基于分圆法的一类素数平方周期跳频序列族

徐善顶*①② 曹喜望②③ 许广魁②④
①(南京工程学院数理部 南京 211167)
②(南京航空航天大学数学系 南京 211106)
③(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)
④(淮南师范学院数学与计算科学系 淮南 232038)

摘 要：最大汉明相关与平均汉明相关是评价跳频序列族性能的两个重要参数。该文首先给出了源于Fermat商的广义分圆类的性质；其次，基于此广义分圆法构造了一类$\mathbb{Z}_p$上的长度为p^2，序列族的大小为p的跳频序列族；最后证明了该跳频序列族关于最大汉明相关界与平均汉明相关界都是最优的。

关键词：跳频序列；Fermat商；分圆；最大汉明相关界；平均汉明相关界
中图分类号：TN914.41 **文献标识码**：A **文章编号**：1009-5896(2015)10-2460-06
DOI: 10.11999/JEIT150168

Class of Optimal Frequency-hopping Sequences Set with the Square of Prime Length Based on Cyclotomy

Xu Shan-ding①② Cao Xi-wang②③ Xu Guang-kui②④
①(*Department of Mathematics and Physics*, *Nanjing Institute of Technology*, *Nanjing* 211167, *China*)
②(*School of Mathematical Science*, *Nanjing University of Aeronautics and Astronautics*, *Nanjing* 211106, *China*)
③(*State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*)
④(*School of Mathematical Science*, *Huainan Normal University*, *Huainan* 232038, *China*)

Abstract: The Maximum Hamming Correlation (MHC) and the Average Hamming Correlation (AHC) are two important performance measures of the frequency-hopping sequences. Firstly, some properties of generalized cyclotomy are derived from Fermat quotient. Secondly, based on the generalized cyclotomy, a class of optimal frequency-hopping sequences set with length of sequences p^2 and size being p defined on $\mathbb{Z}_p$ is constructed. Finally, it is proved that the proposed frequency-hopping sequences set is optimal with respect to the maximum Hamming correlation bound and the average Hamming correlation bound.

Key words: Frequency-hopping sequence; Fermat quotient; Cyclotomy; Maximum Hamming correlation bound; Average Hamming correlation bound

1 引言

跳频技术被广泛应用于现代通信系统，比如超宽频、蓝牙、军事及雷达等。其中，用于控制载波频率跳变的地址码序列称为跳频序列(Frequency-Hopping Sequence, FHS)，它的性能对跳频系统有重大影响。在实际应用中，我们尽可能使用非平凡汉明自相关值和汉明互相关值较小的跳频序列以减少信号之间的彼此干扰，同时还要求序列的数目比较多以容纳尽可能多用户。但是，跳频序列族的参数受限于一些理论界[1−3]，因此构造关于这些界的最优跳频序列族成了设计的热点。目前关于跳频序列族的汉明相关最优性的评价指标主要有如下两种：一种是最大汉明相关[1,2](MHC)，代表的是跳频系统的最坏情形，目前大多数跳频序列的设计主要是针对它的最优构造[4−8]。另一种是平均汉明相关[3](AHC)，代表的是跳频系统的平均干扰状况，所以设计出达到平均汉明相关界的跳频序列族[9−12]也意义重大。然而，公开发表的能同时达到最大汉明相关界与平均汉明相关界的跳频序列族[1,13,14]却比较少，这也成了序列设计中的一个重要课题。

分圆是一个很古老的数论问题，分圆数和广义分圆数被广泛应用于数论问题、组合数学、序列设

收稿日期：2015-01-29；改回日期：2015-05-29；网络出版：2015-07-06
*通信作者：徐善顶 sdxzx11@163.com
基金项目：国家自然科学基金(11371011)和南京工程学院校级科研基金(QKJA201307)
Foundation Items: The National Natural Science Foundation of China (11371011); The Foundation of Nanjing Institute of Technology (QKJA201307)

计、编码理论以及密码学等。近年来，许多编码学者陆续利用 Gauss 经典分圆、Whiteman 广义分圆、Ding-Helleseth 广义分圆及其推广构造了一系列性能良好的序列。本文基于 Fermat 商[15]导出的广义分圆法[16]构造了一类长度为 p^2 的跳频序列族，同时给出了各类汉明相关值的计算公式辅以验证其最优性。随后证明所构造的序列族不仅关于最大汉明相关界与平均汉明相关界都是最优的，而且序列族中的每个序列关于 L-G 界(见引理 1)也是最优的。

2　基本概念

设 $\mathcal{F}=\{f_0,f_1,\cdots,f_{v-1}\}$ 为字符集，$X=\{x_0,x_1,\cdots,x_{L-1}\}$ $(x_i\in\mathcal{F},0\le i<L)$ 称为大小为 v 的字符集 $\mathcal{F}$ 上的一个跳频序列，L 称为跳频序列 X 的长度或周期。令 U 是大小为 v 的字符集 $\mathcal{F}$ 上的长度为 L 的 M 个跳频序列构成的序列族，对于 U 内的任意两个跳频序列 $X=\{x_0,x_1,\cdots,x_{L-1}\}$ $(x_i\in\mathcal{F},0\le i<L)$ 与 $Y=\{y_0,y_1,\cdots,y_{L-1}\}$ $(y_i\in\mathcal{F},0\le i<L)$，其(周期)汉明相关函数定义为

$$H_{X,Y}(\omega)=\sum_{t=0}^{L-1}h\left[x_t,y_{t+\omega}\right],\ 0\le\omega<L \tag{1}$$

这里函数 $h[x,y]$ 的定义为：当 $x=y$ 时 $h[x,y]=1$，否则为 0。式(1)中，下标 $t+\omega$ 按模 L 运算。若 $X=Y$ 且 $\omega\ne0$ 时，$H_{X,X}(\omega)$ 称为序列 X 的非平凡汉明自相关(函数)，简记为 $H_X(\omega)$。若 $X\ne Y$ 时，$H_{X,Y}(\omega)$ 称为序列 X 与 Y 的汉明互相关(函数)。

对于任意的 $X,Y\in U$ 且 $X\ne Y$，令

$$H(X)=\max_{1\le\omega<L}\left\{H_X(\omega)\right\};\ H(X,Y)=\max_{0\le\omega<L}\left\{H_{X,Y}(\omega)\right\} \tag{2}$$

Lempel 和 Greenberger[1]于 1974 年给出了跳频序列 X 的最大汉明自相关 $H(X)$ 的一个下界：

引理 1　(L-G 界[1]) 设 X 是大小为 v 的字符集 $\mathcal{F}$ 上的长度为 L 的任意跳频序列，则

$$H(X)\ge\left\lceil\frac{(L-b)(L+b-v)}{v(L-1)}\right\rceil \tag{3}$$

其中，$b=\langle L\rangle_v$ 表示 L 模 v 的最小非负整数，$\lceil x\rceil$ 表示大于或等于 x 的最小整数。

对于任意跳频序列族 U，最大汉明自相关 $H_a(U)$、最大汉明互相关 $H_c(U)$ 以及最大汉明相关 $H(U)$ 分别定义为

$$\left.\begin{aligned}H_a(U)&=\max_{X\in U}\{H(X)\}\\H_c(U)&=\max_{X,Y\in U,X\ne Y}\{H(X,Y)\}\\H(U)&=\max\{H_a(U),H_c(U)\}\end{aligned}\right\} \tag{4}$$

关于跳频序列族 U，Peng 和 Fan[2]于 2004 年给出了如下理论界：

引理 2[2]　设 U 是大小为 v 的字符集 $\mathcal{F}$ 上的长度为 L 的 M 个跳频序列构成的序列族，则

$$H(U)\ge\left\lceil\frac{(LM-v)L}{(LM-1)v}\right\rceil \tag{5}$$

关于跳频序列族的另外两个重要参数：平均汉明自相关和平均汉明互相关，分别定义如下。

定义 1[17]　设 U 是 $\mathcal{F}$ 上的长度为 L 的 M 个跳频序列的集合且 $|\mathcal{F}|=v$，则分别称为

$$\left.\begin{aligned}S_a(U)&=\sum_{X\in U,1\le\omega<L}H_X(\omega)\\S_c(U)&=\frac{1}{2}\sum_{X,Y\in U,X\ne Y,0\le\omega<L}H_{X,Y}(\omega)\end{aligned}\right\} \tag{6}$$

为跳频序列族 U 的总汉明自相关和总汉明互相关。同时分别称为

$$A_a(U)=\frac{S_a(U)}{M(L-1)};\ \ A_c(U)=\frac{2S_c(U)}{LM(M-1)} \tag{7}$$

为跳频序列族 U 的平均汉明自相关和平均汉明互相关。

2008 年，Peng 等人[18]给出了跳频序列族 U 的 $A_a(U)$ 和 $A_c(U)$ 的如下理论界：

引理 3[18]　设 U 是 $\mathcal{F}$ 上的长度为 L 的 M 个跳频序列的集合且 $|\mathcal{F}|=v$，则

$$\frac{A_a(U)}{L(M-1)}+\frac{A_c(U)}{L-1}\ge\frac{LM-v}{v(M-1)(L-1)} \tag{8}$$

今后我们将使用以下定义:

(1) 一个跳频序列 $X\in U$ 称为关于 L-G 界最优，如果 $H(X)$ 使得式(3)等号成立；

(2) 一个跳频序列族 U 称为关于最大汉明相关界最优(最优 MHC)，如果 $H(U)$ 使得式(5)等号成立；

(3) 一个跳频序列族 U 称为关于平均汉明相关界最优(最优 AHC)，如果 $A_a(U)$ 和 $A_c(U)$ 使得式(8)等号成立。

3　环 $\mathbb{Z}_{p^2}$ 的广义分圆法与广义分圆数

设 p 是奇素数，$u\in\mathbb{N}$ 且 $p\nmid u$，则 u 模 p 的 Fermat 商[15]定义为：$q_p(u)=\dfrac{u^{p-1}-1}{p}\pmod p$。

取 g 是模 p^2 的本原元且满足 $q_p(g)=1$，从而由文献[16]得

$$D_i=\left\{u:0\le u<p^2,\ \gcd(u,p)=1,\ q_p(u)=i\right\},\quad 0\le i<p \tag{9}$$

是环 $\mathbb{Z}_{p^2}$ 的 p 阶广义分圆类且 D_i 可简化为

$$D_i=\left\{g^{kp+i}\left(\bmod p^2\right):0\le k<p-1\right\},\ \ 0\le i<p \tag{10}$$

注 1：上面定义的关于环 $\mathbb{Z}_{p^2}$ 的 p 阶广义分圆既不同于 Whiteman 广义分圆，又不同于 Ding-Helleseth 广义分圆中环 $\mathbb{Z}_{p^2}$ 的二阶广义分圆，是一种全新的分圆形式。

定义：$P=\{p,2p,\cdots,(p-1)p\}$；$R=\{0\}$。

设 H 是 $\mathbb{Z}_L$ 的一个子集，$a\in\mathbb{Z}_L$，定义：

$$H+a=\{h+a:h\in H\},\ a\cdot H=\{a\cdot h:h\in H\} \tag{11}$$

对于固定的 i 和 j 且 $0\le i,j<p$，定义环 $\mathbb{Z}_{p^2}$ 的阶为 p 的广义分圆数为：$(i,j)=|(D_i+1)\cap D_j|$。

如上定义的广义分圆类与广义分圆数有以下性质：

性质 1[16] 若 $u\in D_i$，$0\le i<p$，那么 $uD_j=D_{i+j(\bmod p)}$，$0\le j<p$。

性质 2 设 D_0 及 (i,j) 分别表示如上所定义的广义分圆类和广义分圆数，则 (1) $-1\in D_0$；(2) $(i,j)=(j,i)$；(3) $(i,j)=(p-i,j-i)$。

证明 (1) 易见 -1 一定不属于 $P\cup R$，所以不妨设 $-1\in D_i$ $(0\le i<p)$。那么存在一个整数 k 且 $0\le k<p-1$ 使得 $-1\equiv g^{kp+i}\ (\bmod p^2)$，从而 $kp+i\equiv\dfrac{p(p-1)}{2}\ (\bmod p^2-p)$。故 $i\equiv 0\ (\bmod p)$，得证。

(2) 因为 $-1\in D_0$，所以存在固定的 k_0 $(0\le k_0<p-1)$，使得 $-1\equiv g^{k_0p}\ (\bmod p^2)$。从而

$$\begin{aligned}(i,j)&=\left|(D_i+1)\cap D_j\right|=\left|\left\{(k_1,k_2):g^{k_1p+i}+1\equiv g^{k_2p+j}\left(\bmod p^2\right),\ 0\le k_1,k_2<p-1\right\}\right|\\&=\left|\left\{(k_1,k_2):g^{(k_2+k_0)p+j}+1\equiv g^{(k_1+k_0)p+i}\left(\bmod p^2\right),\ 0\le k_1,k_2<p-1\right\}\right|=(j,i)\end{aligned} \tag{12}$$

(3)易证。 证毕

性质 3 $\sum_{j=0}^{p-1}(i,j)=\sum_{j=0}^{p-1}(j,i)=p-2,\ 0\le i<p$。

证明 根据广义分圆数的定义，$\sum_{j=0}^{p-1}(i,j)$ 等于方程 $x+1\equiv y(\bmod p^2)$，$x\in D_i$，$y\in\bigcup_{j=0}^{p-1}D_j=\mathbb{Z}_{p^2}^*$ 的解的个数。显然 D_i 中共有 $p-1$ 个元素，故只需研究 D_i+1 中与 p^2 不互素的元素个数，为此分为两种情况：

(1) 元素能被 p^2 整除。由 $-1\in D_0$ 可得属于该情形的元素个数分为两类：当 $i=0$ 时个数为 1，否则为 0；

(2) 元素能被 p 整除而不能被 p^2 整除。研究以下方程在固定 i 时解 k $(0\le k<p-1)$ 的个数：

$$g^{kp+i}+1\equiv 0(\bmod p)\Leftrightarrow kp\equiv\frac{p-1}{2}-i(\bmod p-1) \tag{13}$$

因为 $\gcd(p,p-1)=1$，所以上述方程模 $p-1$ 下 k 有唯一解。

综合(1)与(2)得结论。 证毕

性质 4 $\sum_{i=0}^{p-1}(i,i+m)=\sum_{i=0}^{p-1}(i+m,i)=p-2,\ m\in\mathbb{Z}$。

证明 由性质 2 中(3)可知 $\sum_{i=0}^{p-1}(i,i+m)=\sum_{i=0}^{p-1}(p-i,m)=\sum_{i=0}^{p-1}(i,m)$，再由性质 3 得结论。 证毕

性质 5 对 $m\in\mathbb{Z}_p^*$，有

(1) $$\sum_{i=0}^{p-1}|(D_i+\omega)\cap D_i|=\begin{cases}0, & \omega\in P\\ p-2, & \omega\in\mathbb{Z}_{p^2}^*\end{cases}$$

(2) $$\sum_{i=0}^{p-1}|(D_{i+m}+\omega)\cap D_i|=\begin{cases}0, & \omega\in R\\ p, & \omega\in P\\ p-2, & \omega\in\mathbb{Z}_{p^2}^*\end{cases}$$

证明 (1) 当 $\omega\in P$ 时，设元素 $u\in(D_i+\omega)\cap D_i$。则

$$\begin{aligned}u\equiv g^{k_1p+i}+\omega\equiv g^{k_2p+i}(\bmod p^2),\ 0\le k_1,k_2<p-1\\ \Rightarrow g^{k_1p+i}\equiv g^{k_2p+i}(\bmod p)\\ \Rightarrow k_1p\equiv k_2p(\bmod p-1)\\ \Rightarrow k_1\equiv k_2(\bmod p-1)\Rightarrow k_1=k_2\end{aligned} \tag{14,15}$$

代入式(14)得 $\omega\equiv 0(\bmod p^2)$，与 $\omega\in P$ 矛盾。故此时 $|(D_i+\omega)\cap D_i|=0$。

当 $\omega\in\mathbb{Z}_{p^2}^*$ 时，不妨设 $\omega\in D_j(0\le j<p)$，由性质 1 得 $\omega^{-1}D_i=D_{i-j}$。那么

$$\begin{aligned}\sum_{i=0}^{p-1}|(D_i+\omega)\cap D_i|&=\sum_{i=0}^{p-1}|\left(\omega^{-1}D_i+1\right)\cap\omega^{-1}D_i|\\&=\sum_{i=0}^{p-1}|\left(D_{i-j}+1\right)\cap D_{i-j}|=\sum_{i=0}^{p-1}(i,i)\end{aligned} \tag{16}$$

由性质 4 可得结论。

(2) 当 $\omega\in R$ 时结论显然；当 $\omega\in\mathbb{Z}_{p^2}^*$ 时证明方法类似式(16)，故省略。

当 $\omega\in P$ 时，设元素 $u\in(D_{i+m}+\omega)\cap D_i$。则

$$\begin{aligned}u\equiv g^{k_1p+i+m}+\omega\equiv g^{k_2p+i}\left(\bmod p^2\right),\ 0\le k_1,k_2<p-1\\ \Rightarrow g^{k_1p+i+m}\equiv g^{k_2p+i}(\bmod p)\\ \Rightarrow k_1p\equiv k_2p-m(\bmod p-1)\end{aligned} \tag{17,18}$$

不妨设 $k_1p=k_2p-m+n(p-1)$，其中 $1\le n<p$ 且由 m 惟一确定。代入式(17)得

$$g^{k_2p+n(p-1)+i}+\omega\equiv g^{k_2p+i}\left(\bmod p^2\right) \tag{19}$$

即 $g^{k_2p+i}[1-g^{n(p-1)}]\equiv\omega(\bmod p^2)$。又显然有 $1-g^{n(p-1)}\equiv 0\ (\bmod p)$ 且 $1-g^{n(p-1)}\not\equiv 0\ (\bmod p^2)$，因而

$g^{k_2p+i}[1-g^{n(p-1)}]\in P$。下面证明对于固定的$i\in\mathbb{Z}_p$与$m\in\mathbb{Z}_p^*$，$\{g^{k_2p+i}[1-g^{n(p-1)}]:0\le k_2<p-1\}$元素两两不等。一旦$m$确定，则$n$确定，从而存在固定的$r$ $(1\le r<p)$使得$1-g^{n(p-1)}=rp$。假如存在k_2与k_2'且$0\le k_2,k_2'<p-1$使得

$$g^{k_2p+i}\left[1-g^{n(p-1)}\right]\equiv g^{k_2'p+i}\left[1-g^{n(p-1)}\right]\left(\mathrm{mod}\ p^2\right) \quad (20)$$

故$g^{k_2p+i}rp\equiv g^{k_2'p+i}rp(\mathrm{mod}\ p^2)$。又因为$\gcd(r,p)=1$，所以$g^{k_2p+i}\equiv g^{k_2'p+i}(\mathrm{mod}\ p)$。因此

$$\text{式}(20)\Leftrightarrow k_2p\equiv k_2'p(\mathrm{mod}\ p-1)$$
$$\Leftrightarrow k_2\equiv k_2'(\mathrm{mod}\ p-1)\Leftrightarrow k_2=k_2' \quad (21)$$

所以当$\omega\in P$时，皆有$|(D_{i+m}+\omega)\cap D_i|=1$。故(2)成立。　　证毕

性质 6 对任一给定的i，$0\le i<p$，有

$$\left|(D_i+\omega)\cap(P\cup R)\right|=\left|((P\cup R)+\omega)\cap D_i\right|=\begin{cases}0, & \omega\in P\cup R\\ 1, & \omega\in\mathbb{Z}_{p^2}^*\end{cases} \quad (22)$$

证明　当$\omega\in P\cup R$时，结论显然成立；当$\omega\in\mathbb{Z}_{p^2}^*$时，设元素$u\in(D_i+\omega)$。则

$$u\equiv g^{kp+i}+\omega(\mathrm{mod}\ p^2)\in P\cup R\Leftrightarrow g^{kp+i}$$
$$\equiv-\omega(\mathrm{mod}\ p)\Leftrightarrow kp\equiv\mathrm{ind}_g(-\omega)-i(\mathrm{mod}\ p-1) \quad (23)$$

其中$\mathrm{ind}_g(-\omega)$表示$-\omega$(对于本原元g)模p的指数。因为$\gcd(p,p-1)=1$，所以同余方程式(23)模$p-1$下k有唯一解。另一等式类似证明。　　证毕

性质 7 $\left|((P\cup R)+\omega)\cap(P\cup R)\right|=\begin{cases}p, & \omega\in P\cup R\\ 0, & \omega\in\mathbb{Z}_{p^2}^*\end{cases}$

4　新的跳频序列族的构造

本节将构造一类新的跳频序列族，并利用上节的性质给出该跳频序列族的汉明相关值的分布，随后证明了所构造的序列族不仅具有最优 MHC 与最优 AHC，而且序列族中的每个序列关于 L-G 界也是最优的。

设$C_0=D_0\cup P\cup R$；$C_i=D_i$，$i=1,2,\cdots,p-1$。易见$\bigcup_{i=0}^{p-1}C_i=\mathbb{Z}_{p^2}$与$C_i\cap C_j=\varnothing$(当$i\ne j$时)。

令$X=\{x_0,x_1,\cdots,x_{L-1}\}$是$\mathcal{F}$上的长度为$L$的跳频序列，那么称

$$\mathrm{supp}_X(k)=\{t:x_t=k,0\le t<L\},\quad k\in\mathcal{F} \quad (24)$$

为元素$k\in\mathcal{F}$在序列X中的支撑集。

定义 2　设p是奇素数，C_i $(0\le i<p)$定义同上。定义跳频序列族$U=\{X^{(i)}:i=0,1,\cdots,p-1\}$，其中$X^{(i)}=\{x_0^{(i)},x_1^{(i)},\cdots,x_{p^2-1}^{(i)}\}$的支撑集为

$$\mathrm{supp}_{X^{(i)}}(j)=C_{i+j\,(\mathrm{mod}\,p)},\quad 0\le j<p \quad (25)$$

定理 1　设p是奇素数，则如上定义的跳频序列族U具有如下性质：

(1)序列族的大小$|U|=p$，序列的长度为$L=p^2$，字符集的大小为$|\mathcal{F}|=p$；

(2)对于任意跳频序列$X^{(i)}\in U(0\le i<p)$，非平凡汉明自相关为$H_{X^{(i)}}(\omega)=p$；

(3)对于任意两个不同的跳频序列$X^{(i)},X^{(j)}\in U$，汉明互相关为

$$H_{X^{(i)},X^{(j)}}(\omega)=\begin{cases}0, & \omega\in R\\ p, & \omega\in P\cup\mathbb{Z}_{p^2}^*\end{cases} \quad (26)$$

证明　(1) 显然成立；

(2) 当$\omega\ne0$时，有

$$\begin{aligned}H_{X^{(i)}}(\omega)&=\sum_{t=0}^{p^2-1}h\left[x_t^{(i)},x_{t+\omega}^{(i)}\right]=\sum_{j=0}^{p-1}\left|\left(C_{j+i}+\omega\right)\cap C_{j+i}\right|\\&=\sum_{j=0}^{p-1}\left|\left(C_j+\omega\right)\cap C_j\right|=\sum_{j=0}^{p-1}\left|\left(D_j+\omega\right)\cap D_j\right|\\&\quad+2\left|\left(D_0+\omega\right)\cap(P\cup R)\right|\\&\quad+\left|((P\cup R)+\omega)\cap(P\cup R)\right|\end{aligned} \quad (27)$$

由性质 5，性质 6，性质 7 可得结论。

(3) 对于$0\le i\ne j<p$而言有

$$\begin{aligned}H_{X^{(i)},X^{(j)}}(\omega)&=\sum_{t=0}^{p^2-1}h\left[x_t^{(i)},x_{t+\omega}^{(j)}\right]\\&=\sum_{l=0}^{p-1}\left|\left(C_{l+i}+\omega\right)\cap C_{l+j}\right|\\&=\sum_{l=0}^{p-1}\left|\left(C_{l+i-j}+\omega\right)\cap C_l\right|\\&=\sum_{l=0}^{p-1}\left|\left(D_{l+i-j}+\omega\right)\cap D_l\right|\\&\quad+\left|\left(D_{i-j}+\omega\right)\cap(P\cup R)\right|\\&\quad+\left|((P\cup R)+\omega)\cap D_{j-i}\right|\end{aligned} \quad (28)$$

由p是奇素数可知，$i-j\not\equiv j-i\ (\mathrm{mod}\ p)$。则由性质 5，性质 6 可得结论。　　证毕

定理 2　(1) U中的每个跳频序列关于 L-G 界皆是最优的；

(2) 跳频序列族U具有最优 MHC。

证明　(1)对于任意跳频序列$X^{(i)}\in U(0\le i<p)$，有$b=\langle L\rangle_v=0$。因此，

$$\left\lceil\frac{(L-b)(L+b-v)}{v(L-1)}\right\rceil=\left\lceil\frac{p^2}{p+1}\right\rceil=\left\lceil p-\frac{p}{p+1}\right\rceil$$
$$=p=H\left(X^{(i)}\right) \quad (29)$$

(2)对于跳频序列族U而言，

$$\left\lceil \frac{(LM-\upsilon)L}{(LM-1)\upsilon} \right\rceil = \left\lceil \frac{p^4-p^2}{p^3-1} \right\rceil = \left\lceil p - \frac{p^2-p}{p^3-1} \right\rceil = p = H(U)。$$

证毕

定理 3 跳频序列族 U 的平均汉明自相关和平均汉明互相关分别为

$$A_a(U) = p, \quad A_c(U) = p - 1/p \tag{30}$$

进一步地，跳频序列族 U 具有最优 AHC。

证明 由 $S_a(U)$ 和 $S_c(U)$ 的定义可知

$$\left.\begin{aligned} S_a(U) &= \sum_{X\in U, 1\le\omega<p^2} H_X(\omega) = p^2\left(p^2-1\right) \\ S_c(U) &= \frac{1}{2}\sum_{X,Y\in U, X\ne Y, 0\le\omega<p^2} H_{X,Y}(\omega) \\ &= \frac{1}{2}p^2\left(p^2-1\right)(p-1) \end{aligned}\right\} \tag{31}$$

再由平均汉明自相关和平均汉明互相关的定义可得式(30)。把式(30)代入式(8)可得：

$$\frac{A_a(U)}{L(M-1)} + \frac{A_c(U)}{L-1} = \frac{p^2\left(p^2-1\right)+p^2\left(p^2-1\right)(p-1)}{p^2\left(p^2-1\right)p(p-1)} = \frac{1}{p-1} \ge \frac{LM-\upsilon}{\upsilon(M-1)(L-1)} \tag{32}$$

其中，$\dfrac{LM-\upsilon}{\upsilon(M-1)(L-1)} = \dfrac{p^3-p}{p(p-1)(p^2-1)}$。因此，跳频序列族 U 具有最优 AHC。 证毕

注 2： 本节与文献[13]构造的相似与不同之处：

(1)相似：与文献[13]所构造的跳频序列族相比，本节构造的序列族不仅具有与其相同的序列周期 L 、序列个数 $|U|$ 和字符集大小 $|\mathcal{F}|$，而且具有相同的最优汉明相关特性，即：所构造的序列族具有最优 MHC 和最优 AHC，其中每个序列关于 L-G 界也是最优的(见表 1)。

(2)不同：首先，本文与文献[13]所构造的跳频序列形式完全不同；其次，文献[13]中的构造主要利用广义 bent 函数，其序列族定义形式和最优性证明过程相对复杂。而本节中的构造主要采用的是广义分圆法，不仅定义字符集更加简洁，而且序列族构造方法简单可行，从而具有更强的应用背景。

例 1 当 $p=7$ 时，则环 $\mathbb{Z}_{49}$ 的七阶广义分圆类 $D_i\ (0\le i\le 6)$ 为

D_0={1,31,30,48,18,19}

D_1={3,44,41,46,5,8}

D_2={9,34,25,40,15,24}

D_3={27,4,26,22,45,23}

D_4={32,12,29,17,37,20}

D_5={47,36,38,2,13,11}

D_6={43,10,16,6,39,33}

跳频序列族 U 为

$X^{(0)}$={0,0,5,1,3,1,6,0,1,2,6,5,4,5,0,2,6,4,0,0,4,0,3,3,
2,2,3,3,0,4,0,0,4,6,2,0,5,4,5,6,2,1,0,6,1,3,1,5,0}

$X^{(1)}$={6,6,4,0,2,0,5,6,0,1,5,4,3,4,6,1,5,3,6,6,3,6,2,2,1,
1,2,2,6,3,6,6,3,5,1,6,4,3,4,5,1,0,6,5,0,2,0,4,6}

$X^{(2)}$={5,5,3,6,1,6,4,5,6,0,4,3,2,3,5,0,4,2,5,5,2,5,1,1,0,
0,1,1,5,2,5,5,2,4,0,5,3,2,3,4,0,6,5,4,6,1,6,3,5}

$X^{(3)}$={4,4,2,5,0,5,3,4,5,6,3,2,1,2,4,6,3,1,4,4,1,4,0,0,6,
6,0,0,4,1,4,4,1,3,6,4,2,1,2,3,6,5,4,3,5,0,5,2,4}

$X^{(4)}$={3,3,1,4,6,4,2,3,4,5,2,1,0,1,3,5,2,0,3,3,0,3,6,6,5,
5,6,6,3,0,3,3,0,2,5,3,1,0,1,2,5,4,3,2,4,6,4,1,3}

$X^{(5)}$={2,2,0,3,5,3,1,2,3,4,1,0,6,0,2,4,1,6,2,2,6,2,5,5,4,
4,5,5,2,6,2,2,6,1,4,2,0,6,0,1,4,3,2,1,3,5,3,0,2}

$X^{(6)}$={1,1,6,2,4,2,0,1,2,3,0,6,5,6,1,3,0,5,1,1,5,1,4,4,3,
3,4,4,1,5,1,1,5,0,3,1,6,5,6,0,3,2,1,0,2,4,2,6,1}

跳频序列 $X^{(i)}\ (0\le i\le 6)$ 的汉明自相关为

$H_{X^{(i)}}$={49,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,
7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7}

跳频序列 $X^{(i)}$ 与 $X^{(j)}\ (0\le i\ne j\le 6)$ 的汉明互相关为

$H_{X^{(i)},X^{(j)}}$={0,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,
7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7}

跳频序列族 U 最大汉明自相关和最大汉明互相关都为 7；跳频序列族 U 平均汉明自相关和平均汉明互相关分别为 7 和 6.8571。

表 1 几类相关跳频序列族的比较(其中 p 为奇素数)

跳频序列族	L	$\mathcal{F}$	$\lvert\mathcal{F}\rvert$	$\lvert U\rvert$	L-G 界	MHC	AHC
文献[9]	p^2	$\mathbb{Z}_{p^2}$	p^2	$(p-1)^2$	最优	非最优	最优
文献[13]	p^2	$p\mathbb{Z}_p$	p	p	最优	最优	最优
文献[14]	p^2-p	$\mathbb{Z}_p$	p	p	最优	最优	最优
本文	p^2	$\mathbb{Z}_p$	p	p	最优	最优	最优

5　结束语

本文利用由Fermat商导出的$\mathbb{Z}_{p^2}$上的广义分圆构造了一类新的跳频序列族，并且证明了该序列族具有最优MHC与最优AHC。其构造方法简单可行，并且汉明相关性能好。不足之处是序列的参数比较固定，使用环境较为局限。

参 考 文 献

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

[2] Peng D Y and Fan P Z. Lower bounds on the Hamming auto-and cross-correlations of frequency-hopping sequences[J]. *IEEE Transactions on Information Theory*, 2004, 50(9): 2149–2154.

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

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

[5] Zhang Y, Ke P H, and Zhang S Y. Optimal frequency-hopping sequences based on cyclotomy[C]. First International Workshop on Education Technology and Computer Science, Wuhan, China, 2009: 1122–1126.

[6] Zhou Z C, Tang X H, Peng D Y, *et al*.. New constructions for optimal sets of frequency-hopping sequences[J]. *IEEE Transactions on Information Theory*, 2011, 57(6): 3831–3840.

[7] Zeng X Y, Cai H, Tang X H, *et al*.. Optimal frequency hopping sequences of odd length[J]. *IEEE Transactions on Information Theory*, 2013, 59(5): 3237–3248.

[8] Ren W L, Fu F W, and Zhou Z C. New sets of frequency-hopping sequences with optimal Hamming correlation[J]. *Designs, Codes and Cryptography*, 2014, 72(2): 423–434.

[9] 刘方, 彭代渊. 一类具有最优平均汉明相关特性的跳频序列族[J]. 电子与信息学报, 2010, 32(5): 1257–1261.
Liu F and Peng D Y. A class of frequency-hopping sequence family with optimal average Hamming correlation property[J]. *Journal of Electronics & Information Technology*, 2010, 32(5): 1257–1261.

[10] Liu F, Peng D Y, and Zhou Z C. A new frequency-hopping sequence set based upon generalized cyclotomy[J]. *Designs, Codes and Cryptography*, 2013, 69(2): 247–259.

[11] 柯品惠, 章海辉, 张胜元. 新的具有最优平均汉明相关性的跳频序列族[J]. 通信学报, 2012, 33(9): 168–175.
Ke P H, Zhang H H, and Zhang S Y. New class of frequency-hopping sequence set with optimal average Hamming correlation property[J]. *Journal on Communications*, 2012, 33(9): 168–175.

[12] Zhang A X, Zhou Z C, and Feng K Q. A lower bound on the average Hamming correlation of frequency-hopping sequence sets[J]. *Advances in Mathematics of Communications*, 2015, 9(1): 55–62.

[13] Kumar P V. Frequency-hopping code sequence designs having large linear span[J]. *IEEE Transactions on Information Theory*, 1988, 34(1): 146–151.

[14] Chung J H and Yang K. A new class of balanced near-perfect nonlinear mappings and its application to sequence design[J]. *IEEE Transactions on Information Theory*, 2013, 59(2): 1090–1097.

[15] Agoh T, Dilcher K, and Skula L. Fermat quotients for composite moduli[J]. *Journal of Number Theory,* 1997, 66(1): 29–50.

[16] Chen Z X. Trace representation and linear complexity of binary sequences derived from Fermat quotients[J]. *Science China*, 2014, 57(11): 1–10.

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

[18] Peng D Y, Peng T, Tang X H, *et al*.. A class of optimal frequency hopping sequences based upon the theory of power residues[C]. Sequences and Their Applications (SETA 2008), Lexington, KY, USA, 2008: 188–196.

徐善项：　男，1979 年生，讲师，主要研究方向为跳频序列分析与设计.

曹喜望：　男，1965 年生，教授，主要研究方向为代数组合论与代数密码学.

许广魁：　男，1981 年生，讲师，主要研究方向为代数组合论与代数密码学.