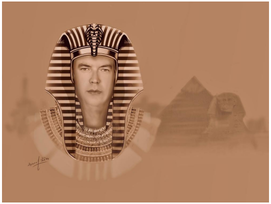
Generator polynomial matrices of the Galois hulls of multi-twisted codes

available from arXiv:2305.15237

Patrick Solé
joint work with
Ramy TakiEldin

CNRS/I2M, Marseilles, France,



Cyclic codes

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ of length n, or equivalently, a subspace of $\mathbb{F}_q^n$. We call $\mathcal{C}$ cyclic if it is invariant under the cyclic shift which is given by the linear transformation

$$\mathcal{T} : (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \mapsto (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$$

on $\mathbb{F}_q^n$. The polynomial representation of

$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}_q^n$ is $\sum_{i=0}^{n-1} a_i x^i$.

This map induces an $\mathbb{F}_q$-vector space isomorphism between $\mathbb{F}_q^n$ and the quotient ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$.

Hence, a cyclic code has the structure of an ideal in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$.

A cyclic code over $\mathbb{F}_q$ of length n can also be viewed as an ideal in the polynomial ring $\mathbb{F}_q[x]$ containing $\langle x^n - 1 \rangle$.

Constacyclic codes

Same definition with the shift replaced by the constashift of constant λ

$$\mathcal{T}_\lambda : (c_0, c_1, c_2, \ldots, c_{n-1}) \mapsto (\lambda c_{n-1}, c_0, c_1, c_2, \ldots, c_{n-2})$$

This gives $\mathcal{C}$ the structure of an ideal in $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$.

Ideals of $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ are in a one-to-one correspondence with ideals of $\mathbb{F}_q[x]$ containing $\langle x^n - \lambda\rangle$.
Example: Negacyclic codes for the Lee metric . Let $q = 5$ and $n = 2$. A perfect code is obained for

$$< 12 >= \{00, 12, 24, 31, 43\}.$$

Quasi-cyclic codes

If $\mathcal{C}$ is a quasi-cyclic code (QC) over $\mathbb{F}_q$ of length $n = m\ell$, of index ℓ and co-index m, then $\mathcal{C}$ is invariant under

$$\mathcal{T} : (c_{0,1}, c_{0,2}, \dots, c_{0,\ell}, c_{1,1}, c_{1,2}, \dots, c_{1,\ell}, \dots, c_{m-1,1}, c_{m-1,2}, \dots, c_{m-1,\ell})$$
$$\mapsto (c_{m-1,1}, c_{m-1,2}, \dots, c_{m-1,\ell}, c_{0,1}, c_{0,2}, \dots, c_{0,\ell}, \dots, c_{m-2,1}, c_{m-2,2}, \dots$$

This gives $\mathcal{C}$ the structure of an $\mathbb{F}_q[x]$- submodule of

$\oplus_{j=1}^{\ell} \mathbb{F}_q[x]/\langle x^m - 1\rangle$.

Submodules of $\oplus_{j=1}^{\ell} \mathbb{F}_q[x]/\langle x^m - 1\rangle$ are in one-to-one correspondence with submodules of $(\mathbb{F}_q[x])^{\ell}$ containing the submodule $\oplus_{j=1}^{\ell} \langle x^m - 1\rangle$.

Example: Shortened Hamming code $[6, 4, 3]_2$, with $\ell = 2$, $m = 3$

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Generalized Quasi-cyclic codes

Similar to QC codes but with a variable co-index. This gives $\mathcal{C}$ the structure of an $\mathbb{F}_q[x]$-submodule of $\oplus_{j=1}^{\ell}\mathbb{F}_q[x]/\langle x^{m_j}-1\rangle$. Submodules of $\oplus_{j=1}^{\ell}\mathbb{F}_q[x]/\langle x^{m_j}-1\rangle$ are in one-to-one

correspondence with submodules of $(\mathbb{F}_q[x])^{\ell}$ containing the submodule $\oplus_{j=1}^{\ell}\langle x^{m_j}-1\rangle$.

Example: Cordaro-Wagner code $[10,2,6]_2$, with $m_1=3, m_2=4, m_3=3$

$$G=\begin{pmatrix}1&1&1&0&0&0&0&1&1&1\\0&0&0&1&1&1&1&1&1&1\end{pmatrix}$$

Quasi-twisted codes

Similar to QC codes but with nontrivial shift constant.
This gives $\mathcal{C}$ the structure of an $\mathbb{F}_q[x]$-submodule of $\oplus_{j=1}^{\ell}\mathbb{F}_q[x]/\langle x^m - \lambda\rangle$.
Submodules of $\oplus_{j=1}^{\ell}\mathbb{F}_q[x]/\langle x^m - \lambda\rangle$ are in one-to-one correspondence with submodules of $(\mathbb{F}_q[x])^{\ell}$ containing the submodule $\oplus_{j=1}^{\ell}\langle x^m - \lambda\rangle$.
Example: tetracode $[4,2,3]_3$, with $\lambda = -1$ and $\ell = m = 2$.

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

Multi-twisted codes

If $\mathcal{C}$ is a Λ- MT code over $\mathbb{F}_q$ of length $n = \sum_{j=1}^{\ell} m_j$ and shift constants $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$, then $\mathcal{C}$ is invariant under

$$\mathcal{T}_\Lambda : (c_{0,1}, c_{1,1}, \ldots, c_{m_1-1,1}, c_{0,2}, c_{1,2}, \ldots, c_{m_2-1,2}, \ldots, c_{0,\ell}, c_{1,\ell}, \ldots, c_{m_\ell-1,\ell}$$
$$\mapsto (\lambda_1 c_{m_1-1,1}, c_{0,1}, \ldots, c_{m_1-2,1}, \lambda_2 c_{m_2-1,2}, c_{0,2}, \ldots, c_{m_2-2,2}, \ldots, \lambda_\ell c_{m_\ell-1,\ell}, c_{0,\ell}, \ldots, c_{m_\ell-2,\ell})$$

This gives $\mathcal{C}$ the structure of an $\mathbb{F}_q[x]$-submodule of

$$\oplus_{j=1}^{\ell} \mathbb{F}_q[x]/\langle x^{m_j} - \lambda_j \rangle.$$

Submodules of $\oplus_{j=1}^{\ell} \mathbb{F}_q[x]/\langle x^{m_j} - \lambda_j \rangle$ are in one-to-one correspondence with the submodules of $(\mathbb{F}_q[x])^{\ell}$ containing the submodule $\oplus_{j=1}^{\ell} \langle x^{m_j} - \lambda_j \rangle$.

Historical perspective

I tried to list the earliest or most important articles inroducing the following classes of codes.

- Cyclic codes: (Prange, 1957), (Bose and Ray-chaudhuri, 1960), (Hocquenghem, 1959)
- Constacyclic codes: (Berlekamp, 1968), (Krishna, Sarwate, 1990)
- Quasi-cyclic codes: (C.L. Chen, W.W. Peterson, E.J. Weldon, 1969), (Kasami, 1974)
- Quasi-twisted codes: (Aydin et al 2001)
- Generalized Quasi-cyclic codes: (Siap, Kuhlan, 2005)
- Multitwisted codes: (Aydin et al., 2017)

Generator polynomial matrices

If $\mathcal{C}$ is QC, it has a generator polynomial matrix (GPM) **G** such that

$$\mathbf{A}\mathbf{G} = \mathrm{diag}(x^m - 1)I_\ell.$$

The dimension of $\mathcal{C}$ is, taking determinant of both sides

$$\dim(\mathcal{C}) = \deg(\det(\mathbf{A})) = m\ell - \deg(\det(\mathbf{G})).$$

GPM matrices of MT codes

Thus, $\mathcal{C}$ has a GPM $\mathbf{G}$ such that

$$\mathbf{AG} = \mathrm{diag}\left[x^{m_j} - \lambda_j\right]. \qquad \text{(Identical Equation)}$$

The dimension of $\mathcal{C}$ is
$\dim(\mathcal{C}) = \deg(\det(\mathbf{A})) = \sum_{j=1}^{\ell} m_j - \deg(\det(\mathbf{G}))$.

The Hermite normal form of $\mathbf{G}$ yields the reduced GPM of $\mathcal{C}$.
If N denotes the order of $\mathcal{T}_\Lambda$, then $N = \mathrm{lcm}\{t_1 m_1, t_2 m_2, \ldots, t_\ell m_\ell\}$, where t_i is the multiplicative order of λ_i.

Duality

The Euclidean dual

$$\mathcal{C}^{\perp} = \{\mathbf{a} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathbf{a} \rangle = 0 \quad \forall \mathbf{c} \in \mathcal{C}\}.$$

Let $q = p^e$ and let $0 \leq \kappa < e$. The κ-Galois dual of $\mathcal{C}$ is

$$\mathcal{C}^{\perp_\kappa} = \{\mathbf{a} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathbf{a} \rangle_\kappa = 0 \quad \forall \mathbf{c} \in \mathcal{C}\}$$

where

$$\langle \mathbf{c}, \mathbf{a} \rangle_\kappa = \sum_{i=1}^{n} c_i \ a_i^{p^\kappa} = \sum_{i=1}^{n} c_i \ \sigma^\kappa(a_i) = \langle \mathbf{c}, \sigma^\kappa(\mathbf{a}) \rangle.$$

It follows that $\mathcal{C}^{\perp_\kappa} = \sigma^{e-\kappa}\left(\mathcal{C}^{\perp}\right)$. In addition,

1. If $\mathcal{C}$ is cyclic, then $\mathcal{C}^{\perp_\kappa}$ is cyclic.
2. If $\mathcal{C}$ is λ-constacyclic, then $\mathcal{C}^{\perp_\kappa}$ is $\sigma^{e-\kappa}\left(\lambda^{-1}\right)$-constacyclic.
3. If $\mathcal{C}$ is QC, then $\mathcal{C}^{\perp_\kappa}$ is QC.
4. If $\mathcal{C}$ is Λ-MT, then $\mathcal{C}^{\perp_\kappa}$ is $\sigma^{e-\kappa}\left(\Lambda^{-1}\right)$-MT.

GPM of the duals

Let $\mathcal{C}$ be a Λ-MT code over $\mathbb{F}_{p^e}$ of index ℓ and block lengths $(m_1, m_2, \dots, m_\ell)$, where $\Lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$. Let $\mathbf{G}$ be the reduced GPM of $\mathcal{C}$ and let $\mathbf{A}$ be the polynomial matrix satisfying the identical equation of $\mathbf{G}$. For any $0 \leq \kappa < e$, construct the polynomial matrix $\mathbf{H}$ such that for each $1 \leq i \leq \ell$

$$\mathrm{Col}_i\left(\mathbf{H}\right) \equiv \mathrm{Row}_i\left(\mathrm{diag}\left[x^{m_j}\right]\mathbf{A}\left(\frac{1}{x}\right)\mathrm{diag}\left[x^{-d_j}\right]\right) \pmod{x^{m_i} - \frac{1}{\lambda_i}}.$$

1. Then $\mathbf{H}$ is a GPM for $\mathcal{C}^\perp$.
2. Hence $\mathbf{H}_\kappa = \sigma^{e-\kappa}\left(\mathbf{H}\right)$ is a GPM for $\mathcal{C}^{\perp_\kappa}$.

Structure of the dual of MT codes

We shall now consider a sufficient condition under which the Galois hull of a MT code is MT as well.

Let $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ and let $\mathcal{C}$ be a Λ-MT code over $\mathbb{F}_q$ of index ℓ and block lengths $(m_1, m_2, \ldots, m_\ell)$.

If $\lambda_j^{-p^{e-\kappa}} = \lambda_j$ for $1 \leq j \leq \ell$, then the Galois hull of C, $h_\kappa(\mathcal{C})$ is Λ-MT code over $\mathbb{F}_q$ of index ℓ and block lengths $(m_1, m_2, \ldots, m_\ell)$.

Numerical Example I

Let $p = 2$, $e = 4$, $q = 16$, $n = 9$, $\ell = 3$, $m_1 = 3$, $m_2 = 2$, $m_3 = 4$, and $\lambda_1 = \lambda_2 = \lambda_3 = 1$. Consider the GQC code $\mathcal{C}$ over $\mathbb{F}_q$ of index ℓ, co-indices (m_1, m_2, m_3), and reduced GPM

$$\mathbf{G} = \begin{pmatrix} x^2 + x + 1 & 1 & \theta^5 x + \theta^5 \\ 0 & x + 1 & \theta^5 x^2 + \theta^5 \\ 0 & 0 & x^3 + x^2 + x + 1 \end{pmatrix}$$

where $\theta \in \mathbb{F}_q$ such that $\theta^4 + \theta + 1 = 0$. The matrix that satisfies the identical equation of $\mathbf{G}$ is

$$\mathbf{A} = \begin{pmatrix} x + 1 & 1 & 0 \\ 0 & x + 1 & \theta^5 \\ 0 & 0 & x + 1 \end{pmatrix}.$$

Numerical Example II

The construction of a GPM $\mathbf{H}$ for the Euclidean dual $\mathcal{C}^{\perp}$ gives

$$\mathrm{Col}_i\left(\mathbf{H}\right) \equiv \mathrm{Row}_i\left(\mathrm{diag}\left[x^3, x^2, x^4\right]\mathbf{A}\left(\frac{1}{x}\right)\mathrm{diag}\left[x^{-2}, x^{-1}, x^{-3}\right]\right) \pmod{x^{m_i}-1}$$

for $i = 1, 2, 3$. That is,

$$\mathbf{H} = \begin{pmatrix} x+1 & 0 & 0 \\ x^2 & x+1 & 0 \\ 0 & \theta^5 x & x+1 \end{pmatrix}.$$

If we let $\kappa = 3$, then the κ-Galois dual $\mathcal{C}^{\perp_3}$ of $\mathcal{C}$ is GQC as well, with GPM

$$\mathbf{H}_3 = \sigma\left(\mathbf{H}\right) = \begin{pmatrix} x+1 & 0 & 0 \\ x^2 & x+1 & 0 \\ 0 & \theta^{10} x & x+1 \end{pmatrix}.$$

Numerical Example III

We claim that $\mathcal{C}$ is κ-Galois self-orthogonal. In fact, $\mathcal{C} \subseteq \mathcal{C}^{\perp_3}$ if and only if $\mathbf{G} = \mathbf{M}\mathbf{H}_3$ for some polynomial matrix $\mathbf{M}$. Our claim is true because $\mathbf{G} = \mathbf{M}\mathbf{H}_3$ for

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & \theta^5 \\ x^2 & x+1 & \theta^5 x + \theta^5 \\ \theta^{10} x^3 & \theta^{10} x^2 + \theta^{10} x & x^2 + 1 \end{pmatrix}.$$

Previous work I

Let $\mathcal{C}$ be a Λ-MT code over $\mathbb{F}_{p^e}$ of index ℓ and block lengths $(m_1, m_2, \ldots, m_\ell)$, where $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$. Let $\mathbf{G}$ be the reduced GPM of $\mathcal{C}$ and let $\mathbf{A}$ be the polynomial matrix satisfying the identical equation of $\mathbf{G}$. For any $0 \leq \kappa < e$, construct the polynomial matrix $\mathbf{H}$ such that for each $1 \leq i \leq \ell$

$$\mathrm{Col}_i(\mathbf{H}) \equiv \mathrm{Row}_i\left(\mathrm{diag}\left[x^{m_j}\right]\mathbf{A}\left(\frac{1}{x}\right)\mathrm{diag}\left[x^{-d_j}\right]\right) \pmod{x^{m_i} - \frac{1}{\lambda_i}}.$$

1. Then $\mathbf{H}$ is a GPM for $\mathcal{C}^\perp$.
2. Hence $\mathbf{H}_\kappa = \sigma^{e-\kappa}(\mathbf{H})$ is a GPM for $\mathcal{C}^{\perp_\kappa}$.

Previous work II

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_{p^e}$ of length n with a generator matrix S. For any $0 \leq \kappa < e$,

$$\mathrm{Rank}\left(S\sigma^{\kappa}\left(S^{t}\right)\right) = \dim\left(\mathcal{C}\right) - \dim\left(h_{\kappa}\left(\mathcal{C}\right)\right)$$

Published: 27 September 2019

Galois hulls of linear codes over finite fields

Hongwei Liu & Xu Pan Designs, Codes and Cryptography **88**, 241–255 (2020)

Theorem 3.1 *Let C be an $[n, k]$ linear code over $\mathbb{F}_q$ with a generator matrix G. Let h be the dimension of the ℓ-Galois hull $h_\ell(C) = C \bigcap C^{\perp_\ell}$ of C, and let $r = k - h$. Then there exists a generator matrix G_0 of C such that*

$$G_0\sigma^{\ell}(G_0^T) = \begin{pmatrix} O_{h\times h} & H_{h\times r} \\ O_{r\times h} & P_{r\times r} \end{pmatrix},$$

where $O_{h\times h}$ and $O_{r\times h}$ are respectively zero matrices of sizes $h \times h$ and $r \times h$, and the rank $r(Q)$ of $Q = \begin{pmatrix} H_{h\times r} \\ P_{r\times r} \end{pmatrix}$ is r. Furthermore, the rank $r(G\sigma^{\ell}(G^T))$ of $G\sigma^{\ell}(G^T)$ is r for any generator matrix G of C.

Research program

Can we determine the dimension of $h_\kappa(\mathcal{C})$ **for a MT code** $\mathcal{C}$ **from a GPM instead of a generator matrix?**

Can we provide a GPM for $h_\kappa(\mathcal{C})$ **?**

A canonical QC code attached an MT code

With each GPM $\mathbf{G}$ of an MT code we will associate a QC code of index ℓ and co-index N,

$$N = \operatorname{lcm}\{t_1 m_1, t_2 m_2, \ldots, t_\ell m_\ell\},$$

where t_j is the multiplicative order of λ_j in the relevant finite field. Let $\mathbf{G}$ be a GPM of a Λ-MT code, where $\Lambda^{-p^{-\kappa}} = \Lambda$. We define

$$\mathfrak{B}_{\mathbf{G}} \equiv \mathbf{G}\,\mathrm{diag}\left[\frac{x^N - 1}{x^{m_j} - \lambda_j}\right] \sigma^{\kappa}\left(\mathbf{G}\left(\frac{1}{x}\right)\mathrm{diag}\left[x^{m_j}\right]\right)^t \pmod{\left(x^N - 1\right)}$$

such that entries of $\mathfrak{B}_{\mathbf{G}}$ are of degree at most $N-1$. Again, by $\mathbf{G}\left(\frac{1}{x}\right)$ we mean to replace x by $\frac{1}{x}$ in $\mathbf{G}$.

The dimension of the hull I

Let $\mathcal{Q}_{\mathbf{G}}$ be the row span of $\mathfrak{B}_{\mathbf{G}}$. This code is QC of length $N\ell$ and index ℓ over $\mathbb{F}_q$, and is generated as an $\mathbb{F}_q[x]$-module by the rows of the polynomial matrix

$$\begin{pmatrix} \mathfrak{B}_{\mathbf{G}} \\ \left(x^N - 1\right) \mathbf{I}_\ell \end{pmatrix}.$$

Furthermore, the dimension of $\mathcal{Q}_{\mathbf{G}}$ as an $\mathbb{F}_q$-vector space is

$$\dim\left(\mathcal{Q}_{\mathbf{G}}\right) = \dim\left(\mathcal{C}\right) - \dim\left(h_\kappa\left(\mathcal{C}\right)\right).$$

In particular, the code $\mathcal{C}$ is κ-Galois self-orthogonal iff

$$\dim\left(\mathcal{Q}_{\mathbf{G}}\right) = 0.$$

It is κ-Galois LCD iff $\dim\left(\mathcal{Q}_{\mathbf{G}}\right) = \dim\left(\mathcal{C}\right)$.

The dimension of the hull II

The dimension $\dim(h_\kappa(\mathcal{C}))$ can be computed from the determinantal divisors of $\mathfrak{B}_{\mathbf{G}}$.

$$\dim(h_\kappa(\mathcal{C})) = \dim(\mathcal{C}) + \deg\left(\gcd_{0\le i\le \ell}\left\{\left(x^N-1\right)^{\ell-i}\mathfrak{d}_i(\mathfrak{B}_{\mathbf{G}})\right\}\right) - N\ell$$

where $\mathfrak{d}_i(\mathfrak{B}_{\mathbf{G}})$ is the i-th determinantal divisor of $\mathfrak{B}_{\mathbf{G}}$.
The code $\mathcal{C}$ is κ-Galois LCD if and only if $\dim(\mathcal{Q}_{\mathbf{G}}) = \dim(\mathcal{C})$ if and only if

$$\deg\left(\gcd_{0\le i\le \ell}\left\{\left(x^N-1\right)^{\ell-i}\mathfrak{d}_i(\mathfrak{B}_{\mathbf{G}})\right\}\right) = N\ell - \dim(\mathcal{C}).$$

The last slide

Merci beaucoup!!!!!

Viel dank!!!!

Grazie Mille!!!!

Grazcha fich!!!!