国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第16卷第2期 1994年6月 Vol. 16 No. 2

No Sequences 互相关函数值的分配*

李 超 谢端强

（国防科技大学系统工程与数学系 长沙 410073）

摘 要 讨论了 No Sequences 的互相关特性，证明了 No Sequences 的互相关函数一定取集合 $\{2^n-1, -2^m-1, -1, 2^m-1\}$ 中的每一个值，并且给出它们各自的分配。

关键词 迹函数；乘法特征；互相关函数

分类号 TN918.1

在扩频通信和密码学中，伪随机序列具有广泛的应用，一个理想的伪随机序列应当具有较低的非平凡相关函数值，同时具有大的线性复杂度。自 1984 年 Scholtz 和 Welch 利用迹函数构造二元 GMW 序列[1]以来，国内外许多学者都热衷于利用有限域上迹函数的优美理论来构造各种相关特性良好的伪随机序列，如二元 Kasami 序列[2]，P 元 GMW 序列[3]，P 元 Kasami 序列[4]，扩展的 GMW 序列[5],[9]。1989 年 J. S. NO 和 P. V. Kumar 利用迹函数构造一类具有理想相关特性和大的线性复杂度的二元序列——NO Sequences[6]，证明了 NO Sequences 的互相关函数可能取值为 $\{2^n-1, -2^m-1, -1, 2^m-1\}$。本文进一步证明 NO Sequences 的互相关函数一定取集合 $\{2^n-1, -2^m-1, -1, 2^m-1\}$ 中每一个值，并给出它们各自的分配情况。

1 No Sequences 模型

首先介绍文献［6］中 NO Sequences 的概念。设 n 为一个正偶数，$N=2^n-1$，$m=\frac{n}{2}$，$T=2^m+1$，令 $S=\{S_i(t) \mid 0\leqslant t\leqslant N-1,\ 1\leqslant i\leqslant 2^m\}$，其中 $S_i(t)=\mathrm{tr}_1^m\{[tr_m^n(g^{2t})+r_i g^{T\cdot t}]^r\}$。这里 $tr_L^K(\cdot)$ 表示从有限域 $GF(2^K)$ 到 $GF(2^L)$ 的迹函数，g 为 $GF(2^n)$ 中本原元，$1\leqslant r<2^m-1$，$(r, 2^m-1)=1$，$\gamma^i(i=1,2,\cdots,2^m)$ 取遍 $GF(2^m)$ 中每个元，则序列族 $S=\{S_i(t)\}$ 称为 NO Sequences.

易知，当 γ_i 取 $GF(2^m)$ 中零元时，NO Sequences 为一类特殊的二元 GMW 序列，而当 $r=1$ 时，No Sequences 为一类特殊的二元 Kasami 序列。

下面我们来分析 No Sequences 的互相关特性。

* 1993 年 8 月 15 日收稿

2 主要结论及其证明

引理 1[7] 设 $tr_L^K(\cdot)$ 是从有限域 GF(2^K)到 GF(2^L)的迹函数(L|K)，即对任意 $\alpha\in$ GF(2^K)，$tr_L^K(\alpha)=\alpha+\alpha^{2^L}+\cdots+\alpha^{2^{(\frac{K}{L}-1)L}}$则下列性质成立：

(1) 对任意 $\alpha\in GF(2^K)$，$j=0,1,2,\cdots$，$tr_L^K(\alpha)=tr_L^K(\alpha^{2^{Lj}})$ 和 $(tr_L^K(\alpha))^{2^j}=tr_L^K(\alpha^{2^j})$

(2) 对任意 $\alpha.\ \beta\in GF(2^K)$，$a,b\in GF(2^L)$

$$tr_L^K(a\alpha+b\beta)=atr_L^K(\alpha)+btr_L^K(\beta)$$

(3) 对任意 $b\in GF(2^L)$，方程 $tr_L^K(\alpha)=b$ 在 $GF(2^K)$中恰有 2^{K-L}个解 α.

(4) 对任意 $\alpha\in GF(2^K)$，$tr_1^K(\alpha)=tr_1^L(tr_L^K(\alpha))$.

(5) 令 $T=\dfrac{2^K-1}{2^L-1}$，则对任意 i、j，有 $tr_L^K(a\alpha^{j+iT})=\alpha^{iT}tr_L^K(a\alpha^j)$

引理 2[8] 设 α 为 GF(2^n)中本原元，则对任意 $\delta\in GF^*(2^n)=GF(2^n)-\{0\}$，序列 $\{tr_1^n(\alpha^t\delta)\}_{t\geqslant 0}$为二元 n 级 m 序列。

引理 3[7] 方程 $x^k=\beta$(其中 $\beta\in GF(2^n)$)在 $GF(2^n)$中解数为 $N(x^k=\beta)=\sum_{j=0}^{C-1}\lambda^j(\beta)$。其中 $C=(k,2^n-1)$而 λ 为 $GF(2^n)$中阶为 C 的乘法特征。

引理 4 设 λ 是 GF(2^n)中的阶为 2^m-1 的乘法特征，$\mathrm{Ker}\lambda=\{\alpha\,|\,\alpha\in GF(2^n)、\lambda(\alpha)=1\}$则 $\mathrm{Ker}\lambda=\{g^{i(2^m-1)}\,|\,0\leqslant i\leqslant T-1\}$，式中 g 为 GF*(2^n)的本原元，$T=\dfrac{2^n-1}{2^m-1}$.

证明 由于 λ 为 GF(2^n)的阶为 2^m-1 的乘法特征，故由 [7]，对$\forall\ \alpha=g^k$ ($0\leqslant k\leqslant 2^n-2$)

$$\lambda(\alpha)=\lambda(g^k)=e^{\frac{2\pi i}{2^m-1}\cdot k}$$

于是 $\lambda(\alpha)=1$ 当且仅当 $2^m-1|k$，故 $\mathrm{Ker}\lambda=\{g^{i(2^m-1)}\,|\,0\leqslant i\leqslant T-1\}$。

引理 5 设 $n=2m$，$T=\dfrac{2^n-1}{2^m-1}=2^m+1$，$\beta\in GF^*(2^n)$，则方程 $tr_m^n(\beta x^2)=x^T$ 在 GF(2^n) 中非零解数为 $t_0(2^m-1)$，式中 $t_0=|\{\gamma\,|\,\gamma\in\mathrm{GF}(2^n),\ tr_m^n(\gamma)=1,\ 且\ \lambda(\beta^{-1}r)=1\}|$.

证明 由引理 1 性质 (3)，方程 $tr_m^n(x)=1$ 在 GF(2^n)中共有 $2^{n-m}=2^m$ 个解。不妨设为 β_1、β_2，$\cdots$，β_{2m}，易知 $\beta_i\neq 0$ ($i=1,2,\cdots,2^m$)，对每一个 β_i，由引理 3，方程 $\beta x^{2^m-1}=\beta_i$ 在 GF (2^n) 中非零解数为 $N(\beta x^{2^m-1}=\beta_i)=\sum_{j=0}^{C-1}\lambda^j(\beta^{-1}\beta_i)$ 其中 $C=(2^m-1,2^n-1)=2^m-1$. λ 为 GF (2^n) 中阶为 2^m-1 的乘法特征。

如果 $\lambda(\beta^{-1}\beta_i)\neq 1$ 则

$$N(\beta x^{2^m-1}=\beta_i)=\sum_{j=0}^{2^m-2}\lambda^j(\beta^{-1}\beta_i)=\frac{\lambda^{2^m-1}(\beta^{-1}\beta_i)-1}{\lambda(\beta^{-1}\beta_i)-1}=\frac{1-1}{\lambda(\beta^{-1}\beta_k)-1}=0$$

如果 $\lambda(\beta^{-1}\beta_i)=1$ 则

$$N(\beta x^{2^m-1}=\beta_i)=\sum_{j=0}^{2^m-2}\lambda^j(\beta^{-1}\beta_i)=2^m-1$$

而当 $N(\beta x^{2^m-1}=\beta_i)=2^m-1$ 时，不妨设 r_{i1}，r_{i2}，…，r_{i2^m-1} 为 $\beta x^{2^m-1}=\beta_i$ 在 $GF(2^n)$ 中全部解，易知 $r_{ij}\neq 0$（$j=1,2,\cdots,2^m-1$），于是 r_{i1}^{-1}，r_{i2}^{-1}，…，$r_{i2^m-1}^{-1}$ 均为 $tr_m^n(\beta x^2)=x^T$ 在 GF（2^n）中的非零根。又由于若 $tr_m^n(\beta x^2)=x^T$ 在 GF（2^n）中有非零根 γ，则 r 必为上述某个 r_{ij}^{-1}. 故方程 $tr_m^n(\beta x^2)=x^T$ 在 GF（2^n）中非零解数为 $t_0(2^m-1)$，其中 $t_0=|\{r|r\in \mathrm{GF}(2^n), tr_m^n(r)=1 \text{ 且 } \lambda(\beta^{-1}r)=1\}|$，$\lambda$ 为 GF（2^n）中阶为 2^m-1 的乘法特征。

定理 1　设 $R_{i,j}(\tau)$ 为 No Sequences 的互相关函数，则 $R_{i,j}(\tau)$ 一定取 $\{2^n-1, -2^m-1, -1, 2^m-1\}$ 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 $(2^n-2)2^{n-1}$次

证明　设 $t=Tt_1+t_2$，$0\leqslant t_1\leqslant 2^m-2$，$0\leqslant t_2\leqslant T-1$，由引理 1 性质（5）

$$tr_m^n(g^{2(Tt_1+t_2)})=tr_m^n(g^{2Tt_1+2t_2})=g^{2Tt_1}tr_m^n(g^{2t_2})$$

又 $T=2^m+1\equiv 2 \pmod{2^m-1}$，于是 $T^2\equiv 2T \pmod{2^n-1}$ 故 $g^{T^2t_1}=g^{2Tt_1}$，从而

$$S_i(t)=tr_1^m\{[tr_m^n(g^{2t})+r_ig^{Tt}]^r\}=tr_1^m\{[tr_m^n(g^{2(Tt_1+t_2)})+r_ig^{T(t_1T+t_2)}]^r\}$$

$$=tr_1^m\{[g^{2Tt_1}tr_m^n(g^{2t_2})+r_ig^{T^2t_1}g^{Tt_2}]^r\}=tr_1^m\{g^{2Tr_1}[tr_m^n(g^{2t_2})+r_ig^{Tt_2}]^r\}$$

于是 $R_{i,j}(\tau)=\sum_{t=0}^{N-1}(-1)^{S_i(t+\tau)+S_j(\tau)}=\sum_{t_1=0}^{2^m-1}\sum_{t_2=0}^{T-1}(-1)tr_1^m\{g^{2rTt_1}f_1(t_2)\}$

式中 $f_1(t_2)=[tr_m^n(g^{2(t_2+\tau)})+r_ig^{T(t_2+\tau)}]^r+[tr_m^n(g^{2t_2})+r_jg^{Tt_2}]^r$

由于 g 为 $GF(2^n)$ 中本原元，故 g^T 为 $GF(2^m)$ 中本原元，又 $(2, 2^m-1)=(r, 2^m-1)=1$，故 g^{2rT} 为 $GF(2^m)$ 中本原元。

由引理 2，当 $f_1(t_2)\neq 0$ 时，$\{tr_1^m(g^{2rTt_1}f_1(t_2))\}_{t\geqslant 0}$ 为二元 m 级 m 序列。

若设 $z_1=|\{t_2|0\leqslant t_2\leqslant T-1, f_1(t_2)=0\}|$，则

$$R_{i,j}(\tau)=z_1(2^m-1)+(T-z_1)(2^{m-1}-1)-(T-z_1)2^{m-1}$$

$$=(z_1-1)2^m-1$$

下面来计算 z_1 的值，令 $z_2=|\{t|0\leqslant t\leqslant N-1, f_1(t)=0\}|$

由于 $f_1(t+T)=g^{2rT}f_1(t)\ 0\leqslant t\leqslant N-1$

故 $z_1=\dfrac{z_2}{z^m-1}$　又由于 $(r, 2^m-1)=1$

于是 $[tr_m^n(g^{2(t+\tau)}+r_ig^{T(t+\tau)}]^r+[tr_m^n(g^{2t})+r_jg^{Tt}]^r=0$

当且仅当 $tr_m^n\{g^{2t}(1+g^{2\tau})\}+g^{Tt}(r_ig^{T\tau}+r_j)=0$

令 $x=g^t$，$0\leqslant t\leqslant N-1$　$\delta_1=1+g^{2\tau}$　$\delta_2=r_ig^{T\tau}+r_j$，则 x，$\delta_1\in GF(2^n)$，$\delta_2\in GF(2^m)$

于是 $Z_2=|\{x\}\ x\in GF^*(2^n), tr_m^n(x^2\delta_1)=x^T\delta_2\}|$

下面分情况讨论：

（1）若 $\tau=0$ 并且 $r_i=r_j$（这是平凡情况），这时 $\delta_1=\delta_2=0$，故对任意 $x\in GF^*(2^n)$ 都有 $tr_m^n(x^2\delta_1)=x^T\delta_2$，于是 $Z_2=2^n-1$，$Z_1=\dfrac{2^n-1}{2^m-1}=T$

$R_{ij}(\tau)=(z_1-1)2^m-1=2^n-1$

由 τ，r_i，r_j 的取法，可知 2^n-1 出现 2^m 次

(2) 若 $\tau=0$ 并且 $r_i\neq r_j$

则 $\delta_1=0$，$\delta_2\neq 0$ 于是

$z_2=0$　　$z_1=0$

$R_{i,j}(\tau)=(0-1)2^m-1=-2^m-1$

由 τ，r_i，r_j 取法可知　-2^m-1 这时出现 $2^m(2^m-1)$ 次

(3) 若 $\tau\neq 0$　则 $\delta_1\neq 0$

如果 $\delta_2=r_j+r_i\alpha^{T\tau}=0$，则 $tr_m^n(x^2\delta_1)=x^2\delta_2=0$，即 $z_2=|\{x\in GF^*(2^n)$ $tr_m^n(x^2\delta_1)=0\}$.

$tr_m^n(y)=0$ 在 $GF^*(2^n)$ 中共有 $2^{n-m}-1=2^n-1$ 个解，不防设为 y_1，y_2，…，y_{2^m-1}，对每个 y_i $(1\leqslant i\leqslant 2^m-1)$，由于 $(2,2^n-1)=1$，由引理 3，方程 $\delta_1x^2=y_i$ 在 $GF^*(2^n)$ 中恰好有一解。故 $tr_m^n(x^2\delta_1)=0$ 在 $GF^*(2^n)$ 中恰有 2^m-1 个解，于是 $z_2=2^m-1$，$z_1=\dfrac{z_2}{2^m-1}=1$，$R_{i,j}(\tau)=(z_1-1)2^m-1=-1$.

由 τ，r_i，r_j 取法，可知 -1 出现 $(2^n-2)2^m$ 次。

如果 $\delta_2=r_j+r_i\alpha^{T\tau}\neq 0$，令 $\beta=\delta_1\delta_2^{-1}$，则由引理 5

方程 $tr_m^n(x^2\beta)=x^T$ 在 $GF(2^n)$ 中非零解数为 $t_0(2^m-1)$，其中 $t_0=|\{r|r\in GF(2^n)$，$tr_m^n(r)=1$，且 $\lambda(\beta^{-1}r)=1\}|$，这里 λ 为 $GF(2^n)$ 的阶为 2^m-1 的乘法特征。

下证 $t_0=0$ 或 $t_0=2$

事实上，若 $t_0\neq 0$，则存在 $r\in GF^*(2^n)$ 使得 $tr_m^n(r)=1$，并且 $\lambda(\beta^{-1}r)=1$

由 $\lambda(\beta^{-1}r)=1$，存在 $x_0\in GF^*(2^n)$ 使得

$x_0^{2^m-1}=\beta^{-1}r$　　即 $r=\beta x_0^{2^m-1}$

又 $tr_m^n(r)=1$，则 $r+r^{2^m}=1$

即　$\beta x_0^{2^m-1}+(\beta x_0^{2^m-1})^{2^m}=1$

$\beta x_0^{2^m-1}+\beta^{2^m}x_0^{1-2^m}=1$

上式两边同乘以 $x_0^{2^m-1}$ 得

$$\beta(x_0^{2^m-1})^2-x_0^{2^m-1}+\beta^{2^m}=0,\text{既有 }\beta(\beta^{-1}r)^2-(\beta^{-1}r)+\beta^{2^m}=0$$

从而　$r^2-r+\beta^{2^m+1}=0$

于是，r 为 $f(y)=y^2-y+\beta^{2^m+1}$ 的一个根。

又 $f'(y)=-1$　故 $(f(y),f'(y))=1$　即

$f(y)$ 无重根，不妨设 α_1，α_2 为 $f(y)$ 在 $GF(2^n)$ 的扩域中两个根。由于 $\alpha_1+\alpha_2=1$，故 α_1，α_2 或者同在 $GF(2^n)$ 中，或者均不在 $GF(2^n)$ 中。但 $r\in GF(2^n)$，而 r 为 α_1，α_2 中一个，故 α_1，α_2 一定同在 $GF(2^n)$ 中，并且若设 $\alpha_1=r$，则必有 $tr_m^n(\alpha_2)=1$ 且 $\lambda(\beta^{-1}\alpha_2)=1$。这是由于：由 $\alpha_1\alpha_2=\beta^{2^m+1}$ 有 $(\beta^{-1}\alpha_1)(\beta^{-1}\alpha_2)=\beta^{2^m-1}$，于是 $\lambda(\beta^{-1}\alpha_1)\lambda(\beta^{-1}\alpha_2)=\lambda(\beta^{2^m-1})=\lambda^{2^m-1}(\beta)=1$，又 $\lambda(\beta^{-1}\alpha_1)=1$，于是 $\lambda(\beta^{-1}\alpha_2)=1$.

由于 $tr_m^n(\alpha_1+\alpha_2)=tr_m^n(1)=2$，故

$$tr_m^n(\alpha_2)=2-tr_m^n(\alpha_1)=2-1=1$$

于是 $t_0=2$，即当 $\tau\neq 0$ 时，如果 $\delta_2=r_j+r_i\alpha^{T\tau}\neq 0$，则

$R_{i,j}(\tau)$ 或者取 -2^m-1，或者取 2^m-1，而

$R_{i,j}(\tau)$ 取 2^m-1 当且仅当 $t_0=2$。当 τ，r_i 取定之后，则存在常数 μ 和变元 x，使 $\beta=(1+g^{2\tau})(r_j+r_ig^{T\tau})^{-1}=g^{\mu}(g^T)^x$。这里 x 依赖于 r_j 而变化。设：

$$A(m,n)=\{r|r\in GF(2^n)\quad tr_m^n(r)=1\}=\{g^{t_1},g^{t_2},\cdots,g^{t_{2^m}}\}$$

任意取定某个 t_i $(1\leqslant i\leqslant 2^m)$，由于 $(T,2^m-1)=1$，故同余方程 $u+Tx\equiv t_i \pmod{2^m-1}$ 有唯一解 x_0. 对于这样 x_0，相应 $\beta_0=g^{\mu}(g^T)^{x_0}$ 必满足 $\lambda(\beta_0^{-1}g^{t_i})=\lambda(g^{-u-Tx_0+t_i})\lambda(g^{k(2^m-1)})=1$，于是对这样 β_0，必有 $R_{i,j}(\tau)=2^m-1$，这时，β_0 共有 $(2^n-2)2^m$ 种取法。又由于 $t_0=2$，即对于每一个这样 β_0，在 $\{t_1,t_2,\cdots,t_{2^m}\}$ 中恰有两个值满足同一个同余方程。故 t_i 取法共有 $2^m/2=2^{m-1}$ 种，于是 $R_{i,j}(\tau)=2^m-1$ 共出现 $(2^m-2)2^m2^{m-1}=(2^n-2)2^{n-1}$ 次，而这时 $R_{i,j}(\tau)=-2^m-1$ 出现次数：

$(2^n-2)2^m(2^m-1)-(2^n-2)2^m2^{m-1}=(2^n-2)2^m(2^{m-1}-1)$. (证毕)

参 考 文 献

1 R A Scholtz, L R Welch. IEEE Trans I. T, 1984, 30: 548～553

2 M K Simon, R A Scholtz. Rdckricde MD Computer Scitence Press, 1985, 1

3 Markus Antweiler, Leopold Bomer, IEEE Trans I. T, 1992, 38 (1)

4 Shyh-Chang Liu, John J. Komo. IEEE Trans I, T, 1992, 38 (4)

5 Feng Keqin. Applied Mathematics—A Journal of Chinese Univercity, 1992

6 J S No, P V Kurnar. IEEE Trans I. T, 1989, 35 (2)

7 R Lidl, H Niederreiter, Finite Field 1983

8 万哲先. 代数和编码. 科学出版社, 1976

9 李超, 一类复数序列的自相关函数. 科学通报, 1993, 38 (23)

Distribution of Crosscorrelation Function Values of No Sequences

Li Chao Xie Danqiang

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

Abstract

In this paper we discuss the orosscorrelation properties of No sequences. We prove that the crosscorrelation function of No sequences must take on each value of the set $\{2^n-1,-2^m-1,-1,2^m-1\}$, and present the distribution of these crosscorrelation values.

Key words trace function; multiplicative character; crosscorrelation function