第 36 卷 第 5 期 计 算 机 工 程 2010 年 3 月
Vol.36 No.5 Computer Engineering March 2010
·安全技术· 文章编号：1000—3428(2010)05—0137—03 文献标识码：A 中图分类号：TN918.1

新的二元互素序列的迹表示和线性复杂度

闫统江[1]，李淑清[2]
(1. 中国石油大学数学与计算科学学院，东营 257061；2. 中国石油大学计算机与通信工程学院，东营 257061)

摘 要： 利用周期分别为奇素数 p 和 q 的 Legendre 序列构造大量新的周期为 pq 的二元序列，根据这些序列与 Legendre 序列在结构上的联系，给出它们的迹表示，依据 E.L. Key 方法得到其线性复杂度。结果表明该类序列具有良好的符号平衡性和线性复杂度性质，作为密钥流序列可抵抗 Berlekamp-Massey 算法的攻击。

关键词： 流密码；Legendre 序列；Jacobi 序列；迹表示；线性复杂度

Trace Representations and Linear Complexity of New Binary Related-prime Sequences

YAN Tong-jiang[1], LI Shu-qing[2]
(1. College of Mathematics and Computational Science, China University of Petroleum, Dongying 257061;
2. College of Computer and Communication Engineering, China University of Petroleum, Dongying 257061)

【Abstract】 Lots of new binary sequences of period p and q are presented. These sequences are formed with the Legendre sequences with the periods p and q, where p and q are different odd primes. Based on the constructive relation of these sequences with Legendre sequences, this paper obtains the trace presentations from their defining pairs. Linear complexity is calculated by E.L. Key method. The results show that these sequences possess better properties of symbol balance and linear complexity. Used as key streams, they can resist the attack from the application of the Berlekamp-Massey algorithm.

【Key words】 stream cipher; Legendre sequences; Jacobi sequences; trace representations; linear complexity

1 概述

具有特定性质的伪随机序列在流密码中有着广泛的应用。度量周期序列 s^∞ 的伪随机性的一个重要指标是它的线性复杂度 $L(s^\infty)$，即生成 s^∞ 的最短线性反馈移位寄存器(LFSR)的级数。根据著名的 Berlekamp-Massey 算法，如果 $L(s^\infty)>N/2$ (N 是 s^∞ 的周期)，则认为 s^∞ 具有好的线性复杂度性质。有限域 F_{2^n} 到其子域 F_2 的关于变量 x 的迹函数记为 $Tr_1^n(x)=\sum_{0\leqslant i<n} x^{2^i}$。迹函数具有双线性性质，即

(1) $Tr_1^n(kx)=kTr_1^n(x),\forall k\in GF$

(2) $Tr_1^n(x+y)=Tr_1^n(x)+Tr_1^n(y)$

如果二元序列 $s^\infty(t)$ 可以表示为

$s(t)=Tr_1^n(\alpha^t),\ \alpha\in GF(2^n)$

则称为二元序列 $s^\infty(t)$ 的迹表示。每个序列都有唯一的迹表示。根据序列的迹表示不仅可以研究序列的线性复杂度和相关性等密码学性质，而且可以得到生成该序列的线性反馈移位寄存器。

令 p 和 q 是不同的奇素数，不妨设 $p<q$，$N=pq$。互素序列又被称为修改的 Jacobi 序列(MJS)[1]或 Whiteman 广义割圆序列[2]，其定义可由式 (1) 在 a=0 时给出

$$J_{p,q}^{(a)}(t)=\begin{cases}0 & t\equiv 0 \bmod pq\\ 1 & t\equiv 0 \bmod p,\ t\not\equiv 0 \bmod q\\ 0 & t\not\equiv 0 \bmod p, t+a\equiv 0 \bmod q\\ \left(\frac{t}{p}\right)\oplus\left(\frac{t+a}{q}\right) & \text{其他}\end{cases} \quad (1)$$

其中，⊕表示布尔加法运算；(-)表示简约 Legendre 符号函数。显然它是由起点为 0 的 Jacobi 序列[3]经过简单修改得到的，而且包括著名的孪生素数序列。研究表明，这类序列具有高线性复杂度、低周期自相关值、互相关值及很好的平衡性质[2]。它的迹表示由文献[4]给出。本文研究的序列由式 (1) 给出，不同的是这里 a 满足条件：$1\leqslant a\leqslant q-1$。显然它是由非零起点的 Jacobi 序列经过类似修改得到的，称之为 NRP。由定义可知，当 p 和 q 的值接近时，它具有很好的符号平衡性。尽管它的构造类似于前面的互素序列，但其符号分布完全不同。假设 $P=\{p,2p,\cdots,(q-1)p\}, Q=\{q,2q,\cdots,(p-1)q\}$。令 e_q, e_p 满足

$$e_q=\begin{cases}1 \bmod q\\ 0 \bmod p\end{cases}$$

$$e_p=\begin{cases}1 \bmod p\\ 0 \bmod q\end{cases}$$

由中国剩余定理可知，$e_q, e_p \bmod pq$ 唯一存在。A_0, A_1 的生成多项式分别为

$$A_0(x)=\sum_{t\in A_0} x^t \bmod(x^p-1),\ A_1(x)=\sum_{t\in A_1} x^t \bmod(x^p-1)$$

假设

基金项目： 国家自然科学基金资助项目(60473028)；中科院开放课题基金资助项目

作者简介： 闫统江(1973－)，男，副教授、博士，主研方向：密码学；李淑清，硕士研究生

收稿日期： 2009-08-06 **E-mail：** yantoji@163.com

$$A(x)=\frac{p-1}{2}+a_0A_0(x)+a_1A_1(x)\bmod(x^p-1) \tag{2}$$

其中，$(a_0,a_1)=\begin{cases}(1,\ 0) & p\equiv\pm1\bmod 8\\ (\omega,\omega^2) & p\equiv\pm3\bmod 8\end{cases}$；$\omega\in F_4\setminus F_2$ 为 3 次本原单位根。

由文献[5]可知，总可以找到 p 次本原单位根 α，使

$$A_0(\alpha)=\begin{cases}1 & p\equiv 1\bmod 8\\ 0 & p\equiv -1\bmod 8\\ \omega^2 & p\equiv 3\bmod 8\\ \omega & p\equiv -3\bmod 8\end{cases} \tag{3}$$

如果某个 p 次本原单位根 α 不满足上述条件，则 α^u 必定满足此条件，其中，u 为 F_p 的任一个生成元。依据 α 的选取，当 $p\equiv 1\bmod 8$，$p\equiv -1\bmod 8$，$p\equiv 3\bmod 8$，$p\equiv -3\bmod 8$ 时，分别有 $A_1(\alpha)=0,\ 1,\ \omega,\ \omega^2$。

2 NRP的定义对

由文献[4]可知，对于周期为 N 的二元序列 $s^\infty(t)$，总存在一个本原 N 次单位根 γ 和一个多项式 $g(x)=\sum_{0\leqslant i<N}\rho(i)x^i$，使 $s(t)=g(\gamma^t)$。则称 $(g(x),\gamma)$ 为序列 $s^\infty(t)$ 的定义对。

引理 1 若 $A(x)$，α 由式(2)、式(3)定义，Legendre 序列 $b_p=\{b_p(t)\,|\,t\geqslant 0\}$ 定义为 $b_p(t)=\begin{cases}1 & t\in A_0\\ 0 & t\in F_p/A_0\end{cases}$，则 b_p 的定义对为 $(A(x),\alpha)$，其中，$A_0\triangleq\{x^2\,|\,x\in F_p^*\}$，$A_1\triangleq F_p^*\setminus A_0$，$F_p^*=F_p\setminus\{0\}$。

相应地，对于 q，假设 $F_q^*=F_q\setminus\{0\}$，$B_0\triangleq\{x^2\,|\,x\in F_q^*\}$，$B_1\triangleq F_q^*\setminus B_0$，则

$$B_i(x)=\sum_{t+a\in B_i}x^{t+a}\bmod(x^q-1)$$

$$B(x)=\frac{q-1}{2}+b_0B_0(x)+b_1B_1(x)$$

其中，

$$(b_0,b_1)=\begin{cases}(1,0) & q\equiv\pm1\bmod 8\\ (\omega,\omega^2) & q\equiv\pm3\bmod 8\end{cases}$$

$$b_q(t+a)=\begin{cases}1 & t+a\in B_0\\ 0 & t+a\in F_q\setminus B_0\end{cases}$$

由引理 1 可知，总可以找到 q 次本原单位根 β，使 $b_q(t+a)$ 的定义对为 $(B(x),\beta)$，当 $q\equiv 1,-1,3,-3\bmod 8$ 时，分别有 $B_0(\beta)=1,0,\omega^2,\omega$。

设 T 为奇整数，周期为 T 的序列 $\delta_T=\{\delta_T(t)\,|\,t\geqslant 0\}$ 定义为 $\delta_T(t)=\begin{cases}1 & t\equiv 0\bmod p\\ 0 & \text{其他}\end{cases}$，取 T 次本原单位根 γ，假设 $\Delta_T(x)=\sum_{0\leqslant i<T}x^i$，则 $(\Delta_T(x),\gamma)$ 为序列 δ_T 的定义对。

给定序列 $s=\{s(t)\,|\,t\geqslant 0\}$，它的 λ - 跳 (λ-jump) 序列 $s^{[\lambda]}=\{s^{[\lambda]}(t)\,|\,t\geqslant 0\}$ 定义为 $s^{[\lambda]}(t)=\begin{cases}s(t) & t\equiv 0\bmod\lambda\\ 0 & \text{其他}\end{cases}$。易证 $\left|\{t\,|\,t\in P\text{且}t+a\in Q\}\right|=1$。

引理 2

$$J_{p,q}^{(a)}(t)=b_p(t)+b_q(t+a)+b_p^{(q)}(t+a)+b_q^{[p]}(t+a)+\delta_{pq}(t)+\delta_p(t)$$

其中，$b_p^{(q)}(t+a)=b_p(t)\delta_q(t+a)$，$b_q^{[p]}(t+a)=b_q(t+a)\delta_p(t)$。

证明：剩余类环 Z_{pq} 具有以下的分解：

$$Z_{pq}=\{t\,|\,t\equiv 0\bmod pq\}\cap\{t\,|\,t\equiv 0\bmod p,t\neq 0\bmod q\}\cap$$
$$\{t\,|\,t\neq 0\bmod p,t+a\equiv 0\bmod q\}\cap\{t\,|\,\gcd(t,pq)=1,t+a\notin Q\}$$

本引理剩余的证明见表 1。

表 1 $J_{p,q}^{(a)}$ 分序列在不同条件下的取值

	$t\equiv 0\bmod pq$	$t\equiv 0\bmod p$ $t\neq 0\bmod q$	$t\neq 0\bmod p$ $t+a\equiv 0\bmod q$	$\gcd(t,pq)=1$ $t+a\notin Q$
$B_p(t)$	0	0	(t/p)	(t/p)
$B_p(t+a)$	(a/q)	$(t+a/q)$	0	$(t+p/q)$
$b_p^{(q)}(t+a)$	0	0	(t/p)	0
$b_q^{[p]}(t+a)$	(a/q)	$(t+a/q)$	0	0
$\delta_{pq}(t)$	1	0	0	0
$\delta_p(t)$	1	1	0	0

其中，$b_p^{(q)}(t+a)=\begin{cases}b_p(t) & t\notin P\text{且}t+a\in Q\\ 0 & \text{其他}\end{cases}$，$b_q^{[p]}(t+a)=\begin{cases}b_q(t+a) & t\in P\\ 0 & \text{其他}\end{cases}$。

证毕。

引理 3 引理 2 中 $J_{p,q}^{(a)}$ 的 6 个分序列的定义对见表 2。

表 2 $J_{p,q}^{(a)}$ 的序列的定义对

序列	定义对
$b_p(t)$	$(A(x^{e_p}),\alpha\beta)$
$b_q(t+a)$	$(B(x^{e_q}),\alpha\beta)$
$b_p^{(q)}(t+a)$	$(A(x^{e_p})\Delta_q(x^{e_q}\beta^a),\alpha\beta)$
$b_q^{[p]}(t+a)$	$(B(x^{e_q})\Delta_p(x^{e_p}),\alpha\beta)$
$\delta_p(t)$	$\Delta_p(x^{e_p}),\alpha\beta)$
$\delta_{pq}(t)$	$(\Delta_{pq}(x),\alpha\beta)$

证明：由引理 2 可得：

引理 4[4] 若 $f(x)\equiv g(x)\pmod{x^p-1}$，则 $f(x^{e_p})\equiv g(x^{e_p})\pmod{x^{pq}-1}$。

引理 5[4]

$$\Delta_{pq}(x)=1+\sum_{1\leqslant i<p}x^{e_pi}+\sum_{1\leqslant j<q}x^{e_qj}+\sum_{\substack{1\leqslant j<q\\ 1\leqslant i<p}}x^{e_pi+e_qj}\bmod x^{pq}-1,$$

$$\sum_{1\leqslant i<p}x^{e_pi}+\sum_{i=0,1}A_i(x^{e_p})x^{e_q}\bmod x^{pq}-1$$

$$\sum_{\substack{1\leqslant j<q\\ 1\leqslant i<p}}x^{e_pi+e_qj}=\sum_{\substack{i=0,1\\ j=0,1}}A_i(x^{e_p})B_j(x^{e_q})\bmod x^{pq}-1$$

引理 6 $J_{p,q}^{(a)}(t)$ 的定义对为 $(g(x),\alpha\beta)$，其中

$$g(x)=\frac{q-1}{2}\sum_{1\leqslant i<p}(x^{e_p})^i+\sum_{1\leqslant j<q}(1+\frac{p-1}{2}\beta^{aj})x^{e_qj}+$$
$$\sum_{\substack{i=0,1\\ j=0,1}}a_iA_i(x^{e_p})B_j\left(x^{e_q}\beta^a\right)+\sum_{\substack{i=0,1\\ j=0,1}}(b_j+1)A_i(x^{e_p})B_j(x^{e_q})$$

证明：根据引理 5，因为 $\sum_{1\leqslant j<q}x^{e_qj}=\sum_{i=0,1}B_i(x^{e_q})\bmod x^{pq}-1$，$\sum_{1\leqslant j<q}(x^{e_q}\beta^a)^j=\sum_{1\leqslant j<q}(x\beta^a)^{e_qj}=\sum_{j=0,1}B_j\left((x\beta^a)^{e_q}\right)=\sum_{j=0,1}B_j\left(x^{e_q}\beta^a\right)$，所以

$$g(x)=A(x^{e_p})+B(x^{e_q})+A(x^{e_p})\Delta_q(x^{e_q}\beta^a)+B(x^{e_q})\Delta_p(x^{e_p})+$$
$$\Delta_p(x^{e_p})+\Delta_{pq}(x)=A(x^{e_p})\left(1+\Delta_q(x^{e_q}\beta^a)\right)+B(x^{e_q})\left(1+\Delta_p(x^{e_p})\right)+$$
$$\Delta_p(x^{e_p})+\Delta_{pq}(x)=\frac{q-1}{2}\sum_{1\leqslant i<p}x^{e_pi}+\sum_{1\leqslant j<q}(1+\frac{p-1}{2}\beta^{aj})x^{e_qj}+$$
$$\sum_{\substack{i=0,1\\ j=0,1}}a_iA_i(x^{e_p})B_j\left(x^{e_q}\beta^a\right)+\sum_{\substack{i=0,1\\ j=0,1}}(b_j+1)A_i(x^{e_p})B_j(x^{e_q})$$

3 NRP的迹表示和线性复杂度

记 m,n 分别是 2 模 p 和 q 的阶，$c_p=\frac{p-1}{m},c_q=\frac{q-1}{n}$，$d=(m,n)$，$M=mn/d$，$u,v$ 分别是 F_p^*,F_q^* 的生成元，则有：

引理 7[4] F_2 上 $(p-1)(q-1)$ 个 pq 次本原单位根的等价类 S 可表示为

$$S=\{\alpha^{u^i}\beta^{v^j}\mid 0\leqslant i<c_p,0\leqslant j<c_qd\}$$

定理 1 符号 p,q,α,β,ω 的定义同上，序列 $J_{p,q}^{(a)}=\{J_{p,q}^{(a)}(t)\mid t\geqslant 0\}$ 有如下的迹表示：

如果 $p\equiv\pm1\bmod 8,q\equiv\pm1\bmod 8$，则

$$J_{p,q}^{(a)}(t)=\frac{q-1}{2}\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})+\sum_{0\leqslant j<c_q}\left[Tr_1^n\left(\beta^{v^jt}(1+\frac{p-1}{2}\beta^{av^j})\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 0\bmod 2}}Tr_1^M\left[\beta^{v^ja}\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 1\bmod 2}}Tr_1^M\left(\alpha^{u^it}\beta^{v^it}\right)+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 0\bmod 2\\ j\equiv 1\bmod 2}}Tr_1^M\left[(\beta^{v^ja}+1)\left(\alpha^{u^it}\beta^{v^it}\right)\right]$$

如果 $p\equiv\pm1\bmod 8,q\equiv\pm3\bmod 8$，则

$$J_{p,q}^{(a)}(t)=\frac{q-1}{2}\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})+\sum_{0\leqslant j<c_q}\left[Tr_1^n\left(\beta^{v^jt}(1+\frac{p-1}{2}\beta^{av^j})\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 0\bmod 2}}Tr_1^M\left[(\beta^{av^j}-\omega^2)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 1\bmod 2}}Tr_1^M\left[(-\omega)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 0\bmod 2\\ j\equiv 1\bmod 2}}Tr_1^M\left[(\beta^{av^j}-\omega)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 1\bmod 2\\ j\equiv 0\bmod 2}}Tr_1^M\left[(-\omega^2)\left(\alpha^{u^it}\beta^{v^it}\right)\right]$$

如果 $p\equiv\pm3\bmod 8,q\equiv\pm1\bmod 8$，则

$$J_{p,q}^{(a)}(t)=\frac{q-1}{2}\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})+\sum_{0\leqslant j<c_q}\left[Tr_1^n\left(\beta^{v^jt}(1+\frac{p-1}{2}\beta^{av^j})\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 0\bmod 2}}Tr_1^M\left[\omega\beta^{av^j}\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 1\bmod 2}}Tr_1^M\left[(\omega^2\beta^{av^j}+1)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 0\bmod 2\\ j\equiv 1\bmod 2}}Tr_1^M\left[(\omega\beta^{av^j}+1)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 1\bmod 2\\ j\equiv 0\bmod 2}}Tr_1^M\left[(\omega^2\beta^{av^j})\left(\alpha^{u^it}\beta^{v^it}\right)\right]$$

如果 $p\equiv\pm3\bmod 8,q\equiv\pm3\bmod 8$，则

$$J_{p,q}^{(a)}(t)=\frac{q-1}{2}\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})+\sum_{0\leqslant j<c_q}\left[Tr_1^n\left(\beta^{v^jt}(1+\frac{p-1}{2}\beta^{av^j})\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 0\bmod 2}}Tr_1^M\left[(\omega\beta^{av^j}-\omega^2)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i=j\equiv 1\bmod 2}}Tr_1^M\left[(\omega^2\beta^{av^j}-\omega)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 0\bmod 2\\ j\equiv 1\bmod 2}}Tr_1^M\left[(\omega\beta^{av^j}-\omega)\left(\alpha^{u^it}\beta^{v^it}\right)\right]+\sum_{\substack{0\leqslant i<c_p\\0\leqslant j<c_qd\\ i\equiv 1\bmod 2\\ j\equiv 0\bmod 2}}Tr_1^M\left[(\omega^2\beta^{av^j}-\omega^2)\left(\alpha^{u^it}\beta^{v^it}\right)\right]$$

证明：注意到 $<u^{c_p}>=<2>$ 是 F_p^* 的子群。从而

$$F_p^*=\bigcup_{0\leqslant i<c_p}u^i<u^{c_p}>=\bigcup_{0\leqslant i<c_p}u^i<2>$$

$$\sum_{1\leqslant j<q}x^j=\sum_{j\in F_q^*}x^j=\sum_{j\in\cup_{i=0}^{c_q-1}v^i<2>}x^j=\sum_{i=0}^{c_q-1}\sum_{k=0}^{n-1}x^{v^j2^k}=$$

$$\sum_{0\leqslant i<c_q}Tr_1^n(x^{v^j})\bmod x^q-1$$

$$\sum_{1\leqslant i<p}(x^{e_p})^i=\sum_{0\leqslant i<c_p}Tr_1^m(x^{e_pu^i})\bmod x^{pq}-1$$

$$\sum_{1\leqslant i<p}(x^{e_p})^i|_{x=(\alpha\beta)^t}=\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})$$

$$\sum_{1\leqslant i<q}(x^{e_q})^j|_{x=(\alpha\beta)^t}=\sum_{0\leqslant j<c_q}Tr_1^n(\beta^{v^jt})$$

$$\sum_{1\leqslant j<q}(x^{e_q}\beta^a)^j=\sum_{0\leqslant j<c_q}Tr_1^n(x\beta^a)^{e_qv^j}\bmod x^{pq}-1$$

$$\sum_{1\leqslant j<q}(x^{e_q}\beta^a)^j|_{x=(\alpha\beta)^t}=\sum_{1\leqslant j<c_q}Tr_1^n(\alpha^t\beta^{t+a})^{e_qv^j}=\sum_{0\leqslant j<c_q}Tr_1^n\left((\beta^{v^j})^{t+a}\right),$$

$$\sum_{\substack{i=0,1\\ j=0,1}}(b_j+1)A_i(x^{e_p})B_j(x^{e_q})=\sum_{\substack{i,j=0,1\\ 0\leqslant t_1<(p-1)/2\\ 0\leqslant s_1<(q-1)/2}}(b_j+1)x^{e_pu^{i+2\eta_1}+e_qv^{j+2\eta_1}}=$$

$$\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}(b_j+1)x^{e_pu^i+e_qv^j}\ \square\ \eta(x)\bmod x^{pq}-1,\ \eta\left((\alpha\beta)^t\right)=$$

$$\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}(b_j+1)(\alpha\beta)^{t(e_pu^i+e_qv^j)}=\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}(b_j+1)(\alpha^{u^i}\beta^{v^j})^t=$$

$$\sum_{\substack{0\leqslant i<c_p\\ 0\leqslant j<c_qd}}(b_j+1)Tr_1^M\left((\alpha^{u^i}\beta^{v^j})^t\right)\sum_{\substack{i=0,1\\ j=0,1}}a_iA_i(x^{e_p})B_j\left(x^{e_q}\beta^a\right)=$$

$$\sum_{\substack{i=0,1\\ j=0,1}}a_i\sum_{t\in A_i}x^{e_pt}\sum_{s\in B_j}(x^{e_q}\beta^a)^s=\sum_{\substack{i=0,1\\ j=0,1}}a_i\sum_{\substack{t\in A_i\\ s\in B_j}}x^{e_pt+e_qs}\beta^{as}=$$

$$\sum_{\substack{i,j=0,1\\ 0\leqslant t_1<(p-1)/2\\ 0\leqslant s_1<(q-1)/2}}a_ix^{e_pu^{i+2\eta_1}+e_qv^{j+2\eta_1}}\beta^{av^{j+2\eta_1}}=\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}a_ix^{e_pu^i+e_qv^j}\beta^{av^j}\bmod x^{pq}-1$$

$$\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}a_ix^{e_pu^i+e_qv^j}\beta^{av^j}|_{x=(\alpha\beta)^t}=\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}a_i(\alpha\beta)^{t(e_pu^i+e_qv^j)}\beta^{av^j}=$$

$$\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}a_i(\alpha^{u^i}\beta^{v^j})^t\beta^{av^j}=\sum_{\substack{0\leqslant i<p-1\\ 0\leqslant j<q-1}}a_i\alpha^{u^it}\beta^{(t+a)v^j}=\sum_{\substack{0\leqslant i<c_p\\ 0\leqslant j<c_qd}}a_iTr_1^M\left(\alpha^{u^it}\beta^{(t+a)v^j}\right)$$

所以，

$$J_{p,q}^{(a)}(t)=\frac{q-1}{2}\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})+\frac{p-1}{2}\sum_{0\leqslant j<c_q}Tr_1^n\left((\beta^{t+a})^{v^j}\right)+$$
$$\sum_{0\leqslant j<c_q}Tr_1^n(\beta^{v^jt})+\sum_{\substack{0\leqslant i<c_p\\ 0\leqslant j<c_qd}}a_iTr_1^M\left(\alpha^{u^it}\beta^{(t+a)v^j}\right)+\sum_{\substack{0\leqslant i<c_p\\ 0\leqslant j<c_qd}}(b_j+1)Tr_1^M\left((\alpha^{u^i}\beta^{v^j})^t\right)=$$
$$\frac{q-1}{2}\sum_{0\leqslant i<c_p}Tr_1^m(\alpha^{u^it})+\sum_{0\leqslant j<c_q}\left[Tr_1^n\left(\beta^{v^jt}(1+\frac{p-1}{2}\beta^{av^j})\right)\right]+$$
$$\sum_{\substack{0\leqslant i<c_p\\ 0\leqslant j<c_qd}}\left[Tr_1^M\left((\alpha^{u^i}\beta^{v^j})^t(a_i\beta^{av^j}+b_j+1)\right)\right]$$

又因为

$$(a_0,a_1)=\begin{cases}(1,0) & p\equiv\pm1\bmod 8\\ (\omega,\omega^2) & p\equiv\pm3\bmod 8\end{cases}$$

$$(b_0+1,b_1+1)=\begin{cases}(0,1) & q\equiv\pm1\bmod 8\\ (1+\omega,1+\omega^2)=(-\omega^2,-\omega) & q\equiv\pm3\bmod 8\end{cases}$$

所以该定理得证。

采用文献[6]中的方法，根据定理1中NRP的迹表示，可直接得到其线性复杂度。

定理 2 序列 $J_{p,q}^{(a)}$ 的线性复杂度 $L(s^\infty)$ 为

$$L(s^\infty)=(p-1)\varepsilon(\frac{q-1}{2})+(q-1)+\begin{cases}\dfrac{3(p-1)(q-1)}{4} & p,q\equiv\pm1\bmod 8\\ (p-1)(q-1) & \text{其他}\end{cases}$$

其中，$\varepsilon(\dfrac{q-1}{2})=i$ 当且仅当 $\dfrac{q-1}{2}\equiv i\bmod 2$。

证明：由 p,q,α,β,ω 的定义可知，定理 1 的迹表达式中 $\alpha^{u^it}\beta^{v^jt}$ 前的系数均不为 0，从而该定理得证。

4 结束语

由定理 2 可知，NRP 具有很好的线性复杂度。同时，本文另外的工作证明它们也具有非常低的自相关值和互相关值。作为密钥流序列，它们可抵抗 Berlekamp-Massey 算法的攻击以及差分攻击。这些序列可采用类似文献[2]的改进的 Jacobi 序列的生成方法实现。总之，这类新的序列有很好的应用价值。 （下转第 142 页）