

一类周期为素数倍数的跳频序列族

徐善顶^{1,2}, 曹喜望^{2,3}, 许广魁^{2,4}

(1. 南京工程学院数理部, 江苏南京 211167; 2. 南京航空航天大学数学系, 江苏南京 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, 安徽淮南 232038)

摘 要: 跳频技术具有抗干扰、抗截获、码分多址和频带共享等优点, 在军事无线电通信、民用移动通信、现代雷达和声纳等电子系统中具有重要的应用. 其中跳频序列是跳频系统中不可或缺的一部分. 本文基于有限域上的分圆法和中國剩余定理, 首先构造了一类周期为素数倍数的跳频序列族, 随后利用分圆数的性质导出了此序列族的汉明相关值. 研究表明, 该序列族不仅关于 Peng-Fan 界是最优的, 而且每个序列关于 Lempel-Greenberger 界也是最优(或次最优)的. 另外, 已有的基于分圆法的最优跳频序列构造是本文的特例.

关键词: 分圆; 跳频序列; 汉明相关; Lempel-Greenberger 界; Peng-Fan 界

中图分类号: TN914.43 **文献标识码:** A **文章编号:** 0372-2112 (2015)10-1930-06

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.3969/j.issn.0372-2112.2015.10.008

A Class of Frequency-Hopping Sequences Set with a Multiple of Prime Number Length

XU Shan-ding^{1,2}, CAO Xi-wang^{2,3}, XU Guang-kui^{2,4}

(1. Department of Mathematics and Physics, Nanjing Institute of Technology, Nanjing, Jiangsu 211167, China;

2. School of Mathematical Science, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu 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, Anhui 232038, China)

Abstract: Frequency-hopping spread spectrum (FHSS) systems, with properties of anti-jamming, anti-intercept, code division multiple access (CDMA), channel sharing, etc, are usually applied in military radio communication, mobile communication, modern radar and sonar echolocation systems. Frequency-hopping sequences (FHS) is an integral part of FHSS systems. Based on the cyclotomy over the finite field and the Chinese remainder theorem, a class of FHSs set with a multiple of prime number length is constructed and the Hamming correlations of the new set are derived by some basic properties of the cyclotomic numbers. The results show that the proposed set is optimal with respect to the Peng-Fan bound and each FHS of the set is optimal or near optimal with respect to the Lempel-Greenberger bound. Furthermore, the previous constructions of optimal FHS sets based on cyclotomy are special cases of this paper.

Key words: cyclotomy; frequency-hopping sequence; Hamming correlation; Lempel-Greenberger bound; Peng-Fan bound

1 引言

跳频系统是指收发双方的载波频率按照某种跳频图案在很宽频带范围内跳变的通信收发系统. 与常规通信系统相比, 跳频系统具有抗干扰、抗截获、码分多址和频带共享等优点, 因此常被应用于军事无线电通信、民用移动通信、现代雷达和声纳等电子系统. 其中, 用于控制载波频率跳变的地址码序列称为跳频序列, 它的性能

对跳频系统有重大影响. 为此, 我们采用的跳频序列应满足其非平凡汉明自相关值和汉明交错相关值(定义见下节)尽可能小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的用户. 但是, 跳频序列族的参数受限于一些理论界^[1~3]. 对于跳频序列的设计, 我们比较关心的是满足 Lempel-Greenberger 界^[1]或 Peng-Fan 界^[2]的跳频序列. 目前已有许多编码学者利用代数或组合方法构造出了关于这些界的最优跳频序

列(族),详见文献[1,4~17].

分圆是基础数论的一个古老话题.分圆数和广义分圆数与 Waring 问题、差集、序列、编码理论和密码学关系密切.具体地,Chu 与 Colbourn^[5]利用有限域 $GF(p)$ (p 为素数)上的分圆法设计出达到理论界的最优跳频序列.随后 Chung 与 Yang^[10]对上述构造作了很小的改动得到了更多的跳频序列.通过引进离散对数函数,Ding 与 Yin^[9]把文献[5]中的构造推广到一般的有限域 $GF(p^n)$,借助它的分圆构造了更多具有灵活参数的最优跳频序列族.后来,Han 与 Yang^[11]从 Sidelnikov 序列的观点改进了文献[9]中的构造.最近,Zhang 等^[12,13]利用 $GF(p)$ 与 $GF(2^n)$ 上的分圆设计出新的最优跳频序列,Liu 等^[16]利用 $\mathbf{Z}_{pq}$ 上的广义分圆构造出具有最优汉明相关性能的跳频序列族,而 Ren 等^[17]推广了先前文献[9]与[13]中的构造,得到了更多最优的跳频序列族.基于分圆法和中国剩余定理,本文构造了一类周期为素数倍数的最优跳频序列族.它不仅包含文献[5]与[12]中的构造作为特例,而且通过选择某些特定的参数,我们可以得到许多先前构造无法得到的最优跳频序列族.

2 预备知识

本节首先简单介绍跳频序列的相关知识,随后介绍用于序列构造的有限域上的分圆.

2.1 跳频序列的相关知识

设 $F = \{f_0, f_1, \dots, f_{v-1}\}$ 为字符集, $X = \{x_0, x_1, \dots, x_{L-1}\} (x_i \in F, 0 \leq i < L)$ 称为大小为 v 的字符集 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 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 $X = \{x_0, x_1, \dots, x_{L-1}\} (x_i \in F, 0 \leq i < L)$ 与 $Y = \{y_0, y_1, \dots, y_{L-1}\} (y_i \in F, 0 \leq i < L)$,其(周期)汉明相关函数定义为

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

这里函数 $h[x, y]$ 的定义为:当 $x = y$ 时 $h[x, y] = 1$,否则为 0. 式中,下标 $t + \tau$ 按模 L 运算.若 $X = Y$ 且 $\tau \neq 0$ 时, $H_{X,X}(\tau)$ 称为序列 X 的非平凡汉明自相关,简记为 $H_X(\tau)$.若 $X \neq Y$ 时, $H_{X,Y}(\tau)$ 称为序列 X 与 Y 的汉明交错相关.

对于任意的 $X, Y \in U$ 且 $X \neq Y$, 令 $H(X) = \max_{1 \leq \tau < L} \{H_X(\tau)\}; H(X, Y) = \max_{0 \leq \tau < L} \{H_{X,Y}(\tau)\}$.

本文中,令 (L, v, λ) 表示大小为 v 的字符集 F 上的长度为 L 的一个跳频序列 X 且 $\lambda = H(X)$. 此时称序列 X 具有参数 (L, v, λ) .

Lempel 和 Greenberger 在 1974 年给出了 $H(X)$ 的一

个下界:

引理 1^[1] (Lempel-Greenberger 界) 设 X 是一个 (L, v, λ) 跳频序列,则

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

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.

Lempel-Greenberger 界可写为以下简单形式.

推论 1^[4] 设 X 是一个 (L, v, λ) 跳频序列,则

$$H(X) \geq \lambda_a = \begin{cases} a, & L \neq v \\ 0, & L = v \end{cases} \quad (3)$$

其中 $L = av + b, 0 \leq b < v$.

一个 (L, v, λ) 跳频序列 X 称为最优,如果 $H(X) = \lambda_a$; 一个 (L, v, λ) 跳频序列 X 称为次最优,如果 $H(X) = \lambda_a + 1$.

对于跳频序列族 U ,最大汉明自相关 $H_a(U)$ 、最大汉明交错相关 $H_c(U)$ 以及最大汉明相关 $H(U)$ 定义如下:

$$H_a(U) = \max_{X \in U} \{H(X)\}; H_c(U) = \max_{X, Y \in U, X \neq Y} \{H(X, Y)\}; H(U) = \max \{H_a(U), H_c(U)\}.$$

本文使用 $(L, v, \lambda; M)$ 表示大小为 v 的字符集 F 上的长度为 L 的 M 个跳频序列构成的一个序列族 U 且 $\lambda = H(U)$. 此时称序列族 U 具有参数 $(L, v, \lambda; M)$.

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

引理 2^[2] (Peng-Fan 界) 设 U 是一个 $(L, v, \lambda; M)$ 跳频序列族,则

$$(L-1)vH_a(U) + (M-1)LvH_c(U) \geq (LM-v)L \quad (4)$$

作为 Peng-Fan 界的简单形式以下推论被广泛应用.

推论 2^[2] 设 U 是一个 $(L, v, \lambda; M)$ 跳频序列族,则

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

一个 $(L, v, \lambda; M)$ 跳频序列族 U 称为最优,如果 $H(U)$ 使得式(5)等号成立.

2.2 有限域上的分圆

设 p 是一个素数, n 是一个自然数,定义 $q = p^n = ef + 1$, 其中 $e > 1$. 我们知道存在唯一一个含有 q 个元素的有限域 $G = GF(q)$, 其中 $GF(q)^*$ 表示 G 的所有非零元的集合. 令 α 是 G 的一个本原元,则有限域 G 的 e 阶分圆类有如下定义: $C_i = \{\alpha^{es+i} : s = 0, 1, \dots, f-1\}, 0 \leq i < e$.

对于正整数 $L, \mathbf{Z}_L = \{0, 1, \dots, L-1\}$ 表示模 L 的剩

余类环. 设 $a \in \mathbf{Z}_L, H \subseteq \mathbf{Z}_L$, 定义:

$$H + a = \{h + a; h \in H\}, \quad a \cdot H = \{ah; h \in H\}.$$

对于固定的 i 和 j 且 $0 \leq i, j < e$, 定义阶为 e 的分圆数为: $|(i, j) = |(C_i + 1) \cap C_j|$.

引理 3^[18] 上面定义的分圆数具有以下基本性质:

$$(1) \alpha^i C_j = C_{i+j}, 0 \leq i, j < e;$$

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

$$(3) \sum_{i=0}^{e-1} (i, j) = f - \eta_j, \text{ 当 } j = 0 \text{ 时 } \eta_j = 1, \text{ 否则 } \eta_j = 0;$$

$$(4) \sum_{i=0}^{e-1} (k + i, i) = f - \eta_k, \text{ 当 } k = 0 \text{ 时 } \eta_k = 1, \text{ 否则 } \eta_k = 0.$$

为求解下节所构造的跳频序列的汉明相关函数, 下面我们将给出一个重要的引理.

引理 4 对于任意的 $k \in \mathbf{Z}_e \setminus \{0\}$ 和任意的 $\omega \in \text{GF}(q)^*$, 我们有

$$(1) \sum_{i=0}^{e-1} |(C_i + \omega) \cap C_i| = f - 1;$$

$$(2) \sum_{i=0}^{e-1} |(C_{i+k} + \omega) \cap C_i| = f.$$

证明 (1) 对于任意的 $\omega \in C_j$, 不妨令 $\omega = \alpha^{e s_1 + j} (0 \leq s_1 < f)$. 求解 $|(C_i + \omega) \cap C_i|$ 等价于研究下面同余式在固定 s_1 时解 $s_2, s_3 (0 \leq s_2, s_3 < f)$ 的个数. 因为 $\alpha^{e s_2 + i} + \alpha^{e s_1 + j} = \alpha^{e s_3 + i}$ 等价于 $\alpha^{e(s_2 - s_1) + (i - j)} + 1 = \alpha^{e(s_3 - s_1) + (i - j)}$, 所以 $|(C_i + \omega) \cap C_i| = (i - j, i - j)$. 从而由引理 3 可得 $\sum_{i=0}^{e-1} |(C_i + \omega) \cap C_i| = \sum_{i=0}^{e-1} (i - j, i - j) = f - 1$.

$$(2) \text{ 对于任意的 } \omega \in C_j, \text{ 同理可得 } \sum_{i=0}^{e-1} |(C_{i+k} + \omega) \cap C_i| = \sum_{i=0}^{e-1} (k + i - j, i - j) = f.$$

3 新的跳频序列(族)的构造

本节中, 首先利用有限域上的分圆法和中国剩余定理给出了一类最优跳频序列(族)的代数构造. 随后说明本节构造不仅包含文献[5]与[12]中的构造作为特例, 而且可以产生具有新参数的最优跳频序列(族).

从现在起, 我们总是假设 p 是一个素数且 $p = ef + 1 (e > 1)$, $\{C_i; 0 \leq i < e\}$ 是有限域 $\text{GF}(p)$ 的 e 阶分圆类, 而 n 是一个正整数且 n 不能被 p 整除. 令 $X = \{x_0, x_1, \dots, x_{L-1}\}$ 是 F 上的长度为 L 的跳频序列, 那么称 $\text{Supp}_X(m) = \{t; x_t = m, 0 \leq t < L\}$ 为元素 $m \in F$ 在序列 X 中的支撑集. 若 $L = np$, 则由 n 不能被 p 整除与中国剩余定理可知 $\mathbf{Z}_{np}$ 同构于 $\mathbf{Z}_n \times \mathbf{Z}_p$, 即对于任意的整数 $t (0 \leq t < np)$ 都有唯一的表示 $t = (t_1, t_2)$, 其中 $t_1 = \langle t \rangle_n, t_2$

$= \langle t \rangle_p$. 从而在此一一对应下有

$$\text{Supp}_X(m) = \{(t_1, t_2); x_{(t_1, t_2)} = m, (t_1, t_2) \in \mathbf{Z}_n \times \mathbf{Z}_p\} \quad (6)$$

定义 1 设 $p, e, n, C_i (0 \leq i < e)$ 定义同上, 函数 g 是 $\mathbf{Z}_n$ 到 $\mathbf{Z}_e$ 的一个单射. 对于 $0 \leq i, k < e$, 令 $E_i^k = \alpha^k C_i$. 定义 $\mathbf{Z}_{e+1}$ 上长度为 np 的一个跳频序列 X , 其中

$$\text{Supp}_X(e) = \bigcup_{j=0}^{n-1} [\{j\} \times \{0\}]; \quad \text{Supp}_X(i) = \bigcup_{j=0}^{n-1} [\{j\} \times E_i^{g(j)}], 0 \leq i < e.$$

下面给出跳频序列 X 的汉明自相关特性.

定理 1 当 $n = 1$ 时, 如上定义的序列 X 具有参数 $(p, e + 1, f - 1)$; 当 $n \neq 1$ 时, 序列 X 具有参数 $(np, e + 1, nf)$. 此外, 当 $n = 1, f \leq e + 2$ 或者 $n \neq 1, f = 1$ 时, X 为最优的; 当 $n \neq 1, e + 1 \geq n(f - 1)$ 且 $f \geq 2$ 时, X 为次最优的.

证明 由中国剩余定理可得, 对于 $\forall \tau \in \mathbf{Z}_{np}$, 可记 $\tau = (\tau_1, \tau_2) \in \mathbf{Z}_n \times \mathbf{Z}_p$. 当 $\tau \neq 0$ 时, 有

$$\begin{aligned} H_X(\tau) &= \sum_{i=0}^e \left| \{0 \leq t < np; x_t = x_{t+\tau} = i\} \right| \\ &= \left| \bigcup_{j=0}^{n-1} [\{j\} \times \{0\}] \cap \bigcup_{j=0}^{n-1} [\{j + \tau_1\} \times \{\tau_2\}] \right| \\ &\quad + \sum_{i=0}^{e-1} \left| \bigcup_{j=0}^{n-1} [\{j\} \times E_i^{g(j)}] \cap \bigcup_{j=0}^{n-1} [\{j + \tau_1\} \times (E_i^{g(j)} + \tau_2)] \right| \\ &= n \cdot |\{0\} \cap \{\tau_2\}| \\ &\quad + \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} |E_i^{g(j)} \cap (E_i^{g(j-\tau_1)} + \tau_2)| \end{aligned} \quad (7)$$

为计算 X 的非平凡汉明自相关, 下面我们分三种情况讨论:

情况 1: 当 $\tau_1 = 0, \tau_2 \neq 0$ 时, 由引理 4 得

$$\begin{aligned} \text{式 (7)} &= \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} |C_{i+g(j)} \cap (C_{i+g(j)} + \tau_2)| = n \cdot \\ &\sum_{i=0}^{e-1} |C_i \cap (C_i + \tau_2)| = n(f - 1); \end{aligned}$$

情况 2: 当 $\tau_1 \neq 0, \tau_2 = 0$ 时, 由 g 是单射得

$$\text{式 (7)} = n + \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} |C_{i+g(j)} \cap C_{i+g(j-\tau_1)}| = n;$$

情况 3: 当 $\tau_1 \neq 0, \tau_2 \neq 0$ 时, 由 g 是单射和引理 4 得

$$\begin{aligned} \text{式 (7)} &= \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} |C_{i+g(j)} \cap (C_{i+g(j-\tau_1)} + \tau_2)| = \\ &\sum_{j=0}^{n-1} \sum_{i=0}^{e-1} |C_i \cap (C_{i+g(j-\tau_1)-g(j)} + \tau_2)| = nf. \end{aligned}$$

注意当 $n = 1$ 时, 情况 2 与情况 3 皆不存在. 因此, 当 $n = 1$ 时 $H(X) = f - 1$, 当 $n \neq 1$ 时 $H(X) = nf$. 此外, 当 $n = 1$ 时, 易见 $L = p = ef + 1 = (f - 1)(e + 1) + e - f + 2$; 从而由推论 1 可知当 $f \leq e + 2$ 时序列 X 为最优的. 当 $n \neq 1$ 时, 我们有 $L = np = n(ef + 1) = nf(e + 1) - n(f - 1) = (nf - 1)(e + 1) + (e + 1) - n(f - 1)$; 从而由

推论 1 可得其余结论.

定义 2 设 $p, e, n, C_i, E_i^k (0 \leq i, k < e)$ 定义同上, 而常数 $M = \lfloor e/n \rfloor \geq 1$. 令函数 g 是 $\mathbf{Z}_n \times \mathbf{Z}_M$ 到 $\mathbf{Z}_e$ 的一个二元单射, 定义 $\mathbf{Z}_{e+1}$ 上长度为 np 的一个跳频序列族 $U = \{X^{(s)} : s = 0, 1, \dots, M-1\}$, 其中 $X^{(s)} = \{x_0^{(s)}, x_1^{(s)}, \dots, x_{np-1}^{(s)}\}$ 的支撑集为

$$\text{Supp}_{X^{(s)}}(e) = \bigcup_{j=0}^{n-1} [\{j\} \times \{0\}]; \text{Supp}_{X^{(s)}}(i) = \bigcup_{j=0}^{n-1} [\{j\} \times E_i^{g(j,s)}], 0 \leq i < e.$$

下面研究跳频序列族 U 的汉明相关性质.

定理 2 如上定义的序列族 U 具有参数 $(np, e+1, nf; \lfloor e/n \rfloor)$. 当 $e \geq nf$ 时, 序列族 U 关于 Peng-Fan 界是最优的. 此外, 当 $n=1, f \leq e+2$ 或者 $n \neq 1, f=1$ 时, 序列 $X^{(s)} (0 \leq s < M)$ 皆为最优的; 当 $n \neq 1, e+1 \geq n(f-1)$ 且 $f \geq 2$ 时, 序列 $X^{(s)} (0 \leq s < M)$ 皆为次最优的.

证明 与定理 1 证明类似, 我们很容易证得当 $n=1$ 时, 序列 $X^{(s)} (0 \leq s < M)$ 具有参数 $(p, e+1, f-1)$; 当 $n \neq 1$ 时, 序列 $X^{(s)} (0 \leq s < M)$ 具有参数 $(np, e+1, nf)$. 因此, 当 $n=1, f \leq e+2$ 或者 $n \neq 1, f=1$ 时, $X^{(s)} (0 \leq s < M)$ 皆为最优的; 当 $n \neq 1, e+1 \geq n(f-1)$ 且 $f \geq 2$ 时, $X^{(s)} (0 \leq s < M)$ 皆为次最优的.

下面研究跳频序列族 U 中任意两个不同序列之间的汉明交错相关. 对于 $\forall \tau \in \mathbf{Z}_{np}$, 可记 $\tau = (\tau_1, \tau_2) \in \mathbf{Z}_n \times \mathbf{Z}_p$. 令 $X^{(s)}$ 与 $X^{(r)}$ 是跳频序列族 U 中两个不同的序列, 则有 $0 \leq s \neq r < M$ 且

$$\begin{aligned} H_{X^{(s)}, X^{(r)}}(\tau) &= \sum_{i=0}^e \left| \{0 \leq t < np : x_t^{(s)} = x_{t+\tau}^{(r)} = i\} \right| \\ &= \left| \bigcup_{j=0}^{n-1} [\{j\} \times \{0\}] \cap \bigcup_{j=0}^{n-1} [\{j+\tau_1\} \times \{\tau_2\}] \right| \\ &\quad + \sum_{i=0}^{e-1} \left| \bigcup_{j=0}^{n-1} [\{j\} \times E_i^{g(j,s)}] \cap \bigcup_{j=0}^{n-1} [\{j+\tau_1\} \times (E_i^{g(j,s)} + \tau_2)] \right| \\ &= n \cdot |\{0\} \cap \{\tau_2\}| + \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| E_i^{g(j,r)} \cap (E_i^{g(j-\tau_1,s)} + \tau_2) \right| \end{aligned} \tag{8}$$

为计算序列 $X^{(s)}$ 与 $X^{(r)}$ 的汉明交错相关, 下面我们分四种情况讨论:

情况 1: 当 $\tau_1=0, \tau_2=0$ 时, 由 g 是二元单射和 $r \neq s$ 得 式(8) $= n + \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| E_i^{g(j,r)} \cap E_i^{g(j,s)} \right| = n$;

情况 2: 当 $\tau_1=0, \tau_2 \neq 0$ 时, 由 g 是二元单射和引理 4 得

$$\begin{aligned} \text{式(8)} &= \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| C_{i+g(j,r)} \cap (C_{i+g(j,s)} + \tau_2) \right| = \\ &\sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| C_i \cap (C_{i+g(j,s)-g(j,r)} + \tau_2) \right| = nf; \end{aligned}$$

情况 3: 当 $\tau_1 \neq 0, \tau_2=0$ 时, 由 g 是二元单射得 式(8) $= n + \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| E_i^{g(j,r)} \cap E_i^{g(j-\tau_1,s)} \right| = n$;

情况 4: 当 $\tau_1 \neq 0, \tau_2 \neq 0$ 时, 由 g 是二元单射和引理 4 得

$$\begin{aligned} \text{式(8)} &= \sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| C_{i+g(j,r)} \cap (C_{i+g(j-\tau_1,s)} + \tau_2) \right| = \\ &\sum_{j=0}^{n-1} \sum_{i=0}^{e-1} \left| C_i \cap (C_{i+g(j-\tau_1,s)-g(j,r)} + \tau_2) \right| = nf. \end{aligned}$$

注意当 $n=1$ 时, 情况 3 与情况 4 皆不存在. 综合情况 1~4, 易见 $H(X^{(s)}, X^{(r)}) = nf$. 从而 $H(U) = nf$. 因此序列族 U 具有参数 $(np, e+1, nf; \lfloor e/n \rfloor)$.

最后我们证明序列族 U 关于 Peng-Fan 界是最优的. 由 Peng-Fan 界可得

$$\left\lceil \frac{(LM-v)L}{(LM-1)v} \right\rceil = \left\lceil nf - n \cdot \frac{npMf + e^2f + e + 1 - npM - f}{(npM-1)(e+1)} \right\rceil \tag{9}$$

因为 $M = \lfloor e/n \rfloor$, 所以当 $e \geq nf$ 时显然有 $0 < n \cdot \frac{npMf + e^2f + e + 1 - npM - f}{(npM-1)(e+1)} < 1$; 从而由推论 2 可得此跳频序列族 U 关于 Peng-Fan 界是最优的.

以下将给出本节构造与已知相关构造的比较, 其中(1)与(2)指出本节构造包含文献[5]与[12]中的构造作为特例. 在此之前, 我们列出它们的最优构造参数, 见表 1.

文献	L	v	M	λ	限制	L - G 界	P - F 界
[5]	p	$e+1$	e	f	$2 \leq f \leq e+2$	最优	最优
[12]	$2p$	$e+1$	$\lfloor e/2 \rfloor$	f	$2 \leq f < (e+9)/6$	次最优	最优
[9]	$p-1$	$e+1$	e	f	$f \leq e-1$	最优	最优
[17]	$n(p-1)$	$e+1$	$\lfloor e/n \rfloor$	nf	$\gcd(n, ef) = 1, n(f+1) \leq e$	次最优	最优
定理 2	np	$e+1$	$\lfloor e/n \rfloor$	nf	$nf \leq e$	$n=1$ 或 $n \neq 1, f=1$ 最优, 其余次最优	最优

(1)Chu 与 Colbourn^[5]由 $\text{GF}(p)$ 上的分圆构造了单个最优 $(p, e+1, f)$ 跳频序列和一类最优 $(p, e+1, f; e)$ 跳频序列族. 通过我们的方法, 文献[5]中构造 2 (即定理 2) 等价于本节定理 1 中 $n=1, g(0)=0$ 时的构造, 文

献[5]中构造 3 (即引理 5) 等价于本节定理 2 中 $n=1, g(0, s) = s (0 \leq s < e)$ 时的简单构造.

(2)Zhang 与 Ke^[12]由 $\text{GF}(p)$ 上的分圆构造了单个最优 $(2p, e+1, 2f)$ 跳频序列和一类最优 $(2p, e+1, 2f;$

- Liu Fang, Peng Dai-yuan, Fan Jia, Tang Xiao-hu. A new class of frequency-hopping sequences with optimal Hamming autocorrelation[J]. Acta Electronica Sinica, 2013, 41(1): 13 – 17.
- [7] Ge G N, Fuji-Hara R, Miao Y. Further combinatorial constructions for optimal frequency-hopping sequences[J]. Journal of Combinatorial Theory, Series A, 2006, 113(8): 1699 – 1718.
- [8] Ding C S, Moisio M J, Yuan J. Algebraic constructions of optimal frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2007, 53(7): 2606 – 2610.
- [9] Ding C S, Yin J. Sets of optimal frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2008, 54(8): 3741 – 3745.
- [10] Chung J H, Han Y K, Yang K. New classes of optimal frequency-hopping sequences by interleaving techniques[J]. IEEE Transactions on Information Theory, 2009, 55(12): 5783 – 5791.
- [11] Han Y K, Yang K. On the Sidelnikov sequences as frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2009, 55(9): 4279 – 4285.
- [12] 张云, 柯品惠, 张胜元. 基于分圆类的最优跳频序列族[J]. 福建师范大学学报: 自然科学版, 2009, 25(2): 1 – 5.
Zhang Yun, Ke Pin-hui, Zhang Sheng-yuan. Optimal frequency-hopping sequences based on cyclotomy[J]. Journal of Fujian Normal University: Natural Science Edition, 2009, 25(2): 1 – 5.
- [13] 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: IEEE, 2009. 1122 – 1126.
- [14] Zhou Z C, Tang X H, Peng D Y, Parampalli U. New constructions for optimal sets of frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2011, 57(6): 3831 – 3840.
- [15] Zhou Z C, Tang X H, Niu X H, Parampalli U. New classes of frequency-hopping sequences with optimal partial correlation[J]. IEEE Transactions on Information Theory, 2012, 58(1): 453 – 458.
- [16] Liu F, Peng D Y, Zhou Z C. A new frequency-hopping sequence set based upon generalized cyclotomy[J]. Designs, Codes and Cryptography, 2012, 69(2): 247 – 259.
- [17] Ren W L, Fu F W, Zhou Z C. New sets of frequency-hopping sequences with optimal Hamming correlation[J]. Designs, Codes and Cryptography, 2014, 72(2): 423 – 434.
- [18] Storer T. Cyclotomy and Difference Sets[M]. Chicago: Markham Publishing Company, 1967.

作者简介



徐善顶 男, 1979 年 11 月出生于山东省兖州市. 现为南京航空航天大学数学系博士研究生. 主要研究方向为代数编码及信息安全.
E-mail: sdxzx11@163.com



曹喜望 男, 1965 年 06 月出生于湖北省麻城市. 现为南京航空航天大学教授、博士生导师. 主要研究方向为代数组合论, 代数密码学.
E-mail: xwcao@nuaa.edu.cn