Scientific Research

A Family of Binary Sequences with Large Linear Span

Jun CHEN, Yun CHEN

Information Security Institute, Chengdu University of Information Technology, 610225, Chengdu, China

Email: chenjun@cuit.edu.cn, chy@cuit.edu.cns

Abstract: A new family of binary sequences $S^{(r)}$ based on d-form function and Niho sequence is constructed for n=4m, where gcd(2^m-1,r)=1. It is shown that the total number of the sequences with period 2^n-1 is 2^n and maximum correlation of the family is $2^{n/2+2}$-1. Especially, the linear span of the new sequences is proved to be larger than $n2^{n/2-3}$, when r=2^{m-1}-1. Compared to the sequences family constructed in literature [14], the new family in this paper has larger linear span under the conditions of the same maximum correlation and family size..

Keywords: pseudorandom sequence; linear span; low cross-correlation; d-form sequence

一类具有大线性复杂度的二元序列集

陈　俊，陈　运

成都信息工程学院信息安全研究所，成都，中国，610225

Email:　chenjun@cuit..edu.cn, chy@cuit.edu.cn

摘　要:对正整数 $n=4m$，基于 d-型函数和 Niho 序列集，文中构造了一类周期为 2^n-1，序列数目为 2^n，最大相关函数值为 $2^{n/2+2}-1$ 的序列集 $S^{(r)}$，其中 $\gcd(r,2^n-1)=1$；特别地，当 $r=2^{m-1}-1$ 时，证明了该序列集中的序列的线性复杂度都大于 $n2^{n/2-3}$。文中构造的序列集与文献[14]中构造的序列集具有相同的相关函数值和序列数目，但拥有更大的线性复杂度。

关键词：伪随机序列；线性复杂度；低相关性；d-型序列

1 引言

在码分多址通信系统中，广泛使用具有低相关特性、较多序列数目和大线性复杂度的伪随机序列集。序列间的低相关性可降低来自同一信道中其他用户的干扰，较多的序列数目可以增加系统的容量，而较大的线性复杂度可以抵抗基于 Berlekamp-Massey 算法实施的攻击。因此，构造同时具有低相关特性和大线性复杂度，又包含较多序列的伪随机序列集具有重要的意义。

人们已经构造出了许多具有低相关特性的序列集，如文献[1],[2],[3],[5],[6],[7],[8],[9]中的序列集。这些序列集都不同时具有低相关特性、大线性复杂和较多的序列数目,例如文献[7],[8],[9]中的序列集具有低相关特性和大线性复杂度，但序列的数目相对于其长度较少，文献[2],[3]中序列集拥有最优的相关特性，但序列数目较少且线性复杂度很低，文献[1],[5],[6]中序列集有较多的序列数目和较好的相关特性，但线性复杂度同样很低。

资助信息：国家自然科学基金资助项目(60873216)

本文基于 d-型函数和 Niho 序列集，构造了一类新的序列集，该序列集的序列数目为 2^n,相关函数的最大边峰值为 $2^{n/2+2}-1$,线性复杂度大于 $n2^{n/2-3}$。

2 预备知识

设 $S=\{s_i \mid 0\le i\le M-1\}$ 是由 M 条周期为 N 的二元序列组成的序列集，其中 $s_i=\{s_i(t)\}_{t=0}^{N-1}$, $s_i(t)\in\{0,1\}$.

序列 s_i 和 s_j 的周期相关函数定义为：

$$R_{i,j}(\tau)=\sum_{t=0}^{N-1}(-1)^{s_i(t)+s_j(t+\tau)}$$

其中 $0\le i,j\le M-1$，$0\le\tau<N$，$t+\tau$ 是模 N 加。

序列集 S 的周期相关函数的最大边峰值 $R_{\max}$ 定义为 $R_{\max}=\max\{|R_{i,j}(\tau)| i\ne j$ 或 $\tau\ne 0\}$。

令 $GF(2^n)$ 表示含有 2^n 个元素的有限域。

设正整数 n,m,e 满足 $n=me$，定义从 $GF(2^n)$ 到 $GF(2^m)$ 的迹函数为

$$tr_m^n(x)=\sum_{k=0}^{e-1}x^{2^{mk}},$$

其中 $x\in GF(2^n)$。

迹函数的性质参见文献[4]。

定义 1[7] 设 $n=me$，$e\geq 2$，$H(x)$ 是从 $GF(2^n)$ 到 $GF(2^m)$ 的函数，d 是一个正整数，如果对于任意的 $x\in GF(2^n)$ 和 $y\in GF(2^m)$，有

$$H(yx)=y^dH(x),$$

那么称 $H(x)$ 为从 $GF(2^n)$ 到 $GF(2^m)$ 的 d-型函数。

定义 2[7] 设 $n=me$，$e\geq 2$，$H(x)$ 是从 $GF(2^n)$ 到 $GF(2^m)$ 的 d-型函数，r 是一个正整数，并且满足条件 $\gcd(r,2^m-1)=\gcd(d,2^m-1)=1$，$\alpha$ 是 $GF(2^n)$ 的一个本原元，那么称序列

$$s=\left\{s(t)=tr_1^m\left([H(\alpha^t)]^r\right)\right\}_{t=0}^{2^n-2}$$

为 d-型序列。

引理 1[7] 设 $n=me$，$e\geq 2$，$r\geq 1$，$\gcd(r,2^m-1)=1$，$f_0(x),f_1(x)\cdots,f_{M-1}(x)$ 分别是从 $GF(2^n)$ 到 $GF(2^m)$ 的 d-型函数，并且满足 $\gcd(d,2^m-1)=1$。令 α 是有限域 $GF(2^n)$ 的一个本原元，序列集定义为

$$S^{(r)}=\{s_0^{(r)},s_1^{(r)},\cdots,s_{M-1}^{(r)}\},$$

其中

$$s_i^{(r)}=\{s_i^{(r)}(t)=tr_1^m([f_i(\alpha^t)]^r)\}_{t=0}^{2^n-2},$$

则 $S^{(r)}$ 和 $S^{(1)}$ 具有相同的相关函数值。

3. 序列集的构造

下文中总令 α 表示有限域 $GF(2^n)$ 的一个本原元，$\gamma_i\in GF(2^n),i=0,1,\cdots,2^n-1$，$r=2^{m-1}-1$，$n=4m$。

定义新序列集为，

$$S^{(r)}=\{s_0^{(r)},s_1^{(r)},\cdots,s_{2^n-1}^{(r)}\},$$

其中 $s_i^{(r)}=\{s_i^{(r)}(t)=tr_1^m\{[tr_m^n(\alpha^t+\gamma_i\alpha^{(3\cdot 2^{2m}-2)t}]^r\}\}_{t=0}^{2^n-2}$.

对 $0\leq i\leq 2^n-1$，令 $f_i(x)=tr_m^n(x+\gamma_i x^{3\cdot 2^{2m}-2})$，则有 $s_i^{(r)}(t)=tr_1^m\{[f_i(\alpha^t)]^r\}$。

因为对任意的 $z\in GF(2^m)$，有 $z^{2^m-1}=1$，所以

$$\begin{aligned}f_i(zx)&=tr_m^n[zx+\gamma_i(zx)^{3\cdot 2^{2m}-2}]\\&=ztr_m^n(x)+ztr_m^n(\gamma_i x^{3\cdot 2^{2m}-2})\\&=zf_i(x).\end{aligned}$$

从而 $f_0(x),f_1(x),f_2(x),\cdots,f_{2^n-1}(x)$ 分别是从 $GF(2^n)$ 到 $GF(2^m)$ 的 1-型函数。又因为 $\gcd(2^m-1,2^{m-1}-1)=1$，所以根据定义 2，序列

$$s_i^{(r)}=\{s_i^{(r)}(t)=tr_1^m\{[f_i(\alpha^t)]^r\}\}_{t=0}^{2^n-2}$$

是 1-型序列，因此由引理 1 知 $S^{(r)}$ 和 $S^{(1)}$ 具有相同的相关函数值。

由文[12]知，$S^{(1)}$ 的最大边峰值 $R_{\max}=2^{n/2+2}-1$. 因此本文构造的序列集 $S^{(r)}$ 的最大边峰值同样也为 $2^{n/2+2}-1$。

下面证明序列集 $S^{(r)}$ 中的序列具有较大的线性复杂度，并且大于(除 $\gamma_i=0$ 外)文献[14]中序列的线性复杂度。

令 $LS(s_i^{(r)})$ 为序列 $s_i^{(r)}$ 的线性复杂度。由文献[11]知，若将 $s_i^{(r)}(t)$ 表示成 α^t 的多项式，则 $s_i^{(r)}$ 的线性复杂度就等于该多项式中包含的 α^t 的单项式的数目。若令 $x=\alpha^t$，则 $s_i^{(r)}(x)=tr_1^m\{[tr_m^{4m}(x+\gamma_i x^{3\cdot 2^{2m}-2})]^r\}$ 的展开式中关于 x 的单项式的个数就等于 $LS(s_i^{(r)})$。

令 $y=x^{2^{2m}-1}$，则

$$\begin{aligned}s_i^{(r)}(x)&=tr_1^m\{[tr_m^{4m}(x+\gamma_i x^{3\cdot 2^{2m}-2})]^r\}\\&=tr_1^m\{[tr_m^{2m}(xy^{-2}(\gamma_i^{2^{2m}}+y^2+y^3+\gamma_i y^5))]^r\}\\&=\sum_{k=0}^{m-1}\{\sum_{j=0}^{1}[xy^{-2}(\gamma_i^{2^{2m}}\\&\quad+y^2+y^3+\gamma_i y^5)]^{2^{mj}}\}^{2^k r}.\end{aligned}$$

若令 $\Delta_k(x)=\{\sum_{j=0}^{1}[xy^{-2}(\gamma_i^{2^{2m}}+y^2+y^3+\gamma_i y^5)]^{2^{mj}}\}^{2^k r}$ 则有如下的引理。

引理 2 对 $k\neq k'$，$\Delta_k(x)$ 的展开式中关于变量 x 的单项式的指数与 $\Delta_{k'}(x)$ 的展开式中关于变量 x 的单项式的指数互不相同。

证明：令 **A** 和 **B** 分别表示 $(\sum_{j=0}^{1}x^{2^{mj}})^{2^k r}$ 和 $\Delta_k(x)$ 的展开式中关于变量 x 的指数构成的集合。那么，因为 $y=x^{2^{2m}-1}$，所以若将集合 **A** 和 **B** 中的每个元素都模 $2^{2m}-1$，则 **A** 和 **B** 相等，即 $\mathbf{A}\equiv\mathbf{B}\bmod 2^{2m}-1$。因此，只需要比较 $(\sum_{j=0}^{1}x^{2^{mj}})^r$ 和 $(\sum_{j=0}^{1}x^{2^{mj}})^{2^k r}$ 的展开式中是否有相同指数(模 $2^{2m}-1$ 情况下)的 x 的单项式。

根据文献[7]中引理 1 的证明可以知道 $(\sum_{j=0}^{1}x^{2^{mj}})^r$ 和 $(\sum_{j=0}^{1}x^{2^{mj}})^{2^k r}$ 中不存在相同指数(模 $2^{2m}-1$ 情况下)的 x 的单项式，从而有引理 2 成立。证毕。

若用 $|\Delta_k(x)|$ 表示 $\Delta_k(x)$ 中关于 x 的单项式的数目，则由引理 2 可知，$LS(s_i^{(r)})=m\cdot|\Delta_0(x)|$.

采用与文献[7]中命题 3 相同的证明方法，可以证明 $\Delta_0(x)=\sum_{\bar{a}}[xy^{-2}(\gamma_i^{2^{2m}}+y^2+y^3+\gamma_i y^5)]^{\sum_{l=0}^{1}a_l 2^{ml}}$，其中的求和取遍所有满足 $a_0+a_1=2^{m-1}-1$ 及 $a_0\geq 0$，$a_1\geq 0$ 的向量 $\bar{a}=(a_0,a_1)$。

令 $\mathrm{T}_{\bar{a}}=[xy^{-2}(\gamma_i^{2^{2m}}+y^2+y^3+\gamma_i y^5)]^{\sum_{l=0}^{1}a_l 2^{ml}}$，则有下面的引理成立。

引理 3 若向量 $\bar{a}=(a_0,a_1)\neq\bar{a}'=(a_0',a_1')$，则 $\mathrm{T}_{\bar{a}}$ 和 $\mathrm{T}_{\bar{a}'}$ 的展开式中不存在指数相同的 x 的单项式。

证明：因为 $y=x^{2^{2m}-1}$，所以 $T_{\bar{a}}$ 的展开式中，变量 x 的指数模 $2^{2m}-1$ 同余 $\sum_{l=0}^{1}a_l 2^{ml}$。因为 $\sum_{l=0}^{1}a_l 2^{ml}$ 是某个正整数的 2^m 进制表示，并且 $\sum_{l=0}^{1}a_l 2^{ml}<2^{2m}+1$，所以当 $(a_0,a_1)\neq(a_0',a_1')$，一定有 $\sum_{l=0}^{1}a_l 2^{ml}\neq\sum_{l=0}^{1}a_l' 2^{ml}$，从而引理 3 成立。证毕。

根据引理 2 和引理 3，有如下的命题成立。

命题 1　序列 $s_i^{(r)}$ 的线性复杂度

$$LS(s_i^{(r)})=m\cdot\sum_{\bar{a}}|(\gamma_i^{2^{2m}}+y^2+y^3+\gamma_i y^5)^{\sum_{l=0}^{1}a_l 2^{ml}}| \quad (1)$$

其中 $\bar{a}=(a_0,a_1)$，$a_0+a_1=2^{m-1}-1$，$a_0\geq 0$ 和 $a_1\geq 0$。

$$令\ \Gamma_i(y)=(\gamma_i^{2^{2m}}+y^2+y^3+\gamma_i y^5)^{\sum_{l=0}^{1}a_l 2^{ml}}. \quad (2)$$

因为当 $\sum_{l=0}^{1}a_l 2^{ml}$ 为一般值时，很难精确计算在 $\Gamma_i(y)$ 的展开式中，单项式 y 的数目，所以下面考虑当 $\sum_{l=0}^{1}a_l 2^{ml}$ 取某些特殊值时，$\Gamma_i(y)$ 的展开式中关于 y 的单项式的数目，为此需要引理 4 和 5。

引理 4　设 $c=\sum_{j=0}^{l}t_j 2^{2j}+2^{2l+l'}\sum_{i=0}^{s}k_i 2^{2i}$，$l'\geq 2$。如果存在不全为零的整数 $t_0,t_1,\cdots,t_l,k_0,k_1,\cdots,k_s$，使得 $c=0$，那么一定存在某个 t_j 或 k_i，使得 $t_j\equiv 0 \bmod 4$ 或 $k_i\equiv 0 \bmod 4$，但 $t_j\neq 0$ 且 $k_i\neq 0$。

证明：假设 $\sum_{j=u}^{l}t_j 2^{2j}+2^{2l+l'}\sum_{i=0}^{s}k_i 2^{2i}=0$，其中 u 是使得 $t_u\neq 0$ 的最小正整数，则有

$$\sum_{j=u}^{l}t_j 2^{2j-2u}+2^{2l+l'-2u}\sum_{i=0}^{s}k_i 2^{2i}=0$$

从而 $t_u\equiv 0 \bmod 4$。同样，若 $t_j=0, j=0,1,\cdots,l$，而存在不全为零的 $k_0,k_1,\cdots,k_s$ 使得 $\sum_{i=0}^{s}k_i 2^{2i}=0$，那么一定有某个 $k_v\equiv 0 \bmod 4$，但 $k_v\neq 0$。证毕。

引理 5　设 m 为正奇数，整数 a 满足

$$-2(2^{2m}+1)<c<2(2^{2m}+1)$$

其中 $c=\sum_{j=0}^{(m-3)/2}t_j 2^{2j}+2^{m+1}\sum_{i=0}^{(m-3)/2}k_i 2^{2i}$，$t_j,k_i\in\{-5,-3,-2,-1,0,1,2,3,5\}$，那么若 $c\equiv 0 \bmod 2^{2m}+1$，则一定有 $c=0$，并且对所有的 i,j，有 $t_j=0,k_i=0$.

证明：根据题设条件易知，如果 $c\equiv 0 \bmod 2^{2m}+1$，那么有 $c=0$ 或 $c=\pm(2^{2m}+1)$。下面采用反证法证明 $c=\pm(2^{2m}+1)$ 不成立。

不妨设 $c=2^{2m}+1$，c 如题设所述。此时有

$$\sum_{j=0}^{(m-3)/2}t_j 2^{2j}+2^{m+1}\sum_{i=0}^{(m-3)/2}k_i 2^{2i}=2^{2m}+1 \quad (3)$$

从而有 $t_0\equiv 1 \bmod 4$。故而(3)变换为

$$\sum_{j=1}^{(m-3)/2}t_j 2^{2j}+2^{m+1}\sum_{i=0}^{(m-3)/2}k_i 2^{2i}=2^{2m}+4b_0 \quad (4)$$

其中 $b_0\in\{-1,0,1\}$。

由(4)式可知，必有 $t_1\neq 0$。否则，若 $b_0\neq 0$，则(4)显然不成立；而若 $b_0=0$，则由引理 4 知，此时存在某个 $t_j\equiv 0 \bmod 4$，$j>1$，而 $t_j\neq 0$；或者存在某个 $k_i\equiv 0 \bmod 4$，而 $k_i\neq 0$。此与题设矛盾。由对(3)的讨论知，若(4)式成立，则可变换为

$$\sum_{j=2}^{(m-3)/2}t_j 4^{j-1}+2^{m-1}\sum_{i=0}^{(m-3)/2}k_i 4^i=4^{m-1}+4b_1 \quad (5)$$

其中 $b_1\in\{-1,0,1\}$。

对(5)式进行如同对(4)的讨论知道，此时必有 $t_2\neq 0$。将这样的讨论重复下去可知，若(3)式要成立，则必有下式成立，即有

$$4^2\sum_{i=0}^{(m-3)/2}k_i 4^i=4^{(m+3)/2}+4b_{(m-3)/2} \quad (6)$$

其中 $b_{(m-3)/2}\in\{-1,0,1\}$。

若 $b_{(m-3)/2}\neq 0$，则(6)式显然不成立;若 $b_{(m-3)/2}=0$，则由引理 4 知,此时存在 $k_i\equiv 0 \bmod 4$，但 $k_i\neq 0$。此与题设矛盾。

综上所述，在题设的条件下只能有 $c=0$。再根据引理 4 知，对所有的 i,j，有 $t_j=0,k_i=0$。证毕。

引理 6　当 m 为奇数时，如果 $a_0=(2^{m-1}-1)/3$，$a_1=(2^m-2)/3$ 或 $a_0=(2^m-2)/3$，$a_1=(2^{m-1}-1)/3$，那么 $\Gamma_i(y)$ 的展开式中 y 的指数在模 $2^{2m}+1$ 的情况下互不相同；当 m 为偶数时，如果 $a_0=(2^m-1)/3$，且 $a_1=(2^{m-1}-2)/3$ 或 $a_0=(2^{m-1}-2)/3$，$a_1=(2^m-1)/3$，那么 $\Gamma_i(y)$ 的展开式中 y 的指数在模 $2^{2m}+1$ 的情况下也互不相同。

证明：情形 1. m 为奇数。

1).如果 $a_0=(2^{m-1}-1)/3, a_1=(2^m-2)/3$，那么满足 $a_0+a_1=2^{m-1}-1$。

令 b 表示 $\Gamma_i(y)$ 的展开式中 y 的指数，则有

$$b=\sum_{j=0}^{(m-3)/2}t_j 2^{2j}+2^{m+1}\sum_{i=0}^{(m-3)/2}k_i 2^{2i} \quad (7)$$

其中 $t_j,k_i\in\{0,2,3,5\}$。

如果存在 $b'=\sum_{j=0}^{(m-3)/2}t_j' 2^{2j}+2^{m+1}\sum_{i=0}^{(m-3)/2}k_i' 2^{2i}$，使得 $b\equiv b' \bmod 2^{2m}+1$，那么因为

$$b-b'=\sum_{j=0}^{(m-3)/2}(t_j-t_j')2^{2j}+2^{m+1}\sum_{i=0}^{(m-3)/2}(k_i-k_i')2^{2i} \quad (8)$$

其中 $(t_j-t_j'),(k_i-k_i')\in\{-5,-3,-2,-1,0,1,2,3,5\}$，所以可知 $-2(2^{2m}+1)<b-b'<2(2^{2m}+1)$，从而根据引理 5 可得，$b=b'$，并且 $t_j=t_j'$，$k_i=k_i'$。

2).如果 $a_0=(2^m-2)/3, a_1=(2^{m-1}-1)/3$，，那么也有 $a_0+a_1=2^{m-1}-1$。

此时 $\Gamma_i(y)$ 的展开式中变量 y 的指数 b 为

$$b=2\sum_{j=0}^{(m-3)/2}t_j 2^{2j}+2^m\sum_{i=0}^{(m-3)/2}k_i 2^{2i} \quad (9)$$

其中 $t_j,k_i\in\{0,2,3,5\}$。

如果存在 $b'=2\sum_{j=0}^{(m-3)/2}t_j' 2^{2j}+2^m\sum_{i=0}^{(m-3)/2}k_i' 2^{2i}$，使得

978-1-935068-10-5 © 2010 SciRes.

$b-b'\equiv 0 \bmod 2^{2m}+1$，那么又因为 $-2(2^{2m}+1)<b-b'<2(2^{2m}+1)$，并且 $b-b'$ 为偶数，所以一定有 $b-b'=0$，从而再根据引理 4 可知，此时有 $t_j=t_j',k_i=k_i'$。

情形 2. m 为偶数。

1). 如果 $a_0=(2^m-1)/3,a_1=(2^{m-1}-2)/3$，那么我们有 $a_0+a_1 2^m=(2^{2m-1}-2^m-1)/3$，且 $a_0+a_1=2^{m-1}-1$。

此时 $\Gamma_i(y)$ 的展开式中，变量 y 的指数 b 满足 $b\le 5(a_0+a_1 2^m)<2^{2m}+1$，并且

$$b=\sum_{j=0}^{(m-2)/2}t_j 2^{2j}+2^{m+1}\sum_{i=0}^{(m-4)/2}k_i 2^{2i}, \qquad (10)$$

其中 $t_j,k_i\in\{0,2,3,5\}$。

若存在 $b'=\sum_{j=0}^{(m-2)/2}t_j' 2^{2j}+2^{m+1}\sum_{i=0}^{(m-4)/2}k_i' 2^{2i}$，使得 $b-b'=\sum_{j=0}^{(m-2)/2}(t_j-t_j')2^{2j}+2^{m+1}\sum_{i=0}^{(m-4)/2}(k_i-k_i')2^{2i}=0$，其中 $(t_j-t_j'),(k_i-k_i')\in\{-5,-3,-2,-1,0,1,2,3,5\}$，则由引理 4 可知，此时有，$t_j=t_j',k_i=k_i'$。

2). 如果 $a_0=(2^{m-1}-2)/3,a_1=(2^m-1)/3$，那么也有 $a_0+a_1=2^{m-1}-1$，且 $a_0+a_1 2^m=(2^{2m}-2^{m-1}-2)/3$。

此时，$\Gamma_i(y)$ 中 y 的指数 b 为

$$b=2\sum_{j=0}^{(m-4)/2}t_j 2^{2j}+2^m\sum_{i=0}^{(m-2)/2}k_i 2^{2i}. \qquad (11)$$

如果存在 $b'=2\sum_{j=0}^{(m-4)/2}t_j' 2^{2j}+2^m\sum_{i=0}^{(m-2)/2}k_i' 2^{2i}$，使得 $b-b'\equiv 0 \bmod 2^{2m}+1$，其中 $t_j',k_i'\in\{0,2,3,5\}$. 那么因为 $-2(2^{2m}+1)<b-b'<2(2^{2m}+1)$，并且 $b-b'$ 是偶数，所以有 $b-b'=0$，从而由引理 4，对所有的 i,j，有 $t_j=t_j'$，$k_i=k_i'$。

根据情形 1 和情形 2 知，当向量 (a_0,a_1) 的选择满足引理 6 中题设条件时，$\Gamma_i(y)$ 的展开式中，y 的指数在模 $2^{2m}+1$ 的情况下互不相同。证毕。

定理 1　设 $r=2^{m-1}-1$，那么当 $\gamma_i\neq 0$ 时，序列 $s_i^{(r)}$ 的线性复杂度 $LS(s_i^{(r)})>n\cdot 2^{n/2-3}$；而当 $\gamma_i=0$ 时，$LS(s_i^{(r)})=n\cdot 2^{n/2-4}$。

证明：在(2)式中,当向量 (a_0,a_1) 的选择满足引理 6 中的条件时，有 $a_0+a_1=2^{m-1}-1$。根据引理 6 知，当 $\gamma_i\neq 0$ 时，$\Gamma_i(y)$ 的展开式中共有 4^{m-1} 个指数(模 $2^{2m}+1$)互不相同的 y 的单项式。再由命题 1 知，当 $\gamma_i\neq 0$ 时，序列 $s_i^{(r)}$ 的线性复杂度 $LS(s_i^{(r)})>m\cdot 2\cdot 4^{m-1}=n\cdot 2^{n/2-3}$；而当 $\gamma_i=0$ 时，序列为 GMW 序列，因此其线性复杂度 $LS(s_i^{(r)})=n\cdot 2^{n/2-4}$。证毕。

表 1 列出了本文构造的序列集 $S^{(r)}$ 与文[14]中序列集的性质比较。

Table 1. the comparison between this sequence set and the sequence set in the paper [14]

表 1　本文序列集与文[14]中序列集的比较

序列	n	序列数目	最大边峰值	最大线性复杂度
文[14]中序列	$4m$	2^n	$2^{(n+4)/2}-1$	$n\cdot 2^{n/2-3}$
本文的序列	$4m$	2^n	$2^{(n+2)/2}-1$	$>n\cdot 2^{n/2-3}$

表 2 中给出了当 $n=4m,m=3,4,\cdots,7$ 时,本文序列的线性复杂度的数值解与文献[14]中序列的线性复杂度。

Table 2 the comparison of linear complexity between this sequence and the sequence in the paper [14]

表 2　本文序列与文[14]中序列的线性复杂度比较

m	本文中序列的线性复杂度 (序列数目)	文献[14]中序列的线性复杂度 (序列数目)
3	48(1),168(1),180(其余)	96（全部）
4	256(1),1344(1),1632(其余)	512（全部）
5	1280(1),13580(其余)	2560(全部)
6	6144(1),72864(1),108480 其余)	12288(全部)
7	28672(1),498792(1),831208(其余)	57344(全部)

由表 1 可知，本文构造的序列集 $S^{(r)}$ 与文[14]中序列集有相同的序列数目、序列长度和最大边峰值，但拥有更大(除 GMW 序列外)的线性复杂度，并且从表 2 可以看出，随着 m 的增大，本文中序列的线性复杂度远大于文[14]中序列的线性复杂度。

4 结论

本文基于 d-型函数和 Niho 序列集构造了一类具有大线性复杂度的低相关序列集，该序列集与文献[14]中的序列集有相同的相关函数值和序列数目，但拥有更大的线性复杂度。若将这类序列用于码分多址通信系统，可以提高系统的安全性。

References (参考文献)

[1] Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions [J]. IEEE Trans. Inform. Theory, 1968, 14(1), P154-156.
[2] Kasami T. Weight distribution Formula for some class of cyclic codes[R]. Coordinated Sci Lab, Univ Illinois,Urbana, IL, 1996.
[3] Olsen J D, Scholtz R A and Welch L R. Bent function sequences [J]. IEEE Trans. Inform. Theory, 1982, 28(6), P858-864.
[4] Lidl R, Niederreiter H. Introduction to Finite Fields and their Applications. Cambridge: Cambridge University Press, 1994.
[5] Kasami T. Weight distribution of Bose-Chaudhuri-Hocq-uen ghem codes [M]. Combinatorial Mathematics and Its Applic ations, R. C. Bose and T. A. Dowling, Eds. Chapel Hill, NC: Univ. North Carolina Press, 1969, P335–357.
[6] Zeng X, Liu J Q and Hu L. Generalized Kasami sequences: the

large set [J], IEEE Trans. Inform. Theory, 2007, 53(7):, P2587-2598.
[7] Klapper A. d-form sequences: families of sequences with low correlation values and large linear spans [J]. IEEE Trans. Inform. Theory, 1995, 41(2):, P423-431.
[8] No J S, Kumar P V. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span [J]. IEEE Trans. Inform. Theory, 1989, 35(2):, P371-379.
[9] Zeng X, Hu L, Liu J Q, and Zhu Y. A family of binary sequences with optimal correlation property and large linear span [A]. In 2006 IEEE International Conference on Communications (ICC 2006).
[10] Zeng X, Hu L and Jiang W. A family of binary sequences with 4-valued optimal out-of-phase correlation and large linear span [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences., 2007, E89-A(7):, P2029-2035.
[11] Key E L. An analysis of the structure and complexity of nonlinear binary sequence generators [J]. IEEE Trans. Inform. Theory, 1976, 22(6):, P732-736.
[12] [Niho Y. Multivalued Cross-Correlation Functions between Two Maximal Linear Recursive Sequences [D]. Ph.D. Dissertation, Univ. Southern Calif., Los Angeles, 1972.
[13] Helleseth T. Some results about the cross-correlation function between two maximal linear sequences[J]. Discrete Math.16(1976), P301-307
[14] Tang Jinbing, ZENG Xiangyong, HU Lei. On the linear span of a class of low correlation sequence family[J], Journal on Communications, 2008, 29(7), P75-80 (Ch).

978-1-935068-10-5