基于模$2p^m$的欧拉商的二元序列的线性复杂度

杜小妮　　李　丽*　　张福军

(西北师范大学数学与统计学院　兰州　730070)

摘　要：基于欧拉商模奇素数幂构造的伪随机序列均具有良好的密码学性质。该文根据剩余类环理论，利用模$2p^m$ (p为奇素数，整数$m\ge 1$)的欧拉商构造了一类周期为$2p^{m+1}$的二元序列，并在$2^{p-1}\not\equiv 1(\bmod\ p^2)$的条件下借助有限域$F_2$上确定多项式根的方法，给出了序列的线性复杂度。结果表明，序列的线性复杂度取值为$2(p^{m+1}-p)$或$2(p^{m+1}-1)$不小于其周期的1/2，能够抵抗Berlekamp-Massey(B-M)算法的攻击，是密码学意义上性质良好的伪随机序列。

关键词：有限域；二元序列；欧拉商；线性复杂度；极小多项式

中图分类号：TN918.4　　**文献标识码**：A　　**文章编号**：1009-5896(2019)12-3000-06

DOI: 10.11999/JEIT190071

Linear Complexity of Binary Sequences Derived from Euler Quotients Modulo $2p^m$

DU Xiaoni　　LI Li　　ZHANG Fujun

(*College of Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Families of pseudorandom sequences derived from Euler quotients modulo odd prime power possess sound cryptographic properties. In this paper, according to the theory of residue class ring, a new classes of binary sequences with period $2p^{m+1}$ is constructed using Euler quotients modulo $2p^m$, where p is an odd prime and integer $m\ge 1$. Under the condition of $2^{p-1}\not\equiv 1(\bmod\ p^2)$, the linear complexity of the sequence is examined with the method of determining the roots of polynomial over finite field F_2. The results show that the linear complexity of the sequence takes the value $2(p^{m+1}-p)$ or $2(p^{m+1}-1)$, which is larger than half of its period and can resist the attack of Berlekamp-Massey (B-M) algorithm. It is a good sequence from the viewpoint of cryptography.

Key words: Finite fields; Binary sequences; Euler quotients; Linear complexity; Minimal polynomial

1　引言

伪随机序列在扩频通信、雷达系统及流密码等领域有着极为广泛的应用[1–3]，序列的线性复杂度是度量序列伪随机性的一个重要指标。若(s_u)为有限域$F_2=\{0,1\}$上周期为N的序列，其线性复杂度定义为生成序列最短线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)的长度L，即使

$$s_{u+L}+c_{L-1}s_{u+L-1}+\cdots+c_1s_{u+1}+c_0s_u=0,\quad \forall u\ge 0 \tag{1}$$

成立的最小正整数L，其中$c_0=1$，$c_1,c_2,\cdots,c_{L-1}\in F_2$。令$M(x)=x^L+c_{L-1}x^{L-1}+\cdots+c_0\in F_2[x]$是序列$(s_u)$的极小多项式。定义$S(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}\in F_2[x]$为$(s_u)$的生成多项式，易得

$$M(x)=(x^N-1)/\gcd\Big(x^N-1,S(x)\Big) \tag{2}$$

因此，

$$L((s_u))=N-\deg\Big(\gcd(x^N-1,S(x))\Big) \tag{3}$$

根据B-M算法，若序列(s_u)的线性复杂度$L((s_u))\ge \dfrac{N}{2}$，则认为该序列能够抵抗已知明文的攻击。

已有大量文献研究了序列的线性复杂度，如文献[4,5]讨论了Jacobi和Legendre多项式商序列的线性复杂度，文献[6–9]讨论了广义分圆序列的线性复

收稿日期：2019-01-24；改回日期：2019-06-20；网络出版：2019-07-09

*通信作者：　李丽　ymxlili36@126.com

基金项目：国家自然科学基金(61462077, 61562077, 61772022)，上海市自然科学基金(16ZR1411200)

Foundation Items: The National Natural Science Foundation of China (61462077, 61562077, 61772022), The Shanghai Municipal Natural Science Foundation (16ZR1411200)

杂度。2012年Chen等人[10-13]研究了基于费马商及其扩展函数定义的周期为p^2的二元序列的线性复杂度，并将研究成果推广到了模数为奇素数幂的欧拉商。现有的文献研究集中于模素数幂的欧拉商构造的模为奇数的序列。而关于模偶数的欧拉商的文献非常少，文献[14]确定了基于Carmichael商模$2p$和$2^e(e>2)$构造的二元序列的线性复杂度，2018年Zhang等人[15]给出了基于模$2p$的欧拉商构造的周期为$2p^2$(p为奇素数)的序列的线性复杂度，而周期为$2p^{m+1}(m>1)$的二元序列尚未被研究。因而，本文在文献[15]的基础上进行了推广，即基于欧拉商模$2p^m$定义的二元序列，并求出了该序列的线性复杂度。

设p是奇素数，整数$m\ge 1, u\ge 0$且$\gcd(u,2p)$=1，模$2p^m$的欧拉商[13] $q_{2p^m}(u)$定义为

$$q_{2p^m}(u)\equiv\frac{u^{\varphi(2p^m)}-1}{2p^m}(\bmod\ 2p^m) \tag{4}$$

其中，$0\le q_{2p^m}(u)\le 2p^m-1$, $\varphi(-)$为欧拉函数。当$\gcd(u,2p)\ne 1$时，定义$q_{2p^m}(u)=0$。

定义二元门限序列(e_u)为

$$e_u=\begin{cases}0\ , & 0\le\dfrac{q_{2p^m}(u)}{2p^m}<\dfrac{1}{2}\\ 1\ , & \dfrac{1}{2}\le\dfrac{q_{2p^m}(u)}{2p^m}<1\end{cases} \tag{5}$$

易证序列(e_u)的周期为$2p^{m+1}$，因为对任意的$k\in Z$，以及$\gcd(u,2p)=1$，有

$$q_{2p^m}(u+2kp^m)\equiv q_{2p^m}(u)+kp^{m-1}(p-1)u^{-1}\cdot(\bmod\ 2p^m) \tag{6}$$

下文中将讨论序列(e_u)的线性复杂度。为确定序列的线性复杂度，本文给出序列的等价定义，首先引入如下记号。注意到当$\gcd(u,2p)=1$时，总有

$$q_{2p^m}(u)\equiv\frac{\left(u^{\frac{p^{m-1}(p-1)}{2}}-1\right)\left(u^{\frac{p^{m-1}(p-1)}{2}}+1\right)}{2p^m}\cdot(\bmod\ 2p^m) \tag{7}$$

所以$q_{2p^m}(u)$总是偶数。另外，

$$q_{2p^m}(uv)\equiv q_{2p^m}(u)+q_{2p^m}(v)(\bmod\ 2p^m),\quad \gcd(uv,2p)=1 \tag{8}$$

令$u\in R=Z_{2p^{m+1}}/Z^*_{2p^{m+1}}$，其中，$Z_{2p^{m+1}}$表示模$2p^{m+1}$的剩余类环，$Z^*_{2p^{m+1}}$表示$Z_{2p^{m+1}}$中的全体可逆元组成的集合。定义

$$D_l{}^{(m)}=\left\{u: q_{2p^m}(u)=2l(\bmod 2p^m), u\in Z^*_{2p^{m+1}}\right\},\quad 0\le l\le p^m-1 \tag{9}$$

总假设g是模$2p^{m+1}$的一个本原元且满足$q_{2p^m}(g)=2$。否则，若$q_{2p^m}(g)=2a\ne 2$，显然$\gcd(a,p)=1$，当$\gcd(a^{-1},p-1)=1$且由式(8)可得，$q_{2p^m}(g^{a^{-1}})=2$，其中，a^{-1}为a模p^m的逆元。从而对所有的$0\le k<p-1$，有$q_{2p^m}(g^{a^{-1}+kp^m})\equiv 2(\bmod\ 2p^m)$。因此由式(8)得

$$D_0{}^{(m)}=\left\{g^{kp^m}(\bmod\ 2p^{m+1}):0\le k\le p-2\right\} \tag{10}$$

是乘法群$Z^*_{2p^{m+1}}$的1个子群，此外对于$l=0,1,\cdots,p^m-1$，有

$$D_l{}^{(m)}=g^l D_0{}^{(m)}=\left\{g^l\cdot a(\bmod\ 2p^{m+1}):a\in D_0^{(m)}\right\} \tag{11}$$

因此，每一个$D_l{}^{(m)}$的基数$\#D_l{}^{(m)}=p-1$且$D_l{}^{(m)}(0\le l\le p^m-1)$构成了集合$Z^*_{2p^{m+1}}$的一个划分，即$Z^*_{2p^{m+1}}=\bigcup_{l=0}^{p^m-1}D_l{}^{(m)}$。故序列$(e_u)$的等价定义为

$$e_u=\begin{cases}0\ , & u\in D_0^{(m)}\bigcup\cdots\bigcup D^{(m)}_{(p^m-1)/2}\bigcup R,\\ 1\ , & u\in D^{(m)}_{(p^m+1)/2}\bigcup\cdots\bigcup D^{(m)}_{p^m-1},\end{cases}\quad u\ge 0, u\in R=Z_{2p^{m+1}}/Z^*_{2p^{m+1}} \tag{12}$$

下文将研究当$2^{p-1}\not\equiv 1(\bmod\ p^2)$时序列$(e_u)$的线性复杂度。

2　主要结论及其证明

2.1　主要结论

若$m=1$时，Zhang等人[15]给出了如下结论：

定理1[15]　设(e_u)是周期为$2p^2$的二元序列，若$2^{p-1}\not\equiv 1(\bmod\ p^2)$，则$(e_u)$的线性复杂度满足

$$L((e_u))=\begin{cases}2(p^2-p), & p\equiv 1(\bmod\ 4)\\ 2(p^2-1), & p\equiv 3(\bmod\ 4)\end{cases} \tag{13}$$

若$m>1$时，定理1可推广为定理2。

定理2　设(e_u)为式(5)定义的周期为$2p^{m+1}$的二元序列，若$2^{p-1}\not\equiv 1(\bmod\ p^2)$，则$(e_u)$的线性复杂度满足

$$L((e_u))=\begin{cases}2(p^{m+1}-p), & p\equiv 1(\bmod 4)\\ 2(p^{m+1}-p), & p\equiv 3(\bmod 4),\ m\text{为偶数}\\ 2(p^{m+1}-1), & p\equiv 3(\bmod 4),\ m\text{为奇数}\end{cases} \tag{14}$$

2.2 辅助引理

本节将给出证明主要结论所需的引理。

假设$\bar{F}_2$是F_2的代数闭包，$\beta\in\bar{F}_2$为p^{m+1}次本原单位根，则$\beta^{p^{m+1}}=1$。如无特殊说明，$D^{(n)}$的下标总是模p^n，其中$n\ge 1$。为了方便起见，定义

$$D_l^{(n+1)}(\bmod\ 2p^{n+1})=\{u(\bmod\ 2p^{n+1}):u\in D_l^{(n+1)}\} \tag{15}$$

引理1 对任意的$0\le l<p^m$，若$u(\bmod\ 2p^{m+1})\in D_{l'}^{(m)}$, $0\le l'<p^m$，则有

$$uD_l^{(m)}=\left\{uv(\bmod\ 2p^{m+1}):v\in D_l^{(m)}\right\}=D_{l+l'}^{(m)} \tag{16}$$

证明 若$u\in D_{l'}^{(m)}$，$v\in D_l^{(m)}$，则有$q_{2p^m}(u)=2l'$，$q_{2p^m}(v)=2l$，由式(8)可知

$$q_{2p^m}(uv)=q_{2p^m}(u)+q_{2p^m}(v)=2(l+l')\cdot(\bmod\ 2p^m) \tag{17}$$

从而$uD_l^{(m)}=D_{l+l'}^{(m)}$，该引理得证。

引理2 (1) 若$1\le n\le m$, $0\le l\le p^m-1$，则$D_l^{(m)}(\bmod\ 2p^{n+1})=D_l^{(n)}$；

(2) 若$0\le l\le p^m-1$，则$D_l^{(m)}(\bmod\ 2p)=Z_{2p}^*$；

(3) 若$r\ge 1$，则$\{u(\bmod\ p^r):u\in Z_{2p^r}^*\}=Z_{p^r}^*$[15]。

证明 (1) 只需证当$m=n+1$时成立，对任意的$1\le n\le m$，可以利用数学归纳法直接得证。首先对任意的$u\in D_l^{(n+1)}$，由文献[16]的命题4.1易得

$$q_{2p^n}(u)\equiv q_{2p^{n+1}}(u)\equiv 2l(\bmod\ 2p^n) \tag{18}$$

因为$2p^{n+1}$是$q_{2p^n}(u)$的周期，所以$u(\bmod\ 2p^{n+1})\in D_l^{(n)}$，进而有

$$D_l^{(n+1)}(\bmod\ 2p^{n+1})\subseteq D_l^{(n)} \tag{19}$$

其次，若对任意的$u,u'\in D_l^{(n+1)}$，有$u\equiv u'(\bmod\ 2p^{n+1})$成立，不妨设$u=u'+2k_0p^{n+1}$，其中$k_0\in Z_p$，根据式(6)有

$$\begin{aligned}2l&\equiv q_{2p^{n+1}}(u)\equiv q_{2p^{n+1}}(u'+2k_0p^{n+1})\\&\equiv q_{2p^{n+1}}(u')+k_0p^n(p-1)(u')^{-1}(\bmod\ 2p^{n+1})\end{aligned} \tag{20}$$

只有当$k_0=0, u=u'$时，

$$q_{2p^{n+1}}(u)\equiv q_{2p^{n+1}}(u')(\bmod\ 2p^{n+1}) \tag{21}$$

因此，

$$\#\{u(\bmod\ 2p^{n+1}):u\in D_l^{(n+1)}\}=p-1 \tag{22}$$

又因为$\#D_l^{(n)}=p-1$，从而该结论得证。

(2) 由文献[15]的引理3可知$\{u(\bmod\ 2p):u\in D_l^{(1)}\}=Z_{2p}^*$，由引理2的证明(1)得$\{u(\bmod\ 2p):u\in D_l^{(m)}\}=Z_{2p}^*$。

定义多项式

$$D_l^{(m)}(x)=\sum_{u\in D_l^{(m)}}x^u\in F_2[x]\quad 0\le l\le p^m-1 \tag{23}$$

则(e_u)的生成多项式为

$$E(x)=\sum_{u=0}^{2p^{m+1}-1}e_ux^u=\sum_{l=\frac{p^m+1}{2}}^{p^m-1}D_l^{(m)}(x)\in F_2[x] \tag{24}$$

如无特殊说明，下文中的计算均在有限域F_2中进行。 证毕

引理3 (1) 若$v\in Z_{2p^{m+1}}^*$，则$\sum_{l=0}^{p^m-1}D_l^{(m)}(\beta^v)=0$；

若之前加(2)若$0\le l<p^m$，则

$$D_l^{(m)}(\beta^{kp^m})=\begin{cases}1, & k\not\equiv 0(\bmod\ p)\\ 0, & 其他\end{cases} \tag{25}$$

证明 (1) 因为$Z_{2p^{m+1}}^*=\bigcup_{l=0}^{p^m-1}D_l^{(m)}$，所以

$$\sum_{l=0}^{p^m-1}D_l^{(m)}(\beta^v)=\sum_{l=0}^{p^m-1}\sum_{u\in D_l^{(m)}}\beta^{vu}=\sum_{u\in Z_{2p^{m+1}}^*}\beta^{vu} \tag{26}$$

则由引理2(3)可得

$$\begin{aligned}\sum_{l=0}^{p^m-1}D_l^{(m)}(\beta^v)&=\sum_{u\in Z_{p^{m+1}}^*}\beta^{vu}\\&=\sum_{u=0}^{p^{m+1}-1}\beta^{vu}-\sum_{u\in Z_{p^m}}(\beta^{pv})^u=0\end{aligned} \tag{27}$$

(2) 设$\theta=\beta^{p^m}\in\bar{F}_2$，即$\theta$是$p$次本原单位根，若对任意的$0\le l<p^m$，根据引理2(2)有

$$D_l^{(m)}(\beta^{kp^m})=\sum_{u\in D_l^{(m)}}\theta^{ku}=\sum_{j\in Z_{2p}^*}\theta^{kj} \tag{28}$$

当$k\not\equiv 0(\bmod\ p)$时，由引理2(3)得

$$\sum_{j\in Z_{2p}^*}\theta^{kj}=\sum_{j\in Z_p^*}\theta^{kj}=1+\frac{1-\theta^{kp}}{1-\theta^k}=1 \tag{29}$$

否则，

$$\sum_{j\in Z_{2p}^*}\theta^{kj}=\sum_{j\in Z_p^*}1=p-1=0 \tag{30}$$

证毕

为了方便，对$1\le n\le m, 0\le l\le p^n-1$，定义

$$\Lambda_l^{(n)}(x)=\sum_{i=\frac{p^n+1}{2}}^{p^n-1}D_{i+l}^{(n)}(x)\in F_2[x] \tag{31}$$

显然$E(x)=\Lambda_0^{(m)}(x)$。需要注意的是，由于

$\beta \in \bar{F}_2$ 是p^{m+1}次本原单位根，对所有的$0 \le u < p^{m+1}$，有$\beta^{p^{m+1}+u} = \beta^u$，所以在引理4和引理5中将只讨论$0 \le u \le p^{m+1}-1$的情形。

引理4　设$\beta \in \bar{F}_2$为p^{m+1}次本原单位根，则

$$E(x) = \begin{cases} 0, & u = 0, \\ \dfrac{p^m-1}{2}, & u \in p^m Z_p^*, \\ \varLambda_0^{(n)}(\beta^{vp^{m-n}}), & u \in p^{m-n} Z_{p^{n+1}}^*, \\ & 1 \le n \le m \end{cases} \tag{32}$$

证明　(1) 当$u=0$，由于$\#D_l{}^{(m)} = p-1$，所以

$$E(\beta^0) = E(1) = \sum_{l=\frac{p^m+1}{2}}^{p^m-1} \sum_{j \in D_l^{(m)}} 1 = \frac{(p^m-1)(p-1)}{2} \equiv 0 \tag{33}$$

(2) 当$u \in p^m Z_p^*$时，令$u = kp^m$，则$k \in Z_p^*$，由引理3(2)易知

$$E(\beta^u) = E(\beta^{kp^m}) = \sum_{l=\frac{p^m+1}{2}}^{p^m-1} D_l^{(m)}(\beta^{kp^m}) = \sum_{l=\frac{p^m+1}{2}}^{p^m-1} 1 = \frac{p^m-1}{2} \tag{34}$$

(3) 当$u \in p^{m-n} Z_{p^{n+1}}^*, 1 \le n \le m, 0 \le l \le p^n-1$时，令$u = vp^{m-n}, v \in Z_{p^{n+1}}^*$，则

$$E(\beta^u) = \sum_{l=\frac{p^m+1}{2}}^{p^m-1} \sum_{j \in D_l^{(m)}} \beta^{(vp^{m-n})^j} \tag{35}$$

l从$(p^m+1)/2$到p^m-1时，$l(\bmod\ p^n)$取遍$0,1,\cdots,p^n-1, 1+(p^{m-n}-1)/2$次，以及从$(p^n+1)/2$到$p^n-1$额外1次。注意到，$Z_{2p^{n+1}}^* = \bigcup_{l=0}^{p^n-1} D_l{}^{(n)}$且$\beta^{p^{m-n}} \in \bar{F}_2$是$p^{n+1}$次本原单位根，由引理2(2)和引理3(1)可知

$$E(\beta^u) = \sum_{l=0}^{p^n-1} \sum_{j \in D_l^{(n)}} \beta^{(vp^{m-n})^j} + \sum_{l=\frac{p^n+1}{2}}^{p^n-1} \sum_{j \in D_l^{(n)}} \beta^{(vp^{m-n})^j} = \varLambda_0^{(n)}(\beta^{vp^{m-n}}) \tag{36}$$

故此引理得证。

引理5　设$\beta \in \bar{F}_2$是p^{m+1}次本原单位根，若$2^{p-1} \not\equiv 1(\bmod\ p^2)$，则对任意的$1 \le n \le m$，$u \in p^{m-n} Z_{p^{n+1}}^*$，有$E(\beta^u) \ne 0$。

证明　当$u \in p^{m-n} Z_{p^{n+1}}^*$，对任意的$0 \le l \le p^n-1$，根据引理1和引理4，只需证$\varLambda_l^{(n)}(\beta^{p^{m-n}}) \ne 0$，假设存在$1 \le n_0 \le m$　$0 \le l_0 \le p^{n_0}-1$，使得$\varLambda_{l_0}^{(n_0)}(\beta^{p^{m-n_0}}) = 0$，限定$2^{p-1} \not\equiv 1(\bmod\ p^2)$，由文献[15]的引理6，令$h = 2+p^2$，因为$h$是奇数，所以$h^{p-1} \not\equiv 1(\bmod\ 2p^{m+1})$，因此$q_{2p^m}(h) = 2\ell \ne 0$且$h \in D_\ell{}^{(m)}$，由引理1可知，对$0 \le j \le p^n-1$，有

$$0 = (\varLambda_{l_0}^{(n_0)}(\beta^{p^{m-n_0}}))^{2^j} = \varLambda_{l_0}^{(n_0)}(\beta^{p^{m-n_0}h^j}) = \varLambda_{l_0+j\ell}^{(n_0)}(\beta^{p^{m-n_0}}) \tag{37}$$

即对所有的$0 \le l \le p^n-1$，都有$\varLambda_l^{(n)}(\beta^{p^{m-n}}) = 0$。令$v \in D_k^{(n)}, 0 \le k \le p^n-1$，根据引理1

$$\varLambda_l^{(n)}(\beta^{vp^{m-n}}) = \sum_{i=\frac{p^n+1}{2}}^{p^n-1} \sum_{j \in D_{l+i}^{(n)}} \beta^{vp^{m-n}j} = \varLambda_{l+k}^{(n)}(\beta^{p^{m-n}}) = 0 \tag{38}$$

显然对任意的$v \in Z_{2p^{n+1}}^* = \bigcup_{k=0}^{p^n-1} D_k{}^{(n)}$，有$\varLambda_l^{(n)}(\beta^{vp^{m-n}}) = 0$，由引理2(3)可得，对任意的$v \in Z_{p^{n+1}}^*$，有$\varLambda_l^{(n)}(\beta^{vp^{m-n}}) = 0$，其中，

$$\varLambda_l^{(n)}(\beta^u) = \varLambda_l^{(n)}(\beta^{vp^{m-n}}) = 0, u = vp^{m-n}, v \in Z_{p^{n+1}}^* \tag{39}$$

记$\varLambda_l^{(n)\prime}(x)$表示$\varLambda_l^{(n)}(x)$的导数，即$\varLambda_l^{(n)\prime}(x) = \sum_{i=\frac{p^n+1}{2}}^{p^n-1} \sum_{v \in D_{l+i}^{(n)}} x^{v-1}(\bmod\ 2)$。特别地，$\varLambda_l^{(n)\prime}(\beta^u) = \beta^{-u}\varLambda_l^{(n)}(\beta^u) = 0$，对所有的$u \in p^{m-n} Z_{p^{n+1}}^*$，$0 \le l \le p^n-1$成立，即对任意的$u \in p^{m-n} Z_{p^{n+1}}^*$均为$\varLambda_l^{(n)}(x)$的二重根。

另一方面，对任意的$u \in p^{m-n} Z_{p^{n+1}}^*$，$\Gamma^{(n)}(x)$的重根$\beta^u$有$p^{n+1}-p^n$个，其中，

$$\Gamma^{(n)}(x) = \left(\frac{x^{p^{n+1}}-1}{x^{p^n}-1}\right)^2 = 1 + x^{2p^n} + x^{4p^n} + \cdots + x^{2(p-1)p^n} \tag{40}$$

因此，$\Gamma^{(n)}(x) | \varLambda_l^{(n)}(x)$, $0 \le l \le p^n-1$。特别地，令$\varLambda_0^{(n)}(x) = \Gamma^{(n)}(x)\pi^{(n)}(x)$，根据$\varLambda_0^{(n)}(x)$的定义，可以看出$\varLambda_0^{(n)}(x)$有$(p^n-1)(p-1)/2$项且$\deg \varLambda_0^{(n)}(x) < 2p^{n+1}$，则$\deg \pi^{(n)}(x) = \deg \varLambda_0^{(n)}(x) - \deg \Gamma^{(n)}(x) < 2p^n$，故令$\pi^{(n)}(x) = \sum_{j=0}^{t-1} x^{v_j}$，其中$0 \le v_0 < v_1 < \cdots < v_{t-1} < 2p^n$，因此

$$\Gamma^{(n)}(x)\pi^{(n)}(x) = \sum_{k=0}^{p-1} \sum_{j=0}^{t-1} x^{v_j + 2kp^n} (\bmod\ x^{2p^{n+1}}-1) \tag{41}$$

显然，$\Gamma^{(n)}(x)\pi^{(n)}(x)$总共有$pt$项，这与

$\Lambda_0^{(n)}(x)$有$(p^n-1)(p-1)/2$项矛盾。从而对任意的$0\le l\le p^n-1$，有$\Lambda_l^{(n)}(\beta)\neq 0$。即对所有的$u\in p^{m-n}Z_{p^{n+1}}^*$，都有$E(\beta^u)=\Lambda_0^{(n)}(\beta^u)\neq 0$。 证毕

2.3 定理2的证明

证明 注意到在F_2上，$x^{2p^{n+1}}-1=(x^{p^{n+1}}-1)^2=\Gamma^{(n)}(x)(x^{p^n}-1)^2$，则由引理4和引理5可得，当$p\equiv 1(\bmod\ 4)$时，$u\in p^mZ_p$，有$E(\beta^u)=0$，即$E(x)$和$x^{p^n}-1$公共根的个数为$p$，由式(3)知$L((e_u))=2(p^{m+1}-p)$。当$p\equiv 3(\bmod\ 4)$且$m$为偶数时，若$u\in p^mZ_p$，有$E(\beta^u)=0$，即$E(x)$和$x^{p^n}-1$公共根的个数为$p$，此时$L((e_u))=2(p^{m+1}-p)$，而当$p\equiv 3(\bmod\ 4)$且$m$为奇数时，仅有$E(\beta^0)=0$为$E(x)$的二重根，此时$L((e_u))=2(p^{m+1}-1)$，定理得证。

3 结束语

本文利用模$2p^m$的欧拉商构造了一类周期为$2p^{m+1}$的二元门限序列(e_u)，并在$2^{p-1}\not\equiv 1(\bmod\ p^2)$的条件下，研究了该序列的线性复杂度。结果表明，线性复杂度的取值为$2(p^{m+1}-p)$或$2(p^{m+1}-1)$依赖于素数p模4的余数以及m的奇偶性。显然序列的线性复杂度均大于周期的一半，因而用作密钥流序列能够抵抗B-M算法的攻击，在保密通讯中可以有广泛的应用。此外，需要说明的是，满足条件$2^{p-1}\equiv 1(\bmod\ p^2)$的素数是非常稀少的，到目前为止，当$p<1.25\times 10^{15}$时，仅有两个素数$p=1093$和$p=3511$为Wieferich素数。因此，本文的结果对于大多数素数p都是对的，对满足条件$2^{p-1}\equiv 1(\bmod\ p^2)$的素数$p$，序列$(e_u)$的线性复杂度留做后续研究。

参 考 文 献

[1] DING Cunsheng, XIAO Guozhen, and SHAN Weijuan. The Stability Theory of Stream Ciphers[M]. Berlin, Heidelberg: Springer-Verlag, 1991: 251–321.

[2] GOLOMB S W and GONG Guang. Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar[M]. Cambridge, UK: Cambridge University Press, 2005: 174–175.

[3] SU Wei, YANG Yang, ZHOU Zhengchun, *et al*. New quaternary sequences of even length with optimal auto-correlation[J]. *Science China Information Sciences*, 2018, 61(2): 022308. doi: 10.1007/s11432-016-9087-2.

[4] DAI Zongduo, GONG Guang, and SONG H Y. A trace representation of binary Jacobi sequences[J]. *Discrete Mathematics*, 2009, 309(6): 1517–1527. doi: 10.1016/j.disc.2008.02.024.

[5] CHEN Zhixiong. Linear complexity of Legendre-polynomial quotients[J]. *IET Information Security*, 2018, 12(5): 414–418. doi: 10.1049/iet-ifs.2017.0307.

[6] 李瑞芳, 柯品惠. 一类新的周期为$2pq$的二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2014, 36(3): 650–654. doi: 10.3724/SP.J.1146.2013.00751.

LI Ruifang and KE Pinhui. The linear complexity of a new class of generalized cyclotomic sequences with period $2pq$[J]. *Journal of Electronics & Information Technology*, 2014, 36(3): 650–654. doi: 10.3724/SP.J.1146.2013.00751.

[7] 杜小妮, 王国辉, 魏万银. 周期为$2p^2$的四阶二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2015, 37(10): 2490–2494.

DU Xiaoni, WANG Guohui, and WEI Wanyin. Linear complexity of binary generalized cyclotomic sequences of order four with period $2p^2$[J]. *Journal of Electronics & Information Technology*, 2015, 37(10): 2490–2494.

[8] 杜小妮, 赵丽萍, 王莲花. Z_4上周期为$2p^2$的四元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2018, 40(12): 2992–2997. doi: 10.11999/JEIT180189.

DU Xiaoni, ZHAO Liping, and WANG Lianhua. Linear complexity of quaternary sequences over Z_4 derived from generalized cyclotomic classes modulo $2p^2$[J]. *Journal of Electronics & Information Technology*, 2018, 40(12): 2992–2997. doi: 10.11999/JEIT180189.

[9] EDEMSKIY V, LI Chunlei, ZENG Xiangyong, *et al*. The linear complexity of generalized cyclotomic binary sequences of period p^n[J]. *Designs, Codes and Cryptography*, 2019, 87(5): 1183–1197. doi: 10.1007/s10623-018-0513-2.

[10] CHEN Zhixiong and DU Xiaoni. On the linear complexity of binary threshold sequences derived from Fermat quotients[J]. *Designs, Codes and Cryptography*, 2013, 67(3): 317–323. doi: 10.1007/s10623-012-9608-3.

[11] CHEN Zhixiong and WINTERHOF A. On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients[J]. *International Journal of Number Theory*, 2012, 8(3): 631–641. doi: 10.1142/S1793042112500352.

[12] DU Xiaoni, KLAPPER A, and CHEN Zhixiong. Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations[J]. *Information Processing Letters*, 2012, 112(6): 233–237. doi: 10.1016/j.ipl.2011.11.017.

[13] DU Xiaoni, CHEN Zhixiong, and HU Lei. Linear complexity

of binary sequences derived from Euler quotients with prime-power modulus[J]. *Information Processing Letters*, 2012, 112(14/15): 604–609. doi: 10.1016/j.ipl.2012.04.011.

[14] WU Chenhuang, CHEN Zhixiong, and DU Xiaoni. Binary threshold sequences derived from Carmichael quotients with even numbers modulus[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2012, E95.A(7): 1197–1199. doi: 10.1587/transfun.E95.A.1197.

[15] ZHANG Jingwei and ZHAO Changan. Linear complexity and trace presentation of sequences with period $2p^2$[C]. 2018 IEEE International Symposium on Information Theory, Vail, USA, 2018: 2206–2210. doi: 10.1109/ISIT.2018.8437917.

[16] AGOH T, DILCHER K, and SKULA L. Fermat quotients for composite moduli[J]. *Journal of Number Theory*, 1997, 66(1): 29–50. doi: 10.1006/jnth.1997.2162.

杜小妮：女，1972年生，教授，博士生导师，研究方向为密码学与信息安全.

李　丽：女，1991年生，硕士生，研究方向为密码学与信息安全.

张福军：男，1995年生，硕士生，研究方向为密码学与信息安全.