

## 코드분할 다중통신용 새로운 다진법 코드의 개발

김철기, 신동찬, 이수룡(3사관학교)

## A New Family of Nonbinary Sequences Having Large Complexity For CDMA

Chulki Kim, Dongchan Shin, Sooryong Lee  
(Korea 3rd Military Academy)

## 요 약

코드분할 다중통신(Code Division Multiple Access Communication)은 Spread Spectrum 통신의 발전된 형태로서 군사목적상 이동 무선통신(Combat Multiple Communication)을 위해서 최근들어 급속도로 중요시 되고있다. 잘 알려진 바와 같이 두가지 가장 일반적인 다중통신 방식은 주파수 분할 다중통신방식과 시분할 다중통신 방식이다. 주파수 분할 다중통신 방식에서는 모든 사용자가 각각 다른주파수를 사용하여 동시에 신호를 보내고 시분할 다중통신에서는 같은 주파수를 사용하되 시간대를 달리하고 있다. 이 두가지 방식을 결합하여 모든사용자가 같은 시각과 같은 주파수를 공유하여 통신을 가능케 할수 있는 방식이 코드분할 다중통신이다. 여기에서 사용자는 각각 고유한 코드를 부여받는다. 이때 각 코드간에는 낮은 상관계수(Cross-correlation)를 가져야 하며, 이러한 성질을 만족하는 코드 집합을 구하기위한 노력이 경주되었으며 현재까지 2진법 코드 집합으로서 Gold, Kasami, No 코드가 알려져 있으며, 복잡성(Complexity)을 증가시키기 위한 노력으로서 (군사목적에 중요) 다진법 코드에 대한 연구가 활발해지고 있으나 공개된 것은 없었다. 최근에 (1990), 다진법 코드로서 Kumar 코드가 발표되었다. 그러나 이러한 코드들은 복잡성(Complexity or Linear Span)을 증가시키지는 못하였다. 본 논문은 복잡성(Complexity)이 증가한 새로운 다진법 코드의 집합을 제안하였다. 각 집합은  $P^n$ 개의 코드로 구성되며, 최대 상관계수 값은  $P^{n(p-1)-1}$  이다. ( $n=2m$ )

## I. INTRODUCTION

In 1970 Trachtenberg introduced the nonbinary sequence set which has period  $p^n-1$  and family size of  $p^{n+1}$  and the maximum nontrivial correlation value of  $1 + \sqrt{p^{n+1}}$  ( $p$  prime,  $n$  odd). In 1976 Hellesteth introduced the nonbinary sequence set which has period  $p^n-1$  and family size of  $p^{n+1}$  and the maximum nontrivial correlation value of  $1 + 2\sqrt{p^n}$  ( $p$  prime,  $n$  even,  $p^{n/2} \not\equiv 2 \pmod{3}$ ). In 1990 Kumar and Moreno introduced the

nonbinary sequence set which has period  $p^n-1$  and family size of  $p^n$  and the maximum nontrivial correlation value of  $1+\sqrt{p^n}$  ( $p$  prime). In 1991 Liu and Komo introduced the nonbinary Kasami sequence set which has period  $p^n-1$  and family size of  $p^{n/2}$  and the maximum nontrivial correlation value of  $1+p^{n/2}$  ( $p$  prime,  $n$  even). But linear span of those sequence sets are just the number of linear shift registers for generating each sequence set since those sequence sets are just from the addition of linear feedback shift registers. In 1990 Antweiler and Bömer introduced the nonbinary GMW sequence with large linear span but it is not a family of sequence for CDMA applications.

This paper presents the new nonbinary sequence set with large linear span for CDMA applications which has more members rather than the nonbinary No family extension ( family size is increased from  $p^{n/2}$  to  $p^n$  ).

## II. THE NEW FAMILY

The trace function, which maps the elements  $\alpha$  of  $GF(p^n)$  into elements of a subfield  $GF(p^m)$  can be generalized in the following way:

$$\text{Tr}_m^n(\alpha) = \sum_{i=0}^{n/m-1} \alpha^{p^{im}}$$

with  $n$  divisible by  $m$  and  $p$  a prime number.

We define the new sequence set over  $GF(p)$  ( $p$  prime) as

$$S = \{s_i(t) | 0 \leq t \leq N-1, 1 \leq i \leq p^n\} \quad (1)$$

where

$$s_i(t) = \text{Tr}_1^m \{ [\text{Tr}_m^n(\alpha^{pt}) + \alpha^{Tr} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)t})]^r \} \quad (2)$$

where  $\alpha$  is a primitive element of  $GF(p^n)$ , the integer  $r$ ,  $0 < r < p^m-1$ , satisfies  $\text{gcd}(r, p^m-1) = 1$ ,  $\gamma_i \in GF(p^n)$ ,  $N = p^n+1$ ,  $m = n/2$ ,  $T = p^m+1$ . It can be noted that if  $p=2$ , this sequence set represent exactly binary No sequence set. The correlation function,  $R_{ij}(t)$ ,  $1 \leq i, j \leq p^n$ , of the  $i$ th and  $j$ th nonbinary sequences corresponding to  $s_i(t)$  and  $s_j(t)$  is the inner product of the nonbinary sequences given as

$$R_{ij}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t+\tau)-s_j(t)} \quad 0 \leq \tau \leq N-1 \quad (3)$$

where  $t+\tau$  is modulo  $N$  addition.

$$\begin{aligned} s_i(t) &= \text{Tr}_1^m \{ [\text{Tr}_m^n(\alpha^{pt}) + \alpha^{Tt} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)t})]^r \} \\ &= \text{Tr}_1^m \{ [\text{Tr}_m^n(\alpha^{p(t_1 T + t_2)}) + \alpha^{T(t_1 T + t_2)} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)(t_1 T + t_2)})]^r \} \end{aligned} \quad (4)$$

where  $t=t_1 T+t_2$ ,  $0 \leq t_1 \leq p^m-1$ ,  $0 \leq t_2 \leq T-1$ . Noting that

$$\text{Tr}_m^n(\alpha^{p(t_1 T + t_2)}) = \text{Tr}_m^n(\alpha^{pt_1 T} \alpha^{pt_2}) = \alpha^{pt_1 T} \text{Tr}_m^n(\alpha^{pt_2}) \quad (5)$$

and that

$$\alpha^{T(t_1 T + t_2)} = \alpha^{t_1 T^2} \alpha^{Tt_2} = \alpha^{2t_1 T} \alpha^{Tt_2} \quad (6)$$

and that

$$\text{Tr}_m^n(\gamma_i \alpha^{(p-2)(t_1 T + t_2)}) = \text{Tr}_m^n(\gamma_i \alpha^{(p-2)t_1 T} \alpha^{(p-2)t_2}) = \alpha^{(p-2)t_1 T} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)t_2}) \quad (7)$$

So,

$$\begin{aligned} s_i(t) &= \text{Tr}_1^m \{ [\alpha^{pt_1 T} \text{Tr}_m^n(\alpha^{pt_2}) + \alpha^{2t_1 T} \alpha^{t_2 T} \alpha^{(p-2)t_1 T} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)t_2})]^r \} \\ &= \text{Tr}_1^m \{ \alpha^{pt_1 T} [\text{Tr}_m^n(\alpha^{pt_2}) + \alpha^{t_2 T} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)t_2})]^r \} \end{aligned} \quad (8)$$

As a result, we have that

$$\begin{aligned} s_i(t+\tau) - s_j(t) &= \text{Tr}_1^m \{ \alpha^{pt_1 T} [ \{ \text{Tr}_m^n(\alpha^{p(t_2+\tau)}) + \alpha^{T(t_2+\tau)} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)(t_2+\tau)}) \}^r \\ &\quad - \{ \text{Tr}_m^n(\alpha^{pt_2}) + \alpha^{t_2 T} \text{Tr}_m^n(\gamma_j \alpha^{(p-2)t_2}) \}^r ] \} \end{aligned} \quad (9)$$

where we define

$$\begin{aligned} f_1(t_2) &= \{ \text{Tr}_m^n(\alpha^{p(t_2+\tau)}) + \alpha^{T(t_2+\tau)} \text{Tr}_m^n(\gamma_i \alpha^{(p-2)(t_2+\tau)}) \}^r \\ &\quad - \{ \text{Tr}_m^n(\alpha^{pt_2}) + \alpha^{t_2 T} \text{Tr}_m^n(\gamma_j \alpha^{(p-2)t_2}) \}^r \end{aligned} \quad (10)$$

Noting that

$$s_i(t+\tau) - s_j(t) = \text{Tr}_1^m \{ \alpha^{pt_1 T} f_1(t_2) \} \quad (11)$$

As a result, we have that

If  $f_1(t_2) \neq 0$ ,  $0 \leq t_2 \leq T-1$ , then  $s_i(t+\tau) - s_j(t)$  is a  $m$ -sequence of length  $p^m-1$ .

If  $f_1(t_2) = 0$ , we obtains  $p^m-1$  zeroes as  $t_1$  varies over the range  $0$  to  $p^m-2$ .

We define that  $z_1$  denotes the number of values of  $t_2$  which

$$z_1 = |\{t_2, 0 \leq t_2 \leq T-1 \mid f_1(t_2) = 0\}|$$

then  $s_i(t+\tau)-s_j(\tau)$  takes on the value 0 a total of  $z_1(p^m-1)+(T-z_1)(p^m-1)$  times and takes on the other value  $\{1,2,3, \dots, p-1\}$  a total of  $(T-z_1)p^{m-1}$

$$f_1(t)=\{\text{Tr}_m^n(\alpha^{p(t+\tau)})+\alpha^{T(t+\tau)}\text{Tr}_m^n(\gamma_i\alpha^{(p-2)(t+\tau)})\}^r - \{\text{Tr}_m^n(\alpha^{pt})+\alpha^{tT}\text{Tr}_m^n(\gamma_j\alpha^{(p-2)t})\}^r \quad 0 \leq t \leq N-1 \quad (12)$$

note that,

$$f_1(t+T)=\alpha^{pT}f_1(t), \quad 0 \leq t \leq N-1 \quad (13)$$

Consequently, if  $z_2$  denotes the number of zeroes of the function  $f_1(t)$  as  $t$  varies over the range 0 to  $N-1$ , then it must be that

$$z_2=(p^m-1)z_1 \quad (14)$$

Next, define

$$f_2(t)=\text{Tr}_m^n(\alpha^{p(t+\tau)})+\alpha^{T(t+\tau)}\text{Tr}_m^n(\gamma_i\alpha^{(p-2)(t+\tau)})-\text{Tr}_m^n(\alpha^{pt})-\alpha^{tT}\text{Tr}_m^n(\gamma_j\alpha^{(p-2)t}) \quad (15)$$

Since  $\gcd(r,p^m-1)=1$ ,

$$f_1(t)=0 \Leftrightarrow f_2(t)=0, \quad 0 \leq t \leq N-1 \quad (16)$$

Thus it suffices to count the number of zeroes of the function  $f_2(t)$ .

Let  $x=\alpha^t$  so that  $x$  ranges over all the nonzero elements of  $\text{GF}(p^n)$  as  $t$  varies over 0 to  $N-1$ .

$$\begin{aligned} f_2(x) &= (\alpha^{p\tau}-1)x^p + (\alpha^{p\tau}-1)^{p^m}x^{p^{m+1}} + \gamma_i\alpha^{(T+p-2)\tau}x^{(T+p-2)} \\ &\quad + \gamma_i^{p^m}\alpha^{\{T+(p-2)p^m\}\tau}x^{\{T+(p-2)p^m\}} - \gamma_jx^{(T+p-2)} - \gamma_j^{p^m}x^{\{T+p^m(p-2)\}} \\ &= x^p\{(\alpha^{p\tau}-1) + (\alpha^{p\tau}-1)^{p^m}x^{p(p^m-1)} + (\gamma_i\alpha^{(p^m+p-1)\tau} - \gamma_j)x^{p^m-1} \\ &\quad + (\gamma_i^{p^m}\alpha^{(p^{m+1}-p^m+1)\tau} - \gamma_j^{p^m})x^{(p^{m+1}-p^m-p+1)}\} \end{aligned} \quad (17)$$

Let  $y=x^{p^m-1}$ . Since  $(p-1)(p^m-1)=p^{m+1}-p^m-p+1$ ,

$$\begin{aligned} f_2(x) &= x^p\{(\alpha^{p\tau}-1) + (\alpha^{p\tau}-1)^{p^m}y^p + (\gamma_i\alpha^{(p^m+p-1)\tau} - \gamma_j)y \\ &\quad + (\gamma_i^{p^m}\alpha^{(p^{m+1}-p^m+1)\tau} - \gamma_j^{p^m})y^{(p-1)}\} \end{aligned} \quad (18)$$

Here we distinguish between two cases:

Case1:  $\tau=0$  and  $\gamma_i \neq \gamma_j$

$$f_2(x)=x^py\{(\gamma_i-\gamma_j) + (\gamma_i^{p^m}-\gamma_j^{p^m})y^{(p-2)}\} \quad (19)$$

In this case,  $f_2(x)$  vanishes if and only if  $(p-2)$ th degree polynomial of  $y$  in (19) vanishes. Since the coefficients of the polynomial lie in  $GF(p^n)$ , the polynomial has  $0,1,2,\dots,(p-2)$  roots over  $GF(p^n)$ .

Case 2:  $\tau \neq 0$

Similarly,  $f_2(x)$  vanishes if and only if  $p$ th degree polynomial of  $y$  in (18) vanishes. And the polynomial has  $0,1,2,\dots,p$  roots over  $GF(p^n)$ . Thus,  $z_2=0, (p^m-1), 2(p^m-1), 3(p^m-1), \dots, p(p^m-1)$  since  $y = \alpha^{(p^m-1)t}$ . Thus, the values of  $z_1$  are 0 or 1 or 2 or ... or  $p$ . As a result, all possible values of  $R_{ij}(\tau)$  are of the form

$$\begin{aligned} R_{ij}(\tau) &= \omega^{s_i(t+\tau)-s_j(t)} \\ &= \omega^0 \{z_1(p^m - 1) + (T - z_1)(p^{m-1} - 1)\} \\ &\quad + \omega^1 (T - z_1)p^{m-1} + \omega^2 (T - z_1)p^{m-1} + \dots + \omega^{p-1} (T - z_1)p^{m-1} \\ &= z_1 p^m - T + (T - z_1)p^{m-1} (\omega^0 + \omega^1 + \dots + \omega^{p-1}) \end{aligned} \tag{20}$$

where  $(\omega^0 + \omega^1 + \dots + \omega^{p-1}) = 0$  So,

$$R_{ij}(\tau) = z_1 p^m - T = p^m (z_1 - 1) - 1 \tag{21}$$

If  $p=2$ ,  $R_{ij}(\tau) = 2^m (z_1 - 1) - 1$ . Thus the sequence family presented here includes a family of binary No sequence. And also  $p=3$ ,  $R_{ij}(\tau) = 3^m (z_1 - 1) - 1$ .

The maximum  $R_{ij}(\tau) \leq 2 \cdot 3^m - 1$  ( the same as Helleseth's maximum value.)

### III. EXAMPLE

Let  $p=3, n=4(m=2), r=5$ , and the minimum polynomial of  $\alpha$  over  $GF(3^4)$  is  $p(x)=x^4+x+2$  which is primitive. Then,  $N=80, M=9$ , and  $T=10$ . From (2), the  $i$ th sequence of  $S$  is given as

$$s_i(t) = \text{Tr}_1^2 \{ [\text{Tr}_2^4 (\alpha^{3t}) + \alpha^{10t} \text{Tr}_2^4 (\gamma_i \alpha^{(3-2)t})]^5 \}, \quad \gamma_i \in GF(3^4) \tag{22}$$

or can be rewritten as

$$s_i(t) = \text{Tr}_1^2 \{ [\text{Tr}_2^4 (\alpha^{3t}) + \text{Tr}_2^4 (\gamma_i \alpha^{11t})]^5 \} \tag{23}$$

Here  $\beta=\alpha^9$  and is a primitive element of  $GF(3^2)$  and  $m_\beta(x)=x^2+x+2$ . The minimum polynomials  $m_{\alpha^3}(x)$  and  $m_{\alpha^{11}}(x)$  of  $\alpha$  over  $GF(3^2)$ , respectively, turn out to be

$$m_{\alpha^3}(x)=x^2-\beta^2x+\beta^3 \quad (24)$$

$$m_{\alpha^{11}}(x)=x^2-\beta^7x+\beta^3 \quad (25)$$

Choosing  $\{1,\beta\}$  as a basis for  $GF(3^2)$  over  $GF(3)$ , the elements  $\beta^t$  can be expressed in the form

$$\beta^t = \nu_0 + \nu_1\beta \quad (26)$$

where the coefficients  $\nu_i$  are functions of  $t$  and lie in  $GF(3)$ .

$$\begin{aligned} \beta^2\beta^t &= \beta^2(\nu_0 + \nu_1\beta) \\ &= \nu_0 + 2\nu_1 + (2\nu_0 + 2\nu_1)\beta \end{aligned} \quad (27)$$

$$\begin{aligned} \beta^3\beta^t &= \beta^3(\nu_0 + \nu_1\beta) \\ &= 2\nu_0 + 2\nu_1 + 2\nu_0\beta \end{aligned} \quad (28)$$

$$\begin{aligned} \beta^7\beta^t &= \beta^7(\nu_0 + \nu_1\beta) \\ &= \nu_0 + \nu_1 + \nu_0\beta \end{aligned} \quad (29)$$

$$(\beta^t)^5 = \nu_0 + 2\nu_0\nu_1^2 + 2\nu_0^2\nu_1 + (\nu_0^2\nu_1 + 2\nu_1 + 2\nu_0\nu_1^2)\beta \quad (30)$$

By the trace function property, it is sufficient for the purpose of implementation to determine only one coefficient function of (30). Finally, different sequences within the family are obtained by simply change the initial contents of bottom shift register for a fixed set of initial contents for the upper shift register. For calculating the linear span of (23), consider how many additional roots come out of this nonlinear operation. (This is Key's result) Now,

$$[\text{Tr}_2^4(\alpha^{3t}) + \text{Tr}_2^4(\gamma_i\alpha^{11t})]^5 = [\alpha^{3t} + \alpha^{27t} + \gamma_i\alpha^{11t} + \gamma_i^9\alpha^{19t}]^5 \quad (31)$$

which after some work expand to

$$\begin{aligned} &= \alpha^{15t}(1 + \gamma_i^{45} + 2\gamma_i + 2\gamma_i^{28}) + \alpha^{55t}(1 + \gamma_i^5 + 2\gamma_i^9 + 2\gamma_i^{12}) \\ &+ \alpha^{63t}(2\gamma_i^{13} + 2\gamma_i^3 + \gamma_i^{27} + 1) + \alpha^{7t}(2\gamma_i^{37} + \gamma_i^3 + 2\gamma_i^{27} + 1) \\ &+ \alpha^{39t}(2 + 2\gamma_i + 2\gamma_i^{10} + \gamma_i^3 + \gamma_i^{18}) + \alpha^{31t}(2 + 2\gamma_i^9 + \gamma_i^2 + 2\gamma_i^{10} + \gamma_i^{27}) \\ &+ \alpha^{23t}(2\gamma_i^{36} + \gamma_i^2 + 2\gamma_i^9 + 2\gamma_i) + \alpha^{47t}(2\gamma_i^9 + 2\gamma_i^4 + \gamma_i^{18} + 2\gamma_i) \end{aligned}$$

$$+\alpha^{79t}(2\gamma_i^{36} + 2\gamma_i^{12} + \gamma_i^{29}) + \alpha^{71t}(2\gamma_i^{28} + \gamma_i^{21} + 2\gamma_i^4) \quad (32)$$

Since the conjugates of  $\alpha^5$  are  $\alpha^{15}, \alpha^{45}, \alpha^{55}, \text{Tr}_1^2(\alpha^{15t})$  and  $\text{Tr}_1^2(\alpha^{55t})$  are phase shift of the sequence. Then since the sum of phase shifts of the same sequence is a different phase shift of the sequence,

$$\text{Tr}_1^2(\alpha^{15t} + \alpha^{55t}) = D^{i_1} \text{Tr}_1^2(\alpha^{5t}) \quad (33)$$

Similarly, the conjugates of  $\alpha^7$  are  $\alpha^{21}, \alpha^{63}, \alpha^{29}$  which yields

$$\text{Tr}_1^2(\alpha^{7t} + \alpha^{63t}) = D^{i_2} \text{Tr}_1^2(\alpha^{7t}) \quad (34)$$

and the conjugates of  $\alpha^{13}$  are  $\alpha^{39}, \alpha^{37}, \alpha^{31}$  which yields

$$\text{Tr}_1^2(\alpha^{39t} + \alpha^{31t}) = D^{i_3} \text{Tr}_1^2(\alpha^{13t}) \quad (35)$$

and the conjugates of  $\alpha^{23}$  are  $\alpha^{69}, \alpha^{47}, \alpha^{61}$  which yields

$$\text{Tr}_1^2(\alpha^{47t} + \alpha^{23t}) = D^{i_4} \text{Tr}_1^2(\alpha^{23t}) \quad (36)$$

and the conjugates of  $\alpha^{53}$  are  $\alpha^{79}, \alpha^{77}, \alpha^{71}$  which yields

$$\text{Tr}_1^2(\alpha^{71t} + \alpha^{79t}) = D^{i_5} \text{Tr}_1^2(\alpha^{53t}) \quad (37)$$

Thus, (23) turns out the addition of five different sequences depending upon  $\gamma_i$  value as

$$s_i(t) = D^{i_1} \text{Tr}_1^2(\alpha^{5t}) + D^{i_2} \text{Tr}_1^2(\alpha^{7t}) + D^{i_3} \text{Tr}_1^2(\alpha^{13t}) + D^{i_4} \text{Tr}_1^2(\alpha^{23t}) + D^{i_5} \text{Tr}_1^2(\alpha^{53t}) \quad (38)$$

The minimum polynomials with roots  $\alpha^L$  that generates the sequences  $\text{Tr}_1^4(\alpha^{Lt})$ ,

$L=5,7,13,23,53$  are given as

$$\begin{aligned} M_{\alpha^5}(x) &= (x - \alpha^5)(x - \alpha^{15})(x - \alpha^{45})(x - \alpha^{55}) \\ M_{\alpha^7}(x) &= (x - \alpha^7)(x - \alpha^{21})(x - \alpha^{63})(x - \alpha^{29}) \\ M_{\alpha^{13}}(x) &= (x - \alpha^{13})(x - \alpha^{39})(x - \alpha^{37})(x - \alpha^{31}) \\ M_{\alpha^{23}}(x) &= (x - \alpha^{23})(x - \alpha^{69})(x - \alpha^{47})(x - \alpha^{61}) \\ M_{\alpha^{53}}(x) &= (x - \alpha^{53})(x - \alpha^{79})(x - \alpha^{77})(x - \alpha^{71}) \end{aligned} \quad (39)$$

For  $\gamma_i=0$ ,  $s_i(t)$  includes only the sequences generated by  $\alpha^{5t}$  and  $\alpha^{13t}$  and  $\alpha^{7t}$ . Thus, the characteristic polynomial  $f(x)$  of  $s_i(t)$  is, in this case,

$$f(x) = M_{\alpha^5}(x) M_{\alpha^{13}}(x) M_{\alpha^7}(x) \quad (40)$$

which yields a linear span of 12. And this is the same as the result of the complex GMW sequence[5]. The linear span of complex GMW sequence is,

$$L = m \prod_{i=0}^{M-1} \binom{n/m + r_i - 1}{r_i} \tag{41}$$

where  $r = \sum_{i=0}^{M-1} r_i p^i$ . For  $\gamma_i \neq 0$ , we consider which value  $\gamma_i$  (range over all of  $GF(3^4)$ )

taking on each value exactly once as  $i$  ranges between 0 and 79 makes the coefficients of  $\alpha^{Lt}$  vanish. (Table 1)

Table 1. Linear Span depending on  $\gamma_i$  value

$i:(\gamma_i=\alpha^i)$	coefficients of $\alpha^{Lt=0}$	Linear Span
0	$\alpha^{15t}, \alpha^{55t}, \alpha^{7t}, \alpha^{63t}$	12
40	$\alpha^{15t}, \alpha^{55t}, \alpha^{71t}, \alpha^{79t}$	12
20	$\alpha^{15t}, \alpha^{55t}$	16
1,3,9,26,27,62,74,78	$\alpha^{71t}, \alpha^{79t}$	16
other values	No	20

For  $\gamma_i = \alpha^0$ , the  $\alpha^{5t}$  and  $\alpha^{7t}$  terms cancels out and yields a linear span of 12. For  $\gamma_i = \alpha^{40}$ , the  $\alpha^{5t}$  and  $\alpha^{71t}$  terms cancels out and yields a linear span of 12. For  $\gamma_i = \alpha^{20}, \alpha^{60}$  the  $\alpha^{5t}$  term cancels out and yields a linear span of 16. For  $\gamma_i = \alpha^1, \alpha^3, \alpha^9, \alpha^{26}, \alpha^{27}, \alpha^{62}, \alpha^{74}, \alpha^{78}$ , the  $\alpha^{71t}$  term cancels out and yields a linear span of 16. And for all other values, all terms are retained and

$$f(x) = M_{\alpha^5}(x) M_{\alpha^7}(x) M_{\alpha^{13}}(x) M_{\alpha^{23}}(x) M_{\alpha^{33}}(x) \tag{41}$$

which yields a linear span 20 which shows the increase of linear span.

#### IV. CONCLUSION

It has been shown that new family of sequences can be obtained by nonlinear operation of the addition of two sequences which increase the linear span of the



sequence. The correlation values of a new family have  $p+2$  levels with maximum nontrivial correlation of  $p^m(p-1)$ . Further work is needed to have a general formula of linear span of this sequence set. (This work is almost done by C.Kim and Kumar)

#### V. REFERENCES

- [1] Trachtenberg, H. M., "On the Crosscorrelation Functions of Maximal Recurring Sequences," Ph.D. Dissertation, University of Southern California, 1970.
- [2] Helleseth, T., "Some Result about the Crosscorrelation Function Between Two Maximal Linear Sequences," *Discrete Mathematics*, 16, pp.209-232, 1976.
- [3] Kumar, P.V., and Moreno, O., "Polyphase Sequences With Periodic Correlation Properties Better Than Binary Sequences," *IEEE International Symposium on Information Theory*, San Diego, January 1990.
- [4] Liu, S.C., and Komo, J.J., "Nonbinary Kasami Sequences over  $GF(p)$ ," *IEEE International Symposium on Information Theory*, Budapest, Hungary, June 1991.
- [5] Antweiler, M., and Bömer, L., "Complex Sequences over  $GF(p^M)$  with a Two Level Autocorrelation Function and a Large Linear Span," *IEEE International Symposium on Information Theory*, San Diego, January 1990.
- [6] Jong-Seon No and Kumar, P.V., "A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span," *IEEE Tran. on Information Theory*, Vol. 35, No. 2, March 1989.

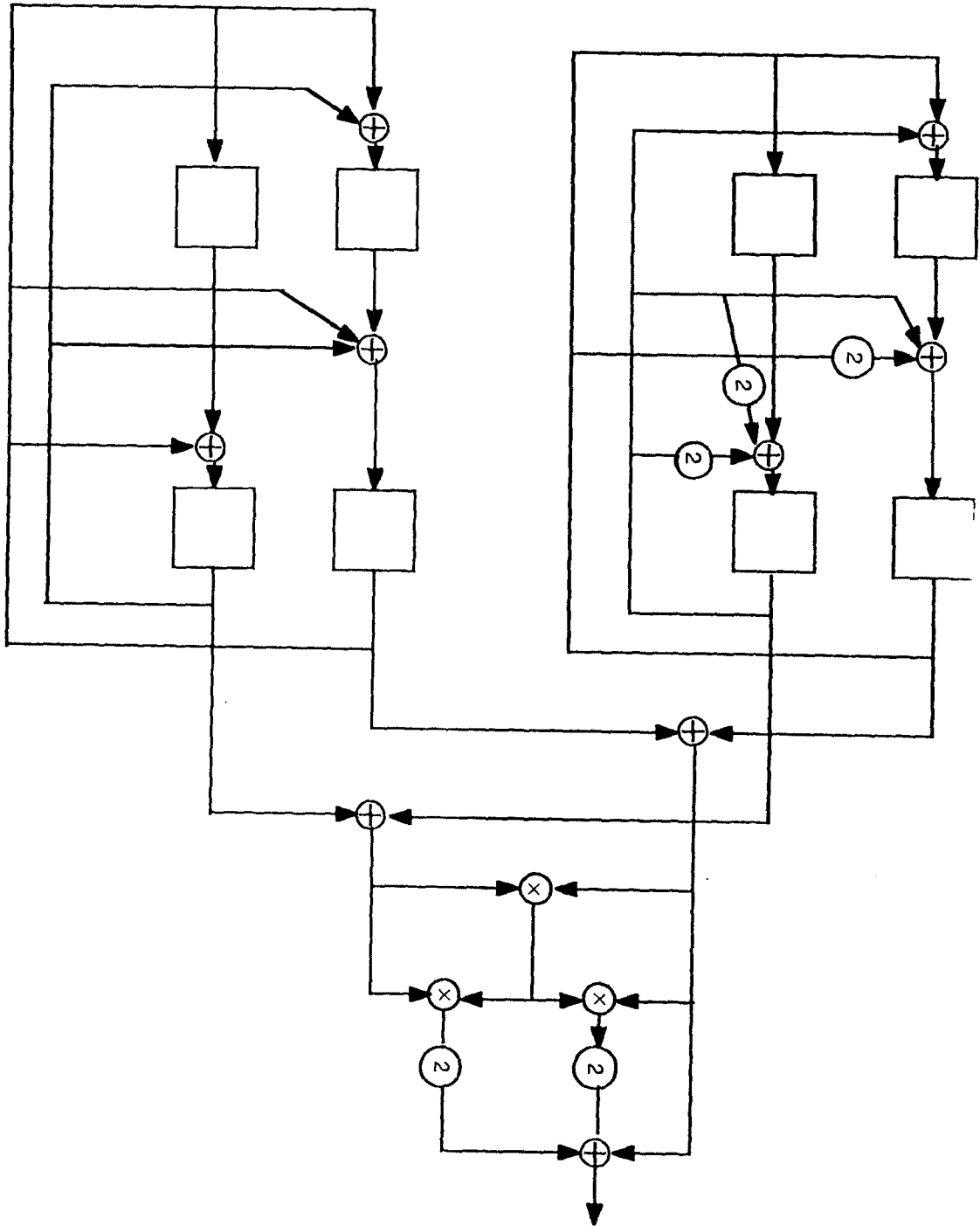


Fig. 1. Generation of New Sequence Set of Period 80