广义平方素数码

刘青格 邵定蓉 李署坚
(北京航空航天大学电子信息工程学院 北京 100083)

摘 要：基于有限扩域与有限基域的对应关系，该文将素数码的构造思想延伸到有限扩域，基于有限扩域乘法，以一般二次既约多项式为模，构造出一类周期增大、序列数目增多的跳频序列族——广义平方素数码，该码具有理想汉明自相关特性和最大互相关值为 2 的几乎理想的汉明互相关特性。通过分组，得到具有最大互相关值为 1 的理想汉明互相关特性的跳频序列组。

关键词：素数码；跳频序列；广义平方素数码；有限扩域
中图分类号：TN914.4 **文献标识码**：A **文章编号**：1009-5896(2008)03-0652-04

General Quadratic Prime Codes

Liu Qing-ge Shao Ding-rong Li Shu-jian
(*School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics*, *Beijing* 100083, *China*)

Abstract: Based on the relationship between the extension Galois fields and the prime Galois fields, this paper presents a new construction of frequency-hopping sequences, here designated as general quadratic prime codes, by expanding the construct idea of prime codes to extension Galois fields. Taking a general quadratic irreducible polynomial as the module and based on the multiplication of extension Galois fields, quadratic prime codes with more sequences and longer period possess ideal Hamming autocorrelation and nearly ideal Hamming cross-correlation properties of no greater than two. Furthermore, general quadratic prime codes can be further partitioned to get frequency hopping sequences groups in which the maximum Hamming cross-correlation between any two FH sequences in the same group is at most one.

Key words: Prime code; Frequency-hopping sequence; General quadratic prime code; Extension Galois fields

1 引言

跳频通信中[1]，跳频序列的性能对跳频通信系统的性能有着决定性的影响[2]，寻求和设计具有理想性能的跳频序列族是研究跳频通信系统的重要课题之一[3,4]。素数码[5,6]是一类具有理想汉明相关性能的跳频序列族，是基于有限域 $\mathrm{GF}(P)$ 上的线性同余即模 P 乘构造的结果，基于素数码构造跳频序列族已成为跳频序列设计的一大分支[7−9]。级联素数码[9]是素数码序列时移、频移后级联得到的一类跳频序列族，是素数码在有限扩域 $\mathrm{GF}(P^2)$ 上的直观尝试性扩展。本文基于有限扩域 $\mathrm{GF}(P^2)$ 与有限域 $\mathrm{GF}(P)$ 的对应关系[10]，将素数码的构造思想直接延伸到 $\mathrm{GF}(P^2)$ 上，构造出一类新的跳频序列族，命名为广义平方素数码，序列长度增加到 P^2，序列数目增加到 P^2-1，具有自相关旁瓣为 0、最大互相关值为 2 的较理想汉明相关性能。说明一点，本文采用周期汉明相关来衡量跳频序列族的性能，简称汉明相关[1]。

文章内容作如下安排：首先对应素数码的构造，得出广义平方素数码的构造式；然后分析广义平方素数码的汉明相关特性；最后为得到具有理想汉明相关性能的跳频序列组，将广义平方素数码进行了分组，并证明同一组中序列具有理想汉明互相关性能；最后是结论。

2 广义平方素数码的构造

设素数码的构造式如下所示：

$$k(m,l)\equiv ml(\mathrm{mod}\,P),\quad 0\le m,l<P \tag{1}$$

其中 m 表示码字序号，l 表示时隙，k 表示序列 m 中时隙 l 对应的频隙，P 为素数。

基于有限域理论[10]，有限扩域 $\mathrm{GF}\left(P^2\right)$ 中的元素可以表示为 $\mathrm{GF}(P)$ 中元素的二维向量、一次多项式和 P 进制数。有限扩域 $\mathrm{GF}\left(P^2\right)$ 的乘法则是以 $\mathrm{GF}(P)$ 中元素为系数的一次多项式以某一二次既约多项式为模相乘实现。

根据以上分析，素数码是 $\mathrm{GF}(P)$ 中域乘法即模 P 乘构造得到的跳频序列，与此对应，分析 $\mathrm{GF}\left(P^2\right)$ 中域乘法即以二次既约多项式为模乘法运算的结果。以 $\mathrm{GF}(P)$ 中元素为系数的一次多项式表示新的跳频序列的各个参数，即 $m(x)=ax+b$，$l(x)=ix+j$ 及 $k(x)=k_1x+k_0$，分别对应于素数码中的码字序号 m，时隙 l 和频隙 k，其中 $a,b,i,j,k_1,k_0\in\mathrm{GF}(P)$。取

2006-08-14 收到，2007-06-18 改回

一般二次既约多项式 $f(x)=x^2-y_1x-y_0$ 对应于素数码构造式(1)中的素数 P，决定 $\mathrm{GF}\left(P^2\right)$ 的域乘法，其中 $y_1,y_0\in\mathrm{GF}\cdot(P)$ 且 $y_0\neq 0$。

由此，与素数码构造式(1)相对应，演绎出新的跳频序列的构造式

$$\begin{aligned}k[m(x),l(x)]&\equiv[m(x)l(x)]\bmod f(x)\\&\equiv\left[(ax+b)(ix+j)\right]\bmod\left(x^2-y_1x-y_0\right)\\&\equiv\left[aj\oplus\left(b\oplus y_1a\right)i\right]+\left(bj\oplus y_0ai\right)\end{aligned}\tag{2}$$

其中“$\oplus$”表示模 P 加，$a,b,i,j\in\mathrm{GF}(P)$。若 $(a,b)=(0,0)$，得到的序列为全零序列，因此，式(2)中 $(a,b)\neq(0,0)$。

为与一般跳频序列的表达相一致，将构造式(2)的多项式表示转换为二维向量表示，则新序列 $Q_{a,b}=\left(q_{a,b,0,0},q_{a,b,0,1},\cdots,q_{a,b,0,P-1},q_{a,b,1,0},q_{a,b,1,1},\cdots,q_{a,b,1,P-1},\cdots,q_{a,b,m,n},\cdots,q_{a,b,P-1,0},q_{a,b,P-1,1},\cdots,q_{a,b,P-1,P-1}\right)$ 的构造式为

$$q_{a,b,i,j}=\left[aj\oplus\left(b\oplus y_1a\right)i,bj\oplus y_0ai\right]\tag{3}$$

其中 (a,b)，(i,j) 和 $\left[aj\oplus\left(b\oplus y_1a\right)i,bj\oplus y_0ai\right]$ 分别为码字序号、时隙和频隙的二维向量表示，$(a,b)\neq(0,0)$，$y_1,y_0\in\mathrm{GF}(P)$ 且 $y_0\neq 0$。

由于新序列的长度为 P^2，而且以一般二次既约多项式为模构造，故在这里命名为广义平方素数码。从而，P^2-1 个长度为 P^2 的跳频序列得以构造。此外，式(3)中频隙 $\left[aj\oplus\left(b\oplus y_1a\right)i,bj\oplus y_0ai\right]$ 可以看作 P 进制表示，进而可以转换为十进制整数表示，即 $\left[aj\oplus\left(b\oplus y_1a\right)i\right]P+\left(bj\oplus y_0ai\right)$。

例 1　以 $P=5$ 和 $\mathrm{GF}(5)$ 上二次既约多项式 $f(x)=x^2+2x+3$ 为例，构造出 24 个长为 25 的跳频序列 $Q_{a,b}$，$(a,b)\neq(0,0)$。图 1 为以下序列的跳频图案。

$$\begin{aligned}Q_{2,3}=[&(0,0),(2,3),(4,1),(1,4),(3,2),(4,4),(1,2),\\&(3,0),(0,3),(2,1),(3,3),(0,1),(2,4),\\&(4,2),(1,0),(2,2),(4,0),(1,3),(3,1),\\&(0,4),(1,1),(3,4),(0,2),(2,0),(4,3)]\end{aligned}$$

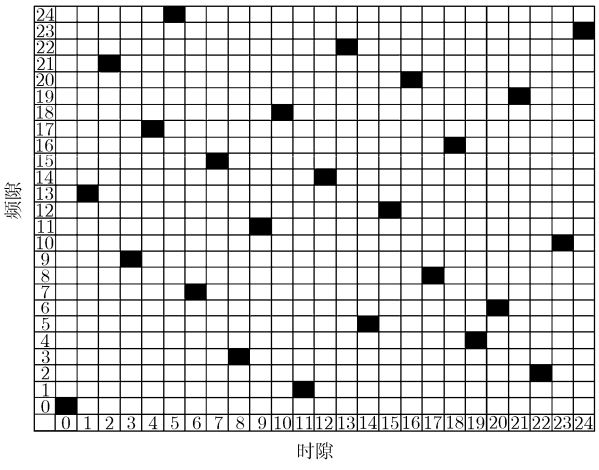

图 1　P=5 和 $f(x)=x^2+2x+3$ 的跳频图案 $Q_{2,3}$

对应的十进制整数表示为

$$\begin{aligned}Q_{2,3}=\big(&0,\ 13,\ \ 21,\ 9,\ 17,\ 24,\ 7,\ 15,\ 3,\ 11,\ 18,\ 1,\ 14,\\&22,\ 5,\ 12,\ 20,\ \ 8,\ \ 16,\ \ 4,\ \ 6,\ \ 19,\ \ 2,\ \ 10,\ \ 23\big)\end{aligned}$$

3　汉明相关性能

下面分析广义平方素数码的汉明相关性能，这是反映跳频序列性能的最主要方面[1]。

3.1 汉明自相关性能

定理 1　任一跳频序列的汉明自相关旁瓣为0。

证明　假设汉明自相关旁瓣不为 0，不妨设为 1，即设 $Q_{a,b}$ 与其移位序列 $Q'_{a,b}$ 存在一次碰撞，有

$$q_{a,b,i_1,j_1}=q_{a,b,i_1',j_1'}$$

其中 $(a,b)\neq(0,0)$ 且 $(i_1,j_1)\neq\left(i_1',j_1'\right)$。

由式(3)，得

$$\begin{aligned}&\left[aj_1\oplus\left(b\oplus y_1a\right)i_1,bj_1\oplus y_0ai_1\right]\\&\quad=\left[aj_1'\oplus\left(b\oplus y_1a\right)i_1',bj_1'\oplus y_0ai_1'\right]\end{aligned}$$

变换整理，得

$$a\left(j_1-j_1'\right)=\left(b+y_1a\right)\left(i_1'-i_1\right)\tag{4}$$

$$b\left(j_1-j_1'\right)=y_0a\left(i_1'-i_1\right)\tag{5}$$

式(4)与式(5)相乘，根据 $(a,b)\neq(0,0)$ 和 $\left(i_1,j_1\right)\neq\left(i_1',j_1'\right)$，变换整理得

$$b^2+y_1ab=y_0a^2\tag{6}$$

假设 $a=0$，式(6)成立只有 $b=0$，与 $(a,b)\neq(0,0)$ 相矛盾；

假设 $a\neq 0$，式(6)可变换为

$$y_0=\left(\frac{b}{a}\right)^2+y_1\left(\frac{b}{a}\right)\tag{7}$$

由 $f(x)=x^2-y_1x-y_0$ 为 $\mathrm{GF}(P)$ 上的二次既约多项式，根据既约多项式定义以及相关有限域理论[10]，$f(x)$ 除常量和它本身外没有其它因式因子。

将式(7)代入既约多项式 $f(x)$，得

$$\begin{aligned}f(x)&=x^2-y_1x-\left(\frac{b}{a}\right)^2-y_1\left(\frac{b}{a}\right)\\&=\left(x+\frac{b}{a}\right)\left(x-y_1-\frac{b}{a}\right)\end{aligned}$$

从而 $f(x)$ 可分解为一次多项式的乘积，与既约多项式的定义相矛盾。因此，跳频序列的汉明自相关旁瓣为 0，定理 1 得证。　　证毕

3.2 汉明互相关性能

定理 2　任意两个不同序列的最大汉明互相关值为 2。

为证明该定理，需首先证明一引理。

引理 1　对于任意两个不同序列 $Q_{a,b}$ 和 $Q_{a',b'}$，$(a,b)\neq\left(a',b'\right)$，任意时移 H 和频移 V，$H=h_1P+h_2$ 且 $h_1,h_2,V\in\mathrm{GF}(P)$，对于 $Q_{a,b}$ 中 $j+h_2<P$ 和 $j+h_2\geq P$ 分别最多存在一次碰撞，其中，j 为序列 $Q_{a,b}$ 中 $q_{a,b,i,j}$ 的时间位置的索引。

证明 假设对于任意两个不同序列 $Q_{a,b}$ 和 $Q_{a',b'}$，任意时移 H 和频移 V，对于 $j+h_2<P$ 至少存在两次碰撞，则有

$$q_{a,b,i_1,j_1}=q_{a',b',i_1',j_1'}\oplus V \tag{8}$$

$$q_{a,b,i_2,j_2}=q_{a',b',i_2',j_2'}\oplus V \tag{9}$$

同时成立。其中 $i_1'=i_1+h_1$，$i_2'=i_2+h_1$，$j_1'=j_1+h_2$，$j_2'=j_2+h_2$，且 $(i_1,j_1)\neq(i_2,j_2)$。

由式(3)，有

$$\begin{aligned}&\left[aj_1\oplus\left(b\oplus y_1a\right)i_1,bj_1\oplus y_0ai_1\right]\\&=\left[a'j_1'\oplus\left(b'+y_1a'\right)i_1',b'j_1'\oplus y_0a'i_1'\oplus V\right]\end{aligned} \tag{10}$$

$$\begin{aligned}&\left[aj_2\oplus\left(b\oplus y_1a\right)i_2,bj_2\oplus y_0ai_2\right]\\&=\left[a'j_2'\oplus\left(b'\oplus y_1a'\right)i_2',b'j_2'\oplus y_0a'i_2'\oplus V\right]\end{aligned} \tag{11}$$

式(10)，式(11)经变换整理得

$$y_0\left(a-a'\right)^2=\left(b-b'\right)^2+y_1\left(a-a'\right)\left(b-b'\right) \tag{12}$$

假设 $a'=a$，式(12)成立只有 $b=b'$，与 $\left(a,b\right)\neq\left(a',b'\right)$ 相矛盾；

假设 $a'\neq a$，式(12)可变换为

$$y_0=\left(\frac{b-b'}{a-a'}\right)^2+y_1\left(\frac{b-b'}{a-a'}\right) \tag{13}$$

将式(13)代入既约多项式 $f(x)$，有

$$f\left(x\right)=\left(x+\frac{b-b'}{a-a'}\right)\left(x-y_1-\frac{b-b'}{a-a'}\right)$$

由此，$f(x)$ 可分解为一次多项式的乘积，与既约多项式的定义相矛盾。从而，对于序列 $Q_{a,b}$ 中 $j+h_2<P$ 最多存在一次碰撞。同理可得，对于 $j+h_2\geq P$ 最多存在一次碰撞，引理 1 得证。 证毕

由引理 1，知对于序列 $Q_{a,b}$ 中 $j+h_2<P$ 和 $j+h_2\geq P$ 分别最多存在一次碰撞，因此总碰撞次数不会大于 2，即最大汉明互相关值为 2，定理 2 得证。 证毕

3.3 分组

为得到具有理想汉明相关性能的跳频序列，将 P^2-1 个序列分组，将所有码子序号 (a,b) 满足 $b\equiv ag(\mathrm{mod}\,P)$ 的序列分到 G_g 组，将所有 $a=0$ 的序列归为 G_P 组。这样，得到 $P+1$ 组，每组 $P-1$ 个序列。具体分组如下：

$$\left.\begin{aligned}G_0&=\left\{Q_{1,0},Q_{2,0},\cdots,Q_{P-1,0}\right\}\\G_1&=\left\{Q_{1,1},Q_{2,2},\cdots,Q_{P-1,P-1}\right\}\\&\vdots\\G_g&=\left\{Q_{1,g},Q_{2,2\otimes g},\cdots,Q_{P-1,(P-1)\otimes g}\right\}\\&\vdots\\G_{P-1}&=\left\{Q_{1,P-1},Q_{2,P-2},\cdots,Q_{P-1,1}\right\}\\G_P&=\left\{Q_{0,1},Q_{0,2},\cdots,Q_{0,P-1}\right\}\end{aligned}\right\} \tag{14}$$

其中 “$\otimes$” 表示模 P 乘，g 表示各个组的编号，$g\in\left\{0,1,2,\cdots,P\right\}$。

例 2 以 $P=3$ 和既约多项式 $f(x)=x^2+x+2$ 为例，构造广义平方素数码，共分为4组，见表1。表2为对应的十进制整数表示。

表1 $P=3$ 和 $f(x)=x^2+x+2$ 对应的4个分组

G_0	$Q_{1,0}=[(0,0),(1,0),(2,0),(2,1),(0,1),(1,1),(1,2),(2,2),(0,2)]$
	$Q_{2,0}=[(0,0),(2,0),(1,0),(1,2),(0,2),(2,2),(2,1),(1,1),(0,1)]$
G_1	$Q_{1,1}=[(0,0),(1,1),(2,2),(0,1),(1,2),(2,0),(0,2),(1,0),(2,1)]$
	$Q_{2,2}=[(0,0),(2,2),(1,1),(0,2),(2,1),(1,0),(0,1),(2,0),(1,2)]$
G_2	$Q_{1,2}=[(0,0),(1,2),(2,1),(1,1),(2,0),(0,2),(2,2),(0,1),(1,0)]$
	$Q_{2,1}=[(0,0),(2,1),(1,2),(2,2),(1,0),(0,1),(1,1),(0,2),(2,0)]$
G_3	$Q_{0,1}=[(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)]$
	$Q_{0,2}=[(0,0),(0,2),(0,1),(2,0),(2,2),(2,1),(1,0),(1,2),(1,1)]$

表 2 对应表 1 的十进制整数表示

G_0	$Q_{1,0}=[0\ 3\ 6\ 7\ 1\ 4\ 5\ 8\ 2]$
	$Q_{2,0}=[0\ 6\ 3\ 5\ 2\ 8\ 7\ 4\ 1]$
G_1	$Q_{1,1}=[0\ 4\ 8\ 1\ 5\ 6\ 2\ 3\ 7]$
	$Q_{2,2}=[0\ 8\ 4\ 2\ 7\ 3\ 1\ 6\ 5]$
G_2	$Q_{1,2}=[0\ 5\ 7\ 4\ 6\ 2\ 8\ 1\ 3]$
	$Q_{2,1}=[0\ 7\ 5\ 8\ 3\ 1\ 4\ 2\ 6]$
G_3	$Q_{0,1}=[0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8]$
	$Q_{0,2}=[0\ 2\ 1\ 6\ 8\ 7\ 3\ 5\ 4]$

定理3 同一组中不同序列间的最大汉明互相关值为1。

证明 假设同一组中任意两个不同序列 $Q_{a,b}$ 和 $Q_{a',b'}$，任意时移 $H=h_1P+h_2$ 和频移 V，存在两次碰撞，由引理1

$$q_{a,b,i_3,j_3}=q_{a',b',i_3',j_3'}\oplus V \tag{15}$$

$$q_{a,b,i_4,j_4}=q_{a',b',i_4',j_4'}\oplus V \tag{16}$$

同时成立。其中 $i_3'=i_3+h_1$，$j_3'=j_3+h_2$，$i_4'=i_4+h_1+1$，$j_4'=j_4+h_2-P$，且 $(i_3,j_3)\neq(i_4,j_4)$。

由式(3)，有

$$\begin{aligned}&\left[aj_3\oplus\left(b\oplus y_1a\right)i_3,bj_3\oplus y_0ai_3\right]\\&=\left[a'j_3'\oplus\left(b\oplus y_1a'\right)i_3',b'j_3'\oplus y_0a'i_3'\oplus V\right]\end{aligned} \tag{17}$$

$$\begin{aligned}&\left[aj_4\oplus\left(b\oplus y_1a\right)i_4,bj_4\oplus y_0ai_4\right]\\&=\left[a'j_4'\oplus\left(b'\oplus y_1a'\right)i_4',b'j_4'\oplus y_0a'i_4'\oplus V\right]\end{aligned} \tag{18}$$

对于任一给定组 G_g，$g\in\{0,1,2,\cdots,P\}$，有 $b\equiv ag\cdot(\mathrm{mod}\,P)$ 和 $b'\equiv a'g\left(\mathrm{mod}\,P\right)$ 同时成立。

式(17)，式(18)经变换整理得

$$\left(a-a'\right)\left(j_3-j_4\right)=\left(g+y_1\right)\left[\left(a'-a\right)\left(i_3-i_4-1\right)-a\right] \tag{19}$$

$$g\left(a-a'\right)\left(j_3-j_4\right)=y_0\left[\left(a'-a\right)\left(i_3-i_4-1\right)-a\right] \tag{20}$$

式(19)与式(20)相乘，根据$\left(a,b\right)\neq\left(a',b'\right)$和$\left(i_3,j_3\right)\neq\left(i_4,j_4\right)$，变换整理得

$$y_0=g^2+y_1g \tag{21}$$

将式(21)代入二次既约多项式$f(x)$，有

$$f(x)=(x+g)(x-y_1-g)$$

与既约多项式定义相矛盾。从而，同一组G_g，$g\in\{0,1,\cdots,P\}$，中任意两个不同序列的最大汉明互相关值为 1，定理 3 得证。　　证毕

因此，首选同一组中的序列分配给系统的用户。

4　结束语

本文以一般二次既约多项式为模，将素数码的构造思想直接延伸到有限扩域$\mathrm{GF}(P^2)$上，由$\mathrm{GF}(P^2)$的域乘法构造出一类跳频序列族——广义平方素数码，序列长度为P^2，序列数目为P^2-1，满足自相关旁瓣为 0 和最大汉明互相关值为 2 的较理想汉明相关特性。进一步通过分组，同一组中序列满足最大汉明互相关值为 1 的理想汉明相关特性。上述研究提供了跳频序列族的一种构造方法，对于素数码在有限扩域上的扩展具有重要理论意义。

参 考 文 献

[1] 梅文华, 王淑波, 邱永红等. 跳频通信[M]. 北京: 国防工业出版社, 2005: 28–84.
Mei W H, Wang S B, and Qiu Y H. Frequency Hopping Communications [M]. Beijing: China National Defense Industry Press, 2005: 28–84.

[2] Dixon R C. Spread Spectrum Systems [M]. 2nd Ed. New York: John-Wiley & Sons, 1976: 26–38.

[3] 梅文华, 杨义先, 周炯槃. 跳频序列设计理论的研究进展 [J]. 通信学报, 2003, 24(2): 92–101.
Mei W H, Yang Y X, and Zhou Q P. Survey of theoretical bounds and practical constructions for frequency hopping sequences [J]. *Journal of China Institute of Communications*, 2003, 24(2): 92–101.

[4] 彭代渊. 新型扩频序列及其理论界研究[D]. 成都: 西南交通大学, 2005: 81–101.
Peng D Y. Investigation of novel spreading sequences and their theoretical bounds. Chengdu: Southwest Jiaotong University, 2005: 81–101.

[5] Titlebaum E L. Time-frequency hop signals— Part I: Coding based upon the theory of linear congruences[J]. *IEEE Trans. on AES*, 1981, 17(4): 490–493.

[6] Shaar A A and Davies P A. Prime sequences: quasi-optimal sequences for OR channel code division multiplexing [J]. *Electronics Letters*, 1983, 19(21): 888–890.

[7] Kwong W C, Yang G C, and Zhang J G. 2^n prime codes and coding architecture for optical code-division multiple- access [J]. *IEEE Trans. on Communications*, 1996, 44(9): 1152–1162.

[8] Yang G C and Kwong W C. Prime Codes with Applications to CDMA Optical and Wireless Networks [M]. London: Artech House, 2002: 43–111.

[9] Chi-Fu Hong and Guu-Chang Yang. Concatenated prime codes [J]. *IEEE Communications Letters*, 1999, 3(9): 260–262.

[10] Rudolf L and Harald N. Finite Fields [M]. In Encyclopedia of Mathematics and Its Applications, vol. 20, Reading, MA: Addison-Wesley, 1983: 18–107.

刘青格：　女，1977 年生，博士生，研究方向为扩频通信.

邵定蓉：　男，1937 年生，教授，博士生导师，感兴趣的领域是通信与电子系统.

李署坚：　男，1952 年生，副教授，硕士生导师，研究方向为扩频通信.