Squares of bivariate Goppa codes

Wesley Basener, Giuseppe Cotardo, Jenna Krebs, Yihan Liu, Gretchen L. Matthews*, and Eric Ufferman

Department of Mathematics, Virginia Tech

Received: 22nd June 2023 | Accepted: 15th July 2023

Abstract *In this paper, we study squares of bivariate Goppa codes, as they relate to the Goppa code distinguishing problem for bivariate Goppa codes. Introduced in 2021, multivariate Goppa codes are subfield subcodes of certain evaluation codes defined by evaluating polynomials in m variables. The evaluation codes are augmented Cartesian codes, a generalization of Reed-Muller codes. Classical Goppa codes are obtained by taking $m = 1$. The multivariate Goppa code distinguishing problem is to distinguish efficiently a generator matrix of a multivariate Goppa code from a randomly drawn one. Because a randomly drawn code has a large square, codes with small squares may be considered distinguishable, revealing structure which facilitates private key recovery in a code-based cryptosystem.*

Keywords: Goppa code, McEliece cryptosystem, square

2010 Mathematics Subject Classification:

1 INTRODUCTION

Code-based cryptosystems originated with the McEliece cryptosystem in 1978 [14], soon followed by the Niederreiter cryptosystem [16], and are receiving current attention due to their potential to resist attacks facilitated or sped up by quantum algorithms. The McEliece cryptosystem which relies on binary Goppa codes is the basis for a current candidates in the fourth round of the NIST Post-Quantum Cryptography Standardization Process. The Goppa code distinguishing problem established in 2001 by Courtois, Finiasz, and Sendrier [3] is tied to the security of the McEliece public key cryptosystem [14]. The problem is to efficiently distinguish a generator matrix of a binary Goppa code from a randomly selected one. Squares of codes, taken with respect to a coordinate-wise product (sometimes called a Schur, component-wise, or star product), are connected to this problem. Since the work of Wieschebrink in 2010 [18] as well as that of Márquez-Corbella and Pellikaan [13], squares of codes have been considered as a tool for potential attacks on the code-based public key cryptosystems; see, for instance, [5], [4]. In particular, the strategy is to exploit the algebraic structure of the code underlying the code-based cryptosystem (such as the binary Goppa codes in McEleice or Neiderrieter) which may ultimately distinguish the code from a random one. The first successful application of this approach [18] was the attack on a cryptosystem based on subcodes of GRS codes [1]. This approach has been successful with high-rate Goppa codes [6], [7].

In this paper, we study squares of bivariate Goppa codes, as an initial step in considering a multivariate Goppa code distinguishing problem. Because a randomly drawn code has a large square (with high probability) [2, Theorem 2.3], codes with small squares may be considered distinguishable, revealing structure which facilitates private key recovery in a code-based cryptosystem. This work is motivated by the introduction of m-variate Goppa codes [8] which contain as a special case classical Goppa codes (by taking $m = 1$) as well as the recent work of Mora and Tillich [15] on the Goppa code distinguishing problem.

The multivariate Goppa code distinguishing problem is to distinguish efficiently a generator matrix of a bivariate Goppa code from a randomly drawn one. The univariate case was considered recently in Mora and Tillich [15], in which the authors study squares of alternate codes, a family of subfield subcodes of Reed-Solomon codes which contain Goppa codes. The multivariate Goppa codes are subfield subcodes of certain evaluation codes defined by evaluating polynomials in m variables. The evaluation codes are augmented Cartesian codes, a generalization of Reed-Muller codes. Classical Goppa codes are obtained by taking $m = 1$. Here, we make progress toward this larger goal by studying squares of bivariate Goppa codes. We show that unlike their univariate counterparts, the associated evaluation codes do not have squares of the same form. However, their dimensions are bounded above by dimensions of such codes, presenting the possiblity of a distinguisher attack.

This paper is organized as follows. Section 2 reviews basic coding theory terminology as well as the particular families of codes to be considered in the paper. Section 3 includes the results. A conclusion is given in Section 4.

*Corresponding Author: gmatthews@vt.edu

2 PRELIMINARIES

In this section, we introduce the code operations and constructions that will be used in the remainder of the paper. First, we recall some basic definitions and notation. An $[n, k, d]$ code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ in which any two distinct codewords differ in at least d coordinates. Its dual is $C^\perp = \left\{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ for all } c \in C\right\}$ where $v \cdot c = \sum_{i=1}^n v_i c_i$ is the standard dot product. A generator matrix for C is any matrix which has C as its row space. Often, we take a generator matrix for an $[n, k, d]$ code over $\mathbb{F}_q$ to be a $k \times n$ matrix whose rows are a basis for the code as an $\mathbb{F}_q$-vector space. The coordinates of a code of length n are indexed by elements of the set $[n] := \{1, \ldots, n\}$. The set of nonnegative integers is denoted by $\mathbb{N}$, the set of $m \times n$ matrices over $\mathbb{F}_q$ by $\mathbb{F}_q^{m\times n}$, and $\mathbb{F}_q^n := \mathbb{F}_q^{1\times n}$.

2.1 CODE OPERATIONS

In this subsection, we review basic operations and make some relevant observations. We will consider codes over the finite field $\mathbb{F}_{q^t}$ with q^t elements as well as codes over its subfield $\mathbb{F}_q$, so the extension

$$\begin{array}{c} \mathbb{F}_{q^t} \\ | \, t \\ \mathbb{F}_q \end{array}$$

will play a crucial role. Given an $[n, k, d]$ code $C \subseteq \mathbb{F}_{q^t}^n$, its subfield subcode over $\mathbb{F}_q$ is

$$C_{|\mathbb{F}_q} := \left\{c \in C : c \in \mathbb{F}_q^n\right\} = C \cap \mathbb{F}_q^n$$

which is an $[n, \geq k - t\,(n-k)\,, \geq d]$ code over $\mathbb{F}_q$. Another way to produce a code over $\mathbb{F}_q$ from one over $\mathbb{F}_{q^t}$ is via the field trace. Recall that the field trace with respect to the extension $\mathbb{F}_{q^t}/\mathbb{F}_q$ is given by

$$\begin{array}{rccc} \mathrm{tr}\colon & \mathbb{F}_{q^t} & \to & \mathbb{F}_q \\ & a & \mapsto & a^{q^{t-1}} + \cdots + a^{q^0}. \end{array}$$

The trace code of C is

$$\mathrm{tr}\,(C) := \{(\mathrm{tr}\,(c_1), \ldots, \mathrm{tr}\,(c_n)) : (c_1, \ldots, c_n) \in C\},$$

which is an $[n, k', d']$ code over $\mathbb{F}_q$ where $k \leq k' \leq tk$ and $d' \leq d$ by [11, Ch. 7. §7.]. Delsarte's Theorem relates these two constructions which yield codes over $\mathbb{F}_q$ from those over $\mathbb{F}_{q^t}$:

$$C_{|\mathbb{F}_q} = \left(\mathrm{tr}\left(C^\perp\right)\right)^\perp.$$

The multivariate Goppa codes are related to tensor products of other codes. The tensor product of an $[n_1, k_1]$ code C_1 with

$$G_1 = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n_1} \\ a_{21} & a_{22} & \cdots & a_{2n_1} \\ \vdots & \vdots & & \vdots \\ a_{k_1 1} & a_{k_1 2} & \cdots & a_{k_1 n_1} \end{pmatrix} \in \mathbb{F}_2^{k_1 \times n_1}$$

and an $[n_2, k_2]$ code C_2 with generator matrix $G_2 \in \mathbb{F}_2^{k_2\times n_2}$ is the code with a generator matrix

$$G_1 \otimes G_2 = \begin{bmatrix} a_{11}G_2 & a_{12}G_2 & \cdots & a_{1n_1}G_2 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2n_1}G_2 \\ \vdots & \vdots & & \vdots \\ a_{k_1 1}G_2 & a_{k_1 2}G_2 & \cdots & a_{k_1 n_1}G_2 \end{bmatrix} \in \mathbb{F}_2^{k_1 k_2 \times n_1 n_2}.$$

As described in Section 1, coordinate-wise products of codes have played a role in the analysis of some code-based cryptosystems; this natural operation has also recently been used in secure distributed matrix multiplication [12]. We note the recent work by Mora and Tillich which collects useful information about these operations [15].

Definition 1. *The star product, also called the Schur product or coordinate-wise product, of vectors $u, v \in \mathbb{F}_q^n$ is*

$$u \star v := (u_1 v_1, \ldots, u_n v_n) \in \mathbb{F}_q^n.$$

The star product (or Schur product or coordinate-wise product) of two codes C and C' over $\mathbb{F}_q$ of length n over $\mathbb{F}_q$ is

$$C \star C' = \langle c \star c' : c \in C, c' \in C' \rangle,$$

the $\mathbb{F}_q$-span of the coordinate-wise products of codewords of C and C'.

Notice that the star product of two codes of length n is also a code of length n over the same alphabet. We are most interested in the square of a code C, meaning the star product of a code with itself:

$$C^{\star 2} := C \star C.$$

Given an $[n, k, d]$ code C, its square $C^{\star}2$ is a code of length n and

$$\dim C^{\star 2} \leq \min\left\{n, \binom{k+1}{2}\right\}.$$

According to the following result given by Cascudo, Cramer, Mirandola, and Zémor in 2015, even more can be said for random codes.

Proposition 1. *[2, Theorem 2.3] Let $n : \mathbb{N} \to \mathbb{N}$ be such that $n(k) \geq \binom{k+1}{2}$. Then for some positive real number δ and k large enough,*

$$\Pr\left[\dim C^{\star 2} = \binom{k+1}{2}\right] \geq 1 - 2^{-\delta\left(n(k) - \binom{k+1}{2}\right)}$$

where C is chosen uniformly at random from the family of all $[n(k), k]$ codes over $\mathbb{F}_q$ whose generator matrices are in systematic form.

Loosely speaking, Proposition 1 states that a random code C over $\mathbb{F}_q$ of length n with $C^{\star 2} \neq \mathbb{F}_q^n$ has dimension as large as possible, meaning

$$\dim C^{\star 2} = \binom{k+1}{2} \tag{1}$$

However, as we will see in Section 3, particular families of linear codes fail to achieve the dimension of the square given in Equation 1. As such, the square can serve as a distinguisher from a random code. Before establishing this, we first introduce the code families that will be useful in this paper.

2.2 CODE CONSTRUCTIONS

Each of the codes we consider may be built from an evaluation code, which is the image of a map of the form

$$\begin{array}{rccc} \mathrm{ev}_{S,\lambda}: & V & \to & \mathbb{F}_q^n \\ & f & \mapsto & (\lambda_1 f(s_1), \ldots, \lambda_n f(s_n)) \end{array}$$

where $\lambda \in (\mathbb{F}_q^*)^n$,

$$V = \left\{f : S \to \mathbb{F}_q\right\}$$

is a vector space of functions taking values in $\mathbb{F}_q$ when evaluated at elements $S := \{s_1, \ldots, s_n\}$. For instance, a $[n, k]$ generalized Reed-Solomon code

$$GRS(S, k, \lambda) = \mathrm{ev}_{S,\lambda}\left(\mathbb{F}_q[x]_{<k}\right)$$

where $\mathbb{F}_q[x]_{<k}$ is the set of polynomials in the indeterminate x of degree at most $k-1$ and $S \subseteq \mathbb{F}_q$. The $[q^m, \sum_{i=0}^{r}\binom{m}{i}, q^{m-r}]$ Reed-Muller code over $\mathbb{F}_q$ is

$$RM(r, m) = ev_{\mathbb{F}_q^m, 1}\left(\mathbb{F}_q[x_1, \ldots, x_m]_{\leq r}\right)$$

where $\mathbb{F}_q[x_1, \ldots, x_m]_{\leq r}$ is the set of polynomials in the m indeterminates of total degree at most r and $1 \in \mathbb{F}_q^n$ is the all-ones vector.

More generally, we may consider as an evaluation set

$$S = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m,$$

a Cartesian product of subsets of the alphabet $\mathbb{F}_{q^t}$. For $i \in [m]$, let $n_i = |S_i|$. For an integer vector $a \in \mathbb{N}^m$, $x^a := x_1^{a_1} \ldots x_m^{a_m} \in \mathbb{F}_{q^t}[x_1, \ldots, x_m]$. Let $L \in \mathbb{F}_{q^t}[x_1, \ldots, x_m]$ be given by $L(x_1, \ldots, x_m) := \prod_{j=1}^{m} L'_j(x_j)$ where

$$L_j(x_j) := \prod_{s \in S_j}(x_j - s) \in \mathbb{F}_{q^t}[x_j]$$

and $L'_j(x_j)$ denotes the formal derivative of $L_j(x_j)$.Given

$$g := g_1(x_1) \cdots g_m(x_m) \in \mathbb{F}_{q^t}[x_1, \ldots, x_m]$$

such that $g(s) \neq 0$ for all $s \in S$, define a set of exponent vectors

$$\mathcal{A}_g := \prod_{j\in[m]} \{0,\dots,n_j-1\} \setminus \prod_{j\in[m]} \{n_j - \deg g_j,\dots,n_j-1\}$$

and a set of multivariate polynomials

$$\mathcal{L}\left(\mathcal{A}_g\right) = \left\langle x^a : a \in \mathcal{A}_g \right\rangle \subseteq \mathbb{F}_{q^t}[x_1,\dots,x_m].$$

These ingredients allow for defining particularly useful evaluation codes, called augmented Cartesian codes [10].

Definition 2. *Given $S \subseteq \mathbb{F}_{q^t}$ and L, $g := g_1(x_1)\dots g_m(x_m) \in \mathbb{F}_{q^t}[x_1,\dots,x_m]$ as above, the augmented Cartesian code defined by S and g is*

$$ACar(S,g) = \mathrm{ev}_{S,\lambda}\left(\mathcal{L}\left(\mathcal{A}_g\right)\right)$$

where $\lambda_i := \frac{L(s_i)}{g(s_i)}$ for all $i \in [n]$.

Example 1. *Let $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ where $\alpha^3+\alpha+1=0$. Suppose $S_1 = \left\{0,1,\alpha,\alpha+1,\alpha^2\right\}$, $S_2 = \{0,1,\alpha,\alpha+1\} \subseteq \mathbb{F}_8$, $g_1(x_1) = (x_1-\alpha^2+\alpha)(x_1-(\alpha^2+1))(x_1-(\alpha^2+\alpha+1)) \in \mathbb{F}_8[x_1]$, and $g_2(x_2) = (x_2-\alpha^2+\alpha)(x_2-(\alpha^2+1)) \in \mathbb{F}_8[x_2]$. Then $n_1 = \mid S_1 \mid = 5$, $n_2 = \mid S_2 \mid = 4$, $\deg g_1 = 3$, and $\deg g_2 = 2$. As a result,*

$$\mathcal{A}_g = [0,4]\times[0,3] \setminus [2,4]\times[2,3].$$

Consequently, $ACar(S,g)$ is a $[20,14]$ code.

The exponent vectors that give rise to codewords in $ACar(S,g)$ are pictured in Figure 1 which also gives insight into the origins of the names of the codes. Here, considering only codewords that arise from evaluating functions $x_1^{a_1}x_2^{a_2}$ with $a_1+a_2 \leq 3$ is similar to the functions that define a Reed-Muller code. The code featured in this example is augmented in that there are also codewords from functions $x_1x_2^3$, $x_1^3x_2$, x_2^4, x_1^4, and $x_1^4x_2$. It also differs from a Reed-Muller code in that the evaluation set is a proper subset of $\mathbb{F}_8^2$.

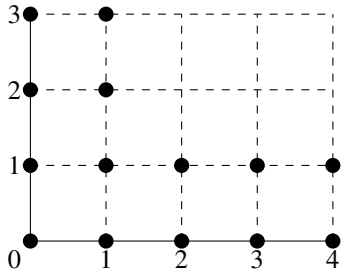

Figure 1: Exponents $(a_1,a_2) \in \mathcal{A}_g$ for the augmented Cartesian code in Example 1, meaning those with monomials $x_1^{a_1}x_2^{a_2}$ whose evaluation defines codewords

Remark 1. *Observe that for $m=2$, any set of exponent vectors $\mathcal{A}_g$ for an augmented Cartesian code is of the form $A \setminus B$ where A and B are both boxes, meaning direct products of intervals. This will be a useful fact when understanding the squares of these codes.*

We note that generalized Reed-Solomon codes are augmented Cartesian codes and Reed-Muller codes are subcodes of augmented Cartesian codes; in fact, these codes were inspired by designing Reed-Muller-type codes with higher rates [9]. Recall that a classical Goppa code, and more generally an alternate code, is a subfield subcode of a generalized Reed-Solomon code. Similarly, a multivariate Goppa code is a subfield subcode of an augmented Cartesian code. More precisely, we have the following definition.

Definition 3. *Given $g = g_1(x_1)\dots g_m(x_m) \in \mathbb{F}_{q^t}[x_1,\dots,x_m]$ and $S \subseteq \mathbb{F}_{q^t}^m$ such that $g(s) \neq 0$ for all $s \in S$, the multivariate Goppa code with defining polynomial g and evaluation set S is*

$$\Gamma(S,g) = ACar(S,g)_{|\mathbb{F}_q}.$$

In particular, the bivariate Goppa code defined by $g = g_1(x_1)g_2(x_2)$ is

$$\Gamma(S,g) = ev_{S_1\times S_2,\lambda}\left(\mathcal{A}_g\right)_{|\mathbb{F}_q}$$

where

$$\mathcal{A}_g = [0,n_1-1]\times[0,n_2-1] \setminus \{n_1-\deg g_1, n_1-1\}\times\{n_2-\deg g_2, n_2-1\}.$$

Remark 2. *The multivariate Goppa code $\Gamma(S, g)$ is a code over $\mathbb{F}_q$ of length $n = \mid S \mid$, dimension k satisfying $n - \deg g \leq k \leq t(n - \deg g)$, and minimum distance at least $\min\{\deg g_j + 1 : j \in [m]\}$ [8, Corollary 15].*

Multivariate Goppa are intimately related to generalized Reed-Solomon codes.

Lemma 1. *[8, Corollary 15] The dual of an multivariate Goppa code defined by $S = S_1 \times S_n \subseteq \mathbb{F}_{q^t}^m$ and $g = g_1(x_1) \dots g_m(x_m) \in \mathbb{F}_{q^t}[x_1, \dots, x_m]$ such that $g(s) \neq 0$ for all $s \in S$ is*

$$\Gamma(S, g)^{\perp} = \mathrm{tr}\left(\bigotimes_{i=1}^{m} GRS\left(S_j, \deg g_j, \left(g_j(s_1)^{-1}, \dots, g_j(s_n)^{-1}\right)\right)\right).$$

This fact may prove useful in examining the square of the dual of multivariate Goppa codes, as considered in [15], though we focus our present attention on the bivariate Goppa codes themselves.

3 BOUNDING SQUARES

In this section, we consider squares of bivariate Goppa codes and their relatives, such as the augmented Cartesian codes from which they arise. To begin, we recall the well-known fact that squares of generalized Reed-Solomon codes are again generalized Reed-Solomon codes. In particular,

$$GRS(S, k, \lambda)^{\star 2} = GRS(S, 2k - 1, \lambda \star \lambda),$$

as suggested by the facts that

$$(\lambda_1 f(s_1), \dots, \lambda_n f(s_n)) \star \left(\lambda_1' h(s_1), \dots, \lambda_n' h(s_n)\right) = \left(\lambda_1 \lambda_1' fh(s_1), \dots, \lambda_n \lambda_n' fh(s_n)\right)$$

and for $f, h \in \mathbb{F}_q[x]_{<k}$, $\deg(fh) \leq 2(k-1) = 2k - 2$. Similarly, the square of a Reed-Muller code $RM(r, m)$ satisfies

$$RM(r, m)^{\star 2} = RM(2r, m)$$

as demonstrated in [17, Proposition 2]. Similar behavior has been observed for algebraic geometry codes defined by divisors of degree at least $2g - 1$ on a curve of genus g [5].

We now consider the squares of augmented Cartesian codes with $m = 2$.

Lemma 2. *The square of an augmented Cartesian code defined by $S \subseteq \mathbb{F}_{q^t}^2$ and $g = g_1(x_1)g_2(x_2) \in \mathbb{F}_{q^t}[x_1, x_2]$ such that $g(s) \neq 0$ for all $s \in S$ is*

$$ACar(S, g)^{\star 2} = \left\{\left(\lambda_1^2 f(s_1), \dots, \lambda_n^2 f(s_n)\right) : f \in \mathcal{L}\left(\mathcal{A}_g'\right)\right\}$$

where

$$\mathcal{A}_g' = [0, 2(n_1 - 1)] \times [0, 2(n_2 - 1)] \setminus (U \cup L),$$

with

$$U := [2(n_1 - \deg g_1) - 1, 2(n_1 - 1)] \times [2n_2 - \deg g_2 - 1, 2(n_2 - 1)]$$

and

$$L := [2n_1 - \deg g_1 - 1, 2(n_1 - 1),] \times [2(n_2 - \deg g_2) - 1, 2(n_2 - 1)].$$

Proof. We first show that $x^a x^b \in \mathcal{L}\left(\mathcal{A}_g'\right)$ for all $a, b \in \mathcal{A}_g$. Hence, we must prove that $a + b \in \mathcal{A}_g'$. Suppose not. Then $a + b \in U$ or $a + b \in L$. Without loss of generality, we may assume $a + b \in U$, meaning $(a_1 + b_1, a_2 + b_2) \in U$. It follows that $a_1 + b_1 \in [2(n_1 - \deg g_1) - 1, 2(n_1 - 1)]$ and $a_2 + b_2 \in [2n_2 - \deg g_2 - 1, 2(n_2 - 1)]$. However, this contradicts that $(a_1, a_2), (b_1, b_2) \in \mathcal{A}_g$, establishing that $a + b \in \mathcal{A}_g'$.

It remains to prove that any $x_1^{a_1} x_2^{a_2} \in \mathcal{L}\left(\mathcal{A}_g'\right)$ can be written as $x_1^{b_1} x_2^{b_2} x_1^{b_1'} x_2^{b_2'}$ with $(b_1, b_2), (b_1', b_2') \in \mathcal{A}_g$. Suppose $(a_1, a_2) \in [0, n_1 - 1] \times [0, 2(n_2 - 1)]$. If $a_2 \leq n_2 - 1$, then $(a_1, a_2) \in \mathcal{A}_g$ and $x_1^{a_1} x_2^{a_2} = x_1^{a_1} x_2^{a_2} x_1^0 x_2^0$. Note that

$$x_1^{a_1} x_2^{a_2} = x_1^{a_1} x_2^{n_2 - 1} x_1^0 x_2^{a_2 - (n_2 - 1)}$$

If $a_2 > n_2 - 1$, then $a_2 - (n_2) - 1) \leq n_2 - 1$ and $x_1^{a_1} x_2^{n_2 - 1}, x_1^0 x_2^{a_2 - (n_2 - 1)} \in \mathcal{A}_g$. A similar argument holds if $(a_1, a_2) \in [0, 2(n_1 - 1)] \times [0, n_2 - 1]$. Finally, suppose that $(a_1, a_2) \in [n_1, 2n_1 - \deg g_1 - 2] \times [n_2, 2n_2 - \deg g_2 - 2]$. Then

$$x_1^{a_1} x_2^{a_2} = x_1^{n_1 - 1} x_2^{a_2 - (n_2 - 1)} x_1^{a_1 - (n_1 - 1)} x_2^{n_2 - 1}.$$

Noting that $a_1 - n_1 + 1 \leq n_1 - \deg g_1 - 1$ and $a_2 - n_2 + 1 \leq n_2 - \deg g_2 - 1$, we see that $x_1^{n_1 - 1} x_2^{a_2 - (n_2 - 1)}, x_1^{a_1 - (n_1 - 1)} x_2^{n_2 - 1} \in \mathcal{A}_g$, completing the proof. □

Corollary 1. *The square of an augmented Cartesian code with $m = 2$ is an evaluation code, but it is not necessarily of the form whose subfield subcode defines a bivariate Goppa code.*

Example 2. *Consider the code $ACar(S, g)$ from Example 1. According to Theorem 2, $ACar(S, g)^{\star 2} = ev_{S,\mathcal{A}^2}\left(\mathcal{A}'_g\right)$ where*

$$A'_g = [0, 8] \times [0, 6] \setminus ([3, 8] \times [5, 6] \cup [6, 8] \times [3, 6])$$

The exponent vectors that give rise to codewords in $ACar(S, g)$ are pictured in Figure 2. Notice that the complement

$$[3, 8] \times [5, 6] \cup [6, 8] \times [3, 6]$$

does not have the box form specified in Remark 1. Hence, the square of the augmented Cartesian code from which the bivariate Goppa code $\Gamma(S, g)$ is obtained is not an augmented Cartesian code that defines a bivariate Goppa code.

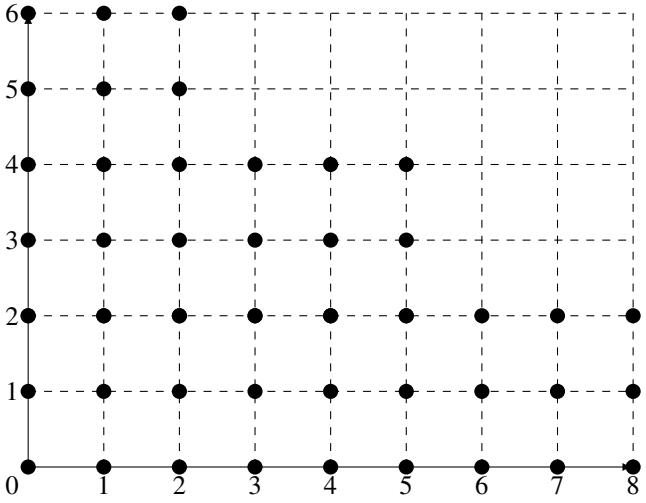

Figure 2: Exponents $(a_1, a_2) \in \mathcal{A}'_g$ for the square of the augmented Cartesian code in Example 1, meaning those with monomials $x_1^{a_1} x_2^{a_2}$ whose evaluation defines codewords in the square

Remark 3. *Note that, unlike Reed-Solomon and Reed-Muller codes, the square of an augmented Cartesian code $A(S, g)$ is not necessarily of the same form. Even so, its dimension is bounded above by that of a code of the same form.*

Because the bivariate Goppa codes are subfield subcodes of augmented Cartesian codes, we next consider the interplay of the square and the subfield subcode operations.

Proposition 2. *Given a code C over $\mathbb{F}_{q^t}$,*

$$\left(C_{|\mathbb{F}_q}\right)^{\star 2} \subseteq \left(C^{\star 2}\right)_{|\mathbb{F}_q}.$$

Proof. Consider a code C over $\mathbb{F}_{q^t}$, and let n denote its length. Fix a basis $\{b_1, \ldots, b_l\}$ for $C_{|\mathbb{F}_q}$. Then $b_i \in C \cap \mathbb{F}_q^n$ for all $i \in [n]$. Now suppose $x \in \left(C_{|\mathbb{F}_q}\right)^{\star 2}$. Hence, $x = \sum_{i,j \in [l]} a_{ij} \left(b_i \star b_j\right)$ for some $a_{ij} \in \mathbb{F}_q$. Clearly, by construction, $x \in C^{\star 2}$ and $x \in \mathbb{F}_q^n$ by definition. Hence, $x \in \left(C^{\star 2}\right)_{|\mathbb{F}_q}$. □

Remark 4. *We note that the containment in Proposition 2 may be strict. Consider, for instance, the code*

$$C = \left\langle (1, \alpha^2) \right\rangle \subseteq \mathbb{F}_9^2$$

where $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ and $\alpha^2 + 2\alpha + 2 = 0$. Then

$$C = \{(1, \alpha + 1), (\alpha, 2\alpha + 1), (\alpha + 1, 2), (2\alpha + 1, 2\alpha), (2, 2\alpha + 2), (2\alpha, \alpha + 2), (2\alpha + 2, 1), (\alpha + 2, \alpha), (0, 0)\}.$$

It follows that

$$C_{|\mathbb{F}_3} = \{(0,0)\}$$

so that

$$\left(C_{|\mathbb{F}_3}\right)^{\star 2} = \{(0,0)\}.$$

However,

$$(\alpha+1,2) \star (\alpha+1,2) = (2,1) \in C^{\star 2} \cap \mathbb{F}_3^2 = \left(C^{\star 2}\right)_{|\mathbb{F}_3}.$$

Hence,

$$\left(C_{|\mathbb{F}_3}\right)^{\star 2} \subsetneq \left(C^{\star 2}\right)_{|\mathbb{F}_3}.$$

Theorem 1. *The square of a bivariate Goppa code with evaluation set $S = S_1 \times S_2 \subseteq \mathbb{F}_{q^t}^2$ and defining polynomial $g = g_1(x_1)g_2(x_2) \in \mathbb{F}_{q^t}[x_1, x_2]$ such that $g(s) \neq 0$ for all $s \in S$ is*

$$\Gamma(S,g)^{\star 2} \subseteq \left(ACar\,(S,g)^{\star 2}\right)_{|\mathbb{F}_q} = \left(ev_{S,\lambda^2}\left(\mathcal{L}\left(\mathcal{A}'_g\right)\right)\right)_{|\mathbb{F}_q}.$$

Proof. Recall that $\Gamma(S,g) = ACar(S,g)_{|\mathbb{F}_q}$. By Proposition 2, its square satisfies

$$\Gamma(S,g)^{\star 2} \subseteq \left(ACar(S,g)^{\star 2}\right)_{|\mathbb{F}_q}.$$

The result now follows from Lemma 2. □

Theorem 1 allows us to provide a bound on the dimension of the square of a bivariate Goppa code.

Corollary 2. *The square of the bivariate Goppa code $\Gamma(S,g)$ with evaluation set $S = S_1 \times S_2 \subseteq \mathbb{F}_{q^t}^2$ and defining polynomial $g = g_1(x_1)g_2(x_2) \in \mathbb{F}_{q^t}[x_1, x_2]$ such that $g(s) \neq 0$ for all $s \in S$ has dimension at most $(2n_1 - 1)(2n_2 - 1) - 3\deg g_1 \deg g_2 - \deg g_1$.*

Proof. Notice that the dimension of $\Gamma(S,g)$ is at most $|\,\mathcal{A}'_g\,|$. Then observe that

$$\begin{aligned}
|\,\mathcal{A}'_g\,| &= (2n_1-1)(2n_2-1) - |\,U\,| - |\,L \setminus U\,| \\
&= (2n_1-1)(2n_2-1) \\
&\quad -(2n_1 - 2 - 2(n_1 - \deg g_1 - 1))(2n_2 - 2 - (2n_2 - \deg g_2 - 1) + 1) \\
&\quad -(2n_1 - 2 - (2n_1 - \deg g_1 - 1) + 1)(2n_2 - \deg g_2 - 1 - 2(n_2 - \deg g_2 - 1)) \\
&= (2n_1-1)(2n_2-1) - 3\deg g_1 \deg g_2 - \deg g_1.
\end{aligned}$$

□

4 CONCLUSION

In this paper, we considered squares of bivariate Goppa codes. We demonstrated that they arise from augmented Cartesian codes in two variables whose squares are not in general of the same form. By considering the relationship between the squaring and subfield subcode operations, we obtain a bound on the dimensions of squares of bivariate Goppa codes. It remains to determine the squares of m-variate Goppa codes for $m > 3$ as well as to determine their roles in potential attacks on a code-based cryptosystem.

ACKNOWLEDGMENT

This work was supported by the Commonwealth Cyber Initiative and the MAA Tensor Foundation. The work of the second and fifth authors is supported in part by NSF DMS-2201075.

REFERENCES

[1] Thierry P. Berger and Pierre Loidreau. "How to Mask the Structure of Codes for a Cryptographic Use". In: *Designs, Codes and Cryptography* 35 (2005), pp. 63–79. DOI: 10.1007/s10623-003-6151-2.

[2] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. "Squares of Random Linear Codes". In: *IEEE Transactions on Information Theory* 61.3 (2015), pp. 1159–1173. DOI: 10.1109/TIT.2015.2393251.

[3] Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier. "How to Achieve a McEliece-Based Digital Signature Scheme". In: *Advances in Cryptology — ASIACRYPT 2001*. Ed. by Colin Boyd. Springer Berlin Heidelberg, 2001, pp. 157–174. ISBN: 978-3-540-45682-7.

[4] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. "Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed–Solomon codes". In: *Designs, Codes and Cryptography* 73 (2014), pp. 641–666. DOI: 10.1007/s10623-014-9967-z.

[5] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. "Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes". In: *IEEE Transactions on Information Theory* 63.8 (2017), pp. 5404–5418. DOI: 10.1109/TIT.2017.2712636.

[6] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. "A Distinguisher for High Rate McEliece Cryptosystems". In: *2011 IEEE Information Theory Workshop*. 2011, pp. 282–286. DOI: 10.1109/ITW.2011.6089437.

[7] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. "A Distinguisher for High-Rate McEliece Cryptosystems". In: *IEEE Transactions on Information Theory* 59.10 (2013), pp. 6830–6844. DOI: 10.1109/TIT.2013.2272036.

[8] Hiram H. López and Gretchen L. Matthews. "Multivariate Goppa Codes". In: *IEEE Transactions on Information Theory* 69.1 (2023), pp. 126–137. DOI: 10.1109/TIT.2022.3201692.

[9] Hiram H. López, Gretchen L. Matthews, and Daniel Valvo. "Augmented Reed-Muller Codes of High Rate and Erasure Repair". In: *2021 IEEE International Symposium on Information Theory (ISIT)*. 2021, pp. 438–443. DOI: 10.1109/ISIT45174.2021.9517854.

[10] Hiram H. López, Gretchen L. Matthews, and Daniel Valvo. "Erasures Repair for Decreasing Monomial-Cartesian and Augmented Reed-Muller Codes of High Rate". In: *IEEE Transactions on Information Theory* (2021). DOI: 10.1109/TIT.2021.3130096.

[11] Florence Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-correcting Codes*. North-Holland, 1977.

[12] Okko Makkonen and Camilla Hollanti. "General Framework for Linear Secure Distributed Matrix Multiplication with Byzantine Servers". In: *2022 IEEE Information Theory Workshop (ITW)*. 2022, pp. 143–148. DOI: 10.1109/ITW54588.2022.9965828.

[13] Irene Márquez-Corbella and Ruud Pellikaan. "Error-Correcting Pairs: A New Approach to Code-Based Cryptography". In: *20th Conference on Applications of Computer Algebra (ACA 2014)*. New York, United States, July 2014. URL: https://hal.science/hal-01088433.

[14] Robert J. McEliece. "A Public-Key Cryptosystem Based On Algebraic Coding Theory". In: *Deep Space Network Progress Report* 44 (Jan. 1978), pp. 114–116.

[15] Rocco Mora and Jean-Pierre Tillich. "On the Dimension and Structure of the Square of the Dual of a Goppa Code". In: *Designs, Codes and Cryptography* 91 (2023), pp. 1351–1372. DOI: 10.1007/s10623-022-01153-w.

[16] Harald Niederreiter. "Knapsack-Type Cryptosystems and Algebraic Coding Theory". In: *Problems of Control and Information Theory* 15.2 (1986), pp. 157–166.

[17] Ayoub Otmani and Hervé Talé Kalachi. "Square Code Attack on a Modified Sidelnikov Cryptosystem". In: *Codes, Cryptology, and Information Security*. Ed. by Said El Hajji, Abderrahmane Nitaj, Claude Carlet, and El Mamoun Souidi. Cham: Springer International Publishing, 2015, pp. 173–183. ISBN: 978-3-319-18681-8.

[18] Christian Wieschebrink. "Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes". In: *Post-Quantum Cryptography*. Ed. by Nicolas Sendrier. Springer Berlin Heidelberg, 2010, pp. 61–72. ISBN: 978-3-642-12929-2.