Multivariate Goppa Codes

joint work with Hiram Lopez

Gretchen L. Matthews

August 10, 2022

Virginia Tech
Department of Mathematics
Division of Computational Modeling & Data Analytics
Hume Center for National Security & Technology
supported by NSF DMS-2201075 and NSF DMS-1855136

Big idea

Multivariate polynomials provide a generalization of classical Goppa codes and utility in several applications, including simultaneous protection against side channel attacks and fault injection attacts and quantum error correction.

Codes

Let $\mathbb{F}$ be a finite field.

An $[n, k, d]$ code C over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$ with minimum distance

$$d = \min\{\left|\{i : c_i \neq c'_i\}\right| : c, c' \in C, c \neq c'\}.$$

Codes

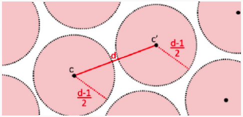
Let $\mathbb{F}$ be a finite field.

An $[n, k, d]$ code C over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$ with minimum distance

$$d = \min\{\left|\{i : c_i \neq c'_i\}\right| : c, c' \in C, c \neq c'\}.$$

An $[n, k, d]$ code C can

- correct any $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors and
- recover any $d - 1$ erasures.



Codes

The dual of an $[n, k, d]$ code C over $\mathbb{F}_q$ is

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

which is an $[n, n-k, d']$ code.

Codes

A generator matrix for an $[n, k, d]$ code C over $\mathbb{F}_q$ is

$$\begin{bmatrix} — & c_1 & — \\ — & c_2 & — \\ & \vdots & \\ — & c_k & — \end{bmatrix} \in \mathbb{F}_q^{k \times n}$$

where C is spanned by the codewords $c_1, \ldots, c_k \in \mathbb{F}_q^n$.

Codes

A generator matrix for an $[n, k, d]$ code C over $\mathbb{F}_q$ is

$$\begin{bmatrix} — & c_1 & — \\ — & c_2 & — \\ & \vdots & \\ — & c_k & — \end{bmatrix} \in \mathbb{F}_q^{k \times n}$$

where C is spanned by the codewords $c_1, \ldots, c_k \in \mathbb{F}_q^n$.

A parity check matrix for C is any matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ such that

$$Hc^T = 0 \ \forall c \in C.$$

Codes from polynomials

Let $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$.

Fix positive integers $k \leq n \leq q$. The Reed-Solomon code C_k is

$$C_k = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n.$$

Codes from polynomials

Let $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$.

Fix positive integers $k \leq n \leq q$. The Reed-Solomon code C_k is

$$C_k = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n.$$

C_k is an $[n, k, n-(k-1)]$ code.

Codes from polynomials

Let $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$.

Fix positive integers $k \leq n \leq q$. The Reed-Solomon code C_k is

$$C_k = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n.$$

C_k is an $[n, k, n-(k-1)]$ code. If $n = q$, then $C_k^\perp = C_{n-k}$.

Codes from polynomials

Let $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$.

Fix positive integers $k \leq n \leq q$. The Reed-Solomon code C_k is

$$C_k = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n.$$

C_k is an $[n, k, n-(k-1)]$ code. If $n = q$, then $C_k^\perp = C_{n-k}$.

generalized Reed-Solomon (GRS) code

$$C_{v,k} := \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n$$

where $v \in \mathbb{F}_q^n$.

Codes from polynomials

Let $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$.

Fix positive integers $k \leq n \leq q$. The Reed-Solomon code C_k is

$$C_k = \{(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n.$$

C_k is an $[n, k, n-(k-1)]$ code. If $n = q$, then $C_k^\perp = C_{n-k}$.

generalized Reed-Solomon (GRS) code

$$C_{v,k} := \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n$$

where $v \in \mathbb{F}_q^n$.

In general, $C_k^\perp = C_{v,n-k}$ where $v_i := \left(\prod_{j \in [n] \setminus \{i\}} \alpha_i - \alpha_j\right)^{-1}$.

Codes from polynomials

Let $g \in \mathbb{F}_{q^t}[x]$ and $S = \{s_1, \ldots, s_n\} \subseteq \mathbb{F}_{q^t}$. Assume $g(s_i) \neq 0 \ \forall i \in [n]$. Then

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

Codes from polynomials

Let $g \in \mathbb{F}_{q^t}[x]$ and $S = \{s_1, \ldots, s_n\} \subseteq \mathbb{F}_{q^t}$. Assume $g(s_i) \neq 0 \ \forall i \in [n]$. Then

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

generalized Reed-Solomon (GRS) code via a Goppa code

A GRS code via a Goppa code is of the form

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

GRS codes via Goppa codes were introduced in 2021 by Y. Gao, Q. Yue, X. Huang, and J. Zhang.

Going multivariate

Write $\mathbb{F}_q^m := \{s_1, \ldots, s_n\}$ where $n = q^m$, and let $k \in \mathbb{Z}_+^m$.

Reed-Muller code

A Reed-Muller code is $RM(q, m, k) :=$

$$\{(f(s_1), f(s_2), \ldots, f(s_n)) : f \in \mathbb{F}_q[x_1, \ldots, x_m]_{<k}\} \subseteq \mathbb{F}_q^n.$$

Going multivariate

Write $\mathbb{F}_q^m := \{s_1, \ldots, s_n\}$ where $n = q^m$, and let $k \in \mathbb{Z}_+^m$.

Reed-Muller code

A Reed-Muller code is $RM(q, m, k) :=$

$$\{(f(s_1), f(s_2), \ldots, f(s_n)) : f \in \mathbb{F}_q[x_1, \ldots, x_m]_{<k}\} \subseteq \mathbb{F}_q^n.$$

$RM(q, m, k)$ is a $[q^m, \sum_{i=0}^{k} \binom{m}{i}, q^{m-k}]$ code.

Going multivariate

Write $\mathbb{F}_q^m := \{s_1, \ldots, s_n\}$ where $n = q^m$, and let $k \in \mathbb{Z}_+^m$.

Reed-Muller code

A Reed-Muller code is $RM(q, m, k) :=$

$$\{(f(s_1), f(s_2), \ldots, f(s_n)) : f \in \mathbb{F}_q[x_1, \ldots, x_m]_{<k}\} \subseteq \mathbb{F}_q^n.$$

$RM(q, m, k)$ is a $[q^m, \sum_{i=0}^{k} \binom{m}{i}, q^{m-k}]$ code.

monomial Cartesian code

Given $\mathcal{L} \subseteq \mathbb{F}_q[x_1, \ldots, x_m]$ and $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_m = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^m$, a monomial Cartesian code is

$$\{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n.$$

The McEliece cryptosystem (1978) employs Goppa codes.

code-based cryptosystem abstracted from (McEliece, 1978)

Let $\mathcal{C}$ be an $[n, k, \geq 2t - 1]$ code with generator matrix G and efficient decoding algorithm $\mathcal{D}$. Let S be a $k \times k$ random invertible matrix and P be an $n \times n$ random permutation matrix. Let $G^{\text{PUB}} = SGP$.

Public Key: (G^{PUB}, t) Private Key: $(S, P, \mathcal{D})$

The McEliece cryptosystem (1978) employs Goppa codes.

code-based cryptosystem abstracted from (McEliece, 1978)

Let $\mathcal{C}$ be an $[n, k, \geq 2t-1]$ code with generator matrix G and efficient decoding algorithm $\mathcal{D}$. Let S be a $k \times k$ random invertible matrix and P be an $n \times n$ random permutation matrix. Let $G^{\text{PUB}} = SGP$.

Public Key: (G^{PUB}, t) Private Key: $(S, P, \mathcal{D})$

Encryption

$m' = mG^{\text{PUB}} + e$,

where $\text{wt}(e) \leq t$.

The McEliece cryptosystem (1978) employs Goppa codes.

code-based cryptosystem abstracted from (McEliece, 1978)

Let $\mathcal{C}$ be an $[n, k, \geq 2t - 1]$ code with generator matrix G and efficient decoding algorithm $\mathcal{D}$. Let S be a $k \times k$ random invertible matrix and P be an $n \times n$ random permutation matrix. Let $G^{\text{PUB}} = SGP$.

Public Key: (G^{PUB}, t) Private Key: $(S, P, \mathcal{D})$

Encryption

$m' = mG^{\text{PUB}} + e,$

where $\text{wt}(e) \leq t$.

Decryption

1. $m'P^{-1}$

The McEliece cryptosystem (1978) employs Goppa codes.

code-based cryptosystem abstracted from (McEliece, 1978)

Let $\mathcal{C}$ be an $[n, k, \geq 2t-1]$ code with generator matrix G and efficient decoding algorithm $\mathcal{D}$. Let S be a $k \times k$ random invertible matrix and P be an $n \times n$ random permutation matrix. Let $G^{\text{PUB}} = SGP$.

Public Key: (G^{PUB}, t) Private Key: $(S, P, \mathcal{D})$

Encryption

$m' = mG^{\text{PUB}} + e$,

where $\text{wt}(e) \leq t$.

Decryption

1. $m'P^{-1} = mSGPP^{-1} + eP^{-1}$

The McEliece cryptosystem (1978) employs Goppa codes.

code-based cryptosystem abstracted from (McEliece, 1978)

Let $\mathcal{C}$ be an $[n, k, \geq 2t-1]$ code with generator matrix G and efficient decoding algorithm $\mathcal{D}$. Let S be a $k \times k$ random invertible matrix and P be an $n \times n$ random permutation matrix. Let $G^{\text{PUB}} = SGP$.

Public Key: (G^{PUB}, t) Private Key: $(S, P, \mathcal{D})$

Encryption

$m' = mG^{\text{PUB}} + e$,

where $\text{wt}(e) \leq t$.

Decryption

1. $m'P^{-1} = mSGPP^{-1} + eP^{-1} = mSG + eP^{-1}$
2. Apply $\mathcal{D}$ to recover mS
3. $mSS^{-1} = m$

Subfield subcodes

Consider a prime power q and $t \in \mathbb{Z}_+$ so that

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

Th subfield subcode of an $[n, k, d]$ code $C \subseteq \mathbb{F}_{q^t}$ relative to $\mathbb{F}_{q^t}/\mathbb{F}_q$ is

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

Subfield subcodes

Consider a prime power q and $t \in \mathbb{Z}_+$ so that

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

Th subfield subcode of an $[n, k, d]$ code $C \subseteq \mathbb{F}_{q^t}$ relative to $\mathbb{F}_{q^t}/\mathbb{F}_q$ is

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

The code $C|_{\mathbb{F}_q}$ is an $[n, \geq k - (t-1)(n-k), \geq d]$ code over $\mathbb{F}_q$.

Trace codes

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

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

trace code

Given an $[n, k, d]$ code $C \subseteq \mathbb{F}_{q^t}$,

$$tr(C) := \{(tr(c_1), \ldots, tr(c_n)) : (c_1, \ldots, c_n) \in C\} \subseteq \mathbb{F}^n_q.$$

Trace codes

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

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

trace code

Given an $[n, k, d]$ code $C \subseteq \mathbb{F}_{q^t}$,

$$tr(C) := \{(tr(c_1), \ldots, tr(c_n)) : (c_1, \ldots, c_n) \in C\} \subseteq \mathbb{F}_q^n.$$

$tr(C)$ is an $[n, k^*, d^*]$ over $\mathbb{F}_q$, where $k \leq k^* \leq tk$ and $d^* \leq d$.

Relating subfield subcodes and trace codes

Delsarte's Theorem

$$(C_q)^{\perp} = tr\left(C^{\perp}\right).$$

Multivariate Goppa codes

Consider

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

where

$$g_i \in \mathbb{F}_{q^t}[x_i] \; \forall i \in [m],$$

Multivariate Goppa codes

Consider

$$g := g_1 \cdots g_m \in \mathbb{F}_{q^t}[\boldsymbol{x}] := \mathbb{F}_{q^t}[x_1, \dots, x_m],$$

where

$$g_i \in \mathbb{F}_{q^t}[x_i] \ \forall i \in [m],$$

and $\mathcal{S} := S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$, $S_i \neq \emptyset$. Let $\mathcal{S} = \{\boldsymbol{s}_1, \dots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}^m$.

Multivariate Goppa codes

Consider

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

where

$$g_i \in \mathbb{F}_{q^t}[x_i] \ \forall i \in [m],$$

and $\mathcal{S} := S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$, $S_i \neq \emptyset$. Let $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}^m$. Assume that $g(\boldsymbol{s}_i) \neq 0$ for all $i \in [n]$ and $\boldsymbol{s}_i := (s_{i1}, \ldots, s_{im}) \in \mathcal{S}$.

Multivariate Goppa codes

Consider

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

where

$$g_i \in \mathbb{F}_{q^t}[x_i] \ \forall i \in [m],$$

and $\mathcal{S} := S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$, $S_i \neq \emptyset$. Let $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}^m$. Assume that $g(\boldsymbol{s}_i) \neq 0$ for all $i \in [n]$ and $\boldsymbol{s}_i := (s_{i1}, \ldots, s_{im}) \in \mathcal{S}$.

Multivariate Goppa code

A *multivariate Goppa code* is $\Gamma(\mathcal{S}, g) :=$

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

Multivariate Goppa codes

Note: $\Gamma(\mathcal{S}, g) :=$

$$\left\{ c \in \mathbb{F}_q^n : \begin{array}{l} \sum_{i=1}^n c_i \left[\prod_{l \in [n] \setminus \{i\}}^n \prod_{j=1}^m (x_j - s_{ij}) \right] = g(x) \prod_{i=1}^n \left[\prod_{j=1}^m (x_j - s_{ij}) \right] q(x) \\ \text{for some } q(x) \in \mathbb{F}_{q^t}[\boldsymbol{x}] \end{array} \right\}.$$

Multivariate Goppa codes

(Classical) Goppa codes

Taking $m = 1$, we obtain the

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

where $g(x) \in \mathbb{F}_{q^t}[x]$ and $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}$.

Multivariate Goppa codes

(Classical) Goppa codes

Taking $m = 1$, we obtain the

$$\Gamma(\mathcal{S}, g) = \left\{ (c_1, \dots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{(x - s_i)} = 0 \mod g(\boldsymbol{x}) \right\}$$

where $g(x) \in \mathbb{F}_{q^t}[x]$ and $\mathcal{S} = \{\boldsymbol{s}_1, \dots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_{q^t}$.

GRS codes via Goppa

Setting $m = t = 1$ gives the codes considered by Y. Gao, Q. Yue, X. Huang, and J. Zhang (2021):

$$\Gamma(\mathcal{S}, g) = \left\{ (c_1, \dots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{(x - s_i)} = 0 \mod g(\boldsymbol{x}) \right\}$$

where $g(x) \in \mathbb{F}_q[x]$ and $\mathcal{S} = \{\boldsymbol{s}_1, \dots, \boldsymbol{s}_n\} \subseteq \mathbb{F}_q$.

Multivariate Goppa codes

Recall that

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

Note: $\Gamma(\mathcal{S}, g)$ is a code over $\mathbb{F}_q$ of length $n := \mid \mathcal{S} \mid$ where

$$\mathcal{S} \subseteq \mathbb{F}_{q^t}^m;$$

thus,

$$n \leq q^{tm}.$$

Multivariate Goppa codes

Recall that

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

Note: $\Gamma(\mathcal{S}, g)$ is a code over $\mathbb{F}_q$ of length $n := \mid \mathcal{S} \mid$ where

$$\mathcal{S} \subseteq \mathbb{F}_{q^t}^m;$$

thus,

$$n \leq q^{tm}.$$

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.

Multivariate Goppa codes

tensor product of generalized Reed-Solomon codes via Goppa codes

If $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$ and $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[x_1, \ldots, x_m]$,

$$\mathsf{T}(\mathcal{S}, g) := \bigotimes_{j=1}^{m} \mathsf{GRS}(S_j, g_j) \subseteq \mathbb{F}_{q^t}^n.$$

Multivariate Goppa codes

tensor product of generalized Reed-Solomon codes via Goppa codes

If $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$ and $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[x_1, \ldots, x_m]$,

$$\mathrm{T}(\mathcal{S}, g) := \bigotimes_{j=1}^{m} \mathrm{GRS}(S_j, g_j) \subseteq \mathbb{F}_{q^t}^n.$$

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

Multivariate Goppa codes

tensor product of generalized Reed-Solomon codes via Goppa codes

If $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$ and $g = g_1 \cdots g_m \in \mathbb{F}_{q^t}[x_1, \ldots, x_m]$,

$$\mathrm{T}(\mathcal{S}, g) := \bigotimes_{j=1}^{m} \mathrm{GRS}(S_j, g_j) \subseteq \mathbb{F}_{q^t}^n.$$

$\mathrm{T}(\mathcal{S}, g)$ 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 $\mathrm{T}(\mathcal{S}, g)$ is

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

where the rows are indexed by $\boldsymbol{a} \in \mathbb{N}^{\deg(g_1)-1 \times \cdots \times \deg(g_m)-1}$.

Multivariate Goppa codes via parity check matrices

Theorem (parity check matrix representation)

If T is a generator matrix of $\mathsf{T}(\mathcal{S}, g)$, then

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

that is, a parity check matrix for the multivariate Goppa code is of the form

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

Augmented codes

Consider $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$,
$L_j(x_j) := \prod_{s \in S_j} (x_j - s) \in \mathbb{F}_{q^t}[x_j]$ for each $j \in [m]$, and the product

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

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

Augmented codes

Consider $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq \mathbb{F}_{q^t}^m$,
$L_j(x_j) := \prod_{s \in S_j} (x_j - s) \in \mathbb{F}_{q^t}[x_j]$ for each $j \in [m]$, and the product

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

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

augmented Cartesian codes

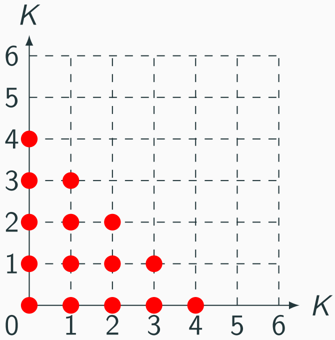
Suppose $h \in \mathbb{F}_{q^t}[\boldsymbol{x}]$ is such that $h(\mathcal{S}) \neq 0$. An augmented Cartesian code is

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

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

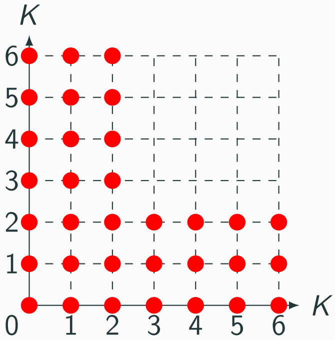
Example: Reed-Muller code

$RM(7, 2, 4)$

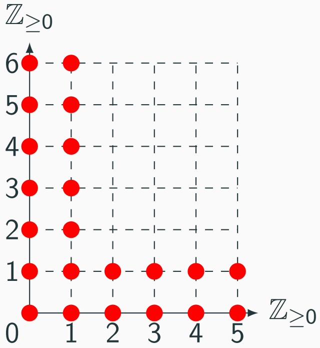


Example: Augmented Reed-Muller code

$ARM(7, 2, 4)$



Example: Augmented Cartesian code



Multivariate Goppa codes as subfield subcodes

Theorem (subfield subcode representation)

A multivariate Goppa code is a subfield subcode of an augmented Cartesian code, meaning

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

Duals of multivariate Goppa codes as trace codes

Theorem

The dual of a multivariate Goppa code is

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

Parameters of multivariate Goppa codes

Theorem

The multivariate Goppa code $\Gamma(\mathcal{S}, g)$ is an $[n, k, d]$ code with

- length $n = \mid \mathcal{S} \mid$.
- dimension k satisfying

$$n - t \deg(g) \leq k \leq n - \deg(g).$$

- minimum distance

$$d \geq \min \left\{\deg(g_j) + 1\right\}_{j \in [m]} .$$

Properties of multivariate Goppa codes

Proposition

- $\Gamma(\mathcal{S}, gg') \subseteq \Gamma(\mathcal{S}, g)$.
- $\Gamma(\mathcal{S}, g) \cap \Gamma(\mathcal{S}, g') = \Gamma(\mathcal{S}, \mathsf{lcm}(g, g'))$.

Hulls

The hull of a code C is $Hull(C) := C \cap C^{\perp}$.

Hulls

The hull of a code C is $\mathit{Hull}(C) := C \cap C^{\perp}$.

A code is

- self-orthogonal (meaning $C \subseteq C^{\perp}$) iff $\mathit{Hull}(C) = C$.
- self-dual (meaning $C = C^{\perp}$) iff $\mathit{Hull}(C) = C^{\perp}$
- linearly complementary dual (LCD) iff $\mathit{Hull}(C) = \{0\}$.

Hulls

The hull of a code C is $Hull(C) := C \cap C^{\perp}$.

A code is

- self-orthogonal (meaning $C \subseteq C^{\perp}$) iff $Hull(C) = C$.
- self-dual (meaning $C = C^{\perp}$) iff $Hull(C) = C^{\perp}$
- linearly complementary dual (LCD) iff $Hull(C) = \{0\}$.

Hulls play a role in the complexity of algorithms:

- Sendrier's support splitting algorithm is exponential in the dimension of a hull.
- Bardet, Otmani, and Saeed-Taha proved that the permutation code equivalence between codes $C, C' \subseteq \mathbb{F}_q^n$ can be decided in $O\left(hn^{w+dim(Hull(C))+1}t(n)\right)$ operations where $t(n)$ is the complexity of deciding isomorphism of graphs on n vertices with weights from $\mathbb{F}_q$.

Hulls of multivariate Goppa codes

Theorem

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

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

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

- $\deg(g_{j^*}) \geq n_{j^*}/2$,
- $\deg(f_{j^*} g_{j^*}) = n_{j^*}$,
- $\deg(f_j) = \deg(g_j) = n_j$, for all $j \in [m] \setminus \{j^*\}$, and
- $\deg_{x_{j^*}} \left(\frac{fg}{L} \right) = 0$.

Hulls of multivariate Goppa codes

Theorem

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

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

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

- $\deg(g_{j^*}) \geq n_{j^*}/2$,
- $\deg(f_{j^*} g_{j^*}) = n_{j^*}$,
- $\deg(f_j) = \deg(g_j) = n_j$, for all $j \in [m] \setminus \{j^*\}$, and
- $\deg_{x_{j^*}}\left(\frac{fg}{L}\right) = 0$.

We say that f and g satisfying the theorem above satisfy condition $(*)$.

Hulls of multivariate Goppa codes

Corollary

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

Corollary

- $\Gamma(\mathcal{S}, g)$ is LCD if $t = 1$ and $\deg_{x_j}(\mathrm{lcm}(f, g)) \geq n_j$ for all $j \in [m]$.
- $\Gamma(\mathcal{S}, g)$ is self-orthogonal if $t = 1$ and f divides g.
- $\Gamma(\mathcal{S}, g)$ is self-dual if $t = 1$ and $f = g$.

Example: family of long LCD codes

Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$. Let $S_1 := \{0, 1, a, a^7\}$ and $S_2 := \{1, a^5, a^7\}$.
Set

$$f_1 := x + 1,$$

$$g_1 := 2x^3 + a^5x^2 + a^5x + 1,$$

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 $p(x) = x^3 + a^5x^2 + a^2x + a^6$. Set

$$g := g_1(x)g_2(x_1)\cdots g_2(x_m).$$

Then $\Gamma(\mathcal{S}, g)^\perp$ is a $[4 \cdot 3^m, 3^{m+1}]$ LCD code over $\mathbb{F}_9$.

Example: family of long self-orthogonal codes

Assume $\mathbb{F}_{3^2}^* = \langle a \rangle$. Let $S_1 := \{0, 1, 2, a\}$ and $S_2 := \left\{1, a^5, a^7\right\}$. Set

$$f_1 := ax^3 + 2x^2 + a^7 x + a,$$

$$g_1 := a^2 x + 1,$$

and

$$f_2 := g_2 := x^3 + ax^2 + 2x.$$

Then

$$f_1 g_1 = L_1' + a^3 L_1 \qquad \text{and} \qquad f_2 g_2 = a^2 L_2' + pL_2,$$

where $p(x) = x^3 + a^5 x^2 + a^2 x + a^6$. Set

$$g := g_1(x) g_2(x_1) \cdots g_2(x_m).$$

Then $\Gamma(\mathcal{S}, g)^\perp$ is a $[4 \cdot 3^m, 3^m]$ self-orthogonal code over $\mathbb{F}_9$.

q-ary entanglement-assisted quantum error-correcting codes

Lemma [K. Guenda, S. Jitman, and T. A. Gulliver, 2018]

Given an $[n, k, d]$ code C over $\mathbb{F}_q$, there exist EAQECCs with parameters

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

q-ary EAQECCs from multivariate Goppa codes

Theorem

Let $\mathcal{S} \subseteq \mathbb{F}_{q^t}^m$, g and f satisfy condition $(*)$. Then the code $T(\mathcal{S}, g)$ gives rise to EAQECCs with parameters

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

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

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

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

q-ary EAQECCs from multivariate Goppa codes

Corollary

Let $\mathcal{S} \subseteq \mathbb{F}_q^m$, g and f satisfy condition $(*)$. Then the code $T(\mathcal{S}, g)$ gives rise to an MDS EAQECC.

q-ary EAQECCs from multivariate Goppa codes

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

Table 1: New EAQECCs. For every row, we assume that $\mathbb{F}_q^* = \langle a \rangle$.

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 $p(x) = x^2 + a^7x + a$. 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 $\deg(g) = 3 \cdot 2^m$, 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.

References

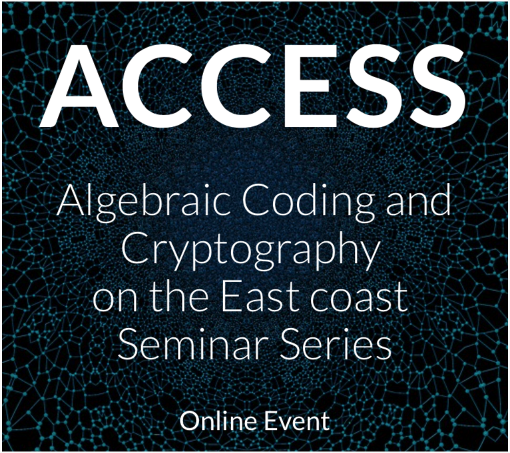
Yanyan Gao, Qin Yue, Xinmei Huang, and Jun Zhang. Hulls of generalized Reed-Solomon codes via Goppa codes and their applications to quantum codes. *IEEE Transactions on Information Theory*, 67(10):6619–6626, 2021. doi:10.1109/TIT.2021.3074526.

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.

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*, 68(3):1651–1662, 2022. doi:10.1109/TIT.2021.3130096.

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.

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



Thank you! gmatthews@vt.edu