MULTIVARIATE GOPPA CODES

HIRAM H. LÓPEZ AND GRETCHEN L. MATTHEWS

Abstract. In this paper, we introduce multivariate Goppa codes, which contain as a special case the well-known, classical Goppa codes. We provide a parity check matrix for a multivariate Goppa code in terms of a tensor product of generalized Reed-Solomon codes. We prove that multivariate Goppa codes are subfield subcodes of augmented Cartesian codes. By showing how this new family of codes relates to tensor products of generalized Reed-Solomon codes and augmented codes, we obtain information about the parameters, subcodes, duals, and hulls of multivariate Goppa codes. We see that in certain cases, the hulls of multivariate Goppa codes (resp., tensor product of generalized Reed-Solomon codes), are also multivariate Goppa codes (resp. tensor product of generalized Reed-Solomon codes). We utilize the multivariate Goppa codes to obtain entanglement-assisted quantum error-correcting codes and to build families of long LCD, self-dual, or self-orthogonal codes.

1. Introduction

Goppa codes were introduced in 1971 by V. D. Goppa [14, 15] using a polynomial $g(x)$, called a generator polynomial, over the finite field $\mathbb{F}_q$ with q elements. Properties of a Goppa code are tied to those of the generator polynomial. For instance, such codes have minimum distance at least $\deg(g)+1$. Many Goppa codes have parameters exceeding the Gilbert bound. Moreover, Goppa codes have efficient decoding algorithms. The McEliece cryptosystem, of current interest as the basis for one of only remaining candidates in the NIST Post-Quantum Cryptography Standardization [1, 4], employs Goppa codes [28]. Goppa codes can be viewed from several different perspectives, each giving a window into their capabilities. We aim in this work to generalize Goppa codes to a multivariable case.

Let $\mathbb{F}_{q^t}$ be a finite field with q^t elements. The polynomial ring over $\mathbb{F}_{q^t}$ in m variables is denoted by $\mathbb{F}_{q^t}[x_1, \ldots, x_m]$ or $\mathbb{F}_{q^t}[\boldsymbol{x}]$, when there is no ambiguity on the number of variables. A multivariate Goppa code is defined as follows. Fix non-empty subsets $S_1, \ldots, S_m \subseteq \mathbb{F}_{q^t}$ and their *Cartesian product*

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

Enumerate the elements of $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\} \subseteq F_{q^t}^m$. Take $g \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $g(\boldsymbol{s}_i) \neq 0$ for all $i \in [n]$. In addition, assume that g can be expressed as a product $g = g_1 \cdots g_m$,

2010 *Mathematics Subject Classification.* 94B05; 11T71; 14G50.

Key words and phrases. Goppa codes, augmented Cartesian codes, tensor products of Reed-Solomon codes, quantum error-correcting, LCD, self-dual, self-orthogonal.

The first author was partially supported by an AMS–Simons Travel Grant. The second author was supported by NSF DMS-1855136, NSF DMS-2037833, and the Commonwealth Cyber Initiative.

where $g_i \in \mathbb{F}_{q^t}[x_i]$. The *multivariate Goppa code* is denoted and defined by

$$\Gamma(\mathcal{S}, g) := \left\{ (c_1, \ldots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{\prod_{j=1}^{m}(x_j - s_{ij})} = 0 \mod g(\boldsymbol{x}) \right\},$$

where $\boldsymbol{s}_i := (s_{i1}, \ldots, s_{im}) \in \mathcal{S}$.

Taking $m = 1$, we obtain the Goppa codes as in [3, 14, 15]. Setting $m = t = 1$ gives the codes considered in [12]. It is worth noting that $\Gamma(\mathcal{S}, g)$ is a code over $\mathbb{F}_q$ of length n given by $\mid \mathcal{S} \mid$ where $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$; thus, $n \leq q^{tm}$. Hence, allowing larger values of t and m provides longer codes over the same field. As we will see in Corollary 5 at the end of Section 2, taking larger values of m allows one to obtain codes of the same lengths over the same field but with potentially larger dimensions.

As usual, an $[n, k, d]$ code over $\mathbb{F}_{q^t}$ is a code of length n, dimension k, and minimum distance $d := \min\{|\operatorname{supp}(c)| : 0 \neq c \in C\}$, where $\operatorname{supp}(c)$ denotes the support of c, that is, the set of all non-zero entries of c. Given $v \in \mathbb{F}^n$, we denote its i^{th} component by v_i where $i \in [n]$. The dual of an $[n, k, d]$ code C is

$$C^{\perp} := \{w \in \mathbb{F}^n : w \cdot c = 0 \ \forall c \in C\};$$

that is, the dual is taken with respect to the Euclidean inner product. The *hull* of C is $\operatorname{Hull}(C) = C \cap C^{\perp}$. The code C is *linear complementary dual* (*LCD*) [27] if $\operatorname{Hull}(C) = \{\mathbf{0}\}$ and is *self-orthogonal* if $C \subseteq C^{\perp}$.

In Section 2, we recall the definition of a generalized Reed-Solomon (GRS) code, which is a well-known code that depends of an integer k and a polynomial $g \in \mathbb{F}_{q^t}[x]$. When $k = \deg(g)$, the GRS code is called a GRS code via a Goppa code. This family was recently studied by Y. Gao, Q. Yue, X. Huang, and J. Zhang in [12] where the authors describe conditions, using the properties of classical Goppa codes, so the dual of a GRS code via a Goppa code is again a GRS code via a Goppa code. Thus, having the control over the dual, the authors are able to find the hull and give applications to quantum, LCD, self-orthogonal, and self-dual codes. Then we introduce the tensor product of GRS codes and the tensor product of GRS codes via a Goppa code. The former has been studied before due to their decoding properties. In [13], the authors provide a list decoding algorithm for the tensor product of GRS codes. In [8], they authors use the tensor product of GRS codes to decode *hyperbolic codes*, which are augmented Reed-Muller codes, in the sense that the dimension is greater than or equal, but the minimum distance is the same. The tensor product of GRS codes via a Goppa code is important in obtaining the following result, which is proved in Section 2. Given a multivariate Goppa code $\Gamma(\mathcal{S}, g)$,

$$\Gamma(\mathcal{S}, g) = \{\boldsymbol{c} \in \mathbb{F}_q^n : \mathrm{T}\, \boldsymbol{c}^T = 0\},$$

where T is a generator matrix of certain tensor product of GRS codes via a Goppa code that depends of g. As a consequence, we see that the Goppa code $\Gamma(\mathcal{S}, g)$ is a subfield subcode of the dual of a tensor product of GRS codes via Goppa codes.

In Section 3, we prove that the multivariate Goppa code $\Gamma(\mathcal{S}, g)$ is a subfield subcode of an augmented Cartesian code. Augmented Cartesian (ACar) codes are a family of evaluation codes recently introduced in [22, 25] where the authors present linear exact repair schemes for the ACar and give examples where ACar codes provide a lower bandwidth (resp., bitwidth) than RS codes (resp., Hermitian) codes when the dimension and basefield are fixed. Even more, ACar are decreasing monomial-Cartesian codes, which

have applications to certain polar codes [7]. In this paper, we demonstrate that

$$\Gamma(\mathcal{S}, g) = \mathrm{ACar}\left(\mathcal{S}, g\right)_q,$$

where $\mathrm{ACar}\left(\mathcal{S}, g\right)_q$ represents the subfield subcode of certain ACar code which yields information about the basic parameters of the multivariate Goppa code $\Gamma(\mathcal{S}, g)$.

In Section 4, we study the three families just described: multivariate Goppa codes, tensor product of GRS codes via a Goppa code, and augmented Cartesian codes. Each of these families depend of a polynomial g in $\mathbb{F}_{q^t}[\boldsymbol{x}]$. We give conditions on g to determine determine subcodes, intersections, and hulls. One of the main results states that for certain f, g in $\mathbb{F}_{q^t}[\boldsymbol{x}]$, then

(i) $\mathrm{Hull}\left(\mathrm{T}(\mathcal{S}, g)\right) = \mathrm{T}(\mathcal{S}, \gcd(f, g)) = \mathrm{Hull}\left(\mathrm{ACar}(\mathcal{S}, g)\right)$, and
(ii) $\Gamma(\mathcal{S}, \mathrm{lcm}(f, g)) \subseteq \mathrm{Hull}\left(\Gamma(\mathcal{S}, g)\right)$, with equality when $t = 1$.

In Section 5, we design quantum, LCD, self-orthogonal, and self-dual codes from multivariate Goppa codes and tensor product of GRS codes via Goppa codes, relying on the results of Section 4. One of the main contributions in Section 5 provides an algorithm to find LCD, self-orthogonal and self-dual codes. This approach is different than that given in [12]. An immediate difference is that using GRS codes, the length of the code is always bounded by the size of the field whereas this restriction is not needed in Section 5, for instance, for the tensor product. Even more, the results of Section 5 enable a single set of defining polynomials to produce a family of codes with different lengths over a certain field (cf. [12, Theorem 2.6]). We provide some examples at the end of Section 5. Finally, a brief summary is given as a conclusion in Section 6.

More information about basic theory for coding theory can be found in [20, 26, 29]. References for the theory of vanishing ideals and algebraic concepts used in this work are [9, 11, 19, 30].

2. A parity check matrix given by the tensor product of GRS codes

In this section, we introduce the tensor product of generalized Reed-Solomon codes via Goppa codes. We show that this family provides a parity check matrix for the multivariate Goppa codes. As a consequence, we are able to give bounds for the dimension of the Goppa code. In addition, we give a representation for the dual of a multivariate Goppa code in terms of the trace of the tensor product.

The set of $m \times n$ matrices over $\mathbb{F}_{q^t}$ is denoted $\mathbb{F}_{q^t}^{m\times n}$. The Kronecker product of matrices $A = [a_{ij}] \in \mathbb{F}_{q^t}^{r\times s}$ and $B \in \mathbb{F}_{q^t}^{m_1\times m_2}$ is the matrix that can be expressed in block form as

$$A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1s}B \\ a_{21}B & a_{22}B & \cdots & a_{2s}B \\ \vdots & \vdots & & \vdots \\ a_{r1}B & a_{r2}B & \cdots & a_{rs}B \end{pmatrix} \in \mathbb{F}_{q^t}^{rm_1\times sm_2}.$$

A generator matrix for an $[n, k, d]$ code C is any matrix whose row span is C. Given a generator matrix G_1 of a code $\mathcal{C}_1$ and a generator matrix G_2 of a code $\mathcal{C}_2$, the code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is defined as the code whose generator matrix is $G_1 \otimes G_2$.

Next, we relate the multivariate Goppa codes to generalized Reed-Solomon codes. Given $k \in \mathbb{Z}^+$, $\mathbb{F}_{q^t}[x]_{<k}$ denotes the set of polynomials of degree less than k. Recall that

a *generalized Reed-Solomon* (GRS) code is defined by

$$\mathrm{GRS}(S,k,g) := \left\{ \left(g(s_1)^{-1} f(s_1), \ldots, g(s_n)^{-1} f(s_n) \right) : f \in \mathbb{F}_{q^t}[x]_{<k} \right\},$$

where $g \in \mathbb{F}_{q^t}[x]$ and $S \subseteq \mathbb{F}_{q^t}$. GRS codes in the particular case $t = 1$ and $k = \deg(g)$ are called *GRS codes via a Goppa code* and denoted by $\mathrm{GRS}(S, g)$, *i.e.*

$$\mathrm{GRS}(S,g) := \mathrm{GRS}(S, \deg(g), g).$$

GRS codes via a Goppa code where studied in [12]. We note that $\mathrm{GRS}(S,k,g)$ is an $[n, k, n-k+1]$ code over $\mathbb{F}_{q^t}$ with $n \leq q^t$, meaning it is maximum distance separable (MDS). As we will see, tensor products of generalized Reed-Solomon codes play an important role in the duals of multivariate Goppa codes. In what follows, $n_i = |S_i|$, the cardinality of S_i for $i \in [m] := \{1, \ldots, m\}$. From now on, when we take an element $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$, we mean that every $g_i \in \mathbb{F}_{q^t}[x_i]$. The expression $g(\mathcal{S}) \neq 0$ represents that $g(\boldsymbol{s}) \neq 0$ for all $\boldsymbol{s} \in \mathcal{S}$.

Definition 1. Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$ and $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $g(\mathcal{S}) \neq 0$. Take $\boldsymbol{k} = (k_1, \ldots, k_m) \in \mathbb{Z}^m$ with $0 \leq k_j \leq n_j$ for all $j \in [m]$. We define the tensor product of generalized Reed-Solomon codes as

$$\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g) := \bigotimes_{j=1}^{m} \mathrm{GRS}(S_j, k_j, g_j).$$

The tensor product of generalized Reed-Solomon codes via Goppa codes is

$$\mathrm{T}(\mathcal{S}, g) := \bigotimes_{j=1}^{m} \mathrm{GRS}(S_j, \deg(g_j), g_j).$$

A generator matrix of $\mathrm{T}(\mathcal{S}, g)$ may be specified entrywise by

$$\left(\frac{\boldsymbol{s}_i^{\boldsymbol{a}}}{g(\boldsymbol{s}_i)} \right)_{a,j} \in \mathbb{F}_{q^t}^{\deg(g) \times n} \tag{1}$$

where the rows and columns are indexed by $\boldsymbol{a} \in \mathbb{N}^{\deg(g_1)-1 \times \cdots \times \deg(g_m)-1}$ and $i \in [n]$, respectively.

Remark 2. *Observe that the tensor product of generalized Reed-Solomon codes* $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g)$ *has the following basic parameters.*

(i) *Length* $n = \mid \mathcal{S} \mid$.
(ii) *Dimension* $k = \prod_{j=1}^{m} k_j$.
(iii) *Minimum distance* $d = \prod_{j=1}^{m} (n_j - k_j + 1)$.

In particular, $\mathrm{T}(\mathcal{S}, g)$ *is an* $[n, \deg(g), \prod_{j=1}^{m}(n_j - \deg(g_j) + 1)\}]$ *code over* $\mathbb{F}_{q^t}$.

Remark 3. *Note that* $\mathrm{GRS}(S_j, k_j, g_j) = \{\mathbf{0}\}$ *if and only if* $k_j = 0$. *Thus,* $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g) = \{\mathbf{0}\}$ *if and only if there is* $j \in [m]$ *such that* $k_j = 0$. *In addition,* $\mathrm{GRS}(S_j, k_j, g_j) = \mathbb{F}_{q^t}^{n_j}$ *if and only if* $k_j = n_j$. *Thus,* $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g) = \mathbb{F}_{q^t}^{n}$ *if and only if* $\boldsymbol{k} = (n_1, \ldots, n_m)$.

To relate multivariate Goppa codes to those codes in Definition 1, observe that given any two polynomials $p(x_1) = p_\ell x_1^\ell + \cdots + p_1 x_1 + p_0 = (x_1^\ell, \ldots, x_1, 1) \cdot (p_\ell, \ldots, p_1, p_0) \in$

$\mathbb{F}_{q^t}[x_1]$ and $q(x_2) = q_k x_2^k + \cdots + q_1 x_2 + q_0 = (x_2^k, \ldots, x_2, 1) \cdot (q_k, \ldots, q_1, q_0) \in \mathbb{F}_{q^t}[x_2]$, we may abuse notation and write

$$p(x_1)q(x_2) = \left(\begin{pmatrix} x_1^\ell \\ \vdots \\ x_1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} x_2^k \\ \vdots \\ x_2 \\ 1 \end{pmatrix} \right)^T \left(\begin{pmatrix} p_\ell \\ \vdots \\ p_1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} q_k \\ \vdots \\ q_1 \\ 1 \end{pmatrix} \right).$$

In addition, if $s \in \mathbb{F}_{q^t}$, then, modulo $q(x_2)$, the following two equations are valid

$$\frac{1}{(x_2 - s)} = \frac{(-1)}{q(s)} \frac{(q(x_2) - q(s))}{(x_2 - s)} \tag{2}$$

$$= \frac{(-1)}{q(s)} \begin{pmatrix} x_2^{k-1} \\ \vdots \\ x_2 \\ 1 \end{pmatrix}^T \begin{pmatrix} q_k & 0 & \cdots & 0 \\ q_{k-1} & q_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ q_1 & q_2 & \cdots & q_k \end{pmatrix} \begin{pmatrix} 1 \\ s \\ \vdots \\ s^{k-1} \end{pmatrix}. \tag{3}$$

We come to one of the main results of this section, which gives a representation of a multivariate Goppa code in terms of a tensor product of GRS codes.

Theorem 4. *Given a multivariate Goppa code* $\Gamma(\mathcal{S}, g)$*,*

$$\Gamma(\mathcal{S}, g) = \{\boldsymbol{c} \in \mathbb{F}_q^n : \mathrm{T}\, \boldsymbol{c}^T = 0\},$$

where T *is a generator matrix of* $\mathrm{T}(\mathcal{S}, g)$*; that is,* $\Gamma(\mathcal{S}, g)$ *is a subfield subcode of the dual of a tensor product of GRS codes via Goppa codes.*

Proof. According to (1), the following vectors generate the code $\mathrm{T}(\mathcal{S}, g)$

$$\left(\frac{\boldsymbol{s}_1^{\boldsymbol{a}}}{g(\boldsymbol{s}_1)}, \ldots, \frac{\boldsymbol{s}_n^{\boldsymbol{a}}}{g(\boldsymbol{s}_n)} \right) = \left(\frac{s_{11}^{a_1} \cdots s_{1m}^{a_m}}{g_1(s_{11}) \cdots g_m(s_{1m})}, \ldots, \frac{s_{n1}^{a_1} \cdots s_{nm}^{a_m}}{g_1(s_{n1}) \cdots g_m(s_{nm})} \right), \tag{4}$$

where for $i \in [n]$, $\boldsymbol{s}_i = (s_{i1}, \ldots, s_{im}) \in \mathbb{F}_{q^t}^m$ and $0 \leq a_j < \deg(g_j)$ for $j \in [m]$.

The proof consists of verifying that the elements in $\Gamma(\mathcal{S}, g)$ are orthogonal to the vectors shown in Equation 4. We proceed by induction on m. Consider the case $m = 1$. Assume $g(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_k x^k$. Equation 3 implies that if $\boldsymbol{c} = (c_1, \ldots, c_n) \in \Gamma(\mathcal{S}, g)$, then

$$\sum_{i=1}^n \frac{c_i}{(x - s_i)} = \sum_{i=1}^n \frac{-c_i}{g(s_i)} \begin{pmatrix} x^{k-1} \\ \vdots \\ x \\ 1 \end{pmatrix}^T \begin{pmatrix} \gamma_k & 0 & \cdots & 0 \\ \gamma_{k-1} & \gamma_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_1 & \gamma_2 & \cdots & \gamma_k \end{pmatrix} \begin{pmatrix} 1 \\ s_i \\ \vdots \\ s_i^{k-1} \end{pmatrix}$$

$$= \begin{pmatrix} x^{k-1} \\ \vdots \\ x \\ 1 \end{pmatrix}^T \begin{pmatrix} \gamma_k & 0 & \cdots & 0 \\ \gamma_{k-1} & \gamma_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_1 & \gamma_2 & \cdots & \gamma_k \end{pmatrix} \sum_{i=1}^n \frac{-c_i}{g(s_i)} \begin{pmatrix} 1 \\ s_i \\ \vdots \\ s_i^{k-1} \end{pmatrix} \tag{5}$$

$$= 0 \mod g(x). \tag{6}$$

Observe that the polynomial in (5) has degree $k-1$. As $\deg(g)=k$, Equation 6 implies that the coefficients of the polynomial given in Equation (5) are zero. Hence, we see that

$$\begin{pmatrix} \gamma_k & 0 & \cdots & 0 \\ \gamma_{k-1} & \gamma_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_1 & \gamma_2 & \cdots & \gamma_k \end{pmatrix} \begin{pmatrix} \frac{1}{g(s_1)} & \frac{1}{g(s_2)} & \cdots & \frac{1}{g(s_n)} \\ \frac{s_1}{g(s_1)} & \frac{s_2}{g(s_2)} & \cdots & \frac{s_n}{g(s_n)} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{s_1^{k-1}}{g(s_1)} & \frac{s_2^{k-1}}{g(s_2)} & \cdots & \frac{s_n^{k-1}}{g(s_n)} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

As the matrix in terms of γ's is invertible, after we multiply both sides of previous equation by the inverse of this matrix, we see that the element $\boldsymbol{c} \in \Gamma(\mathcal{S}, g)$ is orthogonal to the vectors $\left(\frac{s_1^{a_1}}{g(s_1)}, \ldots, \frac{s_n^{a_1}}{g(s_n)}\right)$, where $0 \leq a_1 < k = \deg(g)$. These are the vectors that appear in Equation (4) when $m = 1$.

Now we focus on the case $m = 2$. Assume $\deg(g_1) = k_1$ and $\deg(g_2) = k_2$. By Equation 3, there exist invertible matrices A and B, that depend of the coefficients of g_1 and g_2, respectively, such that

$$\begin{aligned} & \sum_{i=1}^{n} \frac{c_i}{(x_1 - s_{i1})(x_2 - s_{i2})} \\ = & \sum_{i=1}^{n} \frac{c_i}{g_1(s_{i1})g_2(s_{i2})} \left(\begin{pmatrix} x_1^{k_1-1} \\ \vdots \\ x_1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} x_2^{k_2-1} \\ \vdots \\ x_2 \\ 1 \end{pmatrix} \right)^T A \otimes B \begin{pmatrix} 1 \\ s_{i1} \\ \vdots \\ s_{i1}^{k_1-1} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ s_{i2} \\ \vdots \\ s_{i2}^{k_2-1} \end{pmatrix} \\ = & \left(\begin{pmatrix} x_1^{k_1-1} \\ \vdots \\ x_1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} x_2^{k_2-1} \\ \vdots \\ x_2 \\ 1 \end{pmatrix} \right)^T A \otimes B \sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\begin{pmatrix} 1 \\ s_{i1} \\ \vdots \\ s_{i1}^{k_1-1} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ s_{i2} \\ \vdots \\ s_{i2}^{k_2-1} \end{pmatrix} \right) \\ = & \ 0 \mod g(\boldsymbol{x}). \end{aligned}$$

As $\deg_{x_1}(g) = k_1$ and $\deg_{x_2}(g) = k_2$, the previous equation implies

$$A \otimes B \sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\begin{pmatrix} 1 \\ s_{i1} \\ \vdots \\ s_{i1}^{k_1-1} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ s_{i2} \\ \vdots \\ s_{i2}^{k_2-1} \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiplying both sides by the inverse $(A \otimes B)^{-1} = B^{-1} \otimes A^{-1}$, we finally obtain

$$\sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\begin{pmatrix} 1 \\ s_{i1} \\ \vdots \\ s_{i1}^{k_1-1} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ s_{i2} \\ \vdots \\ s_{i2}^{k_2-1} \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We conclude that if $\boldsymbol{c} \in \Gamma(\mathcal{S}, g)$, then $\boldsymbol{c} \cdot \left(\frac{s_{11}^{a_1} s_{12}^{a_2}}{g_1(s_{11})g_2(s_{12})}, \ldots, \frac{s_{n1}^{a_1} s_{n2}^{a_2}}{g_1(s_{n1})g_2(s_{n2})} \right) = 0$, where $0 \leq a_j < k_j = \deg(g_j)$, for $j \in [2]$. These are the vectors that appear in Equation (4),

for $m = 2$. For the general case, observe that following the steps of the case $m = 2$, we saw that $\sum_{i=1}^{n} \frac{c_i}{\prod_{j=1}^{m}(x_j - s_{ij})} = 0 \mod g(\boldsymbol{x})$ implies that

$$\sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\begin{pmatrix} 1 \\ s_{i1} \\ \vdots \\ s_{i1}^{k_1-1} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 \\ s_{in} \\ \vdots \\ s_{in}^{k_n-1} \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

From this fact, we conclude that if $\boldsymbol{c} \in \Gamma(\mathcal{S}, g)$, then $\boldsymbol{c}$ is orthogonal to the vectors that appear in Equation (4). □

Recall that given a code $C \subseteq \mathbb{F}_{q^t}^n$, the subfield subcode over $\mathbb{F}_q$ is

$$C_q := \left\{ \boldsymbol{c} \in C : \boldsymbol{c} \in \mathbb{F}_q^n \right\}$$

and the *field trace* with respect to the extension $\mathbb{F}_{q^t}^n / \mathbb{F}_q$ is defined as the map

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

The *trace code* of an $[n, k, d]$ code C over $\mathbb{F}_{q^t}$ is defined by

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

By [26, Ch. 7. §7.], $tr(C)$ is an $[n, k^*, d^*]$ over $\mathbb{F}_q$, where $k \leq k^* \leq tk$ and $d^* \geq d$. According to Delsarte's Theorem [10, Theorem 2], $C_q^{\perp} = tr\left(C^{\perp}\right)$. Putting this together with the fact that $\Gamma(\mathcal{S}, g) = \left(\mathrm{T}(\mathcal{S}, g)^{\perp}\right)_q$, as shown in Theorem 4, we obtain the following consequences.

Corollary 5. *The multivariate Goppa code $\Gamma(\mathcal{S}, g)$ has length $n = \mid \mathcal{S} \mid$ and dimension k satisfying $n - t\deg(g) \leq k \leq n - \deg(g)$. Moreover, the dual is the trace code of a tensor product of generalized Reed-Solomon codes via Goppa codes, specifically,*

$$\Gamma(\mathcal{S}, g)^{\perp} = tr(\mathrm{T}(\mathcal{S}, g)).$$

Example 6. Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$ is the multiplicative group of the finite field $\mathbb{F}_{3^2}$. Take $S_1 = S_2 = \{a^i : i \in [8]\}$ and $g_1 = g_2 = x^2 + a$. Using the coding theory package [2] for Macaulay2 [17], and Magma [5], we obtain that $\Gamma(\mathcal{S}, g)$ is an $[64, 56, 4]$ code over $\mathbb{F}_3$, which has parameters matching the best known linear code of length 64 and dimension 56 over this field [16]. If we were to restrict ourselves to taking $m = 1$, then $64 \leq q^t = 3^t$ requires $t \geq 4$ to obtain a code of length 64. Furthermore, $4 = \deg(g) + 1$ implies $\deg(g) = 3$. Consequently, we are only guaranteed that such a code has dimension $64 - 4\deg(g) = 64 - 12 = 52$.

In the next section, we will gain another perspective on the multivariate Goppa codes. It will allow us to round out Corollary 5 by describing the minimum distance of the multivariate Goppa codes.

3. As subfield subcodes of augmented codes

In this section, we show that every multivariate Goppa code is a subfield subcode of an augmented Cartesian code [22, 25]. This useful property allows us to determine the minimum distance of the multivariate Goppa codes and establishes the necessary results for determining hulls in Section 4.

We review first the necessary facts on augmented Cartesian codes. For a lattice point $\boldsymbol{a} \in \mathbb{N}^m$, $\boldsymbol{x}^{\boldsymbol{a}} = x_1^{a_1} \cdots x_m^{a_m}$ denotes the corresponding monomial in $\mathbb{F}_{q^t}[\boldsymbol{x}]$. The *graded-lexicographic order* $\prec$ on the set of monomials of $\mathbb{F}_{q^t}[\boldsymbol{x}]$ which is defined as $x_1^{a_1} \cdots x_m^{a_m} \prec x_1^{b_1} \cdots x_m^{b_m}$ if and only if $\sum_{i=1}^m a_i < \sum_{i=1}^m b_i$ or $\sum_{i=1}^m a_i = \sum_{i=1}^m b_i$ and the leftmost nonzero entry in $(b_1 - a_1, \ldots, b_m - a_m)$ is positive. The ideal generated by $f_1, \ldots, f_r \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ is denoted $(f_1, \ldots, f_r) \subseteq \mathbb{F}_{q^t}[\boldsymbol{x}]$. The subspace of polynomials of $\mathbb{F}_{q^t}[\boldsymbol{x}]$ that are $\mathbb{F}_{q^t}$-linear combinations of monomials $\boldsymbol{x}^{\boldsymbol{a}} \in \mathbb{F}_{q^t}[\boldsymbol{x}]$, where $\boldsymbol{a} \in \mathcal{A} \subseteq \mathbb{N}^m$, is denoted by $\mathcal{L}(\mathcal{A})$, *i.e.*

$$\mathcal{L}(\mathcal{A}) := \mathrm{Span}_{\mathbb{F}_{q^t}}\{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in \mathcal{A}\} \subseteq \mathbb{F}_{q^t}[\boldsymbol{x}].$$

Together, the Cartesian product $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}^m$, the lattice points $\mathcal{A}$, and a polynomial $h \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $h(\boldsymbol{s}) \neq 0$, for all $\boldsymbol{s} \in \mathcal{S}$, define the *evaluation map*

$$\begin{array}{rccc} \mathrm{ev}(\mathcal{S}, h)\colon & \mathcal{L}(\mathcal{A}) & \to & \mathbb{F}_{q^t}^{|\mathcal{S}|} \\ & f & \mapsto & \left(\dfrac{f(\boldsymbol{s}_1)}{h(\boldsymbol{s}_1)}, \ldots, \dfrac{f(\boldsymbol{s}_n)}{h(\boldsymbol{s}_n)}\right). \end{array}$$

The image of the evaluation map $\mathrm{ev}(\mathcal{S}, h)(\mathcal{L}(\mathcal{A}))$, called the *generalized monomial-Cartesian* code associated with $\mathcal{S}, \mathcal{A}$, and h, is denoted by $\mathcal{C}(\mathcal{S}, \mathcal{A}, h) \subseteq \mathbb{F}_{q^t}^{|\mathcal{S}|}$:

$$\mathcal{C}(\mathcal{S}, \mathcal{A}, h) = \left\{ \left(\frac{f(\boldsymbol{s}_1)}{h(\boldsymbol{s}_1)}, \ldots, \frac{f(\boldsymbol{s}_n)}{h(\boldsymbol{s}_n)}\right) : f \in \mathcal{L}(\mathcal{A}) \right\}. \tag{7}$$

We may assume that $\deg_{x_j}(h) < n_j$ for all $j \in [m]$. To see this, consider the polynomial

$$L_j(x_j) := \prod_{s \in S_j} (x_j - s) \tag{8}$$

for each $j \in [m]$. By [23, Lemma 2.3], the *vanishing ideal* of $\mathcal{S}$, consisting of all polynomials of $\mathbb{F}_{q^t}[\boldsymbol{x}]$ that vanish on $\mathcal{S}$, is given by $I(\mathcal{S}) = (L_1(x_1), \ldots, L_m(x_m))$. According to [9, Proposition 4], $\{L_1(x_1), \ldots, L_m(x_m)\}$ is a Gröbner basis of $I(\mathcal{S})$, relative to the graded-lexicographic order $\prec$. Let r be the remainder of h modulo $I(\mathcal{S})$. As $r(\boldsymbol{s}_i) = h(\boldsymbol{s}_i)$ for all $i \in [n]$ and $\deg_{x_j}(r) < \deg(L_j) = n_j$, we may redefine $h := r$. Consequently, $\deg_{x_j}(h) < n_j$. By the same reasoning, we will assume that the degree of each $f \in \mathcal{L}(\mathcal{A})$ in x_i is less than n_i; i.e., we consider $\mathcal{A} \subseteq \prod_{i=1}^m \{0, \ldots, n_i - 1\}$. In this case, the evaluation map $\mathrm{ev}(\mathcal{S}, h)$ is injective. Thus, the length and rate of the monomial-Cartesian code $\mathcal{C}(\mathcal{S}, \mathcal{A}, h)$ are given by $|\mathcal{S}|$ and $\frac{|\mathcal{A}|}{|\mathcal{S}|}$, respectively [21, Proposition 2.1]. If $m = 1$ and $\mathcal{A} = \{0, 1, \ldots, k-1\}$, then $\mathcal{C}(\mathcal{S}, \mathcal{A}, h) = GRS(S, k, h)$, the generalized Reed-Solomon code described in Section 2.

A key characteristic of the monomial-Cartesian codes is that commutative algebra methods may be used to study them. The kernel of the evaluation map $\mathrm{ev}(\mathcal{S}, h)$ is precisely $\mathcal{L}(\mathcal{A}) \cap I(\mathcal{S})$, where $I(\mathcal{S})$ is the vanishing ideal. Thus, algebraic properties of $\mathbb{F}_{q^t}[\boldsymbol{x}]/\left(\mathcal{L}(\mathcal{A}) \cap I(\mathcal{S})\right)$ are related to the basic parameters of $\mathcal{C}(\mathcal{S}, \mathcal{A}, h)$. We now define the polynomial

$$L(\boldsymbol{x}) := \prod_{j=1}^m L_j'(x_j), \tag{9}$$

where $L_j'(x_j)$ denotes the formal derivative of $L_j(x_j)$, defined in Equation (8). The polynomial $L(\boldsymbol{x})$ plays an important role in determining the dual code $\mathcal{C}(\mathcal{S}, \mathcal{A}, h)^{\perp}$,

which was studied in [21] in terms of the vanishing ideal of $\mathcal{S}$ and in [24] in terms of the indicator functions of $\mathcal{S}$.

Given $f_1, f_2 \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $f_2(\boldsymbol{s}) \neq 0$, for all $\boldsymbol{s} \in \mathcal{S}$, we write $\frac{f_1}{f_2} \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ to mean the unique polynomial whose value at $\boldsymbol{s}$ is $\frac{f_1(\boldsymbol{s})}{f_2(\boldsymbol{s})}$, for all $\boldsymbol{s} \in \mathcal{S}$, and $\deg_{x_j}\left(\frac{f_1}{f_2}\right) < n_j$. Observe that this polynomial is unique as it is a linear combination of indicator functions form by standard monomials. See [24, Proposition 4.6 (a)] for a more detailed explanation about this fact and these concepts.

We now define augmented Cartesian codes, a particular family of decreasing monomial-Cartesian codes meaning that they are defined by $\mathcal{A}$ such that if $M \in \mathcal{L}(\mathcal{A})$ and M' divides M, then $M' \in \mathcal{L}(\mathcal{A})$ [7].

Definition 7. Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$ and $h \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ be such that $h(\boldsymbol{s}) \neq 0$, for all $\boldsymbol{s} \in \mathcal{S}$. An *augmented Cartesian code* (ACar code) is defined by

$$\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h) := \mathcal{C}(\mathcal{S}, \mathcal{A}_{Car}(\boldsymbol{k}), h),$$

where $\boldsymbol{k} = (k_1, \ldots, k_m)$, with $0 \leq k_j \leq n_j$, and

$$\mathcal{A}_{Car}(\boldsymbol{k}) := \prod_{j=1}^{m} \{0, \ldots, n_j - 1\} \setminus \prod_{j=1}^{m} \{k_j, \ldots, n_j - 1\}.$$

We also define

$$\mathrm{ACar}\left(\mathcal{S}, h\right) := \mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_h, \frac{L}{h}\right),$$

where $\boldsymbol{k}_h := \left(n_1 - \deg_{x_1}(h), \ldots, n_m - \deg_{x_m}(h)\right)$.

The augmented Cartesian code $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h)$, where $h \in \mathbb{F}_{q^t} \setminus \{0\}$, was recently introduced and studied in [22] due to its local properties. An augmented Cartesian code is shown in Example 10.

Remark 8. *Observe that $ACar(\mathcal{S}, \boldsymbol{k}, h) = \mathbb{F}_{q^t}^n$ if and only if $k_j = n_j$, for some $j \in [m]$. In addition, $ACar(\mathcal{S}, \boldsymbol{k}, h) = \{\boldsymbol{0}\}$ if and only if $\boldsymbol{k} = \boldsymbol{0}$.*

By previous remark, there are instances where $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h)$ may be one of the trivial spaces $\{\boldsymbol{0}\}$ or $\mathbb{F}_{q^t}^n$. In these cases, their basic parameters are also trivial. For the case when $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h)$ is nontrivial, we have the following result.

Lemma 9. *The augmented Cartesian code $ACar(\mathcal{S}, \boldsymbol{k}, h)$ has the following basic parameters.*

(i) *Length* $n = \mid \mathcal{S} \mid$.
(ii) *Dimension* $k = \prod_{j=1}^{m} n_j - \prod_{j=1}^{m}(n_j - k_j)$.
(iii) *Minimum distance* $d = \min\left\{n_j - k_j + 1\right\}_{j \in [m]}$.

In particular, $ACar(\mathcal{S}, h)$ is an $[n, n - \deg(h), \min\{\deg_{x_j}(h) + 1 : j \in [m]\}]$ code over $\mathbb{F}_{q^t}$. Moreover, the dual of the augmented Cartesian code is $ACar(\mathcal{S}, \boldsymbol{k}, h)^{\perp} = \mathcal{C}\left(\mathcal{S}, \mathcal{A}_{Car}^{\perp}(\boldsymbol{k}), \frac{L}{h}\right)$, where $\mathcal{A}_{Car}^{\perp}(\boldsymbol{k}) = \prod_{j=1}^{m} \{0, \ldots, n_j - k_j - 1\}$.

Proof. The length of the code is apparent from the definition. Since $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h)$ is monomially equivalent to $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, 1)$, we can assume that $h = 1$ for (ii) and (iii). Then (ii) is proven in [22, Proposition 3.3]. To prove (iii), note that Remark 8, $\mathrm{ACar}(\mathcal{S}\boldsymbol{k}, h)$

gives $\{\mathbf{0}\}$ if and only if $\boldsymbol{k} = \mathbf{0}$. Assume $\boldsymbol{k} \neq \mathbf{0}$. Following [7, Definition 3.5], a *generating set* of $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h)$ is defined as a set of monomials $\mathcal{B} \subseteq \mathcal{A}_{Car}(\boldsymbol{k})$ with the property that for every monomial $M \in \mathcal{A}_{Car}(\boldsymbol{k})$, there exists a monomial $M' \in \mathcal{B}$ such that M divides M'. Observe that $\mathcal{B} = \left\{ \dfrac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{x_j^{n_j-k_j}} : k_j > 0 \right\}$ is a generating set of $\mathrm{ACar}(\mathcal{S}, \boldsymbol{k}, h)$. Thus, the result follows from [7, Theorem 3.9 (iii)]. Finally, the dual is a consequence of the proof of the case $h = 1$, given in [22, Proposition 3.3], and [7, Theorem 3.3]. □

Example 10. Take $K = \mathbb{F}_{17}$ and $h = 1$. Let $S_1, S_2 \subseteq K$ with $n_1 = |S_1| = 6$ and $n_2 = |S_2| = 7$. The code $\mathrm{ACar}(S_1 \times S_2, (2,2), h)$ is generated by the vectors $\mathrm{ev}(S_1 \times S_2, h)(M)$, where M is a point in Figure 1 (a). The dual code $\mathrm{ACar}(S_1 \times S_2, (2,2), h)^\perp$ is generated by the vectors $\mathrm{ev}(S_1 \times S_2, L)(M)$, where M is a point in Figure 1 (b).

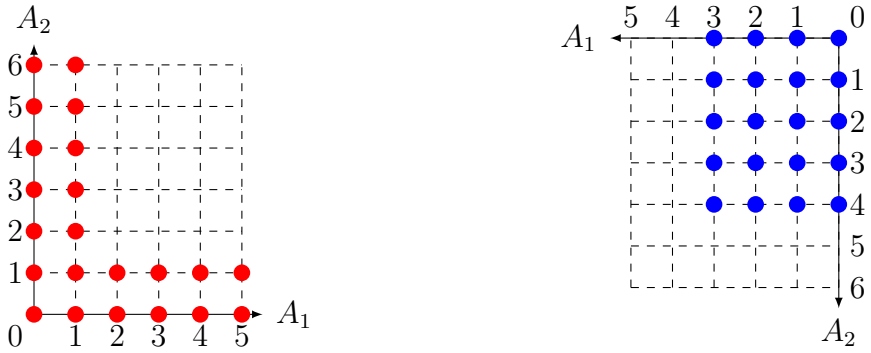

FIGURE 1. The code $\mathrm{ACar}(S_1 \times S_2, (2,2), h)$, with $h = 1$ and $K = \mathbb{F}_{17}$ in Example 10 is generated by the vectors the vectors $\mathrm{ev}(S_1 \times S_2, h)(M)$, where M is a point in (a). The dual code $\mathrm{ACar}(S_1 \times S_2, (2,2), h)^\perp$ is generated by the vectors $\mathrm{ev}(S_1 \times S_2, L)(M)$, where M is a point in (b).

We now show that the dual of the tensor product of generalized Reed-Solomon codes is an augmented Cartesian code.

Theorem 11. *Given a tensor product of generalized RS codes* $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g)$*, its dual is*

$$\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g)^\perp = ACar\left(\mathcal{S}, \boldsymbol{k}', \frac{L}{g}\right),$$

where $\boldsymbol{k}' := (n_1 - k_1, \ldots, n_m - k_m)$*. In particular,* $\mathrm{T}(\mathcal{S}, g)^\perp = ACar(\mathcal{S}, g)$*.*

Proof. By Lemma 9, the dual of the augmented Cartesian code $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}', \frac{L}{g}\right)$ is $\mathcal{C}(\mathcal{S}, \mathcal{A}_{Car}^\perp(\boldsymbol{k}), g)$, where $\mathcal{A}_{Car}^\perp(\boldsymbol{k}) = \prod_{j=1}^m \{0, \ldots, k_j - 1\}$. Observe that $\mathcal{C}(\mathcal{S}, \mathcal{A}_{Car}^\perp(\boldsymbol{k}), g)$ is generated by the vectors

$$\left(\frac{\boldsymbol{s}_1^{\boldsymbol{a}}}{g(\boldsymbol{s}_1)}, \ldots, \frac{\boldsymbol{s}_n^{\boldsymbol{a}}}{g(\boldsymbol{s}_n)}\right) = \left(\frac{s_{11}^{a_1} \cdots s_{1m}^{a_m}}{g_1(s_{11}) \cdots g_m(s_{1m})}, \ldots, \frac{s_{n1}^{a_1} \cdots s_{nm}^{a_m}}{g_1(s_{n1}) \cdots g_m(s_{nm})}\right),$$

where for $i \in [n]$, $\boldsymbol{s}_i = (s_{i1}, \ldots, s_{im})$, and for $j \in [m]$, $0 \leq a_j < k_j$. The result follows from the fact that these vectors also generate $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g)$.

The particular case $\mathrm{T}(\mathcal{S},g)^{\perp} = \mathrm{ACar}\,(\mathcal{S},g)$ is obtained when we take $k_j = \deg(g_j)$, for $j \in [m]$. □

Theorem 12. *The multivariate Goppa code $\Gamma(\mathcal{S},g)$ is the subfield subcode of an augmented Cartesian code. Specifically,*

$$\Gamma(\mathcal{S},g) = ACar(\mathcal{S},g)_q\,.$$

Proof. By Theorem 11, $\mathrm{ACar}\,(\mathcal{S},g)^{\perp} = \mathrm{T}(\mathcal{S},g)$. Observe that if H is a parity check matrix of a code $C \subseteq \mathbb{F}_{q^t}^n$, then $C_q = \left\{\boldsymbol{c} \in \mathbb{F}_q^n : H\boldsymbol{c}^{\perp} = 0\right\}$. Thus, the result follows from Theorem 4. □

The point of view given in Theorem 12 reveals additional information about the parameters of the multivariate Goppa codes, complementing Corollary 5.

Corollary 13. *The multivariate Goppa code $\Gamma(\mathcal{S},g)$ has the following basic parameters.*

(i) *Length* $n = \mid \mathcal{S} \mid$.
(ii) *Dimension* k *satisfying* $n - t\deg(g) \leq k \leq n - \deg(g)$.
(iii) *Minimum distance* $d \geq \min\left\{\deg(g_j)+1\right\}_{j\in[m]}$.

Moreover, the dual is the trace code of a tensor product of generalized Reed-Solomon codes via Goppa codes, specifically,

$$\Gamma(\mathcal{S},g)^{\perp} = tr(\mathrm{T}(\mathcal{S},g)).$$

Proof. Given Corollary 5, it only remains to consider the minimum distance of $\Gamma(\mathcal{S},g)$. By Theorem 12 and Lemma 9 (iii), $d \geq \min\left\{\deg(g_j)+1\right\}_{j\in[m]}$. □

4. Subcodes, intersections, and hulls

In this section, we build on the relationships between multivariate Goppa codes, tensor products of GRS codes, and augmented Cartesian codes to determine subcodes, intersections, and hulls. To do so, we provide conditions on the defining sets of polynomials to yield the desired structures. These results will be key to the construction of entanglement-assisted quantum error correcting codes, LCD, self-orthogonal, or self-dual codes in the next section.

First, the following result helps to identify subcodes of Goppa codes, augmented Cartesian codes and tensor product of GRS codes via Goppa codes.

Proposition 14. *Let $g = g_1\cdots g_m$, $g' = g'_1\cdots g'_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ be such that $g(\mathcal{S}) \neq 0 \neq g'(\mathcal{S})$. Then the following hold:*

(i) $\mathrm{T}(\mathcal{S},g) \subseteq \mathrm{T}(\mathcal{S},gg')$.
(ii) $\Gamma(\mathcal{S},gg') \subseteq \Gamma(\mathcal{S},g)$.
(iii) $ACar(\mathcal{S},gg') \subseteq ACar(\mathcal{S},g)$.

Proof. (i) By Equation (7) and the definition of a GRS code,

$$\begin{aligned}
\mathrm{T}(\mathcal{S}, g) &= \left\{ \left(\frac{f(\boldsymbol{s}_1)}{g(\boldsymbol{s}_1)}, \ldots, \frac{f(\boldsymbol{s}_n)}{g(\boldsymbol{s}_n)} \right) : \deg_{x_j}(f) < \deg(g_j) \right\} \\
&= \left\{ \left(\frac{(fg')(\boldsymbol{s}_1)}{(gg')(\boldsymbol{s}_1)}, \ldots, \frac{(fg')(\boldsymbol{s}_n)}{(gg')(\boldsymbol{s}_n)} \right) : \deg_{x_j}(f) < \deg(g_j) \right\} \\
&\subseteq \left\{ \left(\frac{f'(\boldsymbol{s}_1)}{(gg')(\boldsymbol{s}_1)}, \ldots, \frac{f'(\boldsymbol{s}_n)}{(gg')(\boldsymbol{s}_n)} \right) : \deg_{x_j}(f') < \deg(g_j g_j') \right\} \\
&= \mathrm{T}(\mathcal{S}, gg').
\end{aligned}$$

(ii) By (i), $tr\left(\mathrm{T}(\mathcal{S}, g)\right) \subseteq tr\left(\mathrm{T}(\mathcal{S}, gg')\right)$. Thus, the result follows from Theorem 4.
(iii) This is a consequence of (i) and Theorem 11. □

Next, we see that the intersection of multivariate Goppa codes is again a multivariate Goppa code. In addition to generalizing [12, Theorem 3.1] to multiple variables, the next result demonstrates that in order for the intersection of GRS code via a Goppa code to be of the same type, we only require that the sum of the degrees of the defining polynomials is bounded above rather than that the two polynomials are related to one another as specified in [12, Theorem 3.1].

Theorem 15. *Let* $g = g_1 \cdots g_m$, $g' = g_1' \cdots g_m' \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ *be such that* $g(\mathcal{S}) \neq 0 \neq g'(\mathcal{S})$ *and* $\deg(g_j g_j') \leq n_j$, *for* $j \in [m]$. *Then the following hold:*

(i) $\mathrm{T}(\mathcal{S}, g) \cap \mathrm{T}(\mathcal{S}, g') = \mathrm{T}(\mathcal{S}, \gcd(g, g'))$.
(ii) $\Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g') = \Gamma(\mathcal{S}, \mathrm{lcm}(g, g'))$.
(iii) $ACar(\mathcal{S}, \mathrm{lcm}(g, g')) \subseteq ACar(\mathcal{S}, g) \cap ACar(\mathcal{S}, g')$
$\subseteq ACar(\mathcal{S}, g) + ACar(\mathcal{S}, g') = ACar(\mathcal{S}, \gcd(g, g'))$.

Proof. For $j \in [m]$, define $\gcd_j := \gcd(g_j, g_j') \in \mathbb{F}_{q^t}[x_j]$ and $\mathrm{lcm}_j := \mathrm{lcm}(g_j, g_j') \in \mathbb{F}_{q^t}[x_j]$. Observe that $\gcd := \gcd(g, g') = \gcd_1 \cdots \gcd_m$ and $\mathrm{lcm} := \mathrm{lcm}(g, g') = \mathrm{lcm}_1 \cdots \mathrm{lcm}_m$. There are $p, p', t, t' \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $g = p \gcd, g' = p' \gcd, \mathrm{lcm}(g, g') = gt$ and $\mathrm{lcm}(g, g') = g't'$.

(i) By Proposition 14 (i),

$$\mathrm{T}(\mathcal{S}, \gcd) \subseteq \mathrm{T}(\mathcal{S}, p \gcd) = \mathrm{T}(\mathcal{S}, g)$$

and

$$\mathrm{T}(\mathcal{S}, \gcd) \subseteq \mathrm{T}(\mathcal{S}, p' \gcd) = \mathrm{T}(\mathcal{S}, g').$$

Thus $\mathrm{T}(\mathcal{S}, \gcd) \subseteq \mathrm{T}(\mathcal{S}, g) \cap \mathrm{T}(\mathcal{S}, g')$. Now take $\boldsymbol{c} \in \mathrm{T}(\mathcal{S}, g) \cap \mathrm{T}(\mathcal{S}, g')$. There are $f, f' \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that for $j \in [m], \deg_{x_j}(f) < \deg_{x_j}(g), \deg_{x_j}(f') < \deg_{x_j}(g')$, and

$$\boldsymbol{c} = \left(\frac{f(\boldsymbol{s}_1)}{g(\boldsymbol{s}_1)}, \ldots, \frac{f(\boldsymbol{s}_n)}{g(\boldsymbol{s}_n)} \right) = \left(\frac{f'(\boldsymbol{s}_1)}{g'(\boldsymbol{s}_1)}, \ldots, \frac{f'(\boldsymbol{s}_n)}{g'(\boldsymbol{s}_n)} \right). \tag{10}$$

Observe that $g'f - gf' \in I(\mathcal{S})$. As $\deg_{x_j}(g'f - gf') \leq \max\left\{ \deg_{x_j}(g'f), \deg_{x_j}(gf') \right\} < \deg_{x_j}(gg') \leq n_j$, then $g'f = gf'$. This implies that $\frac{g'}{\gcd} f = \frac{g}{\gcd} f'$. As $\frac{g'}{\gcd}$ and $\frac{g}{\gcd}$ share no common factors, $\frac{g}{\gcd}$ divides f. There is $r \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $f = r\frac{g}{\gcd}$. Thus,

$g'f = r\frac{gg'}{\gcd} = r\,\mathrm{lcm}$, due $\mathrm{lcm}\,\gcd = gg'$. As lcm divides $g'f$, then

$$\begin{aligned}\deg_{x_j}\left(\frac{g'f}{\mathrm{lcm}}\right) &= \deg_{x_j}(g') + \deg_{x_j}(f) - \deg_{x_j}(\mathrm{lcm}) \\ &= \deg_{x_j}(\gcd) + \deg_{x_j}(\mathrm{lcm}) - \deg_{x_j}(g) + \deg_{x_j}(f) - \deg_{x_j}(\mathrm{lcm}) \\ &= \deg_{x_j}(\gcd) - \deg_{x_j}(g) + \deg_{x_j}(f) \\ &< \deg_{x_j}(\gcd),\end{aligned}$$

where the inequality holds because $\deg_{x_j}(f) < \deg_{x_j}(g)$. Equations 10 imply

$$\boldsymbol{c} = \left(\frac{(g'f)(\boldsymbol{s}_1)}{(\mathrm{lcm}\,\gcd)(\boldsymbol{s}_1)}, \ldots, \frac{(g'f)(\boldsymbol{s}_n)}{(\mathrm{lcm}\,\gcd)(\boldsymbol{s}_n)}\right) = \left(\frac{\left(\frac{g'f}{\mathrm{lcm}}\right)(\boldsymbol{s}_1)}{\gcd(\boldsymbol{s}_1)}, \ldots, \frac{\left(\frac{g'f}{\mathrm{lcm}}\right)(\boldsymbol{s}_n)}{\gcd(\boldsymbol{s}_n)}\right).$$

As $\deg_{x_j}\left(\frac{g'f}{\mathrm{lcm}}\right) < \deg_{x_j}(\gcd)$, we obtain that $\boldsymbol{c} \in \mathrm{T}(\mathcal{S}, \gcd)$.

(ii) By Proposition 14 (ii),

$$\Gamma(\mathcal{S}, \mathrm{lcm}) = \Gamma(\mathcal{S}, tg) \subseteq \Gamma(\mathcal{S}, g)$$

and

$$\Gamma(\mathcal{S}, \mathrm{lcm}) = \Gamma(\mathcal{S}, t'g') \subseteq \Gamma(\mathcal{S}, g').$$

We conclude that $\Gamma(\mathcal{S}, \mathrm{lcm}) \subseteq \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g')$. If $\boldsymbol{c} \in \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g')$, then

$$\sum_{i=1}^{n} \frac{c_i}{\prod_{j=1}^{m}(x_j - s_{ij})} = 0 \mod g(\boldsymbol{x})$$

and

$$\sum_{i=1}^{n} \frac{c_i}{\prod_{j=1}^{m}(x_j - s_{ij})} = 0 \mod g'(\boldsymbol{x}).$$

Thus, $\sum_{i=1}^{n} \frac{c_i}{\prod_{j=1}^{m}(x_j - s_{ij})} = 0 \mod \mathrm{lcm}(g, g')(\boldsymbol{x})$, which means that $\boldsymbol{c} \in \Gamma(\mathcal{S}, \mathrm{lcm}(g, g'))$.

(iii) By Proposition 14 (iii),

$$\mathrm{ACar}\,(\mathcal{S}, \mathrm{lcm}) = \mathrm{ACar}(\mathcal{S}, tg) \quad \subseteq \quad \mathrm{ACar}(\mathcal{S}, g)$$

and

$$\mathrm{ACar}(\mathcal{S}, \mathrm{lcm}) = \mathrm{ACar}(\mathcal{S}, t'g') \quad \subseteq \quad \mathrm{ACar}(\mathcal{S}, g').$$

This means that $\mathrm{ACar}(\mathcal{S}, \mathrm{lcm}) \subseteq \mathrm{ACar}(\mathcal{S}, g) \cap \mathrm{ACar}(\mathcal{S}, g')$. By (i) and [26, Ch. 1. §8.], $\mathrm{T}(\mathcal{S}, g)^{\perp} + \mathrm{T}(\mathcal{S}, g')^{\perp} = \mathrm{T}(\mathcal{S}, \gcd)^{\perp}$. Thus, by Theorem 11 we obtain

$$\mathrm{ACar}\,(\mathcal{S}, g) \cap \mathrm{ACar}\,(\mathcal{S}, g') \subseteq \mathrm{ACar}\,(\mathcal{S}, g) + \mathrm{ACar}\,(\mathcal{S}, g') = \mathrm{ACar}\,(\mathcal{S}, \gcd(g, g'))\,.$$

□

Let $(p_i s_i^a)_{a,i} \in \mathbb{F}_{q^t}^{k\times n}$ and $(t_i s_i^a)_{a,i} \in \mathbb{F}_{q^t}^{k\times n}$ be two generator matrices of the same GRS code, where the rows and columns are indexed by $0 \le a < k$ and $i \in [n]$, respectively. In [12, Lemma 2.5], the authors describe a property that these matrices should satisfy. Specifically, if $k \le n/2$, then for $i \in [n]$, $p_i = \lambda t_i$, where $\lambda \in \mathbb{F}_{q^t}^*$. When $k = n$, it is clear that the relation $p_i = \lambda t_i$ is not valid anymore, as in this case, for any coefficients

p_i, t_i, both matrices $(p_i s_i^a)_{a,i} \in \mathbb{F}_{q^t}^{k\times n}$ and $(t_i s_i^a)_{a,i} \in \mathbb{F}_{q^t}^{k\times n}$ generate the full space $\mathbb{F}_{q^t}^n$. The following result extends [12, Lemma 2.5] to more variables and changes the restriction from $k \leq n/2$ to $k < n$. This result will be helpful in characterizing when the dual of a tensor product of GRS codes via Goppa codes is of the same form.

Lemma 16. *Let $f,\ F \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ be such that $f(\mathcal{S}) \neq 0 \neq F(\mathcal{S})$. Define $\boldsymbol{k} := (n_1, \ldots, n_{j^*-1}, k, n_{j^*+1}, \ldots, n_m)$, where $k < n$. Then, $\deg_{x_{j^*}}\left(\frac{F}{f}\right) = 0$ if and only if*

$$\mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, \boldsymbol{k}, F).$$

Proof. ($\Rightarrow$) Assume $\deg_{x_{j^*}}\left(\frac{F}{f}\right) = 0$. Recall $\mathrm{ev}(\mathcal{S}, f)(h) = \left(\frac{h(\boldsymbol{s}_1)}{f(\boldsymbol{s}_1)}, \ldots, \frac{h(\boldsymbol{s}_n)}{f(\boldsymbol{s}_n)}\right)$. Take $\mathrm{ev}(\mathcal{S}, f)(h) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, f)$. Then $\deg_{x_{j^*}}(h) < k$. As $\deg_{x_{j^*}}\left(\frac{F}{f}\right) = 0$, we have that $\deg_{x_{j^*}}\left(h\frac{F}{f}\right) < k$, which means that $\mathrm{ev}(\mathcal{S}, F)(h\frac{F}{f}) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, F)$. Thus, $\mathrm{ev}(\mathcal{S}, f)(h) = \mathrm{ev}(\mathcal{S}, F)(h\frac{F}{f}) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, F)$. Now take $\mathrm{ev}(\mathcal{S}, F)(h) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, F)$. Then $\deg_{x_{j^*}}(h) < k$. As $\deg_{x_{j^*}}\left(\frac{f}{F}\right) = \deg_{x_{j^*}}\left(\frac{F}{f}\right) = 0$, we have that $\deg_{x_{j^*}}\left(h\frac{f}{F}\right) < k$, which means that $\mathrm{ev}(\mathcal{S}, f)(h\frac{f}{F}) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, f)$. Thus, $\mathrm{ev}(\mathcal{S}, F)(h) = \mathrm{ev}(\mathcal{S}, f)(h\frac{f}{F}) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, f)$.

($\Leftarrow$) Assume $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, \boldsymbol{k}, F)$. As $\mathrm{ev}(\mathcal{S}, f)(1), \ldots, \mathrm{ev}(\mathcal{S}, f)(x_{j^*}^{k-1}) \in \mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, \boldsymbol{k}, F)$, there are $\lambda_p^\ell \in \mathbb{F}_{q^t}[\boldsymbol{x}]$, with $p, t \in \{0, \ldots, k-1\}$, such that

$$\begin{aligned}
\mathrm{ev}(\mathcal{S}, f)(1) &= \mathrm{ev}(\mathcal{S}, F)(\lambda_0^0 + \lambda_1^0 x_{j^*} + \cdots + \lambda_{k-1}^0 x_{j^*}^{k-1}),\\
\mathrm{ev}(\mathcal{S}, f)(x_{j^*}) &= \mathrm{ev}(\mathcal{S}, F)(\lambda_0^1 + \lambda_1^1 x_{j^*} + \cdots + \lambda_{k-1}^1 x_{j^*}^{k-1}),\\
&\vdots\\
\mathrm{ev}(\mathcal{S}, f)(x_{j^*}^{k-1}) &= \mathrm{ev}(\mathcal{S}, F)(\lambda_0^{k-1} + \lambda_1^{k-1} x_{j^*} + \cdots + \lambda_{k-1}^{k-1} x_{j^*}^{k-1}),
\end{aligned}$$

where $\deg_{x_j}(\lambda_p^\ell) < n_j$ for $j \in [m] \setminus \{j^*\}$ and $\deg_{x_{j^*}}(\lambda_p^\ell) = 0$ for all $p, t \in \{0, \ldots, k-1\}$. Observe that for every $r \in [k-1]$,

$$\mathrm{ev}(\mathcal{S}, f)(x_{j^*}^r) = \mathrm{ev}(\mathcal{S}, f)(1 \cdot x_{j^*}^r) = \mathrm{ev}(\mathcal{S}, F)((\lambda_0^0 + \lambda_1^0 x_{j^*} + \cdots + \lambda_{k-1}^0 x_{j^*}^{k-1}) \cdot x_{j^*}^r).$$

Thus, for every $r \in [k-1]$,

$$\mathrm{ev}(\mathcal{S}, F)((\lambda_0^0 + \lambda_1^0 x_{j^*} + \cdots + \lambda_{k-1}^0 x_{j^*}^{k-1}) \cdot x_{j^*}^r) = \mathrm{ev}(\mathcal{S}, F)(\lambda_0^r + \lambda_1^r x_{j^*} + \cdots + \lambda_{k-1}^r x_{j^*}^{k-1}),$$

which means that

$$(\lambda_0^0 + \lambda_1^0 x_{j^*} + \cdots + \lambda_{k-1}^0 x_{j^*}^{k-1}) \cdot x_{j^*}^r = \lambda_0^r + \lambda_1^r x_{j^*} + \cdots + \lambda_{k-1}^r x_{j^*}^{k-1} \mod I(\mathcal{S}).$$

Define $h_r := (\lambda_0^0 + \lambda_1^0 x_{j^*} + \cdots + \lambda_{k-1}^0 x_{j^*}^{k-1}) \cdot x_{j^*}^r$ and $h_r' := \lambda_0^r + \lambda_1^r x_{j^*} + \cdots + \lambda_{k-1}^r x_{j^*}^{k-1}$. Recall that the generators of the vanishing ideal $I(\mathcal{S})$ have degree n_j respect to x_j, for $j \in [m]$. As $\deg_{x_j}(\lambda_p^\ell) < n_j$ and $\deg_{x_j}(h_r)$, $\deg_{x_j}(h_r') < n_j$ for $r \in [k-1]$ and $j \in [m] \setminus \{j^*\}$. We can also see that $\deg_{x_{j^*}}(h_r') < k < n_{j^*}$ for $r \in [k-1]$. Thus, in order to be able to compare h_r and h_r', we just need to know $\deg_{x_{j^*}}(h_r)$.

As $\deg_{x_j^*}(h_1) = k < n_{j^*}$, $h_1 = h_1'$. Thus, $\lambda_{k-1}^0 = 0$. As $\lambda_{k-1}^0 = 0$, $\deg_{x_j^*}(h_2) = k < n_{j^*}$. This implies that $h_2 = h_2'$. Thus, $\lambda_{k-2}^0 = 0$. By induction, we see that $\lambda_{k-1}^0 = \lambda_{k-2}^0 = \cdots = \lambda_2^0$. As a consequence, $\deg_{x_j^*}(h_{k-1}) = k < n_{j^*}$. Thus, $h_{k-1} = h_{k-1}'$, which means

that $\lambda_1^0 = 0$. We conclude that $\mathrm{ev}(\mathcal{S}, f)(1) = \mathrm{ev}(\mathcal{S}, F)(\lambda_0^0)$. Then, $\frac{F}{f} = \lambda_0^0$, from which we get that $\deg_{x_{j^*}}\left(\frac{F}{f}\right) = 0$. □

Observe that the condition $\deg_{x_{j^*}}\left(\frac{F}{f}\right) = 0$ means that there is an element $p(\boldsymbol{x})$ in $\mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $\deg_{x_{j^*}}(p) = 0$ and $p(\boldsymbol{s}_i) = \frac{F(\boldsymbol{s}_i)}{f(\boldsymbol{s}_i)}$, which happens if and only if $F - pf \in I(\mathcal{S})$. When $m = 1,\ p = \lambda \in \mathbb{F}_{q^t}$. Since $\deg(F - \lambda f) < n,\ F = \lambda f$. Thus, for the case $m = 1$, *i.e.* only one variable, if $\mathrm{T}(\mathcal{S}, k, f) = \mathrm{T}(\mathcal{S}, k, F)$ and $k < n$, then $F = \lambda f$, which is [12, Lemma 2.5] without the restriction $k \leq \frac{n}{2}$.

By Remark 3, if $\mathrm{T}(\mathcal{S}, g)$ is one of the trivial spaces $\{\mathbf{0}\}$ or $\mathbb{F}_{q^t}^n$, then the dual is also a tensor product of GRS codes via Goppa codes. For the case when $\mathrm{T}(\mathcal{S}, g)$ is nontrivial, we have the following result.

Theorem 17. *Given $g = g_1 \dots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$, there exists $f = f_1 \dots f_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that*

$$\mathrm{T}(\mathcal{S}, g)^{\perp} = \mathrm{T}(\mathcal{S}, f),$$

if and only for some $j^* \in [m]$, the following hold:

(i) $\deg(f_{j^*} g_{j^*}) = n_{j^*}$,
(ii) $\deg(f_j) = \deg(g_j) = n_j$, *for all* $j \in [m] \setminus \{j^*\}$, *and*
(iii) $\deg_{x_{j^*}}\left(\frac{fg}{L}\right) = 0$.

Proof. By Theorem 11, we just need to check that $\mathrm{T}(\mathcal{S}, f) = \mathrm{ACar}(\mathcal{S}, g)$ if and only if (i)-(iii) are valid. By Definition 7, $\mathrm{ACar}(\mathcal{S}, g) = \mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$, where $\boldsymbol{k}_g = (n_1 - \deg(g_1), \dots, n_m - \deg(g_m))$. Thus, we will prove that $\mathrm{T}(\mathcal{S}, f) = \mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$ if and only if (i)-(iii) are true. Denote the j-th standard vector in $\mathbb{F}_{q^t}^m$ by $\boldsymbol{e}_j$.

($\Leftarrow$) Assume (i)-(iii). By (iii), $\deg_{x_{j^*}}\left(\frac{L}{fg}\right) = \deg_{x_{j^*}}\left(\frac{fg}{L}\right) = 0$. There is $p(\boldsymbol{x}) \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $\deg_{x_{j^*}}(p) = 0$ and $p(\boldsymbol{s}_i) = \frac{L(\boldsymbol{s}_i)}{(fg)(\boldsymbol{s}_i)}$. Then $\frac{L(\boldsymbol{s}_i)}{g(\boldsymbol{s}_i)} = (fp)(\boldsymbol{s}_i)$, which means that $\deg_{x_{j^*}}\left(\frac{L}{g}\right) = \deg_{x_{j^*}}(f) = \deg(f_{j^*})$. By (ii), $\boldsymbol{k}_g = (0, \dots, n_{j^*} - \deg(g_{j^*}), \dots, 0)) = (n_{j^*} - \deg(g_{j^*}))\,\boldsymbol{e}_{j^*}$. Using (i), $\boldsymbol{k}_g = \deg(f_{j^*})\boldsymbol{e}_{j^*}$. Thus, due Definition 7, $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$ is generated by the vectors $\left(\frac{\boldsymbol{s}_1^{\boldsymbol{a}}}{\frac{L}{g}(\boldsymbol{s}_1)}, \dots, \frac{\boldsymbol{s}_n^{\boldsymbol{a}}}{\frac{L}{g}(\boldsymbol{s}_n)}\right)$, where $0 \leq a_j < n_j$, for all $j \in [m] \setminus \{j^*\}$, and $0 \leq a_{j^*} < \deg(f_{j^*})$. We conclude that for $\boldsymbol{k} := (n_1, \dots, n_{j^*-1}, \deg(f_{j^*}), n_{j^*+1}, \dots, n_m)$, $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right) = \mathrm{T}\left(\mathcal{S}, \boldsymbol{k}, \frac{L}{g}\right)$. By (ii) $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, f)$. Combining (iii) and Lemma 16, we obtain $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right) = \mathrm{T}\left(\mathcal{S}, \boldsymbol{k}, \frac{L}{g}\right) = \mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, f)$.

($\Rightarrow$) Assume $\mathrm{T}(\mathcal{S}, f) = \mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$, where $\boldsymbol{k}_g = (n_1 - \deg(g_1), \dots, n_m - \deg(g_m))$. By Remark 3, as $\mathrm{T}(\mathcal{S}, f)$ is nontrivial, then $\deg(g_j) > 0$, for $j \in [m]$. According to the proof of Lemma 9 (iii), $\mathcal{B} = \left\{ \frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{x_j^{\deg(g_j)}} : j \in [m] \right\}$ is a generating set of $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$. By Definition 1, there is a unique generating monomial for $\mathrm{T}(\mathcal{S}, f)$, meaning a monomial $\boldsymbol{x}^{\boldsymbol{a}} \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $\boldsymbol{x}^{\boldsymbol{b}}$ divides $\boldsymbol{x}^{\boldsymbol{a}}$ if and only if $\mathrm{ev}(\mathcal{S}, f)(\boldsymbol{x}^{\boldsymbol{b}})$ is in

$\mathrm{T}(\mathcal{S}, f)$. This means that the augmented code $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$ has a unique generating monomial, and it should be one of the elements in $\mathcal{B}$. Thus, there is $j^* \in [m]$ such that $M := \frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{x_{j^*}^{\deg(g_{j^*})}}$ is the generating monomial for both $\mathrm{T}(\mathcal{S}, f)$ and $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$. As M is a generating monomial of $\mathrm{T}(\mathcal{S}, f)$, then $\deg(f_j) = n_j$, for all $j \in [m] \setminus \{j^*\}$, and $\deg(f_{j^*}) = n_{j^*} - \deg(g_{j^*})$. As M is a generating monomial of $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$, then $\boldsymbol{k}_g = (0, \ldots, n_{j^*} - \deg(g_{j^*}), \ldots, 0)$, which implies $\deg(g_j) = n_j$, for all $j \in [m] \setminus \{j^*\}$. Thus, (i)-(ii) are valid and $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, f) = \mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right) = \mathrm{T}\left(\mathcal{S}, \boldsymbol{k}, \frac{L}{g}\right)$, where $\boldsymbol{k} := (n_1, \ldots, n_{j^*-1}, \deg(f_{j^*}), n_{j^*+1}, \ldots, n_m)$. By Lemma 16, (iii) is also true. □

In [12], the authors use Goppa codes (the case $t = m = 1$) to prove that the intersection of certain generalized Reed-Solomon codes are also generalized Reed-Solomon codes. As a consequence, they determine the hulls of certain generalized Reed-Solomon codes. Here, our focus is slightly different. Even so, taking the special case $t = m = 1$ allows us to recover those results. More generally, the hull of a tensor product of generalized Reed-Solomon codes via Goppa codes is also a tensor product of generalized Reed-Solomon codes via Goppa codes, and the hull of a multivariate Goppa code contains a multivariate Goppa code (with equality when $t = 1$). More precisely, we have the following result.

Corollary 18. *Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$, g and f be as in Theorem 17. Then the following hold.*

(i) $\mathrm{Hull}\left(\mathrm{T}(\mathcal{S}, g)\right) = \mathrm{T}(\mathcal{S}, \gcd(f, g)) = \mathrm{Hull}\left(ACar(\mathcal{S}, g)\right)$.
(ii) $\Gamma(\mathcal{S}, \mathrm{lcm}(f, g)) \subseteq \mathrm{Hull}\left(\Gamma(\mathcal{S}, g)\right)$, *with equality when* $t = 1$.

Proof. (i) By Theorems 11 and 17,

$$\mathrm{T}(\mathcal{S}, f) = \mathrm{T}(\mathcal{S}, g)^{\perp} = \mathrm{ACar}(\mathcal{S}, g) \text{ and } \mathrm{T}(\mathcal{S}, g) = \mathrm{T}(\mathcal{S}, f)^{\perp} = \mathrm{ACar}(\mathcal{S}, f).$$

Thus, the result is a consequence of Theorem 15 (i).

(ii) By the poof of (i), $\mathrm{T}(\mathcal{S}, g) = \mathrm{T}(\mathcal{S}, f)^{\perp} = \mathrm{ACar}(\mathcal{S}, f)$. By Corollary 5, $\Gamma(\mathcal{S}, g)^{\perp} = tr\left(\mathrm{T}(\mathcal{S}, g)\right) = tr\left(\mathrm{ACar}(\mathcal{S}, f)\right) \supseteq \Gamma(\mathcal{S}, f)$. Thus,

$$\mathrm{Hull}\left(\Gamma(\mathcal{S}, g)\right) = \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g)^{\perp} \supseteq \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, f) = \Gamma(\mathcal{S}, \mathrm{lcm}(g, f)),$$

where the last equation holds due to Theorem 15 (ii). When $t = 1$, $\mathrm{ACar}(\mathcal{S}, f) = \Gamma(\mathcal{S}, f)$, so $tr\left(\mathrm{ACar}(\mathcal{S}, f)\right) = \Gamma(\mathcal{S}, f)$. □

Using the conditions in Theorem 17, we can also conclude that the dimension of the Hull of the tensor product of GRS via Goppa code is

$$\dim\left(\mathrm{Hull}\left(\mathrm{T}(\mathcal{S}, g)\right)\right) = \dim\left(\mathrm{T}(\mathcal{S}, \gcd(f, g))\right) = \deg\left(\gcd(f, g)\right), \tag{11}$$

and the dimension of the hull of the multivariate Goppa code is lower bounded by

$$\dim\left(\mathrm{Hull}\left(\Gamma(\mathcal{S}, g)\right)\right) \geq \dim\left(\Gamma(\mathcal{S}, \mathrm{lcm}(f, g))\right) \geq n - t\deg\left(\mathrm{lcm}(f, g)\right), \tag{12}$$

with equality when $t = 1$.

5. Quantum, LCD, self-orthogonal and self-dual codes

In this section, we design entanglement quantum error-correcting codes, LCD, self-orthogonal, and self-dual codes from multivariate Goppa codes and tensor product of GRS codes via a Goppa code relying on the hulls found in the previous section.

Entanglement-assisted quantum error-correcting codes, introduced in [6], utilize entangled qubits as an enabling mechanism which allows for any linear code to be used to construct a quantum error-correcting code. These codes are a departure from constructions that employ self-dual codes. Below we use the standard notation $[[n,k,d;c]]_q$ code to mean a q-ary entanglement-assisted quantum error-correcting code (EAQECC) that encodes k qubits into n qubits, with minimum distance d, and c required entangled qubits. Guenda, Jitman and Gulliver [18], building on work of Wilde and Brune [31], showed that the shared entanglement necessary can be captured by the dimension of the hull of the linear code used. In particular, they prove the following.

Lemma 19. [18, Corollary 3.2] *Given an $[n,k,d]$ code C over $\mathbb{F}_q$, there exist EAQECCs with parameters*

$$[[n, k-\dim(Hull(C)), d, n-k-\dim(Hull(C))]]_q \quad \text{and}$$
$$[[n, n-k-\dim(Hull(C)), d(C^\perp), k-\dim(Hull(C))]]_q.$$

Proposition 20. *Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$, g and f be as in Theorem 17. Then the code $\mathrm{T}(\mathcal{S}, g)$ gives rise to EAQECCs with parameters*

$$[[n, \deg(g)-\deg(\gcd), \deg(f_{j^*})+1; \deg(f)-\deg(\gcd)]]_{q^t} \quad \text{and}$$
$$[[n, \deg(f)-\deg(\gcd), \deg(g_{j^*})+1; \deg(g)-\deg(\gcd)]]_{q^t},$$

where $\gcd := \gcd(g, g')$. *The code $\Gamma(\mathcal{S}, g)$ gives rise to EAQECCs with parameters*

$$[[n, \leq t(\deg(\mathrm{lcm})+\deg(g))-n, \geq \deg(f_{j^*})+1; \leq t\deg(\mathrm{lcm})-\deg(g)]]_q \quad \text{and}$$
$$[[n, \leq t\deg(\mathrm{lcm})-\deg(g), \geq \deg(g_{j^*})+1; \leq t(\deg(\mathrm{lcm})+\deg(g))-n]]_q,$$

where $\mathrm{lcm} := \mathrm{lcm}(g, g')$, *and equalities in the parameters of the codes when $t = 1$.*

Proof. The first pair of quantum codes is a consequence of Lemma 19, Remark 2, and Equation (11). The second pair of quantum codes follows from Lemma 19, Corollary 13, and Inequality (12). □

Note that when $t = 1$, which means that $\mathcal{S} \subseteq \mathbb{F}_q^m$, the two pairs of q-ary entanglement-assisted quantum error-correcting codes presented in Proposition 20 coincide. This happens becase in this case, from Corollary 5, we have that $\Gamma(\mathcal{S}, g)^\perp = tr(\mathrm{T}(\mathcal{S}, g)) = \mathrm{T}(\mathcal{S}, g)$, which means that $\mathrm{T}(\mathcal{S}, g) = \Gamma(\mathcal{S}, f)$ and $\mathrm{T}(\mathcal{S}, f) = \Gamma(\mathcal{S}, g)$.

An $[[n,k,d;c]]_q$ EAQECC satisfies the Singleton Bound [6] $n + c - k \geq 2(d-1)$, where $0 \leq c \leq n-1$. The code attaching this bound is called an MDS EAQECC. As a consequence of Proposition 20, we recover [12, Theorem 4.5].

Corollary 21. *Let $\mathcal{S} \subseteq \mathbb{F}_q^m$, g and f be as in Theorem 17. Then the code $\mathrm{T}(\mathcal{S}, g)$ gives rise to an MDS EAQECC.*

Proof. This is a consequence of Proposition 20. □

Using the results of Section 4, we now give conditions to find families of codes that are LCD, self-orthogonal, or self-dual.

Corollary 22. *Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$, g and f be as in Theorem 17. Then the following hold.*

(i) $\mathrm{T}(\mathcal{S}, g)$ *is LCD if there exists* $j \in [m]$ *with* $\gcd(f_j, g_j) \in \mathbb{F}_{q^t}$.
(ii) $\mathrm{T}(\mathcal{S}, g)$ *is self-orthogonal if* g *divides* f.
(iii) $\mathrm{T}(\mathcal{S}, g)$ *is self-dual if* $f = g$.
(iv) $\Gamma(\mathcal{S}, g)$ *is LCD if* $t = 1$ *and* $\deg_{x_j}(\mathrm{lcm}(f, g)) \geq n_j$ *for all* $j \in [m]$.
(v) $\Gamma(\mathcal{S}, g)$ *is self-orthogonal if* $t = 1$ *and* f *divides* g.
(vi) $\Gamma(\mathcal{S}, g)$ *is self-dual if* $t = 1$ *and* $f = g$.

Proof. (i) By Theorems 11 and 17,

$$\mathrm{T}(\mathcal{S}, f) = \mathrm{T}(\mathcal{S}, g)^{\perp} = \mathrm{ACar}(\mathcal{S}, g) \text{ and } \mathrm{T}(\mathcal{S}, g) = \mathrm{T}(\mathcal{S}, f)^{\perp} = \mathrm{ACar}(\mathcal{S}, f).$$

Thus, the result is a consequence of Theorem 15 (i).

(ii) By the poof of (i), $\mathrm{T}(\mathcal{S}, g) = \mathrm{T}(\mathcal{S}, f)^{\perp} = \mathrm{ACar}(\mathcal{S}, f)$. By Corollary 5, $\Gamma(\mathcal{S}, g)^{\perp} = tr\left(\mathrm{T}(\mathcal{S}, g)\right) = tr\left(\mathrm{ACar}(\mathcal{S}, f)\right) \supseteq \Gamma(\mathcal{S}, f)$. Thus,

$$\mathrm{Hull}\left(\Gamma(\mathcal{S}, g)\right) = \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g)^{\perp} \supseteq \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, f) = \Gamma(\mathcal{S}, \mathrm{lcm}(g, f)),$$

where the last equation holds because Theorem 15 (ii). When $t = 1$, $\mathrm{ACar}(\mathcal{S}, f) = \Gamma(\mathcal{S}, f)$, so $tr\left(\mathrm{ACar}(\mathcal{S}, f)\right) = \Gamma(\mathcal{S}, f)$.

By Remark 3, we obtain the conditions about the LCD codes. The self-dual conditions are a consequence of the fact that when $f = g$, then $g = \gcd(f, g) = \mathrm{lcm}(f, g)$. □

Corollary 22 gives a simple path (with some help from the coding theory package [2] for Macaulay2 [17] or Magma [5]) to find codes with a large length that are LCD, self-orthogonal, or self-dual codes. The key steps are the following.

(1) Give sets $S_1, S_2 \subseteq \mathbb{F}_{q^t}$ of cardinalities n_1 and n_2, respectively.
(2) Define $L_i := \prod_{s \in S_i}(x - s) \in \mathbb{F}_{q^t}[x]$. Find the formal derivatives L_i'.
(3) Find $f_1, g_1 \in \mathbb{F}_{q^t}[x]$ such that $f_1 g_1 = \lambda_1 L_1' + \beta_1 L_1$, with $\lambda_1, \beta_1 \in \mathbb{F}_{q^t}$.
(4) Find $f_2, g_2, p \in \mathbb{F}_{q^t}[x]$ such that $f_2 g_2 = \lambda_2 L_2' + p L_2$, with $\deg(p) = n_2$.

Then the codes $\mathrm{T}(\mathcal{S}, g_1 g_{2,m})$ and $\Gamma(\mathcal{S}, g_1 g_{2,m})$, where $g_{2,m} := g_2(x_1) \ldots g_2(x_m)$, have both length $n_1 n_2^m$. As m is independent of the steps (1)-(4), after the appropriate polynomials have been found, codes with different lengths can be derived. Observe that this is a different approach than given in [12]. An immediate difference is that using GRS codes, the length of the code is always bounded by the size of the field. This restriction is not presented in the tensor product. Even more, the results of Section 5 enable a single set of defining polynomials to produce a family of codes with different lengths over a certain field (cf. [12, Theorem 2.6]). We show this in the following examples.

Example 23 (Family of long LCD codes)**.** Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$. Take $S_1 := \{0, 1, a, a^7\}$ and $S_2 := \{1, a^5, a^7\}$. Define the polynomials $f_1 := x + 1$, $g_1 := 2x^3 + a^5 x^2 + a^5 x + 1$, and $f_2 := g_2 := x^3 + ax^2 + 2x$. Then

$$f_1 g_1 = 2L_1' + 2L_1 \qquad \text{and} \qquad f_2 g_2 = a^2 L_2' + pL_2,$$

where $p(x) = x^3 + a^5 x^2 + a^2 x + a^6$. Then, for every $m \geq 0$, define the polynomial in m variables $f_{2,m} := f_2(x_1) \ldots f_2(x_m)$. As $\gcd(f_1, g_1) = 1$, by Remark 2 and Corollary 18, the tensor product $\mathrm{T}(\mathcal{S}, f_1 f_{2,m})$ is a $[4 \cdot 3^m, 3^m]$ LCD code over $\mathbb{F}_9$.

Example 24 (Family of long self-orthogonal codes)**.** Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$. Take $S_1 := \{0, 1, 2, a\}$ and $S_2 := \{1, a^5, a^7\}$. Define the polynomials $f_1 := ax^3 + 2x^2 + a^7x + a$, $g_1 := a^2x + 1$, and $f_2 := g_2 := x^3 + ax^2 + 2x$. Then

$$f_1g_1 = L_1' + a^3L_1 \qquad \text{and} \qquad f_2g_2 = a^2L_2' + pL_2,$$

where $p(x) = x^3 + a^5x^2 + a^2x + a^6$. Then, for every $m \geq 0$, define the polynomial in m variables $g_{2,m} := g_2(x_1) \dots g_2(x_m)$. As g_1 divides f_1, and g_2 divides f_2, by Remark 2 and Corollary 18, the tensor product $\mathrm{T}(\mathcal{S}, g_1g_{2,m})$ is a $[4 \cdot 3^m, 3^m]$ self-orthogonal code over $\mathbb{F}_9$.

Example 25 (Family of long self-dual codes)**.** Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$. Take $S_1 := \{a, a^2, a^3, a^5, a^6, a^7\}$ and $S_2 := \{1, a^5, a^7\}$. Define the polynomials $f_1 := g_1 := x^3 + 2x + 2$ and $f_2 := g_2 := x^3 + ax^2 + 2x$. Then

$$f_1g_1 = L_1' + L_1 \qquad \text{and} \qquad f_2g_2 = a^2L_2' + pL_2,$$

where $p(x) = x^3 + a^5x^2 + a^2x + a^6$. Then, for every $m \geq 0$, define the polynomial in m variables $g_{2,m} := g_2(x_1) \dots g_2(x_m)$. As $g_1 = f_1$, and $g_2 = f_2$, by Remark 2 and Corollary 18, the tensor product $\mathrm{T}(\mathcal{S}, g_1g_{2,m})$ is a $[6 \cdot 3^m, 3^{m+1}]$ self-dual code over $\mathbb{F}_9$.

6. Conclusion

In this paper, we defined multivariate Goppa codes which generalize the classical Goppa codes. Similar to classical Goppa codes, they can be described via a parity checks and as subfield subcodes of a family of evaluation codes. In particular, we show that considering tensor products of generalized Reed-Solomon codes via Goppa codes leads to a parity check matrix whose kernel restricted to the base field yields the multivariate Goppa codes. We also prove that multivariate Goppa codes are subfield subcodes of augmented Cartesian codes. These perspectives provide information about the code parameters as well as their hulls. As a consequence, we obtain some entanglement- assisted quantum error-correcting, LCD, self-orthogonal, and self-dual codes. We leave it as an exercise for the interested reader to translate the results in this paper to expurgated subcodes of multivariate Goppa codes.

References

[1] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth Patterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen. Wang. Classic McEliece: conservative code-based cryptography, 2020."Supporting documentation". URL: `https://classic.mceliece.org/nist/mceliece-20201010.pdf`.

[2] Taylor Ball, Eduardo Camps, Henry Chimal-Dzul, Delio Jaramillo-Velez, Hiram H López, Nathan Nichols, Matthew Perkins, Ivan Soprunov, German Vera-Martínez, and Gwyn Whieldon. Coding theory package for Macaulay2. *Journal of Software for Algebra and Geometry*, to appear. `arXiv:2007.06795`.

[3] E. Berlekamp. Goppa codes. *IEEE Transactions on Information Theory*, 19(5):590–592, 1973. `doi:10.1109/TIT.1973.1055088`.

[4] Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, and Wen. Wang. Classic McEliece: conservative code-based cryptography, 2017."Supporting documentation". URL: `https://classic.mceliece.org/nist.html`.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997. doi:10.1006/jsco.1996.0125.

[6] Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006. doi:10.1126/science.1131563.

[7] Eduardo Camps, Hiram H. López, Gretchen L. Matthews, and Eliseo Sarmiento. Polar decreasing monomial-Cartesian codes. *IEEE Transactions on Information Theory*, 67(6):3664–3674, 2021. doi:10.1109/TIT.2020.3047624.

[8] Eduardo Camps-Moreno, Ignacio García-Marco, Hiram H. López, Irene Márquez-Corbella, Edgar Martínez-Moro, and Eliseo Sarmiento. On decoding hyperbolic codes, 2021. arXiv:2107.12594.

[9] J. Little D. Cox and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics, Springer-Verlag, 2008.

[10] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes (corresp.). *IEEE Transactions on Information Theory*, 21(5):575–576, 1975. doi:10.1109/TIT.1975.1055435.

[11] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.

[12] Yanyan Gao, Qin Yue, Xinmei Huang, and Jun Zhang. Hulls of generalized Reed-Solomon codes via Goppa codes and their applications to quantum codes. *IEEE Transactions on Information Theory*, 67(10):6619–6626, 2021. doi:10.1109/TIT.2021.3074526.

[13] Parikshit Gopalan, Venkatesan Guruswami, and Prasad Raghavendra. List decoding tensor products and interleaved codes. *SIAM Journal on Computing*, 40(5):1432–1462, October 2011. doi:10.1137/090778274.

[14] V. D. Goppa. A new class of linear correcting codes. *Problems Inform. Transmission*, 6(3):207–212, 1970.

[15] V. D. Goppa. A rational representation of codes and (l,g)-codes. *Problems Inform. Transmission*, 7(3):223–229, 1971.

[16] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. URL: http://www.codetables.de.

[17] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. URL: http://www.math.uiuc.edu/Macaulay2/.

[18] Kenza Guenda, Somphong Jitman, and T. Aaron Gulliver. Constructions of good entanglement-assisted quantum error correcting codes. *Designs, Codes and Cryptography*, 86(1):121–136, January 2018. doi:10.1007/s10623-017-0330-z.

[19] J. Harris. *Algebraic Geometry. A first course*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[20] W. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[21] Hiram H. López, Gretchen L. Matthews, and Ivan Soprunov. Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes. *Designs, Codes and Cryptography*, 88(8):1673–1685, 2020. doi:10.1007/s10623-020-00726-x.

[22] Hiram H. López, Gretchen L. Matthews, and Daniel Valvo. Erasures repair for decreasing monomial-cartesian and augmented reed-muller codes of high rate. *IEEE Transactions on Information Theory*, 2021. doi:10.1109/TIT.2021.3130096.

[23] Hiram H. López, Carlos Rentería-Márquez, and Rafael H. Villarreal. Affine Cartesian codes. *Designs, Codes and Cryptography*, 71(1):5–19, 2014. doi:10.1007/s10623-012-9714-2.

[24] Hiram H. López, Ivan Soprunov, and Rafael H. Villarreal. The dual of an evaluation code. *Designs, Codes and Cryptography*, 89(7):1367–1403, 2021. doi:10.1007/s10623-021-00872-w.

[25] 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)*, pages 438–443, 2021. doi:10.1109/ISIT45174.2021.9517854.

[26] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes*. North-Holland, 1977.

[27] James L. Massey. Linear codes with complementary duals. *Discrete Mathematics*, 106-107:337–342, 1992. doi:10.1016/0012-365X(92)90563-U.

[28] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.

[29] J. H. van Lint. *Introduction to coding theory*. Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1999.
[30] R. H. Villarreal. *Monomial Algebras*. Monographs and Research Notes in Mathematics, 2015.
[31] Mark M. Wilde and Todd A. Brun. Optimal entanglement formulas for entanglement-assisted quantum coding. *Phys. Rev. A*, 77:064302, Jun 2008. doi:10.1103/PhysRevA.77.064302.

(Hiram H. López) Department of Mathematics, Cleveland State University, Cleveland, OH USA
Email address: h.lopezvaldez@csuohio.edu

(Gretchen L. Matthews) Department of Mathematics, Virginia Tech, Blacksburg, VA USA
Email address: gmatthews@vt.edu