Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 41-46*

Optimal quasi-cyclic Goppa codes[1]

Sergey Bezzateev bsv@aanet.ru
Natalia Shekhunova sna@delfa.net
Saint Petersburg State University of Aerospace Instrumentation

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. A new class of quasi-cyclic Goppa codes is considered. It is shown that it contains optimal codes.

1 Introduction

A 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

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

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

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

It is known that quasi-cyclic Goppa codes can be constructed as special subclasses of extended Goppa codes or expurgated subcodes. Permutations of elements of the location set L from linear and semilinear projective line group are used for the construction of these codes [2–4].

$$PGL(2,L) = \{f | f(\alpha) = \tfrac{a\alpha+b}{\alpha+c}, \alpha \in L, a,b,c \in GF(q^m), ac-b \neq 0\},$$
$$P\Gamma L(2,L) = \{f | f(\alpha) = \tfrac{a\alpha^{q^l}+b}{\alpha^{q^l}+c}, \alpha \in L, a,b,c \in GF(q^m), ac-b \neq 0, 0 \leq l < m\}.$$

It has been proved in [2], Corollary 1 (*Expurgated subcodes*), Theorem 4 (*Extended codes*) that the equation

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

[1]This research is partially supported by Erasmus Mundus scholarship for the Erasmus Mundus Masters Course NordSecMob.

for any codeword is the necessary and sufficient condition for the quasi-cyclicity of the Goppa code in case the groups of permutations $PGL(2, L)$, $P\Gamma L(2, L)$ are used. It should be noted [2–4] that in this case the element ∞ has been included into the numerator set L (extended code);in case expurgated subcode is considered, a subcode with words satisfied equation (1) only is used.

In this paper a consistent choice of a Goppa polynomial $G(x)$ and numerator set L that provides the fulfilment of (1) for all codewords of the $\Gamma(L, G)$-code is proposed . For the considered subclass of quasi-cyclic Goppa codes we have obtained estimations of the dimension and minimum distance. It is shown that there exist optimal codes among such quasi-cyclic codes.

2 Class of embedded quasi-cyclic separable Goppa codes

Theorem 1. *[6] All codewords of the* $\boldsymbol{a} = (a_1 a_2 \dots a_n)$ $\Gamma(L, G)$*-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:

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

Let us define a set M of elements of the field $GF(q^{2m})$ as following:

$$M = \{\alpha : \alpha^{q^m} = \alpha^{-1}, \alpha \in GF(q^{2m})\}.$$

Theorem 2. *The permutation given by the function*

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

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

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

Lemma 1. *All roots of the polynomial*

$$G(x) = x^{q^l + 1} - ax^{q^l} + a^{q^m} x + 1 \tag{2}$$

are fixed with respect to the permutation $f(x)$ *defined in Theorem 2.*

It is easy to show that $G(x)$ is a separable polynomial.
Let us choose a location set

$$L = M \setminus \{\alpha : G(\alpha) = 0\}. \tag{3}$$

Then the $\Gamma(L, G)$-codes with the such set L and with the Goppa polynomial

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

$$G(x) = x + \beta, \beta \in M \tag{4}$$

satisfy the conditions of Theorem 1.

So, the equation $\sum\limits_{i=1}^{n} a_i = 0$ is satisfied for all words of such codes.

Theorem 3. *$\Gamma(L, G)$-codes given by set $L(3)$ and Goppa polynomials $G(x)(2)$,(4) 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:

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

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

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

These $\widehat{G}(x)$ and $\widehat{L}$ satisfy the conditions of Theorem 1.

Theorem 4. *The $\Gamma(\widehat{L}, \widehat{G})$-code is a quasi-cyclic code with the cycloid length μ, minimum distance*

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

and dimension

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

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 1, 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 $\widehat{G}_i(x)$.

3 Examples

Let us choose a multiplicative subgroup M of the field $GF(2^{10})$

$$M = \left\{\alpha^{31i}, i = 0, \dots, 32\right\}$$

and transformation

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

where α is a primitive element of $GF(2^{10})$ and it is a root of a polynomial $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$.

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 With the exception of the roots of the polynomial $G(x)$:

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

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

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

Example 1. *Using the location set L and Goppa polynomial $G(x) = x^3 + \alpha^{29}x^2 + \alpha^{928}x + 1$ we obtain quasi-cyclic $(30, 14, 8)$-code with the weight distribution*

$$\begin{aligned} &< 0, 1 >, < 8, 225 >, < 10, 840 >, < 12, 2800 >, < 14, 4200 >, \\ &< 16, 4635 >, < 18, 2520 >, < 20, 1008 >, < 22, 120 >, < 24, 35 > . \end{aligned}$$

This is a new optimal quasi-cyclic code with the length of cycloid equal to $\mu = 5$ *[7, 8].*

Example 2. *Using the same set* L *and different polynomials of the second degree*

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

as divisors of the Goppa polynomial $G(x)$ *we obtain 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 equal to $\mu = 5$ *[7, 8].*

Example 3. *Using the same set* L *and different polynomials of the first power*

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

as divisors of $G(x)$ *we obtain 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 equal to $\mu = 5$ *[7, 8].*

4 Conclusion

The new class of classical Goppa codes with separable Goppa polynomials and special location sets L are proposed. It is shown that these codes are quasi-cyclic codes. Moreover, many codes have the best known parameters (minimum distance and dimension).

References

[1] V. D. Goppa, A new class of linear error-correcting codes, *Probl. Inform. Transm.*, **6**, 3 , 24–30, 1970.

[2] T. P. Berger, Goppa and related codes invariant under a prescribed permutation, *IEEE Trans. Inform. Theory.,* **46**, 7, 2628–2633, 2000.

[3] 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, 255–281, 2000.

[4] T. P. Berger, Quasi-cyclic Goppa codes, in *Proc. ISIT2000, Sorrente, Italy, 2000,* 195.

[5] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam, Netherlands, North-Holland, 1977.

[6] S. Bezzateev, N. Shekhunova, Chain of separable binary Goppa codes and their minimal distance, *IEEE Trans. Inform.Theory.,* **54**, 12, 5773–5778, 2008.

[7] Z. Chen, A database on binary quasi-cyclic codes, http://moodle.tec.hkr.se/ chen/research/codes/qc.htm

[8] M. Grassl, Tables of Linear Codes and Quantum Codes. http://www.codetables.de/