CYCLIC SEPARABLE GOPPA CODES

Sergey Bezzateev and Natalia Shekhunova

bsv@aanet.ru sna@delfa.net

Saint Petersburg State University of Aerospace Instrumentation

Russia

Algebraic and Combinatorial Coding Theory
June 15-21, 2012
Pomorie, Bulgaria

Outline

- Overview of previous results on cyclicity of Goppa codes
- Two problems
- Known solutions for the problem 1
- Solution for the problem 2 (main result)
- Sufficient conditions for Goppa code cyclicity
- Examples
- Conclusion

Goppa codes of length n are determined by two objects:

- Goppa polynomial $G(x)$ of degree t with coefficients from the field $GF(q^m)$,
- a set $L = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, 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** $= (a_1 a_2 \dots a_n)$ such that

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

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 $G(x) = x^t$.

Definition

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

Definition

The polynomial $G(x)$ with the coefficients from $GF(2^m)$ is called irreducible polynomial if it has no roots in the field $GF(2^m)$.

Lemma

Any separable polynomial $G(x), \deg G(x) = 2$ with the coefficients from the field $GF(2^m)$ can be presented in the form
$G(x) = x^2 + Ax + 1$, *where* $A \in GF(2^m)$.

Definition

Linear transformation $\theta(x) = ax + b$

$$\alpha \to a\alpha + b, a, b \in GF(2^m), a \neq 0, \alpha \in GF(2^m).$$

Definition

Bilinear transformation $\theta(x) = \frac{ax+b}{cx+d}$

$$\alpha \to \frac{a\alpha + b}{c\alpha + d}, a, b, c, d \in GF(2^m), c \neq 0, ab + cd \neq 0,$$

$\alpha \in GF(2^m) \bigcup \{\infty\}$.
Inverse transformation : $\theta^{-1}(x) = \frac{dx+b}{cx+a}$

Lemma (A.L. Vishnevetskyi, On cyclicity of extended Goppa codes, *Probl. Inform. Transm*, 1982, v.18, n.3, p.14-18.)

$\theta(\prod_{\beta}(x-\beta)) \sim \prod_{\beta}(x-\theta^{-1}(\beta))$ *for any transformation* $\theta(x) = \frac{ax+b}{cx+d}, c = 1, a, b, d \in GF(2^m), ad + b \neq 0.$

Remark

Let us represent the operations determined for the element $\{\infty\}$:

- $\theta^{-1}(\infty) = \frac{d\infty+b}{\infty+a} = \frac{d+\frac{b}{\infty}}{1+\frac{a}{\infty}} = d,$
- $\frac{1}{G(\infty)} = \frac{1}{\infty^2+(a+d)\infty+b} = \frac{\frac{1}{\infty^2}}{1+\frac{a+d}{\infty}+\frac{b}{\infty^2}} = 0,$
- similarly, we can obtain $\frac{\infty}{G(\infty)} = 0$ и $\frac{\infty^2}{G(\infty)} = 1.$

Lemma [F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, 1976]
Let a transformation

$$\theta(x) = \frac{ax+b}{cx+d}, c = 1, a, b, d \in GF(2^m),\ ad+b \neq 0$$

sets automorphism on the set $L \subseteq GF(2^m) \bigcup \{\infty\}$,

$$\theta^{-1}(L) = L \text{ и } G(x) = x^2 + (a+d)x + b,$$
$$\theta(G(x)) = G(\theta(x)) = \tfrac{b+ad}{x^2+d^2} G(x),$$

$(L, G)-$ code be a cyclic code iff **the weight of every codeword is even**.

Extension of Goppa code by addition common parity check

Extended cyclic Goppa codes

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

Cyclic subcode of the $(L, G)-$ code with the parity-check matrix H_{PC}

Parity-check cyclic subcodes

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

Code parameters

$$\begin{cases} n = |GF(2^m) \bigcup \{\infty\}| = 2^m(+1) & \text{if } G(x) \text{ is irreducible over } GF(2^m), \\ n = |GF(2^m) \bigcup \{\infty\}| - 2 = 2^m - 2(+1) & \text{if } G(x) \text{ has two roots in } GF(2^m), \end{cases}$$

$$k = n - 2m - 1, \quad d \geq 6.$$

References

1. E.R. Berlecamp , O. Moreno , Extended Double-Error-Gorrecting Binary Goppa Codes Are Cyclic, *IEEE Trans. Inform. Theory*, 1973, v. 19, n. 6, p. 817-818.
2. Tzeng K. K., Zimmermann K. On Extending Goppa Codes to Cyclic Codes, *IEEE Trans. Inform. Theory*, 1975, v. 21, n. 6, p. 712-716.
3. K.K. Tzeng K. K., C.Y. Yu , Characterization Theorems for Extending Goppa Codes to Cyclic Codes, *IEEE Trans. Inform. Theory*, 1979, v. 25, № 2, p. 246-250.
4. O. Moreno, Symmetries of Binary Goppa Codes, *IEEE Trans. Inform. Theory*, 1979, v. 25, n. 5, p. 609-612.
5. A.L. Vishnevetskiy , On cyclicity of extended Goppa codes, *Probl. Inform. Transm.*, 1982, v.18, n.3, p. 14-18.
6. T.P.Berger, Goppa and Related Codes Invariant Under a Prescribed Permutation, *IEEE Trans. Inform. Theory*, 2000, v. 46, n.7, p.2628-2633.
7. 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.
8. T.P. Berger , Quasi-cyclic Goppa codes, in *Proc. ISIT2000, Sorrente, Italie*, 2000, p. 195.
9. T.P. Berger ,New Classes of Cyclic Extended Goppa Codes,*IEEE Trans. Inform. Theory*, 1999, v. 45, n.4, p.1264-1266.

1. Is it exists another extended cyclic Goppa codes ? [F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, 1976]
2. Is it exists separable cyclic Goppa codes with $L \subseteq GF(2^m)$?

Extended cyclic Goppa codes with $\deg G(x) = 2^w + 1$
[O.Moreno 1979, T.Berger 2000]

Transformation $\theta(x) = \frac{ax^{2^w}+b}{x^{2^w}+d}$,
$G(x) = x^{2^w+1} + ax^{2^w} + dx + b$,
$L \subseteq GF(2^m) \bigcup \{\infty\}$,
$k \geq n - m(2^w + 1) - 1$,
$d \geq 2^{w+1} + 4$ and all codewords should have even weight.

We should find such the set L and the polynomial $G(x)$ that (L, G)-code will be the code with all codewords of even weights without adding of further lines or columns in it parity-check matrix.

Lemma (Bezzateev S.V., Shekhunova N.A., Special classes of Goppa Codes with improved estimations of parameters , *Probl. Inform. Transm.*,2010,v.46., n.3, p. 29-50.)

(L, G)-code with Goppa polynomial $G(x) = x^{2^l-1} + 1$ and the set $L = GF(2^{2l}) \backslash GF(2^l)$ has all codewords of even weights.

Theorem

Goppa code with

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

and

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

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

The following conditions are the sufficient conditions for a cyclicity of $(n, k, d \geq 6)$ Goppa code with Goppa polynomial $G(x)$ of the degree 2 and the numerator set $L \subseteq GF(2^m)$:

1. $n < 2^m - 1, n | 2^m + 1$ or $n | 2^m - 1$,
2. $L = \{\alpha_0, \alpha_2, \ldots, \alpha_{n-1}\}, \alpha_i \in GF(2^m), \theta^{-1}(\alpha_i) = \alpha_{i+1(\mod n)}$, $\theta(x) = \frac{ax+b}{cx+d}$,
3. $G(x) = cx^2 + (a+d)x + b$ and $G(x)-$is an irreducible polynomial over the field $GF(2^m)$ or $G(\beta_1) = G(\beta_2) = 0, \beta_1 \neq \beta_2,\ \beta_1, \beta_2 \in GF(2^m),\ \theta^{-1}(\beta_1) = \beta_1,\ \theta^{-1}(\beta_2) = \beta_2$,
4. any codeword $\mathbf{a} = (a_1 a_2 \ldots a_n) \in \Gamma(L, G)$ has even weight, $wt(\mathbf{a}) \equiv 0 \mod 2$.

Let us consider the separable $\Gamma(L, G)-$ code with

$$L = \{\alpha_1, \alpha_2, \dots \alpha_n\}, \alpha_i \in GF(2^m), \alpha_i^{2^l} = \alpha_i^{-1} \text{ for all } i = 1, \dots, n,\ l < m$$

and

$$G(x) : \deg G(x) = t,\ \left(x^t\right)^{2^l} G(x^{-1})^{2^l} = AG(x^{2^l}), A \in GF(2^m).$$

Any code word **a** $= (a_1 a_2 \dots a_n)$ of the code has even weight.

$$\sum_{i=1}^{n} a_i \frac{1}{x + \alpha_i} \equiv 0 \mod G(x),\ wt(a) \equiv 0 \mod 2.$$

The following conditions are sufficients for cyclicity of separable $\Gamma(L,G)-$ code:

1. bilinear transformation $\theta(x)=\frac{ax+b}{cx+d}$ such that $(cx+d)^t\theta(G(x))=AG(x)$, $t=\deg G(x),\ a,b,c,d,A\in GF(2^m)$ and $\theta^{-1}(L)=L$,
2. $L=\{\alpha_0,\alpha_2,\dots,\alpha_{n-1}\},\alpha_i\in GF(2^m),\alpha_i^{2^l}=\alpha_i^{-1},\ l<m,\ G(\alpha_i)\neq 0,$
3. $\left(x^t\right)^{2^l}G(x^{-1})^{2^l}=AG(x^{2^l}),A\in GF(2^m).$

Reversible $(n = 2^l + 1, 2^l - 2l, 6)$ Goppa code with polynomial $G(x)$:

$$G(x) = x^2 + rx + 1, r \in GF(2^l) \setminus \{0\}$$

and with the set L:

$$L = \{1, \alpha, \alpha^2, ...\alpha^{n-1}\}, \alpha \in GF(2^{2l}), \alpha^n = 1$$

is a reversible cyclic separable Goppa code.

The following conditions for a, b, d are sufficient to obtain the $\theta-$ orbit $L \in GF(2^m)$ with the length of cycle $\zeta = |L|$:

$$\zeta \leq 2^l + 1, \zeta |\ 2^l + 1 \text{ or } \zeta |\ 2^l - 1, l < m$$

such that for any element $\alpha \in L$ the relation $\alpha^{2^l} = \alpha^{-1}$ is fulfills.

$$d = \frac{a^{2^l}}{b^{2^l}}$$

and

$$a = \alpha^i, \qquad b = \alpha^{j\eta},$$
$$\eta = 2^l - 1,$$
$$i \in \{1, 2, \dots 2^{2l} - 2\} \setminus \{2^l - 1, 2(2^l - 1), \dots, 2^l(2^l - 1)\}, \quad j \in \{0, 1, 2, \dots 2^l\},$$

α is a primitive element of $GF(2^{2l})$.
In addition, Goppa polynomial $G(x) = x^2 + (a + d)x + b$ will satisfy the following relation

$$G^{2^l}(x^{-1}) = Ax^{-2^{l+1}} G(x^{2^l}), A \in GF(2^m).$$

The transformation

$$\theta^*(x) = \frac{\frac{a}{\sqrt{b}}x+1}{x+\sqrt{b}a^{2^l}}, \quad \begin{array}{l} a = \alpha^i, i \in \{1, 2, \dots 2^{2l}-2\} \setminus \{2^l-1, 2(2^l-1), \dots, 2^l(2^l-1)\} \\ b = \alpha^{j\eta}, \eta = 2^l-1, j \in \{0, 1, \dots, 2^l\}, \\ \alpha - \text{is a primitive element of } GF(2^{2l}) \end{array}$$

define the set

$$L = \{1, \alpha_2, \dots, \alpha_n\}, \alpha_i = \frac{a\alpha_{i-1}+1}{\alpha_{i-1}+a^{2^l}}, 1 < i \le n, \ n \le 2^l+1, \ n|2^l-1 \text{ or } n|2^l+1$$

and polynomial

$$G(x) = x^2 + \left(\frac{a}{\sqrt{b}} + \sqrt{b}a^{2^l}\right)x + 1,$$

Such L and $G(x)$ defines $(n, k = n-2l-1, d \ge 6)$- separable reversible cyclic $(L, G)-$ Goppa code with even weight codewords.

E x a m p l e 1

Let us consider a separable $\Gamma_1(L, G)$ code as a cyclic $(21, 8, 6)$ -code with $G(x) = x^2 + \alpha^{714}x + \alpha^{63}, \alpha$ is a primitive element from $GF(2^{12})$,

$$L = \{\alpha^i, i = 0, 2646, 3717, 1953, 1890, 1008, 2583, 2961, 1323, 2079, 2835, 1197, 1575, 3150, 2268, 2205, 441, 1512, 63, 3906, 252\},$$

transformation $\theta(x) = \frac{\alpha^6 x + \alpha^{63}}{x + \alpha^{447}}$.

The cyclic Goppa code $\Gamma_1(L, G)$ is the cyclic code with length 21 and generator polynomial

$$g(x) = (x + 1)(x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^2 + 1).$$

E x a m p l e 2

Let us consider as example of a separable $\Gamma_2(L, G)$ reversible cyclic code $(33, 22, 6)$ with $G(x) = x^2 + \alpha^{560}x + \alpha^{31}, \alpha$ is a primitive element from $GF(2^{10})$,

$$L = \{\alpha^i, i = 0, 62, 93, 527, 961, 992, 31, 155, 682, 217, 930, 744, 341, 496, 465, 775, 403, 248, 620, 868, 186, 434, 806, 651, 279, 589, 558, 713, 310, 124, 837, 372, 899\},$$

transformation $\theta(x) = \frac{\alpha^{901} x + \alpha^{31}}{x + \alpha^{219}}$.

The cyclic Goppa code $\Gamma_2(L, G)$ is the cyclic code of length 33 and generator polynomial

$$g(x) = (x + 1)(x^{10} + x^7 + x^5 + x^3 + 1).$$

n	l	$i : a = \alpha^i \in GF(2^{2l})$	n, k, d reversible cyclic code
9	3	37	9,2,6
15	4	62	15,6,6
17	4	47	17,8,6
21	6	380	21,8,6
25	10	380	25,4,10
27	9	5623	27,8,6
31	5	126	31,20,6
33	5	64	33,22,6
35	12	5335787	35,10,10
39	12	1756757	39,14,6

Table: Reversible cyclic separable (L, G) codes with $G(x) = x^2 + (a + a^{2^l})x + 1$ and $L = \{1, \alpha_2, \ldots, \alpha_n\}, \alpha_i = \frac{a\alpha_{i-1}+1}{\alpha_{i-1}+a^{2^l}}, 1 < i \leq n$

n	l	$i : a = \alpha^i \in GF(2^{2l})$	n, k, d reversible cyclic code
41	10	119693	41,20,10
43	7	383	43,28,6
45	12	900902	45,20,6
49	21	135647920984	49,6,14
51	8	5612	51,34,6
55	20	58865951927	55,14,10
57	9	18909	57,38,6
63	6	128	63,50,6
65	6	191	65,52,6

Table: Reversible cyclic separable (L, G) codes with $G(x) = x^2 + (a + a^{2^l})x + 1$ and $L = \{1, \alpha_2, \dots, \alpha_n\}, \alpha_i = \frac{a\alpha_{i-1}+1}{\alpha_{i-1}+a^{2^l}}, 1 < i \leq n$

Example from [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.]

$$\text{Set } \theta(x) = \frac{\alpha^3 x^2 + 1}{x^{2^l} + \alpha^{29}}$$

The orbit under θ is

$$\{\alpha^{26}, \alpha^5, \alpha^{24}, \alpha^{30}, \infty, \alpha^3, \alpha^{29}, \alpha^{16}, \alpha^{14}, 0, \alpha^2, \alpha^{28}, \alpha^{22}, \alpha^{18}, 1\}.$$

(L, G) code with irreducible polynomial $G(x) = x^3 + \alpha^3 x^2 + \alpha^{29} x + 1$ and

$$L = \{\alpha^{26}, \alpha^5, \alpha^{24}, \alpha^{30}, \alpha^3, \alpha^{29}, \alpha^{16}, \alpha^{14}, 0, \alpha^2, \alpha^{28}, \alpha^{22}, \alpha^{18}, 1\}$$

give us non cyclic $(14, 2, 9)$ Goppa code with cyclic extension

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

Therefore we obtain $(15, 2, 10)$ extended cyclic Goppa code.

Theorem

The sufficient conditions for the cyclicity of separable $(n, k, d \geq 2^{l+1} + 4)$ Goppa codes with the polynomial $G(x)$ of degree $2^l + 1$ and the numerator set $L \subseteq GF(2^m)$ are the following :

1. n is the orbit length of the transformation $\theta(x) = \frac{ax^{2^l}+b}{cx^{2^l}+d}$ in the set $GF(2^m)$,
2. $L = \{\alpha_0, \alpha_2, \ldots, \alpha_{n-1}\}, \alpha_i \in GF(2^m), \theta^{-1}(\alpha_i) = \alpha_{i+1(\mod n)}$,
3. $G(x) = cx^{2^l+1} + ax^{2^l} + dx + b$, and $G(x)$ is either irreducible polynomial over $GF(2^m)$ or $G(\beta_i) = 0, \beta_i \in GF(2^m),\ \theta^{-1}(\beta_i) = \beta_i$.
4. $wt(\mathbf{a})$ is even for any $\mathbf{a} = (a_1 a_2 \ldots a_n) \in \Gamma(L, G)$.

E x a m p l e 3

Let us consider a separable $\Gamma_3(L, G)$ code as a cyclic $(15, 2, 10)$-code with $G(x) = x^3 + \alpha^{96}x^2 + \alpha^3 x + 1, \alpha$ is a primitive element from $GF(2^{10})$,

$$L = \{\alpha^i, i = 589, 713, 744, 558, 992, 682, 62, 651, 620, 341, 806, 31, 279, 217, 0\},$$

transformation $\theta(x) = \frac{\alpha^3 x^2 + 1}{x^2 + \alpha^{96}}$.

The cyclic Goppa code $\Gamma_3(L, G)$ is the cyclic code of length 15 and generator polynomial

$$g(x) = (x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

Conclusion

- New class of binary cyclic reversible separable Goppa codes
- Sufficient conditions for Goppa code cyclicity

THANK YOU FOR YOUR ATTENTION!