Goppa codes from a Singer cycle

Valentino Smaldore

Università degli Studi di Padova

Seventh Irsee Conference

joint work with G. Korchmáros and F. Romaniello

September 4, 2025

Linear codes

Definition

An $[n, k]_q$-linear code $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$ of dimension k.

Definition

- *The Hamming distance between two codewords $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ is the number of entries in which x and y differ: $d(x, y) = |\{i | x_i \neq y_i\}|$.*
- *The minimum distance of a code $\mathcal{C}$ is $d = d(\mathcal{C}) = min\{d(x, y) | x, y \in \mathcal{C}, x \neq y\}$.*

In this case we say $\mathcal{C}$ is a $[n, k, d]_q$-linear code.

Theorem

Let $\mathcal{C}$ be a $[n, k, d]_q$-linear code. Then, $\mathcal{C}$ can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.
If is used for detection, $\mathcal{C}$ can detect $d - 1$ errors.

Linear codes

Dual codes

Definition

Let $\mathcal{C}$ be an $[n, k]_q$-linear code. Consider the standard inner product in $\mathbb{F}_{q^n}$: $x \cdot y = \sum_{i=1}^{n} x_i y_i$. The dual code $\mathcal{C}^\perp$ is

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_{q^n} \mid x \cdot c = 0, \forall c \in \mathcal{C}\}$$

Theorem

$\mathcal{C}^\perp$ is a $[n, n-k]_q$-code.

Linear codes

Gilbert-Varshamov bound

Proposition (Gilbert-Varshamov Bound)

An $[n, k, d]_q$ code exists if

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i.$$

Goppa codes

Goppa codes

Curves and divisors

p prime, $h \in \mathbb{N}$, $q = p^h$.
$\mathcal{C}$: non-singular plane curve over $\mathbb{F}_q$.

Definition

- *A divisor* $\mathtt{G}$ *is a formal power series of places of* $\mathcal{C}$.
- *The Riemann-Roch space* $\mathcal{L}(\mathtt{G})$ *is the vector space consisting of all rational functions that are regular outside* G.

Theorem (**Riemann-Roch Theorem**)

$$\ell(\mathtt{G}) = deg(\mathtt{G}) - \mathfrak{g} + 1 + \ell(\mathtt{W} - \mathtt{G}),$$

where $\mathfrak{g}$ *is the genus of the curve,* $\ell(\mathtt{G}) = dim(\mathcal{L}(\mathtt{G}))$ *and* $\mathtt{W}$ *is a canonical divisor. In particular, for* $deg(\mathtt{G}) > 2\mathfrak{g} - 2$,

$$\ell(\mathtt{G}) = deg(\mathtt{G}) - \mathfrak{g} + 1.$$

Goppa codes

Construction

The functional code $C_L(\mathtt{D}, \mathtt{G})$ arises as follows: take a divisor $\mathtt{G}$ with support $G \subseteq \mathcal{C}$, and take $P_1, \ldots, P_N = D$, and assume $D \cap G = \emptyset$. Then evaluating the functions $f \in \mathcal{L}(\mathtt{G})$ on D produces a linear code of length N and dimension $\ell(\mathtt{G})$.

Proposition

The minimum distance of $C_L(\mathtt{D}, \mathtt{G})$ is at least $\delta = n - deg(\mathtt{G})$.

Definition

The differential code $C_\Omega(\mathtt{D}, \mathtt{G})$ is the dual code $C_L^\perp(\mathtt{D}, \mathtt{G})$.

Here $\mathcal{C}$ is the Hermitian curve $H(2, q^2) : Y^q + Y - X^{q+1} = 0$, G is an orbit of a large $\Gamma \leq Aut(H(2, q^2)) \cong PGU(3, q)$, $G \cup D = \mathcal{C}$.

Goppa codes

Subgroups of $PGU(3, q)$

Theorem

Let d be a divisor of $q = p^k$. The following is the list of maximal subgroups in $PSU(3, q)$ (up to conjugacy)

(i) *The one-point stabilizer (order $\frac{q^3(q^2-1)}{d}$);*

(ii) *The stabilizer of a non-tangent line (order $\frac{q(q^2-1)(q+1)}{d}$);*

(iii) *the stabilizer of a self-conjugate triangle (order $\frac{6(q+1)}{d}$);*

(iv) *the normalizer of a cyclic Singer group (order $\frac{3(q^2-q+1)}{d}$);*

further when q is odd:

(v) *the stabilizer of a conic $PGL(2, q)$;*

(vi) *$PSU(3, p^m)$, with $m \mid k$ and $\frac{k}{m}$ odd;*

(vii) *the subgroup containing $PSU(3, p^m)$ as index 3 normal subgroup, with $m \mid k$, $\frac{k}{m}$ odd, and 3 divides both $q + 1$ and $\frac{k}{m}$;*

(viii) *the Hessian groups of order 216 when $9 \mid (q + 1)$ and of order 72 and 36 when $3 \mid (q + 1)$;*

(ix) *$PSL(2, 7)$ when either $p = 7$ or -7 is not a square in $\mathbb{F}_q$;*

(x) *A_6 when either $p = 3$ and k is even, or 5 is a square in $\mathbb{F}_q$ and $\mathbb{F}_q$ contains no cubic roots of the unity;*

(xi) *S_6 when $p = 5$ and k odd;*

(xii) *A_7 when $p = 5$ and k odd...*

Goppa codes

Constructions of Goppa codes

Group (i) *On Goppa codes and Weierstrass gaps at several points*, C. Carvalho, F. Torres, Designs, Codes and Cryptography, 2005, 35, pp. 211-225;

Group (v) *Hermitian curves with automorphism group isomorphic to $PGL(2, q)$ with q odd*, G. Korchmáros, P. Speziali, Finite Fields and their Applications, 2017, 44, pp. 1-17;

Group (vi) *Codes and gap sequences of Hermitian curves*, G. Korchmáros, G. P. Nagy, M. Timpanella, IEEE Transactions of Information Theory, 2019, 66(6), pp. 3547-3554.

Singer cycles on $PG(2, q^6)$

The group (iv)

The group of size $3(q^2 - q + 1)$ is the normalizer of a Singer cycle. The Singer cycle acts on the Hermitian curve $H(2, q^2)$ regularly on a point-orbit of lenght $q^2 - q + 1$. The matrices representing such a subgroup of $PGU(3, q)$ may be represented by the 3×3 matrices of the shape

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & c \end{pmatrix},$$

where $X^3 + aX^2 + bX + c \in \mathbb{F}_{q^2}[X]$ is an irreducible polynomial.

Singer cycles on $PG(2,q^6)$

Cubic extension

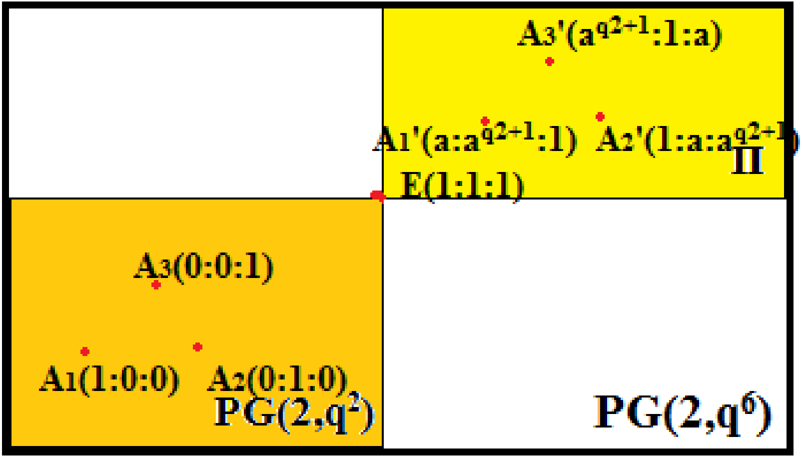
$PG(2,q^2) \subseteq PG(2,q^6)$.
a primitive (q^4+q^2+1)-th root of the unity in $\mathbb{F}_{q^6}$.

$$M = \begin{pmatrix} a & 1 & a^{q^2+1} \\ a^{q^2+1} & a & 1 \\ 1 & a^{q^2+1} & a \end{pmatrix}$$

maps the canonical subplane $PG(2,q^2)$ onto
$\Pi = \{(a^i : a^{i(q^2+1)} : 1) \mid i = 0,1,\dots,q^4+q^2\}$.
$A_1(1:0:0) \mapsto A_1'(a : a^{q^2+1} : 1)$
$A_2(0:1:0) \mapsto A_2'(1 : a : a^{q^2+1})$
$A_3(0:0:1) \mapsto A_3'(a^{q^2+1} : 1 : a)$
$E(1:1:1)$ is fixed.

Singer cycles on $PG(2, q^6)$

Cubic extension



Singer cycles on $PG(2, q^6)$

Cubic extension

Construction

In Π, the Singer cycle is represented by

$$B = \begin{pmatrix} \beta & 0 & 0 \\ 0 & \beta^{q^2+1} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where β is a primitive $(q^2 - q + 1)$-th root of the unity.

Singer cycles on $PG(2, q^6)$

Cubic extension

$\mathcal{C} = v(G(\overline{X_0}, \overline{X_1}, \overline{X_2}))$ is the zero locus of the polynomial

$$G(\overline{X_0}, \overline{X_1}, \overline{X_2}) = \overline{X_1}^2 \overline{X_2}^{2q} + \overline{X_0}^2 \overline{X_1}^{2q} + \overline{X_0}^{2q} \overline{X_2}^2 +$$

$$-2(\overline{X_0}^{q+1} \overline{X_1}^q \overline{X_2} + \overline{X_0}^q \overline{X_1 X_2}^{q+1} + \overline{X_0 X_1}^{q+1} \overline{X_2}^q).$$

$\mathfrak{g}(\mathcal{C}) = \frac{q^2-q}{2}$, $|\mathcal{C}(\mathbb{F}_{q^6})| = q^6 + q^5 - q^4 + 1$.
The singular points of $\mathcal{C}$ have coordinates $(1:0:0)$, $(0:1:0)$, $(0:0:1)$ in the system of coordinates $(\overline{X_0}, \overline{X_1}, \overline{X_2})$.

Singer cycles on $PG(2, q^6)$

Cubic extension

$$M^{-1} = \frac{1}{|M|} \begin{pmatrix} a^2 - a^{q^2+1} & 1 - a^{q^2+2} & a^{2q^2+2} - a \\ a^{2q^2+2} - a & a^2 - a^{q^2+1} & 1 - a^{q^2+2} \\ 1 - a^{q^2+2} & a^{2q^2+2} - a & a^2 - a^{q^2+1} \end{pmatrix}.$$

$\mathcal{D} = v(H(X_0, X_1, X_2))$ is a plane model $H(2, q^2)$, where

$$H(X_0, X_1, X_2) = G(aX_0 + X_1 + a^{q^2+1}X_2,$$

$$a^{q^2+1}X_0 + aX_1 + X_2, X_0 + a^{q^2+1}X_1 + aX_2).$$

The singular points of $\mathcal{D}$ have coordinates defined by the three columns of M^{-1}.

The new codes

The functional code $C_L(\mathtt{D}, \mathtt{G})$

$P_1, \ldots, P_{q^2-q+1}$ orbit of a Singer cycle.
$\mathtt{G} = P_1 + \ldots + P_{q^2-q+1}$.
$\mathtt{D}$ divisor whose support is $H(2, q^2) \setminus \{P_1, \ldots, P_{q^2-q+1}\}$.

Theorem

The code $C_L(\mathtt{D}, \mathtt{G})$ is a $[q(q^2-q+1), \frac{q^2-q}{2}+2, (q-1)(q^2-q+1)]_{q^2}$-linear code.

$n = (q^3+1) - (q^2-q+1) = q^3 - q^2 + q = q(q^2-q+1)$.
$k = deg(\mathtt{G}) - \mathfrak{g} + 1 = q^2 - q + 1 - \frac{q^2-q}{2} + 1 = \frac{q^2-q}{2} + 2$.

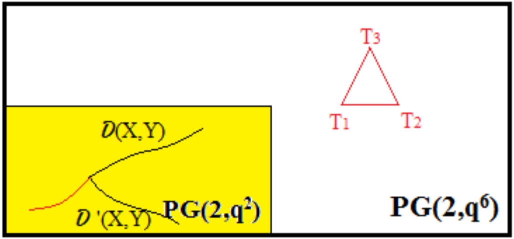
The new codes

The minimum distance of $C_L(\mathtt{D}, \mathtt{G})$

$$\delta = n - deg(\mathtt{G}) = q(q^2 - q + 1) - (q^2 - q + 1) = (q - 1)(q^2 - q + 1).$$

Construction

Take the codeword given by a further Hermitian curve $\mathcal{D}'(X, Y)$, intersecting $\mathcal{D}(X, Y)$ at $q^2 - q + 1$ points, while $q(q^2 - q + 1) - (q^2 - q + 1) = \delta$.



The new codes

The differential code $C_\Omega(\mathtt{D}, \mathtt{G})$

Result

There exists a canonical divisor $\mathtt{W}$ *such that* $C_\Omega(\mathtt{D}, \mathtt{G}) \cong C_L(\mathtt{D}, \mathtt{W} + \mathtt{D} - \mathtt{G})$.

$$\mathtt{W} = \frac{F^2}{L} dx$$

$\mathcal{C}$ is another Hermitian curve F_q of equation $F(x, y) = 0$ through the support of $\mathtt{G}$, and L is the product of $q^2 - q$ lines through an external point R to H_q together with the polar line of R.

$$\mathtt{W} + \mathtt{D} - \mathtt{G} \equiv (q^3 - q^2 - 5q - 3) Y_\infty + 2q\mathtt{T}$$

where $\mathtt{T} = T_1 + T_2 + T_3$, the common points of H_q and F_q in $PG(2, q^6)$. Since $\mathtt{D} + q\mathtt{T} \equiv (q+1)^2 Y_\infty$, this can also be written as

$$(q^2 - 1)(q + 1) Y_\infty - 2\mathtt{D}.$$

The new codes

The differential code $C_\Omega(\mathtt{D}, \mathtt{G})$

Theorem

The code $C_\Omega(\mathtt{D}, \mathtt{G})$ is a $[q(q^2-q+1), q^3-\frac{3}{2}q^2+\frac{3}{2}q-2, \frac{1}{2}(q^2-q+4)]_{q^2}$-linear code.

$k = deg(\mathtt{W}+\mathtt{D}-\mathtt{G}) - \mathfrak{g}(H_q) + 1 = q^3 - \frac{3}{2}q^2 + \frac{3}{2}q - 2.$
$\delta = q(q^2-q+1) - deg(\mathtt{W}+\mathtt{D}-\mathtt{G}) = 3.$
The minimum distance is $d = \frac{1}{2}(q^2-q+4) > 3$.

The new codes

The minimum distance of $C_\Omega(\mathtt{D}, \mathtt{G})$

Construction

Take a chord ℓ of D not passing through Y_∞
Λ is the orbit of ℓ under the action of the Singer cycle and consists of $q^2 - q + 1$ pairwise distinct chords of D not through Y_∞.
Λ together with a further curve C of degree $q - 2$ define a reducible curve L of degree $q^2 - 1$.

$$\mathrm{div}_0(\mathtt{L}) - 2\mathtt{D} = \mathtt{A}_1 + \mathtt{A}_2$$

where $\mathtt{A}_1 = A_1 + \ldots + A_N$ with $N = (q-1)(q^2 - q + 1)$ and $\mathtt{A}_2$ is the intersection divisor $H_q \circ C$.

$$\deg(\mathtt{A}_1) + \deg(\mathtt{A}_2) = q^3 - 2q^2 + 2q - 1 + \frac{1}{2}(q^2 - q - 2).$$

Therefore, the weight of the codeword $\mathtt{A}_1 + \mathtt{A}_2$ equals $d = \frac{1}{2}(q^2 - q + 4)$.


Sorry,
WE´RE
CLOSED