新的具有最优平均汉明相关性的跳频序列族

柯品惠，章海辉，张胜元
（福建师范大学 网络安全与密码技术重点实验室，福建 福州 350007）

摘 要：平均汉明相关值是评价跳频序列族性能的一个重要参数。首先给出了 Whiteman 广义分圆类的一个推广，并且给出该推广的分圆类的一些性质。其次，基于推广的 Whiteman 广义分圆类构造了新的跳频序列族，并证明了新构造的跳频序列族关于平均汉明相关界是最优的。

关键词：跳频序列；Whiteman 广义分圆；平均汉明相关界
中图分类号：TN914.43 **文献标识码**：B **文章编号**：1000-436X(2012)09-0168-08

New class of frequency-hopping sequences set with optimal average Hamming correlation property

KE Pin-hui, ZHANG Hai-hui, ZHANG Sheng-yuan
(Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: The average Hamming correlation is an important performance parameter of frequency-hopping sequences. A generalization of Whiteman cyclotomy was proposed and then some properties of the new defined cyclotomy classes were presented. Based on the generalization of Whiteman cyclotomy, new classes of frequency-hopping sequences set were constructed. The proposed frequency-hopping sequences set was shown to be optimal with respect to the average Hamming correlation bound.

Key words: frequency-hopping sequence; Whiteman generalized cyclotomy; average Hamming correlation bound

1 引言

跳频码分多址（FH-CDMA）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，所以在蓝牙、超宽频、雷达等当中都得到了广泛的应用[1,2]。

在跳频多址扩频系统中，当接收器解调来自发送器传送的信号时，会受不明信号的干扰。为了防止相互干扰，采用的跳频序列的汉明互相关值和非平凡的汉明自相关值应尽可能小。

迄今已有的关于跳频序列的汉明相关最优性的判定方式有如下 2 种。

一种是最大的汉明相关值[3,4]，另外一种是平均汉明相关值[5]。近年来,跳频序列的设计已成为人们关注的热点，其中大部分都是针对最大的汉明相关值构造出最优的跳频序列族[6~10]。而平均汉明相关值代表的是跳频多址扩频系统平均误差，因此,设计出具有达到平均汉明相关界的跳频序列族也是非常有意义的。基于模 p 的高次剩余及 Whiteman 广义分圆类，文献[11]和文献[12]分别构造了达到平均汉明相关界的跳频序列族。然而，较之达到最大汉明相关界的跳频序列，公开发表的达到平均汉明相

收稿日期：2011-04-02；修回日期：2011-08-23
基金项目：国家自然科学基金资助项目（61102093，61072080）；福建省高校服务海西建设重点项目——基于数学的信息化技术研究；福建省自然科学基金资助项目（2010J01319）
Foundation Items: The National Natural Science Foundation of China (61102093, 61072080); Key Project of Fujian Provincial Universities——Information Technology Research Based on Mathematics; The Natural Science Foundation of Fujian Province (2010J01)

关界的跳频序列族的结果比较少。

Ding-Helleseth 广义分圆类及 Whiteman 广义分圆类是 2 种重要的分圆类。人们对上述 2 种分圆类进行了各种推广，并由此构造了一系列性质良好的序列。最近，Meidl 在文献[13]中给出了 Ding-Helleseth 广义分圆的推广，进而利用该推广的分圆类构造了多值序列，并分析了该序列的自相关值及错综复杂度等性质。本文首先给出 Whiteman 广义分圆类的一个推广，然后应用推广的广义分圆类构造一类新的跳频序列族，并计算了它们的平均汉明相关值。最后证明了新构造的跳频序列族关于平均汉明相关界是最优的。注意到，当 $d=2n$ 时，此时推广的 Whiteman 广义分圆类等同于 Whiteman 广义分圆类，从而本文的结果推广了文献[12]的结论。

2　预备知识

设 $F=\{f_0,f_1,\L,f_{v-1}\}$ 为频率集，令 U 是 F 上的周期为 L，序列条数为 M 的跳频序列族。U 中的任意 2 条跳频序列 $X=\{x_0,x_1,\L,x_{L-1}\}$，$Y=\{y_0,y_1,\L,y_{L-1}\}$ 的周期汉明相关函数定义为

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

这里

$$h[x_t,y_{t+t}]=\begin{cases}1, & x_t=y_{t+t}\\ 0, & x_t\ne y_{t+t}\end{cases}$$

其中，下标是模 L 运算。若 $X=Y$，$H_{X,X}(t)$ 称为 X 的汉明自相关函数，简记为 $H_X(t)$。X 的最大汉明自相关以及 X 与 Y $(X\ne Y)$ 的最大汉明互相关分别定义为

$$H(X)=\max\nolimits_{1\le t\le L-1}H_X(t)$$

$$H(X,Y)=\max\nolimits_{0\le t\le L-1}H_{X,Y}(t)$$

Lempel 和 Greenberger 在 1974 年给出了 $H(X)$ 的一个下界。

引理 1[3]　设 U 是 F 上周期为 L 的跳频序列，则

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

其中，$|F|=v$，b 是 L 模 v 的非负整数，$\lceil x\rceil$ 表示为大于或等于 x 的最小整数。

对任意给出的一个跳频序列族 U，最大的汉明自相关 $H_a(U)$ 和最大的汉明互相关 $H_c(U)$ 分别定义为

$$H_a(U)=\max\nolimits_{X\in U}H(X)$$

$$H_c(U)=\max\nolimits_{X,Y\in U,X\ne Y}H(X,Y)$$

关于跳频序列族，Peng 和 Fan 在 2004 年给出了如下一个理论界。

引理 2[4]　设 U 是 F 上周期为 L，序列条数为 M 的跳频序列族，$|F|=v$，$I=\left\lfloor\frac{LM}{v}\right\rfloor$，则

$$\begin{cases}(L-1)vH_a(U)+(M-1)LvH_c(U)\ge(LM-v)L,\\ (L-1)MH_a(U)+(M-1)LH_c(U)\ge 2ILM-(I+1)Lv\end{cases} \tag{3}$$

跳频序列族的另外 2 个重要参数平均汉明自相关函数和平均汉明互相关函数分别定义如下：

定义 1[14]　设 U 是 F 上周期为 L，序列条数为 M 的跳频序列族，则分别称

$$S_a(U)=\sum_{X\in U,1\le t\le L-1}H_X(t)$$

$$S_c(U)=\frac{1}{2}\sum_{X,Y\in U,X\ne Y,0\le t\le L-1}H_{X,Y}(t)$$

为 U 的总汉明自相关和汉明互相关。同时分别称

$$A_a(U)=\frac{S_a(U)}{M(L-1)}$$

$$A_c(U)=\frac{2S_c(U)}{LM(M-1)}$$

为 U 的平均汉明自相关和平均汉明互相关。为了简便，本文约定

$$H_a=H_a(U),H_c=H_c(U),S_a=S_a(U),$$

$$S_c=S_c(U),A_a=A_a(U),A_c=A_c(U)$$

最近，Peng 等人给出了 A_a 和 A_c 的如下理论界。

引理 3[15]　设 U 是 F 上的周期为 L，序列条数为 M 的跳频序列族，$|F|=v$，A_a 和 A_c 分别为 U 的平均汉明自相关和平均汉明互相关，则

$$\frac{A_a}{L(M-1)}+\frac{A_c}{L-1}\ge\frac{LM-v}{v(M-1)(L-1)} \tag{4}$$

综上所述，关于跳频序列的最优性，有如下几种判定标准。

1) 对于单条跳频序列 $X\in U$，如果参数 v、L 和 $H(X)$ 使得式 (2) 等式成立，则称 X 是最优的。

2) 对于跳频序列族 U，如果参数 v、L、M、H_c 和 H_c 使得式 (3) 中的任一等式成立，则称 U 关于

最大汉明相关界是最优的。

3) 对于跳频序列族U,如果参数v、L、M、A_a和A_c使得式(4)等式成立,则称U关于平均汉明相关界是最优的。

由式(3)和式(4)易知,如果一个跳频序列集关于最大汉明相关界是最优的,那么它关于平均汉明相关界一定是最优的。但是,平均汉明相关界考虑的是一个序列集的全局性质,此时对一个跳频序列集,即使它关于最大汉明相关界不是最优的,但如果能达到平均汉明界亦是很好的性质[11]。更为重要的是,求平均汉明相关界的直接途径是给出所考虑的序列集的汉明相关值的分布,而一个跳频序列族的汉明相关分布和它对应的循环码的重量分布有密切联系[8],这是需要考虑这一问题的另一个主要原因。

3 广义分圆类及其推广

设p和q是不同的奇素数,$\gcd(p-1,q-1)=2n$,n为整数,根据中国剩余定理,存在p和q的公共本原根,记为g。令x为满足下列同余方程组的整数解:

$$\begin{cases} x=g(\mathrm{mod}p) \\ x=1(\mathrm{mod}q) \end{cases}$$

令$e=(p-1)(q-1)/2n, L=pq$,则Z_L中所有可逆元的集合可表示为

$$Z_L^*=\{g^s x^j : s=0,1,\cdots,e-1,\ j=0,1,\cdots,2n-1\}$$

Whiteman广义分圆类定义如下[16]:

$$D_j'=\{g^s x^j : s=0,1,\cdots,e-1\}, 0\le j\le 2n-1$$

易验证,$Z_L^*=\bigcup_{j=0}^{2n-1} D_j'$。

定义

$$P=\{p,2p,\cdots,(q-1)p\}, Q=\{q,2q,\cdots,(p-1)q\}, R=\{0\}$$

引理4[16] 符号同上,则

$$-1=\begin{cases} g^u x^n(\mathrm{mod}\ L), & (p-1)(q-1)/(2n)^2 \text{为偶数} \\ g^{e/2}(\mathrm{mod}\ L), & (p-1)(q-1)/(2n)^2 \text{为奇数} \end{cases}$$

其中,u是某个给定的整数,且$0\le u\le e-1$。

现在给出Whiteman广义分圆类的一个推广。设$d\mid 2n$,且d为奇素数。定义

$$D_i=\{g^s x^{dt+i} : s=0,1,\cdots,e-1; t=0,1,\cdots,2n/d-1\},\ 0\le i\le d-1$$

很显然,仍然有$Z_L^*=\bigcup_{i=0}^{d-1} D_i$,对于给定的$i$和$j$,$0\le i,j\le d-1$,对应的$d$阶分圆数定义为

$$(i,j)=|(D_i+1)\cap D_j|$$

注意到,如上提出的是基于Whiteman广义分圆类的推广,它不同于Meidl等在文献[13]中提出的分圆类的推广,因为后者是基于Ding-Helleseth广义分圆类的推广。对于新推广的Whiteman广义分圆有如下性质。

性质1 设D_0及(i,j)分别表示如上所定义的推广的Whiteman广义分圆类和分圆数,则:

1) $-1\in D_0$;

2) $(i,j)=(j,i)$;

3) $(i,j)=(d-i,j-i)$。

证明 1) 由$d\mid 2n$,且d为奇素数,可知$d\mid n$,又由引理4可知,$-1\in D_0$。

2)和3)易证。证毕。

性质2 对任一给定的i,$0\le i\le d-1$,有:

$$|(D_i+w)\cap(Q\cup R)|=\begin{cases} 0, & w\in Q \\ \dfrac{p-1}{d}, & w\in P\cup Z_L^* \end{cases} \quad (5)$$

$$|(D_i+w)\cap(P\cup R)|=\begin{cases} 0, & w\in P \\ \dfrac{q-1}{d}, & w\in Q\cup Z_L^* \end{cases} \quad (6)$$

证明 只证式(5)(式(6)可类似证明)。

1) 当$w\in Q$时,结论显然成立。

2) 当$w\in P\cup Z_L^*$时,由$x=1(\mathrm{mod}q)$知,对$0\le s\le e-1, 0\le i\le d-1, 0\le t\le \frac{2n}{d}-1$,元素$z=g^s x^{dt+i}+w\in Q\cup R$,当且仅当

$$g^s+w\equiv 0(\mathrm{mod}\ q)$$

易知,有且只有一个$s_1\in Z_q$使得上述方程成立。因此,可设$s=s_1+k(q-1)$,由$0\le s\le e-1$可知,$0\le k\le \frac{p-1}{2n}-1$,所以对于$z=g^s x^{dt+i}+w\in Q\cup R$总共有

$$\frac{p-1}{2n}\times\frac{2n}{d}=\frac{p-1}{d}$$

个解,即$|(D_i+w)\cap(Q\cup R)|=\frac{p-1}{d}$。证毕。

注1 显然有

$$|(D_i+w)\cap(Q\cup R)|=|((Q\cup R)+w)\cap D_i|$$

$|(D_i+w)\cap(P\cup R)|=|((P\cup R)+w)\cap D_i|$

性质 3

$$\sum_{j=0}^{d-1}(i,j)=\sum_{j=0}^{d-1}(j,i)=\begin{cases}\dfrac{(p-2)(q-2)-1}{d}+1, & i=0(\mathrm{mod}d)\\ \dfrac{(p-2)(q-2)-1}{d}, & i\neq 0(\mathrm{mod}d)\end{cases}$$

证明　根据分圆数的定义，$\sum_{j=0}^{d-1}(i,j)$ 等于方程 $x+1\equiv y(\mathrm{mod}L),\ x\in D_i,\ y\in \cup_{j=0}^{d-1}D_j=Z_L^*$ 的解的个数。易知，D_i 中共有

$$\frac{(p-1)(q-1)}{2n}\times\frac{2n}{d}=\frac{(p-1)(q-1)}{d}$$

个元素。

1) 当 $i\equiv 0(\mathrm{mod}d)$ 时，D_i+1 中与 L 不互素的元素可分为如下 3 种情形。

① 元素能被 L 整除。属于该情形的元素个数为 1。

② 元素能被 p 整除而不能被 L 整除。属于该情形的元素个数为 $\frac{(q-1)}{d}-1$。

③ 元素能被 q 整除而不能被 L 整除。属于该情形的元素个数为 $\frac{(p-1)}{d}-1$。因此，D_i+1 中共有

$$\frac{(p-1)(q-1)}{d}-\left(\frac{(q-1)}{d}-1\right)-\left(\frac{(p-1)}{d}-1\right)-1=\frac{(p-2)(q-2)-1}{d}+1$$

个元素与 L 互素，即

$$\sum_{j=0}^{d-1}(i,j)=\frac{(p-2)(q-2)-1}{d}+1$$

2) 当 $i\neq 0(\mathrm{mod}d)$ 时，D_i+1 中与 L 不互素的元素可分为如下 3 种情形。

① 元素能被 L 整除。属于该情形的元素个数为 0。

② 元素能被 p 整除而不能被 L 整除。属于该情形的元素个数为 $\frac{(q-1)}{d}$。

③ 元素能被 q 整除而不能被 L 整除。属于该情形的元素个数为 $\frac{(p-1)}{d}$。

因此，D_i+1 中共有

$$\frac{(p-1)(q-1)}{d}-\frac{(q-1)}{d}-\frac{(p-1)}{d}=\frac{(p-2)(q-2)-1}{d}$$

个元素与 L 互素，即

$$\sum_{j=0}^{d-1}(i,j)=\frac{(p-2)(q-2)-1}{d}$$

证毕。

性质 4

$$\sum_{i=0}^{d-1}(i,k+i)=\begin{cases}\dfrac{(p-2)(q-2)-1}{d}+1, & k=0(\mathrm{mod}d)\\ \dfrac{(p-2)(q-2)-1}{d}, & k\neq 0(\mathrm{mod}d)\end{cases}$$

证明　由性质 1 中 3)可知，

$$\sum_{i=0}^{d-1}(i,k+i)=\sum_{i=0}^{d-1}(d-i,k)=\sum_{i=0}^{d-1}(i,k)$$

再由性质 3，结论显然成立。证毕。

性质 5　对 $k\in Z_d^*$，有：

$$\sum_{i=0}^{d-1}|(D_i+w)\cap D_i|=\begin{cases}d\cdot\dfrac{p-1}{d}\cdot\left(\dfrac{q-1}{d}-1\right), & w\in P\\ d\cdot\dfrac{q-1}{d}\cdot\left(\dfrac{p-1}{d}-1\right), & w\in Q\\ \dfrac{(p-2)(q-2)-1}{d}+1, & w\in Z_L^*\end{cases}\quad(7)$$

$$\sum_{i=0}^{d-1}|(D_{i+k}+w)\cap D_i|=\begin{cases}d\cdot\dfrac{p-1}{d}\cdot\dfrac{q-1}{d}, & w\in P\cup Q\\ \dfrac{(p-2)(q-2)-1}{d}, & w\in Z_L^*\end{cases}\quad(8)$$

证明　只证式(7)(式(8)可类似证明)。

当 $w\in P$ 时，元素 $z\in(D_i+w)\cap D_i$，此时

$$z=g^{s_1}x^{dt_1+i}=g^{s_2}x^{dt_2+i}+w,$$

$$0\le s_1,s_2\le e-1, 0\le t_1,t_2\le\frac{2n}{d}-1。$$

以下分 2 种情形讨论。

1) 当 $t_1=t_2$ 时，由

$$\begin{cases}x=g(\mathrm{mod}p)\\ x=1(\mathrm{mod}q)\end{cases}$$

可知，$g^{s_1+dt_1+i}=g^{s_2+dt_2+i}(\mathrm{mod}p)$，即 $g^{s_1}=g^{s_2}(\mathrm{mod}p)$。

不妨设 $s_1 = s_2 + m_1(p-1)$，$1 \le m_1 \le \frac{q-1}{2n} - 1$，则有

$$g^{s_2+m_1(p-1)} x^{dt_1+i} = g^{s_2} x^{dt_2+i} + w(\mathrm{mod} pq)$$

即 $g^{s_2} x^{dt_2+i} \left(g^{m_1(p-1)} - 1\right) = w(\mathrm{mod} pq)$。又显然有 $g^{m_1(p-1)} - 1 = 0(\mathrm{mod} p)$，因而，

$$g^{s_2} x^{dt_2+i} \left(g^{m_1(p-1)} - 1\right) \in P$$

由 $g^{s_2} x^{dt_2+i} = g^{s_2} (\mathrm{mod} q)$，设 $s_2 = s_2' + h(q-1)$，$0 \le h \le \frac{p-1}{2n} - 1$，给定一个 h，当 s_2 遍历 $\{h(q-1), h(q-1)+1, \cdots, h(q-1)+q-2\}$ 时，

$$g^{s_2} x^{dt_2+i} = g^{s_2} (\mathrm{mod} q)$$

对应 Z_q^* 中每一个元素恰好均出现一次，也就是 $g^{s_2} x^{dt_2+i} \left(g^{m_1(p-1)} - 1\right)$ 对应 P 中的元素恰好出现一次，所以多重集

$$\left\{ g^{s_2} x^{dt_2+i} \left(g^{m_1(p-1)} - 1\right) : 0 \le s_2 \le e-1, 0 \le t_2 \le \frac{2n}{d} - 1, \right.$$
$$\left. 1 \le m_1 \le \frac{q-1}{2n} - 1 \right\}$$

包含 P 中每一元素的次数为

$$\frac{p-1}{2n} \cdot \frac{2n}{d} \cdot \left(\frac{q-1}{2n} - 1\right) = \frac{p-1}{d} \cdot \left(\frac{q-1}{2n} - 1\right)$$

2) 当 $t_1 \ne t_2$ 时，由

$$\begin{cases} x = g(\mathrm{mod}\, p) \\ x = 1(\mathrm{mod}\, q) \end{cases}$$

可知，$g^{s_1+dt_1+i} \equiv g^{s_2+dt_2+i} (\mathrm{mod}\ p)$，即 $g^{s_1+dt_1} \equiv g^{s_2+dt_2} (\mathrm{mod}\ p)$。假设

$$s_1 + dt_1 = s_2 + dt_2 + m_2(p-1), 0 \le m_2 \le \frac{q-1}{2n} - 1$$

即 $s_1 = s_2 + d(t_2 - t_1) + m_2(p-1)$，则有：

$$g^{s_2+d(t_2-t_1)+m_2(p-1)} x^{dt_1+i} = g^{s_2} x^{dt_2+i} + w(\mathrm{mod}\, pq)$$

即 $g^{s_2} x^{dt_2+i} \left(g^{d(t_2-t_1)+m_2(p-1)} x^{d(t_1-t_2)} - 1\right) = w(\mathrm{mod}\, pq)$。

由 $g^{d(t_2-t_1)+m_2(p-1)} x^{d(t_1-t_2)} - 1 = g^{m_2(p-1)} - 1 = 0(\mathrm{mod}\, p)$，$g^{s_2} x^{dt_2+i} \left(g^{d(t_2-t_1)+m_2(p-1)} x^{d(t_1-t_2)} - 1\right) \in P$。

由 $g^{s_2} x^{dt_2+i} = g^{s_2} (\mathrm{mod}\ q)$，设

$$s_2 = s_2'' + h'(q-1), \quad 0 \le h' \le \frac{p-1}{2n} - 1,$$

给定一个 h'，当 s_2 遍历 $\{h'(q-1), h'(q-1)+1, \cdots, h'(q-1)+q-2\}$ 时，$g^{s_2} x^{dt_2+i} = g^{s_2} (\mathrm{mod}\ q)$ 对应 Z_q^* 中每一个元素恰好均出现一次，也就是 $g^{s_2} x^{dt_2+i} \left(g^{m_2(p-1)} - 1\right)$ 对应 P 中的元素恰好出现一次，所以多重集

$$\left\{ g^{s_2} x^{dt_2+i} \left(g^{d(t_2-t_1)+m_2(p-1)} x^{d(t_1-t_2)} - 1\right) \middle| 0 \le s_2 \le e-1 \right.$$
$$\left. 0 \le t_1 \ne t_2 \le \frac{2n}{d} - 1,\ 0 \le m_2 \le \frac{q-1}{2n} - 1 \right\}$$

包含 P 中每一元素的次数为

$$\frac{p-1}{2n} \cdot \frac{q-1}{2n} \cdot \frac{2n}{d} \cdot \left(\frac{2n}{d} - 1\right) = \frac{p-1}{d} \cdot \left(\frac{q-1}{d} - \frac{q-1}{2n}\right)$$

综合情形 1)和情形 2)，方程 $g^{s_1} x^{dt_1+i} = g^{s_2} x^{dt_2+i} (\mathrm{mod} pq)$ 的解个数为

$$\frac{p-1}{d} \cdot \left(\frac{q-1}{2n} - 1\right) + \frac{p-1}{d} \cdot \left(\frac{q-1}{d} - \frac{q-1}{2n}\right) = \frac{p-1}{d} \cdot \left(\frac{q-1}{d} - 1\right)$$

因此，$\sum_{i=0}^{d-1} |(D_i + w) \cap D_i| = d \cdot \frac{p-1}{d} \cdot \left(\frac{q-1}{d} - 1\right)$。当 $w \in Q$ 时，可类似讨论得到

$$\sum_{i=0}^{d-1} |(D_i + w) \cap D_i| = d \cdot \frac{q-1}{d} \cdot \left(\frac{p-1}{d} - 1\right)$$

最后，当 $w \in D_l$，由定义 $w^{-1} D_i = D_{i-l}$，有：

$$\sum_{i=0}^{d-1} |(D_i + w) \cap D_i| = \sum_{i=0}^{d-1} |(w^{-1} D_i + 1) \cap w^{-1} D_i|$$
$$= \sum_{i=0}^{d-1} |(D_{i-l} + 1) \cap D_{i-l}| = \sum_{i=0}^{d-1} (i, i)$$

由性质 4 可得结论。证毕。

性质 6 对任一给定的 i，$0 \le i \le d-1$，有：

1) $|(D_i + w) \cap R| = \begin{cases} 1, & w \in D_i \\ 0, & w \notin D_i \end{cases}$

2) $|(D_i + w) \cap P| = \begin{cases} 0, & w \in P \\ \frac{q-1}{d} - 1, & w \in D_i \\ \frac{q-1}{d}, & w \in Q \cup (Z_L^*, D_i) \end{cases}$

3) $|(D_i + w) \cap Q| = \begin{cases} 0, & w \in Q \\ \frac{p-1}{d} - 1, & w \in D_i \\ \frac{p-1}{d}, & w \in P \cup (Z_L^*, D_i) \end{cases}$

证明　1) 当 $w \in D_i$ 时，$w^{-1}D_i = D_0$，由性质1可知，$-1 \in D_0$，从而

$$|(D_i + w) \cap R| = |(w^{-1}D_i + 1) \cap R| = |(D_0 + 1) \cap R| = 1$$

当 $w \notin D_i$ 时，结论显然成立。

对 2)及 3)，注意到

$$|(D_i + w) \cap P| = |(D_i + w) \cap (P \cup R)| - |(D_i + w) \cap R|$$

$$|(D_i + w) \cap Q| = |(D_i + w) \cap (Q \cup R)| - |(D_i + w) \cap R|$$

由性质 2 和性质 6 可得结论。证毕。

注 2　显然有：

$$|(D_i + w) \cap P| = |(P + w) \cap D_i|$$

$$|(D_i + w) \cap Q| = |(Q + w) \cap D_i|$$

性质 7[12]

$$|(P + w) \cap (Q \cup R)| = \begin{cases} 0, & w \in Q \\ 1, & w \in P \cup Z_L^* \end{cases}$$

和

$$|(Q + w) \cap (P \cup R)| = \begin{cases} 0, & w \in P \\ 1, & w \in Q \cup Z_L^* \end{cases}$$

注 3　1) 显然有：

$$|(P + w) \cap (Q \cup R)| = |((Q \cup R) + w) \cap P|$$

$$|(Q + w) \cap (P \cup R)| = |((P \cup R) + w) \cap Q|$$

2) 类似地，容易验证

$$|((Q \cup R) + w) \cap (Q \cup R)| = \begin{cases} p, & w \in Q \\ 0, & w \in P \cup Z_L^* \end{cases}$$

$$|(P + w) \cap P| = \begin{cases} q - 2, & w \in P \\ q - 1, & w \in R \\ 0, & w \notin P \cup R \end{cases}$$

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，并利用上一节给出的推广的 Whiteman 广义分圆类的性质给出该跳频序列族的汉明相关值的分布，证明了该类跳频序列族关于平均汉明相关界是最优的。

令

$$C_0 = D_0 \cup P \cup Q \cup R$$

$$C_i = D_i, 1 \le i \le d - 1$$

则有 $\bigcup_{i=0}^{d-1} C_i = Z_L$ 和 $C_i \cap C_j = \varnothing, i \ne j$。

令 $X = \{x_0, x_1, \cdots, x_{L-1}\}$ 是在频率集 $F = \{0, l, \cdots, d-1\}$ 上的周期为 L 的跳频序列，称

$$Supp_x(k) = \{t \mid x_t = k, 0 \le t \le L - 1\}$$

为 $k \in F$ 在序列 X 上的支撑集。

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

$$Supp_{x^{(i)}}(j) = C_{j+i}, 0 \le j \le d - 1$$

这里，$j + i$ 是模 d 运算。

定理 1　令 p 和 q 是不同的奇素数，$\gcd(p-1, q-1) = 2n$，令 $d \mid 2n$，d 为奇素数，则如上定义的跳频序列族 U 满足如下性质。

1) 序列族的大小为 $|U| = d$，序列的周期为 $L = pq$，频率集大小为 $|F| = d$。

2) U 中任意一条跳频序列 $X^{(k)}$ 的汉明相关函数值

$$H_{X^{(k)}}(w) = \begin{cases} \dfrac{(p-1)(q+1)}{d} + q - p + 1, & w \in P \\ \dfrac{(q-1)(p+1)}{d} + p - q + 1, & w \in Q \\ \dfrac{pq-1}{d} + 1, & w \in D_0 \\ \dfrac{pq-1}{d} + 3, & \text{其他} \end{cases}$$

3) U 中任意 2 条不同的跳频序列 $X^{(k)}, X^{(l)}$ 的汉明互相关函数值

$$H_{X^{(k)}, X^{(l)}}(w) = \begin{cases} 0, & w = 0 \\ \dfrac{(p-1)(q+1)}{d}, & w \in P \\ \dfrac{(q-1)(p+1)}{d}, & w \in Q \\ \dfrac{pq-1}{d} - 1, & w \in D_{k-l} \cup D_{l-k} \\ \dfrac{pq-1}{d}, & \text{其他} \end{cases}$$

证明　1) 显然成立。

2) $X^{(k)}$ 在 w 移位的汉明自相关函数为

$$H_{X^{(k)}}(w) = \sum_{i=0}^{d-1} |(D_i + w) \cap D_i| + 2(|(D_0 + w) \cap (P \cup R)| + |(D_0 + w) \cap Q|) + |(P + w) \cap P| + |(P + w) \cap (Q \cup R)| +$$

$(Q \cup R + w) \cap P| + |(Q \cup R + w) \cap (Q \cup R)|$

由性质 2、4、6、7 **可得结论。**

3) **任意不同的** 2 **条跳频序列** $X^{(k)}, X^{(l)} \in U$, $0 \le k \ne l \le d-1$，**在** w **移位的汉明互相关函数为**

$$H_{X^{(k)},X^{(l)}}(w) = \sum_{i=0}^{d-1} |(C_{i+l} + w) \cap C_{i+k}|$$

由 d **是奇素数可知，** $k - l \ne l - k \pmod d$ **，令** $t = l - k$

$$H_{X^{(k)},X^{(l)}}(w) = \sum_{i=0}^{d-1} |(C_{i+l} + w) \cap C_{i+k}|$$

$$= \sum_{i=0}^{d-1} |(C_{i+t} + w) \cap C_i|$$

$$= \sum_{i=0}^{d-1} |(D_{i+t} + w) \cap D_i| + |(D_t + w) \cap (P \cup R)| + |(D_t + w) \cap Q| + |(P \cup R + w) \cap D_{-t}| + |(Q + w) \cap D_{-t}|$$

则由性质 2、5、6 **可得结论。证毕。**

定理 2　跳频序列族 U **的平均汉明自相关和汉明互相关分别为**

$$A_a(U) = \frac{S_a(U)}{M(L-1)}$$

$$= \frac{(pq-1)^2 + (d-1)(p-1)^2 + (d-1)(q-1)^2 + d(pq-1)}{d(pq-1)} \tag{9}$$

$$A_c(U) = \frac{2S_c(U)}{LM(M-1)}$$

$$= \frac{(d-1)(pq-1)^2 - (d-1)(p-1)^2 - (d-1)(q-1)^2}{pqd(d-1)} \tag{10}$$

进一步地，跳频序列族 U **关于平均汉明相关界是最优的。**

证明　由 $S_a(U)$ **和** $S_c(U)$ **的定义可知**

$$S_a(U) = \sum_{0 \le i \le d-1, 1 \le t \le L-1} H_{X^{(i)}}(t)$$

$$= d\{(q-1)(\frac{(p-1)(q+1)}{d} + q - p + 1) +$$

$$(p-1)(\frac{(q-1)(p+1)}{d} + p - q + 1) + \frac{(p-1)(q-1)}{d}$$

$$(\frac{pq-1}{d} + 1) + (d-1)\frac{(p-1)(q-1)}{d}(\frac{pq-1}{d} + 3)\}$$

$$= (pq-1)^2 + (d-1)(p-1)^2 + (d-1)(q-1)^2 + d(pq-1)$$

$$2S_c(U) = \sum_{0 \le i \ne j \le d-1, 0 \le t \le L-1} H_{X^{(i)},X^{(j)}}(t)$$

$$= d(d-1)\left\{(q-1)\frac{(p-1)(q+1)}{d} + (p-1)\frac{(q-1)(p+1)}{d} + 2\frac{(p-1)(q-1)}{d}\left(\frac{pq-1}{d} - 1\right) + (d-2)\frac{(p-1)(q-1)}{d}\frac{pq-1}{d}\right\}$$

$$= (d-1)(pq-1)^2 - (d-1)(p-1)^2 - (d-1)(q-1)^2$$

由平均汉明自相关和平均汉明互相关的定义可得式(9)**和式**(10)**。把式**(9)**和式**(10)**代入式**(4)**可得：**

$$\frac{A_a}{L(M-1)} + \frac{A_c}{L-1} =$$

$$\frac{(pq-1)^2 + (d-1)(p-1)^2 + (d-1)(q-1)^2 + d(pq-1)}{dpq(d-1)(pq-1)} +$$

$$\frac{(d-1)(pq-1)^2 - (d-1)(p-1)^2 - (d-1)(q-1)^2}{dpq(d-1)(pq-1)}$$

$$= \frac{1}{d-1} \ge \frac{LM - v}{v(M-1)(L-1)}$$

其中， $\frac{LM-v}{v(M-1)(L-1)} = \frac{pqd-d}{d(pq-1)(d-1)}$ **。因此，跳频序列族** U **关于平均汉明相关界是最优的。证毕。**

5　结束语

较之达到最大汉明相关界的跳频序列族，具有最优平均汉明相关界的跳频序列族的研究成果要少得多。在文献[12]**的基础上，本文给出了** Whiteman **广义分圆类的一个推广，并且基于推广的** Whiteman **广义分圆类构造了新的跳频序列族，证明了新构造的跳频序列族关于平均汉明相关界是最优的。**

参考文献：

[1] FAN P Z, DAMELL M. Sequence Design for Communications Applications[M]. London: Research Studies Press, 1996.

[2] WIN M Z, SCHOLTZ R A. Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications[J]. IEEE Transactions on Communications, 2002, 48(4):679-691.

[3] LEMPEL A, GREENBERGER H. Families of sequences with optimal Hamming correlation properties[J]. IEEE Transactions on Information Theory, 1974, 20(1): 90-94.

[4] PENG D Y, FAN P Z. Lower bounds on the hamming auto- and cross-correlations of frequency-hopping sequences[J]. IEEE Transac-

tions on Information Theory, 2004, 50(9): 2149-2154.

[5] PENG D Y, *et al*. The average Hamming correlation for the cubic polynomial hopping sequences[A]. IEEE IWCMC 2008, International Conference on Wireless Communications and Mobile Computing[C]. Crete, Greece, 2008. 464-469.

[6] CHU W S, COLBOURN C J. Optimal frequency-hopping sequences via cyclotomy[J]. IEEE Transactions on Information Theory, 2005, 51(3):1139-1141.

[7] KE P H, ZHANG S Y. Frequency-hopping sequences based on d-form functions[J]. The Journal of China University of Posts and Telecommunications, 2010, 17(4): 58-62.

[8] DING C S, YANG Y, TANG X H. Optimal sets of frequency hopping sequences from linear cyclic codes[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3605-3612.

[9] GE G N, MIAO Y, YAO Z X. Optimal frequency hopping sequences: auto- and cross-correlation properties[J]. IEEE Transactions on Information Theory, 2009, 55(2): 867-879.

[10] ZHANG Y, KE P H, ZHANG S Y. Optimal frequency-hopping sequences based on cyclotomy[A]. ETCS 2009, First International Workshop on Education Technology and Computer Science[C]. Wuhan, China, 2009.1122-1126.

[11] **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, PENG D Y. A class of frequency-hopping sequence family with optimal average Hamming correlation property[J]. of Electronics and Information Technology, 2010, 32(5): 1257-1261.

[12] LIU F, *et al*. Construction of frequency hopping sequence set based upon generalized cyclotomy[EB/OL]. http://arxiv.org/abs/1009.3602, 2010.

[13] MEIDL W. Remarks on a cyclotomic sequence[J]. Designs, Codes, and Cryptography, 2009, 51: 33-43.

[14] PENG D Y, PENG T, FAN P Z. Generalized classof cubic frequency-hopping sequences with large family size[J]. IEEE Proceedings on Communications, 2005,152 (6): 897-902.

[15] PENG D Y, *et al*. A class of optimal frequency hopping sequences based upon the theory of power residues[A]. SETA 2008,Proceedings of the 5th International Conference on Sequences and Their Applications[C]. Lexington, KY, USA, 2008. 188-196.

[16] WHITEMAN A L. A family of difference sets[J]. Illinois Journal of Mathematics, 1962, 6: 107-121.

作者简介：

柯品惠（1978-），男，福建建阳人，博士，福建师范大学副教授，主要研究方向为序列设计，现代密码学中的布尔函数。

章海辉（1984-），男，江西九江人，福建师范大学硕士生，主要研究方向为序列设计。

张胜元（1966-），男，福建连城人，福建师范大学教授，主要研究方向为编码密码学、组合数学。