Multivariate Goppa codes

Hiram H. López and Gretchen L. Matthews, *Senior Member, IEEE*

***Abstract*—In this paper, we introduce multivariate Goppa codes, which contain, as a particular 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 a tensor product 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 some instances, 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.**

***Index Terms*—Goppa codes, augmented Cartesian codes, tensor products of Reed-Solomon codes, quantum error-correcting codes, LCD, self-dual, self-orthogonal. 2010 Mathematics Subject Classification. Primary 94B05; Secondary 11T71, 14G50.**

I. Introduction

Goppa codes were introduced in 1971 by V. D. Goppa [13], [14] 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 the only remaining candidates in the NIST Post-Quantum Cryptography Standardization [1], [4] process, employs Goppa codes [27]. Goppa codes can be viewed from several different perspectives, each giving a window into their capabilities. We generalize Goppa codes to a multivariate case in this work.

Consider $g \in \mathbb{F}_{q^t}[\boldsymbol{x}] := \mathbb{F}_{q^t}[x_1, \ldots, x_m]$ and the *Cartesian product* $\mathcal{S} := S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$ of non-empty subsets $S_1, \ldots, S_m \subseteq \mathbb{F}_{q^t}$. Enumerate the elements of $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}^m$. Assume that $g(\boldsymbol{s}_i) \neq 0$ for all $i \in [n]$ and that g can be expressed as a product $g = g_1 \cdots g_m$, where $g_i \in \mathbb{F}_{q^t}[x_i]$. The *multivariate Goppa code* is

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

where $c = (c_1, \ldots, c_n)$ and $\boldsymbol{s}_i := (s_{i1}, \ldots, s_{im}) \in \mathcal{S}$. Taking $m = 1$, we obtain the Goppa codes as in [3], [13], [14]. 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, compared with either classical Goppa codes or generalized Reed-Solomon (GRS) codes. Said differently, smaller alphabets may be used to produce codes of a given length by allowing larger values of t and m. As we will see in Corollary 10, taking larger values of m allows one to obtain codes of the same lengths over the same field with potentially larger dimensions.

To study multivariate Goppa codes, we may use two families of codes that appeared recently in the literature. Generalized Reed-Solomon codes via Goppa codes were studied by Y. Gao, Q. Yue, X. Huang, and J. Zhang in [12], and augmented Cartesian (ACar) codes, a family of evaluation codes that was introduced in [22], [24]. Both families will be reviewed in Section III.

In Section IV, to present a full picture of multivariate Goppa codes similar to that of classical Goppa codes, we will prove the following representations.

> (**Theorem** 8) *Parity check matrix.* If $\mathrm{T}(\mathcal{S}, g)$ is the tensor product of generalized Reed-Solomon codes via Goppa codes, then
>
> $$\Gamma(\mathcal{S}, g) = (\mathrm{T}(\mathcal{S}, g)^{\perp})_q.$$
>
> If T is a generator matrix of $\mathrm{T}(\mathcal{S}, g)$, then
>
> $$\Gamma(\mathcal{S}, g) = \{\boldsymbol{c} \in \mathbb{F}_q^n : \mathrm{T}\, \boldsymbol{c}^T = 0\}.$$
>
> (**Theorem** 14) *Subfield subcode.* If $ACar(\mathcal{S}, g)$ is an augmented Cartesian code, then
>
> $$\Gamma(\mathcal{S}, g) = ACar(\mathcal{S}, g)_q.$$
>
> (**Corollary** 15) *The dual.* If $tr\,(T(\mathcal{S}, g))$ is the trace of the code $T(\mathcal{S}, g)$, then
>
> $$\Gamma(\mathcal{S}, g)^{\perp} = tr\,(T(\mathcal{S}, g)).$$

Moreover, these observations provide information on the basic parameters of the multivariate Goppa code $\Gamma(\mathcal{S}, g)$. Examples that demonstrate the results are provided throughout Section IV.

In Section V, we study subcodes, intersections, and hulls of multivariate Goppa codes. Each of these objects depends

The work of Hiram H. López was partly supported by an AMS–Simons Travel Grant. The work of Gretchen L. Matthews was partly supported by NSF DMS-1855136, NSF DMS-2037833, and the Commonwealth Cyber Initiative. *(Corresponding author: Hiram H. López.)*

H. H. López is with the Department of Mathematics and Statistics, Cleveland State University, Cleveland, OH, USA, e-mail: h.lopezvaldez@csuohio.edu.

G. L. Matthews is with the Department of Mathematics, Virginia Tech, Blacksburg, VA, USA, e-mail: gmatthews@vt.edu.

on the polynomial g in $\mathbb{F}_{q^t}[\boldsymbol{x}]$ used to define the multivariate Goppa code. As a byproduct of this effort, we also obtain results for the tensor products of generalized Reed-Solomon codes via Goppa codes and augmented Cartesian codes. In Section VI, we design quantum, LCD, self-orthogonal, and self-dual codes from multivariate Goppa codes and tensor products of generalized Reed-Solomon codes via Goppa codes. One of the main contributions in Section VI is an algorithm to find LCD, self-orthogonal, and self-dual codes. This approach is different from that given in [12], which requires that the size of the field always bounds the length of the code; this restriction is not needed in this paper, meaning longer codes over smaller alphabets can be defined via the tools introduced in this paper. Even more, the results of Section VI 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 examples near the end of Section VI to demonstrate the constructions of families of long entanglement-assisted quantum error-correcting codes, LCD codes, self-orthogonal, and self-dual codes. Finally, a summary is given as a conclusion in Section VII.

II. Conclusion

This paper defined multivariate Goppa codes that generalize the classical Goppa codes. Similar to classical Goppa codes, they are described via a parity check matrix and as subfield subcodes of a family of evaluation codes. In particular, we showed that the tensor product 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 proved that multivariate Goppa codes are subfield subcodes of augmented Cartesian codes. These perspectives provided information about the code parameters as well as their hulls. Consequently, we obtained q-ary entanglement-assisted quantum error-correcting codes, 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.

III. Preliminaries

This section develops the background that will be useful in this paper. Subsection III-A introduces the notation to be used throughout. More information about coding theory can be found in [20], [25], [30]. Subsections III-B and III-C review particular code constructions that will provide insight into the multivariate Goppa codes. References for vanishing ideals and related algebraic concepts used in this work are [8], [10], [19], [31].

A. Notation

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

$$C^\perp := \left\{\boldsymbol{w} \in \mathbb{F}_{q^t}^n : \boldsymbol{w} \cdot \boldsymbol{c} = 0 \ \forall \boldsymbol{c} \in C\right\};$$

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*) [26] if $\operatorname{Hull}(C) = \{\boldsymbol{0}\}$, *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$.

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

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

Given a generator matrix G_1 of a code C_1 and a generator matrix G_2 of a code C_2, the code $C_1 \otimes C_2$ is defined as the code whose generator matrix is $G_1 \otimes G_2$. Given a positive integer $k \in \mathbb{Z}^+$, $\mathbb{F}_{q^t}[x]_{<k}$ denotes the set of polynomials in indeterminate x of degree less than k.

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 $\mathbb{F}_{q^t}[\boldsymbol{x}]$ where $\mathbb{N}$ is the set of nonnegative integers. The *graded-lexicographic order* $\prec$ on the set of monomials of $\mathbb{F}_{q^t}[\boldsymbol{x}]$ 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 non-zero 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.*

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

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

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

Recall that given an $[n,k,d]$ code $C \subseteq \mathbb{F}_{q^t}^n$, its *subfield subcode* over $\mathbb{F}_q$ and its *trace code* are defined, respectively, by

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

and

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

By [25, Ch. 7. §7.], $tr(C)$ is an $[n, k^*, d^*]$ over $\mathbb{F}_q$, where $k \leq k^* \leq tk$ and $d^* \leq d$. According to Delsarte's Theorem [9, Theorem 2], $C_q^\perp = tr\left(C^\perp\right)$.

B. Tensor products of generalized Reed-Solomon codes

In this subsection, we review the tensor products of generalized Reed-Solomon codes via Goppa codes.

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 $S = \{s_1,\ldots,s_n\} \subseteq \mathbb{F}_{q^t}$. A GRS code in the particular case $k = \deg(g)$ is called a *GRS code 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 Goppa codes were 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 $n \le q^t$, meaning it is maximum distance separable (MDS). As we will see in Section IV, the tensor product of generalized Reed-Solomon codes plays an important role in the duals of multivariate Goppa codes. In preparation, we define the tensor product of generalized Reed-Solomon codes next.

Definition 1. Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$ with $n_j :=\mid S_j \mid$ and $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ be such that $g(\boldsymbol{s}) \neq 0$ for all $\boldsymbol{s} \in \mathcal{S}$ and $\deg(g_j) \le n_j$ for all $j \in [m]$. The *tensor product of generalized Reed-Solomon codes via Goppa codes* is

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

Remark 2. *The code* $\mathrm{T}(\mathcal{S},g)$ *is an* $[n,\deg(g),\prod_{j=1}^m(n_j-\deg(g_j)+1)]$ *code over* $\mathbb{F}_{q^t}$. *A generator matrix of* $\mathrm{T}(\mathcal{S},g)$ *may be specified entrywise by*

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

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.*

Throughout the rest of the paper, we will take $n_i =\mid S_i \mid$, the cardinality of S_i where $S_i \subseteq \mathbb{F}_{q^t}$, for $i \in [m] := \{1,\ldots,m\}$. Moreover, when we take a polynomial $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$, we mean that every $g_i \in \mathbb{F}_{q^t}[x_i]$. The expression $g(\mathcal{S}) \neq 0$ is used to represent that $g(\boldsymbol{s}) \neq 0$ for all $\boldsymbol{s} \in \mathcal{S}$.

At times, we also use as a tool a more granular version of the codes in Definition 1. Given $\boldsymbol{k} = (k_1,\ldots,k_m) \in \mathbb{Z}^m$ with $0 \le k_j \le n_j$ for all $j \in [m]$, the *tensor product of GRS codes* is

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

which is a $[\mid \mathcal{S} \mid, \prod_{j=1}^m k_j, \prod_{j=1}^m (n_j - k_j + 1)]$ code.

Remark 3. *Note that* $\mathrm{GRS}(S_j,k_j,g_j) = \{\boldsymbol{0}\}$ *if and only if* $k_j = 0$. *Thus,* $\mathrm{T}(\mathcal{S},\boldsymbol{k},g) = \{\boldsymbol{0}\}$ *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* $\boldsymbol{k} = (n_1,\ldots,n_m)$.

C. Augmented Cartesian codes

We next review the augmented Cartesian codes recently introduced and studied in [22] due to their local properties.

Consider $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$, the vanishing polynomial

$$L_j(x_j) := \prod_{s \in S_j}(x_j - s) \in \mathbb{F}_{q^t}[x_j] \tag{2}$$

for each $j \in [m]$, and the product

$$L(\boldsymbol{x}) := \prod_{j=1}^{m} L_j'(x_j) \in \mathbb{F}_{q^t}[\boldsymbol{x}], \tag{3}$$

where $L_j'(x_j)$ denotes the formal derivative of $L_j(x_j)$.

Given $f_1, f_2 \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $f_2(\mathcal{S}) \neq 0$, we write $\dfrac{f_1}{f_2} \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ to mean the unique polynomial whose value at $\boldsymbol{s}$ is $\dfrac{f_1(\boldsymbol{s})}{f_2(\boldsymbol{s})}$, for all $\boldsymbol{s} \in \mathcal{S}$, and $\deg_{x_j}\left(\dfrac{f_1}{f_2}\right) < n_j$. Observe that this polynomial can be constructed in the following way. Assume that $\dfrac{f_1(\boldsymbol{s}_i)}{f_2(\boldsymbol{s}_i)} = \lambda_i$, for $i \in [n]$. Let ι_i be the standard indicator function for $\boldsymbol{s}_i \in \mathcal{S}$. These functions ι_i are linear combinations of standard monomials and have the property that $\iota_i(\boldsymbol{s}_\ell) = 1$ when $i = \ell$ and $\iota_i(\boldsymbol{s}_\ell) = 0$ when $i \neq \ell$. See [23, Proposition 4.6 (a)] for a more detailed explanation of this fact and these concepts. We then define $\dfrac{f_1}{f_2} := \lambda_1\iota_1 + \cdots + \lambda_n\iota_n$.

Definition 4. Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$ and $h \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ be such that $h(\mathcal{S}) \neq 0$. An *augmented Cartesian code* (ACar code) is

$$\mathrm{ACar}(\mathcal{S},h) := \\ \left\{\left(\frac{h}{L}(\boldsymbol{s}_1)f(\boldsymbol{s}_1),\ldots,\frac{h}{L}(\boldsymbol{s}_n)f(\boldsymbol{s}_n)\right) : f \in \mathcal{L}(\mathcal{A}_h)\right\},$$

where $\mathcal{A}_h :=$

$$\prod_{j=1}^{m}\{0,\ldots,n_j-1\} \setminus \prod_{j=1}^{m}\left\{n_j - \deg_{x_j}(h),\ldots,n_j-1\right\}.$$

One may note that $\mathrm{ACar}(\mathcal{S},h)$ is monomially equivalent to

$$\left\{(f(\boldsymbol{s}_1),\ldots,f(\boldsymbol{s}_n)) : \deg_{x_j}(f+h) < n_j \text{ for some } j \in [m]\right\},$$

since the polynomial f is in $\mathcal{L}(\mathcal{A}_h)$ if and only if there is $j \in [m]$ such that $\deg_{x_j}(f) < n_j - \deg_{x_j}(h)$. At the same time, the scaling coefficients $\frac{h}{L}(\boldsymbol{s}_i)$ in Definition 4 are important in describing the duals.

Augmented Cartesian codes benefit from the theory developed for evaluation codes and more general monomial codes. Together, the Cartesian product $\mathcal{S} = \{\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}^m$, lattice points $\mathcal{A} \subseteq \mathbb{N}^m$, and a polynomial $h \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $h(\mathcal{S}) \neq 0$, define an *evaluation map*

$$\begin{aligned}\mathrm{ev}(\mathcal{S},h)\colon \mathcal{L}(\mathcal{A}) &\to \mathbb{F}_{q^t}^{|\mathcal{S}|}\\ f &\mapsto \left(h(\boldsymbol{s}_1)^{-1}f(\boldsymbol{s}_1),\ldots,h(\boldsymbol{s}_n)^{-1}f(\boldsymbol{s}_n)\right).\end{aligned}$$

The *generalized monomial-Cartesian* code associated with $\mathcal{S},\mathcal{A}$, and h is the image of the evaluation map $\mathrm{ev}(\mathcal{S},h)(\mathcal{L}(\mathcal{A}))$:

$$\mathcal{C}(\mathcal{S},\mathcal{A},h) := \\ \left\{\left(h(\boldsymbol{s}_1)^{-1}f(\boldsymbol{s}_1),\ldots,h(\boldsymbol{s}_n)^{-1}f(\boldsymbol{s}_n)\right) : f \in \mathcal{L}(\mathcal{A})\right\}. \tag{4}$$

It follows from [23, Theorem 5.4] that we may assume that

$\deg_{x_j}(h) < n_j$ and $\deg_{x_j}(f) < n_j$ for all $f \in \mathcal{L}(\mathcal{A})$ and $j \in [m]$; 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 $\mid \mathcal{S} \mid$ 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 IV. Augmented Cartesian codes are 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].

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 $\mathcal{C}(\mathcal{S},\mathcal{A},h)$. 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 [23] in terms of the indicator functions of $\mathcal{S}$.

In some of the proofs, we utilize a more general form of an augmented Cartesian code 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 $0 \le k_j \le n_j$, and

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

An augmented Cartesian code is shown in Example 7. Note that $\mathrm{ACar}(\mathcal{S},\boldsymbol{k},h)$ is monomially equivalent to the code $\Big\{(f(\boldsymbol{s}_1),\ldots,f(\boldsymbol{s}_n)) : \deg_{x_j}(f) < k_j, \text{ for some } j \in [m]\Big\}$.

Remark 5. *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 $\boldsymbol{k}=\boldsymbol{0}$.*

Because of the 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, the basic parameters are also trivial. For the case when $\mathrm{ACar}(\mathcal{S},\boldsymbol{k},h)$ is nontrivial, we find the basic parameters in the following result. Note that items (i) and (ii) are consequences of [22] with some minor observations, but we add a short proof for completeness.

Lemma 6. *The augmented Cartesian code $ACar(\mathcal{S},h)$ is an $[n, n-\deg(h), \min\{\deg_{x_j}(h)+1 : j \in [m]\}]$ code over $\mathbb{F}_{q^t}$. Moreover, $ACar(\mathcal{S},\boldsymbol{k},h)$ 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 $d = \min\{n_j-k_j+1\}_{j\in[m]}$.*

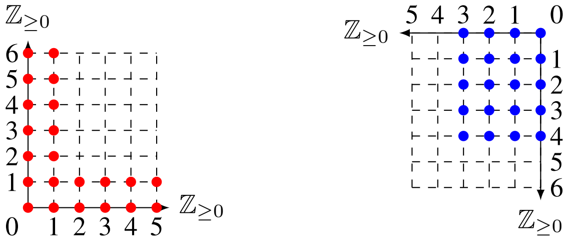
The dual of the augmented Cartesian code is

$$ACar(\mathcal{S},\boldsymbol{k},h)^{\perp} = \mathcal{C}\left(\mathcal{S}, \mathcal{A}_{Car}^{\perp}(\boldsymbol{k}), \frac{L}{h}\right),$$

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 according to Remark 5, we may assume $\boldsymbol{k} \neq \boldsymbol{0}$. 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 7. Let $S_1, S_2 \subseteq \mathbb{F}_{17}$ with $n_1 = \mid S_1 \mid = 6$ and $n_2 = \mid S_2 \mid = 7$. The code $\mathrm{ACar}(S_1 \times S_2,(2,2),1)$ is generated by the vectors $\mathrm{ev}(S_1 \times S_2, 1)(M)$, where M is a point in Figure 1 (a). The dual code $\mathrm{ACar}(S_1 \times S_2,(2,2),1)^{\perp}$ is generated by the vectors of the form $\mathrm{ev}(S_1 \times S_2, L)(M)$, where M is a monomial associated with a point in Figure 1 (b).



(a) (b)

Fig. 1: (a) Evaluation monomials of the code $\mathrm{ACar}(S_1 \times S_2,(2,2),h)$ described in Example 7. (b) Evaluation monomials of the dual code $\mathrm{ACar}(S_1 \times S_2,(2,2),h)^{\perp}$.

IV. Properties of multivariate Goppa codes

As is the case for the classical Goppa codes, multivariate Goppa codes have natural descriptions in terms of their parity-check matrices as well as via subfield subcodes of known codes. In the following two subsections, we illuminate these two points of view and use them to determine the properties of the multivariate Goppa codes.

A. Description of multivariate Goppa codes by parity check matrices

This subsection shows that a tensor product of generalized Reed-Solomon codes via Goppa codes provides a parity check matrix for a multivariate Goppa code. Consequently, we can give bounds for the dimension of a multivariate Goppa code. In addition, the trace of a tensor product supplies a representation for the dual of a multivariate Goppa code.

To relate multivariate Goppa codes to the tensor product in Definition 1, observe that given any two polynomials $p(x_1) = p_\ell x_1^\ell + \cdots + p_1 x_1 + p_0 = (x_1^\ell,\ldots,x_1,x_1^0)\cdot(p_\ell,\ldots,p_1,p_0) \in \mathbb{F}_{q^t}[x_1]$ and $q(x_2) = q_k x_2^k + \cdots + q_1 x_2 + q_0 = (x_2^k,\ldots,x_2,x_2^0)\cdot(q_k,\ldots,q_1,q_0) \in \mathbb{F}_{q^t}[x_2]$, we may abuse notation and write

$$p(x_1)q(x_2) = \left((x_1^\ell,\ldots,x_1^0)^T \otimes (x_2^k,\ldots,x_2^0)^T\right)^T \left((p_\ell,\ldots,p_0)^T \otimes (q_k,\ldots,q_0)^T\right).$$

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

$$\frac{1}{(x_2 - s)} = \frac{(-1)}{q(s)} \frac{(q(x_2) - q(s))}{(x_2 - s)} = \tag{5}$$

$$(x_2^{k-1}, ..., x_2^0) \begin{pmatrix} q_k & 0 & \cdots & 0 \\ q_{k-1} & q_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ q_1 & q_2 & \cdots & q_k \end{pmatrix} (s^0, ..., s^{k-1})^T. \tag{6}$$

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

Theorem 8. *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,

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

a subfield subcode of the dual of a tensor product of generalized Reed-Solomon codes via Goppa codes.

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

$$\left(\frac{\boldsymbol{s}_1^{\boldsymbol{a}}}{g(\boldsymbol{s}_1)}, \ldots, \frac{\boldsymbol{s}_n^{\boldsymbol{a}}}{g(\boldsymbol{s}_n)} \right) = \tag{7}$$

$$\left(\frac{s_{11}^{a_1} \cdots s_{1m}^{a_m}}{g_1(s_{11}) \cdots g_m(s_{1m})}, \ldots, \frac{s_{n1}^{a_1} \cdots s_{nm}^{a_m}}{g_1(s_{n1}) \cdots g_m(s_{nm})} \right),$$

where for $i \in [n]$, $\boldsymbol{s}_i = (s_{i1}, \ldots, s_{im}) \in \mathbb{F}_{q^t}^m$ 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 (7). 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 (6) implies that if $\boldsymbol{c} = (c_1, \ldots, c_n) \in \Gamma(\mathcal{S}, g)$ and $\boldsymbol{\gamma} := \begin{pmatrix} \gamma_k & 0 & \cdots & 0 \\ \gamma_{k-1} & \gamma_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_1 & \gamma_2 & \cdots & \gamma_k \end{pmatrix}$, then

$$\sum_{i=1}^{n} \frac{c_i}{(x - s_i)} = \sum_{i=1}^{n} \frac{-c_i}{g(s_i)} (x^{k-1}, ..., x^0) \, (\boldsymbol{\gamma}) \, (s_i^0, ..., s_i^{k-1})^T$$

$$= (x^{k-1}, ..., x^0) \, (\boldsymbol{\gamma}) \sum_{i=1}^{n} \frac{-c_i}{g(s_i)} (s_i^0, ..., s_i^{k-1})^T \tag{8}$$

$$= 0 \mod g(x). \tag{9}$$

Observe that the polynomial in (8) has degree $k - 1$. As $\deg(g) = k$, Equation (9) implies that the coefficients of the polynomial given in Equation (8) are zero. Hence, we see that

$$(\boldsymbol{\gamma}) \begin{pmatrix} \frac{1}{g(s_1)} & \frac{1}{g(s_2)} & \cdots & \frac{1}{g(s_n)} \\ \frac{s_1}{g(s_1)} & \frac{s_2}{g(s_2)} & \cdots & \frac{s_n}{g(s_n)} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{s_1^{k-1}}{g(s_1)} & \frac{s_2^{k-1}}{g(s_2)} & \cdots & \frac{s_n^{k-1}}{g(s_n)} \end{pmatrix} (c_1, ..., c_n)^T = \boldsymbol{0}.$$

As the matrix $\boldsymbol{\gamma}$ is invertible, after we multiply both sides of previous equation by the inverse of this matrix $\boldsymbol{\gamma}$, 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 (7) when $m = 1$.

Now we focus on the case $m = 2$. Assume $\deg(g_1) = k_1$ and $\deg(g_2) = k_2$. Define the column vectors $\boldsymbol{X}_1 := (x_1^{k_1 - 1}, \ldots, x_1^0)^T$, $\boldsymbol{X}_2 := (x_2^{k_2 - 1}, \ldots, x_2^0)^T$, $\boldsymbol{S}_{i1} := (s_{i1}^0, \ldots, s_{i1}^{k_1 - 1})^T$, and $\boldsymbol{S}_{i2} := (s_{i2}^0, \ldots, s_{i2}^{k_2 - 1})^T$ to easy notation. By Equation (6), there exist invertible matrices A and B, that depend of the coefficients of g_1 and g_2, respectively, such that

$$\sum_{i=1}^{n} \frac{c_i}{(x_1 - s_{i1})(x_2 - s_{i2})}$$

$$= \sum_{i=1}^{n} \frac{c_i}{g_1(s_{i1}) g_2(s_{i2})} \left(\boldsymbol{X}_1 \otimes \boldsymbol{X}_2 \right)^T (A \otimes B) \left(\boldsymbol{S}_{i1} \otimes \boldsymbol{S}_{i2} \right)$$

$$= \left(\boldsymbol{X}_1 \otimes \boldsymbol{X}_2 \right)^T (A \otimes B) \sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\boldsymbol{S}_{i1} \otimes \boldsymbol{S}_{i2} \right)$$

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

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

$$(A \otimes B) \sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\boldsymbol{S}_{i1} \otimes \boldsymbol{S}_{i2} \right) = \boldsymbol{0}.$$

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

$$\sum_{i=1}^{n} \frac{c_i}{g(\boldsymbol{s}_i)} \left(\boldsymbol{S}_{i1} \otimes \boldsymbol{S}_{i2} \right) = \boldsymbol{0}.$$

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

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

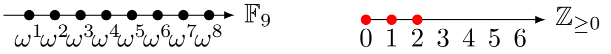
From this fact, we conclude that if $\boldsymbol{c} \in \Gamma(\mathcal{S}, g)$, then $\boldsymbol{c}$ is orthogonal to the vectors that appear in Equation (7). □

The following example considers a classical Goppa code and a multivariate Goppa code defined over the same field.

Example 9. First, let ω be a primitive element of $S := \mathbb{F}_9^*$ and $g := x^3 \in \mathbb{F}_9[x]$. The classical Goppa code $\Gamma(S, g)$ is given by

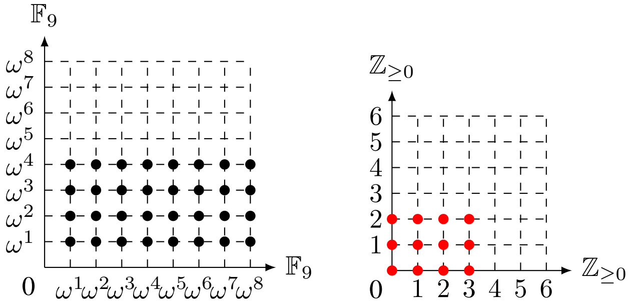
$$\Gamma(S, g) = \left\{ \boldsymbol{c} \in \mathbb{F}_3^8 : \mathrm{T}\, \boldsymbol{c}^T = 0 \right\},$$

where T is a generator matrix of the generalized Reed-Solomon code $\mathrm{GRS}(S, g)$. Note that this $\mathrm{GRS}(S, g)$ code is an $[8, 3, 6]$ evaluation code over $\mathbb{F}_9$ generated by the vectors


$\mathbb{F}_9$
$\omega^1\omega^2\omega^3\omega^4\omega^5\omega^6\omega^7\omega^8$
$\mathbb{Z}_{\geq 0}$
0 1 2 3 4 5 6

(a) Evaluation points (b) Evaluation monomials

Fig. 2: The generalized Reed-Solomon code $\mathrm{GRS}(S, g)$, whose evaluation points and evaluation monomials are shown in (a) and (b), respectively, defines a parity check matrix for the classical Goppa code $\Gamma(S, g)$ described in Example 9.



(a) Evaluation points (b) Evaluation monomials

Fig. 3: The tensor product $\mathrm{T}(\mathcal{S}, g)$, whose evaluation points and evaluation monomials are shown in (a) and (b), respectively, defines a parity check matrix for the multivariate Goppa code $\Gamma(\mathcal{S}, g)$ described in Example 9.

$\left(\frac{f(\omega^1)}{g(\omega^1)}, \ldots, \frac{f(\omega^8)}{g(\omega^8)}\right)$, where f is a polynomial in $\mathbb{F}_9[x]$ of degree less than 3. The evaluation points and the evaluation monomials of the $\mathrm{GRS}(S, g)$ code are represented in Figure 2 (a) and (b), respectively. Using the coding theory package [2] for Macaulay2 [17], and Magma [5], we obtain that $\Gamma(S, g)$ is an $[8, 4, 4]$ code over $\mathbb{F}_3$.

Now, let ω be a primitive element of $S_1 := \mathbb{F}_9^*$, $g_1 := x^4 \in \mathbb{F}_9[x]$, $S_2 := \left\{\omega^1, \omega^2, \omega^3, \omega^4\right\}$, $g_2 := (y - \omega^5)(y - \omega^6)(y - \omega^7) \in \mathbb{F}_9[y]$, and $g := g_1 g_2$. The multivariate Goppa code $\Gamma(\mathcal{S}, g)$ is given by

$$\Gamma(\mathcal{S}, g) = \left\{\boldsymbol{c} \in \mathbb{F}_3^{32} : \mathrm{T}\, \boldsymbol{c}^T = 0\right\},$$

where T is a generator matrix of the tensor product $\mathrm{T}(\mathcal{S}, g) = \mathrm{GRS}(S_1, g_1) \otimes \mathrm{GRS}(S_2, g_2)$. Let $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{32}$ be the points of the set $S_1 \times S_2$. This tensor product $\mathrm{T}(\mathcal{S}, g)$ is a $[32, 12, 10]$ evaluation code over $\mathbb{F}_9$ generated by the vectors $\left(\frac{f(\boldsymbol{s}_1)}{g(\boldsymbol{s}_1)}, \ldots, \frac{f(\boldsymbol{s}_{32})}{g(\boldsymbol{s}_{32})}\right)$, where f is a polynomial in $\mathbb{F}_9[x, y]$ with $\deg_x(f) < 4$ and $\deg_y(f) < 3$. The evaluation points and evaluation monomials are represented in Figure 3 (a) and (b), respectively. Using the coding theory package [2] for Macaulay2 [17], and Magma [5], we obtain that $\Gamma(\mathcal{S}, g)$ is a $[32, 14, 5]$ code over $\mathbb{F}_3$.

Recalling that $\Gamma(\mathcal{S}, g) = \left(\mathrm{T}(\mathcal{S}, g)^\perp\right)_q$, as shown in Theorem 8, we obtain the following consequences.

Corollary 10. *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 11. Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$ is the multiplicative group of the finite field $\mathbb{F}_{3^2}$. Take $S_1 = S_2 = \left\{a^i : i \in [8]\right\}$ 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 a $[64, 56, 4]$ code over $\mathbb{F}_3$, which has parameters matching the best known linear code of length 64 and dimension 56 over this field [15]. 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, in the case $m = 1$, we cannot obtain a comparable code with dimension exceeding $64 - 4\deg(g) = 64 - 12 = 52$.

In the following subsection, we will gain another perspective on the multivariate Goppa codes. It will allow us to round out Corollary 10 by describing the minimum distance of the multivariate Goppa codes.

B. Multivariate Goppa codes as subfield subcodes of augmented codes

This section shows that every multivariate Goppa code is a subfield subcode of an augmented Cartesian code. This valuable property allows us to determine a bound on the minimum distance of the multivariate Goppa codes and establishes the necessary results for determining hulls in Section V.

We now show that the dual of tensor product of GRS codes is an augmented Cartesian code.

Theorem 12. *The dual of a tensor product of generalized Reed-Solomon codes via Goppa codes is an augmented Cartesian code. More precisely, $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, g)^\perp = ACar\left(\mathcal{S}, \boldsymbol{k}', \frac{L}{g}\right)$, where $\boldsymbol{k}' := (n_1 - k_1, \ldots, n_m - k_m)$. In particular,*

$$\mathrm{T}(\mathcal{S}, g)^\perp = ACar\left(\mathcal{S}, g\right).$$

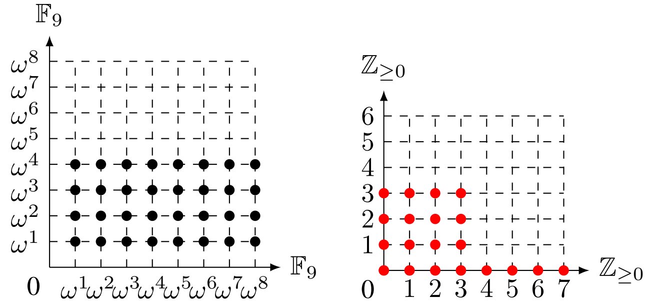
Proof. By Lemma 6, the dual of the augmented Cartesian code $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}', \frac{L}{g}\right)$ is $\mathcal{C}(\mathcal{S}, \mathcal{A}_{Car}^\perp(\boldsymbol{k}), g)$, where $\mathcal{A}_{Car}^\perp(\boldsymbol{k}) = \prod_{j=1}^m \left\{0, \ldots, k_j - 1\right\}$. 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 $\mathrm{T}(\mathcal{S}, g)^\perp = \mathrm{ACar}\left(\mathcal{S}, g\right)$ is obtained when we take $k_j = \deg(g_j)$, for $j \in [m]$. □

Example 13. Let ω be a primitive element of $S_1 := \mathbb{F}_9^*$, $g_1 := x^4 \in \mathbb{F}_9[x]$, $S_2 := \left\{\omega^1, \omega^2, \omega^3, \omega^4\right\}$, $g_2 := (y - \omega^5)(y - \omega^6)(y - \omega^7) \in \mathbb{F}_9[y]$, and $g := g_1 g_2$. Let $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{32}$ be the points of the set $S_1 \times S_2$. The tensor product $\mathrm{T}(\mathcal{S}, g)$ is a $[32, 12, 10]$ evaluation code over $\mathbb{F}_9$ generated by the vectors



(a) Evaluation points (b) Evaluation monomials

Fig. 4: The augmented Cartesian code $\mathrm{ACar}\,(\mathcal{S}, g)$, whose evaluation points and evaluation monomials are shown in (a) and (b), respectively, is the dual of the tensor product $\mathrm{T}(\mathcal{S}, g)$ described in Example 13.

$\left(\frac{f(\boldsymbol{s}_1)}{g(\boldsymbol{s}_1)}, \dots, \frac{f(\boldsymbol{s}_{32})}{g(\boldsymbol{s}_{32})}\right)$, where $f \in \mathbb{F}_9[x, y]$ is a polynomial with $\deg_x(f) < 4$ and $\deg_y(f) < 3$. The evaluation points and monomials are represented in Figure 3 (a) and (b), respectively.

By Theorem 12, $\mathrm{T}(\mathcal{S}, g)^\perp = \mathrm{ACar}\,(\mathcal{S}, g)$. The augmented Cartesian code $\mathrm{ACar}\,(\mathcal{S}, g)$ is an evaluation code over $\mathbb{F}_9$ generated by the vectors $\left(\frac{(gf)(\boldsymbol{s}_1)}{L(\boldsymbol{s}_1)}, \dots, \frac{(gf)(\boldsymbol{s}_{32})}{L(\boldsymbol{s}_{32})}\right)$, where f is a polynomial in $\mathbb{F}_9[x, y]$ with $\deg_x(f) < 4$ or $\deg_y(f) < 1$. The evaluation points and evaluation monomials are represented in Figure 4 (a) and (b), respectively. Using the coding theory package [2] for Macaulay2 [17], and Magma [5], we obtain that $\mathrm{ACar}\,(\mathcal{S}, g)$ is a $[32, 20, 4]$ code over $\mathbb{F}_9$.

Theorem 14. *The multivariate Goppa code $\Gamma(\mathcal{S}, g)$ is a subfield subcode of an augmented Cartesian code. Specifically,*

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

Proof. By Theorem 12, $\mathrm{ACar}\,(\mathcal{S}, g)^\perp = \mathrm{T}(\mathcal{S}, g)$. 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 8. □

The point of view given in Theorem 14 reveals additional information about the parameters of the multivariate Goppa codes, complementing Corollary 10.

Corollary 15. *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 of a multivariate Goppa code 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 10, it only remains to consider the minimum distance of $\Gamma(\mathcal{S}, g)$. By Theorem 14 and Lemma 6 (iii), $d \geq \min\left\{\deg(g_j) + 1\right\}_{j\in[m]}$. □

V. Subcodes, intersections, and hulls

This section builds on the relationships between multivariate Goppa codes, tensor products of GRS codes, and augmented Cartesian codes to determine subcodes, intersections, and hulls. We will get the desired structures by defining sets of polynomials with certain conditions. In the next section, these results will be critical to constructing entanglement-assisted quantum error-correcting codes as well as LCD, self-orthogonal, and self-dual codes.

First, the following result helps identify subcodes of Goppa codes, augmented Cartesian codes, and the tensor product of generalized Reed-Solomon codes via Goppa codes based on the defining polynomials.

Proposition 16. *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) $\mathit{ACar}\,(\mathcal{S}, gg') \subseteq \mathit{ACar}\,(\mathcal{S}, g)$.

Proof. (i) By Equation (4) and the definition of a GRS code,

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

(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 8.

(iii) This fact follows immediately from (i) and Theorem 12. □

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 following result demonstrates that for the intersection of generalized Reed-Solomon codes via Goppa codes to be of the same type, it is only required that the sum of the degrees of the defining polynomials is bounded above. It is worth comparing this condition to that specified in [12, Theorem 3.1], which requires that the two polynomials are related to one another in a particular way, going beyond an assumption on their degrees alone.

Theorem 17. *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 $\deg(g_jg'_j) \leq n_j$, 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) $\Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g') = \Gamma(\mathcal{S}, \operatorname{lcm}(g, g'))$.
(iii) $\mathit{ACar}\,(\mathcal{S}, \operatorname{lcm}(g, g')) \subseteq \mathit{ACar}\,(\mathcal{S}, g) \cap \mathit{ACar}\,(\mathcal{S}, g')$
$\subseteq \mathit{ACar}\,(\mathcal{S}, g) + \mathit{ACar}\,(\mathcal{S}, g') = \mathit{ACar}\,(\mathcal{S}, \gcd(g, g'))$.

Proof. For $j \in [m]$, define $\gcd_j := \gcd(g_j, g'_j) \in \mathbb{F}_{q^t}[x_j]$ and $\operatorname{lcm}_j := \operatorname{lcm}(g_j, g'_j) \in \mathbb{F}_{q^t}[x_j]$. Observe that $\gcd := \gcd(g, g') = \gcd_1 \cdots \gcd_m$ and $\operatorname{lcm} := \operatorname{lcm}(g, g') =$

$\mathrm{lcm}_1 \cdots \mathrm{lcm}_m$. There are $p, p', t, t' \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $g = p\,\mathrm{gcd}, g' = p'\,\mathrm{gcd}, \mathrm{lcm}(g, g') = gt$ and $\mathrm{lcm}(g, g') = g't'$.

(i) By Proposition 16 (i),

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

and

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

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

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

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 $\frac{g'}{\mathrm{gcd}} f = \frac{g}{\mathrm{gcd}} f'$. As $\frac{g'}{\mathrm{gcd}}$ and $\frac{g}{\mathrm{gcd}}$ share no common factors, $\frac{g}{\mathrm{gcd}} \mid f$. Hence, there is $r \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $f = r\frac{g}{\mathrm{gcd}}$. Thus, $g'f = r\frac{gg'}{\mathrm{gcd}} = r\,\mathrm{lcm}$, due to the fact that $\mathrm{lcm}\,\mathrm{gcd} = gg'$. As $\mathrm{lcm} \mid g'f$,

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

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

$$\begin{aligned}
\boldsymbol{c} &= \left(\frac{(g'f)(\boldsymbol{s}_1)}{(\mathrm{lcm}\,\mathrm{gcd})(\boldsymbol{s}_1)}, \dots, \frac{(g'f)(\boldsymbol{s}_n)}{(\mathrm{lcm}\,\mathrm{gcd})(\boldsymbol{s}_n)}\right)\\
&= \left(\frac{\left(\frac{g'f}{\mathrm{lcm}}\right)(\boldsymbol{s}_1)}{\mathrm{gcd}(\boldsymbol{s}_1)}, \dots, \frac{\left(\frac{g'f}{\mathrm{lcm}}\right)(\boldsymbol{s}_n)}{\mathrm{gcd}(\boldsymbol{s}_n)}\right).
\end{aligned}$$

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

(ii) By Proposition 16 (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, $\displaystyle\sum_{i=1}^{n} \frac{c_i}{\prod_{j=1}^{m}(x_j - s_{ij})} = 0 \mod \mathrm{lcm}(g, g')(\boldsymbol{x})$, which means that $\boldsymbol{c} \in \Gamma(\mathcal{S}, \mathrm{lcm}(g, g'))$.

(iii) By Proposition 16 (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 [25, Ch. 1. §8.], $\mathrm{T}(\mathcal{S}, g)^{\perp} + \mathrm{T}(\mathcal{S}, g')^{\perp} = \mathrm{T}(\mathcal{S}, \mathrm{gcd})^{\perp}$. Thus, Theorem 12 implies

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

This completes the proof. □

Example 18. Let $S_1 = S_2 := \left\{\omega^1, \dots, \omega^6\right\}$, where ω is a primitive element of $\mathbb{F}_9^*$, and $\mathcal{S} := S_1 \times S_2$. Consider the polynomials $g_1 := x^2(x - \omega^7), g_2 := y^3, g_1' := x^2(x - \omega^8), g_2' := y(y - \omega^7)(y - \omega^8) \in \mathbb{F}_9[x, y]$. Define $g := g_1 g_2$ and $g' := g_1' g_2'$. As $\deg(g_j g_j') = 6$ for $j \in [2]$, by Theorem 17 we have that

$$\mathrm{T}(\mathcal{S}, g) \cap \mathrm{T}(\mathcal{S}, g') = \mathrm{T}(\mathcal{S}, \mathrm{gcd}(g, g'))$$

and

$$\Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g') = \Gamma(\mathcal{S}, \mathrm{lcm}(g, g')),$$

where $\mathrm{gcd}(g, g') = x^2 y$ and $\mathrm{lcm}(g, g') = x^2(x - \omega^7)(x - \omega^8)y^3(y - \omega^7)(y - \omega^8)$.

Let $\left(p_i s_i^a\right)_{a,i} \in \mathbb{F}_{q^t}^{k \times n}$ and $\left(t_i s_i^a\right)_{a,i} \in \mathbb{F}_{q^t}^{k \times n}$ be two generator matrices of the same GRS code, where the rows and columns are indexed by $0 \leq a < k$ and $i \in [n]$, respectively. In [12, Lemma 2.5], the authors described a property that these matrices should satisfy. Specifically, if $k \leq \frac{n}{2}$, 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. Indeed, in this case, for any coefficients p_i, t_i, both matrices $\left(p_i s_i^a\right)_{a,i} \in \mathbb{F}_{q^t}^{k \times n}$ and $\left(t_i s_i^a\right)_{a,i} \in \mathbb{F}_{q^t}^{k \times n}$ 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 $k \leq \frac{n}{2}$ to $k < n$. This result will be helpful in characterizing when the dual of a tensor product of generalized Reed-Solomon codes via Goppa codes is of the same form.

Lemma 19. *Let $f, F \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ be such that $f(\mathcal{S}) \neq 0 \neq F(\mathcal{S})$. Take $j^* \in [m]$ and a non-negative integer $k < n$. Define $\boldsymbol{k} := (n_1, \dots, n_{j^*-1}, k, n_{j^*+1}, \dots, n_m)$. 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 $\mathrm{ev}(\mathcal{S}, f)(h) = \left(\frac{h(\boldsymbol{s}_1)}{f(\boldsymbol{s}_1)}, \dots, \frac{h(\boldsymbol{s}_n)}{f(\boldsymbol{s}_n)}\right)$. 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

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

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 $r \in [k-1]$,

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

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

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

which means that

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

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 $\{\boldsymbol{0}\}$ or $\mathbb{F}_{q^t}^n$, then the dual is also a tensor product of generalized Reed-Solomon codes via Goppa codes. We have the following result for the case when $\mathrm{T}(\mathcal{S}, g)$ is nontrivial.

Theorem 20. *Given $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$, there exists $f = f_1 \cdots f_m \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ 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 12, 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 4, $\mathrm{ACar}(\mathcal{S}, g) = \mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$, where $\boldsymbol{k}_g = (n_1 - \deg(g_1), \ldots, n_m - \deg(g_m))$. 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), $\boldsymbol{k}_g = (0, \ldots, n_{j^*} - \deg(g_{j^*}), \ldots, 0)) = (n_{j^*} - \deg(g_{j^*}))\,\boldsymbol{e}_{j^*}$. Using (i), $\boldsymbol{k}_g = \deg(f_{j^*})\boldsymbol{e}_{j^*}$. Thus, due to Definition 4, $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right)$ is generated by the vectors $\left(\frac{\boldsymbol{s}_1^{\boldsymbol{a}}}{\frac{L}{g}(\boldsymbol{s}_1)}, \ldots, \frac{\boldsymbol{s}_n^{\boldsymbol{a}}}{\frac{L}{g}(\boldsymbol{s}_n)}\right)$, 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 $\boldsymbol{k} := (n_1, \ldots, n_{j^*-1}, \deg(f_{j^*}), n_{j^*+1}, \ldots, n_m)$, $\mathrm{ACar}\left(\mathcal{S}, \boldsymbol{k}_g, \frac{L}{g}\right) = \mathrm{T}\left(\mathcal{S}, \boldsymbol{k}, \frac{L}{g}\right)$. By (ii) $\mathrm{T}(\mathcal{S}, \boldsymbol{k}, f) = \mathrm{T}(\mathcal{S}, f)$. Combining (iii) and Lemma 19, 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 $\boldsymbol{k}_g = (n_1 - \deg(g_1), \ldots, n_m - \deg(g_m))$. 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 6 (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 19, (iii) is also true. □

Remark 21. *Observe that the condition $\deg_{x_{j^*}}\left(\frac{fg}{L}\right)=0$ means that there is an element $p(\boldsymbol{x})$ in $\mathbb{F}_{q^t}[\boldsymbol{x}]$ such that $\deg_{x_{j^*}}(p)=0$ and $p(\boldsymbol{s}_i)=\frac{fg(\boldsymbol{s}_i)}{L(\boldsymbol{s}_i)}$; which happens if and only if $fg-pL\in I(\mathcal{S})$. Thus, given g, we can find f and p that satisfy $fg-pL\in I(\mathcal{S})$ and the conditions of Theorem 20 using the coding theory package [2] for Macaulay2 [17] or Magma [5].*

Example 22. Let a be a primitive element of $\mathbb{F}_9^*$, $S_1 := \{0,1,a,a^7\}$, and $S_2 := \{0,a^2,a^6\}$. Define the polynomials $f_1 := x+1$, $g_1 := 2x^3+a^5x^2+a^5x+1$, and $f_2 := g_2 := y^3+a^2y^2+y+a^6$. Note the following.

(i) $\deg(f_1g_1)=4=|S_1|$.
(ii) $\deg(f_2)=\deg(g_2)=|S_2|=3$.

Also, $f_1g_1 = 2L_1'+2L_1$ and $f_2g_2 = 2L_2'+pL_2$, where $p(x)=y^3+a^6y^2+a^2$. Then, $f_1f_2g_1g_2-pL\in I(\mathcal{S})$ and by Remark 21,

(iii) $\deg_{x_1}\left(\frac{f_1f_2g_1g_2}{L}\right)=0$.

Thus, by Theorem 20, $\mathrm{T}(\mathcal{S},g_1g_2)^\perp=\mathrm{T}(\mathcal{S},f_1f_2)$.

In [12], the authors used Goppa codes (the case $t=m=1$) to prove that the intersection of specific GRS codes is also a GRS code. As a consequence, they determine the hulls of specific generalized Reed-Solomon codes. Our focus is slightly different here, but taking the particular 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 23. *Let $\mathcal{S}\subseteq\mathbb{F}_{q^t}^m$, g and f be as in Theorem 20. 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 Theorem 12 and Theorem 20, $\mathrm{T}(\mathcal{S},f)=\mathrm{T}(\mathcal{S},g)^\perp=\mathrm{ACar}(\mathcal{S},g)$ 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 17 (i).

(ii) By the proof of (i), $\mathrm{T}(\mathcal{S},g)=\mathrm{T}(\mathcal{S},f)^\perp=\mathrm{ACar}(\mathcal{S},f)$. By Corollary 10, $\Gamma(\mathcal{S},g)^\perp=tr\left(\mathrm{T}(\mathcal{S},g)\right)=tr\left(\mathrm{ACar}(\mathcal{S},f)\right)\supseteq\Gamma(\mathcal{S},f)$. 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 17 (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 20, we can also conclude that the dimension of the hull of a tensor product of generalized Reed-Solomon codes via Goppa codes is

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

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

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

with equality when $t=1$.

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

In this section, we design q-ary entanglement-assisted quantum error-correcting codes as well as LCD, self-orthogonal, and self-dual codes from multivariate Goppa codes and tensor products of generalized Reed-Solomon codes via Goppa codes relying on the hulls found in the previous section.

Entanglement-assisted quantum error-correcting codes (EAQECCs), introduced in [6], utilize entangled qubits as an enabling mechanism that 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 EAQECC that encodes k qubits into n qubits, with minimum distance d, and c required entangled qubits. K. Guenda, S. Jitman, and A. Gulliver [18], building on the work of M. M. Wilde and T. A. Brune [32], showed that the necessary entanglement could be captured by the dimension of the hull of the linear code used. In particular, they prove the following.

Lemma 24. *[18, Corollary 3.2] Given an $[n,k,d]$ code C over $\mathbb{F}_q$, there exist EAQECCs with parameters*

$$[[n,k-\dim\left(Hull(C)\right),d,n-k-\dim\left(Hull(C)\right)]]_q \quad \textit{and}$$

$$[[n,n-k-\dim\left(Hull(C)\right),d(C^\perp),k-\dim\left(Hull(C)\right)]]_q.$$

The lemma above can be coupled with information gained about the hulls of multivariate Goppa codes and tensor products of generalized Reed-Solomon codes via Goppa codes in the previous section to produce EAQECCs, as shown in the following result.

Proposition 25. *Let $\mathcal{S}\subseteq\mathbb{F}_{q^t}^m$, g and f be as in Theorem 20. Then the code $\mathrm{T}(\mathcal{S},g)$ gives rise to EAQECCs with parameters*

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

and

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

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

$$\begin{aligned}&[[n,\leq t(\deg(\mathrm{lcm})+\deg(g))-n,\geq\deg(f_{j^*})+1;\\&\leq t\deg\left(\mathrm{lcm}\right)-\deg\left(g\right)]]_q \quad \textit{and}\\&[[n,\leq t\deg\left(\mathrm{lcm}\right)-\deg\left(g\right),\geq\deg(g_{j^*})+1;\\&\leq t(\deg(\mathrm{lcm})+\deg(g))-n]]_q,\end{aligned}$$

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 24, Remark 2, and Equation (11). The second pair of quantum codes follows from Lemma 24, Corollary 15, and Inequality (12). □

Note that when $t = 1$, meaning $\mathcal{S} \subseteq \mathbb{F}_q^m$, the two pairs of q-ary entanglement-assisted quantum error-correcting codes presented in Proposition 25 coincide. Indeed, when $t = 1$, Corollary 10 implies $\Gamma(\mathcal{S}, g)^\perp = tr(\mathrm{T}(\mathcal{S}, g)) = \mathrm{T}(\mathcal{S}, g)$, 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 [16]:

$$\begin{aligned}
&k \leq c + \max\{0, n - 2d + 2\},\\
&k \leq n - d + 1,\\
&k \leq \frac{(n - d + 1)(c + 2d - 2 - n)}{3d - 3 - n} \qquad \textit{if } d - 1 \geq \frac{n}{2},
\end{aligned}$$

where $0 \leq c \leq n - 1$. The code attaching this bound is called an MDS EAQECC. As a consequence of Proposition 25, we recover [12, Theorem 4.5].

Corollary 26. *Let $\mathcal{S} \subseteq \mathbb{F}_q^m$, g and f be as in Theorem 20. Then the code $\mathrm{T}(\mathcal{S}, g)$ gives rise to an MDS EAQECC.*

Proof. This is a consequence of Proposition 25. □

Besides the MDS EAQECCs, another significant consequence of Proposition 25 is the construction of families of EAQECCs of length n over $\mathbb{F}_q$, with $n > q$.

Example 27 (Family of long EAQECCs)**.** Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$. Take $S_1 := \{0, 1, a, a^7\}$ and $S_2 := \{1, a^6\}$. Define the polynomials $f_1 := ax+1$, $g_1 := x^3+a^6x^2+1$, $f_2 := x^2+a^2x+2$, and $g_2 := x^2 + a^2$. Then

$$f_1 g_1 = 2L_1' + aL_1 \qquad \text{and} \qquad f_2 g_2 = a^2 L_2' + pL_2,$$

where $p(x) = x^2 + a^7 x + a$. Then, for every $m \geq 0$, define the polynomials in $m + 1$ variables $f := f_1(x) f_2(x_1) \cdots f_2(x_m), g := g_1(x) g_2(x_1) \cdots g_2(x_m) \in \mathbb{F}_9[x_1, \ldots, x_m]$. Since $\gcd(f, g) = 1$, $\deg(f) = 2^m$, and $\deg(g) = 3 \cdot 2^m$, by Proposition 25 there exists a $[[4 \cdot 2^m, 2^m, 4; 3 \cdot 2^m]]$ EAQECC over $\mathbb{F}_9$. Note that when $m = 0$, this is an MDS EAQECC over $\mathbb{F}_9$. Larger values of m give rise to longer codes (of length 2^{m+2}) over $\mathbb{F}_9$ that are not MDS but have a known gap to the Singleton Bound.

Table I shows that by puncturing the dual of multivariate Goppa codes, we can improve the minimum distance or the dimension of some of the best-known EAQECCs recently published by L. Sok [29]. Other recent related work appears in [11], [28].

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

Corollary 28. *Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$, g and f be as in Theorem 20. 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 $f = g$.*

$\mathcal{S}$	$g(x, y)$	Puncturing $\Gamma(\mathcal{S}, g)^\perp$ the following entries	Parameters
$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^3 + x + a)\,(y)$	$\{8, \ldots, 15\}$	$[[8, 2, 6; 6]]_8$
$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^3 + x + a)\,(y)$	$\{10, \ldots, 16\}$	$[[9, 2, 7; 7]]_8$
$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^3 + x + a)\,(y)$	$\{11, \ldots, 16\}$	$[[10, 2, 8; 8]]_8$
$\mathbb{F}_8 \times \{a^1, a^2\}$	$(x^3 + x + a)\,(y)$	$\{12, \ldots, 16\}$	$[[11, 2, 9; 9]]_8$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)\,(y)$	$\{19, \ldots, 32\}$	$[[18, 2, 16; 16]]_{16}$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)\,(y)$	$\{21, \ldots, 32\}$	$[[20, 2, 18; 18]]_{16}$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^3 + a)\,(y)$	$\{23, \ldots, 32\}$	$[[22, 2, 20; 20]]_{16}$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^4 + x^2 + ax + a^2)\,(y)$	$\{26, \ldots, 32\}$	$[[25, 3, 21; 20]]_{16}$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^4 + x^2 + ax + a^2)\,(y)$	$\{28, \ldots, 32\}$	$[[27, 3, 23; 24]]_{16}$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^4 + x^2 + ax + a^2)\,(y)$	$\{30, \ldots, 32\}$	$[[29, 3, 25; 26]]_{16}$
$\mathbb{F}_{16} \times \{a^1, a^2\}$	$(x^4 + x^2 + ax + a^2)\,(y)$	$\{32\}$	$[[31, 3, 27; 28]]_{16}$
$\mathbb{F}_{25} \times \{a^1, a^2, a^3\}$	$(x^4 + a)\,(y)$	$\{60, \ldots, 75\}$	$[[59, 3, 53; 56]]_{25}$
$\mathbb{F}_{49} \times \{a^1, \ldots, a^4\}$	$(x^4 + a)\,(y)$	$\{168, \ldots, 196\}$	$[[167, 3, 159; 164]]_{49}$
$\mathbb{F}_{49} \times \{a^1, \ldots, a^4\}$	$(x^4 + a)\,(y)$	$\{175, \ldots, 196\}$	$[[174, 3, 166; 171]]_{49}$

TABLE I: New EAQECCs. For every row, we assume that $\mathbb{F}_q^* = \langle a \rangle$.

(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 Theorem 12 and Theorem 20, $\mathrm{T}(\mathcal{S}, f) = \mathrm{T}(\mathcal{S}, g)^\perp = \mathrm{ACar}(\mathcal{S}, g)$ 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 17 (i).

(ii) By the proof of (i), $\mathrm{T}(\mathcal{S}, g) = \mathrm{T}(\mathcal{S}, f)^\perp = \mathrm{ACar}(\mathcal{S}, f)$. By Corollary 10, $\Gamma(\mathcal{S}, g)^\perp = tr\,(\mathrm{T}(\mathcal{S}, g)) = tr\,(\mathrm{ACar}(\mathcal{S}, f)) \supseteq \Gamma(\mathcal{S}, f)$. Thus, $\mathrm{Hull}\,(\Gamma(\mathcal{S}, g)) = \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g)^\perp \supseteq \Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, f) = \Gamma(\mathcal{S}, \mathrm{lcm}(g, f))$, where the last equation holds because of Theorem 17 (ii).

(iii) If $f = g$, then $g = \gcd(f, g) = \mathrm{lcm}(f, g) = f$. Thus, (iii) is a consequence of (ii).

(iv) By Corollary 23,

$$\mathrm{Hull}\,(\Gamma(\mathcal{S}, g)) = \Gamma(\mathcal{S}, \mathrm{lcm}(f, g)) = \mathrm{ACar}(\mathcal{S}, \mathrm{lcm}(f, g)).$$

If $\deg_{x_j}(\mathrm{lcm}(f, g)) \geq n_j$ for all $j \in [m]$, then $\mathrm{T}(\mathcal{S}, \mathrm{lcm}(f, g)) = \mathbb{F}_{q^t}^n$ by Remark 3. Thus, $\mathrm{ACar}(\mathcal{S}, \mathrm{lcm}(f, g)) = \mathrm{T}(\mathcal{S}, \mathrm{lcm}(f, g))^\perp = \{\mathbf{0}\}$ by Theorem 12.

(v) and (vi) Note that when $t = 1$, $\Gamma(\mathcal{S}, g) = \mathrm{ACar}(\mathcal{S}, g)$. So, $\Gamma(\mathcal{S}, g)^\perp = \mathrm{T}(\mathcal{S}, g)$. Thus, (v) and (vi) are consequences of (ii) and (iii), respectively. □

Corollary 28 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 $f_2 g_2 = \lambda_2 L_2' + pL_2$, 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 steps (1)-(4), codes with different lengths can be derived after the appropriate polynomials have been found.

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

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

where $p(x) = x^3 + a^5x^2 + a^2x + a^6$. Then, for every $m \geq 0$, define the polynomial in $m+1$ variables $g := g_1(x)g_2(x_1)\cdots g_2(x_m)$. As $\gcd(f_1, g_1) = 1$, by Corollary 28 (i), the tensor product $\mathrm{T}(\mathcal{S}, g)$ is a $[4\cdot 3^m, 3^{m+1}]$ LCD code over $\mathbb{F}_9$.

Example 30 (Family of long self-orthogonal codes)**.** Assume $\mathbb{F}_{3^2}^* = \langle a\rangle$. Take $S_1 := \{0, 1, 2, a\}$ and $S_2 := \left\{1, a^5, a^7\right\}$. 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 $m+1$ variables $g := g_1(x)g_2(x_1)\cdots g_2(x_m)$. As g_1 divides f_1 and g_2 divides f_2, by Corollary 28 (ii), the tensor product $\mathrm{T}(\mathcal{S}, g)$ is a $[4\cdot 3^m, 3^m]$ self-orthogonal code over $\mathbb{F}_9$.

Example 31 (Family of long self-dual codes)**.** Assume $\mathbb{F}_{3^2}^* = \langle a\rangle$. Take $S_1 := \left\{a, a^2, a^3, a^5, a^6, a^7\right\}$ and $S_2 := \left\{1, a^5, a^7\right\}$. 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 $m+1$ variables $g := g_1(x)g_2(x_1)\cdots g_2(x_m)$. As $g_1 = f_1$, and $g_2 = f_2$, by Corollary 28 (iii), the tensor product $\mathrm{T}(\mathcal{S}, g)$ is a $[6\cdot 3^m, 3^{m+1}]$ self-dual code over $\mathbb{F}_9$.

VII. Conclusion

This paper defined multivariate Goppa codes that generalize the classical Goppa codes. Similar to classical Goppa codes, they are described via a parity check matrix and as subfield subcodes of a family of evaluation codes. In particular, we showed that the tensor product 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 proved that multivariate Goppa codes are subfield subcodes of augmented Cartesian codes. These perspectives provided information about the code parameters as well as their hulls. Consequently, we obtained q-ary entanglement-assisted quantum error-correcting codes, 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] M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. Patterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, and W. Wang. Classic McEliece: conservative code-based cryptography, 2020."Supporting documentation".

[2] T. Ball, E. Camps, H. Chimal-Dzul, D. Jaramillo-Velez, H. H. López, N. Nichols, M. Perkins, I. Soprunov, G. Vera-Martínez, and G. Whieldon. Coding theory package for Macaulay2. *Journal of Software for Algebra and Geometry*, 11(1):113–122, 2021.

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

[4] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang. Classic McEliece: conservative code-based cryptography, 2017."Supporting documentation".

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[6] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[7] E. Camps, H. H. López, G. L. Matthews, and E. Sarmiento. Polar decreasing monomial-Cartesian codes. *IEEE Transactions on Information Theory*, 67(6):3664–3674, 2021.

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

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

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

[11] J. Fan, J. Li, Y. Zhou, M.-H. Hsieh, and H. V. Poor. Entanglement-assisted concatenated quantum codes. *Proceedings of the National Academy of Sciences*, 119(24):e2202235119, 2022.

[12] Y. Gao, Q. Yue, X. Huang, and J. 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.

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

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

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

[16] M. Grassl, F. Huber, and A. Winter. Entropic proofs of Singleton bounds for quantum error-correcting codes. *IEEE Transactions on Information Theory*, 68(6):3942–3950, 2022.

[17] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.

[18] K. Guenda, S. Jitman, and T. A. Gulliver. Constructions of good entanglement-assisted quantum error correcting codes. *Designs, Codes and Cryptography*, 86(1):121–136, Jan. 2018.

[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] H. H. López, G. L. Matthews, and I. 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.

[22] H. H. López, G. L. Matthews, and D. Valvo. Erasures repair for decreasing monomial-cartesian and augmented reed-muller codes of high rate. *IEEE Transactions on Information Theory*, 2021.

[23] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Designs, Codes and Cryptography*, 89(7):1367–1403, 2021.

[24] H. H. López, G. L. Matthews, and D. Valvo. Augmented Reed-Muller codes of high rate and erasure repair. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 438–443, 2021.

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

[26] J. L. Massey. Linear codes with complementary duals. *Discrete Mathematics*, 106-107:337–342, 1992.

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

[28] L. Sok. A new construction of linear codes with one-dimensional hull. *Designs, Codes and Cryptography*, 2022.

[29] L. Sok. On linear codes with one-dimensional euclidean hull and their applications to EAQECCs. *IEEE Transactions on Information Theory*, 68(7):4329–4343, 2022.

[30] J. H. van Lint. *Introduction to coding theory*. Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1999.

[31] R. H. Villarreal. *Monomial Algebras*. Monographs and Research Notes in Mathematics, 2015.

[32] M. M. Wilde and T. A. Brun. Optimal entanglement formulas for entanglement-assisted quantum coding. *Phys. Rev. A*, 77:064302, Jun 2008.

Hiram H. López is an Assistant Professor at Cleveland State University. He earned a B.S. degree in applied mathematics from the Autonomous University of Aguascalientes in 2008 and a Ph.D. degree in mathematics from CINVESTAV-IPN in 2016. After a postdoctoral position at Clemson University from 2016 to 2018, he joined Cleveland State University in 2019. His research interests include coding theory, commutative algebraic, and image processing.

Gretchen L. Matthews is a Professor in the Department of Mathematics at Virginia Tech. She earned a B.S. degree in mathematics from Oklahoma State University in 1995 and a Ph.D. degree in mathematics from Louisiana State University in 1999. Following postdoctoral work at the University of Tennessee, she was on the faculty at Clemson University before joining Virginia Tech in 2018. Her research interests include algebraic geometry and combinatorics and their applications to coding theory and cryptography.