·计算机与信息技术·

基于分圆理论和中国剩余定理的最优平均汉明相关跳频序列集构造

蔡红斌, 牛宪华*, 张秀杰
(西华大学计算机与软件工程学院, 四川 成都 610039)

摘　要：在跳频通信系统中, 跳频序列的性能对整个跳频通信系统有着决定性的影响。设计出满足理论界要求的跳频序列集是研究跳频通信系统的关键内容。平均汉明相关值是衡量跳频序列性能优劣的重要指标。文章首先根据环上分圆的性质选取基序列, 然后基于分圆理论和中国剩余定理, 扩展序列构造了一类具有灵活参数的跳频序列集, 并证明了所得到的跳频序列集关于平均汉明相关理论界最优。

关键词：跳频通信; 跳频序列集; 平均汉明相关; 中国剩余定理; 分圆理论

中图分类号：TN914.41　　**文献标志码**：A　　**文章编号**：1673–159X(2021)01 − 0027 − 07

doi:10.12198/j.issn.1673 − 159X.3689

Construction of Frequency-Hopping Sequence Sets with Optimal Average Hamming Correlation Based on Cyclotomy and Chinese Remainder Theorem

CAI Hongbin, NIU Xianhua*, ZHANG Xiujie
(*School of Computer and Software Engineering*, *Xihua University*, *Chengdu* 610039 *China*)

Abstract: In frequency hopping communication system, frequency hopping sequences have a decisive influence on the entire frequency hopping communication system. Constructing a set of frequency hopping sequences that meet the requirements of the theoretical bound is the key content of researching frequency hopping communication systems. The average Hamming correlation is used to measure the average error of the frequency hopping communication system. In this paper, we first choose a basis sequence based on cyclotomy and then a set of frequency hopping sequences is constructed based on cyclotomy and the Chinese

收稿日期:2020 − 08 − 29

基金项目:国家自然科学基金项目(61401369); 中国博士后基金项目(2019M663475); 教育部春晖计划 2018 项目; 四川省青年科技基金项目(2017JQ0059)。

第一作者:蔡红斌(1994—), 男, 硕士, 主要研究方向为跳频序列分析与设计。
ORCID: 0000 − 0003 − 3371 − 140X　　E-mail: 1284591798@qq.com

*** 通信作者**:牛宪华(1983—), 女, 教授, 博士, 主要研究方向跳频序列分析与设计、信息安全。
ORCID: 0000 − 0003 − 0980 − 08770　　E-mail: rurustef1212@gmail.com

引用格式:蔡红斌, 牛宪华, 张秀杰. 基于分圆理论和中国剩余定理的最优平均汉明相关跳频序列集构造[J]. 西华大学学报(自然科学版), 2021, 40(1): 27 − 33.

CAI Hongbin, NIU Xianhua, ZHANG Xiujie. Construction of Frequency-Hopping Sequence Sets with Optimal Average Hamming Correlation Based on Cyclotomy and Chinese Remainder Theorem[J]. Journal of Xihua University(Natural Science Edition), 2021, 40(1): 27 − 33.

remainder theorem in the finite field. The results show that the proposed set with more flexible parameters is optimal with respect to the average Hamming correlation.

Keywords: frequency hopping communication; frequency-hopping sequence set; average Hamming correlation; Chinese remainder theorem; cyclotomy

跳频通信系统的收发双方利用载波跳变实现频谱扩展。跳频系统因具有抗干扰能力优异、截获率低、抗衰落能力强等优点被广泛应用于无线电通信、现代雷达、声纳等电子系统[1]。在跳频通信系统中,控制载波频率跳变的伪随机码称为跳频序列。跳频序列的优劣对跳频系统的性能有着决定性的影响。跳频序列包含一些重要参数,如跳频序列集的频隙个数、周期长度、序列数目、序列的平均(最大)汉明自(互)相关值。通常要求跳频序列集具有如下特点: 1) 平均(最大)汉明自(互)相关值要尽可能低; 2) 序列数目尽可能多; 3) 各个频隙点出现的次数尽可能均匀; 4) 具有良好的随机性和较大的线性复杂度; 5) 易于实现。

跳频序列集的各参数之间相互约束,跳频序列理论界给出了不同参数之间应满足的约束关系。目前关于跳频序列理论界的研究已经取得了丰富的成果[2-5]。Lempel 等[2] 给出单条跳频序列最大汉明自相关理论界; Peng 等[3] 推导了跳频序列集最大汉明相关理论界。上述 2 个理论界为构造最大汉明相关最优的跳频序列设计提供了理论基础。Peng 等[4] 指出跳频序列的平均汉明相关可以衡量跳频通信系统的平均误差,更利于评价系统性能,并推导了平均汉明相关的理论界,然后基于多项式方法构造了一类满足平均汉明相关理论界的最优跳频序列集。Han 等[6] 利用交织技术构造了一类满足平均相关理论界最优的跳频序列集。

分圆理论是构造最优跳频序列的有效工具。Chu 等[7] 基于有限域 F_p 上的分圆理论得到了一类满足 Peng-Fan 界最优的跳频序列集。Ding 等[8] 基于有限域F_{p^n}上的分圆,得到了一类具有新参数的最优跳频序列集。刘方等[9] 基于广义分圆理论构造了一类满足平均汉明相关理论界最优的跳频序列集。柯品惠等[10] 推广了广义分圆理论并构造了一类满足平均汉明相关理论界最优的跳频序列集。Zeng 等[11] 基于环上的分圆,给出了一类具有灵活参数的跳频序列集。Xu 等[12] 在文献 [11] 的基础上给出了一类最优跳频序列集的扩展构造。

本文基于分圆理论和中国剩余定理,构造了一类具有新参数的最优平均汉明相关跳频序列集,即根据中国剩余定理在文献 [11] 的基础上,得到一类序列长度更长且满足 Peng-Liu-Tang 界的最优平均汉明相关跳频序列集。

1 预备知识

首先介绍本文中主要用到的一些符号。

1) $\lfloor a \rfloor$: 不大于 a 的最大整数。

2) $\lceil a \rceil$: 不小于 a 的最小整数。

3) v: $v=\prod_{i=1}^{k} p_i^{m_i}$, p_i 为素数,其中 $2<p_1<p_2<\cdots<p_k$, m_i 是任意正整数。

4) (N, l, λ): 在大小为 l 的频隙集 F 上,序列长度为 N 且最大汉明自相关值是 λ 的跳频序列。

5) $(N, l, \lambda; M)$: 在大小为 l 的频隙集 F 上,序列长度为 N,序列数目为 M,且最大汉明互相关值是 λ 的跳频序列集。

6) $Z_v=\{0, 1, 2, \cdots, v\text{-}1\}$: 一个有 v 个元素的模 v 剩余类环。

7) q: $q=p^n$, p 为任意奇素数。

8) $\langle t \rangle_n$: t 模 n 的最小非负剩余。

9) F_q: q 元有限域。

10) F_q^*: F_q 中所有非零元的集合。

1.1 跳频序列基本概念

令 F 是一个大小为 l 的频隙集, S 是定义在频隙集 F 上,长度为 N 的 M 条跳频序列构成的跳频序列集。对于 S 内任意 2 条跳频序列 $\boldsymbol{x}^i=\{x^i(0), x^i(1), \cdots, x^i(N-1)\}$和$\boldsymbol{x}^j=\{x^j(0), x^j(0), \cdots, x^j(N-1)\}$, $0 \leqslant i, j \leqslant M-1$,在时延为 τ 时,其周期汉明相关函数定义为

$$H_{\boldsymbol{x}^i\boldsymbol{x}^j}(\tau)=\sum_{r=0}^{N-1}h(x_r^i,x_{r+\tau}^j),\ 0\leqslant\tau<N$$

其中当 $a=b$ 时, $h(a,b)=1$, 否则, $h(a,b)=0$。下标 $r+\tau$ 按模 N 运算。

对所有 $0\leqslant r<N$, 若 $x_r^i=x_r^j$, 则 $\boldsymbol{x}^i=\boldsymbol{x}^j$, 否则 $\boldsymbol{x}^i\neq\boldsymbol{x}^j$; 若 $\boldsymbol{x}^i=\boldsymbol{x}^j$, 这种情况下称 $H_{\boldsymbol{x}^i\boldsymbol{x}^j}(\tau)$ 为序列的汉明自相关函数; 若 $\boldsymbol{x}^i\neq\boldsymbol{x}^j$, 则称 $H_{\boldsymbol{x}^i\boldsymbol{x}^j}(\tau)$ 为序列集 S 的汉明互相关函数。跳频序列集 S 的最大汉明自相关 $H_a(S)$、最大汉明互相关 $H_c(S)$ 和最大汉明相关 $H(S)$ 定义为:

$$H_a(S)=\max_{\boldsymbol{x}^i,\boldsymbol{x}^j\in S}\{\{H_{\boldsymbol{x}^i\boldsymbol{x}^j}(\tau)\}|1\leqslant\tau<N\}$$
$$H_c(S)=\max_{\boldsymbol{x}^i,\boldsymbol{x}^j\in S,\boldsymbol{x}^i\neq\boldsymbol{x}^j}\{\{H_{\boldsymbol{x}^i\boldsymbol{x}^j}(\tau)|0\leqslant\tau<N\}$$
$$H(S)=\max\{H_a(S),H_c(S)\}$$

简记: $\lambda_a=H_a(S)$, $\lambda_c=H_c(S)$, $\lambda=H(S)$。

理论界是评价跳频序列(集)优劣性的一个重要指标, 对序列设计起指导作用。

1974 年, Lempel 和 Greenberger 给出了跳频序列周期汉明自相关理论界。

引理 1[2] **(Lempel-Greenberger 界)**　对于一个定义在大小为 l 频隙集 F 上, 长度为 N 的跳频序列 X, 其最大汉明自相关满足

$$H(X)\geqslant\left\lceil\frac{(N-\varepsilon)(N+\varepsilon-l)}{l(N-1)}\right\rceil\qquad(1)$$

其中 ε 是 N 模 l 的最小非负剩余。

如果一个 (N,l,λ) 跳频序列 X 的最大汉明自相关满足不等式 (1) 的最小整数解, 则称其为最优跳频序列。

2004 年, Peng 和 Fan 给出了跳频序列集最大汉明相关理论界。

引理 2[3] **(Peng-Fan 界)**　设 F 是一个大小为 l 的频隙集, 对于一个定义在频隙集 F 上的 M 个长度为 N 的跳频序列构成的跳频序列集 S, 其最大汉明相关满足

$$H(S)\geqslant\left\lceil\frac{(NM-l)N}{(NM-1)l}\right\rceil\qquad(2)$$

如果跳频序列集 S 的最大汉明相关是不等式 (2) 的最小整数解, 则该跳频序列集可以被称作最优跳频序列集。

作为衡量跳频序列集性能的重要参数, 跳频序列平均汉明自相关和平均汉明互相关的定义在 2010 年 Peng 等[4] 给出。

定义 1[6]　设 F 是一个大小为 l 的频隙集, 对于一个定义在频隙集 F 上的 M 个长度为 N 的跳频序列构成的跳频序列集 S 有

$$S_a(S)=\sum_{0\leqslant i\leqslant M-1,1\leqslant\tau<N-1}H_{\boldsymbol{x}^i}(\tau)$$
$$S_c(S)=\frac{1}{2}\sum_{0\leqslant i\neq j\leqslant M-1,1\leqslant\tau\leqslant N-1}H_{\boldsymbol{x}^i\boldsymbol{x}^j}(\tau)$$

它们分别是序列集 S 的汉明自相关的总和、汉明互相关的总和。序列集 S 的平均汉明自相关和互相关分别是:

$$A_a(S)=\frac{S_a(S)}{M(N-1)}$$
$$A_c(S)=\frac{2S_c(S)}{NM(M-1)}$$

引理 3[4]　设 F 是一个大小为 l 的频隙集, 对于一个定义在频隙集 F 上的 M 个长度为 N 的跳频序列构成的跳频序列集 S, 则有不等式

$$\frac{A_a}{N(M-1)}+\frac{A_c}{(N-1)}\geqslant\frac{NM-l}{l(M-1)(N-1)}\qquad(3)$$

式中 A_a 和 A_c 分别是序列集 S 的平均汉明自相关和平均汉明互相关。如果跳频序列集 S 的平均汉明相关值满足不等式 (3) 的等号成立, 则该跳频序列集可以被称为满足平均最优的跳频序列集。

推论 1　设 F 是一个大小为 l 的频隙集, 对于一个定义在频隙集 F 上的长度为 N 的跳频序列 X, 有

$$A_a\geqslant\frac{(N-\varepsilon)(N+\varepsilon-l)}{l(N-1)}$$

推论 1 的结果可以由文献 [2] 中引理 4 得出。

1.2　有限域上的分圆

2008 年 Ding 等[8] 给出了有限域 F_q 上的分圆, 本节将简单介绍有限域上的分圆理论。设 $q=p^n=ef+1$, 其中 p 是一个素数, n 是一个正整数, $e>1$。设 α 是 F_q 的一个本原根, 则 F_q^* 可划分为一个 e 阶分圆类, 该分圆类定义为

$$C_i=\{\alpha^{es+i}|s=0,1,2,\cdots,f-1\},\ 0\leqslant i<e$$

设对于正整数 N, 模 N 剩余类环 $Z_N=\{0,1,2,\cdots,N-1\}$。对于 $a\in Z_N$, 令 D 为 Z_N 的一个子集, 定义

$$D+a\in\{d+a|d\in D\},\ aD\in\{ad|d\in D\}$$

对于任意点 $x\in C_i$, $y\in C_j$, $0\leqslant i\neq j<e$, 定义方程 $x-y=1$ 的解是 e 阶分圆类的 e 阶分圆数, 对于任

意 i 和 j, 也可将 e 阶分圆数表示为

$$(i,j)=|(C_i+1)\cap C_j|$$

引理 4 定义的 e 阶分圆数具有如下基本性质:

1) $a_iC_j=C_{i+j}$, $0\leqslant i\neq j<e_1$;

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

3) $\sum_{i=0}^{e-1}(i,j)=\begin{cases} f-1 & j=0 \\ f & j\neq 0 \end{cases}$;

4) $\sum_{i=0}^{e-1}(\theta+i,i)=\begin{cases} f-1 & \theta=0 \\ f & \theta\neq 0 \end{cases}, 0\leqslant\theta<e$。

1.3 环上的分圆

2013 年, Zeng 等[11] 给出了环上的分圆。

设 $v=\prod_{i=1}^{k}p_i^{m_i}$, e_1 是奇素数 $p_1<p_2<\cdots<p_k$ 的一个公因子, 则存在 k 个 f_i 使得 $p_i-1=e_1f_i$, $1\leqslant i\leqslant k$, $e_1>1$。

根据中国剩余定理可得:

$$Z_v=Z_{p_1^{m_1}}\times Z_{p_2^{m_2}}\times\cdots\times Z_{p_k^{m_k}}$$

$$Z_v^*=Z_{\varphi(p_1^{m_1})}\times Z_{\varphi(p_2^{m_2})}\times\cdots\times Z_{\varphi(p_k^{m_k})}$$

对于模 v 剩余类环 $Z_v=\{0,1,2,\cdots,v-1\}$, 令 A 是 Z_v 的一个子集, b 是 Z_v 中的一个元素, 则有:

$$b+A=A+b=\{a+b|a\in A\}$$

$$bA=Ab=\{ba|a\in A\}$$

设 v_1 表示 v 的一个因子, 根据中国剩余定理, 存在一个整数 ω_{v_1} 满足模 v_1 乘法阶是 e_1。定义 $D(v_1)=\{\omega_{v_1}^d|0\leqslant d\leqslant e_1-1\}$, 故可知 $D(v_1)$ 是 $Z_{v_1}^*$ 的一个循环子群且阶为 e_1。

下面定义集合 Ω_v, 为

$$\Omega_v=\{Z_{(p_1-1)p_1^{m_1-1}/e_1}\times Z_{(p_2-1)p_2^{m_2-1}}\times\cdots\times Z_{(p_k-1)p_k^{m_k-1}}\}$$

当 $t\geqslant 1$ 时, 定义 $H^{\boldsymbol{I}_{v_1}}=\{h_1^{a_1},h_2^{a_2},\cdots,h_k^{a_k}\}$, 其中 $\boldsymbol{I}_{v_1}=\{a_1,a_2,\cdots,a_k\}$, $h_i(0\leqslant h_i\leqslant v-1)$ 是满足

$$h_i\equiv\begin{cases} 1(\bmod p_j^{m_j}) & \\ g_i(\bmod p_i^{m_i}) & 1\leqslant i\neq j\leqslant k \end{cases}$$

的唯一解。对任意正整数 j, $1\leqslant j\leqslant k$, g_i 是模 $p_i^j(1\leqslant i\leqslant k)$ 的一个本原根。

根据 $D(v_1)$ 及它的陪集, 可以给出一个对 Z_v 的划分, 定义

$$D_{\boldsymbol{I}_{v_1}}^{(v_1)}=H^{\boldsymbol{I}_{v_1}}D(v_1)=\{<H^{\boldsymbol{I}_{v_1}}\omega_{v_1}^d>_{v_1}|0\leqslant d\leqslant e_1-1\}$$

其中 $\boldsymbol{I}_{v_1}=\{a_1,a_2,\cdots,a_k\}\in\Omega_{v_1}$。因此可以得出, $D_{\boldsymbol{I}_{v_1}}^{(v_1)}$ 是 $Z_{v_1}^*$ 的一个子集, $Z_{v_1}^*=\bigcup_{\boldsymbol{I}\in\Omega_{v_1}}D_{\boldsymbol{I}_{v_1}}^{(v_1)}$。

引理 5 对于任意的 v_1, v_1 是 v 的一个因子, 可知

$$Z_v\backslash\{0\}=\bigcup_{v_1>1,v_1|v}\left(\bigcup_{\boldsymbol{I}_{v_1}\in\Omega_{v_1}}\frac{v}{v_1}D_{\boldsymbol{I}_{v_1}}^{(v_1)}\right)$$

综上所述, 有 $\left|D_{\boldsymbol{I}_{v_1}}^{(v_1)}\right|=e_1$, 设 $\left|\left\{\frac{v}{v_1}D_{I_{v1}}^{(v_1)}|I_{v1}\in\Omega_{v1},1<v_1|v\right\}\right|=\frac{v-1}{e_1}$, 故可构造的阶为 $\frac{v-1}{e_1}$ 的分圆类。下面给出分圆类 $D_{\boldsymbol{I}}$ 的定义, 为

$$D_{\boldsymbol{I}}=\sum_{v_1|v,v_1>1}D_{\boldsymbol{I}_{v_1}}^{(v_1)}=\left\{\sum_{v_1|v,v_1>1}<H^{\boldsymbol{I}_{v_1}}\omega_{v_1}^d>_{v_1}|0\leqslant d\leqslant e_1-1\right\}$$

引理 6 对于整数 β 及 2 个 k 维向量 $\boldsymbol{I}=\{a_1,a_2,\cdots,a_k\}$, $\boldsymbol{J}=\{b_1,b_2,\cdots,b_k\}$, $\boldsymbol{I},\boldsymbol{J}\in\Omega_v$, 设 $D_{\boldsymbol{I}_0}^{(v_1)}=D(v_1)$, 则新的分圆数具有如下性质:

1) $\boldsymbol{I}+\boldsymbol{J}=(a_1+b_1,a_2+b_2,\cdots,a_k+b_k)$;

2) $\beta\boldsymbol{I}=(\beta a_1,\beta a_2,\cdots,\beta a_k)$;

3) $\boldsymbol{I}+\beta=\boldsymbol{I}+\beta\boldsymbol{I}_0$

2 跳频序列集的构造

本节基于环上的分圆理论和中国剩余定理给出了一类跳频序列集的构造, 并证明了所构造的跳频序列集满足平均汉明相关理论界最优。

定义集合 $A=\left\{\frac{v}{v_1}D_{\boldsymbol{I}_{v_1}}^{(v_1)}|\boldsymbol{I}_{v_1}\in\Omega_{v_1},1<v_1|v\right\}$, 其中, 当 $\boldsymbol{I}_{v_1}\in\Omega_{v_1},1<v_1|v$ 时, 有 $\left|D_{\boldsymbol{I}_{v_1}}^{(v_1)}\right|=e_1$, $|A|=\frac{v-1}{e_1}$。

设 n 是一个正整数且 n 小于 v。由中国剩余定理可知, 当 n 不能被 v 整除时, Z_{nv} 中任意一元素 h, 都可写成 $Z_n\times Z_v$ 中的一个元素 (h_1,h_2), 其中 $h_1=<h>_n$, $h_2=<h>_v$。

基于环上分圆的性质, 可以给出新的跳频序列集的构造方法。

构造 令 $t=\frac{v-1}{e_1}$, 选取一个定义在 Z_t 上一个序列周期为 v-1, 序列集大小为 f_1 的跳频序列集 $S=\{\boldsymbol{x}^1,\boldsymbol{x}^2,\cdots,\boldsymbol{x}^{f_1}\}$, $\boldsymbol{x}^i=\{x^i(0),x^i(1),\cdots,x^i(nv-1)\}$。当 $1<v_1,v_1|v,\boldsymbol{I}_{v_1}\in\Omega_{v_1}$ 时, $\boldsymbol{x}_j^i=\beta\left(\frac{v}{v_1}D_{\boldsymbol{I}_{v_1}}^{(v_1)}\right)$, 其中 $j\in\left[\{w\}\times\left\{\frac{v}{v_1}D_{\boldsymbol{I}_{v_1}+g(w,s)}^{(v_1)}\right\}\right]$, 函数 β 是从集合 A 到 Z 的双射, 函数 $g(w,s)$ 是 $Z_n\times Z_{f_1}$ 到 Z_t 的一个二元单射, 其中 $w\in Z_n$, $w\in Z_{f_1}$。

定理 1 根据构造方法构造的跳频序列集有

如下性质。

1)构造得到跳频序列集的序列长度为 $n(v-1)$,频隙点个数为$\frac{v-1}{e_1}$,跳频序列集 S 平均自相关和互相关总和分别是:

$$S_{\mathrm{a}}(S)=Mn(\frac{v-1}{e_1})e_1(ne_1-1)$$

$$2S_{\mathrm{c}}(S)=M(M-1)n(\frac{v-1}{e_1})e_1ne_1$$

2)由构造得到的跳频序列集 S 满足平均汉明相关理论界最优。

证明　1) 定义$<\tau_1>_n,<\tau_2>_{v-1}$, $\boldsymbol{x}^s,\boldsymbol{x}^r$ 是跳频序列集 S 里任意 2 条序列

$$H_{\boldsymbol{x}^s\boldsymbol{x}^r}(\tau)=\sum_{u=0}^{t}|\{0\leqslant m<n(v-1)|x_m^s=x_{m+\tau}^r=u\}|=$$
$$\sum_{\substack{1<v_1,v_1|v\\ \boldsymbol{I}_{v_1}\in\Omega_{v_1}}}\left|\bigcup_{w=0}^{n-1}\left(\{w\}\times\left\{D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,s)}\right\}\right)\cap\right.$$
$$\left.\bigcup_{k=0}^{n-1}\left(\{w+\tau_1\}\times\left\{D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,r)}+\tau_2\right\}\right)\right|$$

为求 2 条序列的汉明相关性,将上面讨论的结果 τ_1,τ_2 的取值分成 4 种情况考虑。

情况 1, 当 $\tau_1=0,\tau_2=0$ 时, 由 g 是二元单射,得到

$$S_{\mathrm{c}}(S)=\sum_{\substack{(\tau_1,\tau_2)=(0,0)\\ \tau_1\neq0,\tau_2\neq0\\ 0\leqslant s\neq r<M}}^{(0,0)}H_{\boldsymbol{x}^s\boldsymbol{x}^r}(\tau)=$$
$$\sum_{u=0}^{t}|\{0\leqslant m<n(v-1)|x_m^s=x_{m+\tau}^r=u\}|=$$
$$n\cdot\sum_{\substack{1<v_1,v_1|v\\ \boldsymbol{I}_{v_1}\in\Omega_{v_1}\\ 0\leqslant s\neq r<M}}\left|\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,s)}\right)\cap\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,r)}\right)\right|=0$$

情况 2, 当 $\tau_1\neq0,\tau_2=0$ 时, 由 g 是二元单射, 得到

$$S_{\mathrm{c}}(S)=\sum_{\substack{(\tau_1,\tau_2)=(1,0)\\ \tau_1\neq0,\tau_2\neq0\\ 0\leqslant s\neq r<M}}^{(n,0)}H_{\boldsymbol{x}^s\boldsymbol{x}^r}(\tau)=\sum_{u=0}^{t}|\{0\leqslant m<$$
$$n(v-1)|x_m^s=x_{m+\tau}^r=u\}|=$$
$$n\cdot\sum_{\substack{1<v_1,v_1|v\\ \boldsymbol{I}_{v_1}\in\Omega_{v_1}\\ 0\leqslant s\neq r<M}}\left|\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,s)}\right)\cap\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w-\tau_1,r)}\right)\right|=0$$

情况 3, 当 $\tau_1=0,\tau_2\neq0$ 时, 由 g 是二元单射,得到

$$S_{\mathrm{c}}(S)=\sum_{\substack{(\tau_1,\tau_2)=(0,1)\\ \tau_1=0,\tau_2\neq0\\ 0\leqslant s\neq r<M}}^{(0,v-1)}H_{\boldsymbol{x}^s\boldsymbol{x}^r}(\tau)=\sum_{u=0}^{t}|\{0\leqslant m<$$
$$n(v-1)|x_m^s=x_{m+\tau}^r=u\}|=$$
$$n\cdot\sum_{\substack{(\tau_1,\tau_2)=(0,1)\\ \tau_1\neq0,\tau_2\neq0\\ 0\leqslant s\neq r<M}}^{(0,v-1)}\sum_{\substack{1<v_1,v_1|v\\ \boldsymbol{I}_{v_1}\in\Omega_{v_1}}}\left|\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,s)}\right)\cap\right.$$
$$\left.\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,r)}+\tau_2\right)\right|=$$
$$\frac{1}{2}M(M-1)n\left(\frac{v-1}{e_1}\right)\frac{e_1}{n}(ne_1)$$

情况 4, 当 $\tau_1\neq0,\tau_2\neq0$ 时, 由 g 是二元单射,得到

$$S_{\mathrm{c}}(S)=\sum_{\substack{(\tau_1,\tau_2)=(1,1)\\ \tau_1\neq0,\tau_2\neq0\\ 0\leqslant s\neq r<M}}^{(n,v-1)}H_{\boldsymbol{x}^s\boldsymbol{x}^r}(\tau)=\sum_{u=0}^{t}|\{0\leqslant m<$$
$$n(v-1)|x_m^s=x_{m+\tau}^r=u\}|=$$
$$n\cdot\sum_{\substack{(\tau_1,\tau_2)=(1,1)\\ \tau_1\neq0,\tau_2\neq0\\ 0\leqslant s\neq r<M}}^{(n,v-1)}\sum_{\substack{1<v_1,v_1|v\\ \boldsymbol{I}_{v_1}\in\Omega_{v_1}}}\left|\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w,s)}\right)\cap\right.$$
$$\left.\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}+g(w-\tau_1,r)}+\tau_2\right)\right|=\frac{1}{2}M(M-1)n\left(\frac{v-1}{e_1}\right)\frac{e_1(n-1)}{n}(ne_1)$$

上面讨论的是序列集的汉明互相关总和,即 $s\neq r$ 的情况。当 $s=r$ 时, 在 $\tau_1=0,\tau_2\neq0$ 的情况下 $S_{\mathrm{a}}(S)=Mn\left(\frac{v-1}{e_1}\right)\frac{e_1}{n}[n(e_1-1)]$。其余情况下和互相关结果相同。故综合上面各种情况,可以得到:

$$S_{\mathrm{a}}(S)=Mn\left(\frac{v-1}{e_1}\right)e_1(ne_1-1)$$

$$2S_{\mathrm{c}}(S)=M(M-1)n\left(\frac{v-1}{e_1}\right)e_1ne_1$$

2) 根据分圆的性质,汉明自(互)相关的总和是在所有时延下各频点碰撞次数的总和。结合构造得到的跳频序列集频点个数为$\frac{v-1}{e_1}$,由性质 1) 可得,汉明自相关总和互相关总和分别为:

$$S_{\mathrm{a}}(S)=Mn\left(\frac{v-1}{e_1}\right)e_1(ne_1-1)$$

$$2S_{\mathrm{c}}(S)=M(M-1)n\left(\frac{v-1}{e_1}\right)e_1ne_1$$

故平均汉明自(互)相关为:

$$A_a(S)=\frac{S_a(S)}{M(N-1)}=\frac{n\left(\frac{v-1}{e_1}\right)e_1(ne_1-1)}{(nv-n-1)}=\frac{\{n(e_1-1)(v-1)+(n-1)(v-1)ne_1\}}{(nv-n-1)} \quad (4)$$

$$A_c(S)=\frac{2S_c(S)}{NM(M-1)}=\frac{\{ne_1(v-1)n\}}{(nv-n)} \quad (5)$$

接下来证明跳频序列集 S 关于平均汉明相关理论界是最优的。

将式 (4)、式 (5) 代入平均汉明相关理论界不等式(3)中, 可得

$$\frac{A_a}{N(M-1)}+\frac{A_c}{(N-1)}=\frac{\{n(e_1-1)(v-1)+(n-1)(v-1)ne_1\}}{(nv-n-1)(nv-n)(M-1)}+\frac{\{ne_1(v-1)n\}}{(nv-n-1)(nv-n)}=\frac{(v-1)(n^2e_1M-n)l}{(nv-n-1)(nv-n)(M-1)l}=\frac{(v-1)(n^2e_1M-n)\frac{v-1}{e_1}}{(nv-n-1)(nv-n)(M-1)\frac{v-1}{e_1}}=\frac{\left\{(v-1)\left[(n^2M-\frac{n}{e_1})(v-1\right]\right\}}{(nv-n-1)(nv-n)(M-1)\frac{v-1}{e_1}}=\frac{\left\{n(v-1)\left[(nM-\frac{1}{e_1})(v-1\right]\right\}}{(nv-n-1)(nv-n)(M-1)\frac{v-1}{e_1}}=\frac{\left\{n(v-1)\left[(n(v-1)M-\frac{v-1}{e_1}\right]\right\}}{(nv-n-1)(nv-n)(M-1)\frac{v-1}{e_1}}=\frac{NM-l}{l(M-1)(N-1)}$$

故可得结论

$$\frac{A_a}{N(M-1)}+\frac{A_c}{(N-1)}\geqslant\frac{NM-l}{l(N-1)(M-1)}$$

构造中结果可使等号成立, 故满足理论界要求, 因此跳频序列集关于平均相关理论界是最优的。证毕。

例 当 $v=247=13\times19$ 时, $v_1\in\{13, 19, 247\}$, e_1 是 12 与 18 的公因子, 取 e_1=2 故 f_1 =6, 又可知 2 是 13, 19 的公共本原根。

根据构造, 可以给出集合 A 为

$$\left\{D^{247}_{(0,0)}, D^{247}_{(0,1)}, D^{247}_{(0,2)}, D^{247}_{(0,3)}, \cdots, D^{247}_{(0,17)}, D^{247}_{(1,0)}, D^{247}_{(1,1)}, \cdots, D^{247}_{(1,17)}, D^{247}_{(2,0)}, D^{247}_{(2,1)}, \cdots, D^{247}_{(2,17)}, D^{247}_{(3,0)}, D^{247}_{(3,1)}, \cdots, D^{247}_{(3,17)}, D^{247}_{(4,0)}, \cdots, D^{247}_{(4,17)}, D^{247}_{(5,0)}, \cdots, D^{247}_{(5,17)}, 13D^{19}_{(0)}, 13D^{19}_{(1)}, \cdots, 13D^{19}_{(8)}, 19D^{13}_{(0)}, 19D^{13}_{(1)}, \cdots, 19D^{13}_{(5)}\right\}$$

当 $\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}}$ 是集合 A 第 i 个子集合时, 定义 $\beta\left(\frac{v}{v_1}D^{(v_1)}_{\boldsymbol{I}_{v_1}}\right)=i$, $0\leqslant i\leqslant122$, 通过构造, 可以得到跳频序列集 $S=\{\boldsymbol{x}^1,\boldsymbol{x}^2,\boldsymbol{x}^3\}$:

$\boldsymbol{x}^1$={107, 19, 85, 38, 61, 85, 105, 57, 53, 61, 2, 6, 116, 7, 29, 76, 27, 53, 122, 80, 55, 40, 64, 25, 94, 109, 3, 26, 70, 29, 60, 95, …, 95, 60, 29, 70, 26, 3, 109, 94, 25, 64, 40, 55, 80, 122, 53, 27, 76, 29, 7, 116, 6, 2, 61, 53, 57, 105, 85, 61, 38, 85, 19, 107}

$\boldsymbol{x}^2$={69, 107, 47, 0, 23, 47, 67, 19, 15, 23, 72, 76, 114, 77, 99, 38, 97, 15, 120, 42, 35, 2, 26, 95, 56, 116, 73, 96, 32, 99, 22, …, 22, 99, 32, 96, 73, 116, 56, 95, 26, 2, 35, 42, 120, 15, 97, 38, 99, 77, 114, 76, 72, 23, 15, 19, 67, 47, 23, 0, 47, 107, 69}

$\boldsymbol{x}^3$={31, 69, 9, 88, 93, 9, 29, 107, 85, 93, 52, 38, 112, 39, 61, 0, 59, 85, 118, 4, 105, 72, 96, 57, 18, 114, 53, 58, 102, 61, 92, …, 92, 61, 102, 58, 53, 114, 18, 57, 96, 72, 105, 4, 118, 85, 59, 0, 61, 39, 112, 38, 52, 93, 85, 107, 29, 9, 93, 88, 9, 69, 31}

经计算, 例构造的长度为 492, 频点个数为 123, 序列大小为 3 的跳频序列集的平均汉明自相关值和平均汉明互相关值分别是 3.006 109 979 63 和 4, 代入平均汉明相关理论界, 满足理论界最优。故跳频序列集 S 是一个满足平均汉明相关理论界最优的跳频序列集。

3 结论

本文首先根据环上分圆的性质, 选取序列长度为 v-1, 频点个数为$\frac{v-1}{e_1}$, 序列大小为 f_1 的跳频序列集为基序列, 然后利用分圆法和中国剩余定理将序列扩展到序列长度为 $n(v$-1), 频点个数为$\frac{v-1}{e_1}$, 序列大小为$\left\lfloor\frac{f_1}{n}\right\rfloor$的跳频序列集, 并证明了所得到的跳频序列集关于平均汉明相关理论界最优。新构造的跳频序列集参数限制条件更少, 参数更加灵活。表 1 示出了基于分圆理论的最优跳频序列集的参数比较结果。与文献 [12] 相比, 本文构造结果满足平均汉明相关理论界最优; 与文献 [15] 相比, 本文构造结果参数更加灵活。

表 1　分圆法构造跳频序列集的参数比较

N	l	M	λ	限制条件	L-G界	P-F界	平均界	文献
p	f+1	f	e	$2 \leqslant e \leqslant f$+2	最优	最优	非最优	[7]
p	f	f	e	–	非最优	非最优	最优	[13]
$2p$	f+1	$\lfloor f/2 \rfloor$	$2e$	$2 \leqslant e \leqslant (f$+9)/6	非最优	最优	非最优	[14]
p^2	p	p	p	–	最优	最优	最优	[15]
p^2	p^2	$(p-1)^2$	p^2	–	非最优	非最优	最优	[9]
np	f+1	$\lfloor f/n \rfloor$	ne	$ne \leqslant f$	非最优	最优	非最优	[16]
$q-1$	f+1	f	e	$f \leqslant e-1$	最优	最优	非最优	[8]
$n.(q-1)$	f+1	$\lfloor f/n \rfloor$	ne	$\gcd(n,ef)=1$ $n,f \leqslant e$	非最优	最优	最优	[17]
np	$(p-1)/e$+1	$\lfloor f_1/n \rfloor$	ne	$1 < e \leqslant f_1$, $n(e+1) < f_1$	非最优	最优	非最优	[18]
$n(p-1)$	$(p-1)/e$	$\lfloor f_1/n \rfloor$	–	$n < f_1$	非最优	非最优	最优	定理1
p_1p_2	d	d	$(p_1p_2-1)/d$	$\gcd(p_1-1,p_2-1)=2n,d \mid 2n,d$是奇素数	非最优	非最优	最优	[14]
v	$(v-1)/e_1+1$	f_1	e_1	v是非素数或$1 < e_1+1 \leqslant f_1$	最优	最优	最优	[11]
v	$(v-1)/2e_1$	f_1/n	$2ne_1$	e_1是奇数, $p_i \equiv 3 \pmod 4$	最优	–	非最优	[11]
kv	v	$(p_1-1)/n$	k	k不能被p整除	最优	最优	最优	[18]
nv	$(v-1)/e_1+1$	$\lfloor f_1/n \rfloor$	ne_1	v是非素数且$n < f_1$	非最优	最优	非最优	[12]
$n(v-1)$	$(v-1)/e_1$	$\lfloor f_1/n \rfloor$	–	v是非素数且$n < f_1$	非最优	非最优	最优	定理1

注: $q=p^n=ef+1$, $v=\prod_{i=1}^{k} p_i^{m_i}$, 表示不同奇素数的幂次乘积; $m_1,\cdots,m_k$为正整数; $p_1<p_2<\cdots<p_k$是不同奇素数; $p_i=e_1f_i+1$(e是$p_1,p_2,\cdots,p_t$的公因子且$e_1>1$); n是满足不能被v整除且小于v的正整数。

参　考　文　献

[1] 梅文华. 跳频序列设计 [M]. 北京: 国防工业出版社, 2016.

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

[3] 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, 50(9): 2149 − 2154.

[4] PENG D Y, NIU X H, TANG X H. Average Hamming correlation for the cubic polynomial hopping sequences[J]. IET Commun, 2010, 4(15): 775 − 1786.

[5] REN W L, FU F W, ZHOU Z C. On the average partial Hamming correlation of frequency hopping sequences[J]. IEICE Trans Fundam, 2013, E96-A(5): 1010 − 1013.

[6] HAN H Y, PENG D Y, LIU X. On the average Hamming correlation of frequency hopping sequences[J]. IEICE Trans Fundam, 2014, E97(A): 1430 − 1433.

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

[8] DING C S, YIN J. Sets of optimal frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2008, 54(8): 3741 − 3745.

[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.

[10] 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.

[11] ZENG X Y, CAI H, TANG X H. Optimal frequency hopping sequences of odd length[J]. IEEE Transactions on Information Theory, 2013, 59(5): 3237 − 3248.

[12] XU S, CAO X. A new family of optimal FHS sets with composite lengths[J]. Discrete Mathematics, 2019, 342(5): 1446 − 1455.

[13] CHUNG J, YANG K. New frequency-hopping sequence sets with optimal average and good maximum Hamming correlations[J]. IET Commun, 2013, 6: 2048 − 2053.

[14] 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.

[15] 徐善顶, 曹喜望, 许广魁. 基于分圆法的一类素数平方周期跳频序列族[J]. 电子与信息学报, 2015, 37(10): 2460 − 2465.

[16] 徐善顶, 曹喜望, 许广魁. 一类周期为素数倍数的跳频序列族[J]. 电子学报, 2015, 43(10): 1930 − 1937.

[17] REN W L, FU F W, ZHOU Z C. A new frequency-hopping sequences with optimal Hamming correlation[J]. Designs, Codes and Cryptography, 2014, 72(2): 423 − 434.

[18] CHUNG J H, YANG K. New class of optimal frequency-hopping sequences by interleaving techniques[J]. IEEE Transactions on Information Theory, 2009, 55(12): 5783 − 5791.

(编校: 饶莉)