OPTIMAL QUASI-CYCLIC GOPPA CODES

Sergey Bezzateev and Natalia Shekhunova

bsv@aanet.ru sna@delfa.net

Saint Petersburg State University of Aerospace Instrumentation

Russia

Optimal Codes and Related Topics
September 6-12, 2013
Albena, Bulgaria

Outline

- Definitions
- Overview of previous results on cyclicity of Goppa codes
- Two transformations
- Known solutions for a linear transformation
- Known solutions for a bilinear transformation
- Solution for the bilinear transformation (main result)
- Parameters of new subclass of quasi-cyclic Goppa codes (main result)
- Examples

Goppa codes of length n are determined by two objects:

- Goppa polynomial $G(x) = \prod_{i=1}^{t}(x - \beta_i)$ of degree t with coefficients from the field $GF(q^m)$,

Definition

Goppa code is called as a separable code if a Goppa polynomial $G(x)$ has no multiple roots.

- a set $L = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq GF(q^m)$, $\beta_i \notin L, i = 1, \dots, t$.

The Goppa code consists of all q-ary vectors $\mathbf{a} = (a_1 a_2 \dots a_n)$ such that

$$\boldsymbol{a}H^T = \mathbf{0}, H = \begin{bmatrix} \frac{1}{\alpha_1 - \beta_1} & \cdots & \frac{1}{\alpha_i - \beta_1} & \cdots & \frac{1}{\alpha_n - \beta_1} \\ \frac{1}{\alpha_1 - \beta_2} & \cdots & \frac{1}{\alpha_i - \beta_2} & \cdots & \frac{1}{\alpha_n - \beta_2} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_1 - \beta_t} & \cdots & \frac{1}{\alpha_i - \beta_t} & \cdots & \frac{1}{\alpha_n - \beta_t} \end{bmatrix}.$$

[K.K.Tzeng, K.Zimmermann, "On Extending Goppa Codes to Cyclic Codes", *IEEE Trans. Inform. Theory*, v. 21, n. 6, p. 712-716, 1975.]

f is a permutation on L such that

$$\alpha_{((i+1) \mod l)+jl+1} = f(\alpha_{i+jl+1}), l \mid n, i = 0, \ldots, l-1, j = 0, \ldots \frac{n}{l} - 1.$$

$$H = \begin{bmatrix} \frac{1}{f(\alpha_1)-\beta_1} & \cdots & \frac{1}{f(\alpha_i)-\beta_1} & \cdots & \frac{1}{f(\alpha_n)-\beta_1} \\ \frac{1}{f(\alpha_1)-\beta_2} & \cdots & \frac{1}{f(\alpha_i)-\beta_2} & \cdots & \frac{1}{f(\alpha_n)-\beta_2} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{1}{f(\alpha_1)-\beta_t} & \cdots & \frac{1}{f(\alpha_i)-\beta_t} & \cdots & \frac{1}{f(\alpha_n)-\beta_t} \end{bmatrix} = \begin{bmatrix} \frac{1}{\alpha_1-\varphi(\beta_1)} & \cdots & \frac{1}{\alpha_i-\varphi(\beta_1)} & \cdots & \frac{1}{\alpha_n-\varphi(\beta_1)} \\ \frac{1}{\alpha_1-\varphi(\beta_2)} & \cdots & \frac{1}{\alpha_i-\varphi(\beta_2)} & \cdots & \frac{1}{\alpha_n-\varphi(\beta_2)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_1-\varphi(\beta_t)} & \cdots & \frac{1}{\alpha_i-\varphi(\beta_t)} & \cdots & \frac{1}{\alpha_n-\varphi(\beta_t)} \end{bmatrix},$$

where φ determine some permutation on $\{\beta_1, \ldots, \beta_t\}$.

Definition (Linear transformation)

Linear transformation $f_1(x) = ax + 1, a \in GF(q^m), a \neq 0,$

$$\alpha \to a\alpha + 1, \alpha \in GF(q^m).$$

In general case $f_1(x) = ax^{q^l} + 1, l < m$

Definition (Bilinear transformation)

Bilinear transformation $f_2(x) = \frac{ax+b}{x+d}$, $a, b, d \in GF(q^m), ab - d \neq 0,$

$$\alpha \to \frac{a\alpha + b}{\alpha + d}, \alpha \in GF(q^m) \bigcup \{\infty\}.$$

In general case $f_2(x) = \frac{ax^{q^l}+b}{x^{q^l}+d}, l < m$

Known solutions for a linear transformation

$$\frac{1}{\alpha_i-\beta_j} \to \quad \frac{1}{f_1(\alpha_i)-\beta_j} = \frac{1}{a\alpha_i^{q^l}+1-\beta_j} = \left(\frac{a^{q^{-l}}}{\alpha_i-((\beta_j-1)/a)^{q^{-l}}}\right)^{q^l} = \left(\frac{a^{q^{-l}}}{\alpha_i-\varphi(\beta_j)}\right)^{q^l},$$

where $\varphi(x) = \left(\frac{x-1}{a}\right)^{q^{-l}}$.

Only quasi-cyclic separable Goppa codes exists

Theorem (V.D. Goppa, The new class of linear error-correction codes, *Probl. Inform. Transm*, v.6, no.3, 1970, pp.24–30.)

If a code satisfying with the condition

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

is a cyclic code, it is BCH-code and $G(x) = x^t$.

1.S.V. Bezzateev , N. A. Shekhunova, Quasi-cyclic Goppa codes, *Proceedings of ISIT*, 1994, p. 499.

2. T.P.Berger, Goppa and Related Codes Invariant Under a Prescribed Permutation, *IEEE Trans. Inform. Theory*, 2000, v. 46, n.7, pp.2628-2633.

3.G.Bommier, F. Blanchet, Binary Quasi-Cyclic Goppa Codes, *Designs, Codes and Cryptography*, 20, 2000, pp. 107–124.

$$\frac{1}{\alpha_i-\beta_j} \to \frac{1}{f_1(\alpha_i)-\beta_j} = \frac{1}{\frac{a\alpha_i^{q^l}+b}{\alpha_i^{q^l}+d}-\beta_j} = A\left(\frac{1}{\alpha_i-\left(\frac{d\beta_j-b}{\beta_j-a}\right)^{q^{-l}}}\right)^{q^l}$$

$$+B\left(\frac{\alpha_i}{\alpha_i-\left(\frac{d\beta_j-b}{\beta_j-a}\right)^{q^{-l}}}\right)^{q^l} = A\left(\frac{1}{\alpha_i-\varphi(\beta_j)}\right)^{q^l} + B\left(\frac{\alpha_i}{\alpha_i-\varphi(\beta_j)}\right)^{q^l},$$

where $\varphi(x) = \left(\frac{dx-b}{x-a}\right)^{q^{-l}}$.

Lemma (Generalization of Lemma from F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, 1976)

Let a transformation

$$f_2(x) = \frac{ax^{q^l}+b}{x^{q^l}+d}, a, b, d \in GF(2^m),\ ad-b \neq 0$$

sets automorphism on the set $L \subseteq GF(2^m)\bigcup\{\infty\}$.
A Goppa code be a quasi-cyclic code iff for any codeword $\boldsymbol{a} = (a_1 a_2 \ldots a_n)$ *of this code* $\sum_{i=1}^{n} a_i = 0$.

Extension of Goppa code by addition common parity check

Extended quasi-cyclic Goppa codes

$$H_E = \begin{bmatrix} H_{(L,G)} & 0 \\ 1 \dots 1 & 1 \end{bmatrix} \begin{cases} \sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} + a_\infty \frac{1}{x-\infty} \equiv 0 \mod G(x) \\ a_1 + a_2 + \dots + a_\infty = 0 \end{cases}$$

Quasi-cyclic subcode of the Goppa code with the parity-check matrix H_{PC}

Expurgated quasi-cyclic Goppa codes

$$H_{PC} = \begin{bmatrix} H_{(L,G)} \\ 1 \dots 1 \end{bmatrix} \begin{cases} \sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \equiv 0 \mod G(x) \\ a_1 + a_2 + \dots a_n = 0 \end{cases}$$

1. T.P.Berger, Goppa and Related Codes Invariant Under a Prescribed Permutation, *IEEE Trans. Inform. Theory*, 2000, v. 46, n.7, p.2628-2633.
2. T.P.Berger, On the Cyclicity of Goppa Codes, Parity-Check Subcodes of Goppa Codes, and Extended Goppa Codes, *Finite Fields and Their Applications*, 6, 2000, p.255-281.
3. H. Stichtenoth, Which extended Goppa codes are cyclic?, *J. Comb. Theory*, vol. A 51, pp. 205–220, 1989.

We should find such the set L and the polynomial $G(x)$ that the Goppa code will be the code with all codewords $\boldsymbol{a} = (a_1 a_2 \dots a_n)$ such that $\sum_{i=1}^{n} a_i = 0$ without adding of further lines or columns in it parity-check matrix.

Theorem (Theorem about code from S.Bezzateev, N.Shekhunova, Chain of Separable Binary Goppa Codes and Their Minimal Distance, *IEEE Trans. Inform. Theory.*, **54**, 12, 5773–5778, 2008.)

All codewords $\boldsymbol{a} = (a_1 a_2 \dots a_n)$ *of the Goppa code with* $L \subseteq GF(q^{2m})$ *and* $G(x)$:

$$\forall \alpha \in L,\ G(\alpha)^{q^m} = A\alpha^{-t} G(\alpha), A \in GF(q^{2m}), t = \deg G(x)$$

satisfy the equation:

$$\sum_{i=1}^{n} a_i = 0.$$

Theorem (For case $l = 0$, $f_2(x) = \frac{ax+b}{x+d}$, S. Bezzateev ,N. Shekhunova, Cyclic separable Goppa codes, ACCT-13, June 15-21, 2012, Pomorie, Bulgaria pp. 88-92)

Goppa code with

$$G(x) = x^2 + Ax + 1, A \in GF(q^m)$$

and

$$L \subseteq M = \{\alpha_i : \alpha_i^{q^m+1} = 1, \alpha_i \in GF(q^{2m}), i = 1, \ldots, n\}$$

is $(n, n - 2m - 1, d \geq 6)$ *cyclic reversible code.*

$f_2(x) = -\frac{ax+1}{x+a^{q^m}}, a \in GF(q^{2m}) \setminus GF(q^m), A = a + a^{q^m}$

Theorem

The permutation given by the function

$$f_2(x) = \frac{ax^{q^l} + b}{x^{q^l} + d}, \ a, b, d \in GF(q^{2m}), ad - b \neq 0, 0 \leq l < m$$

is automorphism mapping on the set M *if and only if*

$$b = 1, \ d = a^{q^m}.$$

Lemma

All roots of the polynomial

$$G(x) = x^{q^l+1} - ax^{q^l} + a^{q^m}x - 1 \quad (1)$$

are fixed with respect to the permutation $f_2(x)$ *defined in Theorem above.*

It is easy to show that $G(x)$ is a separable polynomial.

Let us choose a location set

$$L = M \setminus \{\alpha : G(\alpha) = 0\}. \tag{2}$$

Then the Goppa codes with the such set L and with the Goppa polynomial

$$G(x) = x^{q^l+1} - ax^{q^l} + a^{q^m}x - 1 \text{ or}$$

$$G(x) = x + \beta, \beta \in M \tag{3}$$

satisfy the condition of the **Theorem about code** and therefore $\sum_{i=1}^{n} a_i = 0$ for all words $\boldsymbol{a} = (a_1 a_2 \dots a_n)$ of such codes.

Theorem

The Goppa codes given by set

$$L = M \setminus \{\alpha : G(\alpha) = 0\}$$

and polynomials

$$G(x) = x^{q^l+1} - ax^{q^l} + a^{q^m}x - 1 \text{ or } G(x) = x + \beta$$

have:

- *the minimum distance* $d \geq t + 2, t = \deg G(x)$ *(for* $q = 2$, $d \geq 2t + 2$*),*
- *and dimension* $k \geq n - mt - 1$.

Let us choose a subset $\widehat{L}$ as a set of numerators of codeword positions:

$$\widehat{L} \subseteq L,\ \widehat{L} = \{L_1, L_2, \ldots, L_r\},\ \forall i,\ L_i = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_\mu}\},$$
$$\alpha_{i_{j+1}} = \frac{a\alpha_{i_j}^{q^l}+1}{\alpha_{i_j}^{q^l}+a^{q^m}},\ \forall j, \alpha_{i_j} \in M,\ a \in GF(q^{2m}) \setminus GF(q^m), r\mu = n.$$

and the Goppa polynomial $\widehat{G}(x)$:

$$\widehat{G}(x)|G(x),\ G(x) = x^{q^l+1} - ax^{q^l} + a^{q^m}x + 1,\ \widehat{G}(\alpha)^{q^m} = A\alpha^{-\tau}\widehat{G}(\alpha),$$
$$A \in GF(q^{2m}), \alpha \in L, \tau = \deg \widehat{G}(x).$$

The code with such $\widehat{G}(x)$ and $\widehat{L}$ have for all codewords $\sum_{i=1}^{n} a_i = 0$.

Theorem

The Goppa code is a quasi-cyclic code with the cycloid length μ, minimum distance

$$d \geq degG(x) + 2$$

and dimension

$$k \geq n - m \cdot \deg G(x) - 1, \; n = r\mu.$$

It is obvious that if $G(x)$ is decomposed over $GF(q^{2m})$:

$$G(x) = \prod_{i=1}^{\tau} \widehat{G}_i(x)$$

and if every polynomial $\widehat{G}_i(x)$ satisfies the conditions of **Theorem about code** , then we obtain a set of embedded quasi-cyclic Goppa codes.
For example, if all roots of polynomial $G(x)$ belong to the set M, i.e.

$$G(x) = \prod_{i=1}^{t}(x + \beta_i), \beta_i \in M, t = \deg G(x),$$

then the polynomials $x + \beta_i$ can be chosen as $\widehat{G}_i(x)$.

$$M = \left\{ \alpha^{31i}, i = 0, \ldots, 32 \right\} \subset GF(2^{10}),$$

$$f_2(x) = \frac{\alpha^{29}x^2 + 1}{x^2 + (\alpha^{29})^{32}} = \frac{\alpha^{29}x^2 + 1}{x^2 + \alpha^{928}},$$

The roots of a polynomial

$$x^3 + \alpha^{29}x^2 + \alpha^{928}x + 1 = (x + \alpha^{310}) \cdot (x + \alpha^{806}) \cdot (x + \alpha^{930}),$$

where $\alpha^{310}, \alpha^{806}, \alpha^{930} \in M$, are fixed points for this transformation.

$$L = M \setminus \{\alpha^{310}, \alpha^{806}, \alpha^{930}\} = \{L_1, L_2, L_3, L_4, L_5, L_6\},$$

where L_i is the $i-$th cycloid that is an orbit of the permutation $f(x)$:

$$\begin{aligned}
L_1 &= \left\{1, \alpha^{527}, \alpha^{279}, \alpha^{496}, \alpha^{248}\right\}, \\
L_2 &= \left\{\alpha^{31}, \alpha^{217}, \alpha^{775}, \alpha^{465}, \alpha^{899}\right\}, \\
L_3 &= \left\{\alpha^{62}, \alpha^{93}, \alpha^{744}, \alpha^{372}, \alpha^{992}\right\}, \\
L_4 &= \left\{\alpha^{124}, \alpha^{589}, \alpha^{155}, \alpha^{341}, \alpha^{713}\right\}, \\
L_5 &= \left\{\alpha^{186}, \alpha^{682}, \alpha^{651}, \alpha^{837}, \alpha^{558}\right\}, \\
L_6 &= \left\{\alpha^{403}, \alpha^{961}, \alpha^{620}, \alpha^{434}, \alpha^{868}\right\}.
\end{aligned}$$

New Optimal $(30, 14, 8)$ Quasi-cyclic Goppa Code

$G(x) = x^3 + \alpha^{29}x^2 + \alpha^{928}x + 1 = (x + \alpha^{310}) \cdot (x + \alpha^{806}) \cdot (x + \alpha^{930})$
we obtain quasi-cyclic $(30, 14, 8)$-code with the weight distribution

$$< 0, 1 >, < 8, 225 >, < 10, 840 >, < 12, 2800 >, < 14, 4200 >,$$
$$< 16, 4635 >, < 18, 2520 >, < 20, 1008 >, < 22, 120 >, < 24, 35 > .$$

This is a new optimal quasi-cyclic code with the length of cycloid $\mu = 5$
[Z.Chen, A Database on Binary Quasi-Cyclic Codes,
http://moodle.tec.hkr.se/ chen/research/codes/qc.htm]

$$\begin{aligned} G_1(x) = & \quad x^2 + \alpha^{307}x + \alpha^{713} & = (x + \alpha^{806}) \cdot (x + \alpha^{930}), \\ G_2(x) = & \quad x^2 + \alpha^{360}x + \alpha^{93} & = (x + \alpha^{310}) \cdot (x + \alpha^{806}), \\ G_3(x) = & \quad x^2 + \alpha^{455}x + \alpha^{217} & = (x + \alpha^{310}) \cdot (x + \alpha^{930}) \end{aligned}$$

new equivalent optimal quasi-cyclic $(30, 19, 6)$-codes with weight distribution

$$< 0, 1 >, < 6, 675 >, < 8, 5635 >, < 10, 29127 >, < 12, 85120 >, < 14, 141270 >, \\ < 16, 142335 >, < 18, 84630 >, < 20, 29040 >, < 22, 5895 >, < 24, 525 >, \\ < 26, 35 >$$

and the length of cycloid $\mu = 5$.

$$\begin{aligned} G_{11}(x) = G_{22}(x) = & \quad x + \alpha^{806}, \\ G_{12}(x) = G_{32}(x) = & \quad x + \alpha^{930}, \\ G_{21}(x) = G_{31}(x) = & \quad x + \alpha^{310} \end{aligned}$$

new equivalent optimal quasi-cyclic $(30, 24, 4)$- codes with the weight distribution

$$< 0, 1 >, < 4, 945 >, < 6, 18200 >, < 8, 183885 >, < 10, 936936 >, \\ < 12, 2705885 >, < 14, 4541040 >, < 16, 4547475 >, < 18, 2700880 >, \\ < 20, 939939 >, < 22, 182520 >, < 24, 18655 >, < 26, 840 >, < 28, 15 >$$

and the length of cycloid $\mu = 5$.

$$M = \left\{ \alpha^{63i}, i = 0, \ldots, 65 \right\},$$

where α is a primitive element in $GF(2^{12})$.
Transformation $f_2(x) = \frac{\alpha x^2+1}{x^2+\alpha^{64}}$, $L \subset M$ and $G(x) = x^3 + \alpha x^2 + \alpha^{64} x + 1$.
new optimal $(54, 35, 8)$ quasi-cyclic Goppa code with the length of cycloid $\mu = 9$ and weight distribution

$$< 0, 1 >, < 8, 4185 >, < 10, 92394 >, < 12, 1303146 >, < 14, 12386925 >,$$
$$< 16, 80476578 >, < 18, 369718008 >, < 20, 1226018808 >,$$
$$< 22, 2977435773 >, < 24, 5350668570 >, < 26, 7161764796 >,$$
$$< 28, 7161764796 >, < 30, 5350668570 >, < 32, 2977435773 >,$$
$$< 34, 1226018808 >, < 36, 369718008 >, < 38, 80476578 >,$$
$$< 40, 12386925 >, < 42, 1303146 >, < 44, 92394 >, < 46, 4185 >, < 54, 1 >$$

By using transformation $f_2(x) = \frac{\alpha^3 x^2 + 1}{x^2 + \alpha^{192}}, L \subset M$ and $G(x) = x^3 + \alpha^3 x^2 + \alpha^{192} x + 1$ we obtain another new optimal $(54, 35, 8)$ quasi-cyclic Goppa code with the length of cycloid $\mu = 9$ and weight distribution

$$< 0, 1 >, < 8, 4491 >, < 10, 89568 >, < 12, 1314402 >, < 14, 12361248 >,$$
$$< 16, 80518176 >, < 18, 369647168 >, < 20, 1226164536 >,$$
$$< 22, 2977190208 >, < 24, 5350912302 >, < 26, 7161712128 >,$$
$$< 28, 7161582636 >, < 30, 5350876032 >, < 32, 2977434585 >,$$
$$< 34, 1225819584 >, < 36, 369939320 >, < 38, 80351424 >,$$
$$< 40, 12427911 >, < 42, 1294368 >, < 44, 94914 >, < 46, 3168 >, < 48, 198 >$$

New Optimal $(60, 41, 8)$ Quasi-cyclic Goppa Code

Transformation $f(x) = \frac{\alpha^5 x^2 + 1}{x^2 + \alpha^{320}}$, $L \subset M$ and $G(x) = x^3 + \alpha^5 x^2 + \alpha^{320} x + 1$.
We obtain another new optimal $(60, 41, 8)$ quasi-cyclic Goppa code with the length of cycloid $\mu = 12$ and weight distribution

$$< 0, 1 >, < 8, 10878 >, < 10, 284640 >, < 12, 5346029 >, < 14, 66136896 >,$$
$$< 16, 570819819 >, < 18, 3528475232 >, < 20, 15990913998 >, < 22, 53994120960 >$$
$$< 24, 137528849492 >, < 26, 266594862528 >, < 28, 395659873671 >,$$
$$< 30, 451143867264 >, < 32, 395659873671 >, < 34, 266594862528 >,$$
$$< 36, 137528849492 >, < 38, 53994120960 >, < 40, 15990913998 >,$$
$$< 42, 3528475232 >, < 44, 570819819 >, < 46, 66136896 >,$$
$$< 48, 5346029 >, < 50, 284640 >, < 52, 10878 >, < 60, 1 >$$

THANK YOU FOR YOUR ATTENTION!