基于 m-序列的跳频序列集的构造与二维相关性分析

刘元慧[①②] 许成谦*[①] 方汶铭[①②]
[①](燕山大学信息科学与工程学院 秦皇岛 066004)
[②](燕山大学理学院 秦皇岛 066004)

摘 要：在雷达等高速移动的通信系统中，由于传输过程中的时延和多普勒频移，在分析跳频序列的性能时，需要对其时频 2 维汉明相关性进行分析。线性移位寄存器序列(m-序列)具有良好的随机、平衡等性质，因此 m-序列已被广泛应用到跳频序列的构造中。该文对基于 m-序列的跳频序列集的时频 2 维汉明相关性进行分析，计算了其时频 2 维汉明相关值的分布；构造了具有新参数的跳频序列集。在相同多普勒频移下，新序列集的 2 维相关性与已有基于 m-序列的跳频序列集的 2 维相关性相比较更稳定。

关键词：跳频序列；m -序列；时频 2 维汉明相关值；2 维最大汉明相关值
中图分类号：TN911.2 **文献标识码**：A **文章编号**：1009-5896(2017)10-2449-07
DOI: 10.11999/JEIT170051

Construction and Two-dimensional Correlation Analysis of Frequency Hopping Sequences Based on m-Sequence

LIU Yuanhui[①②] XU Chengqian[①] FANG Wenming[①②]
[①](*School of Information Science and Engineering*, *Yanshan University*, *Qinhuangdao* 066004, *China*)
[②](*School of Sciences*, *Yanshan University*, *Qinhuangdao* 066004, *China*)

Abstract: In the high-speed mobile communication system such as the radar, due to time delay and Doppler shift in the transmission process, it is needed to analyze Time-Frequency (TF) two-dimensional (2-D) Hamming correlation of the Frequency Hopping Sequence (FHS). Linear feedback shift register sequence (m-sequence) has good random and balance properties, so it is widely used to the construction of FHSs. In this paper, the TF 2-D Hamming correlation of FHS set constructed by m-sequence is analyzed, the distribution of its TF 2-D Hamming correlation is calculated, and an FHS set with new parameters is constructed. Under the same Doppler shift, the 2-D correlation of the new sequence set is more stable than the 2-D correlation of the existing ones.

Key words: Frequency Hopping Sequence (FHS); m-sequence; Time-frequency two-dimensional Hamming correlation; Two-dimensional maximum Hamming correlation

1 引言

在现代雷达技术中，强抗干扰、低截获概率可以提高雷达的生存及作战能力。跳频编码信号具有良好的抗干扰、低截获等优良性能，是现代雷达设计中重要的脉冲压缩技术[1]。在高速移动的雷达通信系统中，由于信号传输过程中时延和多普勒频移等原因造成频率重合干扰，使接收机的解调输出发生误码。考虑了时延和频移的跳频(FH)相关函数称为时频 2 维汉明相关函数。构造跳频序列(FHS)并研究其时频 2 维汉明相关函数具有重要的应用价值[2]。

线性移位寄存器序列(m -序列)已被深入研究并取得大量成果，且广泛应用到 FHS 的构造中。Lempel 和 Greenberger[3]在 1974 年基于有限域 F_p 上 m -序列的状态序列，将相邻的 r 个状态序列和某个 r 重逐项模 p 相加，再利用 σ 变换构造了具有最优汉明相关值的 FHS。梅文华等人[4,5]、Han 等人[6]和 Zhou 等人[7]将此方法改进，分别利用 m -序列的非相邻 r 个状态序列、采样序列和移位采样序列构造了最优(部分)(低相关区)FHS。梅文华和杨义先[8,9]基于有限域和有限扩展域上的 m -序列构造了最优 FHS。1990 年，Komo 和 Liu[10]利用 m -序列的分量序列构造 FHS。Udaya 和 Siddiqi[11]于 1998 年利用多项式剩余类环上的 m -序列设计了最优 FHS。2011 年，Zhou 等人[12]基于 m -序列的特性，利用具有差平衡

收稿日期：2017-01-16；改回日期：2017-05-16；网络出版：2017-06-27
*通信作者：许成谦 cqxu@ysu.edu.cn
基金项目：国家自然科学基金(61671402, 11304270)，河北省自然科学基金(F2015203150)，博士后基金(2015M570234)
Foundation Items: The National Natural Science Foundation of China (61671402, 11304270), The Natural Science Foundation of Hebei Province (F2015203150), The Postdoctoral Foundation (2015M570234)

性的 d-型函数给出了最优 FHS 的通用构造。2016 年，Han 等人[13]、Xu 等人[14]、Zhou 等人[15]和 Niu 等人[16]分别将 m-序列与交织、中国剩余定理以及组合等方法相结合构造最优(部分)FHS。上面提到的 FHS，分析了时延情形下序列(集)的汉明相关性，序列(集)的 2 维相关性尚未分析。

本文首先对已有的 m-序列的状态序列构造的 FHS 集的 2 维相关性进行分析，计算出其 2 维相关性的分布情况，然后构造了一类具有新参数的 FHS 集。内容组织如下：第 2 节介绍 FHS 的基本概念；第 3 节分析已有的基于 m-序列的 FHS 集的 2 维相关性；第 4 节基于 m-序列构造具有新参数的 FHS 集；第 5 节为结束语。

2 基本概念

2.1 FHS 的时频 2 维汉明相关值函数

FHS 的时频 2 维汉明周期相关函数定义如下：

定义 1 设 $X=\{x(i)\}_{i=0}^{L-1}, Y=\{y(i)\}_{i=0}^{L-1}$ 是两个周期为 L 的 FHS，则序列 X 和 Y 在时延 τ 和频移 υ 下的时频 2 维汉明周期相关函数定义为

$$H_{X,Y}(\tau,\upsilon)=\sum_{i=0}^{L-1}h[x(i),y(i+\tau)+\upsilon] \tag{1}$$

其中，当 $a=b$ 时，$h(a,b)=1$，否则 $h(a,b)=0$；$0\le\tau\le L-1, 0\le\upsilon\le q-1$, $i+\tau$ 为模 L 运算。

当序列 $X=Y$ 时，$H_{X,X}(\tau,\upsilon)$ 为 FHS X 在时延 τ 和频移 υ 下的时频 2 维汉明周期自相关函数。当序列 $X\ne Y$ 时，$H_{X,Y}(\tau,\upsilon)$ 为 FHS X 和 Y 在时延 τ 和频移 υ 下的时频 2 维汉明周期互相关函数。

设 $\mathcal{S}$ 为包含 M 个序列的 FHS 集，定义 2 维最大周期汉明相关值 $H(\mathcal{S})$ 为

$$H(\mathcal{S})=\max\left\{\max_{\substack{X\in\mathcal{S},\,0\le\tau\le L-1\\ 0\le\upsilon\le q-1,(\tau,\upsilon)\ne(0,0)}}\left\{H_{X,X}(\tau,\upsilon)\right\},\ \max_{\substack{X\ne Y\in\mathcal{S},0\le\tau\le L-1\\ 0\le\upsilon\le q-1}}\left\{H_{X,Y}(\tau,\upsilon)\right\}\right\} \tag{2}$$

2.2 FHS 集 2 维汉明相关值的理论界

引理 1 设 $F=\{f_0,f_1,\cdots,f_{q-1}\}$ 是频率数为 q 的频率集合，F 为 q 阶的加法群。$\mathcal{S}$ 是由 F 上 M 个长度为 L 的 FHS 组成的集合，则 $\mathcal{S}$ 的时频 2 维汉明周期自相关最大旁瓣 $H_a(\mathcal{S})$、时频 2 维汉明周期互相关峰值 $H_c(\mathcal{S})$ 和时频 2 维最大汉明周期相关值 $H(\mathcal{S})$ 满足

$$H(\mathcal{S})\ge\lceil L/q\rceil \tag{3}$$

称使得不等式中等号成立的 FHS 集 $\mathcal{S}$ 为时频最优 FHS 集。

3 基于 m-序列的 FHS 集的 2 维相关性分析

在文献[3]和文献[6]中，作者利用 m-序列的状态序列构造了 FHS 集，本节对其 2 维相关性进行分析。

给定素数 p 和正整数 r,n 且 $1\le r\le n$，F_p 是有限域。设 $\mathrm{Z}_{p^r}=\{0,1,\cdots,p^r-1\}$，$\mathrm{F}_p$ 上的 r 元向量集 $\mathrm{F}_p^r=\left\{(w_0w_1\cdots w_{r-1}), w_i\in\mathrm{F}_p, 0\le i\le r-1\right\}$。

定义 2[3] 映射 $\sigma:\mathrm{F}_p^r\to\mathrm{Z}_{p^r}$ 称为 σ-变换，定义为：$\boldsymbol{w}\sigma=\sum_{i=0}^{r-1}w_ip^{r-1-i}, \boldsymbol{w}=(w_0w_1\cdots w_{r-1})\in\mathrm{F}_p^r$。

显然，σ-变换为一一映射，且具有如下性质。

性质 1 对于 F_p^r 中任意两个 r 元向量 $\boldsymbol{w}=(w_0w_1\cdots w_{r-1})$，$\boldsymbol{v}=(v_0v_1\cdots v_{r-1})$，有

$$\boldsymbol{w}\sigma+\boldsymbol{v}\sigma\equiv(\boldsymbol{w}+\boldsymbol{v})\sigma \bmod p^r \tag{4}$$

式中，$\boldsymbol{w}+\boldsymbol{v}$ 的加法按 p 进制加法进行。

引理 2 设 l 为正整数，对于任意的 $\lambda_i\in\mathrm{F}_{p^n}$ $(i=0,1,\cdots,l-1)$ 和 $\boldsymbol{b}=(b_0,b_1,\cdots,b_{l-1})^{\mathrm{T}}\in\mathrm{F}_p^l$，线性方程组

$$\mathrm{Tr}_p^{p^n}(\lambda_ix)=b_i,\ i=0,1,\cdots,l-1 \tag{5}$$

(1)若 $\boldsymbol{b}=(0,0,\cdots,0)^{\mathrm{T}}$，则当 $\mathrm{rank}(\lambda_0,\lambda_1,\cdots,\lambda_{l-1})=e$ 时，式(5)在有限域 F_{p^n} 上有 $p^{n-e}-1$ 个解；

(2)若 $\boldsymbol{b}\ne(0,0,\cdots,0)^{\mathrm{T}}$，则当 $\mathrm{rank}(\lambda_0,\lambda_1,\cdots,\lambda_{l-1})=\mathrm{rank}(\lambda_0,\lambda_1,\cdots,\lambda_{l-1},b)=e$ 时，式(5)在 F_{p^n} 上有 p^{n-e} 个解；

(3)若 $\boldsymbol{b}\ne(0,0,\cdots,0)^{\mathrm{T}}$，则当 $\mathrm{rank}(\lambda_0,\lambda_1,\cdots,\lambda_{l-1})\ne\mathrm{rank}(\lambda_0,\lambda_1,\cdots,\lambda_{l-1},b)$ 时，式(5)在 F_{p^n} 上无解。

证明 设 F_{p^n} 在 F_p 上的一组对偶基分别为 $\{\alpha_0,\alpha_1,\cdots,\alpha_{n-1}\}$ 和 $\{\beta_0,\beta_1,\cdots,\beta_{n-1}\}$，则有 $\mathrm{Tr}_p^{p^n}(\alpha_i\beta_j)=\begin{cases}1, & i=j\\ 0, & \text{else}\end{cases}$。利用这组对偶基，对于任意的 $\lambda_i=\sum_{k=0}^{n-1}\lambda_{i,k}\alpha_k$ 和 $x=\sum_{k=0}^{n-1}x_k\beta_k$，其中 $\lambda_{i,k},x_k\in\mathrm{F}_p$, $0\le i\le l-1, 0\le k\le n-1$，有 $\mathrm{Tr}_p^{p^n}(\lambda_ix)=\sum_{k=0}^{n-1}\lambda_{i,k}x_k$。记 $\Lambda=(\lambda_0,\lambda_1,\cdots,\lambda_{l-1})=(\lambda_{i,j})_{l\times l}, 0\le i,j\le l-1$，$\boldsymbol{x}=(x_0,x_1,\cdots,x_{l-1})^{\mathrm{T}}$，则式(5)写作 $\boldsymbol{\Lambda}x=\boldsymbol{b}$。由文献[12]知，若 $\boldsymbol{b}=(0,0,\cdots,0)^{\mathrm{T}}$，当 $\mathrm{rank}\,\boldsymbol{\Lambda}=e$ 时，式(5)在有限域 F_{p^n} 内有 $p^{n-e}-1$ 个解；若 $\boldsymbol{b}\ne(0,0,\cdots,0)^{\mathrm{T}}$，当 $\mathrm{rank}\,\boldsymbol{\Lambda}=\mathrm{rank}(\boldsymbol{\Lambda},b)=e$ 时，式(5)在 F_{p^n} 上有 p^{n-e} 个解；当 $\mathrm{rank}\,\boldsymbol{\Lambda}\ne\mathrm{rank}(\boldsymbol{\Lambda},b)$ 时，式(5)在 F_{p^n} 上无解。 证毕

基于 m-序列的状态序列，利用 σ-变换构造的 Z_{p^r} 上的 FHS 集[6]如下：

定义 3[6] 设 $m=\{m(k)\}$ 为有限域 F_p 上长度为

p^n-1 的 m -序列。任取 $b_i \in \mathrm{F}_p^*$ ($0 \le i \le p-2$) 和 $a_j \in \mathrm{Z}_{p^r}(0 \le j < p^r)$，定义 FHS 集 $\mathcal{U}=\left\{U_{i,j}^r \mid 0 \le i < p-1, 0 \le j < p^r\right\}$，其中 $U_{i,j}^r=\left\{u_{i,j}^r(k)\right\}_{k=0}^{p^n-2}$，且

$$\left.\begin{aligned} u_{i,j}^r(k) &= s_{i,j}^r(k)\sigma \\ s_{i,j}^r(k) &= b_i \cdot m^r(k) + a_j\sigma^{-1} \\ m^r(k) &= \left(m(k)m(k+1)\cdots m(k+r-1)\right) \end{aligned}\right\} \tag{6}$$

这里，$s_{i,j}^r(k)$ 中加法计算为逐项模 p 运算。

式(6)中构造为文献[6]中构造 1，该构造方法包含了文献[3]中 Lempel 和 Greenberger FHS(LG-FHS)的构造作为特例。不失一般性，我们分析当 $r=2$ 时 FHS 集 $\mathcal{U}$ 的 2 维相关性。

当 $r=2$ 时，对于每一个 $a_j \in \mathrm{Z}_{p^2}, 0 \le j < p^2$，都存在唯一的 $(a_{j_0}, a_{j_1}) \in \mathrm{F}_p^2$，使得 $a_j = a_{j_0} + a_{j_1}p$。那么序列 $U_{i,j}^2=\left\{u_{i,j}^2(k)\right\}$ 表示为

$$\begin{aligned} u_{i,j}^2(k) &= b_i \cdot m(k) + a_{j_0} + \left(b_i \cdot m(k+1) + a_{j_1}\right)\cdot p \\ &= \left(b_i \cdot m(k) + a_{j_0}, b_i \cdot m(k+1) + a_{j_1}\right)\cdot\begin{pmatrix}1\\ p\end{pmatrix} \end{aligned} \tag{7}$$

式中，$k=0,1,\cdots,p^n-2$，分量中加法为模 p 运算。首先给出下面的引理。

引理 3　对于由式(7)定义的两序列 $U_{i,j}^2$ 和 $U_{i',j'}^2$，在时延 τ ($0 \le \tau < p^n-1$) 和频移 υ ($0 \le \upsilon < p^2$) 情形下，设 $\upsilon = v_0 + v_1 p$ ($v_0, v_1 \in \mathrm{F}_p$)。记

$$K=\left|\left\{k \mid u_{i,j}^2(k) = u_{i',j'}^2(k+\tau)+\upsilon, k=0,1,\cdots,p^n-2\right\}\right| \tag{8}$$

$$K_1=\left|\left\{k \left| \begin{array}{c} b_i \cdot m(k) + a_{j_0} = 0 \\ b_{i'} \cdot m(k+\tau) + a_{j_0'} + v_0 = p, \\ b_i \cdot m(k+1) + a_{j_1} = b_{i'} \cdot m(k+1+\tau) + a_{j_1'} + v_1 + 1 \bmod p \end{array} \quad 0 \le k < p^n-1 \right.\right\}\right| \tag{9}$$

$$K_2=\left|\left\{k \left| \begin{array}{c} b_i \cdot m(k) + a_{j_0} = b_{i'} \cdot m(k+\tau) + a_{j_0'} + v_0 \\ b_i \cdot m(k+1) + a_{j_1} = b_{i'} \cdot m(k+1+\tau) + a_{j_1'} + v_1 \end{array}, \quad 0 \le k < p^n-1 \right.\right\}\right| \tag{10}$$

$$K_3=\left|\left\{k \left| \begin{array}{c} b_i \cdot m(k) + a_{j_0} = 0 \\ b_{i'} \cdot m(k+\tau) + a_{j_0'} + v_0 = p, \\ b_i \cdot m(k+1) + a_{j_1} = b_{i'} \cdot m(k+1+\tau) + a_{j_1'} + v_1 \end{array} \quad 0 \le k < p^n-1 \right.\right\}\right| \tag{11}$$

设 $\boldsymbol{A}=\left(b_i\eta, \left(b_i - b_{i'}\alpha^\tau\right)\eta, \left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha\right), \boldsymbol{b}=\left(p-a_{j_0}, a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1 + 1\right)^{\mathrm{T}}$，$\boldsymbol{B}=\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta, \left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha\right)$，$\boldsymbol{b}'=\left(a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1\right)^{\mathrm{T}}$，$\boldsymbol{b}''=\left(p-a_{j_0}, a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1\right)^{\mathrm{T}}$。那么

(1) 若 $v_0 \ne 0$，则 $K=K_1+K_2-K_3$；否则 $K=K_2$。

(2)当 $\alpha^\tau \ne b_{i'}^{-1}b_i$ 时，若 $e=\mathrm{rank}\boldsymbol{A}, e'=\mathrm{rank}\boldsymbol{B}$，则有

$$K_1=\begin{cases} p^{n-e}-1, & \boldsymbol{b}=(0,0,0)^{\mathrm{T}} \\ p^{n-e}, & \boldsymbol{b} \ne (0,0,0)^{\mathrm{T}} \text{且} e=\mathrm{rank}(\boldsymbol{A},\boldsymbol{b}), \\ 0, & \boldsymbol{b} \ne (0,0,0)^{\mathrm{T}} \text{且} e \ne \mathrm{rank}(\boldsymbol{A},\boldsymbol{b}) \end{cases}$$

$$K_2=\begin{cases} p^{n-e'}-1, & \boldsymbol{b}'=(0,0)^{\mathrm{T}} \\ p^{n-e'}, & \boldsymbol{b}' \ne (0,0)^{\mathrm{T}} \text{且} e'=\mathrm{rank}(\boldsymbol{B},\boldsymbol{b}'), \\ 0, & \boldsymbol{b}' \ne (0,0)^{\mathrm{T}} \text{且} e' \ne \mathrm{rank}(\boldsymbol{B},\boldsymbol{b}') \end{cases}$$

$$K_3=\begin{cases} p^{n-e}-1, & \boldsymbol{b}''=(0,0,0)^{\mathrm{T}} \\ p^{n-e}, & \boldsymbol{b}'' \ne (0,0,0)^{\mathrm{T}} \text{且} e=\mathrm{rank}(\boldsymbol{A},\boldsymbol{b}'') \\ 0, & \boldsymbol{b}'' \ne (0,0,0)^{\mathrm{T}} \text{且} e \ne \mathrm{rank}(\boldsymbol{A},\boldsymbol{b}'') \end{cases} \tag{12}$$

证明　根据 K 以及 K_1, K_2 和 K_3 的定义易知，若 $v_0 \ne 0$，则 $K=K_1+K_2-K_3$；否则 $K=K_2$。

设 α 是有限扩展域 F_{p^n} 的本原元，则 F_{p^n} 上长度为 p^n-1 的 m -序列 $m=\{m(k)\}$ 为 $m(k)=\mathrm{Tr}_p^{p^n}(\eta\alpha^k)$，$k=0,1,\cdots,p^n-2$，$\eta \in \mathrm{F}_{p^n}^*$。令 $x=\alpha^k$，则 K_1, K_2 和 K_3 中的方程组可分别化为

$$\left.\begin{aligned} &\mathrm{Tr}_p^{p^n}(b_i\eta x) = p - a_{j_0} \\ &\mathrm{Tr}_p^{p^n}\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta x\right) = a_{j_0'} - a_{j_0} + v_0 \\ &\mathrm{Tr}_p^{p^n}\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha x\right) = a_{j_1'} - a_{j_1} + v_1 + 1 \end{aligned}\right\} \tag{13}$$

$$\left.\begin{aligned} &\mathrm{Tr}_p^{p^n}\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta x\right) = a_{j_0'} - a_{j_0} + v_0 \\ &\mathrm{Tr}_p^{p^n}\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha x\right) = a_{j_1'} - a_{j_1} + v_1 \end{aligned}\right\} \tag{14}$$

$$\left.\begin{aligned} &\mathrm{Tr}_p^{p^n}(b_i\eta x) = p - a_{j_0} \\ &\mathrm{Tr}_p^{p^n}\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta x\right) = a_{j_0'} - a_{j_0} + v_0 \\ &\mathrm{Tr}_p^{p^n}\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha x\right) = a_{j_1'} - a_{j_1} + v_1 \end{aligned}\right\} \tag{15}$$

设 $\boldsymbol{A}=\left(b_i\eta, \left(b_i - b_{i'}\alpha^\tau\right)\eta, \left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha\right), \boldsymbol{b}=\left(p-a_{j_0}, a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1 + 1\right)^{\mathrm{T}}$，$\boldsymbol{B}=\left(\left(b_i - b_{i'}\alpha^\tau\right)\eta, \left(b_i - b_{i'}\alpha^\tau\right)\eta\alpha\right)$，$\boldsymbol{b}'=\left(a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1\right)^{\mathrm{T}}$，

$\boldsymbol{b}''=\left(p-a_{j_0},a_{j_0'}-a_{j_0}+v_0,a_{j_1'}-a_{j_1}+v_1\right)^{\mathrm{T}}$。当 $\alpha^{\tau}\neq b_{i'}^{-1}b_i$ 时，根据引理 2 和根与系数的关系，可得结论。证毕

定理 1 设 $\mathcal{U}$ 是定义 3 构造的 FHS 集，任取 $U_{i,j}^r,U_{i',j'}^r\in\mathcal{U}$，$0\le i,i'<p-1,0\le j,j'<p^r$。时延 τ $(0\le\tau<p^n-1)$和频移 v $(0\le\tau<p^2)$，设 $v=v_0+v_1p$ $(v_0,v_1\in\mathrm{F}_p)$，当 $r=2$ 时，有

(1)序列的 2 维自相关值分布如下：

$$H_{U_{i,j}}(\tau,v)\begin{cases}=p^n-1, & (\tau,v)=(0,0)\\ =p^{n-2}-1, & \tau\neq 0,v=0\\ =0, & \tau=0,v\neq 0\\ =p^{n-2}, & \tau\neq 0,v\neq 0,v=0(\mathrm{mod}\,p)\\ \le p^{n-2}+p^{n-e}, & \text{其它}\end{cases}\tag{16}$$

(2)序列的 2 维互相关值分布如下：

(a)当 $a_j-a_{j'}=0(\mathrm{mod}\,p)$ 时，有

$$H_{U_{i,j},U_{i',j'}}(\tau,v)\begin{cases}=p^n-1, & \alpha^{\tau}=b_{i'}^{-1}b_i\text{且}v\equiv a_j-a_{j'}\\ =p^{n-2}-1, & \alpha^{\tau}\neq b_{i'}^{-1}b_i\text{且}v\equiv a_j-a_{j'}\\ =p^{n-2}, & \alpha^{\tau}\neq b_{i'}^{-1}b_i\text{且}v\equiv 0(\mathrm{mod}\ p)\\ =0, & \alpha^{\tau}=b_{i'}^{-1}b_i\text{且}v\neq a_j-a_{j'}\\ \le p^{n-2}+p^{n-e}, & \text{其它}\end{cases}\tag{17}$$

(b)当 $a_j-a_{j'}\neq 0(\mathrm{mod}\,p)$ 时，有

$$H_{U_{i,j},U_{i',j'}}(\tau,v)\begin{cases}=c\text{或}c', & \alpha^{\tau}=b_{i'}^{-1}b_i\text{且}v\equiv a_j-a_{j'}-sp\\ =p^{n-2}, & \alpha^{\tau}\neq b_{i'}^{-1}b_i\text{且}v=0(\mathrm{mod}\,p)\\ \le p^{n-2}+p^{n-e}, & \text{其它}\end{cases}\tag{18}$$

式中，e 与引理 3 相同；$c+c'=p^n-1$，$v\equiv a_j-a_{j'}$ 和 $v\neq a_j-a_{j'}$ 均为模 p^2 运算，且 $s=0,1$。

证明 根据式(6)，序列 $U_{i,j}^r$ 和 $U_{i',j'}^r$ 在时延 τ $(0\le\tau<p^n-1)$和频移 v $(0\le v<p^r)$下的 2 维周期相关函数：

$$\begin{aligned}H_{U_{i,j},U_{i',j'}}(\tau,v)&=\sum_{k=0}^{p^n-2}h\left(u_{i,j}^r(k),u_{i',j'}^r(k+\tau)+v\right)\\&=\sum_{k=0}^{p^n-2}h\left(s_{i,j}^r(k)\sigma,s_{i',j'}^r(k+\tau)\sigma+v\right)\end{aligned}\tag{19}$$

易知 $H_{U_{i,j},U_{i',j'}}(\tau,v)=K$，$K$ 如式(8)所定义，且 $K=K_1+K_2+K_3$，K_1,K_2 和 K_3 如引理 3 所定义。

(1)当 $U_{i,j}^r=U_{i',j'}^r$ 即 $b_i=b_{i'}$ 且 $a_j=a_{j'}$ 时，K_1,K_2 和 K_3 中方程分别化为

$$\left.\begin{aligned}&\mathrm{Tr}_p^{p^n}\left(b_i\eta\alpha^k\right)=p-a_{j_0}\\&\mathrm{Tr}_p^{p^n}\left(b_i\eta(1-\alpha^{\tau})\alpha^k\right)=v_0\\&\mathrm{Tr}_p^{p^n}\left(b_i\eta\alpha(1-\alpha^{\tau})\alpha^k\right)=v_1+1\end{aligned}\right\}\tag{20}$$

$$\left.\begin{aligned}&\mathrm{Tr}_p^{p^n}\left(b_i\eta(1-\alpha^{\tau})\alpha^k\right)=v_0\\&\mathrm{Tr}_p^{p^n}\left(b_i\eta\alpha(1-\alpha^{\tau})\alpha^k\right)=v_1\end{aligned}\right\}\tag{21}$$

$$\left.\begin{aligned}&\mathrm{Tr}_p^{p^n}(b_i\eta\alpha^k)=p-a_{j_0}\\&\mathrm{Tr}_p^{p^n}\left(b_i\eta(1-\alpha^{\tau})\alpha^k\right)=v_0\\&\mathrm{Tr}_p^{p^n}\left(b_i\eta\alpha(1-\alpha^{\tau})\alpha^k\right)=v_1\end{aligned}\right\}\tag{22}$$

接下来分情况讨论序列 2 维自相关值的分布。

(a)当 $(\tau,v)=(0,0)$ 时，显然平凡时频 2 维自相关值 $H_{U_{i,j}}(0,0)=K_2=p^n-1$。

(b)当 $\tau\neq 0,v=0$ 时，有 $\boldsymbol{b}'=(0,0)^{\mathrm{T}}$ 且 $e'=2$，由引理 3 知 $H_{U_{i,j}}(\tau,0)=K_2=p^{n-2}-1$。

(c)当 $\tau=0,v\neq 0$ 时，式(20)~式(22)无解，故 $H_{U_{i,j}}(0,v)=0$。

(d) 当 $\tau\neq 0,v\neq 0,v=0(\mathrm{mod}\,p)$ 时，有 $\boldsymbol{b}'\neq(0,0)^{\mathrm{T}}$，且 $e'=2$，由引理 3 知 $H_{U_{i,j}}(\tau,v)=K_2=p^{n-2}$。

(e)当 $\tau\neq 0,v\neq 0,v\neq 0(\mathrm{mod}\,p)$ 即 $v_0\neq 0$ 时，有 $\boldsymbol{b}\neq(0,0,0)^{\mathrm{T}},\boldsymbol{b}'\neq(0,0)^{\mathrm{T}},\boldsymbol{b}''\neq(0,0,0)^{\mathrm{T}}$ 且 $e'=2$，由引理 3 知 $K_1=p^{n-e}$ 或 0，$K_2=p^{n-2}$，$K_3=p^{n-e}$ 或 0，从而，$H_{U_{i,j}}(\tau,v)=K_1+K_2-K_3=p^{n-2}\pm p^{n-e},p^{n-2},0$。简记作 $H_{U_{i,j}}(\tau,v)\le p^{n-2}+p^{n-e}$。

(2)当 $U_{i,j}^r\neq U_{i',j'}^r$ 时，分析式(13)~式(15)在有限域 F_{p^n} 中解的个数，得到两序列的 2 维互相关值分布。

(a) 当 $a_j-a_{j'}=0(\mathrm{mod}\,p)$ 时，有 $\boldsymbol{b}=\left(p-a_{j_0},v_0,v_1+1\right)^{\mathrm{T}}$，$\boldsymbol{b}'=(v_0,v_1)^{\mathrm{T}}$，$\boldsymbol{b}''=\left(p-a_{j_0},v_0,v_1\right)^{\mathrm{T}}$。下面按频移 v 的取值分情况讨论。

(i)若 $v\equiv a_j-a_{j'}(\mathrm{mod}\,p^2)$，必然有 $v_0=0$，因此 $K=K_2$。又 $\boldsymbol{b}''=(0,0)^{\mathrm{T}}$，$\mathrm{rank}\boldsymbol{B}=\mathrm{rank}(\boldsymbol{B},\boldsymbol{b}')=e'$。

若 $\alpha^{\tau}=b_{i'}^{-1}b_i$，有 $e'=0$，则 $H_{U_{i,j},U_{i',j'}}(\tau,v)=K_2=p^n-1$；

若 $\alpha^{\tau}\neq b_{i'}^{-1}b_i$，有 $e'=2$，则 $H_{U_{i,j},U_{i',j'}}(\tau,v)=K_2=p^{n-2}-1$。

(ii)若 $v\equiv 0(\mathrm{mod}\ p)\neq a_j-a_{j'}(\mathrm{mod}\,p^2)$，有 $v_0=$

0，$v_1 \neq 0$，因此 $K = K_2$，$\boldsymbol{b}' = (0, v_1)^{\mathrm{T}}$。

若 $\alpha^{\tau} = b_{i'}^{-1} b_i$，显然有 $H_{U_{i,j},U_{i',j'}}(\tau, v) = K_2 = 0$；

若 $\alpha^{\tau} \neq b_{i'}^{-1} b_i$，则 $e' = 2$，$H_{U_{i,j},U_{i',j'}}(\tau, v) = K_2 = p^{n-2}$。

(iii) 若 $v \neq a_j - a_{j'} \left(\mathrm{mod}\, p^2\right) \neq 0 (\mathrm{mod}\, p)$，有 $v_0 \neq 0$，因此 $K = K_1 + K_2 - K_3$。又 $\boldsymbol{b} = \left(p - a_{j_0}, v_0, v_1 + 1\right)^{\mathrm{T}}$，$\boldsymbol{b}' = (v_0, v_1)^{\mathrm{T}}$，$\boldsymbol{b}'' = \left(p - a_{j_0}, v_0, v_1\right)^{\mathrm{T}}$。

若 $\alpha^{\tau} = b_{i'}^{-1} b_i$，显然有 $H_{U_{i,j},U_{i',j'}}(\tau, v) = K_1 + K_2 - K_3 = 0$；

若 $\alpha^{\tau} \neq b_{i'}^{-1} b_i$，有 $e' = 2$，则 $K_1 = p^{n-e}$ 或 0，$K_2 = p^{n-2}$，$K_3 = p^{n-e}$ 或 0，因此 $H_{U_{i,j},U_{i',j'}}(\tau, v) = K_1 + K_2 - K_3 = p^{n-2} \pm p^{n-e}, p^{n-2}, 0$，简记作 $H_{U_{i,j},U_{i',j'}}(\tau, v) \leq p^{n-2} + p^{n-e}$。

(b) 当 $a_j - a_{j'} \neq 0 (\mathrm{mod}\, p)$ 时，$\boldsymbol{b} = \left(p - a_{j_0}, a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1 + 1\right)^{\mathrm{T}}$，$\boldsymbol{b}' = \left(a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1\right)^{\mathrm{T}}$，$\boldsymbol{b}'' = \left(p - a_{j_0}, a_{j_0'} - a_{j_0} + v_0, a_{j_1'} - a_{j_1} + v_1\right)^{\mathrm{T}}$。接下来按频移 v 的取值进行分析。

(i) 若 $\alpha^{\tau} = b_{i'}^{-1} b_i$，$v \equiv a_j - a_{j'} (\mathrm{mod}\, p^2)$ 或 $v \equiv a_j - a_{j'} - p \left(\mathrm{mod}\, p^2\right)$，有 $\boldsymbol{b}' = (0,0)^{\mathrm{T}}$ 或 $\boldsymbol{b} = (0,0,0)^{\mathrm{T}}$，故 $H_{U_{i,j},U_{i',j'}}(\tau, v) = c$ 或 c'，且 $c + c' = p^n - 1$，$0 < c, c' \leq p^n - 1$。

(ii) 若 $\alpha^{\tau} \neq b_{i'}^{-1} b_i$，$v = 0 (\mathrm{mod}\, p)$ 即 $v_0 = 0$，有 $\boldsymbol{b}' \neq (0,0)^{\mathrm{T}}$，且 $e' = 2$，由引理 3 知 $H_{U_{i,j},U_{i',j'}}(\tau, v) = K_2 = p^{n-2}$。

(iii) 若 $\alpha^{\tau} \neq b_{i'}^{-1} b_i$，$v \neq 0 (\mathrm{mod}\, p)$ 即 $v_0 \neq 0$，有 $\boldsymbol{b}' \neq (0,0)^{\mathrm{T}}$，且 $e' = 2$，由引理 3 知 $K_1 = p^{n-e}$ 或 0，$K_2 = p^{n-2}$，$K_3 = p^{n-e}$ 或 0。故 $H_{U_{i,j},U_{i',j'}}(\tau, v) = K_1 + K_2 - K_3 = p^{n-2} \pm p^{n-e}, p^{n-2}$。简记 $H_{U_{i,j},U_{i',j'}}(\tau, v) \leq p^{n-2} + p^{n-e}$。　　证毕

由定理 1 的证明过程发现，当 $\alpha^{\tau} \neq b_{i'}^{-1} b_i$ 时，恒有 $e, e' \geq 2$，因此有下面的推论。

推论 1　当 $r = 2$ 时 FHS 集 $\mathcal{U}$ 的 2 维自相关最大旁瓣 $H_a(\mathcal{U}) \leq 2p^{n-2}$，2 维互相关峰值 $H_c(\mathcal{U}) \leq p^n - 1$。

定理 1 中仅讨论了当 $r = 2$ 时 FHS 集 $\mathcal{U}$ 的 2 维相关值的分布情况，实际上，当 $r > 2$ 时，用类似的方法可得 FHS 集 $\mathcal{U}$ 的 2 维相关值如推论 2。

推论 2　当 $r > 2$ 时 FHS 集 $\mathcal{U}$ 的 2 维自相关最大旁瓣 $H_a(\mathcal{U}) \leq rp^{n-r}$，2 维互相关峰值 $H_c(\mathcal{U}) \leq p^n - 1$。

注 1　定义 3 中构造的 FHS 集 $\mathcal{U}$ 由 Z_{p^r} 上长度为 $p^n - 1$ 的 $p^r(p-1)$ 个 FHS 组成的序列集，其时频 2 维最大汉明相关值 $H(\mathcal{U}) = p^n - 1$，而 $\left\lceil \dfrac{p^n - 1}{p^r} \right\rceil = p^{n-r}$，因此定义 3 中 FHS 集 $\mathcal{U}$ 在引理 1 意义下不是最优的。

注 2　在定义 3 构造的 FHS 集 $\mathcal{U}$ 中令 $b_i \equiv 1$，所得 FHS 集恰好为 LG-FHS 集。LG-FHS 集包含 Z_{p^r} 上 p^r 个长度为 $p^n - 1$ 的 FHS。当 $0 < \tau < p^n - 1$ 时，必有 $1 - \alpha^{\tau} \neq 0$，因此 LG-FHS 集的时频 2 维最大汉明相关值为 rp^{n-r}，又因为 $\left\lceil \dfrac{p^n - 1}{p^r} \right\rceil = p^{n-r}$，所以 LG-FHS 引理 1 意义下不是最优的。

4　基于 m-序列的具有新参数的 FHS 集的构造

将定义 3 中 FHS 集 $\mathcal{U}$ 的构造加以改进，以获得较小的 2 维汉明相关值。构造步骤如下：

构造 A　给定正整数 $n, r\ (2 \leq r \leq n)$ 和素数 p。

(1) 设 F_p 上由本原多项式 $f(x)$ 生成的 m-序列 $m = \{m(k)\}_{k=0}^{p^n-2}$，用 $m^r(k)$ 表示序列 m 中第 k 个相邻或非相邻的 r 重状态序列，即 $m^r(k) = (m(k+\omega_0)\ m(k+\omega_1) \cdots m(k+\omega_{r-1}))$，其中，$0 \leq \omega_i < \omega_{i+1} \leq n-1$。

(2) 构造集合 $D = \left\{a_j \middle| a_j - a_{j'} \equiv 0 (\mathrm{mod}\, p), a_j, a_{j'} \in \mathrm{F}_{p^r}, 0 \leq j, j' \leq p^{r-2} - 1\right\}$。

(3) 选择 $b_i \in \mathrm{F}_p^*\ (0 \leq i \leq p-2)$ 和 $a_j \in D\ (0 \leq j \leq p^{r-2} - 1)$，构造 F_{p^r} 上的 FHS 集 $\mathcal{Y} = \left\{Y_{i,j}^r \middle| 0 \leq i \leq p-2, 0 \leq j \leq p^{r-2} - 1\right\}$，其中 $Y_{i,j}^r = \left\{y_{i,j}^r(k)\right\}$，且

$$\left.\begin{aligned} y_{i,j}^r(k) &= s_{i,j}^r(k)\sigma \\ s_{i,j}^r(k) &= b_i \cdot m^r(k) + a_j \sigma^{-1} \\ m^r(k) &= \left(m\left(k+\omega_0\right) m\left(k+\omega_1\right) \cdots m\left(k+\omega_{r-1}\right)\right) \end{aligned}\right\} \quad (23)$$

式中，$s_{i,j}^r(k)$ 中加法计算为逐项模 p 运算。

定理 2　设 $\mathcal{Y}$ 是由构造 A 生成的 FHS 集，那么 $\mathcal{Y}$ 包含由 F_{p^r} 上的 $p^{r-2}(p-1)$ 个长度为 $p^n - 1$ 的 FHS，时延 $\tau\ (0 \leq \tau < p^n - 1)$ 和频移 $v\ (0 \leq v \leq p-1)$ 时，FHS 集的 2 维最大汉明周期相关值 $H(\mathcal{Y}) = rp^{n-r}$。

证明　利用与定理 1 类似的证明方法，得 $H(\mathcal{Y}) = rp^{n-r}$。

例 1　设 $p = 3, n = 3, r = 2$。设 F_p 上由本原多项式 $f(x) = x^3 + 3x + 1$ 生成的 m-序列为 $m = \{m(k)\}$，

即

$$m=\{0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1,1,2,0,1,1,1\}$$

设集合 $D=\{1,4,7\}$，选择 $b_i\in\{1,2\}(i=0,1)$ 和 $a_j\in D$ ($j=0,1,2$)，设

$$y_{i,j}(k)=\left[\left(b_i\cdot m(k)+a_{j_0}\right)\bmod 3\right]+3\left[\left(b_i\cdot m(k+2)+a_{j_1}\right)\bmod 3\right]$$

得到 FHS 集的 $2\times 3=6$ 个长度为 $3^3-1=26$ 的 FHS，即

$$y_{0,0}=\{1,7,0,7,3,8,6,3,2,7,6,6,0,1,4,2,4,8,3,5,8,0,4,5,5,2\}$$
$$y_{0,1}=\{4,1,3,1,6,2,0,6,5,1,0,0,3,4,7,5,7,2,6,8,2,3,7,8,8,5\}$$
$$y_{0,2}=\{7,4,6,4,0,5,3,0,8,4,3,3,6,7,1,8,1,5,0,2,5,6,1,2,2,8\}$$
$$y_{1,0}=\{1,4,2,4,8,3,5,8,0,4,5,5,2,1,7,0,7,3,8,6,3,2,7,6,6,0\}$$
$$y_{1,1}=\{4,7,5,7,2,6,8,2,3,7,8,8,5,4,1,3,1,6,2,0,6,5,1,0,0,3\}$$
$$y_{1,2}=\{7,1,8,1,5,0,2,5,6,1,2,2,8,7,4,6,4,0,5,3,0,8,4,3,3,6\}$$

容易验证，上述 FHS 的非平凡时频 2 维最大自相关值为 6，频移 $0\le\upsilon\le p-1$ 时，任意两个序列间的时频 2 维最大互相关值为 6。

注 3 构造 A 中得到的 FHS 集 $\mathcal{Y}$ 把定义 3 中相邻的状态序列换为任意(非相邻)的状态序列，很大程度地解决了频率滞留问题[4,5]。

构造 A 中集合 D 的选择，解决了定义 3 中所构造序列间有多个较大 2 维互相关值的问题。遗憾的是，所构造的序列集仍未达到最优。

5 结束语

FHS 集的时频 2 维相关性是影响跳频通信系统多址干扰的重要因素。本文对已有的基于 m -序列状态序列构造的 FHS 集的 2 维相关性进行分析，计算了其 2 维相关值的分布。根据其 2 维相关值的分布情况可知该 FHS 集不是最优的，其 2 维互相关函数具有多个较大峰值。文中构造了具有新参数的 FHS 集，新序列集在多普勒频移较小时比已有 FHS 集有更小的 2 维相关值。构造时频最优的 FHS 集是今后需要研究的问题。

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: 1–19.
MEI Wenhua. Frequency Hopping Sequences Design[M]. Beijing: National Defense Industry Press, 2016: 1–19.

[2] 刘元慧, 许成谦. 两类跳频序列集时频二维汉明相关性的分析[J]. 系统工程与电子技术, 已接收.
LIU Yuanhui and XU Chengqian. Analysis of time-frequency two-dimensional Hamming correlation of two frequency hopping sequence sets[J]. *Systems Engineering and Electronics*, accepted.

[3] LEMPEL A and GREENBERGER H. Families of sequences with optimal Hamming correlation properties[J]. *IEEE Transactions on Information Theory*, 1974, 20(1): 90–94. doi: 10.1109/TIT.1974.1055169.

[4] 梅文华, 陈先福. 具有最佳汉明相关性能的跳频序列族[J]. 国防科技大学学报, 1988, 10(4): 13–19.
MEI Wenhua and CHEN Xianfu. Families of frequency-hopping sequences with optimal Hamming correlation properties[J]. *Journal of National University of Defense Technology*, 1988, 10(4): 13–19.

[5] 梅文华. 基于 m-序列构造最佳跳频序列族[J]. 通信学报, 1991, 12(1): 70–73.
MEI Wenhua. Construct optimal families of frequency-hopping sequences basing on m-sequences[J]. *Journal of China Institute of Communications*, 1991, 12(1): 70–73.

[6] HAN Hongyu, PENG Daiyuan, and UDAYA P. New sets of optimal low-hit-zone frequency-hopping sequences based on m-sequences[J]. *Cryptography Communication*, 2017, 9(4): 511–522. doi: 10.1007/s12095-016-0192-7.

[7] ZHOU Limengnan, PENG Daiyuan, LIANG Hongbin, *et al*. Constructions of optimal low-hit-zone frequency hopping sequence sets[J]. *Designs, Codes and Cryptography*, 2016, (online first): 1–14. doi: 10.1007/s10623-016-0299-z.

[8] MEI Wenhua and YANG Yixian. Families of FH sequences based on pseudorandom sequences over GF(p)[C]. International Conference on Communication Technology Proceedings, Beijing, China, 2000, Vol. 1: 536–538. doi: 10.1109/ICCT.2000.889261.

[9] 梅文华, 杨义先. 基于 GF(p^r) 上 m-序列的最佳跳频序列族[J]. 通信学报, 1996, 17(2): 12–16.
MEI Wenhua and YANG Yixian. Optimal families of FH sequences based on m-sequences over GF(p^r) [J]. *Journal on Communications*, 1996, 17(2): 12–16.

[10] KOMO J J and LIU S. Maximal length sequences for frequency hopping[J]. *IEEE Journal on Selected Areas in Communications*, 1990, 8(5): 819–822. doi: 10.1109/49.56388.

[11] UDAYA P and SIDDIQI M U. Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings[J]. *IEEE Transactions on*

Information Theory, 1998, 44(4): 1492–1503. doi: 10.1109/18.681324.

[12] ZHOU Zhengchun, TANG Xiaohu, PENG Daiyuan, *et al*. New constructions for optimal sets of frequency-hopping sequences[J]. *IEEE Transactions on Information Theory*, 2011, 57(6): 3831–3840. doi: 10.1109/TIT.2011.2137290.

[13] HAN Hongyu, PENG Daiyuan, UDAYA P, *et al*. Construction of low-hit-zone frequency hopping sequences with optimal partial Hamming correlation by interleaving techniques[J]. *Designs, Codes and Cryptography*, 2016, (online first): 1–14. doi: 10.1007/s10623-016-0274-8.

[14] XU Shanding, CAO Xiwang, and XU Guanghui. Recursive construction of optimal frequency-hopping sequence sets[J]. *IET Communications*, 2016, 10(9): 1080–1086. doi: 10.1049/iet-com.2015.0864.

[15] ZHOU Zhengchun, TANG Xiaohu, NIU Xianhua, *et al*. New classes of frequency hopping sequences with optimal partial correlation[J]. *IEEE Transactions on Information Theory*, 2012, 58(1): 453–458. doi: 10.1109/TIT.2011.2167126.

[16] NIU Xianhua, PENG Daiyuan, and ZHOU Zhengchun. Frequency/time hopping sequence sets with optimal partial Hamming correlation properties[J]. *Science China Information Sciences*, 2012, 55(10): 2207–2215. doi: 10.1007/s11432-012-4620-9.

刘元慧：　女，1979 年生，讲师，博士生，研究方向为序列设计和移动通信.

许成谦：　男，1961 年生，教授，博士生导师，主要研究方向为序列设计、编码理论和移动通信.

方汶铭：　男，1979 年生，讲师，博士生，研究方向为序列设计和移动通信.