New Class of Quasi-cyclic Goppa Codes

Sergey Bezzateev and Natalia Shekhunova

bsv@aanet.ru sna@delfa.net

Saint Petersburg University of Aerospace Instrumentation

Russia

Algebraic and Combinatorial Coding Theory
7-13 September, 2014
Svetlogorsk, Russia

Outline

- Definitions and previous known results.
    - Cyclic separable Goppa codes
    - Quasi-cyclic separable Goppa codes
- Generalized Goppa codes.
- Cyclicity of generalized Goppa codes
- Parameters
- Examples.

Goppa codes of length n are determined by two objects:

- Goppa polynomial $G(x)$ of degree t with coefficients from field $GF(q^m)$,
- set $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, where $\alpha_i \neq \alpha_j$, $G(\alpha_i) \neq 0, \alpha_i \in GF(q^m)$.

The Goppa code consists of all q-ary vectors **a** $= (a_1 a_2 \ldots a_n)$ such that

$$\sum_{i=1}^{n} a_i \frac{1}{x - \alpha_i} \equiv 0 \mod G(x) .$$

The Goppa code is called **separable** if the Goppa polynomial G(x) is a **separable** polynomial.

Cyclicity

Cyclic code **C**

$$\boldsymbol{c} \in \mathbf{C}, \boldsymbol{c} = (c_1 c_2 \dots c_n),\ c_i \in GF(q)$$
$$\sigma(\boldsymbol{c}) = (c_n c_1 \dots c_{n-1}),\ \sigma(\boldsymbol{c}) \in \mathbf{C}.$$

Quasi-cyclic code **C**

$$\boldsymbol{c} \in \mathbf{C}, \boldsymbol{c} = (c_1 c_2 \dots c_n),\ c_i \in GF(q)$$
$$\sigma^s(\boldsymbol{c}) = (c_{n-s} c_{n-s+1} \dots c_{n-s-1}),\ \sigma^s(\boldsymbol{c}) \in \mathbf{C}.$$

Theorem (V.D.Goppa, 1970)

If $n = q^m - 1, L = GF(q^m) \setminus \{0\}$ *and such separable Goppa code is cyclic then* $G(x) = x$.

Theorem (S. Bezzateev and N.Shekhunova, 2013)

- *If* $n_1 = q^m + 1, L = \{1, \alpha, \alpha^2, \ldots.\alpha^{n-1}\}, \alpha \in GF(q^{2m}), \alpha^{q^m+1} = 1$ *and* $G(x) = x^2 + rx + 1, r \in GF(q^m) \setminus \{0\}$ *then we have separable reversible cyclic Goppa code.*
- *If* $n_2 = q^m - 1, L = \{1, \alpha, \alpha^2, \ldots.\alpha^{n-1}\} \setminus \{\alpha^j, \alpha^{jq^m}\}, 1 < j < q^m, \alpha \in GF(q^{2m}), \alpha^{q^m+1} = 1$ *and* $G(x) = x^2 + rx + 1, r = \alpha^j + \alpha^{jq^m} \in GF(q^m) \setminus \{0\}$ *then we have separable reversible cyclic Goppa code.*

Out of scope: Cyclic codes from separable Goppa codes with $\deg G(x) = 2$

- **Cyclic extended separable Goppa codes (E.R.Berlekamp and O.Moreno (1973))**

$$H_E = \begin{bmatrix} H_{(L,G)} & 0 \\ 1 \dots 1 & 1 \end{bmatrix}$$

- **Cyclic parity-check subcodes of Goppa codes (T.P.Berger (1999))**

$$H_{PC} = \begin{bmatrix} H_{(L,G)} \\ 1 \dots 1 \end{bmatrix}.$$

IS IT EXISTS CYCLIC SEPARABLE GOPPA CODES
WITH GOPPA POLYNOMIAL OF DEGREE GREATER THAN TWO?

Transformations

- $T(x) = ax + b, a, b \in GF(q^m)$,
- $T(x) = \frac{x^{q^l}+b}{cx^{q^l}+d}, 0 \le l < m, b, c, d \in GF(q^m)$.

If $L \subseteqq GF(q^m), T(L) = L$,
and $G(T(x)) = eG(x), e \in GF(q^m),\ G(x)-$ separable polynomial
then we have quasi-cyclic separable Goppa code.
Classes of quasi-cyclic separable Goppa codes are obtained and discussed by:
O.Moreno, K.Tzeng, K.Zimmermann, E.Bombieri, F.Blancheth, T.Berger, A.Vishnevetskiy, H.Stichtenoth, S.Bezzateev, N.Shekhunova, ...

Definition (N.Shekhunova and E.Mironchikov (1981))

Generalized (L, G)-code with a set L of code position numerators

$$L = \{u_1(x), u_2(x), \ldots, u_n(x)\}, \quad \text{where } u_i(x) \in \mathbb{F}_{q^m}[x],$$
$$\text{and } \deg u_i(x) \leq \tau, \ \gcd(u_i(x), u_j(x)) = 1, \forall i \neq j, \ i, j = [1, \ldots, n]$$

and Goppa polynomial $G(x)$:

$$G(x) \in \mathbb{F}_{q^m}[x] \text{ and } \gcd(G(x), u_i(x)) = 1, \forall i = [1, \ldots, n]$$

is defined by a set of all vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ satisfying the following relation:

$$\sum_{i=1}^{n} a_i \frac{u_i'(x)}{u_i(x)} \equiv 0 \mod G(x),$$

where $u_i'(x)$ is a formal derivative of polynomial $u_i(x)$.

Estimations of redundancy r and the minimum distance d of generalized (L, G)- codes are defined by the following relations :

$$r \leq m \deg G(x), \ d \geq \frac{\deg G(x) + 1}{\tau}.$$

Two approaches to locator set L

as a polynomials from $F_{q^m}[x]$	as an elements of $GF(q^m)$
$\Gamma = \{g(x) \in F_{q^m}[x], \deg g(x) \le \tau\}$, $g(x)$ – irreducible polynomial	$\Lambda = GF(q^m)$
$\tau = 1$, $L = \Gamma \setminus G(x), \deg G(x) = 1.$ Hamming code	$L \subset \Lambda, L = GF(q^l) \subset GF(q^m)$, $l\tau = m$, $G(x) = F_{q^l}[x], \deg G(x) = \tau$, $G(x)$ – irreducible polynomial. Classical irreducible Goppa code
$\tau > 1$, $L = \{g(x) : g(x) \in \Gamma$, $\deg g(x) = 1\} \subset \Gamma$, $G(x) \subset \Gamma,\ \deg G(x) = \tau.$ Classical irreducible Goppa code	$L = \Lambda \setminus \{\alpha_i : G(\alpha_i) = 0$, $\alpha_i \in \Lambda, i = 1, \ldots, \tau\}$, $\tau = \deg G(x)\}.$ Classical reducible Goppa code
$\tau > 1$, $L = \Gamma \setminus G(x),\ \deg G(x) = \tau$, Generalized Goppa code perfect in the weighted Hamming metric	$L = \Lambda \setminus \{\alpha_i : G(\alpha_i) = 0$, $\alpha_i \in \Lambda, i = 1, \ldots, \tau\}$, $\deg G(x) = \tau,\ u_j(x) = \prod_{i=1}^{\eta}(x - \alpha_{j_i})$, $\alpha_{j_i} \in L$ Generalized Goppa code with a set of code position numerators L of the maximum size of degree η

Definition

The generalized (L, G)- code with a set of code position numerators L containing elements of degrees not exceeding τ and Goppa polynomial $G(x)$ satisfying the following equality :

$$G(x)\prod_{i=1}^{n} u_i(x) = x^{q^{\tau m}} - x$$

is called Goppa code with a set of code position numerators L of the maximum size of degree τ or a set L of maximum size.

Cyclic and quasi-cyclic Goppa code with a set of code position numerators L of the maximum size of degree $\tau = 1$

1. Cyclic code $G(x) = x, L = GF(q^m) \setminus \{0\}$;
2. Quasi-cyclic code $G(x) = x^{q^m} - x, L = GF(q^{2m}) \setminus GF(q^m)$.

Proposition

Generalized separable (L,G)-code with the set L of the maximum size of the second degree and the Goppa polynomial

$$G(x) = \prod_{\alpha_i \in GF(q^m)} (x - \alpha_i) = x^{q^m} - x$$

is a quasi-cyclic code.

This code is defined as a set of all vectors $\boldsymbol{a} = (a_1, a_2, \dots, a_n)$ of the length $n = I_{q^m}(2)$ satisfying the relation

$$\sum_{i=1}^{n} a_i \frac{u_i'(x)}{u_i(x)} \equiv 0 \mod G(x),$$

where $u_i(x)$ are all unitary (i.e.,the greatest coefficient is equal to 1) irreducible polynomials of degree 2 over $GF(q^m)$.
$I_{q^m}(2)$ is a number of unitary polynomials of degree 2 irreducible over $GF(q^m)$.

Lemma

The redundancy r of the separable (L,G)- code defined by equalities

$$G(x) = \prod_{\alpha_i \in GF(q^m)} (x-\alpha_i) = x^{q^m} - x$$

and

$$\sum_{i=1}^{n} a_i \frac{u_i'(x)}{u_i(x)} \equiv 0 \mod G(x)\,,$$

with the set L of the maximum size of the second degree satisfies the following relation:

$$r \le m(\deg G(x) - 2) + 1 = m(q^m - 2) + 1.$$

Minimal distance

Theorem

The minimum distance d of this (L, G)- code is defined by the following relation

$$(d-1)2+1 \geq \deg G(x) + 2.$$

This relation can be rewritten as

$$d \geq \frac{\deg G(x)+1}{2} + 1 = \frac{q^m+1}{2} + 1.$$

Theorem

The minimum distance d of the binary generalized separable (L, G)- code with the set L of the maximum size of the second degree satisfies the following relation:

$$(d-1)2+0 \geq 2\deg G(x)+2.$$

The inequality can be rewritten as:

$$d \geq \deg G(x)+1+1=\deg G(x)+2.$$

Moreover, all words of this binary code have even weights.

1. cycloid length $q^{\ell} - 1$,
2. $G(x) = x^{q^{\ell}} - x$,
3. $u_i(x) \in F_{q^{\ell}}[x],\ deg u_i(x) = \tau,\ d \geq \frac{q^{\ell}+1}{\tau},\ n = I_{q^{\ell}}(\tau),\ k \geq n - \ell\tau.$

Example

The binary generalized separable (L, G)- code with the Goppa polynomial $G(x) = x^8 - x$ and the set L of maximum size including all irreducible polynomials of the second degree from $F_{2^3}[x]$ is a quasi-cyclic code of the cycloid length 7 and with parameters

$$n = 28, k = 9, d = 10.$$

This is the optimal binary linear code and it is considered to be a new quasi-cyclic $(28, 9, 10)$- code.

THANK YOU !