Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 76–79*

New Class of Quasi-cyclic Goppa Codes

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

A special class of generalized separable (L, G)-codes with a set of code position numerators L including all irreducible polynomials of degree 2 from $F_{q^m}[x]$ and Goppa polynomial $G(x) = x^{q^m} - x$ is offered. It is shown that this is a new class of quasi-cyclic (L, G)-codes. Improved estimations of the dimension and minimum distance for this class are obtained.

1 Introduction

A special subclass of separable Goppa codes with a set of code position numerators of maximum size from the class of generalized (L, G)-codes [1] is considered.

Definition 1. *Generalized (L, G)-code with a set L of code position numerators*

$$L = \{f_1(x), f_2(x), \ldots, f_n(x)\}, \quad \text{where } f_i(x) \in \mathbb{F}_{q^m}[x],$$
$$\text{and } \deg f_i(x) \le \tau,\ \gcd(f_i(x), f_j(x)) = 1, \forall i \ne j,\ i, j = [1, \ldots, n]$$

and Goppa polynomial $G(x)$:

$$G(x) \in \mathbb{F}_{q^m}[x] \text{ and } \gcd(G(x), f_i(x)) = 1, \forall i = [1, \ldots, n]$$

is defined by a set of all vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ satisfying the following relation:

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

where $f_i'(x)$ is a formal derivative of polynomial $f_i(x)$.

Estimations of redundancy r and the minimum distance d of generalized (L, G)- codes are defined by the following relations [1]:

$$r \le m \deg G(x),\ d \ge \frac{\deg G(x) + 1}{\tau}.$$

Definition 2. *The generalized (L, G)- code with a set of code position numerators L containing elements of degrees not exceeding τ and Goppa polynomial $G(x)$ satisfying the following equality :*

$$G(x) \prod_{i=1}^{n} f_i(x) = x^{q^{\tau m}} - x \tag{2}$$

is called Goppa code with a set of code position numerators L of the maximum size of degree τ or a set L of maximum size.

In other words, we consider the generalized (L, G)- code defined by such a set L of the maximum size and the Goppa polynomial $G(x)$ that containes all irreducible polynomials from $F_{q^m}[x]$ of degrees not greater than τ.

2 Quasi-cyclic codes from the subclass of generalized (L, G)- codes

In this paper when designing a class of quasi-cyclic codes we consider as an example but WLOG only the generalized separable (L, G)-codes with the set L of the maximum size of the second degree.

Proposition 1. *Generalized separable (L, G)-code with the set L of the maximum size of the second degree and the Goppa polynomial*

$$G(x) = \prod_{\alpha_i \in GF(q^m)} (x - \alpha_i) = x^{q^m} - x \tag{3}$$

is a quasi-cyclic code. This code is defined as a set of all vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ of the length $n = I_{q^m}(2)$ satisfying the relation

$$\sum_{i=1}^{n} a_i \frac{u_i'(x)}{u_i(x)} \equiv 0 \mod G(x), \tag{4}$$

where $u_i(x)$ are all unitary (i.e.,the greatest coefficient is equal to 1) irreducible polynomials of degree 2 over $GF(q^m)$. $I_{q^m}(2)$ is a number of unitary polynomials of degree 2 irreducible over $GF(q^m)$.

It is known [3] that

$$I_{q^m}(2) = \frac{q^{2m} - q^m}{2} .$$

Lemma 1. *Generalized separable (L, G)-codes with the set of position numerators L of the maximum size of the second degree that satisfy relations (3) and (4) are quasi-cyclic codes with the cycloid length equal to $q^m - 1$.*

Lemma 2. *The redundancy r of the separable (L, G)- code defined by equalities (3) and (4) with the set L of the maximum size of the second degree satisfies the following relation:*

$$r \leq m(\deg G(x) - 2) + 1 = m(q^m - 2) + 1.$$

Theorem 1. *The minimum distance d of this (L, G)- code(3) is defined by the following relation*

$$(d-1)2 + 1 \geq \deg G(x) + 2.$$

This relation can be rewritten as

$$d \geq \frac{\deg G(x) + 1}{2} + 1 = \frac{q^m + 1}{2} + 1. \tag{5}$$

Theorem 2. *The minimum distance d of the binary generalized separable (L, G)- code with the set L of the maximum size of the second degree is defined by relations (3) and (4) satisfies the following reletion:*

$$(d-1)2 + 0 \geq 2\deg G(x) + 2. \tag{6}$$

The relation can be rewritten as:

$$d \geq \deg G(x) + 2.$$

Moreover, all words of this binary code have even weights.

3 Code examples

Example 1. *The binary generalized separable (L, G)- code with the Goppa polynomial $G(x) = x^8 - x$ and the set L of maximum size including all irreducible polynomials of the second degree from $F_{2^3}[x]$ is a quasi-cyclic code of the cycloid length 7 and with parameters*

$$n = 28, k = 9, d = 10.$$

This is the optimal binary linear code [4] and it is considered to be a new quasi-cyclic $(28, 9, 10)$- code [5].

Example 2. *New quasi-cyclic codes [5] obtained from the generalized separable (L, G)-codes with the set of code position numerators of maximum size over $GF(q)$, Goppa polynomials $G(x) = x^q - x, q = 5, 7, 8, 9$ and L containes all irreducible polynomials of degree 2 from $F_q[x]$:*

- $\mathbf{q = 5}$, $G(x) = x^5 - x$, $n = 10, k = 6, d = 4^*$,
- $\mathbf{q = 7}$, $G(x) = x^7 - x$, $n = 21, k = 15, d = 5^{**}$,

- $\mathbf{q=8}$, $G(x)=x^8-x$, $n=28, k=21, d=6^{**}$,
- $\mathbf{q=9}$, $G(x)=x^9-x$, $n=36, k=28, d=6^{**}$,

** optimal linear code [4],*
*** best known linear code [4].*

4 Conclusion

The subclass of generalized Goppa codes with the special separable Goppa polynomial and with the set of code position numerators of maximum size (the set contains all the irreducible polynomials of degree 2) has been investigated. The estimations of the dimension and minimum distance are obtained. They are found out to be better than the known ones. The examples demonstrate that there are codes with the parameters being the best of all the known ones in this subclass. It is proved that this is the class of quasi-cyclic codes. New quasi-cyclic codes are designed [5]. The approach to the design of quasi-cyclic codes as a special subclass of generalized Goppa codes with a consistent choice of the set of code position numerators L and Goppa polynomial $G(x)$ is offered. It allows designing not only good binary codes (minimum distance satisfies inequality (6)), but also nonbinary codes with the estimation of the minimum distance satisfying relation (5). It should be specially noted that this class of quasi-cyclic codes as the subclass of generalized Goppa codes has a simple coding algorithm that is similar to the coding algorithm for cyclic codes. The problem of the existence of subclasses of (L,G)-codes with simple coding schemes was discussed by the authors with V.Dm. Kolesnik in 2008. It seems that the suggested class of quasi-cyclic (L,G)-codes could be the one of possible solutions. The decoding algorithm of such codes was described in [2].

References

[1] S. V. Bezzateev and N .A. Shekhunova, One generalization of Goppa codes, in *Proceedings of ISIT-97,Ulm, Germany,* 1997, 299.

[2] S. V. Bezzateev and N .A. Shekhunova, Binary generalized (L,G) codes that are perfect in a weighted Hamming metric, *Problems of Information Transmission*, **48** (3), 239–242, 2012.

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

[4] M. Grassl ,Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de. Accessed on 2014-06-20.

[5] Chen's tables of quasi-twisted codes,
http://moodle.tec.hkr.se/ chen/research/codes/searchqc2.htm