第 14 卷 第 6 期　　电 子 科 学 学 刊　　Vol. 14. No. 6
1992 年 11 月　　JOURNAL OF ELECTRONICS　　Nov., 1992

跳 频 码 设 计 新 方 法*

杨 义 先
(北京邮电学院,北京 100088)

摘要　本文首次将有限域中的置换多项式引入跳频码的设计之中，并给出了若干类自相关和互相关特性都很好的全频道跳频码. 例如文中第 2 类码是目前已知的各方面综合性能最好的全频道跳频码.

关键词　编码;跳频码;置换多项式

一、引　　言

近年来人们在跳频码和其它最佳离散信号的设计方面作了大量的工作[1-11]. 到目前为止比较重要的跳频码有以下几类:(1)1981 年提出的基于线性同余式的跳频码(LCC)[1]; (2) 1981 年提出的基于二次同余式的跳频码 (QCC)[2]; (3) 1981 年提出的基于 R-S 码的跳频码 (R-SCC)[10]; (4) 1984 年提出的基于指数函数的跳频码 (ECC 又称为 Costas 阵列)[7-9]; (5) 1988 年提出的基于扩张二次同余式的跳频码 (EQCC)[4] 和 (6) 1990 年提出的基于三次同余式的跳频码 (CCC)[6], 等等. 综合考虑以上各种跳频码，不难看出它们都各有优缺点. LCC 虽然具有良好的互相关特性，但是其自相关特性却很差[1]. QCC 和 EQCC 的自相关和互相关特性虽然都很好，但是它们又都不是全频道码，实际上它们仅用到 $(N-1)/2$ 个频道而造成其它 $(N+1)/2$ 个频道的浪费[2-5]. Costas 阵列的自相关特性很好，而且又是全频道码，但是却难以找出码字个数较多且互相关特性也很好的 Costas 阵列[7-9]. R-SCC 也不是全频道码. 因此从自相关、互相关和全频道三个方面来考虑，CCC 是以上几类跳频码中综合性能最好的跳频码[6].

本文首次将有限域中的置换多项式引入跳频码的设计，得到了若干类自相关和(或)互相关特性很好的全频道跳频码. 特别是文中的第二类跳频码是与 CCC 具有相同的相关特性的全频道码，而且其码字个数还远远多于 CCC, 因此文中的第二类码是目前已知的综合性能最好的全频道跳频码.

二、预 备 知 识

跳频码的表达方式有很多种，其中最方便的一种是用 $N \times N$ 阶的二进制矩阵 $A=$

1991.10.23 收到，1992.07.06 定稿
* 国家青年自然科学基金资助课题.

(a_{km})，$1 \leqslant k, m \leqslant N$ 来表示．这里矩阵 A 的 N 个行代表 N 个频道，N 个列代表 N 个时间段．如果在第 t_m 个时间段中传送频率 f_k 那么就取 a_{km} 为 1，否则取 a_{km} 为 0．显然矩阵 A 还可以用一个名为置位算子 $y(k)$ 的映射按如下方式唯一确定：$a_{km}=1$ 当且仅当 $k=y(m)$，否则 $a_{km}=0$．这里 $y(k)$ 实际上是集合 $\{0,1,\cdots,N-1\}$ 到自身的一个映射．

如果 $y(k)$ 是集合 $\{0,1,\cdots,N-1\}$ 中的一个置换(即 1 对 1 映射)，那么就称相应的跳频码为全频道码．全频道特性也是评价跳频码好坏的一个重要指标，因为非全频道码一方面在某个时间段可能发送几个频率，另一方面又有一些频道闲置不用造成浪费．当然跳频码的最重要评价指标是它们的相关特性．设 $A=(a_{ij})$ 和 $B=(b_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ 是两个 $N \times N$ 阶跳频码，称

$$C(r,s)=\sum_{i,j=0}^{N-1} a_{ij}b_{(i+r)(j+s)}, \quad (|r| \leqslant N-1, |s| \leqslant N-1)$$

为 A 和 B 的互相关函数，特别当 $A=B$ 时就称之为自相关函数．需要强调的是此处只考虑非循环相关，即当 $i+r$ 或 $j+s$ 不属于集合 $\{0,1,\cdots,N-1\}$ 时就令 $b_{(i+r)(j+s)}=0$．

若用置位算子表示跳频码，那么如下的差分函数是研究相关特性的重要手段．

定义 1　置位算子 $y_1(k)$ 和 $y_2(k)$，$(k=0,1,\cdots,N-1)$ 的差分函数定义为

$$(y_2\Delta y_1)(k;t,w)=y_2(k+t)+w-y_1(k) \tag{1}$$

这里 $0 \leqslant k \leqslant N-1$，$-N+1 \leqslant t, w \leqslant N-1$，并且 t 和 w 分别表示时间和频率移位．在(1)式中当 k 不属于集合 $\{0,1,\cdots,N-1\}$ 时，就令 $y(k)=0$．

引理 1[6]　若跳频码 A 和 B 的置位算子分别是 $y_1(k)$ 和 $y_2(k)$，$(0 \leqslant k \leqslant N-1)$，那么相关函数 $C(r,s)$ 的取值不会超过差分函数 $(y_2\Delta y_1)(k;r,s)$ 的关于 k 的零点个数．这里 A 与 B 可能相同也可能相异．以下我们不加区分地使用跳频码 A 和置位算子 $y(k)$ 这两个等价术语．

设计优良跳频码的关键是要找出一组 $N \times N$ 阶的码矩阵 $A_1, A_2, \cdots, A_m$ 使得它们的自相关和(或)互相关函数尽可能地接近一个脉冲函数．由引理 1 知需要使相应置位算子 $y_1(k), \cdots, y_m(k)$ 的差分函数的零点个数尽可能少．为此我们再介绍一些有限域中的

表 1　有限域中的低阶置换多项式

(1) $f(x)=x$，任意 GF(q)	(2) $f(x)=x^2$，GF(2^m)
(3) $f(x)=x^3$，GF(q)　$\not\equiv 1 \bmod 3$	(4) $f(x)=x^3-ax$，(a 非平方)，GF(3^m)
(5) $f(x)=x^4+a_1x^2+a_2x$，(若 $f(x)$ 在 GF(q) 中仅有 0 根)，GF(2^m)	(6) $f(x)=x^5$，GF(q)，$q \not\equiv 1 \bmod 5$
(7) $f(x)=x^5-ax$，(a 非 4 次方)，GF(q)，$q \equiv 0 \bmod 5$	(8) $f(x)=x^5-ax^3+5^{-1}a^2x$，(a任取)，GF(q)，$q \equiv \pm 2 \bmod 5$
(9) $f(x)=x^5-2ax^3+a^2x$，(a 非平方)，GF(q)，$q \equiv 0 \bmod 5$	(10) $f(x)=x^4+3x$ 和 $g(x)=x^4-3x$，GF(7)
(11) $f_1(x)=x^5+2x^2$，$f_2(x)=x^5-2x^2$，$f_3(x;a)=x^5+ax^3+x^2+3a^2x$，($a$ 非平方)和 $f_4(x;b)=x^5+bx^3-x^2+3b^2x$，($b$非平方)，GF(7)	(12) $f(x;a)=x^5+ax^3+3a^2x$，(a 非平方)，GF(13)

置换多项式知识[11].

定义 2[11] 有限域 GF(q), ($q = p^m$, p 为素数)中的多项式 $g(x)$ 称为一个置换多项式,当且仅当映射 $c \to g(c)$ 构成 GF(q) 中元素的一个置换.

文献[11]的第 7 章对置换多项式进行了详细研究. 我们在此仅列出以下两个结论.

引理 2 如果 $f(x)$ 和 $g(x)$ 是 GF(q) 中的置换多项式,那么 $f(g(x))$ 和 $af(x+b)+d$, ($a \neq 0, a, b, d \in \mathrm{GF}(q)$) 也都是 GF($q$) 中的置换多项式.

引理 3 有限域中的低阶置换多项式(见文献[11]第 352 页的表 7.1). 表 1 中的各多项式都是相应有限域中的置换多项式.

三、基于 GF(p) 中置换多项式的跳频码

本节中只考虑 GF(p) (p 为素数)的情形. 利用以下的关键定理 1,我们将在本节中给出至少 8 类自相关和互相关特性都很好的全频道跳频码.

定理 1 设 $f(x)$ 和 $g(x)$是 GF(p) (p 为素数)中的两个置换多项式, 那么置位算子

$$y_1(k) \equiv f(k) \bmod p \tag{2a}$$

$$y_2(k) \equiv g(k) \bmod p \tag{2b}$$

($0 \leqslant k \leqslant p-1$) 都是全频道码,其相关特性为:

(1) 若 $\deg(f(x)) \geqslant 2$ 那么全频道码 $y_1(k) \equiv f(k) \bmod p$ 的自相关函数的旁瓣值不超过 $\deg(f(x)) - 1$.

(2) 全频道码 $y_1(k) \equiv f(k) \bmod p$ 和 $y_2(k) \equiv g(k) \bmod p$ 的互相关函数值不超过 $\max\{\deg(f(x)), \deg(g(x))\}$. 这里 $\deg(\cdot)$ 表示多项式的阶数.

充分利用定理 1 和已知的 GF(p) (p 为素数)中的阶数很小的置换多项式,我们就可以得到如下 8 类自相关和互相关特性都很好(第 1 类除外)的全频道码. 这里需要强调的是定理 1 中的设计方法仅在 GF(p) (p 为素数)域中有效, 而在一般有限域 GF(p^m) (p 为素数, $m \geqslant 2$) 中无效,详见下节的例 1. 另外在定理 1 的(1)中 $\deg(f(x)) \geqslant 2$ 是不可缺少的条件,下面的第 1 类码将有助于理解其原因.

第1类码 它由置位算子类$\{y(k;a) \equiv ak \pmod p : a \neq 0 \bmod p\}$,($0 \leqslant k \leqslant p-1$, p 是任意素数)组成. 其互相关特性很好,实际上其互相关函数值不超过 1. 但是其自相关特性却较差. 实际上此类码就是引言中曾提到过的 LCC 码[1]. (此类码可由定理 1 和引理 3(1) 得到.)

第 2 类码 它是由置位算子类 $\{y(k;a,b,d) \equiv [a(k+b)^3 + d] \bmod p : 0 < a \leqslant p-1,\ 0 \leqslant b,\ d \leqslant p-1\}$ (p 是满足 $p \equiv 2 \bmod 3$ 的素数)所组成的全频道码. 此类码的自相关函数的旁瓣值不超过 2,互相关函数值不超过 3. 此类码是由定理 1、引理 2 和引理 3(3) 得到的. 比较后可知,此类码的自相关和互相关特性都与 CCC[6] 相同,也都是全频道码. 但是第 2 类码中码字个数是 CCC 中码字个数的 p^2倍,因此它比 CCC 更好. 于是可知,此处的第 2 类码是到目前为止各方面综合性能最好的跳频码.

第 3 类码 它是由置位 算 子 类 $\{y_1(k;a,b,d) \equiv [a[(x+b)^4 + 3(x+b)] +$

(a_{km})，$1 \leqslant k, m \leqslant N$ 来表示．这里矩阵 A 的 N 个行代表 N 个频道，N 个列代表 N 个时间段．如果在第 t_m 个时间段中传送频率 f_k 那么就取 a_{km} 为 1，否则取 a_{km} 为 0．显然矩阵 A 还可以用一个名为置位算子 $y(k)$ 的映射按如下方式唯一确定：$a_{km}=1$ 当且仅当 $k=y(m)$，否则 $a_{km}=0$．这里 $y(k)$ 实际上是集合 $\{0,1,\cdots,N-1\}$ 到自身的一个映射．

如果 $y(k)$ 是集合 $\{0,1,\cdots,N-1\}$ 中的一个置换(即 1 对 1 映射)，那么就称相应的跳频码为全频道码．全频道特性也是评价跳频码好坏的一个重要指标，因为非全频道码一方面在某个时间段可能发送几个频率，另一方面又有一些频道闲置不用造成浪费．当然跳频码的最重要评价指标是它们的相关特性．设 $A=(a_{ij})$ 和 $B=(b_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ 是两个 $N \times N$ 阶跳频码，称

$$C(r,s)=\sum_{i,j=0}^{N-1} a_{ij}b_{(i+r)(j+s)}, \quad (|r| \leqslant N-1, |s| \leqslant N-1)$$

为 A 和 B 的互相关函数，特别当 $A=B$ 时就称之为自相关函数．需要强调的是此处只考虑非循环相关，即当 $i+r$ 或 $j+s$ 不属于集合 $\{0,1,\cdots,N-1\}$ 时就令 $b_{(i+r)(j+s)}=0$．

若用置位算子表示跳频码，那么如下的差分函数是研究相关特性的重要手段．

定义 1　置位算子 $y_1(k)$ 和 $y_2(k)$，$(k=0,1,\cdots,N-1)$ 的差分函数定义为

$$(y_2 \Delta y_1)(k;t,w)=y_2(k+t)+w-y_1(k) \tag{1}$$

这里 $0 \leqslant k \leqslant N-1$，$-N+1 \leqslant t$，$w \leqslant N-1$，并且 t 和 w 分别表示时间和频率移位．在(1)式中当 k 不属于集合 $\{0,1,\cdots,N-1\}$ 时，就令 $y(k)=0$．

引理 1[6]　若跳频码 A 和 B 的置位算子分别是 $y_1(k)$ 和 $y_2(k)$，$(0 \leqslant k \leqslant N-1)$，那么相关函数 $C(r,s)$ 的取值不会超过差分函数 $(y_2 \Delta y_1)(k;r,s)$ 的关于 k 的零点个数．这里 A 与 B 可能相同也可能相异．以下我们不加区分地使用跳频码 A 和置位算子 $y(k)$ 这两个等价术语．

设计优良跳频码的关键是要找出一组 $N \times N$ 阶的码矩阵 $A_1, A_2, \cdots, A_m$ 使得它们的自相关和(或)互相关函数尽可能地接近一个脉冲函数．由引理 1 知需要使相应置位算子 $y_1(k), \cdots, y_m(k)$ 的差分函数的零点个数尽可能少．为此我们再介绍一些有限域中的

表 1　有限域中的低阶置换多项式

(1) $f(x)=x$，任意 GF(q)	(2) $f(x)=x^2$，GF(2^m)
(3) $f(x)=x^3$，GF(q)　$\neq 1 \bmod 3$	(4) $f(x)=x^3-ax$，(a 非平方)，GF(3^m)
(5) $f(x)=x^4+a_1x^2+a_2x$，(若 $f(x)$ 在 GF(q) 中仅有 0 根)，GF(2^m)	(6) $f(x)=x^5$，GF(q)，$q \neq 1 \bmod 5$
(7) $f(x)=x^5-ax$，(a 非 4 次方)，GF(q)，$q \equiv 0 \bmod 5$	(8) $f(x)=x^5-ax^3+5^{-1}a^2x$，(a任取)，GF(q)，$q \equiv \pm 2 \bmod 5$
(9) $f(x)=x^5-2ax^3+a^2x$，(a 非平方)，GF(q)，$q \equiv 0 \bmod 5$	(10) $f(x)=x^4+3x$ 和 $g(x)=x^4-3x$，GF(7)
(11) $f_1(x)=x^5+2x^2$，$f_2(x)=x^5-2x^2$，$f_3(x;a)=x^5+ax^3+x^2+3a^2x$，($a$ 非平方)和 $f_4(x;b)=x^5+bx^3-x^2+3b^2x$，($b$非平方)，GF(7)	(12) $f(x;a)=x^5+ax^3+3a^2x$，(a 非平方)，GF(13)

置换多项式知识[11].

定义 2[11] 有限域 GF(q), ($q = p^m$, p 为素数)中的多项式 $g(x)$ 称为一个置换多项式,当且仅当映射 $c \to g(c)$ 构成 GF(q) 中元素的一个置换.

文献[11]的第 7 章对置换多项式进行了详细研究. 我们在此仅列出以下两个结论.

引理 2 如果 $f(x)$ 和 $g(x)$ 是 GF(q) 中的置换多项式,那么 $f(g(x))$ 和 $af(x+b)+d$, ($a \neq 0, a, b, d \in \mathrm{GF}(q)$) 也都是 GF($q$) 中的置换多项式.

引理 3 有限域中的低阶置换多项式(见文献[11]第 352 页的表 7.1). 表 1 中的各多项式都是相应有限域中的置换多项式.

三、基于 GF(p) 中置换多项式的跳频码

本节中只考虑 GF(p) (p 为素数)的情形. 利用以下的关键定理 1,我们将在本节中给出至少 8 类自相关和互相关特性都很好的全频道跳频码.

定理 1 设 $f(x)$ 和 $g(x)$是 GF(p) (p 为素数)中的两个置换多项式, 那么置位算子

$$y_1(k) \equiv f(k) \bmod p \tag{2a}$$

$$y_2(k) \equiv g(k) \bmod p \tag{2b}$$

($0 \leqslant k \leqslant p-1$) 都是全频道码,其相关特性为:

(1) 若 $\deg(f(x)) \geqslant 2$ 那么全频道码 $y_1(k) \equiv f(k) \bmod p$ 的自相关函数的旁瓣值不超过 $\deg(f(x)) - 1$.

(2) 全频道码 $y_1(k) \equiv f(k) \bmod p$ 和 $y_2(k) \equiv g(k) \bmod p$ 的互相关函数值不超过 $\max\{\deg(f(x)), \deg(g(x))\}$. 这里 $\deg(\cdot)$ 表示多项式的阶数.

充分利用定理 1 和已知的 GF(p) (p 为素数)中的阶数很小的置换多项式,我们就可以得到如下 8 类自相关和互相关特性都很好(第 1 类除外)的全频道码. 这里需要强调的是定理 1 中的设计方法仅在 GF(p) (p 为素数)域中有效, 而在一般有限域 GF(p^m) (p 为素数, $m \geqslant 2$) 中无效,详见下节的例 1. 另外在定理 1 的(1)中 $\deg(f(x)) \geqslant 2$ 是不可缺少的条件,下面的第 1 类码将有助于理解其原因.

第1类码 它由置位算子类$\{y(k;a) = ak(\bmod p): a \neq 0 \bmod p\}$,($0 \leqslant k \leqslant p-1$, p 是任意素数)组成. 其互相关特性很好,实际上其互相关函数值不超过 1. 但是其自相关特性却较差. 实际上此类码就是引言中曾提到过的 LCC 码[1]. (此类码可由定理 1 和引理 3(1) 得到.)

第 2 类码 它是由置位算子类 $\{y(k;a,b,d) \equiv [a(k+b)^3 + d] \bmod p: 0 < a \leqslant p-1, 0 \leqslant b, d \leqslant p-1\}$ (p 是满足 $p \equiv 2 \bmod 3$ 的素数)所组成的全频道码. 此类码的自相关函数的旁瓣值不超过 2, 互相关函数值不超过 3. 此类码是由定理 1、引理 2 和引理 3(3) 得到的. 比较后可知,此类码的自相关和互相关特性都与 CCC[6] 相同,也都是全频道码. 但是第 2 类码中码字个数是 CCC 中码字个数的 p^2倍,因此它比 CCC 更好. 于是可知,此处的第 2 类码是到目前为止各方面综合性能最好的跳频码.

第 3 类码 它是由置位算子类 $\{y_1(k; a, b, d) \equiv [a[(x+b)^4 + 3(x+b)] +$

$d]\mathrm{mod}7: a \neq 0,\ 0 \leqslant b,\ d \leqslant 6\}$ 和 $\{y_2(k; a, b, d) \equiv [a[(x+b)^4 - 3(x+b)] + d] \mathrm{mod}7: 0 < a \leqslant 6,\ 0 \leqslant b,\ d \leqslant 6\}$ 组成的全频道码. 它的自相关函数旁瓣值不超过 3，互相关函数值不超过 4. 此类全频道码是由定理 1、引理 2 和引理 3(10)得到的. 虽然此类码的相关特性较好，但是它仍然不是好码，因为它只能传送 7 个频率.

第 4 类码　它是由置位算子类 $\{y_1(k;a,b,d) \equiv [a(k+b)^5 + d]\mathrm{mod}p: 0 < a \leqslant p-1,\ 0 \leqslant b,\ d \leqslant p-1\}$ 和 $\{y_2(k; a, b, d) \equiv [(a+b)^5 + r(k+b)^3 + 5^{-1}r^2(k+b)] + d]\mathrm{mod}p: 0 < a \leqslant p-1, 0 \leqslant r, b, d \leqslant p-1\}$，(素数 $p \equiv 2\mathrm{mod}5$) 组成的全频道码. 它的自相关函数旁瓣值不超过 4，互相关函数值不超过 5. 此类码是由定理 1、引理 2 和引理3(6)、3(8)得到的. 此类码的综合性能也很好.

第 5 类码　此类码是由定理 1、引理 2 和引理 3(6)、3(8)得到的. 它的置位算子类的形式与第 4 类码完全相同. 唯一的区别就是此时素数 p 满足 $p \equiv 3\mathrm{mod}5$，而不是第 4 类那样 $p \equiv 2\mathrm{mod}5$. 此类码是相关特性与第 4 类相同的全频道码，其综合性能也是十分理想的.

第 6 类码　它是由置位算子类$\{y(k; a, b, d) \equiv [a(k+b)^5 + d]\mathrm{mod}p: 0 < a \leqslant p-1, 0 \leqslant b, d \leqslant p-1\}$，(素数 $p \equiv 4\mathrm{mod}5$) 组成的全频道码. 它的自相关函数旁瓣值不超过 4，互相关函数值不超过 5. 此类码是由定理 1、引理 2 和引理 3(6) 得到的. 它也是一类综合性能很好的跳频码.

第 7 类码　它是由置位算子类 $\{y_1(k; a, b, d) \equiv [a[(k+b)^5 + 2(k+b)^2] + d]\mathrm{mod}7: 0 < a \leqslant 6,\ 0 \leqslant b,\ d \leqslant 6\}$；$\{y_2(k; a, b, d) \equiv [a[(k+b)^5 - 2(k+b)^2] + d]\mathrm{mod}7: 0 < a \leqslant 6, 0 \leqslant b, d \leqslant 6\}$；$\{y_3(k; a, b, d, r) \equiv [a[(k+b)^5 + r(k+b)^3 + (k+b)^2 + 3r^2(k+b)] + d]\mathrm{mod}7: 0 < a \leqslant 6, 0 \leqslant b, r, d \leqslant 6,\ r$ 非平方$\}$和 $\{y_4(k; a, b, d, r) \equiv [a[(k+b)^5 + r(k+b)^3 - (k+b)^2 + 3r^2(k+b)] + d]\mathrm{mod}7: 0 < a \leqslant 6, 0 \leqslant b, r, d \leqslant 6,\ r$ 非平方$\}$组成的全频道码. 它的自相关函数旁瓣值不超过 4，互相关函数值不超过 5. 与第 3 类码相似，此类码也不实用. 因为它只能传送 7 个频率. 此类码是由定理 1、引理 2 和引理 3(11) 得到的.

第 8 类码　它是由置位算子类 $\{y(k; a, b, d, r) \equiv [a[(k+b)^5 + r(k+b)^3 + 3r^2(k+b)] + d]\mathrm{mod}13: 0 < a \leqslant 12, 0 \leqslant b, d, r \leqslant 12,\ r$ 非平方$\}$组成的全频道码. 它的自相关函数旁瓣值不超过 4，互相关函数值不超过 5. 遗憾的是此类码只能传送 13 个频率，因此它也不实用.

至此，我们已经利用定理 1 的方法设计出了 8 类跳频码，其中第 2,4,5,6 类码都是各方面综合性能很理想的全频道跳频码. 实际上利用定理 1 的方法还可以得到更多的优良跳频码. 限于篇幅，不赘述.

四、基于 GF(p^m) 中置换多项式的跳频码

第三节考虑了 GF(p) 的情形，现在考虑一般有限域 GF(p^m) 的情形. 读者将很快发现当 $m \geqslant 2$ 时 GF(p^m) 的情形与 GF(p) 完全不同，此时相当复杂，需要精心分析.

设 $\{a_0,a_1,\cdots,a_{q-1}\}$ 表示有限域 GF(q)($q=p^m$) 中的所有 q 个元素. 给定 GF(q) 中的一个置换多项式 $g(x)$ 之后,便可以唯一地确定一个置位算子 $y(k)$, ($0\leqslant k\leqslant q-1$) 如下:

$$y(k)=m,\ \text{当且仅当}\ a_m=g(a_k) \tag{3}$$

这里 $0\leqslant k,\ m\leqslant q-1$.

对有限域 GF(p) (p 为素数),如果令 $a_i=i$,($0\leqslant i\leqslant p-1$) 那么由(3)式所得的置位算子就与(2)式相同. 并且由定理 1 还可以很容易地确定其相关特性. 当在 GF(p^m) ($m\geqslant 2$) 域中考虑时,情况就很复杂了,这时(3)式中置换多项式的阶数 $\deg(g(x))$ 与置位算子 $y(k)$ 的相关特性之间就不再有象定理 1 那样的简单关系了.

一般有限域 GF(q) 的最简单表达式为 $\{0,1=e^0,e^1,e^2,\cdots,e^{q-2}\}$, 这 e 里为 GF(q) 的一个本原元素. 即 $a_0=0$, $a_i=e^{i-1}$, ($1\leqslant i\leqslant q-1$). 在此表达方式之下,(3)式中的置位算子可以重写为

$$y(k)=\begin{cases}0, & \text{如果}\ g(a_k)=0\\ 1+\log[g(a_k)], & \text{其它}\end{cases} \tag{4}$$

此处 $\log(x)$ 是熟知的 GF(q) 中的离散对数函数,即 $\log(a)=b$, 当且仅当 $a=e^b$, (e 为 GF(q) 的本原元素).

例 1 由引理3(2)知 $g(x)=x^2$ 是域 GF(2^m) 中的二阶置换多项式. 由此按(4)式所得的置位算子为

$$y(k)=\begin{cases}0, & \text{当}\ k=0\\ 2k-1, & \text{当}\ 1\leqslant k\leqslant 2^{m-1}\\ 2k-2^m, & \text{当}\ 2^{m-1}+1\leqslant k\leqslant 2^m-1\end{cases} \tag{5}$$

经过简单计算不难看出,当移位值 (r,s) 分别取 $(2^{m-1},-1)$ 时, $y(k)$ 所对应的跳频码的自相关函数的旁瓣值高达 $2^{m-1}-1$. 由此可见, $y(k)$ 是一个自相关特性极差的跳频码.

由例 1 知,当在 GF(p^m) 中考虑问题时,即使是低阶置换多项式,也很难保证相应的跳频码有良好的相关特性. 下面通过仔细分析, 我们找到了几类自相关特性很好的全频道跳频码.

A1 类 它是由 GF(q) 中的置换多项式 $g(x;i,j)=e^ix+e^j$, ($0\leqslant i,j\leqslant q-2$) 按(4)式得到的置位算子:

$$y(k;i,j)=\begin{cases}1+j, & \text{当}\ k=0\\ 0, & \text{当}\ k=1+\log[(p-1)e^{j-i}]\\ 1+\log[e^{i+k-1}+e^j], & \text{其它}\end{cases}$$

这里 e 是有限域 GF(q) 中的本原元素. GF(q) 是任意有限域.

定理 2 A1 类是全频道跳频码,其自相关函数的旁瓣值不超过 5.

A2 类 它是由 GF(2^m) 中的置换多项式 $g(x)=e^ix^2+e^j$, ($0\leqslant i,j\leqslant q-2$, 见引理 2 和引理3(2)),按(4)式得到的置位算子:

$$y(k)=\begin{cases}1+j, & \text{当 } k=0\\ 0, & \text{当 } k=1+\{2^{m-1}\log[(p-1)e^{j-i}]\}\bmod(2^m-1)\\ 1+\log[e^{2(k-1)+i}+e^j], & \text{其它}\end{cases}$$

这里 e 是 GF(2^m) 中的本原元素.

定理 3　A2 类中的跳频码都是全频道码，并且其自相关函数的旁瓣值不超过 5.

实际上更一般地我们还有:

A3 类　由文献[11]第 351 页定理 7.8 知,当 $\gcd(n, q-1)$时，$g(x)=e^ix^n+e_j$ 是 GF(q) 中的置换多项式. 由此按(4)式就得到全频道码 A3 类的置位算子:

$$y(k)=\begin{cases}1+j, & \text{当 } k=0\\ 0, & \text{当 } k=\{n^{-1}\log[(p-1)e^{j-i}]\}(\bmod(q-1))+1\\ 1+\log[e^{n(k-1)+i}+e^j], & \text{其它}\end{cases}$$

这里 e 是 GF(q)($q=p^m$) 中的本原元素.

定理 4　A3 类中的跳频码都是全频道码,它的自相关函数的旁瓣值不超过 5.

与例 1 相反的是此处定理 4 利用高阶的 GF(q) 中的置换多项式得到了自相关特性非常好的全频道跳频码. 由此从另一方面说明了 GF(q) 中情况的复杂性. 此外不难看出,当 $n=1$ 和 2 时定理 4 就分别退化成定理 2 和 3.

A4 类　由引理3(4)知 $f(x)=e^i(x^3-ax)+e^j$, ($0\leqslant i,j\leqslant 3^m-2$, a 非平方) 是 GF(3^m) 中的置换多项式. 由此按(4)式所得的置位算子为

$$y(k)=\begin{cases}1+j, & \text{当 } k=0,\\ 0, & \text{当 } k=r,\ f(e^{r-1})=0\\ 1+\log[e^i[e^{3(k-1)}-ae^{k-1}]+e^j], & \text{其它}\end{cases}$$

定理 5　A4 类中的跳频码都是全频道码，并且其自相关函数的旁瓣值不超过 7.

A5 类　在 GF(2^m) 中引理 3(5) 中的函数 $g(x)$ 是置换多项式. 由此按(4)式得到的置位算子为

$$y(k)=\begin{cases}1+j, & \text{当 } k=0\\ 0, & \text{当 } k=r,\ e^ig(e^{r-1})+e^j=0\\ 1+\log[e^i(e^{4(k-1)}+a_1e^{2(k-1)}+a_2e^{k-1})+e^j], & \text{其它}\end{cases}$$

(这里 e 是 GF(3^m) 中的本原元素. $g(x), a_1, a_2$ 见引理 3(5))

定理 6　A5 类中的跳频码都是全频道码,并且自相关函数的旁瓣值不超过 8.

A6 类　设 $f(x)$ 是引理3(7)中的置换多项式 (GF(q), $q\equiv 0\bmod 5$), 由 $e^if(x)+e^j$, ($0\leqslant i,j\leqslant q-2$) 按(4)式得到的置位算子为

$$y(k)=\begin{cases}1+j, & \text{当 } k=0\\ 0, & \text{当 } k=r,\ e^if(e^{r-1})+e^j=0\\ 1+\log[e^i(e^{5(k-1)}-ae^{k-1})+e^j], & \text{其它}\end{cases}$$

这里 a 和 $f(x)$ 的含义见引理 3(7).

定理 7　A6 类中的跳频码都是全频道码，并且其自相关函数的旁瓣值不超过 9.

A7 类　设 $f(x)$ 是引理 3(8) 中的置换多项式(GF(q), $q\equiv\pm 2\bmod 5$), 由

$$e^if(x)+e^j,\ (0\leqslant i,j\leqslant q-2),$$

按(4)式得到的置位算子为

$$y(k)=\begin{cases}1+j, & \text{当 } k=0\\ 0, & \text{当 } k=r,\ e^{i}f(e^{r-1})+e^{j}=0\\ 1+\log[e^{i}(e^{5(k-1)}+ae^{3(k-1)}+5^{-1}a^{2}e^{k-1})+e^{j}], & \text{其他}\end{cases}$$

这里 a, $f(x)$ 等的含义见引理 3(8).

定理 8 A7 类中的跳频码都是全频道码，并且其自相关函数的旁瓣值不超过 9.

A8 类 设 $f(x)$ 是引理 3(9) 中的置换多项式 $(GF(q), q\equiv 0 \bmod 5)$，由

$$e^{i}f(x)+e^{j},\quad (0\leqslant i,j\leqslant q-2),$$

按(4)式得到的置位算子为

$$y(k)=\begin{cases}1+j, & \text{当 } k=0\\ 0, & \text{当 } k=r,\ e^{i}f(e^{r-1})+e^{j}=0\\ 1+\log\{e^{i}[e^{5(k-1)}-2ae^{3(k-1)}+a^{2}e^{k-1}]+e^{j}\}, & \text{其它}\end{cases}$$

这里 a, $f(x)$ 等的含义见引理 3(9).

定理 9 A8 类中的跳频码都是全频道码，并且其自相关函数的旁瓣值不超过 9.

实际上还可以证明如下一般结果.

定理 10 如果 $f(x)=a+bx+\sum_{i=2}^{n}c_{i}x^{i}$ 是 $GF(q)$ 中的一个置换多项式，并且 $a\neq 0$, $b\neq 0$. 那么与 $f(x)$ 相对应的置位算子:

$$y(k)=\begin{cases}1+\log a, & \text{当 } k=0\\ 0, & \text{当 } k=r,\ f(e^{r-1})=0\\ 1+\log[f(e^{k-1})], & \text{其它}\end{cases}$$

就构成一个全频道跳频码，并且它的自相关函数的旁瓣值不超过 $4+\deg(f(x))$.

参 考 文 献

[1] E. Titlebaum, *IEEE Trans. on AES*. **AES**-17(1981)4, 490—493.
[2] E. Titlebaum et al., *IEEE Trans. on AES*, **AES**-17(1981)4, 494—499.
[3] E. Titlebaum et al., *IEEE Trans. on AES*, **AES**-27(1991)1, 18—29.
[4] J. Bellegarda et al., *IEEE Trans. on AES*, **AES**-24(1988)6, 726—742.
[5] J. Bellegarda et al., *IEEE Trans. on AES*, **AES** 27(1991)1, 167—172.
[6] S. Maric et al., *IEEE Trans. on AES*, **AES**-26(1990)6, 1035—1039.
[7] S. Golomb et al., *Proc. IEEE*, **72**(1984)9, 1143—1163.
[8] D. Drumheller et al., *IEEE Trans. on AES*, **AES** 27(1991)1, 2—10.
[9] 杨义先，电子科学学刊，**13**(1991)4，351—357.
[10] R. Mersereau et al., *IEEE Trans. on AES*. **AES**17(1981)4, 571—578.
[11] R. Lidl et al., Finite Fields, Addison-Wesley Publishing Company, (1983).

A NEW METHOD FOR THE DESIGN OF FULL FREQUENCY HOP CODES

Yang Yixian

(Beijing University of Posts and Telecommunications, Beijing 100088)

Abstract　Permutation polynomials in finite fields are initially introduced into the design of full frequency hop codes. Various kinds of full frequency hop codes with ideal auto-and cross-ambiguity functions are presented in this paper. For example, the codes of class 2 are the best full frequency hop codes up to now.

Key words　Coding; Frequency hop codes; Permutation polynomials