Cyclic Generalized Separable (L, G) Codes

Sergey Bezzateev

Abstract A new class of cyclic generalized separable (L, G) codes is constructed.

Keywords Generalized (L,G) codes • Goppa codes • Cyclic codes

1 Introduction

A classical Goppa code [1] is determined by two objects: a Goppa polynomial $G(x)$ with coefficients from $GF(q^m)$ and location set L of codeword positions

$$L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq GF(q^m), G(\alpha_i) \neq 0, \ \forall \alpha_i \in L.$$

Definition 1 A q-ary vector $\boldsymbol{a} = (a_1 a_2 \ldots a_n)$ is a codeword of (L, G)-code if and only if the following equality is satisfied

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

Definition 2 Goppa code is called separable if the polynomial $G(x)$ does not have multiple roots.

In [1] V.D. Goppa proved that the primitive BCH codes are the only subclass of Goppa codes that are cyclic with $G(x) = (x - \gamma)^t, \gamma \in GF(q^m)$, $L \subseteq GF(q^m) \setminus \{\gamma\}$. Accordingly, the only one class of separable Goppa codes with $G(x) = (x - \gamma), \gamma \in GF(q^m), L \subseteq GF(q^m) \setminus \{\gamma\}$ defined as cyclic.

In 1973 in [2] and later in [3–11] a subclasses of extended separable Goppa codes and subclasses of separable Goppa codes with Goppa polynomials of degree 2 and additional parity check were proposed. It was proved that these codes are cyclic.

S. Bezzateev (✉)
Saint Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya st., 67, Saint Petersburg, 190000 Russia
e-mail: bsv@aanet.ru

R. Pinto et al. (eds.), *Coding Theory and Applications*, CIM Series in Mathematical Sciences 3, DOI 10.1007/978-3-319-17296-5_5

However, the existence among separable Goppa codes any subclass of cyclic codes remained an open problem ([12] Ch.12, Corollary 9, Research Problem 12.3).

In 2013 in [13] the subclass of cyclic separable Goppa codes with a special choice of location set L and and Goppa polynomial $G(X)$ of degree 2 was suggested.

$$\begin{array}{l} L = \{\alpha_1, \alpha_2 \ldots, \alpha_{n-1}, \alpha_n\} \subset \{GF(q^{2m}) \setminus GF(q^m)\} \bigcup \{1\}, \\ \alpha_n = 1, \alpha_i^{q^m} = \alpha_i^{-1} = \alpha_{n-i}, n = q^m \pm 1, \\ G(x) = (x-\beta)(x-\beta^{-1}),\ \beta \in GF(q^{2m}),\ \beta + \beta^{-1} \in GF(q^m), \\ G(\alpha_i) \neq 0, \alpha_i \neq \alpha_j,\ \forall i, j \in \{1, \ldots, n\},\ i \neq j. \end{array}$$

A generalized Goppa code [14] can be constructed by using the following generalization of location set L:

$$L = \left\{ \frac{f_1'(x)}{f_1(x)}, \frac{f_2'(x)}{f_2(x)}, \ldots, \frac{f_n'(x)}{f_n(x)} \right\}, \tag{1}$$

where $f_i'(x)$ is a formal derivative of $f_i(x)$ in $GF(q)$ and

$$\begin{array}{l} f_i(x) = x^\ell + a_{i,\ell-1}x^{\ell-1} + \ldots + a_{i,1}x + a_{i,0}, a_{i,j} \in GF(q^\mu), \\ \gcd(f_i(x), f_j(x)) = 1,\ \gcd(f_i(x), G(x)) = 1,\ \forall i, j,\ i \neq j. \end{array}$$

Definition 3 q-ary vector $\boldsymbol{a} = (a_1 a_2 \ldots a_n)$ is a codeword of generalized (L, G)-code if and only if the following equality is satisfied

$$\sum_{i=1}^{n} a_i \frac{f_i'(x)}{f_i(x)} \equiv 0 \mod G(x). \tag{2}$$

Generalized Goppa codes have allowed to expand a class of cyclic Goppa codes with $G(x) = (x-\gamma)^t$. Many cyclic (n, k, d) codes can be described as generalized Goppa codes [15] with

$$\begin{array}{l} f_i(x) = f(\alpha^i x),\ f(x) = x^\ell + a_{\ell-1}x^{\ell-1} + \ldots + a_1 x + a_0,\ \alpha, a_j \in GF(q^\mu), \\ a_0 \neq 0, \alpha^n = 1,\ n|(q^\mu - 1),\ \gcd(f_i(x), f_j(x)) = 1,\ \forall i, j,\ i \neq j \end{array}$$

and

$$G(x) = x^t.$$

For such codes the design bound for minimum distance $d_G \geq \frac{t+1}{\ell}$ and the corresponding decoding algorithm were determined [16, 17]. However, a subclass of cyclic generalized separable Goppa codes is still remained limited by polynomial $G(x) = (x-\gamma), \gamma \in GF(q^\mu)$.

2 Two Subclasses of Binary Cyclic Generalized Separable Goppa Codes

In this paper we will consider a binary case with two variants of separable Goppa polynomial

$$G(x) = x^n - 1 \text{ and } \hat{G}(x) = x(x^n - 1). \tag{3}$$

We will need the following definitions.

Definition 4 For any integers $n,\ n|(2^m - 1)$ and $l,\ 0 \leq l < n$ a cyclotomic coset m_l is given by

$$m_l = \{l2^j \mod n, \forall j = 0, 1, \ldots, \lambda_l - 1\},$$

where λ_l is the smallest integer greater than 0 such that $l2^{\lambda_l} \equiv l \mod n$.

Definition 5 The minimal polynomial $M_l(x)$ of element $\alpha^l \in GF(2^m)$ is given by

$$M_l(x) = \prod_{j \in m_l} (x - \alpha^j),\ \deg M_l(x) = \lambda_l.$$

Definition 6 The generator polynomial of a cyclic (n, k, d) code C is given by

$$g(x) = \prod_{j \in D} (x - \alpha^j),\ D = \bigcup_{j=1}^{\nu} m_{l_j} \text{ and } g(x) = \prod_{j=1}^{\nu} M_{l_j}(x),\ \deg g(x) = \prod_{j=1}^{\nu} \lambda_{l_j} = n - k,$$

where D is the set containing the indices of the zeros of the generator polynomial $g(x)$. The size of set D is equal to $n - k$.

For some D let's consider a binary linear (η, κ, τ) code C_L with the length η, dimension κ, minimum distance τ and parity-check matrix H_L

$$H_L = \begin{bmatrix} \frac{\beta_1^{j_1}}{G(\beta_1)} & \cdots & \frac{\beta_\eta^{j_1}}{G(\beta_\eta)} \\ \frac{\beta_1^{j_2}}{G(\beta_1)} & \cdots & \frac{\beta_\eta^{j_2}}{G(\beta_\eta)} \\ \vdots & \ddots & \vdots \\ \frac{\beta_1^{j_k}}{G(\beta_1)} & \cdots & \frac{\beta_\eta^{j_k}}{G(\beta_\eta)} \end{bmatrix}, \begin{array}{l} \beta_i \in GF(2^\mu) \setminus \{0, 1\},\ GF(2^\mu) \cap GF(2^m) = \{0, 1\}, \\ N = \{j_1, j_2, \ldots, j_k\}, N \cup D = \{0, 1, \ldots, n - 1\}. \end{array} \tag{4}$$

Let $\mathbf{b} = (b_1\ b_2 \ldots b_\tau\ b_{\tau+1} \ldots b_\eta)$ with $b_i = 1, \forall i = 1, \ldots \tau$ and $b_i = 0, \forall i = \tau + 1, \ldots, \eta$ be a codeword of this code. Then for this vector $\mathbf{b}$ and parity-check matrix H_L we obtain

$$\mathbf{b} \cdot H^T = 0 \text{ and } \sum_{i=1}^{\eta} b_i \frac{\beta_i^{j_l}}{G(\beta_i)} = \sum_{i=1}^{\tau} \frac{\beta_i^{j_l}}{G(\beta_i)} = 0, \forall l = 1, \dots, k. \quad (5)$$

As in [17] we will call C_L as non-zero-locator code for cyclic code C with the set D if for any $m_i \subset D$ exists $j : j \in m_i, \sum_{i=1}^{\tau} \frac{\beta_i^j}{G(\beta_i)} \neq 0$. We associate with codeword $\mathbf{b}$ of this non-zero-locator code C_L the following locator polynomial

$$\begin{aligned} &f(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_\tau),\ \beta_j \in GF(2^\mu),\ j = 1,\dots,\tau, \\ &f_i(x) = (x-\alpha^i\beta_1)(x-\alpha^i\beta_2)\cdots(x-\alpha^i\beta_\tau),\ \alpha \in GF(2^m),\ \alpha^n = 1, \\ &\gcd(f_i(x), f_j(x)) = 1,\ \forall i \neq j,\ \ i,j = 1,\dots,n. \end{aligned} \quad (6)$$

Theorem 7 *Generalized (L, G) code with Goppa polynomial $G(x)$ (3) and locator set L (1) defined by non-zero-locator code C_L (4),(5) and by associated locator polynomial $f(x)$ (6) is a cyclic code C with the set D of indices of zeroes of generator polynomial.*

Proof Parity-check matrix H_G for this code is:

$$H_G = \begin{bmatrix} \alpha_1^{\ell_1} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_1}}{G(\beta_i)} & \dots & \alpha_n^{\ell_1} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_1}}{G(\beta_i)} \\ \alpha_1^{\ell_2} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_2}}{G(\beta_i)} & \dots & \alpha_n^{\ell_2} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_2}}{G(\beta_i)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{\ell_\delta} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_\delta}}{G(\beta_i)} & \dots & \alpha_n^{\ell_\delta} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_\delta}}{G(\beta_i)} \end{bmatrix} = \begin{bmatrix} \alpha_1^{\ell_1} & \dots & \alpha_n^{\ell_1} \\ \alpha_1^{\ell_2} & \dots & \alpha_n^{\ell_2} \\ \vdots & \ddots & \vdots \\ \alpha_1^{\ell_\delta} & \dots & \alpha_n^{\ell_\delta} \end{bmatrix}, \quad (7)$$

where $\{\ell_1, \ell_2, \dots, \ell_\delta\} \subseteq D$.

□

Note 8 By Definition 6 dimension of this code is $k = n - \|D\|$, where $\|D\|$ is a size of the set D.

For the case $\hat{G}(x) = x(x^n - 1)$ we will obtain a similar theorem.

Theorem 9 *Generalized $(L, \hat{G})$ code with Goppa polynomial $\hat{G}(x)$ (3) and locator set L (1) defined by non-zero-code C_L (4),(5) is a cyclic code $\hat{C}$ with the set $\hat{D} \subseteq D \cup m_{-1}$ of indices of zeroes of generator polynomial.*

Proof Parity-check matrix $H_{\hat{G}}$ for this code is:

$$H_{\hat{G}} = \begin{bmatrix} \alpha_1^{-1} \sum_{i=1}^{\tau} \frac{1}{G(\beta_i)} & \dots & \alpha_n^{-1} \sum_{i=1}^{\tau} \frac{1}{G(\beta_i)} \\ \alpha_1^{\ell_1} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_1}}{G(\beta_i)} & \dots & \alpha_n^{\ell_1} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_1}}{G(\beta_i)} \\ \alpha_1^{\ell_2} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_2}}{G(\beta_i)} & \dots & \alpha_n^{\ell_2} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_2}}{G(\beta_i)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{\ell_\delta} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_\delta}}{G(\beta_i)} & \dots & \alpha_n^{\ell_\delta} \sum_{i=1}^{\tau} \frac{\beta_i^{\ell_\delta}}{G(\beta_i)} \end{bmatrix} = \begin{cases} H_G, \text{ if } -1 \in D \text{ or } 0 \in N, \\ \begin{bmatrix} \alpha_1^{-1} \dots \alpha_n^{-1} \\ H_G \end{bmatrix}, \text{ if } -1 \notin D \text{ and } 0 \notin N. \end{cases} \tag{8}$$

□

Theorem 10 *From* (2)*,* (3) *and* (6) *we obtain the following estimation for minimal distance of binary cyclic generalized separable Goppa code:*

$$d_G \geq \frac{2n+1}{\tau} \textit{ for } G(x) = x^n - 1$$

and

$$d_{\hat{G}} \geq \frac{2n+3}{\tau} \textit{ for } \hat{G}(x) = x(x^n - 1).$$

3 Trace Non-zero-Locator Code

As example of non-zero-locator code let's consider a binary linear code with length η , parity-check matrix

$$H_L = \begin{bmatrix} \frac{\beta^{j_1}}{G(\beta)} & \frac{\beta^{2j_1}}{G(\beta^2)} & \cdots & \frac{\beta^{\eta j_1}}{G(\beta^\eta)} \\ \frac{\beta^{j_2}}{G(\beta)} & \frac{\beta^{2j_2}}{G(\beta^2)} & \cdots & \frac{\beta^{\eta j_2}}{G(\beta^\eta)} \\ \vdots & \ddots & \vdots & \\ \frac{\beta^{j_k}}{G(\beta)} & \frac{\beta^{2j_k}}{G(\beta^2)} & \cdots & \frac{\beta^{\eta j_k}}{G(\beta^\eta)} \end{bmatrix}, \quad \begin{array}{l} \beta - \text{ primitive element in } GF(2^\mu), \\ tr(\beta^{j_i}) = 0, \forall i = 1, \dots, k, \\ N = \{j_1, j_2, \dots, j_k\}, \\ N \cup D = \{0, 1, \dots, n-1\}. \end{array} \tag{9}$$

and codeword

$$\mathbf{b} = (b_1 b_2 \dots b_\eta), wt(\boldsymbol{b}) = \mu \text{ and } b_1 = b_2 = b_{2^2} = \dots = b_{2^{\mu-1}} = 1.$$

Now we can rewrite matrix H_G (7) in the following form

$$H_G = \begin{bmatrix} \alpha_1^{\ell_1} tr\left(\frac{\beta^{\ell_1}}{G(\beta)}\right) \dots \alpha_n^{\ell_1} tr\left(\frac{\beta^{\ell_1}}{G(\beta)}\right) \\ \alpha_1^{\ell_2} tr\left(\frac{\beta^{\ell_2}}{G(\beta)}\right) \dots \alpha_n^{\ell_2} tr\left(\frac{\beta^{\ell_2}}{G(\beta)}\right) \\ \vdots \quad \ddots \quad \vdots \\ \alpha_1^{\ell_\delta} tr\left(\frac{\beta^{\ell_\delta}}{G(\beta)}\right) \dots \alpha_n^{\ell_\delta} tr\left(\frac{\beta^{\ell_\delta}}{G(\beta)}\right) \end{bmatrix} = \begin{bmatrix} \alpha_1^{\ell_1} \dots \alpha_n^{\ell_1} \\ \alpha_1^{\ell_2} \dots \alpha_n^{\ell_2} \\ \vdots \ \ddots \ \vdots \\ \alpha_1^{\ell_\delta} \dots \alpha_n^{\ell_\delta} \end{bmatrix}, \tag{10}$$

where $tr\left(\frac{\beta^{\ell_i}}{G(\beta)}\right) \neq 0, i = 1, \dots, \delta, \ \{\ell_1, \ell_2, \dots, \ell_\delta\} \subseteq D.$

For such trace non-zero-locator code we have locator polynomial $f(x)$ from (6):

$$f(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{2^{\mu-1}}) = \Omega_1(x),\ \Omega_1(x) \in \mathbb{F}_2[x],\ \deg \Omega_1(x) = \mu,$$

$\Omega_1(x)$ is a minimal polynomial of element $\beta \in GF(2^\mu)$.

From Theorem 10 we obtain the following estimation for minimal distance of binary cyclic generalized separable Goppa code with trace non-zero-locator code:

$$d_G \geq \frac{2n+1}{\mu} \text{ for } G(x) = x^n - 1$$

and

$$d_{\hat{G}} \geq \frac{2n+3}{\mu} \text{ for } \hat{G}(x) = x(x^n - 1).$$

4 Examples

1.

$$\begin{aligned} & n = 21, \hat{G}(x) = x(x^{21} - 1), \alpha \in GF(2^6), \alpha^{21} = 1, \beta \in GF(2^7), \\ & f(x) = x^7 + x^6 + x^4 + x + 1, f_i(x) = \alpha^{7i} x^7 + \alpha^{6i} x^6 + \alpha^{4i} x^4 + \alpha^i x + 1, \\ & L = \{\tfrac{x^6+1}{x^7+x^6+x^4+x+1}, \tfrac{\alpha^7 x^6+\alpha}{\alpha^7 x^7+\alpha^6 x^6+\alpha^4 x^4+\alpha x+1}, \dots, \tfrac{\alpha^{14} x^6+\alpha^{20}}{\alpha^{14} x^7+\alpha^{15} x^6+\alpha^{17} x^4+\alpha^{20} x+1}\}, \\ & tr\left(\frac{\beta^i}{\hat{G}(\beta)}\right) = 1,\ i = 0, 3, 4, 6, 7, 12, 14, 21, \\ & tr\left(\frac{\beta^i}{\hat{G}(\beta)}\right) = 0,\ i = 1, 2, 5, 8, 9, 10, 11, 13, 15, 16, 17, 18, 19, 20. \end{aligned}$$

Therefore from Theorem 9 we have $(21, 6, 7)$ cyclic code with generator polynomial $g(x) = m_1(x)m_3m_5(x)$. From Theorem 10 we obtain the following estimation for minimum distance for this generalized separable $(L, \hat{G})$ code:

$$d_G \geq \frac{2n+3}{\mu} = \frac{45}{7} > 6 \text{ and we have } d_G = d = 7.$$

2.

$$n = 21, \hat{G}(x) = x^{21} - 1, \alpha \in GF(2^6), \alpha^{21} = 1, \beta \in GF(2^7),$$
$$f(x) = x^7 + x^6 + x^4 + x^2 + 1,\ f_i(x) = \alpha^{7i}x^7 + \alpha^{6i}x^6 + \alpha^{4i}x^4 + \alpha^{2i}x^2 + 1,$$
$$L = \{\frac{x^6}{x^7+x^6+x^4+x^2+1}, \frac{\alpha^7 x^6}{\alpha^7x^7+\alpha^6x^6+\alpha^4x^4+\alpha^2x^2+1}, \ldots, \frac{\alpha^{14}x^6+\alpha^{20}}{\alpha^{14}x^7+\alpha^{15}x^6+\alpha^{17}x^4+\alpha^{19}x^2+1}\},$$
$$tr\left(\frac{\beta^i}{\hat{G}(\beta)}\right) = 1,\ i = 2, 3, 5, 6, 11, 13, 20,$$
$$tr\left(\frac{\beta^i}{\hat{G}(\beta)}\right) = 0,\ i = 0, 1, 4, 7, 8, 9, 10, 12, 14, 15, 16, 17, 18, 19.$$

From Eq. (10) and Theorem 7 we have $(21, 6, 7)$ cyclic code with generator polynomial $g(x) = m_1(x)m_3(x)m_5(x)$. From Theorem 10 we obtain the following estimation for minimum distance for this generalized separable (L, G) code:

$$d_{\hat{G}} \geq \frac{2n+1}{\mu} = \frac{43}{7} > 6 \text{ and we have } d_{\hat{G}} = d = 7.$$

5 Conclusion

The new subclasses of cyclic generalized separable Goppa codes with Goppa polynomials $x^n - 1$ and $x(x^n - 1)$ are proposed. The parameters and examples of the codes from these subclasses are shown.

References

1. Goppa,V.D.: A new class of linear error-correcting codes. Probl. Inf. Trans. **6**(3) , 24–30 (1970)
2. Berlecamp, E.R., Moreno, O.: Extended double-error-gorrecting binary Goppa codes are cyclic. IEEE Trans. Inf. Theory **19**(6), 817–818 (1973)
3. Tzeng, K.K., Zimmermann, K.: On extending Goppa codes to cyclic codes. IEEE Trans. Inf. Theory **21**(6), 712–716 (1975)
4. Tzeng, K.K., Yu, C.Y.: Characterization theorems for extending Goppa codes to cyclic codes. IEEE Trans. Inf. Theory **25**(2), 246–250 (1979)
5. Moreno, O.: Symmetries of binary Goppa codes. IEEE Trans. Inf. Theory **25**(5), 609–612 (1979)
6. Vishnevetskii, A.L.: Cyclicity of extended Goppa codes. Probl. Pered. Inf. **18**(3), 14–18 (1982)
7. Stichenoth, H.: Wich extended Goppa codes are cyclic? J. Comb. Theory **A 51**, 205–220 (1989)
8. B erger, T.P.: Goppa and related codes invariant under a prescribed permutation. IEEE Trans. Inf. Theory **46**(7), 2628–2633 (2000)
9. Berger, T.P.: On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes, and extended Goppa codes. Finite Fields Appl. **6**, 255–281 (2000)
10. Berger, T.P.: Quasi-cyclic Goppa codes. In: Proceedings of ISIT2000, Sorrente, p. 195 (2000)
11. Berger, T.P.: New classes of cyclic extended Goppa codes. IEEE Trans. Inf. Theory **45**(4), 1264–1266 (1999)

12. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
13. Bezzateev, S., Shekhunova, N.: Subclass of cyclic Goppa codes. IEEE Trans. Inf. Theory **59**(11), 7379–7385 (2013)
14. Shekhunova, N.A., Mironchikov, E.T.: Cyclic (L, g)-codes. Probl. Pered. Inf. **17**(2), 3–9 (1981)
15. Bezzateev, S.V., Shekhunova, N.A.: One generalization of Goppa codes. In: Proceedings of ISIT-97, Ulm, p. 299 (1997)
16. Zeh, A., Wachter-Zeh, A., Bezzateev, S.: Decoding cyclic codes up to a new bound on the minimum distance. IEEE Trans. Inf. Theory **58**(6), 3951–3960 (2012)
17. Zeh, A., Bezzateev, S.: A new bound on the minimum distance of cyclic codes using small-minimum-distance cyclic codes. Designs Codes Cryptogr. **71**, 229–246 (2014)