第 20 卷 第 3 期 电 子 科 学 学 刊 Vol.20 No.3
1998 年 5 月 JOURNAL OF ELECTRONICS May 1998

一类大线性复杂度二元 QF 序列的构造 [1]

孙 伟 杨义先

(北京邮电大学信息工程系 北京 100876)

摘 要 本文构造了一类二元 QF 序列，计算了周期、个数、相关函数和线性复杂度。结果表明，当 n 为偶数时，$C_{\max}=q^{n/2+1}+1$，$L_{\max}=m(3n/2)^{m-1}$；当 n 为奇数时，$C_{\max}=q^{n/2+3/2}+1$，$L_{\max}=2^{m-1}mn^{m-1}$。

关键词 QF 序列，线性复杂度，相关函数

中图号 TN914.4, TN918.1

1 引 言

在现代码分多址扩频通信和密码学中，相关性能好，线性复杂度大，包含序列多的序列族具有重要的作用。m-序列容易生成且具有理想的自相关性，遗憾的是互相关性能较差，线性复杂度太小，因而通常采用的方法是对 m-序列进行适当的非线性变换使其相关特性、线性复杂度满足要求，比如 GMW 序列 [1]，级联 GMW 序列 [2]，Bent 序列 [3]，No 序列 [4]，以及更广泛的几何序列 [5]。Klapper 在文献 [6] 中定义了 QF(quadratic form) 序列，并且构造了一类 $(0,j)$-QF 序列。本文构造了另外一类 QF 序列，计算了序列的周期、个数、相关函数和线性复杂度。

设 n 为正整数，$q=2^m$，有限域 $\mathrm{GF}(q^n)$ 到 $\mathrm{GF}(q)$ 的迹函数定义为 $\mathrm{tr}_q^{q^n}(x)=\sum_{i=0}^{n-1}x^{q^i}$。# N 表示集合 N 中元素的个数。

定义 1 [6] 设 α 为 $\mathrm{GF}(q^n)$ 的本原元，$H(x)$ 为 $\mathrm{GF}(q)$-向量空间 $\mathrm{GF}(q^n)$ 上的二次型，$1\le r<q-1$, $\gcd(r,q-1)=1$, $s(i)=\mathrm{tr}_2^q((H(\alpha^i))^r)$，称序列 $S=\{s(i):0\le i\le q^n-2\}$ 为 QF 序列。显然，QF 序列是一类特殊的 d-型序列 [7]，序列的最小周期是 q^n-1 的因子。

定义 2 设 $S=\{s(i):i=0,1,\ldots,L-1\}$ 和 $T=\{t(i):i=0,1,\ldots,L-1\}$ 是周期为 L 的 $\{0,1\}$ 二元序列，那么它们的周期相关函数定义为 $C_{S,T}(\tau)=\sum_{i=0}^{L-1}(-1)^{s(i+\tau)+t(i)}$, $\tau=0,\ldots,L-1$, 其中的 $(i+\tau)$ 取模 L 运算。

定理 1 [7] 设 n,q,r 和本原元 $\alpha\in\mathrm{GF}(q^n)$ 同定义 1，二次型 $H_1(x)$ 和 $H_2(x)$ 分别定义了 QF 序列 S^1 和 S^2，则对任意 τ, $C_{S^1,S^2}(\tau)=(qz_\tau-q^n)/(q-1)-1$，其中 $z_\tau=\#\{x\in\mathrm{GF}(q^n):H_1(x)+H_2(\alpha^\tau x)=0\}$。

令 $t=\lfloor n/2\rfloor$，$\lfloor x\rfloor$ 表示不超过 x 的最大整数，$H_{a,b}(x)=\mathrm{tr}_q^{q^n}(ax^{1+q^t}+bx^{1+q^{t-1}})$，$a,b\in\mathrm{GF}(q^n)$ 且不同时为零。设 $e_1,e_2,\ldots,e_n$ 为 $\mathrm{GF}(q^n)$ 在 $\mathrm{GF}(q)$ 上的一个基，则

$$\begin{aligned}H_{a,b}(x)&=\mathrm{tr}_q^{q^n}\Big(a\Big(\sum_{i=1}^n x_ie_i\Big)^{1+q^t}+b\Big(\sum_{i=1}^n x_ie_i\Big)^{1+q^{t-1}}\Big)\\&=\mathrm{tr}_q^{q^n}\Big(a\sum_{i=1}^n x_ie_i\sum_{j=1}^n x_je_j^{q^t}+b\sum_{i=1}^n x_ie_i\sum_{j=1}^n x_je_j^{q^{t-1}}\Big)\\&=\sum_{i,j=1}^n\mathrm{tr}_q^{q^n}(e_i(ae_j^{q^t}+be_j^{q^{t-1}}))x_ix_j.\end{aligned}$$

[1] 1997-01-15 收到，1997-08-28 定稿
国家杰出青年基金和国家教委跨世纪优秀人才专项基金资助课题

若 $H_{a,b}(x)\equiv 0$, 则 $\mathrm{tr}_q^{q^n}(e_i(ae_j^{q^t}+be_j^{q^{t-1}}))=0$, $1\le i,j\le n$。由于 $e_1,e_2,\ldots,e_n$ 为基，故 $ax^{q^t}=bx^{q^{t-1}}$, 任意 $x\in \mathrm{GF}(q^n)$, 因而 $a=b=0$, 与 a,b 不同时为零矛盾。所以 $H_{a,b}(x)$ 是二次型。

本文正是研究由 $H_{a,b}(x)$ 所定义的 QF 序列 $S=\{s(i)\}$ 的周期、个数、相关函数和线性复杂度，其中 $s(i)=\mathrm{tr}_2^q((\mathrm{tr}_q^{q^n}(a\alpha^{(1+q^t)i}+b\alpha^{(1+q^{t-1})i}))^\tau)$. 我们称之为 $(t,t-1)$-QF 序列。

2　序列的周期和个数

令 $\mathrm{per}(S)$ 表示序列 $S=\{s(i):0\le i\le q^n-2\}$ 的最小周期。

引理 1　设 S 是二次型 $H_{a,b}(x)$ 所确定的 $(t,t-1)$-QF 序列，则 $\mathrm{per}(S)=(q^n-1)/T$, 其中 $T=\#\{0\le\tau\le q^n-2:C_{S,S}(\tau)=q^n-1\}$。

引理 2 [5]　设 q 是偶数，j 为正整数，$d=\gcd(n,j)$, 则

$$\gcd(q^n-1,q^j+1)=\begin{cases}1, & \text{若}n/d\text{是奇数;}\\ q^d+1, & \text{若}n/d\text{是偶数.}\end{cases}$$

引理 3　当 $q,n/2=t$ 为偶数时，$\gcd(q+1,q^t+1)=1$。

证明　根据引理 2, $\gcd(q^n-1,q^{t-1}+1)=q+1$, 所以

$$\begin{aligned}\gcd(q+1,q^t+1)&=\gcd(\gcd(q^n-1,q^{t-1}+1),q^t+1)=\gcd(\gcd(q^n-1,q^t+1),q^{t-1}+1)\\&=\gcd(q^t+1,q^{t-1}+1)=\gcd(q^{t-1}+1,q^{t-1}-q+2)=1.\end{aligned}$$

证毕

根据引理 1 和定理 1, 要使 τ 满足 $C_{S,S}(\tau)=q^n-1=(qz_\tau-q^n)/(q-1)-1$, 则 $z_\tau=q^n$, 即 $\#\{x\in\mathrm{GF}(q^n):\mathrm{tr}_q^{q^n}((a+a\alpha^{(1+q^t)\tau})x^{1+q^t}+(b+b\alpha^{(1+q^{t-1})\tau})x^{1+q^{t-1}})=0\}=q^n$。因而 $a+a\alpha^{(1+q^t)\tau}=0$, $b+b\alpha^{(1+q^{t-1})\tau}=0$。

当 n 为奇数时，根据引理 2, $\gcd(q^n-1,q^t+1)=\gcd(q^n-1,q^{t-1}+1)=1$, 所以 $\tau=0$, 因而 $\mathrm{per}(S)=q^n-1$。

当 n 为偶数时，若 t 为奇数，则 $\gcd(q^n-1,q^t+1)=q^t+1$, $\gcd(q^n-1,q^{t-1}+1)=1$, 所以 $\tau=\begin{cases}0, & b\ne 0;\\ (q^t-1)l, & b=0;\end{cases}$ 其中 $l=0,1,\ldots,q^t$, 因而 $\mathrm{per}(S)=\begin{cases}q^n-1, & b\ne 0;\\ q^{n/2}-1, & b=0.\end{cases}$

若 t 为偶数，根据引理 2, $\gcd(q^n-1,q^t+1)=q^t+1$, $\gcd(q^n-1,q^{t-1}+1)=q+1$。

情况 1　当 $a=0,b\ne 0$ 时。$\alpha^{(1+q^{t-1})\tau}=1$, 当且仅当 $(q^n-1)\mid(q^{t-1}+1)\tau$, 当且仅当 $\frac{q^n-1}{q+1}\mid\frac{q^{t-1}+1}{q+1}\tau$。又因为 $\gcd(\frac{q^n-1}{q+1},\frac{q^{t-1}+1}{q+1})=1$, 所以 $\frac{q^n-1}{q+1}\mid\tau$, 即 $\tau=\frac{q^n-1}{q+1}l$。这样的 τ 有 $q+1$ 个，那么 $\mathrm{per}(S)=(q^n-1)/(q+1)$。

情况 2　当 $a\ne 0$, $b=0$ 时。$\alpha^{(1+q^t)\tau}=1$, 当且仅当 $(q^n-1)\mid(q^t+1)\tau$, 当且仅当 $(q^t-1)\mid\tau$。这样的 τ 有 q^t+1 个，那么 $\mathrm{per}(S)=(q^n-1)/(q^t+1)=q^t-1$。

情况 3　当 $a\ne 0,b\ne 0$ 时。$\alpha^{(1+q^{t-1})\tau}=1$ 且 $\alpha^{(1+q^t)\tau}=1$, 当且仅当 $(q^n-1)\mid(q^{t-1}+1)\tau$ 且 $(q^t-1)\mid\tau$, 当且仅当 $(q^t-1)\mid\tau$ 且 $\frac{q^n-1}{q+1}\mid\frac{q^{t-1}+1}{q+1}\tau$, 当且仅当 $(q^t-1)\mid\tau$ 且 $\frac{q^n-1}{q+1}\mid\tau$ 当

且仅当 $\frac{q^n-1}{q+1} \mid (q^t-1)l$, $0 \le l \le q^t$, 当且仅当 $(q^t-1)l = \frac{q^n-1}{q+1}k$, 当且仅当 $(q^t+1) \mid (q+1)l$。由于 $\gcd(q+1, q^t+1) = 1$, 所以 $l = 0$, 即 $\tau = 0$, 因而 $\mathrm{per}(S) = q^n - 1$。

这样证明了

定理 2 设 S 是一个 $(t, t-1)$-QF 序列, 则

当 n 为奇数时, $\mathrm{per}(S) = q^n - 1$;

当 n 为偶数, t 为奇数时, $\mathrm{per}(S) = \begin{cases} q^n-1, & b \neq 0; \\ q^{n/2}-1, & b = 0; \end{cases}$

当 n 为偶数, t 为偶数时, $\mathrm{per}(S) = \begin{cases} \dfrac{q^n-1}{q+1}, & a = 0, \ b \neq 0; \\ q^{n/2}-1, & a \neq 0, \ b = 0; \\ q^n-1, & a \neq 0, \ b \neq 0. \end{cases}$

定义 3 设 $S = \{s(i)\}$ 和 $T = \{t(i)\}$ 是两个周期序列, 若存在移位 τ 对任意 i, $s(i) = t(i+\tau)$, 则称 S 和 T 是等价的。

定理 3 存在 $q^n + 1$ 个不等价的 $(t, t-1)$-QF 序列。

证明 设 $s(i) = \mathrm{tr}_2^q((\mathrm{tr}_q^{q^n}(a\alpha^{(1+q^t)i} + b\alpha^{(1+q^{t-1})i})^r)$, $t(i) = \mathrm{tr}_2^q((\mathrm{tr}_q^{q^n}(a_1\alpha^{(1+q^t)i} + b_1\alpha^{(1+q^{t-1})i})^r)$ 是两个 $(t, t-1)$-QF 序列, 那么, 根据定理 1, S 和 T 等价, 当且仅当存在 τ 使 $z_\tau = \#\{x \in \mathrm{GF}(q^n) : \mathrm{tr}_q^{q^n}((a + a_1\alpha^{(1+q^t)\tau})x^{1+q^t} + (b + b_1\alpha^{(1+q^{t-1})\tau})x^{1+q^{t-1}}) = 0\} = q^n$, 即存在 τ 使 $a + a_1\alpha^{(1+q^t)\tau} = 0$, $b + b_1\alpha^{(1+q^{t-1})\tau} = 0$。

所以 S 所在的序列等价类为

$$\mathcal{S}_{a,b} = \{\{t(i) = \mathrm{tr}_2^q((\mathrm{tr}_q^{q^n}(a\alpha^{-(1+q^t)\tau}\alpha^{(1+q^t)i} + b\alpha^{-(1+q^{t-1})\tau}\alpha^{(1+q^{t-1})i})^r)\} : 0 \le \tau \le q^n - 2\}.$$

当 n 为奇数时, 根据引理 2, $\gcd(q^n-1, q^t+1) = \gcd(q^n-1, q^{t-1}+1) = 1$; 当 n 为偶数, t 为奇数时, $\gcd(q^n-1, q^t+1) = q^t+1$, $\gcd(q^n-1, q^{t-1}+1) = 1$; 在这两种情况下, $\#\mathcal{S}_{a,b} = q^n - 1$, 故包含 $(q^{2n}-1)/(q^n-1) = q^n + 1$ 个不等价的 $(t, t-1)$-QF 序列.

当 n 为偶数, t 为偶数时, $\gcd(q^n-1, q^t+1) = q^t+1$, $\gcd(q^n-1, q^{t-1}+1) = q+1$, 类似上述计算序列周期的方法得, $(\alpha^{(1+q^t)\tau}, \alpha^{(1+q^{t-1})\tau}) = (\alpha^{(1+q^t)\tau_1}, \alpha^{(1+q^{t-1})\tau_1})$, 当且仅当 $\alpha^{(1+q^t)(\tau-\tau_1)} = 1$, $\alpha^{(1+q^{t-1})(\tau-\tau_1)} = 1$, 当且仅当 $\tau = \tau_1$. 所以 $\#\mathcal{S}_{a,b} = q^n - 1$, 于是包含 $q^n + 1$ 个不等价的序列。

证毕

3 $(t, t-1)$-QF 序列的相关函数

令 $\gamma = a + a_1\alpha^{(1+q^t)\tau}$, $\delta = b + b_1\alpha^{(1+q^{t-1})\tau}$, $f(x) = \mathrm{tr}_q^{q^n}(\gamma x^{1+q^t} + \delta x^{1+q^{t-1}})$, 则 $z_\tau = \{x \in \mathrm{GF}(q^n) : f(x) = 0\}$。设 $W = \{x \in \mathrm{GF}(q^n) : f(x+y) = f(x) + f(y), \forall y \in \mathrm{GF}(q^n)\}$, $W_0 = \{x \in W : f(x) = 0\}$。容易验证 W, W_0 是 $\mathrm{GF}(q^n)$ 的 $\mathrm{GF}(q)$-子模。

引理 4 [9] $\mathrm{rank}(f) = n - \dim W_0$。

引理 5 $\mathrm{rank}(f) = n - \dim W$ 或 $\mathrm{rank}(f) = n - \dim W + 1$。

证明 令 $f|_W$ 表示 $f(x)$ 在子模 W 上的限制, $f|_W : W \to \mathrm{GF}(q)$, 则 $f|_W$ 是 $\mathrm{GF}(q)$-模同态, 由于 $W_0 = \mathrm{kernel}(f|_W)$, 所以根据同态基本定理, $W/W_0 \cong \mathrm{Im}(f|_W)$, 于是 $\dim W_0 =$

$\dim W-\dim\mathrm{Im}(f|_W)$。又 $\mathrm{Im}(f|_W)$ 是 $\mathrm{GF}(q)$ 的子模，则 $\dim\mathrm{Im}(f|_W)\le 1$。当 $\mathrm{Im}(f|_W)=0$ 时，$\dim\mathrm{Im}(f|_W)=0$; 当 $\mathrm{Im}(f|_W)=\mathrm{GF}(q)$ 时，$\dim\mathrm{Im}(f|_W)=1$。　　证毕

引理 6 [10]　$\dim W\equiv n(\mathrm{mod}2)$。

定理 4　当 n 为偶数时，$\dim W=0$ 或 2; 当 n 为奇数时，$\dim W=1$ 或 3。

证明　根据 W 的定义，$x\in W$ 当且仅当对任意 $y\in\mathrm{GF}(q^n)$, $f(x+y)=f(x)+f(y)$, 即 $\mathrm{tr}_q^{q^n}(\gamma xy^{q^t}+\gamma x^{q^t}y+\delta xy^{q^{t-1}}+\delta x^{q^{t-1}}y)=0$。由 y 的任意性得 $\gamma x+\gamma^{q^t}x^{q^{2t}}+\delta^q x^q+\delta^{q^t}x^{q^{2t-1}}=0$。当 n 为偶数时，$n=2t$, 又 $x^{q^{2t}}=x$, 故 $x\in W$, 当且仅当 $\delta^{q^2}x^{q^2}+(\gamma^q+\gamma^{q^{t+1}})x^q+\delta^{q^{t+1}}x=0$。由于 $\delta^{q^2}x^{q^2}+(\gamma^q+\gamma^{q^{t+1}})x^q+\delta^{q^{t+1}}x$ 是 $\mathrm{GF}(q^n)$ 上的线性化多项式，所以在其分裂域上的所有根作成 $\mathrm{GF}(q)$ 上的一个模 V, 并且 $\dim V=2$。又 $W=V\cap\mathrm{GF}(q^n)$, 故 $\dim W\le 2$。因而 $\dim W=0$ 或 2。当 n 为奇数，$t=(n-1)/2$, 类似可知 $W=\{x\in\mathrm{GF}(q^n):\delta^{q^3}x^{q^3}+\gamma^{q^2}x^{q^2}+\gamma^{q^{t+2}}x^q+\delta^{q^{t+2}}x=0\}$, 因而 $\dim W\le 3$, 所以 $\dim W=1$ 或 3。　　证毕

推论 1　当 n 为偶数时，$\mathrm{rank}(f)\in\{n,n-1,n-2\}$; 当 n 为奇数时，$\mathrm{rank}(f)\in\{n,n-1,n-2,n-3\}$。

设 $g(x)=a_0+a_1x+\cdots+a_{q-2}x^{q-2}\in\mathrm{GF}(q)[x]$,

$$A(g)=\begin{pmatrix} a_0 & a_1 & \cdots & a_{q-3} & a_{q-2}\\ a_1 & a_2 & \cdots & a_{q-2} & a_0\\ \vdots & \vdots & & \vdots & \vdots\\ a_{q-2} & a_0 & \cdots & a_{q-4} & a_{q-3}\end{pmatrix}.$$

引理 7 [8]　$g(x)$ 在 $\mathrm{GF}(q)$ 中非零解的个数为 $q-1-\mathrm{rank}(A(g))$。

如前所述，设 $\gamma(\tau)=a+a_1\alpha^{(1+q^t)\tau}$, $\delta(\tau)=b+b_1\alpha^{(1+q^{t-1})\tau}$, $B(\tau)=A(f)$。

由引理 5、引理 7 和定理 4 得到

定理 5　当 n 为偶数时，对任意 τ, $\mathrm{rank}(B(\tau))=q^n-1$ 或 q^n-q^2。若 $\mathrm{rank}(B(\tau))=q^n-1$, 则 $\mathrm{rank}(f)=n$; 若 $\mathrm{rank}(B(\tau))=q^n-q^2$, 则 $\mathrm{rank}(f)=n-1$ 或 $n-2$。

当 n 为奇数时，对任意 τ, $\mathrm{rank}(B(\tau))=q^n-q$ 或 q^n-q^3。若 $\mathrm{rank}(B(\tau))=q^n-q$, 则 $\mathrm{rank}(f)=n$ 或 $n-1$; 若 $\mathrm{rank}(B(\tau))=q^n-q^3$, 则 $\mathrm{rank}(f)=n-2$ 或 $n-3$。

引理 8 [8]　设 q 为偶数，则 $\mathrm{GF}(q)$ 上的任意含有 n 个未知元且秩为 t 的二次型 $H(x)$ 在 $\mathrm{GF}(q^n)$ 的某个基之下都可以化为以下三种标准形式之一：

$$\begin{aligned}&x_1x_2+x_3x_4+\ldots+x_{t-1}x_t;\\ &x_1x_2+x_3x_4+\ldots+x_{t-2}x_{t-1}+x_t^2;\\ &x_1x_2+x_3x_4+\ldots+x_{t-3}x_{t-2}+bx_{t-1}^2+x_{t-1}x_t+bx_t^2.\end{aligned}$$

相应地 $H(x)=c$ 在 $\mathrm{GF}(q^n)$ 中解的个数分别为

$$q^{n-1}+v(c)q^{n-1-t/2};\quad q^{n-1};\quad q^{n-1}-v(c)q^{n-1-t/2},$$

其中 $v(c)=\begin{cases}-1, & c\neq 0;\\ q-1, & c=0.\end{cases}$

总结以上结论，根据定理 1 容易得到

定理 6 当 n 为偶数时，$(t,t-1)$-QF 序列 S 和 T 的相关函数 $C_{S,T}(\tau) \in \{\pm q^{n/2}-1, \pm q^{(n+1)/2}-1; \pm q^{n/(2+1)}-1, -1\}$；当 n 为奇数时，$C_{S,T}(\tau) \in \{\pm q^{n/2}-1, \pm q^{(n+1)/2}-1;\ \pm q^{n/2+1}-1, \pm q^{(n+3)/2}-1, -1\}$。

4 $(t,t-1)$-QF 序列的线性复杂度

线性复杂度指生成序列的线性移位寄存器的最小长度，它是衡量序列好坏的一个重要指标。Klapper 在文献 [9] 中证明了如下定理：

定理 7 设 $k_i = \sum_j q^{e_j(i)} < q^n, i = 1,2,\ldots,d$，并且若 $i \neq j$，则不存在 r 使 $k_i \equiv q^r k_j \bmod(q^n-1)$，$\gamma_i \in \mathrm{GF}(q^n)^*$ 且 $g(x) = \sum_{i=0}^{q-1} a_i x^i$，那么序列 $S = \{s(i) = g(\mathrm{tr}_q^{q^n}(\sum_{j=1}^d \gamma_j \alpha^{k_j i}))\}$ 的线性复杂度为 $\sum_{a_i \neq 0}(\sum_{j=1}^d \xi(k_j))^{wt(i)}$，其中 $\xi(k)$ 表示 k 所在的分圆陪集的元素个数，$wt(i)$ 表示 i 的 2 进制重量。

引理 9 设 $t = \lfloor n/2 \rfloor$，则对任意 r，$1 + q^t \neq q^r(1+q^{t-1}) \bmod(q^n-1)$。

证明 当 n 为偶数时，$t = n/2$，若 $r \leq t$，则 $q^r + q^{r+t-1} < q^n - 1$，所以 $1 + q^t \neq q^r(1+q^{t-1}) \bmod(q^n-1)$。若 $r > t$，由于 $q^{r+t-1} \equiv q^{r+t-1-n} \bmod(q^n-1)$，$q^r + q^{r+t-1-n} < q^n - 1$，故 $1 + q^t \neq q^r(1+q^{t-1}) \bmod(q^n-1)$。当 n 为奇数时同理可证。

定理 8 当 n 为偶数时，$(t,t-1)$-QF 序列的线性复杂度如下：

$$L = \begin{cases} m(n/2)^{wt(r)}, & a \neq 0,\ b = 0; \\ mn^{wt(r)}, & a = 0,\ b \neq 0; \\ m(3n/2)^{wt(r)}, & a \neq 0, b\ \neq 0. \end{cases}$$

证明 由于 $q^t(1+q^t) \equiv 1+q^t \bmod(q^n-1)$，且对任意 r，$1 \leq r < t$，$q^r(1+q^t) \not\equiv 1+q^t \bmod(q^n-1)$，所以 $\xi(1+q^t) = t = n/2$。

当 t 为奇数时，由于 $\gcd(q^n-1, q^{t-1}+1) = 1$，所以 $\xi(1+q^{t-1}) = n$。

当 t 为偶数时，由于 $\gcd(n, t-1) = 1$，故 $\gcd(q^n-1, q^{t-1}+1) = q+1$。若存在 $r > 1$ 使 $q^r(1+q^{t-1}) \equiv 1+q^{t-1} \bmod(q^n-1)$，即 $q^{2t}-1 | (q^r-1)(q^{t-1}+1)$，因而 $\frac{q^{2t-1}}{q+1} | (q^r-1)\frac{q^{t-1}+1}{q+1}$，于是 $\frac{q^{2t}-1}{q+1} | q^r-1$，显然最小的 r 为 n，所以 $\xi(1+q^{t-1}) = n$。

由于 $g(x) = \mathrm{tr}_2^{2^m}(x^r) = \sum_{j=0}^{m-1} x^{r2^j}$，这 m 个单项式 x^{r2^j} 两两不同，且 $wt(r2^j) = wt(r)$，再由定理 7，得证。 证毕

类似地

定理 9 当 n 为奇数时，$(t,t-1)$-QF 序列的线性复杂度如下：

$$L = \begin{cases} m(2n)^{wt(r)}, & a \neq 0, b \neq 0; \\ mn^{wt(r)}, & \text{否则}. \end{cases}$$

由于 $\gcd(2^{m-1}-1, 2^m-1) = 1$ 且 $wt(2^{m-1}-1) = m-1$，所以当 $\gcd(r, 2^m-1) = 1$ 且 r 属于 2^m-1 所在的分圆陪集时线性复杂度达到最大值，即 $L_{max} = \begin{cases} m(3n/2)^{m-1}, & n\text{为偶数}; \\ m(2n)^{m-1}, & n\text{为奇数}. \end{cases}$

5 结　论

本文构造了一类二元 QF 序列，并且计算了周期、个数、相关函数和线性复杂度。可以看出，当 n 为偶数时，相关性能较好；当 n 为奇数时，线性复杂度较大。所以我们可以根据不同的要求选取 n 为偶数或奇数。$(t,t-1)$-QF 序列可以容易地实现，只要将一个 m-序列的两个采样序列移位模 2 加输入一个非线性函数即可。

参 考 文 献

[1] Scholtz R A, Welch L R. GMW sequences. IEEE Trans. on Inform. Theory, 1984, IT-30(3): 548–553.

[2] Klapper A, Chan A H, Goresky M. Cascaded GMW sequences. IEEE Trans. on Inform. Theory, 1993, IT-39(1): 177–183.

[3] Olsen J D, Scholtz R A, Welch L R. Bent-function sequences. IEEE Trans. on Inform. Theory, 1982, IT-28(6): 858–864.

[4] No J, Kumar P V. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span. IEEE Trans. on Inform. Theory, 1989, IT-35(2): 371–379.

[5] Klapper A, Chan A H, Goresky M. Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences. Discrete Appl. Math., 1993, 46: 1–20.

[6] Klapper A. Large families of sequences with near-optimal correlations and large linear span. IEEE Trans. on Inform. Theory, 1996, IT-42(4): 1241–1248.

[7] Klapper A. d-form sequences: Families of sequences with low correlation values and large linear span, IEEE Trans. on Inform. Theory, 1995, IT-41(2): 423–431.

[8] Lidl R, Niederreiter H. Finite Fields. Encyclopedia of Mathematics 20, Cambridge, 1983.

[9] Klapper A, Cross-correlations of geometric sequences in characteristic two. Designs, Codes, and Cryptography, 1993, vol.3: 347–377.

[10] Jacobson N. Lectures in Abstract Algebra. Springer-Verlag, GTM 31, 1957.

CONSTRUCTION OF A FAMILY OF BINARY QF SEQUENCES WITH HIGH LINEAR SPAN

Sun Wei　　Yang Yixian

(*Beijing University of Posts and Telecommunications, Beijing* 100088)

Abstract　A family of binary QF sequences are constructed and their periods, size of the family, correlation functions and linear span are given, which shows that $C_{\max}=q^{n/2+1}+1, L_{\max}=m(3n/2)^{m-1}$ when n is even, $C_{\max}=q^{n/2+3/2}+1, L_{\max}=2^{m-1}mn^{m-1}$ when n is odd.

Key words　QF sequences, Linear span, Correlation function

孙　伟：　男，1969 年生，博士，讲师，研究方向为代数编码，密码序列以及扩频码序列的设计.

杨义先：　男，1961 年生，教授，博士生导师，全国政协委员，研究方向为密码学及信号信息处理.