数理解析研究所講究録
1038 巻 1998 年 223-229

A Class of Generalized Cyclic Codes[1)]

Zhuojun Liu (zliu@mmrc.iss.ac.cn)
Institute of Systems Science, Academia Sinica
Beijing 100080, P. R. China

1. Introduction

Prange was considered to be first people to study cyclic codes in the end of 1950s, see [3] and [8]. Since then, cyclic codes are the most studied of all codes, because they are easy to encode, and include an important family of BCH codes. A code C is cyclic if it is linear and if any cyclic shift of a codeword is also a codeword, i.e., whenever $(c_0, c_1, ..., c_{n-1})$ is in C then so is $(c_{n-1}, c_0, ..., c_{n-2})$. In fact, one could define a cyclic code to be an ideal in the ring of polynomial modulo $x^n - 1$. Equivalently, a cyclic code of length n over F_q consists of all multiples of a generator polynomial $g(x)$, which is the monic polynomial of least degree in the code, and is a divisor of $x^n - 1$. That means each cyclic code of length n will correspond to a factor of $x^n - 1$ over F_q. Therefore, the number of cyclic codes, usually is restricted quite a lot, especially we always assume that n and q are relatively prime.

Instead of $x^n - 1$, by considering any polynomial $f(x)$ of degree n over F_q, we could construct a class of linear codes, one special case of which is cyclic code. We may as well call them to be the generalized cyclic codes, denoted by GCC.

2. GCC Construction

Suppose F_q to be a finite field, and by $F_q[x]$ we denote the set of polynomial in x with coefficients from F_q. It is well known that $R_n = F_q[x]/(x^n - 1)$ is a principle ideal ring, which consists of the residue classes of $F_q[x]$ modulo $x^n - 1$. We associate with the vector $c = (c_0, c_1, ..., c_{n-1})$ in F_q^n the polynomial $c(x) = c_0 + c_1 x + ... + c_{n-1}x^{n-1}$ in R_n. The map

$$\phi : c_0 + c_1 x + ... + c_{n-1}x^{n-1} \longrightarrow (c_0, c_1, ..., c_{n-1}) \tag{1}$$

defines a 1–1 corresponding between R_n and F_q^n. Now, we want to consider more general polynomial $f(x)$ of degree n over $F_q[x]$ rather than $x^n - 1$. Let

$$f(x) = f_0 + f_1 x + ... + f_n x^n.$$

1) This work was supported by the Climbing Project Fundation of P.R. China.

We always assume $f_n \neq 0$ in this paper. Define $R_n(f) = F_q[x]/f$ as the set of the residue classes of $F_q[x]$ modulo f. Similar with the discussion to R_n(cf [8]), we can show $R_n(f)$ forms a principle ideal ring. Clearly $R_n(f)$ is a ring with the operations of $+$ and $*$ under the modulo $f(x)$. Given any ideal I of $R_n(f)$, we select the monic polynomial $g(x)$ of the least degree in I. Then for any $c(x) \in I$, we calculate the remainder

$$c(x) = u(x) * g(x) + r(x),$$

where degree$(g(x))$ > degree$(r(x))$. According to the selection of $g(x)$, it must be $r(x) = 0$, namely

$$c(x) = u(x) * g(x). \tag{2}$$

So, I is a principle ideal. That implies $R_n(f)$ is a principle ideal ring. It is easy to know $g(x)$ is a divisor of $f(x)$, since $f(x) \in R_n(f)$ satisfies (2). On the other hand, for any factor $g(x)$ of $f(x)$, we define I to be a subset of $R_n(f)$ consisting of all multiples of $g(x)$, denoted by $I = < g(x) >$. It is not hard to see I is an ideal of $R_n(f)$. Of course, we can also establish a 1–1 corresponding between $R_n(f)$ and F_q^n, just like (1), still denoted by ϕ.

Definition 2..1 A linear code of length n over F_q with the generating matrix

$$G_{n-r,n} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & & g_r & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & & g_r & 0 \\ & & & & \cdots & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & & g_r \end{pmatrix} \tag{3}$$

is called a generalized cyclic code(GCC), provided $g_r = 1$.

In fact, for any given polynomial $g(x) \in F_q[x]$ of degree $r(\leq n)$ with $g_r = 1$, there always exists a polynomial $f(x) \in F_q[x]$ of degree n, such that $g(x)$ is a divisor of $f(x)$, and $f_n \neq 0$. We have

Lemma 2..1 Suppose $I = < g(x) > \subset R_n(f)$, in which $g(x)$ is a monic polynomial of degree r. Then $\phi(I)$ is an $n - r$ dimensional subspace of F_q^n.

Proof. Let $k = n - r$. For any $c(x) \in I$, according to (2), we have

$$\begin{aligned} c_0 + c_1x + ... + c_{n-1}x^{n-1} &= (u_0 + u_1x + ... + u_{k-1}x^{k-1})(g_0 + g_1x + ... + g_rx^r) \\ &= (u_0, u_1, ..., u_{k-1}) \begin{pmatrix} g \\ xg \\ ... \\ x^{k-1}g \end{pmatrix} \end{aligned}$$

Combining with (3), this implies

$$(c_0, c_1, ..., c_{n-1}) = (u_0, u_1, ..., u_{k-1}) \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & & g_r & \cdots & 0 \\ & & & \cdots & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & & \cdots & g_r \end{pmatrix}$$

Because of $g_r = 1$, we have proved $\phi(I)$ is a k dimensional subspace of F_q^n. □

Since Lemma 2..1, we usually associate $< g(x) >$ a linear code of $[n, n-r]_q$, provided $g(x) \in F_q[x]$ with degree r and $g_r = 1$. This corresponding GCC, according to Definition 2..1, is also said to be generated by $g(x)$. Furthermore, according to (2), $g(x)$ is called a generator polynomial, $u(x)$ a message polynomial, $c(x)$ a codeword polynomial. Obviously, any cyclic code of length n must be a GCC. Meanwhile, GCC can significantly give more linear codes.

Theorem 2..2 For any $n \geq k$, there exist q^r GCC with parameters of $[n, n-r]_q$.

Proof. Clearly, in $F_q[x]$, there are exact q^r different polynomials in the following form

$$g(x) = g_0 + g_1 x + ... + g_{r-1}x^{r-1} + x^r. \tag{4}$$

Now, suppose $b(x)$ is another monic polynomial of degree r. Below, we only need to prove $< g(x) > \neq < b(x) >$, if $g(x) \neq b(x)$. However, this is clearly true. Otherwise, $< g(x) > = < b(x) >$ implies $b(x) \in < g(x) >$. By (2), it must be $b(x) = g(x)$. □

3. Some Applications of GCC

Double-Byte Error-Correcting codes are great important since their significant application to computer industry. By a theorem(theorem 3.1 in [1]), we know there exists a linear code of $[9, 2, \geq 5]_3$. Here, GCC can give more support to [1]. In fact, according to Theorem 2..2, there exist $3^5 = 243$ GCCs of $[9, 4]_3$. By a searching algorithm described in Section 4, one can find four of them have the minimum distance of 5. They are generated by

$x^5 + 2x^3 + x^2 + 2x + 2$,
$x^5 + 2x^3 + 2x^2 + 2x + 1$,
$x^5 + x^4 + 2x^3 + x^2 + 2$,
$x^5 + 2x^4 + 2x^3 + 2x^2 + 1$

respectively. The corresponding generating matrix are

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 2 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 2 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 2 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 2 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 2 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 2 & 0 & 1 \end{pmatrix}$$

On the other hand, since 9 and 3 are not relatively prime, there does not exist cyclic codes with $n = 9$ over F_3 at all. If we remove the limitation that q and n are relatively prime,

we can only get a cyclic code $[9,4,3]_3$ generated by $(x+2)^5$, which is clearly a factor of $x^9-1=(x+2)^9 \bmod 3$. For the following discussion, we need to define

$$D_q(n,k) = \max\{d \mid \text{there is a GCC of } [n,k,d]_q\}.$$

Proposition 3..1 $D_q(n,k) \geq D_q(n+1,k+1)$.

Proof. Suppose $g(x)$ is the generator of a GCC of $[n+1,k+1,D_q(n+1,k+1)]_q$. Its generator matrix will have the form,

$$G_{k+1,n+1} = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ & & & & & & \\ 0 & & & G_{k,n} & & & \end{pmatrix}$$

Clearly, the minimum distance decided by $G_{k,n}$ is at least $D_q(n+1,k+1)$. So, $D_q(n,k) \geq D_q(n+1,k+1)$. □

Proposition 3..2 For any $2^m > n > 2m$, there exists a GCC of $[n, n-2m, \geq 5]_2$.

Proof. We recall a well known results about double-error-correcting BCH code(for example, see page 193 in [8]):

$$g(x) = M^{(1)}(x)M^{(3)}(x)$$

generates a cyclic code of

$$[2^m-1, 2^m-1-2m, \geq 5]_2, m \geq 3,$$

where degree$(g(x)) = 2m$. In addition, for α, a primitive element of F_{2^m},

$$M^{(1)}(\alpha)M^{(3)}(\alpha) = 0.$$

By Proposition 3..1, we have

$$D(n, n-2m) \geq D(2^m-1, 2^m-1-2m) \geq 5,$$

for all $2^m - 1 \geq n > 2m$. Thus we have proved our proposition. □

Now, let us consider a MacWilliams problem(page 184 in [8]): How close can one get: is there a $[90,77,5]_2$ code?

Since $2^7 > 90 > 14$, by Proposition 3..2, we can find a GCC with parameters of $[90,76,\geq 5]_2$. However, we will see there are only cyclic codes of $[90,76,\leq 4]_2$ when we don not insist the condition that n and q have to be relatively prime. Since over F_2, we have irreducible factorization

$$\begin{aligned}
x^{90}-1 &= (x^{12}+x^9+1)^2(x^{12}+x^3+1)^2(x^6+x^3+1)^2(x^4+x^3+1)^2(x^4+x+1)^2 \\
&\quad (x^4+x^3+x^2+x+1)^2(x^2+x+1)^2(x+1)^2 \\
x^{45}-1 &= (x^{12}+x^9+1)(x^{12}+x^3+1)(x^6+x^3+1)(x^4+x^3+1)(x^4+x+1) \\
&\quad (x^4+x^3+x^2+x+1)(x^2+x+1)(x+1) \\
x^{15}-1 &= (x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x+1) \\
x^9-1 &= (x^6+x^3+1)(x^2+x+1)(x+1)
\end{aligned}$$

It is not hard to know all factors of $x^{90}-1$ with degree 14 will be a factor either of

$$(x^{45}-1)(x^{15}-1) = x^{60}+x^{45}+x^{15}+1$$

or

$$(x^{45}-1)(x^{9}-1) = x^{54}+x^{45}+x^{9}+1$$

So, any cyclic codes of $[90,76]_2$ must contain $x^{60}+x^{45}+x^{15}+1$ or $x^{54}+x^{45}+x^{9}+1$ as a codeword polynomial. This shows its minimum distance is at most 4.

4. Comparison of GCC and Cyclic Codes for n = 27

In previous sections, we have seen GCC can give better parameters, say d, relatived to cyclic codes. The idea to get GCC is simple, the method to construct GCC is straightforward. Below is the outline description of a searching algorithm for GCC.

Algorithm 4..1 $D(n,k,p,g(x))$: Algorithm to decide the minimum distance.

Input : n,k,p(a prime), $g(x)$(a generator polynomial);

Output : d, the minimum distance for a given GCC generated by $g(x)$.

Step 1) Construct a generating matrix $G_{k,n}$ from $g(x)$.

Step 2) By seeing all possible codewords to decide d.

Stop. □

Algorithm 4..2 Searching Algorithm for GCC.

Input : n,k,p;

Output : $D_p(n,k)$ and the number of corresponding GCCs.

Step 0)[initial1] Set d1 = 1, N = 0.

Step 1)[initial2] Set PS = all polynomial in $F_p[x]$ with degree $n-k$.

Step 2)[selecting] Select a $g(x)$ from PS, then set $PS = PS - \{g\}$.

Step 3)[deciding d] $d = D(n,k,p,g(x))$.

Step 4)[counting] If $d > d1$ then {d1 = d, N = 1} else if d = d1 then N = N + 1.

Step 5)[continue?] If PS not empty then goto Step 2 else {output N and d}.

Stop. □

We would like to give thorough computations for $n = 27$ to compare the behavior between cyclic codes and GCC for binary case.

k	$D_{cc}(k)$	$N(k, D_{cc}(k))$	$D_{gcc}(k)$	$N(k, D_{gcc}(k))$
1	27	1	27	1
2	18	1	18	23410
3	9	1	15	49000
4	-	0	14	11340
5	-	0	13	320
6	6	1	12	2825
7	6	1	12	12
8	6	1	10	3474
9	3	1	9	379
10	-	0	8	12952
11	-	0	8	1388
12	-	0	8	16
13	-	0	7	2
14	-	0	6	1203
15	-	0	6	283
16	-	0	6	27
17	-	0	5	17
18	2	1	4	185
19	2	1	4	70
20	2	1	4	20
21	2	1	4	10
22	-	0	3	6
23	-	0	2	8
24	2	1	2	4
25	2	1	2	2
26	2	1	2	1
27	1	1	1	1

Fig. 1. Comparison between binary cyclic codes and GCC with n = 27.

In Fig.1, $D_{cc}(k)$ means the best minimum distance of k dimensional binary cyclic code. $N(k, D_{cc}(k))$ is the number of k dimensional binary cyclic codes with minimum distance $D_{cc}(k)$. Notice, since there is no cyclic codes at all for some k, the corresponding $D_{cc}(k)$ has no definition and $N(k, D_{cc}(k)) = 0$. Similarly, we define $D_{gcc}(k)$ as the best minimum distance of k dimensional binary GCC, $N(k, D_{gcc}(k))$ as the number of the possible k dimensional GCC with minimum distance of $D_{gcc}(k)$.

The experiments show GCC can work much better than cyclic codes.

5. Conclusion and Acknowledgement

With the observation of selecting more general polynomial of degree n instead of $x^n - 1$,

we presented a method to construct a class of generalized cyclic codes.

The research at this stage shows GCC is much better than cyclic codes. Meanwhile there are still many questions to be worth of answering for GCC. For example, is GCC a class of good linear codes? Can we find an efficient decoding algorithm for GCC?

The author wishes to acknowledge the discussion with Hong DU and Changyan DI while preparing the manuscript. Thanks also to Gui Liang FENG for his suggestion to write this paper and to Fujio Kako to arrange my visiting Japan under the supporting from JSPS.

参 考 文 献

[1] G. L. Feng, X. W. Wu and T. R. N. Rao, "New Double-Byte Error-Correcting Codes for Memory Systems," Proceedings of 1997 IEEE International Symposium on Information Theory, Ulm, Germany, 1997.

[2] V. D. Goppa, "Geometry and Codes," in *Mathematics and its Application*, vol. 24. Dordrecht, The Netherlands:Kluwer, 1991.

[3] E. Prange, "The use of information sets in decoding cyclic codes," IEEE Tran. Info. Theory, 8(5), 1962.

[4] M. A. Tsfasman, S. G. Vlădut, "Algebraic-Geometric Codes," in *Mathematics and its Applications*, vol. 58. Dordrecht, The Netherlands:Kluwer, 1991.

[5] J. H. Van Lint, "Algebraic geometric codes," in *Coding Theory and Design Theory*, vol. 20(IMA Volumes in Mathematics and its Application). NewYork:Springer-Verlag, 1988, pp. 137-162.

[6] J. H. Van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry*, DMV Seminar vol. 12, Birkhäuser Verlag, Basel Boston Berlin, 1990.

[7] Zhe Xian WAN, "Algebra and Coding theory", Scientific Press, Beijing 1980 (in Chinese).

[8] F.J. MacWilliams, N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland Publishing Company, 1977.