国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第18卷第2期 1996年6月 Vol. 18 No. 2

具有良好相关特性的码序列*

李 超

(国防科技大学系统工程与数学系 长沙 410073)

摘 要 扩频序列是扩频通信中最重要的部分。本文讨论了三类新型的代数型非线性扩频序列的生成方法，序列特性以及它们在扩频通信中的应用。

关键词 自相关，互相关，扩频序列

分类号 O156

Code Sequences with Optimal Correlation Properties

Li Chao

(Department of Systems Engineering and Mathematics, NUDT, Changsha 410073)

Abstract Spreading sequences are one of the most important component for SS communication. This paper discusses the construction method, sequences properties and application field in SS communication of three families of algebraic nonlinear spreading sequences.

Key words autocorrelation, crosscorrelation, spreading sequences

扩频通信是一种新型的通信方式，在这种方式中，信号所占用的带宽远远大于传送信息所需的最小带宽，而带宽的扩展是通过扩频序列实现的。具有良好相关特性的扩频序列对于扩频通信和扩频通信技术的应用具有重要的作用。一个理想的扩频序列族应当具有如下性质：(1) 每个序列的自相关是一个尖锐脉冲；(2) 两个不同序列之间互相关处处为零；(3) 序列平衡；(4) 足够的序列数；(5) 尽可能大的线性复杂度。然而，上述理想条件是目前任何实际序列族所达不到的，因为任何一个序列族，其自相关函数与互相关函数具有相互制约的关系。1976年，L. R. Welch 在文 [1] 中给出了一个序列族最大自相关旁瓣值和最大互相关模值的下限为 $\sqrt{p}$ (其中 p 为序列族的周期)。这个下限称为 Welch 下限。追求序列族的 Welch 下限是扩频序列设计要达到的目标。80年代后，

* 国防八五预研基金资助
1995年11月23日修订

人们利用有限域上迹函数的优美理论构造了许多具有良好相关特性的码序列。本文主要讨论 GMW 序列，NO 序列，Kasami 序列以及它们各种变种形式的相关特性。

1 具有最好自相关的 GMW 序列族

1.1 二元 GMW 序列

1984 年，Scholtz 和 Welch 利用有限域上迹函数给出了 GF (2) 上 GMW 序列定义如下：设 M，J 为正整数，$J|M$，α 为有限域 GF (2^M) 上本原元，r 为正整数，$1\leqslant r\leqslant 2^J-2$，$(r, 2^J-1)=1$，令 $b(n)=\mathrm{tr}_1^J(\mathrm{tr}_J^M\alpha^n)^r$，$n=0, 1, 2, \cdots$，则称二元序列 $\underline{b}=b(0)\,b(1)\,b(2)\cdots b(n)\cdots$ 为二元 GMW 序列。显然，当 $r=1$ 时，$b(n)=\mathrm{tr}_1^J(\mathrm{tr}_J^M\alpha^n)=\mathrm{tr}_1^M(\alpha^n)$。于是 $\{b(n)\}$ 为二元 m 序列，故 GMW 序列是 m 序列的一种推广形式。文 [2] 中给出了二元 GMW 序列的自相关函数：$R(\tau)=\begin{cases}2^M-1 & \text{当 } \tau\equiv 0 \mod 2^M-1\\ -1 & \text{当 } \tau\not\equiv 0 \mod 2^M-1\end{cases}$。易知，GMW 的自相关函数为一个尖锐脉冲。进一步分析可知，GMW 序列一个周期内，长度为 k 的 0 游程个数为 $2^{M-k}-1$，长度为 k 的 1 游程个数为 2^{M-k}，并且 GMW 序列线性复杂度为 $L=J\cdot(M/J)^\omega$，其中 ω 为 r 的二进制表示 "1" 的个数。目前，从理论上给出 GMW 序列的互相关函数还相当困难。利用计算机大量统计分析，可以得到 GMW 序列非平移等价类之间的互相关最大值为 $R_c=\begin{cases}2^{(M+2)/2}-1 & (2|M)\\ 2^{(M+1)/2}-1 & (2\nmid M).\end{cases}$

1.2 GMW 序列的变种

1992 年，Antweiler 和 Böner 在文 [3] 中将二元 GMW 序列推广到一般有限域 GF (P) 上，得到 P 元 GMW 序列。设 M，J 为正整数，$J|M$，α 为 GF (P^M) (P 为素数) 上本原元，r 为正整数，并且 $1\leqslant r\leqslant P^J-2$，$(r, P^J-1)=1$，令 $b(n)=\mathrm{tr}_1^J(\mathrm{tr}_J^M\alpha^n)^r$，$n=0, 1, 2, \cdots$，则称 P 元序列 $\underline{b}=\{b(n)\}=b(0)\,b(1)\,b(2)\cdots$ 为 P 元 GMW 序列。P 元 GMW 序列作为二元 GMW 序列的扩展形式。同样，具有良好的自相关函数 $R_{\underline{b}}(\tau)=\begin{cases}P^M-1 & \tau\equiv 0 \mod P^M-1,\\ -1 & \tau\not\equiv 0, \mod P^M-1\end{cases}$，同时具有大的线性复杂度和良好的统计特性。1993 年，作者利用一系列有限代数扩张 GF (P^{K_1}) $\subseteq$GF ($P^{K_1K_2}$) $\subseteq\cdots\subseteq$GF ($P^{K_1K_2\cdots K_t}$) 来取代文 [3] 中域扩张 GF (P^J) $\subseteq GF$ (P^M)，得到一类更为广泛的 GMW 序列的变种。即作如下构造：设 $t\geqslant 2$，$K=K_1K_2\cdots K_t$，K_i 为正整数，α 为 GF (P^K) 中本原元。r_1，r_2，$\cdots$，r_{t-1} 为满足如下条件的正整数，$1\leqslant r_i\leqslant P^{K_1K_2\cdots K_i}-2$，$(r_i, P^{K_1\cdots K_i}-1)=1$。令

$$b(n)=\mathrm{tr}_1^{K_1}\{\mathrm{tr}_{K_1}^{K_1K_2}[\mathrm{tr}_{K_1K_2}^{K_1K_2K_3}\cdots(\mathrm{tr}_{K_1\cdots K_{t-1}}^{K}\alpha^n)^{r_{t-1}}\cdots]^{r_2}\}^{r_1}$$

其中 $\mathrm{tr}_{K_1\cdots K_{i-1}}^{K_1\cdots K_i}(\cdot)$ 表示从 GF ($P^{K_1\cdots K_i}$) 到 GF ($P^{K_1\cdots K_{i-1}}$) 的迹函数，$i=1, 2, \cdots t$，则称序列 $\underline{b}=\{b(n)\}=b(0)\,b(1)\,b(2)\cdots$ 为广义 GMW 序列。广义 GMW 序列具有如下伪随机特性。

定理 1[6]　(1) 广义 GMW 序列的周期为 P^K-1；(2) 广义 GMW 序列的自相关函数为：

$$R_b(\tau)=\begin{cases}P^K-1 & \text{当 } \tau\equiv 0 \mod P^K-1\\ -1 & \text{当 } \tau\not\equiv 0 \mod P^K-1\end{cases}$$

(3) 令 $C=(C(1), C(2), \cdots C(k))$ 表示 GF (P) 上 k 元素组，$k\leqslant K_1$，$N_{\underline{b}}(c)=|\{j|0\leqslant j\leqslant P^K-2, (b(j), b(j+1), \cdots b(j+k-1))=C\}|$，则

$$N\underline{b}(c)=\begin{cases}P^{K-k}-1 & \text{当 } C=(0,0,\cdots 0)\\ P^{K-k} & \text{当 } C\neq(0,0,\cdots 0)\end{cases}$$

(4) 广义 GMW 序列数为 $\prod_{i=1}^{t}\frac{\phi(P^{K_1\cdots K_i}-1)}{K_1K_2\cdots K_i}$。

关于广义 GMW 序列数的线性复杂度有：

定理 2　(1) 令 w_i 表示 r_i 的 P－adic 表示中的诸位数字之和 $(i=1, 2, \cdots, t-1)$，则广义 GMW 序列的线性复杂度不超过 $K_1K_2^{W_1}K_3^{W_1W_2}\cdots K_t^{W_1W_2\cdots W_{t-1}}$。(2) 广义 GMW 序列能够到达线性复杂度上界的一个必要条件是诸 r_i $(1\leqslant i\leqslant t-1)$ 的 P－adic 表示各位数字不超过 1。(3) 当 $t=3$ 时，设 $r_1=P^{l_1}+P^{l_2}+\cdots+P^{l_\pi}$，$0\leqslant l_1<l_2<\cdots<l_\pi\leqslant K_1-1$，$r_2=P^{j_1}+P^{j_2}+\cdots+P^{j_w}$，$0\leqslant j_1<j_2<\cdots<j_w\leqslant K_1K_2-1$，则广义 GMW 序列线性复杂度到达上界 $K_1K_2^{\pi}K_3^{w}$ 的充分必要条件是，对于任意 j_{i1}，j_{i2} 和 l_{λ_1}，l_{λ_2} $(\lambda_1\neq\lambda_2)$ 均有 $j_{i1}-j_{i2}\not\equiv l_{\lambda_1}-l_{\lambda_2} \mod K_1$。

由上述两个定理可知，GMW 序列及其各种变种形式具有最好为自相关特性和很大的线性复杂度，同时序列数目多，序列平衡性好，但唯一不足之处是互相关特性不是很好，在实用时，需在众多的 GMW 序列中选取互相关性能比较好的子序列族。

2　具有最好互相关的 NO 序列族

2.1　NO 序列族

1989 年，J. S，NO 和 P. V. Kumar[4]在 GMW 序列的基础上，研究发现了另一类具有优异周期相关特性和大的线性复杂度的 NO 序列。其生成方法如下：设 n 为正偶数，$2|n$，$m=\frac{n}{2}$，$N=2^n-1$，$T=(2^n-1)/(2^m-1)=2^m+1$。令 $S=\{S_i(t)|0\leqslant t\leqslant N-1, 1\leqslant i\leqslant 2^m\}$，其中 $S_i(t)=\mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{2t})+r_i\cdot\alpha^{T\cdot t}]^r\}$。这里 α 为 GF (2^n) 中本原元，$1\leqslant r\leqslant 2^m-2$，并且 $(r, 2^m-1)=1$，r_i $(i=1, 2, \cdots, 2^m)$ 取 GF (2^m) 中元素。这样，得到的序列族 S 称为 NO 序列。

定理 3　设 $R_{ij}(\tau)$ 表示 NO 序列的互相关函数，则 $R_{ij}(\tau)$ 一定取集合 $\{2^n-1, -2^m-1, -1, 2^m-1\}$ 中每一个值，并且分配如下：2^n-1 出现 2^m 次；-2^m-1 出现 $2^m(2^m-1)+(2^n-2)2^m(2^{m-1}-1)$ 次；-1 出现 $(2^n-2)2^m$ 次，2^m-1 出现 $(2^n-2)\cdot 2^{n-1}$ 次。

由定理 3 可知，NO 序列的最大自相关旁瓣值和最大互相关模值 2^m-1，它达到 Welch 下限，故具有最好的互相关。

2.2　NO 序列的变种

文[7]给出了 NO 序列的一种变种形式，其定义如下。设 m、n 为正整数，$m|n$，$N=2^n-1$，$T=(2^n-1)/(2^m-1)$，$T\equiv d \mod 2^m-1$。如果 $(d, 2^n-1)=1$，则令 $S=\{S_i(t)|0\leqslant t\leqslant$

$N-1,1\leqslant i\leqslant 2^m\}$，其中 $Si(t)=\mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{dt})+r_i\cdot\alpha^{T\cdot t}]^T\}$。这里 α 为 GF(2^n)中本原元，$1\leqslant r\leqslant 2^m-2,(r,2^m-1)=1,r_i(i=1,2,\cdots,2^m)$取遍 GF($2^m$)中所有元素。称该序列族为广义 NO 序列。易知，当 $n=2^m$ 时，$T=2^m+1,T\equiv 2\bmod 2^m-1$。这时 $d=2,(2,2^n-1)=1$。故定义的序列是 NO 序列一种扩展形式。记 $A(m,n)=\{\beta|\beta\in GF(2^n),\mathrm{tr}_m^n(\beta)=1\}=\{\alpha^{t_1},\alpha^{t_2},\cdots,\alpha^{t_{2^{n-m}}}\},A=\{t_1,t_2,\cdots,t_{2^{n-m}}\}$为相应的指数集合。设 $U=\{\bar{u}_1,\bar{u}_2,\cdots,\bar{u}_t\}$为 A 中整数模 2^m-1 所得到剩余类集。令 $w_i=|\bar{u}_i|\quad i=1,2,\cdots t$，有如下结论。

定理 4[7]　设 $R_{ij}(\tau)$为广义 NO 序列的互相关函数，则 $R_{ij}(\tau)\in\{2^n-1,-1,-T,w_i\cdot 2^m-T(i=1,2,\cdots t)\}$且分配如下：$2^n-1$ 出现 2^m 次；-1 出现 $(2^n-2)\cdot 2^m$ 次；$-T$ 出现 $2^m(2^m-1)+(2^n-2)\cdot 2_m(2^m-t-1)$；$w_i\cdot 2^m-T$ 出现 $(2^n-2).2^m$ 次，$i=1,2,\cdots,t$。在文[7]中，还给出了一个具体算法，来求广义 NO 序列的互相关函数。

3　具有最好相关特性的 Kasami 序列族

1985 年，M. K. Simon 和 J. K. Omura 在文[5]中给出了二元 Kasami 序列族定义：设 n 为正偶数，$m=n/2,N=2^n-1,T=(2^n-1)|(2^m-1)=2^m+1$。$\alpha$ 为 GF(2^n)中一个本原元。令 $S=\{S_i(t)|0\leqslant t\leqslant N-1,1\leqslant i\leqslant 2^m\}$，其中 $S_i(t)=\mathrm{tr}_1^m\{\mathrm{tr}_m^n(\alpha^t)+r_i\cdot\alpha^{T\cdot t}\}$。这里 $r_i\in$ GF(2^m)。在文[5]中，M. K. Simon 和 J. K. Omura 证明如下结论：设 $R_{i,j}(\tau)$为二元 Kasami 序列族 S 的互相关函数，则 $R_{i,j}(\tau)\in\{2^n-1,-1,2^m-1,-2^m-1\}$。由此可知，Kasami 序列互相关函数到达 Welch 下限。它是一类具有良好相关特性的码序列。

1992 年，S. C. Lin 和 J. J. Komo 将二元 Kasami 序列推广到一般有限域 GF(P)上，得到 P 元 Kasami 序列概念。证明了如下结论。

定理 5　设 $R_{ij}(\tau)$表示 P 元 Kasami 序列的互相关函数，则 $R_{ij}(\tau)\in\{P^n-1,-1,-P^m-1,-1-w^KP^m\}$　$K=1,2,\cdots P-1$，并且分配如下：

P^n-1 出现 P^m 次，-1 出现 $(P^n-2)\cdot P^m$ 次

$-P^m-1$ 出现 $P^m(P^m-1)+(P^n-2)P^m(P^{m-1}-1)$ 次

$-1-w^KP^m$ 出现 $(P^n-2)\cdot P^{n-1}$ 次，$k\neq 1,2,\cdots,P-1$，其中 $w=e^{2\pi\sqrt{-1}/P}$。

参 考 文 献

1　Welch L. R. Lower Bounds On the Maximun Cross Correlation of Signals. IEEE Trans IT 1976,20(5):397～399

2　Scholtz R. A. Welch. L. R. GMW Sequences. IEEE Trans IT 1984,30(3):548～553

3　Antweiler M. ,Böherl. Complex Sequenes over GF(P^m) with a Two－level Autocorrelation Function and a large linear span. IEEE Trans IT,1992 38(1):120～129

4　NO J. S,Kumar P. V. A New Faminly of Binary pseudorndom Sequences Having optimal periodic Correlation Properties and Large Linear span. IEEE Trass IT,1989,35(2):371～379

5　Simon M. K. Omura J. K,. Spread spectrum communication. Vol I Rockvide Mp,comp ter Science press., 1985

6　李超. 一类复数序列的自相关函数. 科学通报 1993,38(23)

7　李超. 一类二元序列的互相关函数. 通信学报，1995,16(3)

（责任编辑　潘生）