基于两族函数的低相关二元序列集构造

李胜华[1],曾祥勇[1],胡 磊[2],刘合国[1]
(1.湖北大学数学与计算机科学学院,湖北武汉 430062;2.中科院研究生院信息安全国家重点实验室,北京 100039)

摘 要: 低相关序列集在码分多址(CDMA)扩频通信系统和密码系统中具有极其重要的作用,运用有限域上的函数族能有效地构造相关性较好的序列集.针对 $n\equiv 2(\mathrm{mod}\ 4)$时,本文首次运用阶数为 2^n 的有限域上的两个二次布尔函数族,构造了 $2^{2^{n-2}}$ 个低相关序列集;这里每个序列集包含 2^n+1 条周期为 2^n-1 的二元序列,其最大相关值为 $2^{n/2+1}+1$.这将为通信系统和密码系统提供更多可供选择的序列集.

关键词: 伪随机序列; 低相关; Walsh 谱; 等价类
中图分类号: TN914.5 **文献标识码:** A **文章编号:** 0372-2112 (2007) 11-2215-05

Construction for Families of Binary Sequences with Low Correlation Based on Two Families of Functions

LI Sheng-hua[1], ZENG Xiang-yong[1], HU Lei[2], LIU He-guo[1]
(1. *Faculty of Mathematics and Computer Science, Hubei University, Wuhan, Hubei* 430062, *China*;
2. *State Key Laboratory of Information Security, Graduate School of the Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract: Families of pseudorandom sequences with low correlation are useful in a wide range of applications, such as code-division multiple access(CDMA) communications and cryptology, and the families with desired correlation can be effectively constructed by using function families over finite fields. In this paper, $2^{2^{n-2}}$ families of binary sequences with low correlation are constructed by using two families of Boolean functions over the finite field with 2^n elements, where $n\equiv 2(\mathrm{mod}\ 4)$. There are 2^n+1 binary sequences of period 2^n-1 within each family, and the maximum correlation is $2^{n/2+1}+1$. The proposed construction can provide more families for CDMA communications and cryptology.

Key words: pseudorandom sequence; low correlation; Walsh spectrum; equivalent class

1 引言

低相关伪随机序列在 CDMA 通信系统和密码系统中具有极其重要的作用.在 CDMA 通信系统中具有低相关性的伪随机序列能降低来自同一信道中其他使用者的干扰;另一方面流密码系统中的密钥流序列或数字签名算法中的伪随机序列也应具有低相关性质,这一性质使其能抵抗互相关攻击.经过长期的探索,人们已经积累了许多有限域上低相关序列的构造方法.一种重要的途径是使用密码函数族,如 Bent 序列集[1]由 Bent 函数族构造而成,大、小集合的 Kasami 序列集[2]和 Gold、Gold-like 序列集[3~5]均由二次布尔函数族构造而成.这些序列集都具有较低的相关性,而利用 d-型函数族和函数域能设计高线性复杂度的序列集[6~9].但所有这些低相关序列集只是运用一个函数族来构造,一个自然的问题是能否同时使用两个函数族构造低相关序列集.

本文运用两个二次函数族构造了多个低相关序列集,对上面的问题作了肯定的回答.具体的,在 $n\equiv 2(\mathrm{mod}\ 4)$时,我们运用阶数为 2^n 的有限域上的两个二次布尔函数族构造了 $2^{2^{n-2}}$ 个低相关序列集.所得的每个集合均包含 2^n+1 条周期为 2^n-1 的二元序列,其最大相关值为 $2^{n/2+1}+1$.文献[10,11]中的序列集是本文构造的序列集的两个特例.我们的主要思想是分别在两个函数族中选择若干个函数来构造序列集,这里的选择方案是基于对特征为 2 的有限域的一个等价划分,从而保证所得的序列集具有较好的低相关值.

2 预备知识

以下设 $GF(2^n)$表示元素个数为 2^n 的有限域,$f(x)$是从 $GF(2^n)$到 $GF(2)$的一个函数.

收稿日期:2006-07-07;修回日期:2007-06-07
基金项目:国家自然科学基金(No.60603012, No.60573053);高等学校博士学科点专项科研基金(No.20052512002);湖北省教育厅项目(No.200610004)

设 m,n 为正整数,且 $m|n$, $GF(2^n)$到 $GF(2^m)$的迹函数[12]定义为: $tr_m^n(x)=\sum_{i=0}^{n/m-1}x^{2^{mi}}$.迹函数有如下性质:

(1) $tr_m^n(x^{2^m})=tr_m^n(x)$, $\forall x\in GF(2^n)$;

(2) $tr_1^n(x)=tr_1^m(tr_m^n(x))$, $\forall x\in GF(2^n)$;

(3) $tr_m^n(ax+by)=atr_m^n(x)+btr_m^n(y)$, $\forall x,y\in GF(2^n)$, $a,b\in GF(2^m)$;

(4) $\forall b\in GF(2^m)$, $tr_m^n(x)=b$ 在 $GF(2^n)$中有 2^{n-m} 个根.

$f(x)$的 Walsh 变换[13]定义为:

$$W_f(\lambda)=\sum_{x\in GF(2^n)}(-1)^{f(x)+tr_1^n(\lambda x)}$$

其中 $\lambda\in GF(2^n)$.如果 W_f 的取值为 $\pm 2^{n/2}$,则称 $f(x)$是 Bent 的.

如果 $f(x)$能表示成向量空间 V_2^n 上的代数次数为的布尔函数,则称 $f(x)$为二次型.设 $B_f(x,z)=f(x)+f(z)+f(x+z)$,选取一组基 $\{\gamma_1,\gamma_2,\cdots,\gamma_n\}$,则有 $B_f(x,z)=xQz'$,其中 $x=\sum_{i=1}^{n}x_i\gamma_i$, $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ ($\boldsymbol{x}'$为 $\boldsymbol{x}$ 的转置), $\boldsymbol{Q}$ 为一 $n\times n$ 矩阵.定义 $f(x)$的秩为 $\boldsymbol{Q}$ 的秩,于是 $f(x)$的秩为 $2r$,当且仅当对所有的 $x\in GF(2^n)$,关于 z 的方程 $B_f(x,z)=0$ 有 2^{n-2r}个解[13].

引理 1[13] 如果 $f(x)$的秩为 $2r$, $2\leqslant 2r\leqslant n$,则 $f(x)$的 Walsh 谱值的分布为:

$$W_f(\lambda)=\begin{cases}\pm 2^{n-r}, & 2^{2r-1}\pm 2^{r-1}\text{次}\\ 0, & 2^n-2^{2r}\text{次}\end{cases}$$

设 $S=\{s_0,s_1,\cdots,s_{r-1}\}$是由 r 条周期为 N 的序列组成的序列集. S 中两条序列 $s_i,s_j(0\leqslant i,j<r)$的相关函数 $C_{i,j}(\tau)$定义为: $C_{i,j}(\tau)=\sum_{t=0}^{N-1}(-1)^{s_i(t+\tau)+s_j(t)}$,其中 $0\leqslant\tau\leqslant N-1$.令 $\delta=\max_{i\neq j\text{或}i=j,\tau\neq 0}|C_{i,j}(\tau)|$,称 S 是一个 (N,r,δ)序列集, δ 是 S 的最大相关值.

设 α 为 $GF(2^n)$的本原元,基于 $f(x)$可以定义一个周期为 2^n-1 的二元序列 $a=\{a_i\}_{i\geqslant 0}$,其中 $a_i=f(\alpha_i)$.

引理 2[10] 设 $n=2m\geqslant 4$,含 2^n+1 条二元序列的序列集 S 定义为:

$$s_i(x)=\begin{cases}tr_1^n(v_ix)+\sum_{j=1}^{m-1}tr_1^n(x^{(2^j+1)})+tr_1^m(x^{(2^m+1)}), & 0\leqslant i\leqslant 2^n-1\\ tr_1^n(x), & i=2^n\end{cases}$$

其中 $GF(2^n)=\{v_0,v_1,\cdots,v_{2^n-1}\}$,则 S 的最大相关值为 $2^{n/2+1}+1$,并且其相关函数取以下五个值: -1, $-1\pm 2^{n/2}$, $-1\pm 2^{n/2+1}$.

引理 3[11] 设 $n=em$, e 为正整数, m 为奇数($m\geqslant 3$),含 2^n+1 条二元序列的序列集 U 定义为:

$$u_i(x)=\begin{cases}tr_1^n(u_ix)+\sum_{j=1}^{(m-1)/2}tr_1^n(x^{(2^{ej}+1)}), & 0\leqslant i\leqslant 2^n-1\\ tr_1^n(x), & i=2^n\end{cases}$$

其中 $GF(2^n)=\{u_0,u_1,\cdots,u_{2^n-1}\}$,则 U 的最大相关值为 $2^{(n+e)/2}+1$,并且其相关函数取以下三个值: -1, $-1\pm 2^{(n+e)/2}$.

本文以下部分总设 α 表示 $GF(2^n)$的本原元, $n=2m\geqslant 6$,且 m 为奇数,函数 $p_1(x)$、 $p_2(x)$和 $h(x)$分别定义为

$$p_1(x)=\sum_{j=1}^{(m-1)/2}tr_1^n(x^{2^j+1}),$$

$$p_2(x)=\sum_{j=1}^{m-1}tr_1^n(x^{2^j+1})+tr_1^m(x^{2^m+1}),$$

$$h(x)=p_1(x)+p_2(x)$$

显然,

$$h(x)=\sum_{j=1}^{(m-1)/2}tr_1^n(x^{2^{2j-1}+1})+tr_1^m(x^{2^m+1}) \quad (1)$$

并由文献[10,11],有 $B_{p_1}(x,z)=tr_1^n(x[tr_2^n(z)+z])$, $B_{p_2}(x,z)=tr_1^n(x[tr_1^n(z)+z])$,且 $p_1(x)$和 $p_2(x)$都是 Bent 的.

本文将运用 $p_1(x)$和 $p_2(x)$来构造多个低相关序列集,每个序列集中的一部分序列由 $p_1(x)$构造,另一部分由 $p_2(x)$构造.而分别运用 $p_1(x)$和 $p_2(x)$构造的两个序列的相关值与 $h(x)$在 $GF(2^n)$中两个元素之和处的 Walsh 谱值有关,当谱值为 0 时,它们的相关值很低.因此,为了保证序列的低相关性,下面给出 $GF(2^n)$的一个划分,使得 $h(x)$在不同集合的两个元素之和处的谱值为 0.

3 $GF(2^n)$的一个划分

给出具体划分前,需要以下引理.

引理 4 $tr_2^n(x^{2^m+1})=tr_1^m(x^{2^m+1})$.

证明 显然, $\{(m+1)/2,(m+3)/2,\cdots,m-1\}=\{(m+2i+1)/2|0\leqslant i\leqslant(m-3)/2\}$.由迹函数的定义有,

$$\begin{aligned}tr_2^n(x^{2^m+1})&=\sum_{j=0}^{m-1}(x^{2^m+1})^{2^j}\\&=\sum_{j=0}^{(m-1)/2}x^{2^m+2^j+2^{2j}}+\sum_{j=(m+1)/2}^{m-1}x^{2^m+2^j+2^{2j}}\\&=\sum_{j=0}^{(m-1)/2}x^{2^m+2^j+2^{2j}}+\sum_{j=0}^{(m-3)/2}x^{2^{2m}+2^{2j+1}+2^{m+2j+1}}\\&=\sum_{i=0}^{m-1}x^{2^i+2^{m+i}}=tr_1^m(x^{2^m+1})\end{aligned}$$

证毕

引理 5 $h(x)=[tr_2^n(x)]^3$.

证明 每个固定的整数 j, $\{(2j+2i)\bmod n|0\leqslant i\leqslant m-1\}=\{2k|0\leqslant k\leqslant m-1\}$.因此,

$$\sum_{i=0}^{n-1}(x^{2^{2j-1}+1})^{2^i}=\sum_{i=0}^{m-1}x^{2^{2j-1+2i}+2^{2i}}+\sum_{i=0}^{m-1}x^{2^{2j+2i}+2^{2i+1}}$$
$$=\sum_{i=0}^{m-1}x^{2^{2j-1+2i}+2^{2i}}+\sum_{k=0}^{m-1}x^{2^{2k}+2^{2k-2j+1}}$$
$$=\sum_{i=0}^{m-1}x^{2^{2i}}(x^{2^{2i+2j-1}}+x^{2^{2i-2j+1}})$$

那么,

$$\sum_{j=1}^{(m-1)/2}\sum_{i=0}^{n-1}(x^{2^{2j-1}+1})^{2^i}=\sum_{j=1}^{(m-1)/2}\sum_{i=0}^{m-1}x^{2^{2i}}(x^{2^{2i+2j-1}}+x^{2^{2i-2j+1}})$$
$$=\sum_{i=0}^{m-1}x^{2^{2i}}\sum_{j=1}^{(m-1)/2}(x^{2^{2(j-1)}}+x^{2^{2(m-j)}})^{2^{2i+1}}$$
$$=\sum_{i=0}^{m-1}x^{2^{2i}}(\sum_{k=0}^{m-1}x^{2^{2k}}+x^{2^{m-1}})^{2^{2i+1}}$$
$$=[tr_2^n(x)]^2\sum_{i=0}^{m-1}x^{2^{2i}}+\sum_{i=0}^{m-1}(x^{2^m+1})^{2^{2i}}$$
$$=[tr_2^n(x)]^3+tr_2^n(x^{2^m+1})$$

由式(1)和引理 4,$h(x)=[tr_2^n(x)]^3$. 证毕

引理 6　设 $\Omega=\{\lambda\mid W_h(\lambda)\neq 0\}$,则 $\Omega=GF(2^2)$.

证明　由引理 5,$B_h(x,z)=[tr_2^n(x)]^3[tr_2^n(z)]^3+[tr_2^n(x+z)]^3$,将其简化得 $B_h(x,z)=tr_1^n(x[tr_2^n(z)]^2)$. 根据迹函数的性质,$tr_2^n(z)=0$ 的解数为 2^{n-2},故 hx 的秩为 2. 由引理 1,$|\Omega|=4$.

$$W_h(\lambda)=\sum_{x\in GF(2^n)}(-1)^{h(x)+tr_1^n(\lambda x)}$$
$$=\sum_{x\in\Gamma}(-1)^{tr_1^n(\lambda x)}+\sum_{x\in GF(2^n)\setminus\Gamma}(-1)^{1+tr_1^n(\lambda x)},$$

这里 $\Gamma=\{x\mid tr_2^n(x)=0,x\in GF(2^n)\}$.

当 $\lambda\in GF(2^2)$ 时,$W_h(\lambda)=\sum_{x\in\Gamma}(-1)^0+2^{n-2}$.

$\sum_{x\in GF(2^2)\setminus\{0\}}(-1)^{1+tr_1^2(\lambda x)}=\pm 2^{n-1}$,这说明 $GF(2^n)$ 中使得 $W_h(\lambda)\neq 0$ 的 4 个元素恰好是 $GF(2^2)$ 中的所有元素,即 $\Omega=GF(2^n)$. 证毕

命题 1　存在 $GF(2^n)$ 的一个划分,$G_1,G_2,\cdots,G_{2^{n-2}}$,使得

$$GF(2^n)=\bigcup_{i=1}^{2^{n-2}}G_i,\ G_i\cap G_j=\varnothing,\ \forall\ i\neq j\qquad(2)$$

并且 $h(x)$ 在任意两个不等价元素之和处的 Walsh 谱值为 0.

证明　利用引理 6 中的 Ω 在 $GF(2^n)$ 上定义关系 $\sim$:对 $\forall\ a,b\in GF(2^n)$,$a\sim b$ 当且仅当 $a+b\in\Omega$. 因为 Ω 是 $GF(2^n)$ 的一个子域,所以 $\sim$ 是 $GF(2^n)$ 上的一个等价关系,且该等价关系将 $GF(2^n)$ 划分为 $|GF(2^n)|/|GF(2^2)|=2^{n-2}$ 个等价类,即存在 2^{n-2} 个集合 $G_i,i=1,2,\cdots,2^{n-2}$,满足式(2)且每个等价类形如 $a+\Omega=\{a,a+1,a+\alpha^{(2^n-1)/3},a+a^{2(2^n-1)/3}\}$,$a\in GF(2^n)$. 由引理 6 可知,当 $a\sim b$ 时,$W_h(a+b)\neq 0$,因此当 a,b 不等价时,$W_h(a+b)=0$. 证毕

例 1　设 $GF(2^6)=F_2[x]/(x^6+x+1)$,$\alpha^6+\alpha+1=0$. 根据命题 1,$GF(2^6)$ 可以划分为 16 个子集 $G_i,i=1,2,\cdots,16$,且 $\forall\ a\in G_i,b\in G_j,1\leqslant i\neq j\leqslant 16$,有 $W_h(a+b)=0$. 如果将每个子集 G_i 写成 $\{\alpha^{i_1},\alpha^{i_2},\alpha^{i_3},\alpha^{i_4}\}$ 的形式(约定 $0=\alpha^\infty$),则 $\{i_1,i_2,i_3,i_4\}$ 分别为:$\{\infty,0,21,42\}$;$\{1,6,29,60\}$;$\{2,12,57,58\}$;$\{3,30,32,46\}$;$\{4,24,51,53\}$;$\{5,38,49,62\}$;$\{7,20,26,59\}$;$\{8,39,43,48\}$;$\{9,11,25,45\}$;$\{10,13,35,61\}$;$\{14,40,52,55\}$;$\{15,16,23,33\}$;$\{17,28,41,47\}$;$\{18,22,27,50\}$;$\{19,31,34,56\}$;$\{36,37,44,54\}$.

4　新序列集

设 I_1,I 为指标集,且 $I=\{1,2,3,\cdots,2^{n-2}\}$,$I_1\subseteq I$. 定义二元序列集 $S=\bigcup_{i=1}^{3}S_i$,其中序列集 $S_i(i=1,2,3)$ 分别由下列函数定义:

$$f_1(x)=tr_1^n(ux)+\sum_{j=1}^{(m-1)/2}tr_1^n(x^{2^{2j}+1}),\ u\in\bigcup_{i\in I_1}G_i;$$

$$f_2(x)=tr_1^n(vx)+\sum_{j=1}^{m-1}tr_1^n(x^{2^j+1})+tr_1^m(x^{2^m+1}),$$
$$v\in\bigcup_{i\in I\setminus I_1}G_i;$$

$$f_3(x)=tr_1^n(x),$$

G_i 的定义见命题 1.

下面两个引理讨论当序列 $s\in S_1,t\in S_2$ 时的相关性. 由于对任意的 $0\leqslant\tau<2^n-1$,有 $C_{t,s}(\tau)=C_{s,t}((-\tau)\bmod 2^n-1)$,于是只考虑 $C_{s,t}(\tau)$.

引理 7　$\forall\ s\in S_1,t\in S_2$,有 $C_{s,t}(0)=-1$.

证明　$\forall\ s\in S_1,t\in S_2$,有

$$C_{s,t}(0)=-1+\sum_{x\in GF(2^n)}(-1)^{f_1(x)+f_2(x)}$$
$$=-1+\sum_{x\in GF(2^n)}(-1)^{h(x)+tr_1^n((u+v)x)}$$
$$=-1+W_h(u+v)$$

由于 u,v 不在同一个等价类,由命题 1 有 $W_h(u+v)=0$,即 $C_{s,t}(0)=-1$. 证毕

引理 8　$\forall\ s\in S_1,t\in S_2$,当 $0<\tau<2^n-1$ 时,有 $\max|C_s(\tau)|\leqslant 2^{n/2+1}+1$.

证明　令 $\mu=\alpha^\tau(\mu\neq 0,1)$,$q(x)=p_1(\mu x)+p_2(x)$. 因此,

$$C_{s,t}(\tau)=-1+\sum_{x\in GF(2^n)}(-1)^{f_1(\mu x)+f_2(x)}$$
$$=-1+\sum_{x\in GF(2^n)}(-1)^{q(x)+tr_1^n[(\mu u+v)x]}$$
$$B_q(x,z)=B_{p_1}(\mu x,\mu z)+B_{p_2}(x,z)$$
$$=tr_1^n(\mu x[tr_2^n(\mu z)+\mu z])+tr_1^n(x[tr_1^n(z)+z])$$
$$=tr_1^n(x[\mu^2 z+\mu tr_2^n(\mu z)+tr_1^n(z)+z])$$

考虑下列方程的解数：

$$\mu^2 z + \mu tr_2^n(\mu z) + tr_1^n(z) + z = 0 \quad (3)$$

设 $tr_2^n(\mu z) = a$，$tr_2^n(z) = b(a, b \in GF(2^2))$，由式(3)得

$$z = (a\mu + tr_1^2(b))/(\mu^2 + 1) \quad (4)$$

将式(4)代入 $tr_2^n(\mu z) = a$，$tr_2^n(z) = b$，得下列方程：

$$tr_2^n((a\mu^2 + \mu tr_1^2(b))/(\mu^2 + 1)) = a \quad (5)$$

和

$$tr_2^n((a\mu + tr_1^2(b))/(\mu^2 + 1)) = b \quad (6)$$

设 $tr_2^n(1/(\mu + 1)) = X$，则 $tr_2^n(1/(\mu^2 + 1)) = X^2$. 由于 m 为奇数，故 $tr_2^n(\mu^2/(\mu^2 + 1)) = 1 + X^2$，$tr_2^n(\mu/(\mu^2 + 1)) = X^2 + X$. 此时式(5)和式(6)可分别写为：

$$(a + tr_1^2(b))X^2 + tr_1^2(b)X = 0 \quad (7)$$

和

$$(a + tr_1^2(b))X^2 + aX = b \quad (8)$$

显然式(3)的所有解必须满足式(7)和式(8). 下面分三种情况讨论：

(1)当 $X = 0$ 时，式(7)为恒等式；由式(8)得 $b = 0$. 此时 $z = a\mu/(\mu^2 + 1)$，$a \in GF(2^2)$，则式(3)的解数为 2^2.

(2)当 $X = 1$ 时，由式(7)得 $a = 0$；由式(8)得 $b = tr_1^2(b)$，即 $b = 0$. 此时 $z = 0$，式(3)的解数为 1.

(3)当 $X \in GF(2^2) \setminus \{0,1\}$ 时，由式(7)有 $a = tr_1^2(b) \cdot (x + 1)/x$，将此值代入式(8)，得 $b = 0$，从而 $a = 0$. 此时 $z = 0$，式(3)的解数为 1.

由上述讨论得知 $q(x)$ 的秩为 $n - 2$ 或 n. 根据引理 1，有 $C_{s,t}(\tau) = -1 \pm 2^{n/2}$ 或 $-1 \pm 2^{n/2+1}$，从而 $\max|C_{s,t}(\tau)| \leqslant 2^{n/2+1} + 1$. 证毕

定理 1 二元序列集 S 是一个 $(2^n - 1, 2^n + 1, 2^{n/2+1} + 1)$ 序列集.

证明 显然 S 中的序列数为 $2^n + 1$，每条序列的周期为 $2^n - 1$. 对于 S 中任意两条序列 s 和 t 的相关性，根据 s, t 属于 $S_i(i = 1,2,3)$ 的情况讨论，可由引理 2、3、7 和 8 得出：$\max|C_{s,t}(\tau)| = 2^{n/2+1} + 1$. 证毕

例 2 设 $n = 6$，在例 1 的基础上，选取 $I_1 = \{1\}$. 限于篇幅，下面仅列出新序列集 S 中的两条序列，它们分别属于 S_1 和 S_2.

$s \in S_1(u = \alpha^{21})$：100101100101110001111001101001110100101101101000101011010100010

$t \in S_1(v = \alpha)$：100110100010111110101111001010000000000000010010011110110100101 0

容易验证它们的相关值为 $\{-17, -9, -1, 7, 15\}$.

在本节的构造方法中 I_1 是 I 的任意一个子集，且每个 I_1 对应一个序列集 S. 显然 I 有 $2^{2^{n-2}}$ 个不同的子集，因此能构造 $2^{2^{n-2}}$ 个不同的低相关二元序列集. 特别地，当 $I_1 = \varnothing$ 或 I 时，S 即为引理 2 或引理 3($e = 2$)中的序列集.

表 1 分析了当 $n \equiv 2 \pmod 4$ 时，一些低相关二元序列集的性质，通过比较可以看出在相关性、序列数、周期相同的情况下，运用两族布尔函数构造的新序列集的集合数是非常大的，这为通信和密码系统提供了更多可供选择的序列集.

表 1 一些周期为 $2^n - 1$ 的低相关序列集($n \equiv 2 \pmod 4$，$m = n/2$)

序列集	二次型函数	序列数	最大相关性	集合数
Gold-like	$\sum_{j=1}^{m-1} tr_1^n(x^{2^j+1}) + tr_1^m(x^{2^m+1})$	$2^n + 1$	$2^{n/2+1} + 1$	1
GKW-like($e = 2$)	$\sum_{j=1}^{(m-1)/2} tr_1^n(x^{2^{2j}+1})$	$2^n + 1$	$2^{n/2+1} + 1$	1
新序列集 S	$\sum_{j=1}^{m-1} tr_1^n(x^{2^j+1}) + tr_1^m(x^{2^m+1})$ 和 $\sum_{j=1}^{(m-1)/2} tr_1^n(x^{2^{2j}+1})$	$2^n + 1$	$2^{n/2+1} + 1$	$2^{2^{n-1}}$

5 结束语

基于对有限域的一个等价划分，本文运用两族二次布尔函数设计了多个低相关序列集，这些序列集包含 Udaya(1992)和 Kim(2003)等人分别设计的两类序列集作为特例. 本文构造的序列集为通信和密码系统提供了更多可供选择的序列集.

参考文献：

[1] Olsen J D, Scholtz R A, Welch L R. Bent-function sequences [J]. IEEE Trans on Inform Theory, 1982, 28(6): 858 – 864.

[2] Kasami T. The weight enumerators for several classes of subcodes of the 2nd-order Reed-Muller codes[J]. Inform and Control, 1971, 18(5): 369 – 394.

[3] Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions[J]. IEEE Trans on Inform Theory, 1968, 14(1): 154 – 156.

[4] Boztas S, Kumar P V. Binary sequences with Gold-like correlation but large linear span[J]. IEEE Trans on Inform Theory, 1994, 40(2): 532 – 537.

[5] 王劲松，戚文峰. Bent 序列和 Gold-like 序列的构造[J]. 电子与信息学报，2006，28(1)：80 – 85.
Wang J, Qi W. Construction of Bent sequences and Gold-like

sequences[J]. J of Elec & Inform Technol, 2006, 28(1): 80 – 85. (in Chinese)
[6] Klapper A. D-form sequences: families of sequences with low correlation values and large linear spans[J]. IEEE Trans on Inform Theory, 1995, 41(2): 423 – 431.
[7] Zeng X, Hu L, Liu Q, Zhu Y. Binary sequences with optimal correlation property and large linear span[A]. IEEE ICC'06 [C]. Istanbul, Turkey: IEEE press, 2006. 385 – 390.
[8] Zeng X, Hu L, Jiang W. A family of binary sequences with 4-valued optimal out-of-phase correlation and large linear span [J]. IEICE Trans on Fundamentals, 2006, E89-A (7): 2029 – 2035.
[9] Hu H, Hu L, Feng D. A new class of binary sequences with low correlation and large linear complexity from function fields [A]. Proceedings of ISIT'05[C]. Adelaide, Australia: IEEE press, 2005. 1997 – 2001.
[10] Udaya P. Polyphase and frequency hopping sequences obtained from finite rings[D]. Dept Elec Eng, Indian Inst Technol, Kanpur, 1992.
[11] Kim S H, No J S. New families of binary sequences with low correlation[J]. IEEE Trans on Inform Theory, 2003, 49(11): 3059 – 3065.
[12] Lidl R, Niederreiter H. Finite Fields[M]. Cambridge, U K: Cambridge Univ Press, 1997.
[13] Helleseth T, Kumar P V. Sequences with low correlation, in Handbook of Coding Theory[M]. NewYork: Elservier Science, 1998. 1765 – 1853.

作者简介:

李胜华　女,1972 年生于湖北麻城,湖北大学数学与计算机科学学院讲师,博士研究生. 主要研究方向为算法和序列设计.
E-mail: lsh@hubu.edu.cn

曾祥勇　男,1973 年生于湖北仙桃,湖北大学数学与计算机科学学院副教授,博士. 主要研究方向为密码和序列设计.
E-mail: xzeng@hubu.edu.cn

胡　磊　男,1967 年生于湖北麻城,中国科学院研究生院信息安全国家重点实验室教授,博士生导师. 主要研究方向为密码学与信息安全. E-mail: hu@is.ac.cn

刘合国　男,1967 年生于湖北大冶,湖北大学数学与计算机科学学院教授,博士生导师. 主要研究方向为代数学和格基密码.
E-mail: liuheguo0@163.com