Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 255-259*

Relation between two classes of binary quasi-cyclic Goppa codes

Sergey Bezzateev bsv@aanet.ru
Natalia Shekhunova sna@delfa.net
Saint Petersburg State University of Airspace Instrumentation
Saint-Petersburg, RUSSIA

Abstract. Two classes of binary quasi-cyclic Goppa codes is considered. True parameters and codeword structure of these codes is proposed.

1 Inroduction

Let us consider the relation between two classes of quasi-cyclic Goppa codes $\Gamma(L, G(x))$ and $\Gamma^*(L^*, G^*(x))$, where

$$G(x) = x^{t-1} + 1, \tag{1}$$

$$G^*(x) = x^{t+1} + 1, \tag{2}$$

$t = 2^l, L \subset GF(2^{2l}), L^* \subset GF(2^{2l})$.

In [1], [2] the true values of parameters for these codes have been obtained. The code $\Gamma(L, G(x))$ has the minimal distance

$$d = 2t - 1 \tag{3}$$

and the number of information symbols is

$$k = t^2 - t - 2l(t - \frac{3}{2}). \tag{4}$$

The code $\Gamma^*(L^*, G^*(x))$ has the minimal distance

$$d^* = 2t + 3 \tag{5}$$

and the number of information symbols is

$$k^* = t^2 - t - 2l(t - \frac{3}{2}) - 1. \tag{6}$$

In this paper we will examine the codeword structure of these classes of the codes and we will show how the codewords from one class $\Gamma(L, G(x))$ can be transformed into the codewords of another class $\Gamma^*(L^*, G^*(x))$.

2 Codeword structure of the binary $\Gamma(L, G(x))$code

It is easy to show that $\Gamma(L, G(x))$ code is the quasi-cyclic code with the length of cycloid $(t-1)$ and number of cycloids t. Moreover, the codewords of this code have one fixed position - $\{0\}$. Therefore the total length of the code is

$$n = t(t-1) + 1 \tag{7}$$

The numerators of the codewords of the $\Gamma(L, G(x))$ code can be represented in the following form:

$$L = \{\beta^i, \beta^i\alpha^{t+1}, \beta^i\alpha^{(t+1)2}, ..., \beta^i\alpha^{(t+1)(t-2)}\}_{i=1,...,t} \bigcup \{0\}, \tag{8}$$

where $\beta = \alpha^{2^l-1} = \alpha^{t-1}$, α is the primitive element of $GF(2^{2l})$, and $\{\beta^i, \beta^i\alpha^{t+1}, \beta^i\alpha^{(t+1)2}, ..., \beta^i\alpha^{(t+1)(t-2)}\}$ are numerators of positions that form the correspondent cycloids.

By using the representation of the set L as (8) it is possible to write the parity check matrix H of the code in the following form:

$$H = \left[\begin{bmatrix} \frac{1}{\beta^{i(t-1)}+1} & \frac{1}{\beta^{i(t-1)}+1} & \cdots & \frac{1}{\beta^{i(t-1)}+1} \\ \frac{\beta^i}{\beta^{i(t-1)}+1} & \frac{\beta^i\alpha^{t+1}}{\beta^{i(t-1)}+1} & \cdots & \frac{\beta^i\alpha^{(t+1)(t-2)}}{\beta^{i(t-1)}+1} \\ . & . & \cdots & . \\ \frac{\beta^{i(t-2)}}{\beta^{i(t-1)}+1} & \frac{\beta^{i(t-2)}\alpha^{(t+1)(t-2)}}{\beta^{i(t-1)}+1} & & \frac{\beta^{i(t-2)}\alpha^{(t+1)(t-2)(t-2)}}{\beta^{i(t-1)}+1} \\ 1 & 1 & & 1 \end{bmatrix}_{i=1,...,t} \begin{bmatrix} 1 \\ 0 \\ \cdots \\ 0 \\ 0 \end{bmatrix}\right] \tag{9}$$

It follows from representation (9) that in any code from the $\Gamma(L, G(x))$ code class only the codewords that have 1 on position $\{0\}$ will be the codewords with the minimal weight $d = 2t - 1$. The codewords with 0 on this position have an even weight and it will be shown that the minimal weight of such codewords is equal to $2t + 4$.

3 Transformation of the codewords from the class $\Gamma(L, G(x))$ into codewords of the class $\Gamma^*(L^*, G^*(x))$

Let us consider now $\Gamma_1(L_1, G(x))$ code obtained as truncated $\Gamma(L, G(x))$ code by information position $\{0\}$, i.e., we remove all codewords with 1 on position $\{0\}$ from $\Gamma(L, G(x))$ code. Then $L_1 = L\backslash\{0\}$ and $\Gamma_1(L_1, G(x))$ code is still quasi-cyclic code with parity check matrix

$$H_1 = \begin{bmatrix} \frac{1}{\beta^{i(t-1)}+1} & \frac{1}{\beta^{i(t-1)}+1} & \cdots & \frac{1}{\beta^{i(t-1)}+1} \\ \frac{\beta^i}{\beta^{i(t-1)}+1} & \frac{\beta^i\alpha^{t+1}}{\beta^{i(t-1)}+1} & \cdots & \frac{\beta^i\alpha^{(t+1)(t-2)}}{\beta^{i(t-1)}+1} \\ . & . & \cdots & . \\ \frac{\beta^{i(t-2)}}{\beta^{i(t-1)}+1} & \frac{\beta^{i(t-2)}\alpha^{(t+1)(t-2)}}{\beta^{i(t-1)}+1} & \cdots & \frac{\beta^{i(t-2)}\alpha^{(t+1)(t-2)(t-2)}}{\beta^{i(t-1)}+1} \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{i=1,\dots,t}$$

Lemma 1 *The rows* $\left[\begin{matrix} \frac{\beta^{i(t-1)}}{\beta^{i(t-1)}+1} & \frac{\beta^{i(t-1)}}{\beta^{i(t-1)}+1} & \cdots & \frac{\beta^{i(t-1)}}{\beta^{i(t-1)}+1} \end{matrix} \right]_{i=1,\dots,t}$ *and* $\left[\begin{matrix} \frac{1}{\beta^i(\beta^{i(t-1)}+1)} & \frac{1}{\beta^i\alpha^{t+1}(\beta^{i(t-1)}+1)} & \cdots & \frac{1}{\beta^i\alpha^{(t+1)(t-2)}(\beta^{i(t-1)}+1)} \end{matrix} \right]_{i=1,\dots,t}$ *can be represented as a linear combination of the correponding rows of the parity check matrix* H_1.

From Lemma 1 we obtain that the matrix H_1 can be rewritten in the following form:

$$H_1 = \begin{bmatrix} \frac{1}{\beta^i(\beta^{i(t-1)}+1)} & \frac{1}{\beta^i\alpha^{t+1}(\beta^{i(t-1)}+1)} & \cdots & \frac{1}{\beta^i\alpha^{(t+1)(t-2)}(\beta^{i(t-1)}+1)} \\ \frac{1}{\beta^{i(t-1)}+1} & \frac{1}{\beta^{i(t-1)}+1} & \cdots & \frac{1}{\beta^{i(t-1)}+1} \\ \frac{\beta^i}{\beta^{i(t-1)}+1} & \frac{\beta^i\alpha^{t+1}}{\beta^{i(t-1)}+1} & \cdots & \frac{\beta^i\alpha^{(t+1)(t-2)}}{\beta^{i(t-1)}+1} \\ . & . & \cdots & . \\ \frac{\beta^{i(t-2)}}{\beta^{i(t-1)}+1} & \frac{\beta^{i(t-2)}\alpha^{(t+1)(t-2)}}{\beta^{i(t-1)}+1} & \cdots & \frac{\beta^{i(t-2)}\alpha^{(t+1)(t-2)(t-2)}}{\beta^{i(t-1)}+1} \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{i=1,\dots,t}$$

Obviously that this matrix is parity check matrix for the code $\Gamma_2(L_2, G_2(x))$ where $G_2(x) = x^t + x$, $L_2 = L_1$. This code is still quasi-cyclic with length of cycloid $t-1$ and the number of cycloids is t, i.e., $n_2 = t(t-1)$.

Theorem 1 *The minimal distance of* $\Gamma_2(L_2, G_2(x))$ *code is* $d_2 = 2t+4$ *and number of information symbols is* $k_2 = k_1 - 1$.

Lemma 2 $L_2 = \{GF(2^{2l})\} \backslash \{\{\alpha^{(t+1)i}, i = 0, ..., t-2\} \bigcup \{0\}\}$.

Let us consider now the following substitution: $x \longrightarrow z + \gamma$, where $\gamma \in GF(2^{2l})$ and $\gamma^t + \gamma + 1 = 0$. Then $G_2(x) = x^t + x = z^t + \gamma^t + z + \gamma = z^t + z + 1 = G_3(x)$.

Now, to proceed from the class $\Gamma(L, G(x))$ in to the class $\Gamma^*(L^*, G^*(x))$ let us prove the following statement.

Lemma 3 *There exist* t *different elements* $\gamma \in GF(2^{2l})$ *such that* $\gamma^t + \gamma + 1 = 0$ *where* $t = 2^l$.

Proof. Let us choose some element $\varpi_j \in GF(2^{2l})$ and let $\varpi_j^t + \varpi_j + 1 = \tau \neq 0$, then obviously, that $\tau \in GF(2^l)$. Indeed $\tau^{2l} = \varpi_j^{t2^l} + \varpi_j^{2^l} + 1 = \varpi_j^t + \varpi_j + 1 = \tau$. Therefore $\tau^{2l} = \tau$ and $\tau \in GF(2^l)$. It is easy to show that for any nonzero element τ there exists t different values ϖ_j such that $\varpi_j^t + \varpi_j + 1 = \tau$. Then, as the number of nonzero elements τ from $GF(2^l)$ is $2^l - 1$, we will have $N = (2^l - 1)t$ elements $\varpi_j \in GF(2^{2l})$ such that $\varpi_j^t + \varpi_j + 1 \neq 0$. $N = (2^l - 1)2^l = 2^{2l} - 2^l$.

Therefore in the field $GF(2^{2l})$ $\theta = 2^l$ elements ϖ_j such that $\varpi_j^t + \varpi_j + 1 = 0$ can be found. □

If we will choose one of these ϖ_j as γ then $\gamma^t + \gamma + 1 = 0$. It is easy to show that L_3 can be represented as:

$$L_3 = \{\beta^i + \gamma, \beta^i \alpha^{t+1} + \gamma, \beta^i \alpha^{(t+1)2} + \gamma, ..., \beta^i \alpha^{(t+1)(t-2)} + \gamma\}_{i=1,...,t}$$

Moreover, as $\gamma : G_2(\gamma) = 1$, i.e., element γ is not a root of the $G_2(\gamma)$, then accoding to the Lemma 2 there exist i, j such that :

$$\beta^i \alpha^{(t+1)j} = \gamma,$$

This means that in the set L_3 we have one cycloid with element $\{0\}$. In the set L_3 it is also exist element $\{1\}$, as $G_3(1) \neq 0$.

Obviously, the code $\Gamma_3(L_3, G_3(x))$ has parameters

$$\begin{aligned} n_3 &= t(t-1), \\ k_3 = k_2 &= k_1 - 1 \text{ and} \\ d_3 &= 2t + 4. \end{aligned}$$

Let us consider now $\Gamma_3^*(L_3^*, G_3(x))-$code obtained from $\Gamma_3(L_3^*, G_3(x))$-code by trancation on position $\{0\}$, i.e., $L_3^* = L_3 \backslash \{0\}$.
The code $\Gamma_3^*(L_3^*, G_3(x))$ has parameters:

$$n_3^* = n_3 - 1, \quad k_3^* = k_3 = k_2 = k_1 - 1, \quad d_3^* = d_3 - 1 = d_2 - 1 = 2t + 3.$$

Now let us use the following substitution: $z \longrightarrow \frac{1}{y}$. Then

$$G_3(z) = z^t + z + 1 = y^{-t} + y^{-1} + 1 \longrightarrow G_4(x) = y^t + y^{t-1} + 1.$$

The set L_4^* can be defined as a set of elements of $GF(2^{2l})$ that are inverse by multiplication to the elements of set L_3^*.

$$L_4^* = \{(\beta^i + \gamma)^{-1}, (\beta^i \alpha^{t+1} + \gamma)^{-1}, (\beta^i \alpha^{(t+1)2} + \gamma)^{-1}, ..., (\beta^i \alpha^{(t+1)(t-2)} + \gamma)^{-1}\}_{i=1,...,t}.$$

Code $\Gamma_4^*(L_4^*, G_4(x))$ has parameters

$$\begin{aligned} n_4^* &= n_3^* = n_3 - 1, \\ k_4^* &= k_3^* \text{ and} \\ d_4^* &= d_3 - 1. \end{aligned}$$

Lemma 4 *Code* $\Gamma_4^*(L_4^*, G_4(x)) \equiv \Gamma_5^*(L_5^*, G_5(x))$, *where* $G_5(y) = yG_4(y) = y^{t+1} + y^t + y$ *and* $L_5^* = L_4^*$.

Let us use the following substitution: $y \longrightarrow u + 1$, then

$$G_5(y) = y^{t+1} + y^t + y \longrightarrow (u+1)^{t+1} + (u+1)^t + u = u^{t+1} + 1 = G_6(y).$$

$$L_6 = \{(\beta^i+\gamma)^{-1}+1, (\beta^i\alpha^{t+1}+\gamma)^{-1}+1, (\beta^i\alpha^{(t+1)2}+\gamma)^{-1}+1, ..., (\beta^i\alpha^{(t+1)(t-2)}+\gamma)^{-1}+1\}_{i=1,...,t}$$

From Lemma 2 and the above obtained result about the existence of the element $\{1\}$ in the set L_3 it is obvious that the element $\{0\}$ will appear in set L_6.

Theorem 2 *The class of binary* $\Gamma_6(L_6, G_6(x))$ *codes is the class of binary quasi-cyclic* $\Gamma^*(L^*, G^*(x))$ *codes with Goppa polynomial defined by formula (2) and locator set* $L^* = L_6$.

Any codeword of this code is formed by $(t-2)$ cycloids of the length $t+1$ and one fixed position $\{0\}$.

$\Gamma^*(L^*, G^*(x))$ codes have the following parameters:

$$\begin{aligned} n^* = n_6 = n_5 = n_4^* = n_3 - 1 = t(t-1) - 1, \\ k^* = k_6 = k_5 = k_4^* = k_3^* = k - 1, \\ d^* = d_6 = d_5 = d_3^* = d_3 - 1 = 2t + 3. \end{aligned} \tag{10}$$

Let us write for the sequence of the accomplished transformations: $x \to z+\gamma \to \frac{1}{y} + \gamma \to \frac{1}{u+1} + \gamma$. Therefore $u = \frac{1}{x+\gamma} + 1 = (x+\gamma)^{-1} + 1$.

4 Conclusion

As it was shown above the codewords from the class of the binary quasi- cyclic $\Gamma_1(L_1, G_1(x))$-codes with cycloid length $(t-1)$ and cycloid number t and the fixed position $\{0\}$ can transformed into the class of the binary quasi-cyclic $\Gamma^*(L^*, G^*(x))$-codes with the cycloid length $(t+1)$ and cycloid number $(t-1)$ and fixed position $\{0\}$ by the sequence of simple transformations. The true values for parameters of these codes are defined by formulas (3), (4), (7) and (5), (6), (10) respectively.

References

[1] S. Bezzateev, N. Shekhunova, Subclass of binary Goppa codes with minimal distance equal to the design distance, *IEEE Trans. Inform. Theory* 41, 1995, 554-555.

[2] P. Veron, True dimension of some binary quadratic trace Goppa codes, *Des., Codes Crypt.* 24, 2001, 81-97.