一类具有最优平均汉明相关特性的跳频序列族

刘　方　　彭代渊
(西南交通大学信息编码与传输四川省重点实验室　成都　610031)

摘　要：平均汉明相关是评价跳频序列性能的重要判据之一。该文基于模 p 的高次剩余构造了一类长度为 p^2，序列族的大小为$(p-1)^2$的跳频序列族。该跳频序列族的平均汉明自相关值为 0，平均汉明互相关值为 1，关于平均汉明相关理论界是最优的。

关键词：跳频通信；跳频序列族；平均汉明相关；平均汉明相关界；高次剩余
中图分类号：TN914.43　　**文献标识码**：A　　**文章编号**：1009-5896(2010)05-1257-05
DOI: 10.3724/SP.J.1146.2009.00726

A Class of Frequency-Hopping Sequence Family with Optimal Average Hamming Correlation Property

Liu Fang　　Peng Dai-yuan
(*The Provincial Key Lab of Information Coding and Transmission*, *Southwest Jiaotong University*, *Chengdu* 610031, *China*)

Abstract: The average Hamming correlation is an important performance indicator of the frequency hopping sequences. Based on power residue module p, a class of frequency-hopping sequence family with length of sequences being p^2 and family size $(p-1)^2$ is constructed in this paper. It is shown that the average Hamming autocorrelation of the new frequency hopping sequence family is 0, and the average Hamming crosscorrelation is 1. The family is optimal with respect to the average Hamming correlation bound.

Key words: Frequency-hopping communication; Frequency-hopping sequence family; Average Hamming correlation; Average Hamming correlation bound; Power residue

1　引言

跳频(Frequency-Hopping, FH)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。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。跳频序列设计理论有两个方面的内容，一是寻找跳频序列设计时所受到的理论限制；二是设计出达到或接近理论限的跳频序列。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。近年来，跳频序列的设计已成为人们关注的热点[1−3]。

在设计跳频序列时，通常应考虑以下几个要求：(1)最大汉明自相关值尽可能小；(2)最大汉明互相关值尽可能小；(3)平均汉明自相关值尽可能小；(4)平均汉明互相关值尽可能小；(5)序列数目尽可能多。

基于有限域上的多项式，人们已经构造出了一些具有良好汉明自相关和汉明互相关函数的跳频/跳时序列族[4−12]，本文称这些序列为多项式序列。这些序列的构造均基于 Z_p，其中 Z_p 表示模 p 的剩余类环，p 为一个素数。这些序列的长度和频点个数相同，这限制了序列的长度，并且序列的长度和频点个数仅限于素数，因此在频点个数不是素数的实际应用中受到限制。本文将多项式序列从 Z_P 扩展到 Z_{p^2} 上，得到了一类序列长度为 p^2，序列个数为$(p-1)^2$，并且具有最优平均汉明相关值的跳频序列族。

2　基本概念

设 FH 通信系统中有 q 个频点，频点集合为 $F=\{f_0, f_1, \cdots, f_{q-1}\}$。令 G 为 F 上的周期为 L，序列个数为 M 的跳频序列族。G 中任意两个序列 $X=\{x_0, x_1, \cdots, x_{L-1}\}$和 $Y=\{y_0, y_1, \cdots, y_{L-1}\}$在相对时延为 τ 时的周期汉明相关函数定义为

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

如果 $x_j=y_{j+\tau}$，$h[x_j, y_{j+\tau}]=1$，否则为 0。其中，下标 $j+\tau$ 按(mod L)运算。当 $X=Y$ 时，$H_{X,X}(\cdot)$ 称为汉明自相关函数；当 $X\neq Y$ 时，$H_{X,Y}(\cdot)$ 称为汉明互相

2009-05-12 收到，2009-09-28 改回
国家自然科学基金(60872015，60572142)和四川省应用基础研究计划(2006J13-112)资助课题
通信作者：刘方　hmimy5416@163.com

关函数。

跳频序列族的平均汉明相关是衡量跳频序列性能的一个重要指标。跳频序列族的平均汉明自相关和互相关定义为

定义 1[10] 令 G 是一个在大小为 q 的频隙集 F 上的跳频序列族，其序列数目为 M，序列长度为 L。令

$$S_a(G)=\sum_{x\in G,1\le\tau\le L-1}H(x,x;\tau) \tag{2}$$

$$S_c(G)=\frac{1}{2}\sum_{x,y\in G,x\ne y,0\le\tau\le L-1}H(x,y;\tau) \tag{3}$$

称 $S_a(G)$为 G 的总汉明自相关值，$S_c(G)$为 G 的总汉明互相关值。定义

$$A_a(G)=S_a(G)/M(L-1) \tag{4}$$

$$A_c(G)=2S_c(G)/LM(M-1) \tag{5}$$

称 $A_a(G)$为 G 的平均汉明自相关值，$A_c(G)$为 G 的平均汉明互相关值。

最近，Peng 等人得到了关于 $A_a(G)$和 $A_c(G)$的理论界。

引理 1[11] 设 G 是一个在大小为 q 的频点集 F 上的跳频序列族，其序列数目为 M，序列长度为 L，$A_a(G)$及 $A_c(G)$分别为 G 的平均汉明自相关值和平均汉明互相关值，那么，

$$\frac{A_a(G)}{L(M-1)}+\frac{A_c(G)}{(L-1)}\ge\frac{LM-q}{q(L-1)(M-1)} \tag{6}$$

对于任意序列族 G，如果参数 q，L，M，$A_a(G)$以及 $A_c(G)$使得式(6)的等式成立，那么称序列族 G 具有最优的平均汉明相关特性，或称 G 关于平均汉明相关理论界是最优的。

3 一类具有最优平均汉明相关值的跳频序列族

令 p 为一个素数，$F=\{f_0,f_1,\cdots,f_{p^2-1}\}$ 为一个频隙集，Z_{p^2} 表示模 p^2 的剩余类环，$Z_{p^2}^*=Z_{p^2}\setminus\{0\}$。对任意整数 $x\in Z_{p^2}$，存在唯一的整数 x_1，x_2，使得 $x=x_1+x_2p$。因此对任意频隙 f_x，$x\in Z_{p^2}$，可以将其表示为 f_{x_1,x_2}。下面定义一个具有最优平均汉明相关值的跳频序列族。

定义 2 令 p 为一个素数，k 为任意的正整数。定义一个跳频序列族 G 为

$$\left.\begin{aligned}&G=\{g^{(a_0,a_1)}\mid a_0,a_1\in Z_p^*\}\\&g^{(a_0,a_1)}=\{g_x^{(a_0,a_1)}=f_{a_0x_1^k(\bmod p),a_1x_2^k((\bmod p))}\\&\qquad\mid x\in Z_{p^2},x=x_1+x_2p\}\end{aligned}\right\} \tag{7}$$

为研究序列族 G 的汉明相关性能，需要以下的定义和引理。

定义 3[13] 令 p 为一个素数，a 为一个正整数，并且 $\gcd(a,p)=1$。当同余方程 $x^k\equiv a(\bmod\ p)$ 有解时，a 称为模 p 的 k 次剩余；无解时，a 称为模 p 的 k 次非剩余。

引理 2[13] 如果 a 满足 $a^{(p-1)/\gcd(k,p-1)}\equiv1(\bmod\ p)$，那么同余方程 $x^k\equiv a(\bmod\ p)$ 具有 $\gcd(p-1,\ k)$ 个解，否则无解。

引理 3[13] 在模 p 的既约剩余系中，模 p 的 k 次剩余的元素个数是 $(p-1)/\gcd(p-1,\ k)$。

定义 4 对长度为 L 的任意跳频序列 X，Y，并且 $X\ne Y$，令

$$M_a(X,X)=\sum_{1\le\tau\le L-1}H(X,X;\tau) \tag{8}$$

$$M_c(X,Y)=\sum_{0\le\tau\le L-1}H(X,Y;\tau) \tag{9}$$

本文称 $M_a(X,X)$ 为序列 X 的汉明自相关值总和，$M_c(X,Y)$ 为序列对 X，Y 的汉明互相关值总和。

下面来计算序列族 G 中跳频序列的汉明自相关值总和及汉明互相关值总和。

定理 1 令 $\gcd(p-1,\ k)=1$，G 中任意的跳频序列 $g^{(a_0,a_1)}$ 及 $g^{(b_0,b_1)}$ 有如下的汉明自相关值总和及汉明互相关值总和：

$$M_a(g^{(a_0,a_1)},g^{(a_0,a_1)})=0 \tag{10}$$

$$M_c(g^{(a_0,a_1)},g^{(b_0,b_1)})=\begin{cases}p^2,\ a_0\ne b_0,a_1=b_1且a_0b_0^{-1}为k次剩余,或a_0=b_0,a_1\ne b_1且a_1b_1^{-1}为k次剩余\\p,\ a_0\ne b_0,a_1=b_1且a_0b_0^{-1}为k次非剩余,或a_0=b_0,a_1\ne b_1且a_1b_1^{-1}为k次非剩余\\p^2,\ a_0\ne b_0,a_1\ne b_1且a_0b_0^{-1},a_1b_1^{-1}为k次剩余\\p,a_0\ne b_0,a_1\ne b_1且a_0b_0^{-1}为k次非剩余,a_1b_1^{-1}为k次剩余或a_0\ne b_0,a_1\ne b_1且a_0b_0^{-1}为k次剩余,a_1b_1^{-1}为k次非剩余\\1,\ a_0\ne b_0,a_1\ne b_1且a_0b_0^{-1},a_1b_1^{-1}为k次非剩余\end{cases} \tag{11}$$

证明 由跳频序列的汉明自相关值总和及跳频序列对的汉明互相关值总和的定义，有

(1)对任意序列 $g^{(a_0,a_1)}\in G$，因为每个频点在 $g^{(a_0,a_1)}$ 中仅出现一次，显然 $g^{(a_0,a_1)}$ 在时延 $\tau\ne0$ 时的汉

明自相关为 0，因此有

$$M_a(g^{(a_0,a_1)},g^{(a_0,a_1)})=0 \tag{12}$$

(2)对任意的序列 $g^{(a_0,a_1)},g^{(b_0,b_1)}$，其中 $(a_0,a_1)\neq(b_0,b_1)$，它们之间的汉明互相关为

$$\begin{aligned}
M_c(g^{(a_0,a_1)},g^{(b_0,b_1)}) &= \sum_{0\le\tau\le p^2-1} H\left(g^{(a_0,a_1)},g^{(b_0,b_1)};\tau\right)\\
&= \sum_{0\le\tau\le p^2-1}\sum_{x_1,x_2\in Z_p} h\left(f_{a_0x_1^k(\mathrm{mod}\,p),a_1x_2^k(\mathrm{mod}\,p)},f_{b_0(x_1+\tau)^k(\mathrm{mod}\,p),b_1\lfloor(x+\tau)/p\rfloor^k(\mathrm{mod}\,p)}\right)\\
&= \sum_{0\le\tau\le p^2-1}\sum_{x_1\in Z_p} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0\left(x_1+\tau\right)^k(\mathrm{mod}\,p)\right)\\
&\quad\cdot\sum_{x_2\in Z_p} h\left(a_1x_2^k(\mathrm{mod}\,p),b_1\left(\lfloor(x_1+\tau)/p\rfloor+x_2\right)^k(\mathrm{mod}\,p)\right)\\
&= \sum_{x_1\in Z_p} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0x_1^k(\mathrm{mod}\,p)\right)\sum_{x_2\in Z_p} h\left(a_1x_2^k(\mathrm{mod}\,p),b_1x_2^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{1\le\tau\le p^2-1} h\left(0,b_0\tau^k(\mathrm{mod}\,p)\right)h\left(0,b_1\lfloor\tau/p\rfloor^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{1\le\tau\le p^2-1} h\left(0,b_0\tau^k(\mathrm{mod}\,p)\right)\sum_{x_2\in Z_p^*} h\left(a_1x_2^k(\mathrm{mod}\,p),b_1\left(\lfloor\tau/p\rfloor+x_2\right)^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{1\le\tau\le p^2-1}\sum_{x_1\in Z_p^*} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0(x_1+\tau)^k(\mathrm{mod}\,p)\right)h\left(0,b_1\lfloor(x_1+\tau)/p\rfloor^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{1\le\tau\le p^2-1}\sum_{x_1\in Z_p^*} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0(x_1+\tau)^k(\mathrm{mod}\,p)\right)\\
&\quad\cdot\sum_{x_2\in Z_p^*} h\left(a_1x_2^k(\mathrm{mod}\,p),b_1\left(\lfloor(x_1+\tau)/p\rfloor+x_2\right)^k(\mathrm{mod}\,p)\right)
\end{aligned}\tag{13}$$

(a)当 $a_0\neq b_0,a_1=b_1$ 时，

$$\begin{aligned}
M_c(g^{(a_0,a_1)},g^{(b_0,b_1)}) &= p+\sum_{x_1\in Z_p^*}\sum_{\tau=-x_1,\tau\neq0}^{p-x_1-1} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0\left(x_1+\tau\right)^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{x_1\in Z_p^*}\sum_{m=1}^{p-1}\sum_{\tau=mp-x_1,\tau\neq mp}^{(m+1)p-x_1-1} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0\left(x_1+\tau\right)^k(\mathrm{mod}\,p)\right)h\left(0,b_1\left|(x_1+\tau)/p\right|^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{m=1}^{p-1}\sum_{x_1\in Z_p^*} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0x_1^k(\mathrm{mod}\,p)\right)h\left(0,b_1\left|(x_1+mp)/p\right|^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{x_1,x_2\in Z_p^*}\sum_{\tau=-x_1,\tau\neq0}^{p-x_1-1} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0\left(x_1+\tau\right)^k(\mathrm{mod}\,p)\right)h\left(a_1x_2^k(\mathrm{mod}\,p),b_1x_2^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{x_1,x_2\in Z_p^*}\sum_{m=1}^{p-1}\sum_{\tau=mp-x_1,\tau\neq mp}^{(m+1)p-x_1-1} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0\left(x_1+\tau\right)^k(\mathrm{mod}\,p)\right)\\
&\quad\cdot h\left(a_1x_2^k(\mathrm{mod}\,p),b_1\left(\lfloor(x_1+\tau)/p\rfloor+x_2\right)^k(\mathrm{mod}\,p)\right)\\
&\quad+\sum_{m=1}^{p-1}\sum_{x_1,x_2\in Z_p^*} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0x_1^k(\mathrm{mod}\,p)\right)h\left(a_1x_2^k(\mathrm{mod}\,p),b_1\left(\lfloor(x_1+mp)/p\rfloor+x_2\right)^k(\mathrm{mod}\,p)\right)
\end{aligned}\tag{14}$$

(a$_1$)当 $a_0b_0^{-1}$ 为 k 次剩余时，对式(14)的第 2 项，令

$$N_2=\sum_{x_1\in Z_p^*}\sum_{\tau=-x_1,\tau\neq0}^{p-x_1-1} h\left(a_0x_1^k(\mathrm{mod}\,p),b_0\left(x_1+\tau\right)^k(\mathrm{mod}\,p)\right) \tag{15}$$

则有

$$\begin{aligned}
N_2 &= \sum_{\tau=-x_1,\tau\neq0}^{p-x_1-1}\left|\left\{x_1\left|a_0x_1^k\equiv b_0(x_1+\tau)^k(\mathrm{mod}\,p),1\le x_1<p\right\}\right|\\
&= \sum_{\tau=-x_1,\tau\neq0}^{p-x_1-1}\left|\left\{x_1\left|a_0b_0^{-1}\equiv(1+\tau/x_1)^k(\mathrm{mod}\,p),1\le x_1<p\right\}\right|
\end{aligned}\tag{16}$$

令 $y=1+\tau/x_1$，对任意 $\tau\neq 0(\mathrm{mod}\,p)$，当 x_1 遍历 $Z_p\backslash\{0\}$时，y 遍历 $Z_p\backslash\{1\}$。因为 $a_0b_0^{-1}$ 为 k 次剩余，由引理 2，$y^k\equiv a_0b_0^{-1}(\mathrm{mod}\,p)$ 有 $\gcd(k,p-1)$个解，因此得到

$$N_2=(p-1)\gcd(k,p-1)=p-1 \tag{17}$$

同理，对式(14)的第 5 项 N_5，有 $N_5=(p-1)^2$。

对式(14)的第 3 项 N_3，因为 $1\le m\le p-1, 1\le x_1\le p-1$ 及 $mp-x_1\le\tau\le(m+1)p-x_1-1$ 并且 $\tau\neq mp$，因此 $\lfloor(x_1+\tau)/p\rfloor^k(\mathrm{mod}\,p)\neq 0$，即 $h(0,\lfloor(x_1+\tau)/p\rfloor^k\cdot(\mathrm{mod}\,p))=0$，$N_3=0$。同样，第 4 项也为 0。

对式(14)的第 6 项 N_6，因为 $1\le m\le p-1$，$1\le x_1\le p-1$ 及 $mp-x_1\le\tau\le(m+1)p-x_1-1$ 并且 $\tau\neq mp$，因此，$\lfloor(x_1+\tau)/p\rfloor\neq 0(\mathrm{mod}\,p)$。那么，$a_1x_2^k\equiv b_1(x_2+\lfloor(x_1+\tau)/p\rfloor)^k(\mathrm{mod}\ p)$ 关于 x_2 有 $\gcd(p-1,k)-1=0$ 个解。因此有

$$M_c(g^{(a_0,a_1)},g^{(b_0,b_1)})=p^2 \tag{18}$$

(a_2)当 $a_0b_0^{-1}$ 为 k 次非剩余时，由引理 2，对任意 $\tau\neq 0(\mathrm{mod}\ p)$，$a_0x_1^k\equiv b_0(x_1+\tau)^k(\mathrm{mod}\ p)$ 关于 x_1 无解，因此有

$$M_c(g^{(a_0,a_1)},g^{(b_0,b_1)})=p \tag{19}$$

(b)同理，当 $a_0=b_0, a_1\neq b_1$ 时，

$$M_c(g^{(a_0,a_1)},g^{(b_0,b_1)})=\begin{cases}p^2, & a_1b_1^{-1}\text{为}k\text{次剩余}\\ p, & a_1b_1^{-1}\text{为}k\text{次非剩余}\end{cases} \tag{20}$$

(c)当 $a_0\neq b_0, a_1\neq b_1$ 时，

$$M_c(g^{(a_0,a_1)},g^{(b_0,b_1)})=\begin{cases}p^2, & a_0b_0^{-1},a_1b_1^{-1}\text{为}k\text{次剩余}\\ p, & a_0b_0^{-1}\text{为}k\text{次剩余},a_1b_1^{-1}\text{为}k\text{次非剩余}\\ p, & a_0b_0^{-1}\text{为}k\text{次非剩余},a_1b_1^{-1}\text{为}k\text{次剩余}\\ 1, & a_0b_0^{-1},a_1b_1^{-1}\text{为}k\text{次非剩余}\end{cases} \tag{21}$$

综合以上分析，结论得证。

定理 2 令 p 为一个素数，k 为任意的正整数，并且满足 $\gcd(p-1,k)=1$。跳频序列族 G 的平均汉明自相关值为 0，平均汉明互相关值为 1，跳频序列族 G 是平均汉明相关界下的最优序列族。

证明 对任意的 $a_0,a_1\in Z_p^*$，当 $\gcd(p-1,k)=1$ 时，由定理 1，有

$$S_a(G)=\sum_{a_0,a_1\in F_p^*}M_a\left(g^{(a_0,a_1)},g^{(a_0,a_1)}\right)=0 \tag{22}$$

因此，$A_a(G)=0$。

对任意定值 $1\le a\le p-1$，当 b 遍历所有$\{1,2,\cdots,p-1\}$时，ab^{-1} 遍历$\{1,2,\cdots,p-1\}$，由引理 3，ab^{-1} 取 k 次剩余的次数为$(p-1)$，取 k 次非剩余的次数为 0。由定理 1，有

$$\begin{aligned}2S_c(G)&=\sum_{a_0,a_1\in F_p^*}\sum_{\substack{b_0,b_1\in F_p^*,\\(b_0,b_1)\neq(a_0,a_1)}}M_c(g^{(a_0,a_1)},g^{(b_0,b_1)})\\&=2(p-1)^2(p-2)p^2+(p-1)^2(p-2)^2p^2\\&=p^3(p-1)^2(p-2)\end{aligned} \tag{23}$$

$$A_c(G)=\frac{2S_c(G)}{LM(M-1)}=\frac{p^3(p-1)^2(p-2)}{p^2(p-1)^2(p^2-2p)}=1 \tag{24}$$

由理论界，

$$\begin{aligned}\frac{A_a}{L(M-1)}+\frac{A_c}{(L-1)}&=\frac{1}{p^2-1}\ge\frac{LM-q}{q(L-1)(M-1)}\\&=\frac{p^2(p-1)^2-p^2}{p^2(p^2-1)(p^2-2p)}=\frac{1}{p^2-1}\end{aligned} \tag{25}$$

因此跳频序列族 G 是平均汉明相关界下的最优跳频序列族。 证毕

例 令 $p=5$，$k=3$，得到一个序列长度为 25，序列个数为 16 的一个跳频序列族。

$g^{(1,1)}=\{f_{0,0},f_{1,0},f_{3,0},f_{2,0},f_{4,0},f_{0,1},f_{1,1},f_{3,1},f_{2,1},f_{4,1},f_{0,3},f_{1,3},f_{3,3},f_{2,3},f_{4,3},f_{0,2},f_{1,2},f_{3,2},f_{2,2},f_{4,2},f_{0,4},f_{1,4},f_{3,4},f_{2,4},f_{4,4}\}$;

$g^{(1,2)}=\{f_{0,0},f_{1,0},f_{3,0},f_{2,0},f_{4,0},f_{0,2},f_{1,2},f_{3,2},f_{2,2},f_{4,2},f_{0,1},f_{1,1},f_{3,1},f_{2,1},f_{4,1},f_{0,4},f_{1,4},f_{3,4},f_{2,4},f_{4,4},f_{0,3},f_{1,3},f_{3,3},f_{2,3},f_{4,3}\}$;

$\vdots$

$g^{(4,4)}=\{f_{0,0},f_{4,0},f_{2,0},f_{3,0},f_{1,0},f_{0,4},f_{4,4},f_{2,4},f_{3,4},f_{1,4},f_{0,2},f_{4,2},f_{2,2},f_{3,2},f_{1,2},f_{0,3},f_{4,3},f_{2,3},f_{3,3},f_{1,3},f_{0,1},f_{4,1},f_{2,1},f_{3,1},f_{1,1}\}$。

该跳频序列族的平均汉明自相关值为 0，平均汉明互相关值为 1。

4 结论

基于 k 次同余方程，本文得到了一个 Z_{P^2} 上的长度为 p^2，序列个数为$(p-1)^2$ 的跳频序列族，证明了该序列族具有最优的平均汉明自相关特性。通过选择不同的 k，可以得到不同的跳频序列族。本文的构造方法简单、易行，并且汉明相关性能好。不足之处是序列的长度和频点个数相同，在某些应用环境中受到限制，比如某些需要序列长度相对于频点个数要大很多的通信系统。本文的构造方法同样可以扩展到 Z_{p^3}，Z_{p^4} 等，其汉明相关性能用本文的分析方法同样可以得到。

参 考 文 献

[1] Ding C S. Algebraic constructions of optimal frequency-hopping sequences[J]. *IEEE Transactions on Information Theory*, 2007, 53(7): 2606-2610.

[2] Ding C S and 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, and Yao Z X. Optimal frequency hopping sequences: auto-and cross-correlation properties[J]. *IEEE Transactions on Information Theory*, 2009, 55(2): 867–879.

[4] Titlebaum E L. Time-frequency hop signals part I: coding based upon the theory of linear congruences[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 1981, 17(4): 490–493.

[5] Titlebaum E L. Time-frequency hop signals part II: Coding based upon quadratic congruences[J]. *IEEE Transactions on Aerospace Electronic Systems*, 1981, 17(4): 494–499.

[6] Bellegarda J R and Titlebaum E L. Time-frequency hop codes based upon extended quadratic congruences[J]. *IEEE Transactions on Aerospace Electronic Systems*, *November*, 1988, 24(6): 726–742.

[7] Jia H D, Yuan D, and Peng D Y, *et al*.. On a general class of quadratic hopping sequences[J]. *Science in China*, *Ser. F*, 2008, 51(12): 2101–2114.

[8] Maric S V. Frequency hop multiple access codes based upon the theory of cubic congruences[J]. *IEEE Transactions on Aerospace Electronic Systems*, 1990, 26(6): 1035–1039.

[9] Fan P Z, Lee M H, and Peng D Y. New family of hopping sequences for time/frequency hopping CDMA systems[J]. *IEEE Transactions on Wireless Communications*, 2005, 4(6): 2836–2842.

[10] Peng D Y, Peng T, and Fan P Z. Generalized class of cubic frequency-hopping sequences with large family size[J]. *IEE Proceedings on Communications*, 2005, 152(6): 897–902.

[11] Peng D Y, Peng T, and Tang X H, *et al*.. A class of optimal frequency hopping sequences based upon the theory of power residues[C]. SETA 2008, Proceedings of the 5th international conference on Sequences and Their Applications, Lexington, KY, USA, September 14–18, 2008, 5203: 188–196.

[12] Peng D Y, Niu X H, and Tang X H, *et al*.. The average Hamming correlation for the cubic polynomial hopping sequences[C]. IEEE IWCMC 2008, International Conference on Wireless Communications and Mobile Computing, Crete, Greece, August 6–8, 2008: 464–469.

[13] 潘承洞. 潘承彪. 初等数论[M]. 北京: 北京大学出版社，1991: 226–229.

Pan Cheng-dong and Pan Cheng-biao. Elementary Number Theory. Beijing. Beijing University Press, 1991: 226–229.

刘　方：　女，1981 年生，博士生，从事扩频序列分析与设计.

彭代渊：　男，1955 年生，教授，博士生导师，从事扩频序列分析与设计、密码学、网络信息安全研究.