論 文

GMW CODES

Jong-Seon No* *Regular Member*

GMW 부호

正會員 盧 宗 善*

ABSTRACT

In this paper, new binary cyclic codes(hereafter, refered to as *GMW codes*) which are generated by using GMW sequence, $g(t)=tr_1^J\{[tr_J^K(\alpha^t)]^r\}$, and its cyclic shifts are introduced. Code length of GMW codes is 2^K-1, where K is composite integer, $e\cdot J$. Dimension of the GMW codes is $K\cdot(K/J)^{w-1}$, where w is a Hamming weight of r. Several properties of GMW codes such as designed distance, minimum distance, and weights of codewords are obtained in terms of parameters of GMW sequences. And expansion of GMW sequences in terms of m-sequence and its decimation sequences are introduced and characteristic polynomials of GMW sequences are also derived.

요 약

본논문에서는 GMW시퀀스 $g(t)=tr_1^J\{[tr_J^K(\alpha^t)]^r\}$와 그의 순회 천이 시퀀스에의해서 발생되는 GMW 부호라는 새로운 이진순회부호가 소개되었다. GMW부호의 부호길이는 2^K-1인데 여기서 K는 복합정수 $e\cdot J$이다. GMW부호의 차원은 $K\cdot(K/J)^{w-1}$인데, 여기서 w는 r의 해밍무게이다. 디자인 거리, 최소거리, 그리고 부호의 무게가 GMW시퀀스의 변수에의해 유도되었다. 그리고 GMW 시퀀스의 확장이 m 시퀀스와 그의 순회 천이 시퀀스들의 견지에서 유도되었고, GMW시퀀스의 특성 다항식이 유도되었다.

I. INTRODUCTION

Recently, it is known that cyclic codes can be generated by using pseudorandom sequences, such as m-sequences, Gold sequences, Kasami sequences.

*建國大學校 電子工學科
Dept. of Elec. Eng. Kon-Kuk Univ.
論文番號 : 93-116

We present new binary cyclic codes, GMW codes, which are generated by using GMW sequence[5],

$$g(t)=tr_1^J\{[tr_J^K(\alpha^t)]^r\}. \tag{1}$$

and its cyclic shifts

$$g(t+\tau),=tr_1^J\{[tr_J^K(\alpha^{t+\tau})]^r\},\ 1\le\tau\le 2^K-2, \tag{2}$$

where K is composite integer, $e\cdot J$. Code length of GMW codes is 2^K-1 and dimension of the GMW codes is $K\cdot(K/J)^{w-1}$, where w is the Hamming weight of r in the binary expression. Several properties of GMW codes such as designed distance, minimum distance, and Hamming weights of codewords are obtained in terms of parameters of GMW sequences.

Expansion of GMW sequences in terms of m-sequence and its decimation sequences are introduced and characteristic polynomials of GMW sequences are also introduced in Section II. The definitions of GMW codes and nonnull spectrum of GMW codes are given in Section III. The dimension of GMW codes is also defined here. In Section IV, the designed distance, minimum distance, and Hamming weight of GMW codes are derived.

II. EXPANSIONS OF GMW SEQUENCES

Let K be a composite integer, let J divide K and set $e=K/J$. Under these circumstances, the sequence

$$g(t)=tr_1^J\{[tr_J^K(\alpha^t)]^r\},\ 0\le t\le 2^K-2, \tag{3}$$

is a binary GMW sequence of period $N=2^K-1$, where for any pair of integers m, n, m/n, $tr_m^n(\cdot)$ is the trace function[3] defined by

$$tr_m^n(x)=\sum_{i=0}^{\frac{n}{m}-1}x^{2^{im}} \tag{4}$$

Let α be a primitive element of $GF(2^K)$. Let r, $1\le r<2^J-1$, be relatively prime to 2^J-1 and let the binary representation of r have Hamming weight w. Without loss of generality, r may be expressed in the form

$$r=2^{l_0}+2^{l_1}+2^{l_2}+\cdots+2^{l_{w-1}}, \tag{5}$$

where $0=l_0<l_1<l_2<\cdots<l_{w-1}<J$. The linear span L of the GMW sequence $g(t)$ in (3) is then given by[5]:

$$L=K\cdot\left(\frac{K}{J}\right)^{w-1}. \tag{6}$$

Using(5), the GMW sequences can be represented by summation of m-sequence and its decimation sequences as follows:

THEOREM 1: The GMW sequence $g(t)$ defined in (3) has the expansion

$$tr_1^J\{[tr_J^K(\alpha^t)]^r\}=\sum_{i_0=0}^{e-1}\sum_{i_1=0}^{e-1}\cdots\sum_{i_{w-1}=0}^{e-1}tr_1^K(\alpha^{A\cdot t}), \tag{7}$$

where α is a primitive element of $GF(2^K)$ and

$$A=A(i_1,i_2,\cdots,i_{w-1})=1+2^{l_1+J\cdot i_1}+2^{l_2+J\cdot i_2}+\cdots+2^{l_{w-1}+J\cdot i_{w-1}}. \tag{8}$$

PROOF: Using the binary representation of r in (5), the GMW sequence can be rewritten as

$$\begin{aligned}
g(t)&=tr_1^J\{[tr_J^K(\alpha^t)]^r\}\\
&=tr_1^J\{[tr_J^K(\alpha^t)]^{(2^{l_0}+2^{l_1}+2^{l_2}+\cdots+2^{l_{w-1}})}\}\\
&=tr_1^J\left\{\prod_{j=0}^{w-1}[tr_J^K(\alpha^t)]^{2^{l_j}}\right\}\\
&=tr_1^J\left\{\sum_{j_0=0}^{e-1}\sum_{j_1=0}^{e-1}\cdots\sum_{j_{w-1}=0}^{e-1}\right.\\
&\qquad\left.\alpha^{t\cdot 2^{(l_0+J\cdot j_0)}+2^{(l_1+J\cdot j_1)}+2^{(l_2+J\cdot j_2)}+\cdots+2^{(l_{w-1}+J\cdot j_{w-1})}}\right\}\\
&=\sum_{i_0=0}^{e-1}\sum_{i_1=0}^{e-1}\cdots\sum_{i_{w-1}=0}^{e-1}tr_1^J\left\{\sum_{j=0}^{e-1}\right.\\
&\qquad\left.\alpha^{t\cdot 2^{J\cdot j_0}\cdot(1+2^{(l_1+J\cdot i_1)}+2^{(l_2+J\cdot i_2)}+\cdots+2^{(l_{w-1}+J\cdot i_{w-1})})}\right\}\\
&=\sum_{i_0=0}^{e-1}\sum_{i_1=0}^{e-1}\cdots\sum_{i_{w-1}=0}^{e-1}tr_1^J\left\{\sum_{j=0}^{e-1}\right.
\end{aligned}$$

$$\alpha^{t\cdot 2^{J\cdot j_0}\cdot(1+2^{(l_1+J\cdot i_1)}+2^{(l_2+J\cdot i_2)}+\cdots+2^{(l_{w-1}+J\cdot i_{w-1})})}\Big\}$$

$$=\sum_{i_1=0}^{e-1}\sum_{i_2=0}^{e-1}\cdots\sum_{i_{w-1}=0}^{e-1} tr_1^J\left\{tr_J^K\right.$$

$$\left.\left(\alpha^{(1+2^{(l_1+J\cdot i_1)}+2^{(l_2+J\cdot i_2)}+\cdots+2^{(l_{w-1}+J\cdot i_{w-1})})\cdot t}\right)\right\}$$

$$=\sum_{i_1=0}^{e-1}\sum_{i_2=0}^{e-1}\cdots\sum_{i_{w-1}=0}^{e-1} tr_1^K$$

$$\left(\alpha^{(1+2^{(l_1+J\cdot i_1)}+2^{(l_2+J\cdot i_2)}+\cdots+2^{(l_{w-1}+J\cdot i_{w-1})})\cdot t}\right)$$

$$=\sum_{i_1=0}^{e-1}\sum_{i_2=0}^{e-1}\cdots\sum_{i_{w-1}=0}^{e-1} tr_1^K(\alpha^{A\cdot t}).$$

q.e.d.

The powers of α^t appearing on the righthand side of (7) can be shown to be all distinct thus leading to :

COROLLARY 1 : The characteristic polynomial $Q(z)$ of the sequence $g(t)$ in (3) has the expression

$$Q(z)=\prod_{i_1=0}^{e-1}\prod_{i_2=0}^{e-1}\cdots\prod_{i_{w-1}=0}^{e-1} M_{\alpha^{-A}}(z), \tag{9}$$

where α is a primitive element of $GF(2^K)$ and $M_{\alpha^{-A}}(z)$ is the minimal polynomial of α^{-A} over $GF(2)$.

Ⅲ. DEFINITION OF GMW CODES

Using the definition of GMW sequences in (3) and properties of GMW sequences, GMW codes can be defined as follows :

DEFINITION 1 : We define the GMW code $\underline{G}$ to be the linear cyclic code generated by the GMW sequence $g(t)$ and its cyclic shifts, i.e.,

$$\underline{G}=\langle g(t),\ g(t+1),\ g(t+2),\cdots,g(t+2^K-2)\rangle, \tag{10}$$

where addition of arguments is carried out *mod* 2^K-1 and the notation $\langle\ \rangle$ means the all possible linear combinations of all elements in $\langle\ \rangle$.

□

That is, any codeword $c(t)$ in the GMW code defined in (10) can be expressed as

$$c(t)=\sum_{\tau=0}^{2^K-2} c_\tau\cdot g(t+\tau) \tag{11}$$

where c_τ is in $\{0, 1\}$.

The *null spectrum* of a cyclic code is a useful tool in estimating the minimum distance of the code and may be defined as follows :

Let $\underline{C}$ be any cyclic code of length N and $a(t)$ be any codeword in $\underline{C}$. Then one may define the *Fourier transform* $\{\hat{a}(\lambda)\mid 0\le\lambda\le N-1\}$ of $a(t)$ as follows :

$$\hat{a}(\lambda)=\sum_{t=0}^{N-1} a(t)\cdot\beta^{\lambda\cdot t}, \tag{12}$$

where β be an element of order N in some extension field of $GF(2)$.

The null spectrum Ω of the code $\underline{C}$ is then defined in terms of the Fourier transform coefficient $\hat{a}(\lambda)$, $a(\cdot)\in\underline{C}$ as follows :

$$\Omega=\{\lambda\mid\hat{a}(\lambda)=0,\ \forall\ a(t)\in\underline{C}\}. \tag{13}$$

The nonnull spectrum Ω^c of the code $\underline{C}$ is then simply the complement of Ω, i.e.,

$$\Omega^c=\{\lambda\mid 0\le\lambda\le N-1,\ \lambda\notin\Omega\}. \tag{14}$$

For any odd integer N, the integers *mod* N may be divided into equivalence classes simply by defining two elements to be equivalent if their ratio is a power of 2, i.e.,

$$x\equiv y \text{ iff } x=2^j\cdot y(mod\ N). \tag{15}$$

These equivalence classes are called cyclotomic cosets and we use C_i to denote the cyclotomic coset that contains the integer i. The cyclotomic coset, C_A, in $GF(2^K)$ is given by :

$$C_A=\{a_i\mid a_i=-A\cdot 2^i\ mod(2^K-1),\ \forall i\}. \tag{16}$$

It is wellknown that $\forall i$, α^{a_i} has the same minimal polynomial over $GF(2)$, where α is the primitive element of $GF(2^K)$.

In terms of this notation, the null spectrum of the GMW code $\underline{G}$ described above may after some work be shown to be union of certain cyclomic cosets :

THEOREM 2 : The nonnull spectrum Ω^c of the GMW code $\underline{G}$ generated by the GMW sequence $g(t)$ in (3) is given by

$$\Omega^c = \bigcup_{\forall i_1, i_2, \cdots, i_{w-1}} C_{-A},\ 0 \le i_j \le e-1 \text{ for } 1 \le j \le w-1, \quad (17)$$

where $A = A(i_1, i_2, \cdots, i_{w-1})$

$= 1 + 2^{i_1 + J \cdot i_1} + 2^{i_2 + J \cdot i_2} + \cdots + 2^{i_{w-1} + J \cdot i_{w-1}}$ as before.

The dimension of a linear cyclic code is simply the number of elements contained in the nonnull spectrum of code. Therefore, the dimension of GMW code in (3) can be easily given without proof :

THEOREM 3 : The dimension of the GMW code generated by the GMW sequence $g(t)$ in (3) equals $K \cdot (K/J)^{w-1}$.

This is a simple consequence of the fact that the linear span of the GMW sequence equals $K \cdot (K/J)^{w-1}$.

Ⅳ. PROPERTIES OF GMW CODES

By treating the GMW codes as a cyclic code, one may talk about the *designed distance*[3] of the code, *viz*, the largest number of consecutive elements in its null spectrum and this is the content of THEOREM 4 :

THEOREM 4 : The designed distance δ of the cyclic GMW code $\underline{G}$ defined in (10) is given by

$$\delta = 2^K - 1 + f_{min} - f_{max}, \quad (18)$$

where f_{min} and f_{max} are the minimum and maximum elements in the nonnull spectrum Ω^c of the code, $\underline{G}$.

PROOF : The binary representation of any element of Ω^c can be expressed as $e \times J$ matrix form. Thus, we can assume that f_{max} can be given in the binary representation as

$$f_{max} = A + (2^{K-v} + 2^{K-v+1} + 2^{K-v+2} + \cdots + 2^{K-1}), \quad (19)$$

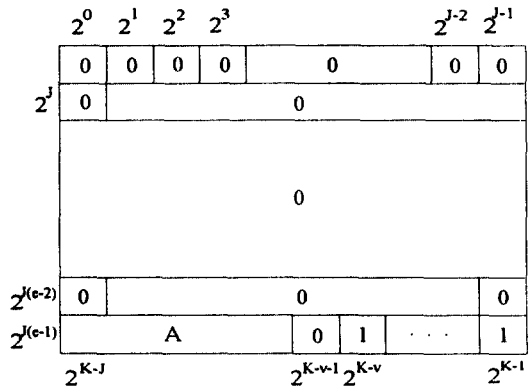

Fig 1. Binary Representation of f_{max} in the Matrix Form.

where v is the largest runlength of "1" in f_{max} and clearly, it is located in the last most significant location in the binary representation and all "1" of r are located in the last row, which is described in Fig.1.

Then,

$$\delta > N - f_{max} = \sum_{i=0}^{K-J-1} 2^i + \bar{A}, \quad (20)$$

where $\bar{A}$ means 1's complement of A. Clearly,

$$\delta > N - f_{max} > 2^{K-v-1}. \quad (21)$$

Assume that

$$\exists\ \delta' = f_u - 1 - f_l \text{ such that } \delta' > \delta \text{ and } f_u, f_l \in \Omega^c. \quad (22)$$

We have to disprove the above statement as given below ;

(i) Assume that some "1" bit of f_u is 2^i, $J \le i \le$

$K-v-1$. We can choose f_s by the columnwise shift of 2^i from f_u in the matrix form. Then

$$f_s = f_u - 2^i + 2^{i-J},\ f_s \in \Omega^c,\ f_s \le f_l \tag{23}$$

and

$$\delta' = f_u - 1 - f_l \le f_u - 1 - f_s = 2^i - 2^{i-J} - 1 < 2^{K-v-1}. \tag{24}$$

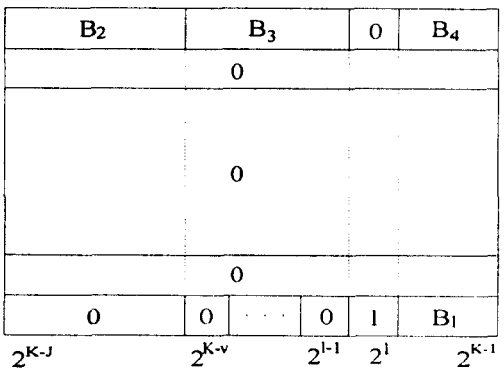

Fig 2. Binary Representation of f_u in the Matrix Form.

This means $\delta' < \delta$, which contradicts to $\delta' > \delta$. In order to satisfy $\delta' > \delta$, any bits in the binary representation of f_u in $[2^l,\ 2^{K-v-1}]$ should be "0".

(ii) Assume that some "1" bits of f_u in the binary representation are in $[2^{K-v},\ 2^{K-1}]$, i.e.,

$$f_u = B_2 + B_3 + B_4 + (2^l + B_1) \tag{25}$$

as in Fig.2.

We can choose f_s by using f_{max} such that $f_s \in \Omega^c$ and $f_s < f_u$ as follows ;

All "1" bits of f_{max} at the same locations as $\bar{B}_1$, is moved to the first row at the same columns, which makes the $\bar{B}_1 \cdot 2^{-J(e-1)}$.

And the bit 2^l of f_{max} is moved to 2^{l-J}. Therefore,

$$f_s = B_1 + (2^{l-1} + 2^{l-2} + \cdots + 2^{K-v}) + A + 2^{l-J} + \bar{B}_1 \cdot 2^{-J(e-1)}. \tag{26}$$

The f_s was deriven by the columnwise shifts of some "1" bits of f_{max}. Therefore, $f_s \in \Omega^c$, $f_s \le f_l$ and

$$\begin{aligned}\delta' &= f_u - 1 - f_l \le f_u - 1 - f_s \\ &= 2^l - (2^{l-1} + 2^{l-2} + \cdots + 2^{K-v}) \\ &\quad - A - 2^{l-J} - \bar{B}_1 \cdot 2^{-J(e-1)} + B_4 + B_3 + B_2 - 1 \\ &= 2^{K-v} - A - (2^{l-J} - B_2 - B_3) - (\bar{B}_1 \cdot 2^{-J(e-1)} - B_4) - 1. \end{aligned} \tag{27}$$

In order to find the contradiction to assumption, we have to compare d with δ'.

$$\begin{aligned}\delta - \delta' &> (N - f_{max}) - (f_u - 1 - f_s) \\ &= \sum_{i=0}^{K-J-1} 2^i + \bar{A} - 2^{K-v} + A + (2^{l-J} - B_2 - B_3) \\ &\quad + (\bar{B}_1 \cdot 2^{-J(e-1)} - B_4) + 1 \\ &= (A + \bar{A} + \sum_{i=0}^{K-J-1} 2^i) - 2^{K-v} + (2^{l-J} - B_2 - B_3) \\ &\quad + (\bar{B}_1 \cdot 2^{-J(e-1)} - B_4) + 1 \\ &= 2^{K-v} - 1 - 2^{K-v} + (2^{l-J} - B_2 - B_3) \\ &\quad + (\bar{B}_1 \cdot 2^{-J(e-1)} - B_4) + 1 \\ &= (2^{l-J} - B_2 - B_3) + (\bar{B}_1 \cdot 2^{-J(e-1)} - B_4) > 0 \end{aligned} \tag{28}$$

This means $\delta > \delta'$ and it contradicts to $\delta' > \delta$.

From(i) and (ii), in order to satisfy $\delta' > \delta$, any "1" bits in the binary repersentation of f_u should be in the first row, i.e.,$[2^0,\ 2^{l-1}]$, which means that we cannot find f_u, f_l such that

$$f_u - f_l > \delta, \tag{29}$$

because

$$f_u - f_l > 2^J \tag{30}$$

and

$$\delta > 2^{K-v-1} > 2^J. \tag{31}$$

q.e.d

This leads easily to the following lower bound on the minimum distance of the code :

COROLLARY 2 : The minimum distance d_{min} of GMW code $\underline{G}$ defined in (10) satisfies

$$d_{min} \geq 2^K - 1 + f_{min} - f_{max} = \delta. \tag{32}$$

Interestingly, it turns out that the Hamming weights of the codewords in $\underline{G}$ satisfies the constraint stated below :

THEOREM 5 : Every codeword in $\underline{G}$ defined in (10) has Hamming weight h, which is a multiple of 2^{J-1}, i.e.,

$$\left\{ (T-S_0)\cdot 2^{J-1} \mid 0 \leq S_0 \leq \lfloor T - \frac{d_{min}}{2^{J-1}} \rfloor \right\}, \tag{33}$$

where T is $(2^K-1)/(2^J-1)$ and d_{min} is given in (32).

PROOF : Any codeword $c(t)$ in polynomial notation of $\underline{G}$ can be represented by the linear combination of time shifted GMW sequences as follows ;

$$c(t) = \sum_{s=1}^{l} g(t+\tau_s), \tag{34}$$

and l-th order full period autocorrelation P_l of GMW sequences $g(t)$, can be given by

$$\begin{aligned} P_l &= \sum_{t=0}^{N-1} (-1)^{\sum_{s=1}^{l} g(t+\tau_s)} \\ &= \sum_{t=0}^{N-1} (-1)^{\sum_{s=1}^{l} tr_1^J(\lfloor tr_J^K(\alpha^{t+\tau_s})\rfloor^r)} \\ &= \sum_{t=0}^{N-1} (-1)^{tr_1^J(\sum_{s=1}^{l} \lfloor tr_J^K(\alpha^{t+\tau_s})\rfloor^r)}. \end{aligned} \tag{35}$$

Let

$$t = T\cdot i + j,\ 0 \leq i \leq 2^J-2,\ 0 \leq j \leq T-1.$$

Then

$$\begin{aligned} P_l &= \sum_{i=0}^{2^J-2} \sum_{j=0}^{T-1} (-1)^{tr_1^J(\{\sum_{s=1}^{l} \lfloor tr_J^K(\alpha^{T\cdot i+j+\tau_s})\rfloor^r\})} \\ &= \sum_{j=0}^{T-1} \sum_{i=0}^{2^J-2} (-1)^{tr_1^J(\{(\alpha^r)^{i\cdot T} \sum_{s=1}^{l} \lfloor tr_J^K(\alpha^{j+\tau_s})\rfloor^r\})}, \end{aligned} \tag{37}$$

Where α^T is a primitive element in $GF(2^J)$, because the smallest value of m is a 2^J-1 such that $(\alpha^T)^m = 1$, and $(\alpha^T)^r$ is also a primitive element in $GF(2^J)$ because $gcd(r,\ 2^J-1) = 1$.

Let

$$f(\alpha^j) = \sum_{s=1}^{l} [tr_J^K(\alpha^{j+\tau_s})]^r. \tag{38}$$

Then, $\forall j$,

$$f(\alpha^j) \in GF(2^J), \tag{39}$$

and $f(\alpha^j)$ is independent of i. Therefore,

$$P_l = \sum_{j=0}^{T-1} \sum_{i=0}^{2^J-2} (-1)^{tr_1^J(\{(\alpha^{r\cdot T})^i \cdot f(\alpha^j)\})}, \tag{40}$$

where $\sum_{i=0}^{2^J-2} (-1)^{tr_1^J(\{(\alpha^{r\cdot T})^i\cdot f(\alpha^j)\})} = \begin{cases} -1, & \text{if } f(\alpha^j) \neq 0 \\ 2^J-1, & \text{if } f(\alpha^j) = 0. \end{cases}$

Let

$$S_0 = \#\text{ of } f(\alpha^j) = 0, \text{ for } 0 \leq j \leq T-1, \tag{41}$$

$$R_0 = \#\text{ of } f(\alpha^j) = 0, \text{ for } 0 \leq j \leq N-1, \tag{42}$$

If $f(\alpha^j) = 0$, then $f(\alpha^{j+T}) = \alpha^{r\cdot T}\cdot f(\alpha^j) = 0$. Thus,

$$S_0 = \frac{R_0}{(2^J-1)}. \tag{43}$$

Hence,

$$\begin{aligned} P_l &= (2^J-1)\cdot S_0 + (T-S_0)(-1) \\ &= 2^J\cdot S_0 - T \end{aligned}$$

$$=2^J\cdot\frac{R_0}{2^J-1}-\frac{2^K-1}{2^J-1}$$

$$=\frac{2^J\cdot R_0-(2^K-1)}{2^J-1} \tag{44}$$

Using relationship between autocorrelation and Hamming weight, $wt(c(t))$, of codeword $c(t)\in \underline{G}$,

$$wt(c(t))=\frac{(N-P_t)}{2}$$

$$=\frac{T\cdot(2^J-1)-2^J\cdot S_0+T}{2}$$

$$=(T-S_0)\cdot 2^{J-1}. \tag{45}$$

Clearly, $wt(c(t))\geq d_{min}\geq d$ and thus,

$$S_0\leq \lfloor T-\frac{d_{min}}{2^{J-1}}\rfloor. \tag{46}$$

q.e.d

V. AN EXAMPLE

As an example, consider the case $K=6$, $r=3$ when $N=63$, $J=3$, and $T=9$. Then the GMW sequence is given as

$$g(t)=tr_1^3\{[tr_3^6(\alpha^t)]^3\}. \tag{47}$$

And the GMW sequence can be expanded as

$$g(t)=tr_1^6(\alpha^{3\cdot t})+tr_1^6(\alpha^{17\cdot t}), \tag{48}$$

where the linear span is easily calculated as

$$L=6\cdot(\frac{6}{3})^{2-1}=12. \tag{49}$$

Therefore, the dimension of GMW code generated by the GMW sequence defined in(47) is 12. As r is 3 and e is 2, $A(i_1)$ can be expressed as

$$A(i_1)=1+2\cdot 2^{i_1},\ 0\leq i_1\leq 1. \tag{50}$$

Thus, $A(0)=3$ and $A(1)=17$. The nonnull spectrum of GMW codes is derived as

$$\Omega^e=C_{-3}\cup C_{-17} \tag{51}$$

$$=\{15, 23, 29, 30, 39, 43, 46, 51, 53, 57, 58, 60\}, \tag{52}$$

where $f_{min}=15$ and $f_{max}=60$. Therefore,

$$\delta=63+15-60=18 \tag{53}$$

and

$$d_{min}\geq\delta=18. \tag{54}$$

That is, the GMW codes generated by GMW sequence in (47) is (63, 12) cyclic code whose minmum distance is greater than or equal to 18. The possible Hamming weight of the codes is integer multiple of $2^{3-1}=4$. Therefore, the minimum distance of GMW code is greater than or equal to 20. The true minimum distance of the (63, 12) GMW code needs to be found. But the maximum value of minimum distance of(63, 12) binary cyclic code is known as 24.

VI. CONCLUSION

New binary cyclic codes which are generated by using the GMW sequence and its cyclic shilfts are introduced. Code length of the GMW code is 2^K-1 and its dimension is $K\cdot(K/J)^{w-1}$, where w is a Hamming weight of r. Several properties of GMW codes such as designed distance, mimimum distance, and weights of codewords are derived in terms of parameters of GMW sequences. The cyclic codes are the most frequently used error correcting codes in digital communication system, because the encoding and decoding algorithm of the cyclic codes are easy to implement. It has been shown that GMW code is binary cyclic code and its minimum distance is large. Therefore, it can be used as a channel code in the digital communication systems. In order to be used in pratical applications, it is needed to find the decoding algorithms of GMW codes by using its properties. The decoding algorithms of GMW codes are

left for further study.

References

1. S. W. Golomb, *Shift Register Sequences*. San Francisco, CA : Holden-Day, 1967 ; revised edition, Laguna Hills, CA : Aegean Park Press, 1982.
2. E. R. Berlekamp, *Algebraic Coding Theory*. New York : McGraw-Hill, 1968.
3. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, the Netherlands : North-Holland, 1977.
4. D. V. Sarwarte and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp.593-620, May 1980.
5. R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp.548-553, May 1984.
6. J. S. No and P.V.Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Inform. Theroy*, vol. IT-35, no.2, pp.371-379, Mar.1989.

盧 宗 善(Jong-Seon No) 정회원

1981년 2월 : 서울대학교 공과대학 전자공학과 학사

1984년 2월 : 서울대학교 대학원 전자공학과 석사

1988년 5월 : (미국)남가주대학교 전자공학과 박사

1988년 2월~1990년 7월 : (미국)메릴랜드 소재 Hughes Network Systems 연구개발부 책임연구원

1990년 9월 1일 : 건국대학교 공과대학 전자공학과 조교수