中山大学学报 (自然科学版)
第 36卷 增 刊 ACTA SCIENTIARUM NATURALIUM Vol. 36 Suppl.
1997年 6月 UNIVERSITATIS SUNYATSENI Jun. 1997

周期为素数 $q=4t+1$序列的伪随机性能分析*

王永澄
(南京航空航天大学电子工程系, 南京 210016)

摘 要 分析了有限域中二次元素的某些性质并介绍了长度为奇素数的伪随机序列的构造, 证明了这些序列的自相关函数, 推导出素数 $q=4t+1$序列的功率谱密度表达式, 分析了它们的游程特性.

关键词 有限域, PN序列, 自相关函数, 功率谱密度
分类号 TP 14

伪随机序列在电子技术各领域得到广泛的应用, 常用的伪随机序列是 m序列和 M序列,但是它们的长度受限于 2^r-1或 2^r(r是大于 1的整数).在有限域理论基础上,可以构成周期长度为奇素数的伪随机序列.本文介绍周期为素数 $q=4t+1$序列的构成和它的随机性能分析,着重分析这些序列的功率谱和游程特性.

1 奇素数有限域、二次元素和二次特征函数

奇素数 q是大于 2的素数,可以表达为素数 $q=4t+1$和素数 $q=4t-1$两种形式 (t为正整数).奇素数有限域 $GF(q)$上的二次元素是满足下式的整数:

$$n\equiv Z_i^2 \pmod q,\ Zi\in GF(q)\text{ 且 }Z_i\neq 0 \tag{1}$$

不满足此式之整数称为非二次元素. 在 $GF(q)=(0,1,\cdots,q-1)$的非零元素中,有一半是二次元素,这些二次元素的集合可用 D表示;另一半是非二次元素,这些非零的非二次元素集合可用 $\overline{D}$表示.奇素数有限域 $GF(q)$上的二次特征函数 $J(z)$定义为[1]:

$$J(z)=\begin{cases}0, & z=0\\ 1, & z\in D\\ -1, & z\in \overline{D}\end{cases} \tag{2}$$

二次特征函数 $J(z)$有如下性质[2]:

$$\sum_{z\in GF(q)} J(z)(z+a)=-1,\qquad a\in GF(q),a\neq 0 \tag{3}$$

$$J(z)=J(-z),\qquad z\in GF(q),q=4t+1 \tag{4}$$

为了下面分析, 我们证明二次元素还有如下性质.

* 收稿日期: 1997-02-05 王永澄, 男, 56岁, 副教授

性质 1 在奇素数有限域 $GF(q)$ 的非 0元素集合 $GF^*(q)=(1,\cdots,q-1)$ 中，若 $q=4t+1$，则二次元素是对称分布的，即：

$$\begin{cases} q-a\in D, & a\in D \\ q-a\in \overline{D}, & a\in \overline{D} \end{cases} \tag{5}$$

其中 D 为二次元素集合.

证明 由 $q=4t+1$，根据(4)式，则有 $J(a)=J(-a)\rightarrow J(a)=J(q-a)$

故若 $a\in D$ 则 $q-a\in D$；若 $a\in \overline{D}$ 则 $q-a\in \overline{D}$.即(5)式.

性质 2 设 D 为奇素数有限域 $GF(q)$ 的二次元素集合，D 为非 0的二次元素集合，则

$$\text{若 } a,b\in D, \quad \text{则 } ab\in D \tag{6}$$

$$\text{若 } a,b\in \overline{D}, \quad \text{则 } ab\in D \tag{7}$$

$$\text{若 } a\in D, b\in \overline{D}, \quad \text{则 } ab\in \overline{D} \tag{8}$$

证明 有限域 $GF(q)$ 非 0元素集合 $GF^*(q)$ 是循环乘法群，设 T 为乘法群的生成元，则 $T^{q-1}=1$，根据式(1)的二次元素定义，二次元素必为生成元 T 的偶次幂，而 T 的奇次幂不是二次元素.设 $a=T^i, b=T^j$，若 $a,b\in D$，则 i,j 均为偶数，$i+j$ 也为偶数.如果 $i+j\leqslant q-2$，则 $ab=T^{i+j}\in D$.如果 $i+j\geqslant q-1$，设 $i+j\equiv r(\mathrm{mod}\, q-1)$，$0\leqslant r<q-1$.因为 $q-1$ 是偶数，则 r 仍为偶数.考虑到 $T^{q-1}=1$，所以 $ab=T^{i+j}=T^r\in D$.(6)式得证.以此类推可证(7)，(8)式.

2 长度为奇素数的伪随机序列的结构及产生

设奇素数有限域为 $GF(q)=\{0,1,\cdots,q-1\}$ 构成对应的序列

$$A=\{a_i\}=\{a_0,a_1,\cdots,a_{q-1}\}=\{-1,J(1),J(2),\cdots,J(q-1)\} \tag{9}$$

例 $q=13=4t+1, t=3$

奇素数有限域为 $GF(13)=(0,1,2,\cdots,12)$，$GF(13)$ 中二次元素集合 D 和非二次元素集合 $\overline{D}$ 分别为：

$$D=\{1,3,4,9,10,12\}, \quad \overline{D}=\{2,5,6,7,8,11\}$$

构成长度为 13的序列为：

$$\begin{aligned} A&=\{-1,\Psi(1),\Psi(2),\cdots,\Psi(12)\} \\ &=\{-1,1,-1,1,1,-1,-1,-1,-1,1,1,-1,1\} \end{aligned}$$

此序列是关于首项 -1 对称的，即，$J(1)=J(12), J(2)=J(11),\cdots$.

3 素数 $4t+1$ 序列的自相关函数和功率谱

素数 $4t+1$ 序列的自相关函数 $R(f)$ 为三值函数[1]：

$$R(f)=\begin{cases} 1 & f=0 \\ -3/q & f\in D \\ 1/q & f\in \overline{D} \end{cases} \tag{10}$$

从自相关函来看，这种 $q=4t+1$ 的素数序列有着良好的类似噪声的性质.下面还可从功率谱和游程特性进一步证实这个结论.

周期波形的功率谱与与自相关函数是一组富氏变换对，对自相关函数进行富氏变换可

求得奇素数序列的功率谱.设这种序列对应的二进制码元宽度为 t_0,序列的自相关函数是三值的,如图 1所示.

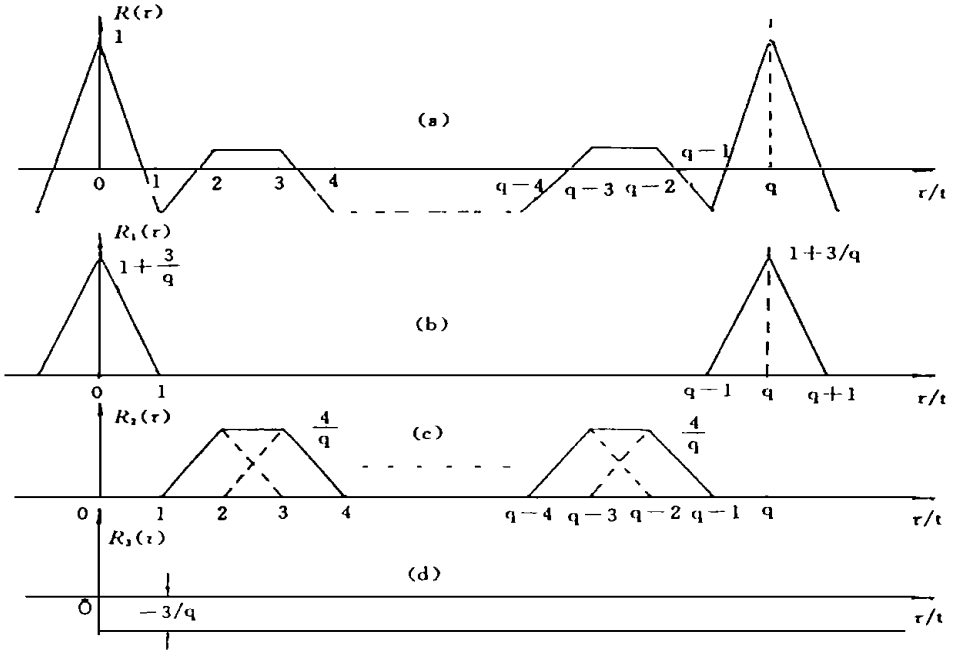

图 1 周期 $q=4t+1$序列自相关波形

图中假设 $1,4,\cdots\in D$; $2,3,\cdots\in\overline{D}$,将自相关函数 $R(\tau)$ 分解为如图 (b, c, d) 3个波形. $R(\tau)=R_1(\tau)+R_2(\tau)+R_3(\tau)$,其中,$R_1(\tau)$ 是一个三角形脉冲串,位于 $\tau=mqt_0$ 处,$m=0,1,2,\cdots$.每个三角形底为 $2t_0$,高为 $1+3/q$. $R_2(\tau)$ 是 $(q-1)/2$个三角形脉冲串,每个三角形顶点位于 $\tau/t_0=i$ 处,$i\in\overline{D}$,图 1b中 $i=2,3,\cdots,q-3,q-2$),三角形底为 2,高为 $4/q$. $R_3(\tau)$ 处是一直线,位于 $-3/q$处.求解 $R_j(\tau)$,$j=1,2,3$的富氏变换,就可得到序列的功率谱 $S_j(f)$,$(j=1,2,3)$.

$$S_1(f)=\frac{q+3}{q^2}\left(\frac{\sin\pi ft_0}{\pi ft_0}\right)^2\sum_{n=-\infty}^{\infty}W\left(f-\frac{c}{qt_0}\right)$$

$$S_2(f)=\frac{4}{q^2}\sum_{i\in\overline{D}}(\exp(-j2\pi fit_0))\left(\frac{\sin\pi ft_0}{\pi ft_0}\right)^2\sum_{n=-\infty}^{\infty}W\left(f-\frac{c}{qt_0}\right)$$

$$S_3(f)=-\frac{3}{q}W(f)$$

其中 $S_2(f)$中每一项乘以相应的因子 $\exp(-j2\pi fit_0)$.这是因为 $R_2(\tau)$每个三角形相对于原点有一位移 $\tau=i$,这里 i不是二次元素,即 $i\in\overline{D}$.由此可得奇素数 $q=4t+1$序列的功率谱

$$S(f)=\left[\frac{q+3}{q^2}+\frac{4}{q^2}\sum_{i\in\overline{D}}(\exp(-j2\pi fit_0))\right]\left(\frac{\sin\pi ft_0}{\pi ft_0}\right)^2\sum_{n=-\infty}^{\infty}W\left(f-\frac{n}{qt_0}\right)-\frac{3}{q}W(f)\quad(11)$$

考虑离散谱线处的频率 $f=n/qt_0$.按照 (5) 式,有 $i\in\overline{D}$,$q-i\in\overline{D}$,则:

$$\sum_{i\in D}(\exp(-j2\pi fit_0)=\sum_{i\in D}(\exp(-j2\pi ni/q)=\sum_{i\in D}\cos(2\pi ni/q) \tag{12}$$

在不同谐波次数 n 处, (12), (11) 式表达如下:

(1) 当 $n=0$ 时 $\sum_{i\in D}\cos(2\pi ni/q)=(q-1)/2$; $S(0)=1/q^2$

(2) 当 $n(\mathrm{mod}\ q)\in D$ 时,因为 $i\in \overline{D}$,设 $k=ni$,按照 (8) 式,则 $k(\mathrm{mod}\ q)\in \overline{D}$,

$$\sum_{i\in D}\cos(2\pi ni/q)=\sum_{k\in \overline{D}}\cos(2\pi k/q)$$

$$S(f)=C_1\left(\frac{\sin\pi ft_0}{\pi ft_0}\right)^2\sum_{n=-\infty}^{\infty}W\left(f-\frac{n}{qt_0}\right)$$

其中 $$C_1=\frac{q+3}{q^2}+\frac{4}{q^2}\sum_{k\in \overline{D}}\cos\left(2\pi\frac{k}{q}\right)$$

(3) 当 $n(\mathrm{mod}\ q)\in \overline{D}$,按照 (7),使用上面类似方法可得

$$S(f)=C_2\left(\frac{\sin\pi ft_0}{\pi ft_0}\right)^2\sum_{n=-8}^{\infty}W\left(f-\frac{n}{qt_0}\right)$$

其中 $$C_2=\frac{q+3}{q^2}+\frac{4}{q^2}\sum_{k\in D}\cos\left(2\pi\frac{k}{q}\right)$$

例 $q=17$, $GF(q)=(0,1,2,\cdots,16)$

$D=\{1,2,4,8,9,13,15,16\}$, $\overline{D}=\{3,5,6,7,10,11,12,14\}$

伪随机序列

$A=\{-1,1,1,-1,1,-1,-1,-1,1,1,1,-1,-1,-1,1,-1,1,1\}$

$\sum_{k\in D}\cos(2\pi k/q)=1.56$; $\sum_{k\in \overline{D}}\cos(2\pi k/q)=-2.56$

$C_1=3.38\times 10^{-2}$, $C_2=9.08\times 10^{-2}$

所以 $n=0$ $S(0)=1/17^2=0.35\times 10^{-2}$

$n(\mathrm{mod}\ 17)\in D$ $S(f)=3.38\times 10^{-2}\left(\frac{\sin m\pi/17}{m\pi/17}\right)^2$

$n(\mathrm{mod}\ 17)\in \overline{D}$ $S(f)=9.08\times 10^{-2}\left(\frac{\sin m\pi/17}{m\pi/17}\right)^2$

这个序列的功率谱如图 2.由图 2可见, $q=4t+1$ 素数序列的功率谱是离散线性谱.直流分量为 $1/q$2.各谱线之间的间隔为码的基频 $f_0=1/qt_0=1/T$ (T为码重覆周期).谐波谱

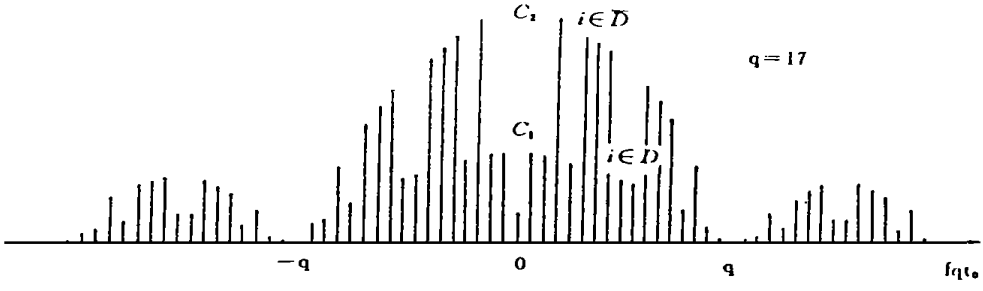

图 2 周期 $q=4t+1$ 序列功率谱

线的包络有 2个.若谐波次数 n是 $GF(q)$上的二次元素,即 $n(\mathrm{mod}\ q)\in D$,这些谱线的包络是 $C_1(\sin\pi f t_0/\pi f t_0)^2$,而谐波次数 n不是 $GF(q)$上的二次元素,即 $n(\mathrm{mod}\ q)\in \overline{D}$,这些谱线的包络是: $C_2(\sin\pi f t_0/\pi f t_0)^2$.这 2个包络幅度 C_1,C_2的平均值为:

$$\frac{C_1+C_2}{2}=\frac{q+3}{q^2}+\frac{2}{q^2}\left(\sum_{k\in\overline{D}}\cos\frac{2\pi k}{q}+\sum_{k\in D}\cos\frac{2\pi k}{q}\right)=\frac{q+1}{q^2}$$

为了分析这种序列功率谱特性,这里列出周期长度为 q的 m序列的功率谱[3]:

$$S(f)=\left[\frac{q+1}{q^2}\left(\frac{\sin\pi f t_0}{\pi f t_0}\right)^2\sum_{n=-\infty}^{\infty}W\left(f-\frac{n}{qt_0}\right)\right]-\frac{1}{q}W(f)\qquad(13)$$

其中 t_0是序列对应的二进制码元的宽度,序列的功率谱见图 3,这种功率谱是线状谱,各谱线强度的包络为 $[(q+1)/q^2]\cdot(\sin\pi f t_0/\pi f t_0)^2$,直流量为 $1/q^2$.

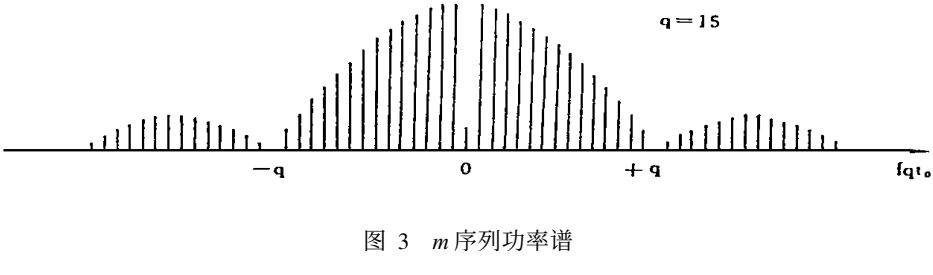

图 3　m序列功率谱

比较(11)和(13)式,图 2和图 3,可以发现素数 $q=4t+1$序列与 m序列功率谱相似,其直流分量相同,为 $1/q^2$,谐波谱线包络均为 $(\sin\pi f t_0/\pi f t_0)^2$,$m$序列功率谱包络只有 1个,素数 $q=4t+1$的序列包络有 2个,但是 2个包络幅度的平均值与 m序列功率谱一个包络的幅度机同,为 $(q+1)/q^2$.

4　序列元素的统计特性

序列元素的统计特性反映了序列的随机性能.同种元素连续出现 n次叫做一个长度为 n的元素游程.素数 $q=4t+1$序列,当 $q<100$时的各种游程数统计见表 1.

表 1　$q=4t+1$序列的游程统计

t	q	游程长度						总游程数
		U_1	U_2	U_3	U_4	U_5	U_6	
1	5	3	1					4
3	13	5	2	0	1			8
4	17	5	3	2				10
7	29	9	3	2	2			16
9	37	11	4	2	3			20
10	41	11	7	2	0	2		22
13	53	15	7	4	0	0	2	28
15	61	17	8	4	0	2	1	32
18	73	19	8	6	5			38
22	89	23	13	4	4	0	2	46
24	97	25	12	8	3	0	2	50

分析上表数据可得出这种序列游程统计特性一般规律:

(1) 在一个周期 $q=4t+1$内,元素 1出现 $(q-1)/2=2t$次,元素 -1出现 $(q+1)/2=2t+1$次. -1比 1多出现一次.

(2) 设各个不同长度游程的总数为 U,在一个周期 $q=4t+1$内, $U=(q+3)/2=2t+2$次.其中 1, -1的不同长度游程各占一半.

(3) 长度为 1的游程 U_1占总游程一半左右;当 t为偶数时, $U_1=U/2=t+1$;当 t为奇数时, $U_1=(U/2)+1=t+2$.

(4) 长度为 2的游程 U_2占总游程的四分之一左右: $U_2\approx U/4$.

(5) 随着游程长度的增加,游程数总趋势逐步递减.也有例外,如有些长度游程不存在.

结论: 在素数有限域上可以构成周期长度为 $q=4t+1$的序列,这些序列有着比较好的(三值)自相关函数.将上述素数 $q=4t+1$序列游程特性与 m序列游程特性[4]相比较可发现两者的功率谱和游程统计特性很相似. 所以,这些序列有良好的伪随机性,与 m序列相比较,这些序列的周期长度比较多,在 100以内, $q=4t+1$奇素数有 11个: 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97. 而 m序列的长度只有 5个: 3, 7, 15, 31, 63. 不同奇素数周期长度的序列可以满足各种技术领域特殊需要.

参 考 文 献

1 Marshall Hall JR. Combinatorial Theory. NY: John Wiley & Sons, 1986. 238~243
2 邵嘉裕. 组合数学. 上海: 同济大学出版社, 1991. 323~343
3 Don J, Toprieri. Principles of Military Communication System. Dedham Massa: Artech House Inc, 1981. 36~41
4 万哲先. 代数与编码. 第二版. 北京: 科学出版社, 1980. 260~329

An Analysis of Pseudorandom Properties of Sequence with Prime Number Periods $q=4t+1$

Wang Yongcheng[*]

Abstract Some properties of quadratic elements in the odd prime number finite field are obtained. The construction of PN sequences with prime number periods $q=4t+1$ are introduced and their autocorrelation functions are concisely determined. Power spectral density expressions of the above sequences are established and their run properties are analyzed.

Keywords finite field, PN sequence, autocorrelation function, power spectral density

* Department of Electronic Engine, Nanjing University of Aeronautics and Astronautics, Nanjing 210016