Bent 序列和 Gold-like 序列的构造

王劲松 戚文峰

(郑州信息工程大学应用数学系 郑州 450002)

摘 要 该文研究 Bent 序列和 Gold-like 序列，设计了 3 类快速生成的 Bent 序列，此外，基于 Klapper(1993)对几何序列相关性的分析，递归地构造了一类 Gold-like 序列，所得的 Gold-like 序列涵括了 Khoo, Gong 和 Stinson(2002)递归生成的 Gold-like 序列。 根据 Olsen, Scholtz 和 Welch(1982)给出的 Bent 序列簇的构造方法，该文得到的 Bent 序列可以迅速地构造 Bent 序列簇。此外，该文得到的 Gold-like 序列可以用来设计大周期的扩频序列簇。

关键词 Bent 序列, Gold-like 序列, Hadamard 变换

中图分类号: TN911.2 **文献标识码：** A **文章编号：** 1009-5896(2006)01-0080-06

Construction of Bent Sequences and Gold-like Sequences

Wang Jin-song Qi Wen-feng

(*Department of Applied Mathematics, Zhengzhou Information Engineering University, Zhengzhou* 450002, *China*)

Abstract In this paper, three families of Bent sequences that can be quickly generated are presented. Then based on the analysis of correlation of geometric sequences by Klapper in 1993, a family of Gold-like sequences is recursively constructed, which contains the Gold-like sequences constructed in 2002 by Khoo, Gong and Stinson. On account of the theory of Olsen, Scholtz and Welch, three Bent sequence families used in a DS CDMA system can be quickly obtained by the Bent sequences here. And sequence families with large periods can be obtained by Gold-like sequences recursively constructed.

Key words Bent sequences, Gold-like sequences, Hadamard transform

1 引言

扩频通信系统中，扩频序列的设计是其核心内容之一。对于扩频序列，低相关特性(异相自相关和互相关)、平衡性、大的序列数量、大的周期和大的线性复杂度是其重要的衡量指标。较小的相关函数意味着系统的多址干扰小，采用平衡的序列意味着通信系统不会产生载波泄露及抗干扰，安全的通信系统要求使用线性复杂度大的序列，多址通信要求每一簇序列个数和序列的周期都较大。人们先后设计出m序列簇[1]、Bent序列簇[2]、Gold序列簇[3]、No 序列簇[4]、Gold-like序列簇[5]和广义Bent序列簇[6]等扩频序列簇。 m序列具有最优的自相关特性, Bent序列簇、广义Bent序列簇、No序列簇、周期为 $2^{2n+1}-1$ 的Gold序列簇和Gold-like序列簇具有最优的互相关特性。但是No序列簇中序列都是不平衡的, Gold序列簇和Gold-like序列簇仅有部分序列是平衡的。而Bent序列簇中序列的数量较多，且每条序列都是线性复杂度较大的平衡序列，因此是一类很好的扩频序列簇。 Bent序列簇设计的关键在于寻找Bent函数[2]，而Gold序列簇和Gold-like序列簇主要基于Gold-like函数来生成[3,5,7-9]。

2002 年, Khoo, Gong和Stinson[7]证明了形如 $\sum_{i=1}^{(n-1)/2} c_i \mathrm{tr}_1^n(x^{2^i+1})$ 的函数是Gold-like函数当且仅当 $\gcd\left(\sum_{i=1}^{(n-1)/2} c_i(x^i + x^{n-i}),\ x^n+1\right)=x+1$，这里$n$是一个奇数。若$\alpha$是GF($2^n$)的一个本原元，用$\alpha^t$代替$x$，便可得到一条Gold-like序列。这三位学者[8]进一步研究了Gold-like序列，由一条短周期的Gold-like序列递归地生成长周期的Gold-like序列。

本文首先给出形如 $\sum_{i=1}^{n/2-1} c_i\ \mathrm{tr}_1^n(x^{(2^i+1)}) + \mathrm{tr}_1^{n/2}(x^{(2^{n/2}+1)})$ 的函数是Bent函数的判断条件，即上述函数是Bent函数当且仅当 $\gcd\left(\sum_{i=1}^{n/2-1} c_i\left(x^i + x^{n-i}\right) + x^{n/2}, x^{n+1}\right)=1$，其中$n$为偶数，$c_i \in \{0, 1\}$。接着设计了 3 类可以快速生成的Bent函数，它们只需经过模 2 加或整数的gcd(最大公因子)运算便可由迹数合成得到。根据Olsen, Scholtz和Welch在文

2004-04-12 收到, 2004-12-10 改回
全国优秀博士学位论文专项基金(200060)和国家自然科学基金(60373092)资助课题

献[2]中给出的 Bent 序列簇的构造方法，由本文设计的 3 类 Bent 函数可迅速地得到 Bent 序列簇，此外，由前 2 类 Bent 函数还可以得到线性复杂度较大的 Bent 序列簇。

其次基于Klapper[10]对几何序列相关性的分析，由短周期的Gold-like函数递归地构造了一类长周期的Gold-like函数，所得Gold-like函数涵括了Khoo，Gong和Stinson在文献[8]中递归生成的Gold-like函数。

注 1　下面将 $\mathrm{tr}_1^{n/2}\left(x^{2^{(n/2)}+1}\right)$ 和形如 $\mathrm{tr}_1^n\left(x^{2^i+1}\right)$ 的单项式均称为Gold-like项。

2　预备知识

设GF(2^n)表示 2^n个元素的有限域，GF(2^n)到GF(2)上的迹函数定义为：$\mathrm{tr}_1^n(x)=\sum_{i=0}^{n-1}x^{2^i}$，其中$x\in$GF($2^n$)。迹函数有如下的性质[11]:

(1) $\mathrm{tr}_1^n(ax+by)=a\ \mathrm{tr}_1^n(x)+b\ \mathrm{tr}_1^n(y)$，对任意的$x$, $y\in$GF(2^n), a, $b\in$GF(2)均成立;

(2) $\mathrm{tr}_1^n(x^2)=\mathrm{tr}_1^n(x)$，对任意的$x\in$GF($2^n$)均成立。

设$a=(a(t))_{t\ge0}$和$b=(b(t))_{t\ge0}$是两条周期为$N=2^n-1$ 的二元序列，它们之间的互相关函数定义为 $C_{a,b}(\tau)=\sum_{t=0}^{N-1}(-1)^{a(t+\tau)+b(t)}$，其中 $0\le\tau\le N-1$。

设$f(x)$是GF(2^n)到GF(2)上的函数，$f(x)$的Hadamard变换定义为：$\hat{f}(\lambda)=\sum_{x\in\mathrm{GF}(2^n)}(-1)^{f(x)+\mathrm{tr}_1^n(\lambda x)}$，其中$\lambda\in$GF($2^n$)。

注 2　如不特殊说明，下面假设α是GF(2^n)的一个本原元。

设$f(x)$是GF(2^n)到GF(2)上的函数，用α^t代替x，那么$f(x)$定义了一条周期整除 2^n-1 的二元序列$a=(a(t))_{t\ge0}$，其中$a(t)=f(\alpha^t)$. 显然，迹函数 $\mathrm{tr}_1^n(x)$ 定义了一条m序列$m=(m(t))_{t\ge0}$[1]，其中$m(t)=\mathrm{tr}_1^n(\alpha^t)$. 若$f(0)=0$，由Hadamard变换，$a$和$m$的互相关函数$C_{a,m}(\tau)$又可表为

$$\begin{aligned}C_{a,m}(\tau)&=\sum_{t=0}^{N-1}(-1)^{a(t)+m(t+\tau)}\\&=\sum_{x\in\mathrm{GF}(2^n)^*}(-1)^{\mathrm{tr}_1^n(\lambda x)+f(x)}\\&=-(-1)^{f(0)}+\sum_{x\in\mathrm{GF}(2^n)}(-1)^{\mathrm{tr}_1^n(\lambda x)+f(x)}\\&=-1+\hat{f}(\lambda)\end{aligned}$$

其中$\lambda=\alpha^\tau\in$GF(2^n)*。

当n为偶数时，若 $\hat{f}$ 的取值为 $2^{n/2}$和$-2^{n/2}$，则称f为Bent函数；当n为奇数时，若 $\hat{f}$ 的取值为 0, $2^{(n+1)/2}$和$-2^{(n+1)/2}$，则称f为Gold-like函数。由它们定义的序列分别叫做Bent序列和Gold-like序列。Bent序列与m序列的相关值为$-1\pm2^{n/2}$，Gold-like序列与m序列的相关值为-1, $-1\pm2^{(n+1)/2}$。

3　Bent 序列的构造

本节给出Gold-like项的线性组合构成Bent函数的判断条件，并得到了 3 类新的可以快速生成的Bent函数，用α^t代替这些Bent函数中的变量x，便可得到Bent序列。

引理 1　设n为偶数，$f(x)=\sum_{i=1}^{n/2-1}c_i\ \mathrm{tr}_1^n(x^{2^i+1})+\mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$是GF($2^n$)上的函数，其中$c_i\in\{0,1\}$，那么$f(x)$是Bent函数当且仅当GF(2)上的循环矩阵

$$\boldsymbol{L}=\begin{pmatrix}c_0&c_1&c_2&c_3&\cdots&c_{n-1}\\c_{n-1}&c_0&c_1&c_2&\cdots&c_{n-2}\\c_{n-2}&c_{n-1}&c_0&c_1&\cdots&c_{n-3}\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\c_1&c_2&c_3&c_4&\cdots&c_0\end{pmatrix}\tag{1}$$

是可逆的，其中$c_0=0$, $c_{n/2}=1$, $c_{n-i}=c_i$, $i=1,2,\cdots,n/2-1$。

证明　因

$$\begin{aligned}\hat{f}2(\lambda)&=\left(\sum_{x\in\mathrm{GF}(2^n)}(-1)f(x)+\mathrm{tr}_1^{n(\lambda x)}\right)^2\\&=\left(\sum_{x\in\mathrm{GF}(2^n)}(-1)f(x)+\mathrm{tr}_1^n(\lambda x)\right)\cdot\left(\sum_{y\in\mathrm{GF}(2^n)}(-1)f(y)+\mathrm{tr}_1^n(\lambda y)\right)\\&=\sum_{x\in\mathrm{GF}(2^n)}\sum_{w\in\mathrm{GF}(2^n)}(-1)f(x)+f(x+w)+\mathrm{tr}_1^n(\lambda w)\\&=\sum_{w\in\mathrm{GF}(2^n)}(-1)\mathrm{tr}_1^n(\lambda w)+f(w)\\&\quad\cdot\left(\sum_{x\in\mathrm{GF}(2^n)}(-1)f(x)+f(w)+f(x+w)\right)\end{aligned}$$

其中 $y=x+w$，而

$$\begin{aligned}&f(x)+f(w)+f(x+w)\\&=\sum_{i=1}^{n/2-1}\mathrm{citr}_1^n\left(x^{2^i+1}+\mathrm{w}^{2^i+1}+(x+w)^{2^i+1}\right)\\&\quad+\mathrm{tr}_1^{\mathrm{n}/2}\left(x^{2^{n/2}}+1+w^{2^{n/2}}+1+(x+\mathrm{w}\right)^{2^{n/2}+1}\\&=\mathrm{tr}_1^n\left(x\cdot\left(\sum_{i=1}^{n/2-1}c^i\left(w^{2^i}+w^{2^{n-i}}\right)+w^{2^{n/2}}\right)\right)\\&=\mathrm{tr}_1^n(x\cdot L(w))\end{aligned}$$

其中 $L(w)=\sum_{i=1}^{n/2-1}c^i\left(w^{2^i}+w^{2^{n-i}}\right)+w^{2^{n/2}}$。显然$L$是GF($2^n$)到GF($2^n$)的一个线性变换，且在一组正规基$\{\alpha,\alpha^2,\cdots,\alpha^{2^{n-1}}\}$下，$\boldsymbol{L}$的矩阵表示由式(1)给出。记Ker$L=\{w\mid L(w)=0\}$，显然Ker$L$构成一个线性空间，设其维数dim(Ker$L$)$=k$。则

$$\sum_{x\in\mathrm{GF}(2^n)}(-1)^{f(x)+f(w)+f(x+w)}=\begin{cases}2^n, & w\in\mathrm{Ker}L\\0, & \text{其他}\end{cases}$$

设w_1, $w_2\in\mathrm{Ker}L$, 由L的定义可知$f(w_1)+f(w_2)+f(w_1+w_2)=0$, 即$f(w)$在Ker$L$上是一个线性变换, 因此$\mathrm{tr}_1^n(\lambda w)+f(w)$在Ker$L$上也是一个线性变换。 于是

$$\sum_{w\in\mathrm{Ker}L}(-1)^{\mathrm{tr}_1^n(\lambda w)+f(w)}=\begin{cases}2^k, & \mathrm{tr}_1^n(\lambda w)+f(w)=0\\ 0, & \text{其他}\end{cases}$$

从而 $\hat{f}(\lambda)$的取值为 $0, 2^{(n+k)/2}$和$-2^{(n+k)/2}$。若f是Bent函数, 则$k=0$, $\hat{f}(\lambda)$的取值为$2^{n/2}$和$-2^{n/2}$。因而f是Bent函数当且仅当循环矩阵L是可逆的。 证毕

矩阵L的行向量可以扩展为一个循环码$c=(c_0, c_1, \cdots, c_{n-1})$。设$c(x)=\sum_{i=1}^{n/2-1}c_i(x^i+x^{n-i})+x^{n/2}$, 由循环码的知识可得$\mathrm{rank}(L)=n$当且仅当$\gcd(c(x), x^n+1)=1$。因此有下面的定理.

定理 1 设n为偶数, $f(x)=\sum_{i=1}^{n/2-1}c_i\,\mathrm{tr}_1^n(x^{2^i+1})+\mathrm{tr}_1^{n/2}\left(x^{2^{n/2}+1}\right)$是GF($2^n$)到GF(2)上的函数, 其中$c_i\in\{0,1\}$。那么$f(x)$是Bent函数当且仅当$\gcd(\gcd\geq\left(\sum_{i=1}^{n/2-1}c_i(x^i+x^{n-i})+x^{n/2}, x^n+1\right)=1$ 。

由定理 1 知, 当 n 为偶数时, 判断 Gold-like 项的线性组合是否构成 Bent 函数只需进行有限域 GF(2)上多项式的 gcd 运算。

注 3 当n为偶数时, Gold-like项的线性组合若构成Bent函数, 则$\mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$这一项必不可少。否则, $f(x)=\sum_{i=1}^{n/2-1}c_i\mathrm{tr}_1^n(x^{2^i+1})$, 类似于引理 1 和定理 1 的证明可知, 此时$f(x)$是Bent函数当且仅当$\gcd(\sum_{i=1}^{n/2-1}c_i(x^i+x^{n-i}), x^n+1)=1$. 而$(x^2+1)\mid(x^i+x^{n-i})$, 故$f(x)$不是Bent函数。 因此, 定理 1 研究的函数表达式中均含有$\mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$这一项。如无特殊说明, 以下记 $c(x)=\sum_{i=1}^{n/2-1}c_i(x^i+x^{n-i})+x^{n/2}$, $g(x)=\gcd(c(x), x^n+1)$。由于$c(1)\neq 0$, 故$\gcd(c(x), x+1)=1$。 设n和e都是正整数且$e\mid n$, 当$n/e=m$是一个大于等于 4 的偶数时, Kim和No[9]证明了$f(x)=\sum_{i=1}^{m/2-1}\mathrm{tr}_1^n(x^{2^{ei}+1})+\mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$是Bent函数。这里给出一个更为简洁的证明, 设$c(x)=\sum_{i=1}^{m-1}x^{ei}$, 又$\gcd(c(x), x^e+1)=1$, 故

$$\begin{aligned}\gcd(c(x), x^n+1)&=\gcd(c(x), x^e+1+(x^e+1)\cdot c(x))\\&=\gcd(c(x), x^e+1)=1\end{aligned}$$

于是由定理 1 知$f(x)$是 Bent 函数。

下面给出 3 类可以快速生成的Bent函数, 它们只需通过模 2 加或整数的gcd运算便可由迹函数合成得到。定理 2 研究一类特殊的域GF(2^n)上的Bent函数, 其中$n=2p$且 2 是mod$p$的本原元, 即$\mathrm{ord}_2(p)=p-1$。定理 3 和定理 4 分别刻画了表达式中除一项外含有所有Gold-like项和含有两项Gold-like项的Bent函数。

定理 2 设$n=2p$, 其中p是一个奇素数且$\mathrm{ord}_2(p)=p-1$, $c_i\in\{0,1\}$, $f(x)$是GF(2^n)到GF(2)上的函数, 其中$f(x)=\sum_{i=1}^{n/2-1}c_i\,\mathrm{tr}_1^n(x^{2^i+1})+\mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$。 若存在$i\in\{1, 2, \ldots, p-1\}$, 使得$c_i+c_{p-i}=0$, 则$f(x)$是Bent函数。

证明 由 $\gcd(c(x), x+1)=1$, 有

$$\gcd(c(x), x^n+1)=\gcd(c(x), (1+x+x^2+\cdots+x^{p-1})^2),$$

记$c'(x)=\sum_{i=1}^{p-1}c_i(x^i+x^{p-i})+1$, 因

$$x^p=(1+x)\cdot(1+x+x^2+\cdots+x^{p-1})+1$$

故由辗转相除法可知

$$\begin{aligned}&\gcd(c(x), 1+x+x^2+\cdots+x^{p-1})\\&=\gcd(c'(x), 1+x+x^2+\cdots+x^{p-1})\end{aligned}$$

而$\mathrm{ord}_2(p)=p-1$, 由 GF(2) 上分圆多项式的分解知$1+x+x^2+\cdots+x^{p-1}$不可约, 于是$\gcd(c'(x), 1+x+x^2+\cdots+x^{p-1})=1$或$1+x+x^2+\cdots+x^{p-1}$。又存在$i\in\{1, 2, \cdots, p-1\}$, 使得$c_i+c_{p-i}=0$, 即$c'(x)\neq 1+x+x^2+\cdots+x^{p-1}$, 则

$$\gcd(c'(x), 1+x+x^2+\cdots+x^{p-1})=1$$

于是

$$\gcd(c(x), 1+x+x^2+\cdots+x^{p-1})=1$$

进而

$$\gcd(c(x), (1+x+x^2+\cdots+x^{p-1})^2)=1$$

由定理 1 知$f(x)$是 Bent 函数。 证毕

满足定理 2 的系数c_i共有$2^{p-1}-2^{(p-1)/2}=2^{n/2-1}-2^{(n-2)/4}$种可能的选取。 对于上面的引理, 自然要问这样的$n$共有多少个。实际上, 前 10 个这样的数是: 6, 10, 22, 26, 38, 58, 74, 106, 118 和 122, 且由黎曼猜想, 存在无限多个满足$\mathrm{ord}_2(p)=p-1$的素数, 因而这样的$n=2p$也有无限多个。

定理 3 若n为正偶数, 正整数i满足$\gcd(3i, n)=1$, $f(x)$是GF(2^n)到GF(2)上的函数, 其中

$$f(x)=\sum_{\substack{j=1\\ j\neq i}}^{n/2-1}\mathrm{tr}_1^n(x^{2^j+1})+\mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$$

即$f(x)$除了x^{2^i+1}这一项外包括所有Gold-like项, 则$f(x)$是Bent函数。

证明 这里$c(x)=\sum_{\substack{j=1\\ j\neq i}}^{n/2-1}(x^j+x^{n-j})+x^{n/2}$, 那么$x^n+1=(1+x)\cdot(1+x^i+x^{n-i}+c(x))$, 又因为$\gcd(1+x, c(x))=1$, $\gcd(1+x^i+x^{n-i}, x+1)=1$, 因此

$$\gcd(c(x), x^n+1)=\gcd\left(c(x), \sum_{j=0}^{n-1}x^j\right)$$

$$= \gcd\left(1+x^i+x^{n-i}, \sum_{j=0}^{n-1} x^j\right)$$
$$= \gcd(1+x^i+x^{n-i}, x^n+1)$$
$$= \gcd(x^i+x^{2i}+x^n, x^n+1)$$
$$= \gcd(1+x^i+x^{2i}, x^n+1)$$

由定理 3 的证明可知当$\gcd(3i, n) = 1$ 时，$\gcd(1+x^i+x^{2i}, x^n+1)=1$。再由定理 1 知$f(x)$是Bent函数。　　证毕

定理 4　若n为正偶数，正整数i满足$\gcd(3i, n)=1$，则$GF(2^n)$到GF(2)上的函数

$$f(x) = \mathrm{tr}_1^n(x^{2^i+1}) + \mathrm{tr}_1^{n/2}(x^{2^{n/2}+1})$$

是 Bent 函数。

证明　因$\gcd(x^i+x^{n-i}+x^{n/2}, x^n+1)\neq 1 \Leftrightarrow$ 在GF(2)的某个扩域内存在a，满足$a^i+a^{n-i}+a^{n/2}=0$ 且$a^n=1$。假设存在这样的a(显然$a\neq 1$)，则有$a^{2i}+a^{n/2+i}+a^n=0$ 和$a^{n/2}=1$。于是$1+a^i+a^{2i}=0$，进而有$a^{3i}=1$。如果a同时满足$a^n=1$ 和$a^{3i}=1$，由$\gcd(3i, n)=1$ 可得$a=1$，这就与假设$a\neq 1$ 矛盾。于是$\gcd(x^i+x^{n-i}+x^{n/2}, x^n+1)=1$，由定理 1 知$f(x)$是Bent函数。　　证毕

4　Gold-like 序列的设计

设$q=2^e$, $GF(q^n)$到$GF(q)$上的迹函数$\mathrm{tr}_q^{q^n}(x)$定义为：$\mathrm{tr}_q^{q^n}(x)=\sum_{i=0}^{n-1}x^{q^i}$。先对下面引理中将要出现的符号和函数作以说明。设$f$和$g$是$GF(q)$到GF(2)上的函数，$r, \delta\in GF(q^n)$，$k$和$j$是两个正整数且满足$k=1+q^j$，$\alpha$是$GF(q^n)$中的一个本原元，$u=(u(t))_{t\geq 0}$和$v=(v(t))_{t\geq 0}$是两条周期为$q^n-1$的二元序列，其中$u(t)=f(\mathrm{tr}_q^{q^n}(\alpha^t))$, $v(t)=g(\mathrm{tr}_q^{q^n}(r\alpha^t+\delta\alpha^{kt}))$。令$I(f)=\sum_{x\in GF(q)}(-1)^{f(x)}$, $F(x)=(-1)^{f(x)}$, $G(x)=(-1)^{g(x)}$，其中$x\in GF(q)$。对u的一个移位τ，记$H(x)=\mathrm{tr}_q^{q^n}(\alpha^\tau x)$, $L(x)=\mathrm{tr}_q^{q^n}(rx)$, $R(x)=\mathrm{tr}_q^{q^n}(\delta x^k)$。

$GF(q^n)$可看作$GF(q)$上的n维向量，选定$GF(q^n)$在$GF(q)$上的一组基，那么$GF(q^n)$中的变量x和$GF(q)^n$中向量$\boldsymbol{x}=(x_1, x_2, \cdots, x_n)$在这组基下一一对应。类似地，可以得到$H(\boldsymbol{x})$, $L(\boldsymbol{x})$和$R(\boldsymbol{x})$，其中$H(\boldsymbol{x})$和$L(\boldsymbol{x})$是线性函数，$R(\boldsymbol{x})$是二次型[10]。若$L(\boldsymbol{x})=\sum_{i=1}^n c_i x_i$，$H(\boldsymbol{x})=\sum_{i=1}^n a_i x_i$，则令$\rho=R(c_1, c_2, \cdots, c_n)$。若$R(\boldsymbol{x})$的秩为$m$ (m为能够表示出R的最少变量个数)，则$R(\boldsymbol{x})$可以表为下面 3 种标准型[11]：

(1) $x_1x_2+x_3x_4+\cdots+x_{m-1}x_m$

(2) $x_1x_2+x_3x_4+\cdots+x_{m-2}x_{m-1}+x_m^2$

(3) $x_1x_2+x_3x_4+\cdots+x_{m-3}x_{m-2}+x_{m-1}^2+x_{m-1}x_m+ax_m^2$

若$R(\boldsymbol{x})$是一个(2)型的二次型，令$\sigma=c_m$，其中m是R的秩。

下面基于$GF(q^n)$中变量x和函数$H(x)$, $L(x)$和$R(x)$进行讨论。

设$D(w, x)=R(x+w)-R(x)-R(w)$，定义 3 个线性空间：

$\mathrm{Null}(R)=\{w \mid R(w)=0$ 且任给 $x, D(w, x)=0\}$,

$\mathrm{Null}(D)=\{w \mid$ 任给 $x, D(w, x)=0\}$,

$\mathrm{KerL}=\{w \mid L(w)=0\}$。

为简单起见，记$\Gamma_{\boldsymbol{u},\boldsymbol{v}}(\tau)=C_{\boldsymbol{u},\boldsymbol{v}}(\tau)-q^{n-2}I(f)I(g)+F(0)G(0)$，于是可以得到下面的引理。

引理 2[10]　基本符号和函数定义同前，设n/d为奇数，其中$d=\gcd(n, j)$，

(1)　若$\mathrm{Null}(D)\subseteq \mathrm{Ker}(L)$，则$\Gamma_{\boldsymbol{u},\boldsymbol{v}}(\tau)$的取值为

(a)　0；

(b)　$-q^{(n+d)/2-2}(I(f)I(g)-q\sum_u F(su)G(u^2+t))$,

(c)　$q^{(n+d)/2-2}(I(f)I(g)-q\sum_u F(su)G(u^2+t))$。

(2)　若$\mathrm{Null}(R)\subseteq \mathrm{Ker}(L)$，但$\mathrm{Null}(D)\subseteq \mathrm{Ker}(L)$不成立，则$\Gamma_{\boldsymbol{u},\boldsymbol{v}}(\tau)$的取值为

(a)　$q^{(n+d)/2-2}I(f)\sum_v(-1)^{\mathrm{tr}_2^q(v+1)}G(\sigma^2v+\rho)$,

(b)　$q^{(n+d)/2-1}F(t)\sum_v(-1)^{\mathrm{tr}_2^q(v+1)}G(\sigma^2v+\rho)$,

(c)　$(-1)^{\mathrm{tr}_2^q((t+\rho)/\sigma^2+1)}q^{(n+d)/2-2}\cdot\left(q\sum_u F(ru+s)G(u^2+\sigma u+t)-I(f)I(g)\right)$。

(3)　若$\mathrm{Null}(R)\subseteq \mathrm{Ker}(L)$不成立，则$\Gamma_{\boldsymbol{u},\boldsymbol{v}}(\tau)$的取值为

(a)　0；

(b)　$q^{(n+d)/2-2}\sum_{u,v}(-1)^{\mathrm{tr}_2^q(ru+tv)}F(u)G(v)$,

(c)　$-q^{(n+d)/2-2}\sum_{u,v}(-1)^{\mathrm{tr}_2^q(ru+tv)}F(u)G(v)$。

这里的参数r, s, t与τ有关.

基于引理 2，下面递归地构造 Gold-like 函数。

定理 6　设n为奇数，$q_0=2^n$，且对$j=1, 2, \cdots, l$，设n_j为奇数，$q_j=q_{j-1}^{j^n}$，$k_j=q_{j-1}^{i^n}j+1$，其中$\gcd(i_j, n_j)=1$. 按下列方式递归地构造$GF(q_j)$到GF(2)上的函数f_j：

$$f_0(x)=f(x)$$
$$f_j(x)=f_{j-1}(\mathrm{tr}_{q_{j-1}}^{q_j}(r_jx+\delta_jx^{k_j})),\quad j=1, \cdots, l$$

其中参数r_j和δ_j的选取如下：

(1) 若$\mathrm{tr}_{q_{j-1}}^{q_j}(r_j)=0$，任取$\delta_j\in GF(q_j)$即可；

(2) 若$\mathrm{tr}_{q_{j-1}}^{q_j}(r_j)\neq 0$，取$\delta_j\in GF(q_j)$且满足$\mathrm{tr}_{q_{j-1}}^{q_j}(\delta_j)\neq 0$。

那么f_j是一个Gold-like函数当且仅当f是一个Gold-like函

数。

证明 若f是一个Gold-like函数, 下面对于$j=1, 2, \cdots, l$, 证明f_j也是Gold-like函数. 对j递归, 若$j=1$, 则

$$\begin{aligned} D(w,x) &= R(x+w) - R(x) - R(w) \\ &= \mathrm{tr}_q^{q_1}\left((x+w)^{q^{i_1}+1} - x^{q^{i_1}+1} - w^{q^{i_1}+1}\right) \\ &= \mathrm{tr}_q^{q_1}\left(x^{q^{i_1}} w + w^{q^{i_1}} x\right) \\ &= \mathrm{tr}_q^{q_1}\left(x\cdot\left(w^{q^{i_1}} \cdot + w^{q^{n_1-i_1}}\right)\right) \end{aligned}$$

若任给$x\in \mathrm{GF}(q_1)$, $D(w, x)=0$ 恒成立, 则 $w^{q^{i_1}} + w^{q^{n_1-i_1}} = 0$。又$n$是奇数, $\gcd(i_1, n_1)=1$, 那么$\gcd(2i_1, n_1)=1$, 所以$w=0$ 或 1。因此$\mathrm{Null}(D)=\{0, 1\}$, 又$R(w)=\mathrm{tr}_q^{q_1}(\delta_1 w^{k_1})$, 若$w=0$, 那么$R(0)=0$;若$w=1$, 那么$R(1)=\mathrm{tr}_q^{q_1}(\delta_1)$。$L(w)=\mathrm{tr}_q^{q_1}(r_1 w^{k_1})$, 若$w=0$, 那么$L(0)=0$; 若$w=1$, 那么$L(1)=\mathrm{tr}_q^{q_1}(r_1)$。

由r_1和δ_1满足的条件, 分成下面 3 种情况讨论:

(1) 若 $\mathrm{tr}_q^{q_1}(r_1)=0$ 且 $\mathrm{tr}_q^{q_1}(\delta_1)=0$, 此时$\mathrm{Null}(R)=\{0, 1\}$, 那么$\mathrm{Null}(D)=\mathrm{Null}(R)$, 又 $1, 0\in \mathrm{Ker}L$, 且有$\mathrm{Null}(D)\subseteq \mathrm{Ker}(L)$, r_1和δ_1满足引理 2 中情况(1)。

(2) 若 $\mathrm{tr}_q^{q_1}(r_1)=0$ 且 $\mathrm{tr}_q^{q_1}(\delta_1)\neq 0$, 那么$\mathrm{Null}(R)=\{0\}$, 又 $1, 0\in \mathrm{Ker}L$, 因此$\mathrm{Null}(D)\subseteq \mathrm{Ker}(L)$, 此时$r_1$和$\delta_1$满足引理 2 中情况(1)。

(3) 若 $\mathrm{tr}_q^{q_1}(r_1)\neq 0$ 且 $\mathrm{tr}_q^{q_1}(\delta_1)\neq 0$, 那么 $\mathrm{Null}(R)=\{0\}$, $0\in \mathrm{Ker}L$ 而 $1\notin \mathrm{Ker}L$, 因此 $\mathrm{Null}(R)\subseteq \mathrm{Ker}(L)$, 但是 $\mathrm{Null}(D)\subseteq \mathrm{Ker}(L)$不成立, 此时$r_1$和$\delta_1$满足引理 2 中情况(2)。

因为$x\to x^2$是$\mathrm{GF}(q)$上的一个置换, $\hat{f}_0(\lambda)$ 取值为 $0, \pm 2^{(n+1)/2}$, 那么 $\hat{f}_0(\lambda^2)$ 取值也为 $0, \pm 2^{(n+1)/2}$。在引理 2 中令u为一条周期为q_1-1的m - 序列, 显然u是平衡的, 此时$T_{\boldsymbol{u},\boldsymbol{v}}(\tau)$相当于 $\hat{f}_1(\lambda)$, 又$\gcd(i_1, n_1)=1$, 若r_1和δ_1满足引理 2 中情况(1), $\hat{f}_1(\lambda)$ 取值为

$$\begin{gathered} 0 \\ \pm q^{(n_1+1)/2-2}\cdot q\cdot 2^{(n+1)/2} = \pm q^{(n_1-1)/2} \\ 2^{(n+1)/2} = \pm 2^{(n_1 n+1)/2} \end{gathered}$$

那么$f_1(x)$是Gold-like函数。若r_1和δ_1满足引理 2 中情况(2), $\hat{f}_1(\lambda)$ 取值为

$$\begin{gathered} 0 \\ \pm q^{(n_1+1)/2-1}\cdot 2^{(n+1)/2} = \pm 2^{(n_1 n+1)/2} \\ \pm q^{(n_1+1)/2-2}\cdot q\cdot 2^{(n+1)/2} = \pm 2^{(n_1 n+1)/2} \end{gathered}$$

那么$f_1(x)$也是Gold-like函数。

假设$j-1$ 时情况成立, 即f_{j-1}是Gold-like函数。在引理 2 中令u为一条周期为q_j-1 的m - 序列, 显然u是平衡的。由假设知$f_{j-1}(x)$是 Gold-like 函数, 那么 $\hat{f}_{j-1}(\lambda^2)$ 的取值为 $0, \pm 2^{(nn_1\cdots n_{j-1}+1)/2}$。类似于$j=1$ 的情况可知, δ_j和r_j的选取满足引理 2 中情况(1)和(2), 因而 $\hat{f}_j(\lambda)$ 的取值为

$$\begin{gathered} 0 \\ q_{j-1}{}^{(n_j+1)/2-2}\cdot q_{j-1}\cdot 2^{(nn_1\cdots n_{j-1}-1)/2} = q_{j-1}{}^{(n_j-1)/2}\cdot 2^{(nn_1\cdots n_{j-1}-1)/2} \\ = 2^{(nn_1\cdots n_j+1)/2} \\ q_{j-1}{}^{(n_j+1)/2-1}\cdot 2^{(nn_1\cdots n_{j-1}-1)/2} = q_{j-1}{}^{(n_j-1)/2}\cdot 2^{(nn_1\cdots n_{j-1}-1)/2} \\ = 2^{(nn_1\cdots n_j+1)/2} \end{gathered}$$

所以 $\hat{f}_j(\lambda)$ 的取值 $0, \pm 2^{(nn_1\cdots n_j+1)/2}$, 那么$f$是一个Gold-like函数。 证毕

由定理 6 可知, 只要选取$f_0(x)$是一个$\mathrm{GF}(2^n)$上Gold-like函数, 即可递归地得到$\mathrm{GF}(2^n)$扩域上的Gold-like函数。用α^t代替定理 6 中得到的Gold-like函数中的变量x, 便可得到Gold-like序列。

注 4 若对$j=1, 2, \cdots, l$, 取$\delta_j=0$, $r_j=1$, 显然满足定理 6 的条件, 此种情况即为Khoo, Gong和Stinson[8]递归生成的Gold-like函数。

5 结束语

扩频通信中需要大量的 Bent 函数和 Gold-like 函数, 本文讨论了一类 Gold-like 项的线性组合构成 Bent 函数的充要条件, 并得到了三类可以快速生成的 Bent 函数, 接着基于 Klapper 对几何序列的分析, 递归地生成一类 Gold-like 函数, 该类 Gold-like 函数可以很容易生成且包括了由 Khoo, Gong 和 Stinson 递归生成的 Gold-like 序列。

此外, 本文得到的均是$\mathrm{GF}(2^n)$上的Bent函数。其实仿照引理 1 和定理 1, 也可对奇素数p设计p元Bent函数。

参 考 文 献

[1] Fan P Z, Darnell M. Sequence Design for Communications Applications. New York: Wiley, 1996: 81 − 85.

[2] Olsen J D, Scholtz R A, aWelch L R. Bent-function sequences. *IEEE Trans. on Information Theory*, 1982, IT-28(6): 858 − 864.

[3] Gold R. Maximal recursive sequences with 3-valued cross correlation function. *IEEE Trans. on Information Theory*, 1968, IT-14(1): 154 − 156.

[4] No J S. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, Univ. So. Calif., Los Angeles, May 1988.

[5] Boztas S, Kumar P V. Binary sequences with gold-like correlation but larger linear span. *IEEE Trans. on Information Theory,* 1994, IT-40(2): 532 − 537.

[6] No J S, Gil G M, Shin D J. Generalized construction of binary bent sequences with optimal correlation property. *IEEE Trans. on Information Theory*, 2003, IT-49(7): 1769 − 1780.

[7] Khoo K, Gong G, Stinson D R. A new family of gold-like sequence. IEEE International Symposium on Information Theory

02, Lausanne, Switzerland, June 30-July 5, 2002: 181.

[8] Khoo K, Gong G,Stinson D R. Sequences with low cross correlation, preprint, http:// www.math.uwaterloo.ca/~ kkhoo/.

[9] Kim S H, No J S. New families of binary sequences with low correlation. *IEEE Trans. on Information Theory*, 2003, IT-49(11): 3059 – 3065.

[10] Klapper A. Cross-correlations of geometric sequences in characteristic two. *Designs*, *Codes*, *and Cryptography*, 1993, 3(4): 347 – 377.

[11] Lidl R, Niederreiter H, Finite Fields. Encyclopaedia of mathematics and its applications. Reading, MA: Addision Wesley, 1983: 54 – 57.

王劲松： 男， 1980 年生, 博士生, 研究兴趣为信息安全、扩频序列设计.

戚文峰： 男， 1963 年生, 教授, 博士生导师, 中国密码学会理事, 主要研究方向为信息安全.