一类具有最优汉明自相关特性的跳频序列

刘 方[1],彭代渊[2],范 佳[1],唐小虎[2]
(1.中国电子科技集团公司第三十研究所,四川成都 610041;2.西南交通大学信息科学与技术学院,四川成都 610031)

摘 要: 在跳频多址通信系统中,设计具有最优汉明相关特性的跳频序列是至关重要的.基于具有平衡性及差平衡性的函数与具有差平衡性的 d-型函数的复合函数,本文构造了一类跳频序列.该类跳频序列的汉明自相关达到了 Lempel-Greenberger 界,是一类最优的跳频序列.

关键词: 跳频序列;汉明自相关;d-型函数;平衡;差平衡
中图分类号: TN914.43 **文献标识码:** A **文章编号:** 0372-2112 (2013)01-0013-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.01.003

A New Class of Frequency-Hopping Sequences with Optimal Hamming Autocorrelation

LIU Fang[1], PENG Dai-yuan[2], FAN Jia[1], TANG Xiao-hu[2]
(1. *The Thirtieth Research Institute of China Electronic Technology Group Corporation*, *Chengdu*, *Sichuan* 610041, *China*;
2. *The College of Information Science & Technology*, *Southwest Jiaotong University*, *Chengdu*, *Sichuan* 610031, *China*)

Abstract: In frequency-hopping (FH) multiple access system, FH sequences with optimal Hamming correlation properties are needed. Based on the composition of the function with balanced and difference-balanced properties and d-form function with difference-balanced property, a new class of FH sequences are constructed. The Hamming autocorrelation of the proposed sequences are optimal with respect to Lempel-Greenberger bound.

Key words: frequency-hopping sequence; Hamming autocorrelation; d-form; balance; difference-balance

1 引言

跳频多址扩频系统具有抗干扰、抗截获的能力,并能做到频谱资源共享,所以在现代化的电子战中,跳频通信已显示出其巨大的优越性.此外,跳频通信也被应用到民用通信中用以抗衰落、抗多径、抗网间干扰和提高频谱利用率.在跳频系统中,载波频率跳变是由一个称为跳频序列的伪随机码控制频率合成器产生的.在军事领域中,要求跳频序列具有较大的线性复杂度,并具有优良的汉明相关性能.跳频序列的性能对跳频系统的性能有很大的影响,寻求和设计具有理想性能的跳频序列是研究跳频通信系统的重要课题之一.

基于代数和组合工具[1~5],人们已经构造出许多具有优良汉明相关特性的跳频序列.基于具有理想自相关特性的 p 元伪随机序列构造具有优良汉明相关特性的跳频序列是一个很重要的方法.文献[6,7]分别利用 m 序列、GMW 序列,构造了具有最优汉明相关特性的跳频序列族.

d-型函数在直接扩频序列的设计中,得到了很多的应用.1995 年,Klapper 首次提出了 d-型函数[8]的概念,并利用 d-型函数构造了一类具有低相关(并非汉明相关)并且线性复杂度大的直接扩频序列.2002 年,No 对 d-型序列进行了扩展,提出了一种 p 元的扩展 d-型序列[9].d-型函数还用于低/零相关区的直接扩频序列的设计[10,11].本文基于具有平衡性及差平衡性的函数与具有差平衡性的 d-型函数的复合函数,提出了一个构造最优跳频序列的方法.通过选择某些特定的 d-型函数,基于本文的构造方法,可以得到具有长周期大线性复杂度的最优跳频序列.

2 基本概念

在跳频通信系统中,当两个或更多的信号在同一时间跳到相同的频道上去,这种情况称为用户间发生相互“碰撞”或称为“击中”,形成多址干扰,引起通信性能下

收稿日期:2010-01-21;修回日期:2012-07-20
基金项目:国家自然科学基金(No.2012CB316100)

降.跳频系统的多址性能可用跳频序列的汉明相关函数来度量.

下面给出跳频序列的周期汉明相关函数的定义.

设跳频通信系统中有 v 个频隙,频隙集合为

$$\boldsymbol{F}=\{f_0,f_1,\cdots,f_{v-1}\}$$

对于任意的 $f_i,f_j\in\boldsymbol{F}$,令

$$h[f_i,f_j]=\begin{cases}1, & \text{若 } f_i=f_j\\ 0, & \text{若 } f_i\neq f_j\end{cases}$$

$\boldsymbol{F}$ 上任意两个跳频序列 $\boldsymbol{X}=\{x_0,x_1,\cdots,x_{L-1}\}$ 和 $\boldsymbol{Y}=\{y_0,y_1,\cdots,y_{L-1}\}$ 在相对时延为 τ 时的周期汉明相关函数定义为

$$H_{X,Y}(\tau)=\sum_{j=0}^{L-1}h[x_j,y_{j+\tau}],\quad 0<\tau\leqslant L-1 \tag{1}$$

其中,下标 $j+\tau$ 按模 L 运算.当 $\boldsymbol{X}=\boldsymbol{Y}$ 时,$H_{X,X}(\cdot)$ 称为汉明自相关函数;当 $\boldsymbol{X}\neq\boldsymbol{Y}$ 时,$H_{X,Y}(\cdot)$ 称为汉明互相关函数.

对于跳频序列集 $\boldsymbol{S}$,其最大汉明自相关函数 $H(\boldsymbol{X})$,最大汉明互相关函数 $H(\boldsymbol{X},\boldsymbol{Y})$ 和最大汉明相关函数 H_m 分别定义为:

$$H(\boldsymbol{X})=\max_{1\leqslant\tau<L}\{H_{X,X}(\tau)\}$$

$$H(\boldsymbol{X},\boldsymbol{Y})=\max_{0\leqslant\tau<L,\boldsymbol{X}\neq\boldsymbol{Y}}\{H_{X,Y}(\tau)\}$$

$$H_m=\max\{\max_{X\in S}H(\boldsymbol{X}),\max_{X,Y\in S,X\neq Y}H(\boldsymbol{X},\boldsymbol{Y})\}$$

对任意实数 r,$\lfloor r\rfloor$ 表示 r 的整数部分,$\lceil r\rceil$ 表示大于或等于 r 的一个最小整数.

对任意的跳频序列 $\boldsymbol{X}$,其周期 L,频隙个数 v,及最大汉明自相关值 $H(\boldsymbol{X})$ 受到理论界的限制.1974 年,Lempel 和 Greenberger 得到了关于 $H(\boldsymbol{X})$ 的一个下界.

引理 1[12] 令 $\boldsymbol{F}$ 是一个具有 v 个频隙的集合,$\boldsymbol{X}$ 为 $\boldsymbol{F}$ 上长为 L 的跳频序列,其最大汉明自相关值满足下面的不等式,

$$H(\boldsymbol{X})\geqslant\left\lceil\frac{(L-b)(L-b+v)}{v(L-1)}\right\rceil \tag{2}$$

其中,b 是 L 模 v 的非负剩余.

对任意的跳频序列集 $\boldsymbol{S}$,Peng 和 Fan 得到了一个关于 $\boldsymbol{S}$ 的最大汉明相关函数 H_m 的一个理论界(称为 Peng-Fan 界).Peng-Fan 界考虑了序列集的大小.

引理 2[13] 令 $\boldsymbol{S}$ 是一个在大小为 v 的频隙集 $\boldsymbol{F}$ 上的跳频序列集,其序列数目为 M,序列长度为 L.令 $I=\lfloor LM/v\rfloor$,则有

$$H_m(\boldsymbol{S})\geqslant\left\lceil\frac{(LM-v)L}{(LM-1)v}\right\rceil \tag{3}$$

或

$$H_m(\boldsymbol{S})\geqslant\left\lceil\frac{2LMI-(I+1)Iv}{(LM-1)M}\right\rceil \tag{4}$$

如果序列 $\boldsymbol{X}$ 的最大汉明自相关值使得式(2)的等式成立,则称序列 $\boldsymbol{X}$ 是最优的跳频序列.对于一个跳频序列集 $\boldsymbol{S}$,如果 $\boldsymbol{S}$ 的最大汉明相关值使得式(3)或式(4)的等式成立,则称 $\boldsymbol{S}$ 是最优的跳频序列集.

本文使用 (L,v,k) 表示 $\boldsymbol{F}$ 上的一个周期为 L,频隙个数为 v,最大汉明自相关值为 k 的跳频序列.

3 具有差平衡性的 d-型函数

令 p 是一个奇素数,m,n,s 为任意的正整数,并且 $m\mid n$,q 为 p 的 s 次幂.$GF(q^n)$ 表示具有 q^n 个元素的有限域.$Tr_{q^n/q^m}(x)$ 表示从 $GF(q^n)$ 到 $GF(q^m)$ 的迹函数,其定义为

$$Tr_{q^n/q^m}(x)=x+x^{q^m}+x^{q^{2m}}+\cdots+x^{q^{m(n/m-1)}},\ x\in GF(q^n)$$

引理 3[14] 令 $\chi(x)=e^{2\pi\sqrt{-1}Tr_{q/p}(x)/p}$,那么对任意的 $y\in GF(q)\setminus\{0\}$,有

$$\sum_{x\in GF(q)}\chi(yx)=0$$

定义 1[14] 令 $f(x)$ 是从 $GF(q^n)$ 到 $GF(q^m)$ 的一个映射.当 x 遍历 $GF(q^n)\setminus\{0\}$ 中的所有元素时,如果 $f(x)$ 取 $GF(q^m)$ 中每个非零元 q^{n-m} 次,取零元 $q^{n-m}-1$ 次,则称 $f(x)$ 具有平衡性;对任意的 $y\in GF(q^n)\setminus\{0,1\}$,如果 $f(yx)-f(x)$ 具有平衡性,则称 $f(x)$ 具有差平衡性.

由引理 3 及定义 1,有,

引理 4 令 $f(x):GF(q^n)\to GF(q)$ 是一个具有差平衡性的函数,并且满足 $f(0)=0$,则对任意的 $y\in GF(q^n)\setminus\{0,1\}$,有

$$\sum_{x\in GF(q^n)\setminus\{0\}}\chi(f(yx)-f(x))=-1$$

定义 2[14] 令 d 为一个正整数,$f(x)$ 是从 $GF(q^n)$ 到 $GF(q^m)$ 的一个映射.如果对任意的 $\lambda\in GF(q^m)$,$x\in GF(q^n)$,有

$$f(\lambda x)=\lambda^d f(x)$$

则称 $f(x)$ 是一个 d-型函数.

任意具有差平衡性的 d-型函数,具有如下一些性质.

引理 5 任何具有差平衡性的 d-型函数 $h(x):GF(q^n)\to GF(q^m)$,同时具有平衡性,并且满足 $h(0)=0$.

证明:对任意 $\gamma\in GF(q^m)\setminus\{0\}$ 并且满足 $\gamma^d\neq1$,有 $h(\gamma x)-h(x)=\gamma^d h(x)-h(x)=(\gamma^d-1)h(x)$.由 $h(x)$ 的差平衡性及 $\gamma^d\neq1$,得到 $h(x)$ 具有平衡性.又 $0=h(0)-h(0)=h(\gamma\cdot0)-h(0)=(\gamma^d-1)\cdot h(0)$,因为 $\gamma^d-1\neq0$,所以 $h(0)=0$.引理得证.

令 $h(x)$ 是从 $GF(q^n)$ 到 $GF(q^m)$ 的一个映射,$T=(q^n-1)/(q^m-1)$,$b,e\in GF(q^m)$,α 是 $GF(q^n)$ 的一个本原元.对任意的 $\delta\in GF(q^n)\setminus GF(q^m)$,$M_\delta(b,e)$ 定义

为

$$M_\delta(b,e)=|\{t\mid h(\delta\alpha^t)=b \quad 且 \quad h(\alpha^t)=e,0\leqslant t<T\}|$$

引理 6[10]　令 $h(x):GF(q^n)\to GF(q^m)$是一个 1-型函数,并且满足差平衡性.那么,有

$$M_\delta(0,0)=\frac{q^{n-2m}-1}{q^m-1}$$

$$\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,0)=\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(0,b)=q^{n-2m}$$

$$\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(be,b)=q^{n-2m},\ \forall\ e\in GF(q^m)\setminus\{0\}$$

注 1　如果 $h(x)$是一个具有差平衡性的 d-型函数,并且满足 $\gcd(d,q^m-1)=1$,那么引理 6 的结论同样成立.

4　一类具有最优汉明自相关特性的跳频序列

下面利用具有平衡性及差平衡性的函数与具有差平衡性的 d-型函数的复合函数构造了一类具有最优汉明自相关特性的跳频序列.不失一般性,假设 $h(x)$为 1-型函数.下面给出序列的定义及其汉明自相关特性.

定义 3　令 n,m 及 r 为正整数,并且满足 $m\mid n$,$\gcd(r,q^m-1)=1$.假设 $f(x):GF(q^m)\to GF(q)$具有平衡性及差平衡性,且 $f(0)=0$. $h(x):GF(q^n)\to GF(q^m)$是一个 1-型函数,并且满足差平衡性.定义跳频序列 $\boldsymbol{u}=\{u(t),t=0,1,\cdots,q^n-2\}$为:

$$u(t)=f(h(\alpha^t)^r),\quad 0\leqslant t<q^n-1 \tag{5}$$

下面我们来计算序列 $\boldsymbol{u}$ 的汉明自相关值.

定理 1　序列 $\boldsymbol{u}=\{u(t),t=0,1,\cdots,q^n-2\}$是一个$(q^n-1,q,q^{n-1}-1)$跳频序列,其最大汉明自相关值达到了 Lempel-Greenberger 界,因此 $\boldsymbol{u}$ 是最优的跳频序列.

证明:

(1)当 $\alpha^\tau=1$ 时,显然有 $H_{\boldsymbol{u},\boldsymbol{u}}(\tau)=q^n-1$.

(2)当 $\alpha^\tau\in GF(q^n)\setminus GF(q^m)$时,令 $T=(q^n-1)/(q^m-1)$,$t=t_1T+t_2,0\leqslant t_1<q^m-1,0\leqslant t_2<T$,则

$$u(t)=f(h(\alpha^{t_1T+t_2})^r)=f(\alpha^{rt_1T}h(\alpha^{t_2})^r)$$

令 $\beta=\alpha^T$,则 β 为 $GF(q^m)$ 的本原元.因此,有

$$u(t)=f(\beta^{rt_1}h(\alpha^{t_2})^r)$$

由引理 6,序列 $\boldsymbol{u}$ 的汉明自相关函数如式(6),其中 $\delta=\alpha^\tau$.令

$$\theta(b,0)=\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,0)\chi(cf(\beta^{rt_1}b^r))$$

由引理 3,引理 5 及 $f(x)$的平衡性,有

$$\begin{aligned}\theta(b,0)&=\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,0)\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\chi(cf(\beta^{rt_1}b^r))\\&=q(q^{m-1}-1)\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,0)\\&=q^{n-2m+1}(q^{m-1}-1)\end{aligned}$$

同理,令

$$\theta(0,b)=\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(0,b)\chi(-cf(\beta^{rt_1}b^r))$$

则有

$$\theta(0,b)=q^{n-2m+1}(q^{m-1}-1)$$

定义 $\theta(be,b)$如式(7)所示.同样,由引理 3,引理 4,引理 5 及 $f(x)$的差平衡性,则可以得到 $\theta(be,b)$如式(8)所示.因此,可以得到 $H_{\boldsymbol{u},\boldsymbol{u}}(\tau)$如式(9)所示.

(3)当 $\alpha^\tau\in GF(q^m)\setminus\{0,1\}$时,由 $f(x)$的差平衡性,$h(x)$的平衡性,以及引理 3,引理 4 可以得到 $H_{\boldsymbol{u},\boldsymbol{u}}(\tau)$如式(10)所示.

$$\begin{aligned}H_{\boldsymbol{u},\boldsymbol{u}}(\tau)&=\frac{1}{q}\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\sum_{t_2=0}^{T-1}\chi(c(f(\beta^{rt_1}h(\delta\alpha^{t_2})^r)-f(\beta^{rt_1}h(\alpha^{t_2})^r)))\\&=\frac{1}{q}\Big[M_\delta(0,0)\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\chi(0)+\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,0)\chi(cf(\beta^{rt_1}b^r))\\&\quad+\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(0,b)\chi(-cf(\beta^{rt_1}b^r))\\&\quad+\sum_{b\in GF(q^m)\setminus\{0\}}\sum_{e\in GF(q^m)\setminus\{0\}}M_\delta(be,b)\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\chi(c(f(\beta^{rt_1}b^re^r)-f(\beta^{rt_1}b^r)))\Big]\end{aligned} \tag{6}$$

$$\theta(be,b)=\sum_{b\in GF(q^m)\setminus\{0\}}\sum_{e\in GF(q^m)\setminus\{0\}}M_\delta(be,b)\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\chi(c(f(\beta^{rt_1}b^re^r)-f(\beta^{rt_1}b^r))) \tag{7}$$

$$\begin{aligned}\theta(be,b)&=\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,b)\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\chi(c(f(\beta^{rt_1}b^r)-f(\beta^{rt_1}b^r)))\\&\quad+\sum_{b\in GF(q^m)\setminus\{0\}}\sum_{e\in GF(q^m)\setminus\{0,1\}}M_\delta(be,b)\sum_{c\in GF(q)}\sum_{t_1=0}^{q^m-2}\chi(c(f(\beta^{rt_1}b^re^r)-f(\beta^{rt_1}b^r)))\\&=q(q^m-1)\sum_{b\in GF(q^m)\setminus\{0\}}M_\delta(b,b)+q(q^{m-1}-1)\sum_{b\in GF(q^m)\setminus\{0\}}\sum_{e\in GF(q^m)\setminus\{0,1\}}M_\delta(be,b)\end{aligned}$$

$$= q^{n-2m+1}(q^m-1) + q^{n-2m+1}(q^{m-1}-1)(q^m-2) \tag{8}$$

$$H_{u,u}(\tau) = \frac{1}{q}\Big[q(q^m-1)(\frac{q^{n-2m}-1}{q^m-1}) + q^{n-2m+1}(q^{m-1}-1) + q^{n-2m+1}(q^{m-1}-1) + q^{n-2m+1}(q^m-1) + q^{n-2m+1}(q^{m-1}-1)(q^m-2)\Big] = q^{n-1}-1 \tag{9}$$

$$H_{u,u}(\tau) = \frac{1}{q}\sum_{c\in GF(q)}\sum_{t=0}^{q^n-2}\chi(c(f(h(\alpha^{t+\tau})^r)-f(h(\alpha^t)^r))) = \frac{1}{q}\sum_{c\in GF(q)}\sum_{t=0}^{q^n-2}\chi(c(f(\alpha^{\tau r}h(\alpha^t)^r)-f(h(\alpha^t)^r))$$
$$= \frac{1}{q}\Big[(q^{n-m}-1)\sum_{c\in GF(q)}\chi(0) + q^{n-m}\sum_{c\in GF(q)}\sum_{b\in GF(q^m)\setminus\{0\}}\chi(c(f(\alpha^{\tau r}b^r)-f(b^r))\Big]$$
$$= \frac{1}{q}\Big[q^{n-m+1} - q + q^{n-m}(q^{m-1}-1)\sum_{c\in GF(q)}\chi(0)\Big] = q^{n-1}-1 \tag{10}$$

因此,对任意的 $0<\tau<q^n-1$, $H_{\boldsymbol{u},\boldsymbol{u}}(\tau)=q^{n-1}-1$.

显然,$\boldsymbol{u}$ 的最大汉明自相关达到了 Lempel-Greenberger 界,因此是最优的跳频序列.定理得证.

基于不同的具有平衡性及差平衡性的函数与具有差平衡性的 d-型函数的复合函数,可以得到不同的跳频序列.本文所提出的构造方法可以得到具有长周期大线性复杂度的最优跳频序列.

2002 年,Helleseth 和 Gong 给出了一类具有差平衡性的 1-型函数(称为 HG 函数).

引理 7[15] 令 p 是一个奇素数,$n=mn_1$, $n_1=(2l+1)k$,其中 n,m,n_1,l,及 k 均为正整数.令 s,$1\leqslant s\leqslant 2l$ 为满足条件:$\gcd(s,2l+1)=1$ 的整数,$b_0=1$, $b_{is}=(-1)^i$,并且对任意的 $i=1,2,\cdots,l$,有 $b_i=b_{2l+1-i}$,其中 b 的下标运算按模 $2l+1$ 进行.令 $u_0=b_0/2=(p+1)/2$,并且对任意的 $i=1,2,\cdots,l$, $u_i=b_{2i}$.定义函数

$$h(x)=Tr_{q^n/q^m}\Big(\sum_{i=0}^{l}u_i x^{(q^{2mi}+1)/2}\Big) \tag{11}$$

则 $h(x)$是一个具有差平衡性的 1-型函数.

由定理 1 和引理 7,得到如下推论.

推论 1 令 $h(x)$是从 $GF(q^n)$到 $GF(q^m)$的 HG 函数,$f(x)$是从 $GF(q^m)$到 $GF(q)$的 HG 函数,则定义 3 中的序列 $\boldsymbol{u}$ 是一个$(q^n-1,q,q^{n-1}-1)$最优跳频序列.

推论 2 令 $h(x)$是从 $GF(q^n)$到 $GF(q^m)$的迹函数,$f(x)$是从 $GF(q^m)$到 $GF(q)$的 HG 函数,则序列 $\boldsymbol{u}$ 是一个$(q^n-1,q,q^{n-1}-1)$最优跳频序列.

例 1 设 $q=p=3$, $m=3$, $n=6$,及 $r=3$,因此 $\gcd(r,p^m-1)=\gcd(3,26)=1$.选取 x^6+x+2 作为 $GF(3^6)$的本原多项式,假设其本原元为 α. $f(x)=Tr_{3^3/3}(x)+2Tr_{3^3/3}(x^5)$是从 $GF(3^3)$到 $GF(3)$的 HG 函数, $h(x)=Tr_{3^6/3^3}(x)$,则我们得到序列

$\boldsymbol{u}=\{u(t)=Tr_{3^3/3}(Tr_{3^6/3^3}(\alpha^t)^3)+2Tr_{3^3/3}(Tr_{3^6/3^3}(\alpha^t)^{3*5}),$
$0\leqslant t\leqslant 3^6-2$

计算得到:

012101221100010112212211111110021010002112022102110202202121202211102100122102111101100012002201100021100022002021202102111220011220201110111212101122011202011211202022212121221112210000210210101102100001222100022010102222220121012200120101002010020100100202220012120111021011021221101100002021022210202012112000002121212200022101100122011101021202112200020221121122222220012020001221011201220101101212101122201200211201222202200021001102200012200011011012101201222110022110102222022121202211022101022122101011112121211222112000012012020220120000211120001102020111111021202110021020021020102222221202102001020010020020001011100212102220120222012112202200001012011120101022122100000121212110001120220021102220202
1000220220212021021112200112202011110112121011220112020112112020222121212211122100002102101011021000012221000220101022222201210122001201010020100201001000202220012120111021011021221101100002021022210202012112000002121212200022101100122011101021202112200020221121122222220012020001221011201220101101212101122201200211201222202200021001102200012200011011012101201222110022110102222022121202211022101022122101011112121211222112000012012020220120000211120001102020111111021202110021020021020102222221202102001020010020020001011100212102220120222012112202200001012011120101022122100000121212110001120220021102220202

该序列是一个(728,3,242)跳频序列,关于 Lempel-Greenberger 界是最优的.利用文献[16]的构造方法,可以得到包含 3 个序列的最优跳频序列集.

5 结论

本文利用具有平衡性及差平衡性的函数与具有差平衡性的 d-型函数的复合函数,构造了一类具有最优汉明自相关的跳频序列.通过选取某些 d-型函数(如 HG 函数),我们可以得到具有长周期大线性复杂度的最优跳频序列.利用文献[16]的构造方法,可以得到一个跳频序列集,该序列集关于 Peng-Fan 界是最优的.

参考文献

[1] 刁哲军,陈嘉兴,刘志华.基于多项式理论的一类最优跳频序列族[J].电子学报,2008,36(7):1334-1337.
DIAO Zhe-jun, CHEN Jia-xing, LIU Zhi-hua. A new family of optimal hopping sequences based upon polynomial theory [J]. Acta Electronica Sinica, 2008, 36(7): 1334-1337. (in Chinese)

[2] Ding C S, Yin J X. Sets of optimal frequency-hopping sequences [J]. IEEE Transactions on Information Theory, 2008, 54(8): 3741-3745.

[3] Ge G N, Miao Y, Yao Z X. Optimal frequency hopping sequences: auto-and cross-correlation properties [J]. IEEE Trans-

actions on Information Theory,2009,55(2):867 – 879.

[4] 李赞,常义林,等.基于分组密码的跳频序列族构造[J].电子学报,2005,33(4):620 – 623.
LI Zan, CHANG Yi-lin, et al. Structure of frequency hopping sequences family based on block cipher[J]. Journal of Electronics,2005,33(4):620 – 623.(in Chinese)

[5] 甘良才,吴燕翔.一类混沌映射产生跳频序列的方法[J].电子学报,2000,28(4):109 – 111.
GAN Liang-cai, WU Yan-xiang. Generating FH sequences by a class of chaotic maps [J]. Acta Electronica Sinica, 2000, 28(4):109 – 111.(in Chinese)

[6] 梅文华,杨义先.基于 $GF(p^k)$上 m 序列的最佳跳频序列族[J].通信学报,1996,17(2):12 – 15.
Mei Wen-hua, Yang Yi-xian. A family of optimal FH sequences based on m sequences over $GF(p^k)$ [J]. Journal of China Institute of Communications, 1996, 17(2): 12 – 15.(in Chinese)

[7] 梅文华,杨义先.基于 GMW 序列构造最佳跳频序列族[J].通信学报,1997,18(11):20 – 24.
Mei Wen-hua, Yang Yi-xian. A family of optimal FH sequences based on GMW sequences [J]. Journal of China Institute of Communications, 1997, 18(11): 20 – 24.(in Chinese)

[8] Klapper A. d-form sequences: Families of sequences with low correlation values and large linear spans [J]. IEEE Transactions on Information Theory, 1995, 41: 423 – 431.

[9] No J S. p-ary unified sequences: p-ary extended d-form sequences with the ideal autocorrelation property [J]. IEEE Transactions on Information Theory, 2002, 48(9): 2540 – 2546.

[10] Jang J W, No J S, Chung H. New sets of optimal p-ary low-correlation zone sequences [J]. IEEE Transactions on Information Theory, 2007, 53(2): 815 – 821.

[11] Z C Zhou, X H Tang. New families of binary low correlation zone sequences based on interleaved quadratic form sequences [J]. IEICE Transaction on Fundamentals, 2008, E91-A(11): 3406 – 3409.

[12] Lempel A, Greenberger H. Families of sequences with optimal Hamming correlation properties [J]. IEEE Transactions on Information Theory, 1974, IT-20(1): 90 – 94.

[13] Peng D Y, Fan P Z. Lower bounds on the Hamming auto-and cross correlations of frequency-hopping sequences [J]. IEEE Transactions on Information Theory, 2004, IT-50: 2149 – 2154.

[14] Golomb S W, Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar [M]. Cambridge University Press, 2005.

[15] Helleseth T, Gong G. New nonbinary sequences with ideal two-level autocorrelation functions [J]. IEEE Transactions on Information Theory, 2002, 48(11): 2868 – 2872.

[16] MEI W H, YANG Y X. Families of FH sequences based on pseudorandom sequences over $GF(p)$ [A]. Proceedings of the International Conferences on Communication Technology [C]. Beijing, China, 2000. 536 – 538.

作者简介

刘　方　女.1981 年 9 月出生,四川成都人.2005 年本科毕业于西南交通大学通信工程系,2011 年博士毕业于西南交通大学通信工程系.现工作于中电 30 所,从事扩频码序列设计研究工作.
E-mail: hmimy5416@163.com

彭代渊　男.1955 年 12 月出生,四川资阳人,教授、博士生导师.1987 年、2005 年分别在西南交通大学获工学硕士和博士学位.现为西南交通大学教授,主要从事扩频序列分析与设计、密码学、信息安全等方面的研究工作.
E-mail: dypeng@swjtu.edu.cn