \mathcal{T}_i(s, g)\right) - \dim_{\mathbb{F}_q} \left(\mathcal{T}_e(s, g) \cap \sum_{i=0}^{i^*-1} \mathcal{T}_i(s, g)\right). \end{aligned}$$

Proof. From (6) and under the assumption on s and s' , we have

$$\begin{aligned} \dim_{\mathbb{F}_q} (\Gamma(\mathcal{P}, sP_\infty, g)^\perp)^{\star 2} &\leq \sum_{i=0}^{\lfloor m/2 \rfloor} \dim_{\mathbb{F}_q} \mathrm{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \\ &\leq \dim_{\mathbb{F}_q} \sum_{i=0}^e \mathcal{T}_i(s, g) + \sum_{i=e+1}^{\lfloor m/2 \rfloor} \mathrm{Tr}(\mathcal{C} \star \mathcal{C}^{q^i}) \\ &\leq \dim_{\mathbb{F}_q} \sum_{i=0}^e \mathcal{T}_i(s, g) + \left(\frac{m-1}{2} - e\right) mk^2, \end{aligned}$$

for all $e \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$. If $i^* \leq e \leq \lfloor \frac{m}{2} \rfloor$, Proposition 3.7 gives

$$\sum_{i=i^*}^e \mathcal{T}_i(s, g) = \mathcal{T}_e(s, g),$$

Consequently, we can write

$$\dim_{\mathbb{F}_q} \left(\sum_{i=0}^e \mathcal{T}_i(s, g)\right) = \dim_{\mathbb{F}_q} \left(\sum_{i=0}^{i^*-1} \mathcal{T}_i(s, g)\right) + \dim_{\mathbb{F}_q} \mathcal{T}_e(s, g) - \dim_{\mathbb{F}_q} \left(\mathcal{T}_e(s, g) \cap \sum_{i=0}^{i^*-1} \mathcal{T}_i(s, g)\right).$$

To finish the proof, we use the fact that $M_e(s, g) = \mathcal{R}(g^{q^e - q^{e-1} + 1})$ (see Proposition 3.6, 2), hence we have

$$\dim_{\mathbb{F}_q} \mathcal{T}_e(s, g) \leq m \cdot \dim_{\mathbb{F}_q} \mathcal{R}(g^{q^e - q^{e-1} + 1}) = ms'(q^e - q^{e-1} + 1).$$

\square

Despite the fact that the upper bound given in Corollary 3.8 can be numerically computed with the knowledge of the degree s and the function g , it is hard to give a close formula for any parameter, since the intersections of the trace codes $\mathcal{T}_i(s, g)$'s are hard to manipulate. However, if we suppose that $i^* = 0$, we can sharpen the above result.

Theorem 3.9. *Suppose that $s \geq (s' - s)q + 2\mathbf{g}_{a,b} - 1$ and let $e^* := \min \left(\lfloor \frac{m}{2} \rfloor, \left\lceil \log_q \left(\frac{k^2}{s'(q-1)^2} \right) \right\rceil + 1 \right)$. Then*

$$\dim_{\mathbb{F}_q}(\Gamma(\mathcal{P}, sP_\infty, g)^\perp)^{\star 2} \leq \binom{mk+1}{2} - \frac{m}{2}(k^2(2e^*+1) + k - 2s'(q^{e^*} - q^{e^*-1} + 1)).$$

Proof. The condition $s \geq (s' - s)q + 2\mathbf{g}_{a,b} - 1$ exactly implies that $i^* = 0$ and

$$\mathcal{T}_0(s, g) \subseteq \mathcal{T}_1(s, g) \subseteq \cdots \subseteq \mathcal{T}_{\lfloor \frac{m}{2} \rfloor}(s, g),$$

by Proposition 3.7. Thus, using Corollary 3.8 and the inequality $\dim_{\mathbb{F}_q} \mathcal{T}_e(s, g) \leq m \dim_{\mathbb{F}_{q^m}} \mathcal{R}(g^{q^e - q^{e-1} + 1})$, we get

$$\begin{aligned} \dim_{\mathbb{F}_q}(\Gamma(\mathcal{P}, sP_\infty, g)^\perp)^{\star 2} &\leq \min \left(ms'(q^e - q^{e-1} + 1) + \left(\frac{m-1}{2} - e \right) mk^2 \right) \\ &\leq \min \left(\frac{m}{2} (2s'(q^e - q^{e-1} + 1) + k^2(m-1) - 2k^2e) \right) \\ &\leq \min \left(\binom{mk+1}{2} - \frac{m}{2} (k^2(2e+1) + k - 2s'(q^e - q^{e-1} + 1)) \right). \end{aligned}$$

the minimum being taking over $e \in \{1, \dots, \lfloor \frac{m}{2} \rfloor\}$. To get the best bound, we need to maximize the function

$$F(e) = ek^2 - s'(q^e - q^{e-1} + 1)$$

over $\{1, \dots, \lfloor \frac{m}{2} \rfloor\}$. We compute the discrete derivative:

$$\begin{aligned} \Delta F(e) = F(e+1) - F(e) &= (e+1)k^2 - s'(q^{e+1} - q^e + 1) - ek^2 + s'(q^e - q^{e-1} + 1) \\ &= k^2 - s'q^{e-1}(q-1)^2. \end{aligned}$$

This function is decreasing with e , and the smallest value for which $\Delta F(e) \leq 0$ corresponds to its maximum. It is the smallest value of e such that $k^2 \leq s'q^{e-1}(q-1)^2$, *i.e.*

$$e = \left\lceil \log_q \left(\frac{k^2}{s'(q-1)^2} \right) \right\rceil + 1.$$

□

This theorem generalizes [MT23, Corollary 27]. Several computational experiments showed that when the code $\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathcal{X}_{a,b}, \mathcal{P}, sP_\infty + (g))$ is sufficiently random, the bound given in Theorem 3.9 is sharp, as claimed by Mora and Tillich [MT23, Remark 28] on $\mathcal{X} = \mathbb{P}^1$. Let us examine the sharpness of the bound in the following examples.

Example 3.10. The codes studied in Example 2.10 are one-point Goppa-like AG codes on $\mathcal{X} = \mathbb{P}^1$. The bound of Theorem 3.9 for $s = 9$ and $s = 10$ respectively gives 400 and 462, instead of 496 and 570. It is worth noting that this new upper bound is still far from the actual dimensions, namely 255 and 295. This comes for the fact that the functions g chosen in Example 2.10 are powers of x , hence their associated principal divisors (g) are supported only by P_0 and P_∞ .

Example 3.11. Set $q = 3$ and $m = 3$. We consider the curve \mathcal{X} over $\mathbb{F}_{q^m} = \mathbb{F}_{729}$ defined by

$$y^2 + y = x^3 + x + 2.$$

This elliptic curve \mathcal{X} is a particular case of $C_{2,3}$ curve with genus $\mathbf{g} = 1$. Set $s' = s + 1$ for $s \geq 0$, and $g \in \mathbb{F}_{q^m}(\mathcal{X})$ such that $g = x^\beta y^\alpha + g'$, where $a\beta + b\alpha = s + 1$; and g' is sampled at random in $\mathcal{L}(sP_\infty)$. For each such g , consider $\mathcal{P}_g := \mathcal{X}(\mathbb{F}_{q^m}) \setminus \text{Supp}(g)$. Using MAGMA, we then compare the true dimension of the square of the dual of $\mathcal{C}_g := \Gamma(\mathcal{P}_g, sP_\infty, g)$ with the upper bound given in Theorem 3.9 for $s \in \{4, \dots, 10\}$. Results can be found in Table 4.

In our computing experiments, we can check that g always has simple zeroes, hence $\left\lfloor \frac{sP_\infty + (g)}{3} \right\rfloor = -P_\infty$. This example illustrates how the bound can be sharp when we are outside the scope of Proposition 2.8.

In the last section, we will discuss how to efficiently choose the parameters of a one-point Goppa-like AG code in order to resist this distinguisher.

n	s	$\dim_{\mathbb{F}_q} \mathcal{C}_g$	$\dim_{\mathbb{F}_q} (\mathcal{C}_g)^{\ast 2}$	$\dim_{\mathbb{F}_q} (\mathcal{C}_g^\perp)^{\ast 2}$	Upper bound in Theorem 3.9
781	4	757	781	234	234
783	5	753	783	327	327
782	6	746	782	402	402
783	7	741	783	483	483
782	8	734	782	570	570
782	9	728	782	663	663
781	10	721	781	762	762

TABLE 4. Sharpness of the bound.

4. ANALYSIS OF THE DISTINGUISHER

In the previous section, we provided an (experimentally) sharp upper bound on the dimension of the square of the dual of a one-point Goppa-like code, which could lead to a distinguisher for the corresponding code. More precisely, let $\mathcal{C} := C_{\mathcal{L}}(\mathcal{X}_{a,b}, \mathcal{P}, sP_\infty + (g))$ be an AG code as above, with $\deg_{a,b}(g) = s' > s \geq 2\mathfrak{g}_{a,b} - 1$. We showed that if s and s' are such that $s \geq (s' - s)q + 2\mathfrak{g}_{a,b} - 1$, then

$$(26) \quad \dim_{\mathbb{F}_q} (\Gamma(\mathcal{P}, sP_\infty, g)^\perp)^{\ast 2} \leq \min \left(\frac{m}{2} \left(2s'(q^{e^*} - q^{e^*-1} + 1) + k^2(m - 1 - 2e^*) \right), n \right),$$

where $e^* := \left\lceil \log_q \left(\frac{k^2}{s'(q-1)^2} \right) \right\rceil + 1$. Thus, the code is distinguishable from a random one if the right hand-side of (26) is smaller than the length n of the code. It is possible to study when this case occurs, by starting to bound from above the maximal possible length: since $\mathcal{P} \cap \text{Supp}(g) = \emptyset$, this maximum is reached when $\mathcal{P} = \mathcal{X}_{a,b}(\mathbb{F}_{q^m}) \setminus \{P_\infty\}$ and g has no rational zero that is

$$n = \#\mathcal{P} = |\mathcal{X}_{a,b}(\mathbb{F}_{q^m})| - 1 \leq q^m + 2\mathfrak{g}_{a,b}\sqrt{q^m},$$

using the Hasse–Weil bound. In order to protect the code against the distinguisher, the parameters have to be chosen such that

$$(27) \quad \frac{m}{2} \left(2s'(q^{e^*} - q^{e^*-1} + 1) + k^2(m - 1 - 2e^*) \right) \geq q^m + 2\mathfrak{g}_{a,b}\sqrt{q^m}.$$

In what follows, we focus on two specific classes of $C_{a,b}$ curves. First, we determine the maximal (with respect to the dimension) codes we can distinguish in the case where $\mathcal{X}_{a,b}$ is an elliptic curve. This case is relevant since it is the closest to the case of classical Goppa codes, and we will see that our results are very similar to the one given in [MT23]. Next up, we focus on the particular case of the Hermitian curve, which also turns out to be a $\mathcal{X}_{a,b}$ curve. It is well-known to be a good candidate to construct efficient codes as it is a maximal curve. Due to its high genus, we then show that any one-point Goppa-like code defined on it cannot be distinguished.

4.1. High rate distinguishable codes in the case of elliptic curves. Let $\mathcal{X}_{a,b}$ be an elliptic curve, *i.e.* $a = 2$ and $b = 3$. For some set of parameters which produces codes of cryptographic size, we compute the maximal distinguishable value of s . To get close to the case of classical Goppa codes, we also fix $s' = s + 1$.

As it was noticed in [MT23] and as we can see above, we are only able to distinguish high rate codes. The smallest distinguishable rates are roughly the same as the one given in [MT23].

4.2. Codes on the Hermitian curve. As the Hermitian curve is a particular case of $C_{a,b}$ curve, we investigate the behaviour of one-point Goppa-like AG codes constructed on it with respect to our distinguisher. In particular, we show that all these codes resist to it, since (27) always holds in this setting, essentially because the genus of the Hermitian curve is too high with respect to the size of the field. Let us first recall some known results about the Hermitian curve ([Sti09]).

Let $m \geq 1$ be an even integer and denote by $q_0 := q^{m/2}$, so that $\mathbb{F}_{q^m} = \mathbb{F}_{q_0^2}$. The Hermitian curve \mathcal{H} over $\mathbb{F}_{q_0^2}$ is defined by the equation

$$\mathcal{H} : y^{q_0} + y = x^{q_0+1}.$$

Its genus is given by $\mathfrak{g}_{\mathcal{H}} = \frac{q_0(q_0-1)}{2}$ and it is a maximal curve, *i.e.* $\#\mathcal{H}(\mathbb{F}_{q_0^2}) = q_0^3 + 1$.

Proposition 4.1. *Suppose $s \geq (s' - s)q + 2\mathfrak{g}_{\mathcal{H}} - 1$. Then for any choice of g and \mathcal{P} , the one-point Goppa-like code $\Gamma(\mathcal{P}, sP_\infty, g)$ resists the distinguisher given in Theorem 3.9.*

q	m	n	Largest distinguishable s	Corresponding rate
2	12	4218	14	0,963
2	13	6688	18	0,982
3	7	2186	15	0,962
3	8	6393	24	0,977
5	5	3043	27	0,961
5	6	4500	22	0,971
5	6	6688	30	0,976
7	4	2395	27	0,957
7	5	4650	26	0,971
7	5	8192	37	0,979
17	3	4820	92	0,943

TABLE 5. Largest distinguishable Goppa-like AG code in elliptic case.

Proof. As discussed at the beginning of the section, the code cannot be distinguished whenever (27) holds. In this case, we know exactly the number of rational points, and thus the length n of the Goppa-like code is at most q_0^3 . Since m is even, we are left to prove that

$$(28) \quad \mathfrak{B}(e^*) := ms'(q^{e^*} - q^{e^*-1} + 1) + \left(\frac{m}{2} - e^*\right)mk^2 \geq q_0^3,$$

where $k := \dim_{\mathbb{F}_{q^m}} C_{\mathcal{L}}(\mathcal{H}, \mathcal{P}, sP_{\infty} + (g)) = s + 1 - \mathfrak{g}_{\mathcal{H}}$.

- If $e^* < \frac{m}{2}$, then $\mathfrak{B}(e^*) > mk^2$. Using the assumption on s and s' , we know that $s \geq 2\mathfrak{g}_{\mathcal{H}} + q - 1$. This yields $k \geq \mathfrak{g}_{\mathcal{H}} + q$ and thus

$$\begin{aligned} \mathfrak{B}(e^*) - q_0^3 &> m(\mathfrak{g}_{\mathcal{H}}^2 + 2\mathfrak{g}_{\mathcal{H}}q + q^2) - q_0^3 \\ &> \frac{m}{4}(q_0^4 - 2q_0^3 + q_0^2) + mq(q_0^2 - q_0 + q) - q_0^3 \\ &\geq \frac{1}{2}(q_0^4 - 2q_0^3 + q_0^2) + 4(q_0^2 - q_0 + 2) - q_0^3 \quad (m \geq 2 \text{ and } q \geq 2) \\ &> \frac{q_0}{2}(q_0^3 - 4q_0^2 + 9q_0 - 8) > 0, \end{aligned}$$

since $q_0 \geq 2$. Inequality (28) holds in this case.

- If $e^* = \frac{m}{2}$, then since $q_0 = q^{m/2}$, we have $\mathfrak{B}\left(\frac{m}{2}\right) = ms'(q_0 - q_0q^{-1} + 1)$. Moreover, $s' > s$ implies $s' \geq 2\mathfrak{g}_{\mathcal{H}} + q$, and

$$\begin{aligned} \mathfrak{B}\left(\frac{m}{2}\right) - q_0^3 &\geq m(2\mathfrak{g}_{\mathcal{H}} + q)(q_0 - q_0q^{-1} + 1) - q_0^3 \\ &\geq 2\left(q_0^2(q_0 - 1)\left(\frac{q-1}{q}\right) + q_0(q_0 - 1) + q_0(q - 1) + q\right) - q_0^3 \\ &\geq q_0^3\left(2\left(\frac{q-1}{q}\right) - 1\right) + 2q_0^2\left(1 - \left(\frac{q-1}{q}\right)\right) + 2(q_0(q - 2) + q). \end{aligned}$$

Clearly, the last expression is minimal for $q = 2$, so we finally gets

$$\mathfrak{B}\left(\frac{m}{2}\right) \geq q_0^2 + 4 > 0,$$

which proves Inequality (28) in this case and conclude the proof. \square

Consequently, in the light of Table 1, it is still reasonable to consider the Hermitian curve to build efficient SSAG code-based cryptosystem.

Acknowledgements. The authors would like to express their gratitude to the anonymous referees for relevant comments that lead to this improved version of the paper. This work was funded in part by the French National Research Agency through ANR *Barracuda* (ANR-21-CE39-0009). The first and the third authors are supported by the French government *Investissements d'Avenir* program ANR-11-LABX-0020-01. Through the LMB, the second author received support from the EIPHI Graduate School (contract ANR-17-EURE-0002).

REFERENCES

- [Bar18] Elise Barelli. *Étude de la sécurité de certaines clés compactes pour le schéma de McEliece utilisant des codes géométriques*. Theses, Université Paris Saclay (COMUE), December 2018.
- [BCC⁺22] Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, and al. Classic McEliece: conservative code-based cryptography: cryptosystem specification. <https://classic.mceliece.org/nist.html>, October 2022.
- [BRS21] Peter Beelen, Johan Rosenkilde, and Grigory Solomatov. Fast Encoding of AG Codes Over Cab Curves. *IEEE Transactions on Information Theory*, 67(3):1641–1655, 2021.
- [CCMZ15] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, 2015.
- [CMCP17] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. *IEEE Transactions on Information Theory*, 63(8):5404–5418, 2017.
- [Cou14] Alain Couvreur. Codes and the Cartier operator. *Proc. Amer. Math. Soc.*, 142(6):1983–1996, 2014.
- [CP20] Alain Couvreur and Isabella Panaccione. Power error locating pairs. *Des. Codes Cryptogr.*, 88(8):1561–1593, 2020.
- [Del75] Philippe Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Transactions on Information Theory*, 21(5):575–576, 1975.
- [Fau09] Cédric Faure. Etudes de systèmes cryptographiques construits à l’aide de codes correcteurs, en métrique de hamming et en métrique rang. *Ph.D. thesis, Ecole Polytechnique X*, 2009.
- [FGO⁺13] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate McEliece cryptosystems. *IEEE Trans. Inform. Theory*, 59(10):6830–6844, 2013.
- [FM08] Cédric Faure and Lorenz Minder. Cryptanalysis of the mceliece cryptosystem over hyperelliptic curves. *Proceedings of the eleventh International Workshop on Algebraic and Combinatorial Coding Theory*, pages 99–107, 2008.
- [GH00] O. Geil and T. Hoholdt. Footprints or generalized Bezout’s theorem. *IEEE Transactions on Information Theory*, 46(2):635–641, 2000.
- [HP95] Tom Hoholdt and Ruud Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 41(6, part 1):1589–1614, 1995. Special issue on algebraic geometry codes.
- [JM96] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Des. Codes Cryptogr.*, 8(3):293–307, 1996.
- [KN21] Sabira El Khalfaoui and Gábor P. Nagy. *Advances in Mathematics of Communications*, 15(2):219–226, 2021.
- [LC16] Phong Le and Sunil Chetty. On the dimension of algebraic-geometric trace codes. *Mathematics*, 4(2):32, 2016.
- [Min07] Lorenz Minder. Cryptography based on error correcting codes. *Ph.D. thesis, Ecole Polytechnique Fédérale de Lausanne*, 2007.
- [Miu93] S. Miura. Algebraic geometric codes on certain place curves. *Electronics and Communication in Japan (Part III: Fundamental Electronic Science)*, 76(12):1–13, 1993.
- [MS86] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. V. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1986.
- [MT23] Rocco Mora and Jean-Pierre Tillich. On the dimension and structure of the square of the dual of a Goppa code. *Designs, Codes and Cryptography*, 91(4):1351–1372, 2023.
- [Mum70] David Mumford. *Varieties defined by quadratic equations*. Questions on algebraic varieties, C.I.M.E., III Ciclo. Edizioni Cremonese, Rome, 1970.
- [NEK21] Gábor P. Nagy and Sabira El Khalfaoui. Towards the security of McEliece’s cryptosystem based on Hermitian subfield subcodes. *Prikl. Diskr. Mat. Suppl.*, (14):168–175, 2021.
- [Pet09] Christiane Peters. Information-set decoding for linear codes over \mathbb{F}_q . *Cryptology ePrint Archive*, 2009.
- [PJ14] Fernando Piñero and Heeralal Janwa. On the subfield subcodes of Hermitian codes. *Designs, codes and cryptography*, 70(1-2):157–173, 2014.
- [Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.
- [Sen94] Nicolas Sendrier. On the structure of a randomly permuted concatenated code. *EUROCODE’94.*, pages 169–173, 1994.
- [Sti09] Henning Stichtenoch. *Algebraic Function Fields and Codes*. Springer, 2nd edition edition, 2009.
- [Tia19] Yongge Tian. *Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry*, 60, 01 2019.
- [Wir88] Michael Wirtz. On the parameters of Goppa codes. *IEEE transactions on information theory*, 34(5):1341–1343, 1988.
- [ZC22] Jianguo Zhao and Li Chen. Parameters and Decoding Performance of Subfield Subcodes of One-Point Elliptic Codes. In *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pages 377–382, 2022.

UNIV RENNES, IRMAR - UMR 6625, F-35000 RENNES, FRANCE
 Email address: sabira.elkhalfaoui@univ-rennes1.fr

UNIVERSITÉ DE FRANCHE-COMTÉ, CNRS LMB, F-25000 BESANÇON, FRANCE
 Email address: mathieu.lhotel@univ-fcomte.fr

UNIV RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE
 Email address: jade.nardi@univ-rennes1.fr