Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 88–92*

Cyclic separable Goppa codes

Sergey V. Bezzateev bsv@aanet.ru
Natalia A. Shekhunova sna@delfa.net
St. Petersburg State University of Aerospace Insrtumentation, Bolshaya Morskaya 67, St. Petersburg, 190000, Russia

Abstract. The cyclicity criterion of separable Goppa codes is presented. It is shown that the extended cyclic Goppa codes are the classical Goppa codes.

1 Introduction

Goppa codes of length n are determined by two objects: the Goppa polynomial $G(x)$ of degree t with coefficients from field $GF(q^m)$ and a 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 $\mathbf{a} = (a_1 a_2 \ldots a_n)$ such that

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

The minimum distance of the Goppa code is $d \geq t+1$ and the code dimension is $k \geq n - mt$. The Goppa code is called separable if the Goppa polynomial G is a separable polynomial [1]. It is known that the minimum distance of binary separable code satisfies inequality $d \geq 2t+1$. In case this polynomial is irreducible over the field $GF(2^m)$ the code is called irreducible. The Goppa code is called classical if the set $L \subseteq GF(q^m)$. L is called a set of numerator positions of the codeword. In this case the length of the codeword is $n = |L| \leq q^m$. The Goppa code is called "extended" or "the Goppa code with an additional parity check" if the set $L = GF(q^m) \bigcup \{\infty\}$. In the case T.Berger [6] calls L as support of the Goppa code. The length of the extended Goppa code is $n = q^m + 1$.

It is known that there are cyclic codes among separable codes. These are binary extended Goppa codes with the Goppa polynomial $G(x) = x^2 + x + A, A \in GF(2^m)$. The cyclicity problem of extended Goppa codes has been studied in [2–4]. [5] is a generalization of these researches where the cyclicity criterion of extended Goppa codes is formulated. Let K be the finite field $GF(2^m)$ and $\overline{K} = K \bigcup \{\infty\}, G = PGL(2, 2^m)$ [5]. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a nonsingular matrix over K , $ad + cb \neq 0$ and transformation $x \rightarrow \theta(x) = \frac{ax+b}{cx+d}$.

Lemma 1. *(Lemma 3 [5]) Let us correspond to an arbitrary element* $\theta \in G$ *the matrix* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *over* K *determined up to a scalar factor and the substitution* $x \to \theta(x) = \frac{ax+b}{cx+d}$. *The length of a nontrivial orbit of substitution* θ *of the set* $\overline{K}$ *is equal to the order* $o(\theta)$ *of element* $\theta \in G$.

Lemma 2. *(Lemma5 [5]) Group* G *that is considered to be a group of substitutions of the set* $\overline{K} = K \bigcup \{\infty\}$ *contains the cycle* θ_1 *of the length* $2^m + 1$ *and the cycle* θ_2 *of the length* $2^m - 1$ *such that* $\theta_2^{-1}(\beta_1) = \beta_1$ *and* $\theta_2^{-1}(\beta_2) = \beta_2$, $\beta_1, \beta_2 \in F$.

Corollary 1. *The group* G *contains the cycles* θ_i *of the length* l_i*: where* l_i *takes values of all possible divisors of* $2^m - 1$ *or* $2^m + 1$, $l_i : l_i | 2^m - 1$ *or* $l_i | 2^m + 1$.

In this work we will generalize the results of papers [5–8] in particular we will present a development of Lemma 6 [5] which was formulated for extended Goppa codes for the case of classical $\Gamma(L, G)$ Goppa code ($L \subseteq GF(2^m)$) .

2 Main results

Theorem 1. *The following condition is sufficient condition for the cyclicity of the separable* $(n, k, d \geq 6)$ *Goppa code with a 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. $L = \{\alpha_0, \alpha_2, \ldots, \alpha_{n-1}\}, \alpha_i \in GF(2^m), \theta^{-1}(\alpha_i) = \alpha_{i+1(\mod n)}$,
   $\theta \in G, \theta(x) = \frac{ax+b}{cx+d}$,
3. $G(x) = cx^2 + (a + d)x + b$ *and* $G(x)$ *is either irreducible over* $GF(2^m)$ *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. $wt(\boldsymbol{a})$ *is even for any* $\boldsymbol{a} = (a_1 a_2 \ldots a_n) \in \Gamma(L, G)$.

Theorem 2. *Let us consider the separable* $\Gamma(L, G)$ *code with*

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

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 codeword $\boldsymbol{a} = (a_1 a_2 \ldots a_n)$ *of this code has an even weight.*

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

Corollary 2. *The sufficient cyclicity condition for the separable* $\Gamma(L, G)$*-code is the following:*

1. *it exists a 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. $L = \{\alpha_0, \alpha_2, \ldots, \alpha_{n-1}\}, \alpha_i \in GF(2^m), \alpha_i^{2^l} = \alpha_i^{-1},\ l < m,\ G(\alpha_i) \neq 0,$
3. $\left(x^t\right)^{2^l} G(x^{-1})^{2^l} = AG(x), A \in GF(2^m).$

Corollary 3. *A reversible* $(n = 2^l+1, 2^l-2l, 6)$ *Goppa code with the polynomial* $G(x) = x^2 + rx + 1, r \in GF(2^l) \setminus \{0\}$ *and the set* $L = \{1, \alpha, \alpha^2, \ldots.\alpha^{n-1}\}, \alpha \in GF(2^{2l}), \alpha^n = 1$ *is a cyclic separable Goppa code.*

Similarly to construction of a cyclic codes as extended Goppa codes [2–4] with support $L = GF(2^l)\bigcup\{\infty\}$ and code length $n = 2^l + 1$ or $n = 2^l - 1$, we can present here the construction of the cyclic $(n, k, d \geq 6)$ codes as a classical Goppa codes with the length $n : n < 2^m + 1$ *and* $n|2^m + 1$ *or* $n|2^m - 1$ with an additional parity check. In other words, the following corollary can be formulated.

Corollary 4. *The cyclic* $(n, k-1, d^* \geq 6)$ *code can be obtained from any* $(n, k, d \geq 5)$ *Goppa code with the separable polynomial* $G(x) = cx^2 + (a+d)x + b, ad + cd \neq 0, a, b, c, d \in GF(2^m)$ *by addition parity check.* n *is a orbit length of a transformation* $\theta(x) = \frac{ax+b}{cx+d}$ *in the set* $GF(2^m)$ *,* d^* *is the least odd integer larger than* d*. If* H_Γ *is a parity-check matrix of* $(n, k, d \geq 5)$ *Goppa code then the parity-check matrix of the cyclic* $(n, k-1, d^*)$ *code can be presented in the following form:* $H_C = \begin{bmatrix} H_\Gamma \\ I \end{bmatrix}, I = [11....1].$

Using group of transformation $\theta(x) = \frac{ax^{2^l}+b}{cx^{2^l}+d},\ l < m-1$ which is considered by O.Moreno for finding symmetry groups of Goppa codes [9], it can prove the following theorem. This theorem defines the cyclicity criterion for the separable $(n, k, d \geq 2^{l+1} + 4)$ Goppa codes with $\deg G(x) = 2^l + 1$ and $L \subseteq GF(2^m)$.

Theorem 3. *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. $wt(\boldsymbol{a})$ is even for any $\boldsymbol{a} = (a_1 a_2 \dots a_n) \in \Gamma(L, G)$.

It is obvious that Corollaries 2, 3, 4 can be generalized for Theorem 3 also.

3 Code examples

Example 1. *(Theorem 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

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

Example 2. *(Corollary 3) Let us consider as example of a separable $\Gamma_3(L,G)$ 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 $\Gamma_3(L,G)$ is the cyclic code of length 33 and generator polynomial

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

Example 3. *(Theorem 3) Let us consider a separable $\Gamma_4(L,G)$ 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 $\Gamma_4(L,G)$ is the cyclic code of length 15 and generator polynomial

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

4 Conclusion

In the paper the cyclicity criterion for Goppa codes with separable polynomial and numerator set has been formulated. It generalizes the known criterion for extended Goppa codes (with length $n = 2^m + 1$). Our results (Theorems 1 and 3) enable to present as cyclic separable Goppa codes with $n \neq 2^m - 1, n \neq 2^{m+1}$ which are not either extended codes, no primitive BCH-codes. As an addition to examples that were considered above, it can be presented (89,66,8) code with Goppa polynomial of the degree two. It is BCH- code with the generator polynomial $g(x) = (x+1)(x^{11} + x^7 + x^6 + x + 1)(x^{11} + x^{10} + x^5 + x^4 + 1)$. And finally, the extended Goppa codes [1–5] could be presented as classical Goppa codes.

References

[1] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, 1986.

[2] 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.

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

[4] K.K. Tzeng , C.Y. Yu , Characterization Theorems for Extending Goppa Codes to Cyclic Codes, *IEEE Trans. Inform. Theory*, 1979, v. 25, n. 2, p. 246-250.

[5] A.L. Vishnevetskiy , On cyclicity of extended Goppa codes, *Probl. Inform. Transm.*, 1982, v.XVIII, n.3, pp. 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 , Quasi-cyclic Goppa codes, in *Proc. ISIT2000, Sorrente, Italie*, 2000, p. 195.

[8] T.P. Berger ,New Classes of Cyclic Extended Goppa Codes,*IEEE Trans. Inform. Theory*, 1999, v. 45, n.4, p.1264-1266.

[9] O. Moreno, Symmetries of Binary Goppa Codes, *IEEE Trans. Inform. Theory*, 1979, v. 25, n. 5, p. 609-612.