基于多项式理论的一类最优跳频序列族

刁哲军, 陈嘉兴, 刘志华
(河北师范大学, 河北石家庄 050031)

摘 要: 本文提出了一类新的应用于跳频(FH)码分多址(CDMA)系统的最优跳频序列族的构造方法. 这类跳频序列族的构造应用的是有限域上的多项式理论与判别式理论. 本文给出了 2 次与 3 次多项式确定的多项式跳频序列族的构造方法, 与已有构造方法相比较, 此方法得到的跳频序列族具有最优汉明相关性质, 且方法简单易行, 所构造的最优多项式跳频序列可以做为军用抗干扰跳频通信系统的候选序列, 有较强的应用前景.

关键词: 码分多址系统 (CDMA); 跳频序列; 汉明相关
中图分类号: TN914. 43 文献标识码: A 文章编号: 0372-2112 (2008) 07-1334-04

A New Family of Optimal Hopping Sequences Based upon Polynomial Theory

DIAO Zhe-jun, CHEN Jia-xing, LIN Zhi-hua
(*Hebei Normal University, Shijiazhuang* 050031, *China*)

Abstract: In this paper, a new family of hopping sequences called an optimal Hamming-correlation set for use in frequency-hopping(FH) code-division multiple-access(CDMA) system is proposed. The construction of the new hopping sequences is based upon the polynomial theory and discriminant theory over the finite field. The polynomial hopping sequences we present are based on polynomial with 2 degree and 3 degree. Comparing with the original method, this method can get hopping sequences with optimal Hamming-correlation and are good candidates for the anti-interference frequency-hopping communication systems in army. In addition the method for constructing the hopping sequences with optimal Hamming-correlation is very simple, feasible and has better applied foreground.

Key words: code-division multiple-access(CDMA); hopping sequences; Hamming-correlation

1 引言

近年来, 适用于码分多址系统(CDMA)的跳频序列研究引起了人们尤其是军事通信学者广泛的关注[1,2]. 这是由于跳频通信系统能够建立迅速, 便于机动, 能与运动中方位不明的以及被敌人分割或被自然障碍阻隔的部队建立通信联络. 它广泛的应用于地面、航空、航海、宇宙航行通信中, 是保障现代作战指挥的主要通信手段, 特别是在对飞机、舰艇、坦克等运动目标进行指挥时, 甚至是唯一的通信手段. 尽管各种各样的跳频系统自然意义和物理意义大相径庭, 但是它们对跳频信号的要求是基本相同的, 即发送者和他所发送的信息不能存在二义性, 并且接收端的接收信号对其他用户所产生的干扰要尽可能的被忽略不计. 在跳频系统中跳频序列的性能对系统的性能有着决定性的影响, 如果跳频序列设计的不好, 即使跳频通信系统的硬件电路设计的非常出色, 也达不到抗干扰的目的. 因此寻求和设计具有理想性能的跳频序列成为人们研究跳频通信系统的热点之一[3,4].

在跳频系统中, 跳频序列彼此之间的干扰主要由它们的汉明互相关所决定, 因此寻找同时具有好的汉明自相关函数, 小的汉明互相关函数值和大的族尺寸的序列是构造具有理想特性跳频序列族的关键. 2005 年, Fan 等人提出了多项式序列的构造方法[5], 所得序列具有大的族尺寸但不具有最优汉明相关的性质. 基于此基础本文通过分析多项式序列的构造方法, 根据方程在特定范围内存在根的个数, 提出了构造最优多项式跳频序列族的方法.

2 构造准备

我们首先介绍一下要用到的符号和定义.

定义 1[5] 设 $C=\{C^{(k)}\}$, $C^{(k)}=\{c_j^{(k)}\}$, $0\leqslant c_j^{(k)}\leqslant N_h-1$, $0\leqslant j\leqslant N_p-1$, $0\leqslant k\leqslant N_u-1$ 为一族跳频序列, 则它们之间的汉明互相关函数如下定义:

收稿日期: 2007-06-04; 修回日期: 2008-05-22
基金项目: 河北省科技厅基金(No. 07407234SD); 河北省教育厅基金(No. 2007472); 河北师范大学基金(No. L2005B27, No. L2007Z10)

$$H_{rs}(\tau)=\sum_{i=0}^{N_p-1}h\left(c_i^{(r)},\ c_{i+\tau}^{(s)}\right) \tag{1}$$

其中

$$h\left(c_i^{(r)},\ c_{i+\tau}^{(s)}\right)=\begin{cases}0, & c_i^{(r)}\neq c_{i+\tau}^{(s)}\\ 1, & c_i^{(r)}=c_{i+\tau}^{(s)}\end{cases} \tag{2}$$

当 $r=s$ 时, 上面的定义变为汉明自相关函数 $H_{rr}(\tau)$.

定义 **2**[5]　最大汉明互相关值 H_{cm}和最大汉明自相关旁瓣值H_{am}分别定义为:

$$H_{cm}=\max\left\{H_{rs}(\tau)\mid C^{(r)},\ C^{(s)}\in C,\ r\neq s,\ \tau=0,1,\ \cdots,N_p-1\right\} \tag{3}$$

$$H_{am}=\max\left\{H_{rr}(\tau)\mid C^{(r)}\in C,\ \tau=1,\ \cdots,N_p-1\right\} \tag{4}$$

跳频序列的设计一般包括 5 个参数: 每帧容纳的频率数(脉冲数) N_h, 跳频序列的周期 N_p, 表示用户的最大数 N_u, 最大汉明互相关值 H_{cm}和最大汉明自相关旁瓣值 H_{am}. 一般来讲, 这些参数以一定的理论限为界, 如 Peng-Fan 界[5]:

$$(N_p-1)N_hH_{am}+(N_u-1)N_pN_hH_{cm}\geqslant(N_pN_u-N_h)N_p \tag{5}$$

特别的, 当时 $N_h=N_p$, 上式变为

$$(N_p-1)H_{am}+(N_u-1)N_pN_hH_{cm}\geqslant(N_u-1)N_p \tag{6}$$

对于一个跳频序列族 S 来讲, 如果 H_{cm}和H_{am}是式(6)的一组最小整数解, 则称(H_{am}, H_{cm})为一个最优汉明相关对, 且 S 称为一个最优汉明相关序列族[5]. 易见, 如果等式 $N_h=N_p$ 成立的话, 上式 S 的一个最优汉明互相关对为$(H_{am}, H_{cm})=(0, 1)$. 本文下面就在 $N_h=N_p$ 的前提下, 构造$(H_{am}, H_{cm})=(0, 1)$ 的最优汉明相关序列族.

3　最优多项式跳频序列的构造和分析

定义 **3**[5]　设 p 为一个素数, m 为一个确定的整数, $m\in\{0, 1, \cdots, p-1\}$, $GF(p)$ 表示带有元素 0, 1, …, $p-1$ 的有限域, $g(x)$ 为 $GF(p)$ 上度为 r 的多项式, 如下:

$$g(x)=a_rx^r+mx^{r-1}+a_{r-2}x^{r-2}+\cdots+a_1x+a_0 \tag{7}$$

其中, $a_r\neq0$, a_{r-2}, …, $a_0\in GF(p)$. 基于多项式 $g(x)$, 除有系数 m 的那一项不变外, 简单的改变式(7)的每一项 $a_i(i=0, 1, \cdots, r-2, r)$来构造跳频序列 $C=\{C^{(f)}\}$:

$$C^{(f)}=\{c_n^{(f)}\},$$

$$c_n^{(f)}=g(n)\bmod p,\ n=0, 1, \cdots, p-1, f=1, 2, \cdots, (p-1)p^{r-1} \tag{8}$$

$C=\{C^{(f)}\}$为一族跳频序列, 序列长度为 p 且族尺寸为 $(p-1)p^{r-1}$. 但是如果只是用了式(7)的某些项, 例如, 不算带有特定系数 m 的那一项外如果有 t 项的话, 那么一族跳频序列数为 $N_u=(p-1)p^{t-1}$, $1\leqslant t\leqslant r$.

引理 **1**[5]　给定两个合适的整数 $r\geqslant1$ 和 $m\in\{0, 1, \cdots, p-1\}$, 设 $C=\{C^{(f)}\}$为一族定义 3 中的多项式跳频序列, 有下列结论 $N_u=(p-1)p^{t-1}$, $1\leqslant t\leqslant r$; $N_h=N_p=p$; $H_{am}=r-1$; $H_{cm}=r$, 其中 t 为不包含带有特定系数那一项外的项数.

定理 **1**　设 $C=\{C^{(f)}\}$是定义 3 中 $r=2$ 时的一个跳频序列族, $g(x)=a_2x^2+mx+a_0$, $g'(x)=b_2x^2+mx+b_0$ 是其任意两个序列所对应的多项式, 则当 $a_2<b_2$ 时, 若 $a_0=b_0$, 那么当时 $m\geqslant\dfrac{-a_2b_2(p-1)}{a_2-b_2}$, $C=\{C^{(f)}\}$是一个最优跳频序列族; 当 $a_2<b_2$ 时, 若 $a_0<b_0$, 则当 $m\geqslant\dfrac{(a_0-b_0)(a_2-b_2)-a_2b_2(p-1)^2}{(a_2-b_2)(p-1)}$时, $C=\{C^{(f)}\}$是一个最优跳频序列族.

证明　先来看二次多项式确定的多项式序列汉明相关性, 由题设可得

$$g(x)-g'(x+\tau)=(a_2-b_2)x^2-2b_2\tau x+a_0-b_0-m\tau-b_2\tau^2 \tag{9}$$

由题设和定义 3, 以下的运算均在 $GF(p)$ 上进行. 不讨论 $a_2=b_2$, 若是那样多项式序列变为 1 次, 由引理 1 知, 形如 $g(x)=a_1x+m$ 所确定的多项式序列构成的序列族已经具有最优汉明相关性了. 由汉明互相关的定义 1 和定义 3 知, 判断多项式跳频序列之间的汉明相关性即是判断它们所对应的多项式方程 $g(x)-g'(x+\tau)=0$ 的解的个数. 不妨设 $a_2<b_2$, 则当方程 $g(x)-g'(x+\tau)=0$ 的判别式小于等于 0 的时候, 方程至多有 1 个解. 此时跳频序列族 $C=\{C^{(f)}\}$的最大互相关值 H_{cm}为 1, 最大自相关值 H_{am}为 0, (讨论 H_{am}可在式(9)中, 令 $a_i=b_i(i=0, 1, 2)$, 易见此时式(9)在上 $GF(p)$ 无解) $C=\{C^{(f)}\}$为一个最优跳频序列族. 方程 $g(x)-g'(x+\tau)=0$ 的判别式为:

$$\Delta=4b_2^2\tau^2-4(a_2-b_2)(a_0-b_0-m\tau-b_2\tau^2) \tag{10}$$

令 $\Delta\leqslant0$, 整理得到 1 个关于 τ 的一元二次不等式:

$$a_2b_2\tau^2+m(a_2-b_2)\tau-(a_0-b_0)(a_2-b_2)\leqslant0 \tag{11}$$

由引理 1 知, $N_p=p$, 所以 $\tau\in\{0, 1, \cdots, p-1\}$, 这样可得下面 2 个不等式:

(1) $-(a_0-b_0)(a_2-b_2)\leqslant0$

(2) $a_2b_2(p-1)^2+m(a_2-b_2)(p-1)-(a_0-b_0)(a_2-b_2)\leqslant0$

(Ⅰ)若, $a_0=b_0$, (1)显然成立, 由(2)得

$$m\geqslant\frac{-a_2b_2(p-1)}{a_2-b_2};$$

(Ⅱ)若 $a_0\neq b_0$, 则由(1)得 $a_0<b_0$, 由(2)得

$$m\geqslant\frac{(a_0-b_0)(a_2-b_2)-a_2b_2(p-1)^2}{(a_2-b_2)(p-1)}.$$

若是 $a_2>b_2$, 讨论方法同上, 当 $a_0=b_0$ 时 $m\geqslant$

$-\frac{a_2 b_2(p-1)}{a_2-b_2}$, m 取值无意义; 若 $a_0 \neq b_0$, 则由(1)得 $a_0 > b_0$, 由(2)得 $m \geqslant \frac{(a_0-b_0)(a_2-b_2)-a_2 b_2(p-1)^2}{(a_2-b_2)(p-1)}$.

证毕.

定理 **2** 设 $C=\{C^{(f)}\}$ 是定义 3 中 $r=3$ 时的一个跳频序列族, $g(x)=a_3x^3+mx^2+a_1x+a_0$, $g'(x)=b_3x^3+mx^2+b_1x+b_0$ 是其任意两个序列所对应的多项式, 则当 $a_1=b_1$ 且 m 小于 $\frac{3b_3(4a_3-b_3)(p-1)}{8(a_3-b_3)}-\frac{3(p-1)(a_3-b_3)-6(a_3-b_3)b_3(p-1)}{8(a_3-b_3)}$ 和 $\sqrt{3b_1b_3}$ 中的较小者时, $C=\{C^{(f)}\}$ 是一个最优跳频序列族.

证明 看 3 次多项式确定的多项式序列汉明相关性, 由题设知

$$\begin{aligned}g(x)-g'(x+\tau)&=(a_3-b_3)x^3-3b_3\tau x^2\\&+(a_1-b_1-2m\tau-3b_3\tau^2)x\\&+(a_0-b_0-m\tau^2-b_3\tau^3-b_1\tau)\end{aligned}\tag{12}$$

由题设和定义 3, 以下的运算均在 $GF(p)$ 上进行. 下面先推导方程 $g(x)-g'(x+\tau)=0$ 仅有一个解所需满足的条件, 方程 $g(x)-g'(x+\tau)=0$ 最多有一个解能保证 $C=\{C^{(f)}\}$ 的最大互相关值为 1. 设方程有一个解 c, 则 $g(x)-g'(x+\tau)$ 能被 $x-c$ 整除. 设

$$g(x)-g'(x+\tau)=(x-c)q(x)+r\tag{13}$$

且设

$$q(x)=c_2x^2+c_1x+c_0\tag{14}$$

$q(x)$ 的次数比 $g(x)-g'(x+\tau)$ 降低 1 次. 其中

$$c_2=a_3-b_3\tag{15}$$

$$c_1=cc_2-3b_3\tau\tag{16}$$

$$c_0=cc_1-3b_3\tau+(a_1-b_12m\tau-3b_3\tau^2)\tag{17}$$

$$\begin{aligned}r&=(a_3-b_3)c^3-3b_3\tau c^2+(a_1-b_1-2m\tau-3b_3\tau^2)c\\&+(a_0-b_0-m\tau^2-b_\tau^3-b_1\tau)=0\end{aligned}\tag{18}$$

下面假设方程还有另外一个不同于 c 的解 d, 推导这种情况不成立时需要满足的条件. 设

$$g(x)-g'(x+\tau)=(x-c)(x-d)(q'(x)+r')\tag{19}$$

则

$$q(x)=(q'(x)+r')(x-d)\tag{20}$$

由上式(14)~(17)知

$$\begin{aligned}q(x)&=x^2(a_3-b_3)+[c(a_3-b_3)-3b_3\tau]x\\&+c^2(a_3-b_3)-3cb_3\tau+a_1-b_1-3b_3\tau^2-2m\tau\end{aligned}\tag{21}$$

设 $a'(x)=d_1x+d_0$, 据多项式理论[6]可知

$$d_1=c_2=a_3-b_3\tag{22}$$

$$\begin{aligned}d_0&=dd_1+c(a_3-b_3)-3b_3\tau\\&=d(a_3-b_3)+c(a_3-b_3)-3b_3\tau\end{aligned}\tag{23}$$

$$\begin{aligned}r'&=dd_0+dc_0=d^2(a_3-b_3)+cd(a_3-b_3)-3b_3\tau d\\&+c^2(a_3-b_3)-3b_3\tau+a_1-b_1-3b_3\tau^2-2m\tau=0\end{aligned}\tag{24}$$

式(24)是一个关于 d 的一元二次方程, 当方程判别式小于 0 时, d 无解. 即

$$\begin{aligned}\Delta&=[c(a_3-b_3)-3b_3\tau]^2-4(a_3-b_3)-3cb_3\tau\\&+a_1-b_1-3b_3\tau^2-2m\tau<0\end{aligned}\tag{25}$$

整理得到 1 个关于 τ 的一元二次不等式:

$$\begin{aligned}&(12a_3b_3-3b_3^2)\tau^2+[6(a_3-b_3)cb_3+8(a_3-b_3)m]\tau\\&-[3c^2(a_3-b_3)^2+4(a_1-b_1)(a_3-b_3)]<0\end{aligned}\tag{26}$$

因为 $\tau\in\{0,1,\cdots,p-1\}$, 所以:

(1)当 $\tau=0$ 时,

$$-[3c^2(a_3-b_3)^2+4(a_1-b_1)(a_3-b_3)]<0\tag{27}$$

(2)当 $\tau=1-p$ 时,

$$\begin{aligned}&(12a_3b_3-3b_3^2)(1-p)^2+[6(a_3-b_3)cb_3+8(a_3-b_3)m]\\&(1-p)-[3c^2(a_3-b_3)^2+4(a_1-b_1)(a_3-b_3)]<0\end{aligned}\tag{28}$$

当 $a_1=b_1$ 时, 条件(1)即式(27)显然成立, 由条件(2)可得

$$m<\frac{3b_3(4a_3-b_3)(p-1)^2-3c^2(a_3-b_3)-6(a_3-b_3)cb_3(p-1)}{8(a_3-b_3)(p-1)}\tag{29}$$

因为 $c\in GF(p)$ 即 $c\in\{0,1,\cdots,p-1\}$, 当 $c=0$ 时, 由式(29)可得

$$b<\frac{3b_3(4a_3-b_3)(p-1)}{8(a_3-b_3)}\tag{30}$$

当 $c=p-1$ 时, 由式(29)可得

$$m<\frac{3b_3(4a_3-b_3)(p-1)-3(p-1)(a_3-b_3)-6(a_3-b_3)b_3(p-1)}{8(a_3-b_3)}\tag{31}$$

因为

$$\begin{aligned}&\frac{3b_3(4a_3-b_3)(p-1)-3(p-1)(a_3-b_3)-6(a_3-b_3)b_3(p-1)}{8(a_3-b_3)}\\&<\frac{3b_3(4a_3-b_3)(p-1)}{8(a_3-b_3)}\end{aligned}\tag{32}$$

所以, 当式(31)成立时由上面的分析知 $C=\{C^{(f)}\}$ 的最大互相关值 H_{am} 为 1.

下面我们来证明当 $m<\sqrt{3b_1b_3}$ 时, 跳频序列族 $C=\{C^{(f)}\}$ 的最大自相关值 H_{am} 为 0. 讨论 $C=\{C^{(f)}\}$ 的最大自相关值 H_{am}, 只需在式(12)中令 $g'(x)=g(x)$, 得下面方程

$$\begin{aligned}g(x+\tau)-g(x)&=3b_3\tau x^2+(2m\tau+3b_3\tau^2)x\\&+(+m\tau^2+b_3\tau^3+b_1\tau)=0\end{aligned}\tag{33}$$

当式(33)的判别式小于 0 时, 式(33)无解, 即 $C=\{C^{(f)}\}$

的最大自相关值H_{am}为 0. 由

$$\Delta = 9b_3^2\tau^4 + 4m^2\tau^2 - 12b_3^2\tau^4 - 12b_3b_1\tau^2 < 0 \quad (34)$$

可得

$$m < \frac{\sqrt{12b_1b_3 + 3b_3^2\tau^2}}{2} \quad (35)$$

因为 $\tau \in \{0, 1, \cdots, p-1\}$, 所以当 $\tau = 0$ 时, m 取得不等式(36)式右半部分的下界, 即可得 $\sqrt{3b_1b_3}$时, 跳频序列族 $C = \{C^{(f)}\}$的最大自相关值H_{am}为 0.

所以取式(31)和式(35)的交集, 可同时满足 $C = \{C^{(f)}\}$的最大互相关值为 1 和最大自相关值为 0, 即当 $a_1 = b_1$ 且 m 小于$\frac{3b_3(4a_3-b_3)(p-1)-3(p-1)(a_3-b_3)}{8(a_3-b_3)} - \frac{6(a_3-b_3)b_3(p-1)}{8(a_3-b_3)}$和 $\sqrt{3b_1b_3}$中的较小者时, $C = \{C^{(f)}\}$是一个最优跳频序列族. 证毕.

定理**2** 说明: 为了构造形如定义 3 中 $r = 3$ 时的一个最优跳频序列族, 可采取如下做法使构造简便: 取 $a_1 = b_1$, 根据所有可能的 a_i 和 b_i($i = 0, 1, 2$)值, 分别求出$\sqrt{3b_1b_3}$和$\frac{3b_3(4a_3-b_3)(p-1)-3(p-1)(a_3-b_3)}{8(a_3-b_3)} - \frac{6(a_3-b_3)b_3(p-1)}{8(a_3-b_3)}$的最小值进行比较, 取其较小者来确定 m 的取值范围.

4　新构造的跳频序列实例分析

为了便于理解上面的结论, 我们举一实例进行说明.

实例**1**　请构造定义 3 中 $r = 3$, $p = 7$ 的一个最优跳频序列族.

解　利用定理 2, 取 $a_1 = b_1 = 1$, 根据定义 3 可求出$\sqrt{3b_1b_3}$的最小值为$\sqrt{3}$, $\frac{3b_3(4a_3-b_3)(p-1)-3(p-1)(a_3-b_3)}{8(a_3-b_3)} - \frac{6(a_3-b_3)b_3(p-1)}{8(a_3-b_3)} = \frac{27a_3b_3}{4(a_3-b_3)} - \frac{9}{4}b_3 - \frac{9}{4}$的最小值为$\frac{18}{5}$, 据定理 2, 当 $m = 0$ 或 $m = 1$ 时, 可构造 $GF(7)$ 上的最优跳频序列族 C 如下:

$$C = \{C^{(f)}\} = \{c_n^{(i,j)}\}$$

$c_n^{(i,j)} = (in^3 + mn^2 + n + j) \bmod 7$, $i \leqslant i \leqslant 6$; $0 \leqslant j$, $n \leqslant 6$

其中 $N_u = (p-1) \times 2 \times p = 6 \times 2 \times 7 = 84$, $N_h = N_p = p = 7$, $H_{am} = 0$, $H_{cm} = 1$.

5　结论

通过以上定理和实例分析我们可以看出新构造的跳频序列族$(H_{am}, H_{cm}) = (0, 1)$, 所以是最优汉明相关序列族, 并且此构造方法简便易行, 有实用性. 因此新构造的序列族在军用抗干扰通信中具有较强的应用前景, 是一种比较理想的伪随机序列族.

参考文献:

[1] S Matsufuji, K Imamura. A spread-spectrum communication system protecting information data from interception[J]. IEEE Transactions on Information Theory. 2000, 46(4): 1691-1695.

[2] Y C Eun, S Y Jin, Y P Hong. Frequency hopping sequences with optimal partial autocorrelation properties[J]. IEEE Transactions on Information Theory. 2004, 50(10): 2438-2442.

[3] S H Kim, J S No. New families of binary sequences with low correlation[J]. IEEE Transactions on Information Theory. 2003, 49(11): 3059-3065.

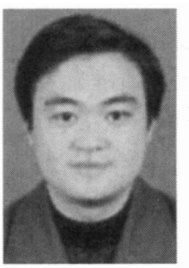
[4] R F Hara, Y Miao, M Mishima. Optimal frequency hopping sequences: a combinatorial approach[J]. IEEE Transactions on Information Theory. 2004, 50(10): 2408-2420.

[5] P Z Fan, Moon Ho Lee and Daiyuan Peng. New Family of Hopping Sequences for Time/Frequency-Hopping CDMA Systems[J]. IEEE Transactions on wireless communications, 2005, 4(6): 2836-2842.

[6] 张禾瑞, 郝　新. 高等代数[M]. 高等教育出版社, 北京, 1983. 9: 58-60.

作者简介:

刁哲军　男, 1961 年出生于河北辛集, 教授, 1982 年获南京理工大学学士学位, 研究方向为信息处理、智能检测、扩展频谱通信.
E-mail: Diaozhj@hebtu.edu.cn



陈嘉兴　(通信作者) 男, 1977 年出生于安徽, 哈尔滨工业大学工学博士, 副教授, 研究方向为扩展频谱通信、移动通信、信道编码.
E-mail: xinghuo2815@163.com

刘志华　女, 1977 年出生于河北沧州, 讲师, 2003 年获燕山大学计算机软件应用专业硕士学位, 研究方向为扩展频谱通信、网络安全.
E-mail: hebtuliuzhihua@163.com