文章编号:1007-5321(2018)02-0081-05　　**DOI**:10.13190/j.jbupt.2017-158

Fermat 数和一类极大周期序列的 2-adic 复杂度

王　艳，李顺波，赵　松，薛改娜
(西安建筑科技大学 理学院, 西安 710055)

摘要: 发现了 Fermat 数和由单圈 T 函数生成的极大周期序列的关系,利用 Fermat 数的素性理论研究了单圈 T 函数生成的第 k 位序列,按状态输出序列的 2-adic 复杂度取值和界. 结果表明,单圈 T 函数序列生成的这 2 种序列不能形成 l 序列.

关　键　词: Fermat 数; 序列; 2-adic 复杂度; 单圈 T 函数
中图分类号: TN918.1　　**文献标志码**: A

Fermat Number and 2-Adic Complexity of a Class of Maximum Period Sequence

WANG Yan,　LI Shun-bo,　ZHAO Song,　XUE Gai-na
(Department of Mathematics, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: The relationship between the Fermat number and the T function generated by single cycle T-function's maximal periodic sequence were found. The 2-adic complexity of the kth coordinate sequence and the state output sequence were studied. Values and bounds of the 2-adic complexity were obtained. It is shown that the two sequences generated by the single cycle T-function cannot form l-sequences.

Key words: Fermat number; sequence; 2-adic complexity; single circle T-function

法国数学家 Pierre de Fermat 于 1640 年提出了形如 $F_n = 2^{2^n} + 1$ 的数(后人称 Fermat 数)为素数的猜想,但 Euler 于 1732 年在研究该问题时发现 F_5 为合数,此后关于 Fermat 数的研究持续了几个世纪. Fermat 数在二进制计算机算法、二元序列的复杂度等研究中都有重要应用.

Lenstra 等[1-2] 利用 Fermat 数的素性和分解问题给出了一类由单圈 T 函数生成的极大周期序列,即第 k 位序列的 2-adic 复杂度,给出了该类序列由带进位的反馈移位寄存器(FCSR, feedback with carry shift register)的生成级数,并由此研究了单圈 T 函数按状态输出序列的 2-adic 复杂度,给出了其 2-adic 复杂度的估计.

1　预备知识

1.1　Fermat 数

定义 1　称形如 $2^{2^n} + 1\,(n = 0, 1, 2, \cdots)$ 的数为 Fermat 数,记作 F_n.

对 Fermat 数的因子分解问题,有如下结论[3]:

1) F_0、F_1、F_2、F_3、F_4 为素数;

2) $F_5 \sim F_{11}$ 为合数,且人们对这些 Fermat 数已全部找到了素因子分解;

3) 对 F_{12}、F_{13}、F_{15}、F_{16}、F_{17}、F_{18}、F_{19}、F_{21}、F_{23} 已经找到部分因子;

收稿日期: 2017-08-04
基金项目: 陕西省自然科学基础研究计划项目(2014JQ1027);西安建筑科技大学基础研究基金项目(JC1416);国家自然科学基金项目(11471255);西安建筑科技大学校人才基金项目(RC1338)
作者简介: 王　艳(1982—), 女, 博士, 副教授, E-mail: wangyan@xauat.edu.cn.

4）对 F_{14}、F_{20}、F_{22}、F_{24} 已证明为合数，但未找到因子；

5）$F_0F_1F_2F_3\cdots F_n = F_{n+1} - 2$；

6）任意 2 个 Fermat 数 F_m、$F_n(m \neq n)$ 互素，即

$$(F_m, F_n) = 1$$

引理 1[3] 若 $2^m + 1$ 是素数，则 $m = 2^n$；反之不真.

引理 2[3] 当 $n \geqslant 2$ 时，F_n 的素因数必为形式

$$p = 2^{n+2}h + 1 \quad (h \in \mathbb{N})$$

引理 3[3] Fermat 合数除 641 外，没有其他小于10^6 的因子.

引理 4[3] 形如 $4t + 3(t \geqslant 1)$ 的素数均不为 Fermat 数的因子.

1.2 序列的 2-adic 复杂度

考虑到线性移位寄存器容易被攻击的问题，Klapper 等[4-5]提出了 FCSR. 一个 FCSR 由 r 个系数 $q_1, q_2, \cdots, q_r$，$(q_i \in \{0,1\}$，$i = 1, 2\cdots, r)$ 以及一个初始存储整数 m_{r-1}（可为任意整数）确定. 其结构如图 1 所示.

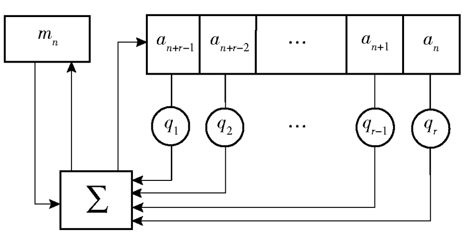

图 1　r 级 FCSR 结构

记 FCSR 的任一个状态为 $(a_{n-1}, a_{n-2}, \cdots, a_{n-r})$，$a_i \in \{0,1\}$，存储整数为 m_{n-1}，则移位寄存器的运算为

A1：计算 $\delta_n = \sum\limits_{k=1}^{r} q_k a_{n-k} + m_{n-1}$；

A2：右移一位，输出寄存器最右端的 a_{n-r}；

A3：令 $a_n = \delta_n \pmod 2$，将其放入寄存器的最左端；

A4：令 $m_n = (\delta_n - a_n)/2 = \lfloor \delta_n / 2 \rfloor$.

引理 5[4] 设 $\underline{x}$ 为最终周期序列. 则 $\alpha = \sum\limits_{i=0}^{\infty} x_i 2^i$ 是 2 个整数的商 p/q，其中 q 为生成 $\underline{x}$ 的 FCSR 的连接整数. 进而 $\underline{x}$ 是严格周期序列，当且仅当 $1 \leqslant \alpha \leqslant 0$.

这说明每一个最终周期序列都可以由一个 FCSR 产生. 反过来，下面的结果说明所有由 FCSR 生成的序列也都是最终周期的.

引理 6[6] 设序列 $\underline{x}$ 由 FCSR 生成，q 为 $\underline{x}$ 的连接整数，则 $\underline{x}$ 为最终周期序列，且存在整数 p 使得 $\alpha = \sum\limits_{i=0}^{\infty} x_i 2^i = p/q$.

设 $\underline{x}$ 为最终周期序列，q 为生成 $\underline{x}$ 的 FCSR 的连接整数，则称 q 为 $\underline{x}$ 的一个连接整数. 称 $\underline{x}$ 的连接整数中的最小的那个为 $\underline{x}$ 的极小连接整数.

下面的结果给出连接整数满足的性质：

引理 7[6] 设 $\underline{x}$ 为严格周期二元序列，q 为 $\underline{x}$ 的极小连接整数，则 q' 为 $\underline{x}$ 的一个连接整数当且仅当 q' 可被 q 整除.

引理 8[6] 设 $\underline{x}$ 为严格周期序列，T 为 $\underline{x}$ 的周期，则 $\underline{x}$ 的极小连接整数 q 满足 $q \leqslant 2^T - 1$.

FCSR 序列的周期完全由其极小连接整数确定. 类似于线性复杂度，2-adic 复杂度衡量一个周期序列需要用多大的 FCSR 来生成. 2-adic 复杂度定义如下.

定义 2[6] 设 $\underline{x}$ 为严格周期序列，$\sum\limits_{i=0}^{\infty} x_i 2^i = p/q$，其中 $\gcd(p, q) = 1$，称 $\phi_2(\underline{x}) = \mathrm{lb}(\Phi(p, q))$ 为 $\underline{x}$ 的 2-adic 复杂度，其中 $\Phi(p, q) = \max(|p|, |q|)$.

2-adic 复杂度度量一个二元序列由 FCSR[4] 生成的难度，它与线性复杂度没有必然的联系，即具有高线性复杂度的序列，其 2-adic 复杂度可能会很低，反之亦然. Klapper 提出了有理逼近算法，即对一条固定序列，只要已知其约 2 倍 2-adic 复杂度比特，就能唯一确定原序列. 这就要求密钥序列必须具有较高的 2-adic 复杂度，才能有效抵抗有理逼近攻击.

引理 9[6] 设 $\underline{x}$ 为严格周期二元序列，极小连接数为 q，则 $\underline{x}$ 的 2-adic 复杂度为 $\phi_2(\underline{x}) = \mathrm{lb}\, q$.

1.3 单圈 T 函数及其生成序列

记 $\boldsymbol{F}_2$ 为二元域，$\boldsymbol{F}_2^n$ 为 $\boldsymbol{F}_2$ 上的 n 维向量空间，其中 n 为正整数，称 $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1}) \in F_2^n$ 为一个 n 长单字. 在剩余类环 $\boldsymbol{Z}/(2^n)$ 中，x 可被表示成 $\sum\limits_{j=0}^{n-1} x_j 2^j$. 称 $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \cdots, \boldsymbol{x}_{m-1})^{\mathrm{T}} \in \boldsymbol{F}_2^{m \times n}$ 为一个多字，其中每一个 $\boldsymbol{x}_i(i = 0, 1, \cdots, m-1)$ 为 n 长单字，显然，多字 $\underline{\boldsymbol{x}}$ 也可被看作一个 $m \times n$ 矩阵.

定义 3[7-10] 设映射 $f: \boldsymbol{F}_2^{m \times n} \to \boldsymbol{F}_2^{l \times n}$ 为 $f(\underline{\boldsymbol{x}}) = \underline{\boldsymbol{x}}$，其中 $\underline{\boldsymbol{x}}$ 和 $\underline{\boldsymbol{y}}$ 是多字. 若输出 $\underline{\boldsymbol{y}}$ 的第 i 列只与输入 $\underline{\boldsymbol{x}}$ 的第 $0, 1, \cdots, i(0 \leqslant i < n)$ 列有关，则称 f 为一个 T 函数. 当 $m = l = 1$ 时，称 f 为一个单字 T 函数；反之称其为多字 T 函数. 注意，后面出现的 T 函数均指

单字 T 函数，其相应性质都可推广到多字 T 函数中.

设 $\boldsymbol{x}_0$ 为初始状态，T 函数 $f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$ 为状态转移函数，即 $f(\boldsymbol{x}_i)=\boldsymbol{x}_{i+1}$，于是可得 f 的状态序列 $\{\boldsymbol{x}_i\}_{i\geqslant 0}$. 若序列 $\{\boldsymbol{x}_i\}_{i\geqslant 0}$ 的极小周期为 $N=2^n$，则称 f 是单圈的.

定义"+"为域上的加法，"$\oplus$"为模 2 加法. 称由 $\boldsymbol{x}_i$ 第 k 位形成的序列 $\{x_{i,k}\}_{i=0}^{2^n-1}$ $(0\leqslant k<n)$ 为 $\boldsymbol{x}_i$ 的第 k 位序列，记为 $\underline{x}_k$. 由文献[11-12]知，$\underline{x}_k$ 的周期为 $N_k=2^{k+1}$，且

$$x_{i+N_k/2,k}=x_{i,k}\oplus 1 \tag{1}$$

T 函数 $f(x)$ 也可被表示为向量布尔函数，即 $f(x)=(f_0(x),f_1(x),\cdots,f_{n-1}(x))$，其中每一个分量函数 $f_k(x)$ $(0\leqslant k<n)$ 称为第 k 位布尔函数，其取值只与 x 的前 k 位有关[11]. 据定义 3 可知，第 k 位序列即为第 k 位分量布尔函数的输出序列.

2　单圈 T 函数序列的 2-adic 复杂度

引理 10　设 $f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$ 为单圈 T 函数，其状态序列 $\{\boldsymbol{x}_i\}_{i\geqslant 0}$ 的第 k 位序列 $\{x_{i,k}\}_{i=0}^{2^n-1}$ $(0\leqslant k<n)$ 的极小连接整数 q 满足 $q\leqslant 2^{2^{k+1}}-1$.

该结果可由引理 9 获得.

定理 1　设 $f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$ 为单圈 T 函数，其状态序列 $\{\boldsymbol{x}_i\}_{i\geqslant 0}$ 的第 k 位序列 $s_k\triangleq\{x_{i,k}\}_{i=0}^{2^n-1}$ $(0\leqslant k<n)$ 的 2-adic 复杂度 $\phi_2(s_k)$ 满足：

1）$k=0,1,2,3,4$ 时，$\phi_2(s_k)=\mathrm{lb}F_k$，其中 F_k 为第 k 个 Fermat 数；

2）$k\geqslant 5$ 时，若 $F_k=p_1p_2\cdots p_t$，记 s_k 的后 1/2 序列对应的十进制数 $\sum\limits_{i=2^{n-1}}^{2^n-1}x_{i,k}2^{i-2^{n-1}}$ 的因子集合为 P，并记 $P\cap\{p_1,p_2,\cdots,p_t\}=\{p_{j_1},p_{j_2},\cdots,p_{j_u}\}$，则 $\phi_2(s_k)=\mathrm{lb}\,\dfrac{F_k}{p_{j_1}p_{j_2}\cdots p_{j_u}}$.

证明　根据 2-adic 复杂度的定义，需讨论

$$\sum_{i=0}^{\infty}x_i2^i=\frac{\sum\limits_{i=0}^{T-1}x_i2^i}{1-2^T}=-\frac{\sum\limits_{i=0}^{2^{k+1}-1}x_i2^i}{2^{2^{k+1}}-1}=-\frac{\sum\limits_{i=0}^{2^{k+1}-1}x_i2^i}{(2^{2^k}-1)(2^{2^k}+1)} \tag{2}$$

由单圈 T 函数的性质，式(2)中分子可表示为

$$\sum_{i=0}^{2^{k+1}-1}x_i2^i=\sum_{i=1}^{2^k-1}(x_{i,k}2^i+x_{i+2^k,k}2^{i+2^k})=\sum_{i=1}^{2^k-1}[x_{i,k}2^i+(x_{i,k}\oplus 1)2^{i+2^k}] \tag{3}$$

考虑到 $\{x_i,x_i\oplus 1\}=\{0,1\}$，记 $S=\{i\,|\,x_{i+2^k,k}=1,0\leqslant i\leqslant 2^k-1\}$，设 $|S|=m$，则 S 也可简记为 $\{i_1,i_2,\cdots,i_m\}$，其中 $i_1<i_2<\cdots<i_m$，于是式(3)可表示为

$$\begin{aligned}&\sum_{i=1}^{2^k-1}[x_{i,k}2^i+(x_{i,k}\oplus 1)2^{i+2^k}]=\\&\sum_{i=1}^{2^k-1}(1\cdot 2^i)+\sum_{i=1,i\in S}^{2^k-1}x_{i,k}(2^{i+2^k}-2^i)=\\&(2^{2^k}-1)+(2^{2^k}-1)(2^{i_1}+2^{i_2}+\cdots+2^{i_m})=\\&(2^{2^k}-1)(1+2^{i_1}+2^{i_2}+\cdots+2^{i_m})\end{aligned}$$

因而式(1)成为

$$\frac{1+2^{i_1}+2^{i_2}+\cdots+2^{i_m}}{2^{2^k}+1} \tag{4}$$

而式(4)分母恰好为第 k 个 Fermat 数，记作 F_k，由文献[1-3]可知，前 5 个 Fermat 数 $F_0=3,F_1=5,F_2=17,F_3=257,F_4=65\ 537$ 均为素数，由引理 10 知 $\phi_2(s_k)=\mathrm{lb}F_k$.

当 $k\geqslant 5$ 时，由文献[1-2]可知，在目前可计算范围内 F_k 为合数，且皆为一次因子，记 $F_k=p_1p_2\cdots p_t$，则问题转化为求式(4)的最简分数. 记 s_k 的后 1/2 序列对应的十进制数 $\sum\limits_{i=2^{n-1}}^{2^n-1}x_{i,k}2^{i-2^{n-1}}$ 的因子集合为 P，并记 $P\cap\{p_1,p_2,\cdots,p_t\}=\{p_{j_1},p_{j_2},\cdots,p_{j_u}\}$，则式(4)的最简分数为

$$\frac{\dfrac{1+2^{i_1}+2^{i_2}+\cdots+2^{i_m}}{p_{j_1}p_{j_2}\cdots p_{j_u}}}{\dfrac{F_k}{p_{j_1}p_{j_2}\cdots p_{j_u}}}$$

因而 $\phi_2(s_k)=\mathrm{lb}\,\dfrac{F_k}{p_{j_1}p_{j_2}\cdots p_{j_u}}$. 特别地，$s_k$ 的后 1/2 序列对应的十进制数 $\sum\limits_{i=2^{n-1}}^{2^n-1}x_{i,k}2^{i-2^{n-1}}$ 恰为 F_k 的某个因子 p_i 时，$\phi_2(s_k)=\mathrm{lb}\,\dfrac{F_k}{p_i}$.　□

推论 1　设 $f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$ 为单圈 T 函数，其状态序列 $\{\boldsymbol{x}_i\}_{i\geqslant 0}$ 的第 k 位序列为 $s_k\triangleq\{x_{i,k}\}_{i=0}^{2^n-1}$ $(2\leqslant k<n)$. 则当式(4)中 $1+2^{i_1}+2^{i_2}+\cdots+2^{i_m}\neq 2^{n+2}h+1$ $(h\in\boldsymbol{N})$ 时，$\phi_2(s_k)=\mathrm{lb}F_k$.

证明　由引理 2 可知，当 $n\geqslant 2$ 时，F_n 的素因数必为形式 $p=2^{n+2}h+1$ $(h\in\boldsymbol{N})$，于是对满足

$$1+2^{i_1}+2^{i_2}+\cdots+2^{i_m}\neq 2^{n+2}h+1$$

的单圈 T 函数 k 位序列，式(4)为既约分式，故

$\phi_2(s_k)=\mathrm{lb}F_k$.

推论2 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列$\{\boldsymbol{x}_i\}_{i\geqslant0}$的第$k$位序列为$s_k\triangleq\{x_{i,k}\}_{i=0}^{2^n-1}$($6\leqslant k<n$),则当$\max\limits_{i_j\in S}i_j=i_m\leqslant19$时,$\phi_2(s_k)=\mathrm{lb}F_k$.

证明 由引理3可知,当$i_m<\mathrm{lb}\ 10^6\approx19.93$时,式(4)分母的因子都大于$10^6$. 此时式(4)的分子$1+2^{i_1}+2^{i_2}+\cdots+2^{i_m}\leqslant10^6$. 于是式(4)为既约分式,故$\phi_2(s_k)=\mathrm{lb}F_k$.

推论3 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列$\{\boldsymbol{x}_i\}_{i\geqslant0}$的第$k$位序列为$s_k\triangleq\{x_{i,k}\}_{i=0}^{2^n-1}$($6\leqslant k<n$),则当式(4)中$1+2^{i_1}+2^{i_2}+\cdots+2^{i_m}$为二进制形如$\cdots11_2$的素数时,$\phi_2(s_k)=\mathrm{lb}F_k$.

证明 由引理4可知,形如$4t+3$($t\geqslant1$)的素数,即二进制形如$\cdots11_2$的素数均不是Fermat数的因子. 因而式(4)为既约分式,故$\phi_2(s_k)=\mathrm{lb}F_k$.

进一步,对单圈T函数的第k位序列,有定理2.

定理2 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列$\{\boldsymbol{x}_i\}_{i\geqslant0}$的第$k$位序列$s_k$($0\leqslant k<n$)的周期为$T$,则$\phi_2(s_k)<T\leqslant\phi(q)<2^{T/2}$($k=0,1,2,\cdots,13$),其中$q$为$s_k$的极小连接整数,$\varphi(q)$为$q$的欧拉函数值.

证明

1) 由定理1可知

$$\phi_2(s_k)\leqslant\mathrm{lb}(2^{2^k}+1)<\mathrm{lb}2^{2^k}2^{2^k}=2^{k+1}=T$$

2) 当$k=0,1,2,\cdots,4$时,$2^{2^k}+1$为素数

$$\varphi(q)=\varphi(2^{2^k}+1)=2^{2^k}\geqslant2^{k+1}=T \tag{5}$$

式(5)中等号成立,当且仅当$k=0,1$.

当$5\leqslant k\leqslant13$时,由F_k的分解式[1-2]可知,所有的$\varphi(q)>2^{k+1}=T$.

3) 由定理1的证明知,序列s_k的极小连接整数$q\leqslant1+2^{2^k}=1+2^{T/2}$;同时,$\varphi(q)\leqslant q-1$对所有整数$q$都成立. 因而,$\varphi(q)<2^{T/2}$. □

对于单圈T函数的按状态输出序列,其周期较大,相应的2-adic复杂度由定理3给出.

定理3 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列为$S$,则$S$具有最大2-adic复杂度$\mathrm{lb}(2^{n\cdot2^{n-1}}+1)$.

证明 记按状态输出序列为

$S=\{x_{i,k}\}_{0\leqslant i\leqslant2^n-1,0\leqslant k\leqslant n-1}\triangleq\{s_j\}_{0\leqslant j\leqslant n\cdot2^n-1}$,考查

$$\sum_{i=0}^{\infty}x_i2^i=\frac{\sum\limits_{i=0}^{T-1}x_i2^i}{1-2^T}=\frac{\sum\limits_{i=0}^{n-1}\sum\limits_{j=0}^{2^n-1}x_{i,j}2^{j+i\cdot2^n}}{1-2^T} \tag{6}$$

根据单圈T函数生成序列的性质,若$x_{i,j}=1$,式(6)的分子前半部分的和为

$$\sum_{i=0}^{n-1}\sum_{j=0}^{2^{n-1}-1}1\times2^{j+i\cdot2^n}=2^{n\cdot2^{n-1}}-1$$

记S的后半部分序列中非0位置的下标为$t_1,t_2,\cdots,t_u$,则式(6)的分子后半部分的和为$(2^{n\cdot2^{n-1}}-1)\times(2^{t_1}+2^{t_2}+\cdots+2^{t_t})$,故式(6)的分子等于$(2^{n\cdot2^{n-1}}-1)(1+2^{t_1}+2^{t_2}+\cdots+2^{t_t})$,式(6)可约分为

$$\frac{1+2^{t_1}+2^{t_2}+\cdots+2^{t_t}}{1+2^{n\cdot2^{n-1}}}$$

因而S的最大2-adic复杂度为$\mathrm{lb}(2^{n\cdot2^{n-1}}+1)$. □

S的2-adic复杂度$\phi_2(S)$依赖于数$2^{n\cdot2^{n-1}}+1$的分解,当$n=2^m$时,这依然是Fermat数的分解问题;$n\neq2^m$且较大时,这对应大整数分解问题.

推论4 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列$S\triangleq\{\boldsymbol{x}_i\}_{i\geqslant0}$的周期为$T$,则$S$的最大2-adic复杂度$\max\ \phi_2(S)$满足

$$\frac{T}{2}<\max\ \phi_2(S)<\frac{T}{2}+1$$

证明 由

$$\max\ \phi_2(S)=\mathrm{lb}(2^{n\cdot2^{n-1}}+1)>\mathrm{lb}\ 2^{n\cdot2^{n-1}}=\frac{T}{2}$$

$$\mathrm{lb}(2^{n\cdot2^{n-1}}+1)<\mathrm{lb}2\times2^{n\cdot2^{n-1}}=\frac{T}{2}+1$$

可得.

对单圈T函数的按状态输出序列,引理8的结果可改进为推论5.

推论5 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列$S=\{\boldsymbol{x}_i\}_{i\geqslant0}$的周期为$T$,$q$为$S$的极小连接整数,则$\varphi(q)<2^{T/2}$.

证明 一方面,由定理3可知,序列S的最大连接整数$q\leqslant1+2^{n\cdot2^{n-1}}=1+2^{T/2}$;另一方面,$\varphi(q)\leqslant q-1$对所有整数$q$都成立. 因此,$\varphi(q)<2^{T/2}$.

推论6 设$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$为单圈T函数,其状态序列$S=\{\boldsymbol{x}_i\}_{i\geqslant0}$的周期为$T$,$q$为$S$的极小连接整数,则不等式

$$T<\varphi(q)$$

在域$\boldsymbol{F}_2$、$\boldsymbol{F}_2^2$、$\boldsymbol{F}_2^4$、$\boldsymbol{F}_2^5$、$\boldsymbol{F}_2^6$、$\boldsymbol{F}_2^7$、$\boldsymbol{F}_2^8$、$\boldsymbol{F}_2^{16}$、$\boldsymbol{F}_2^{32}$中成立.

对$f:\boldsymbol{F}_2^n\to\boldsymbol{F}_2^n$($n=1,2,4,5,6,7,8,16,32$),可以通过计算$T$和$\min\ \{\varphi(q_i)\}$($q_i$为$2^{n2^{n-1}}+1$的素因子)的值比较得到$T<\varphi(q)$.

在分组密码高级加密标准(AES, advanced encryption standard)中,密钥在$\boldsymbol{F}_2^7$、$\boldsymbol{F}_2^8$中取得,流密码SOBER、LEVIARHAN等中,密钥在$\boldsymbol{F}_2^{16}$、$\boldsymbol{F}_2^{32}$中取

得，而推论 6 表明，单圈 T 函数状态序列在这些域中不是 l 序列.

3　结束语

单圈 T 函数生成序列因其具有极大周期、好的游程分布、能将 0 作为初始状态等优点，受到了密码设计者的广泛关注. FCSR 是一类可用于序列密码设计的非线性序列发生器，序列的 2-adic 复杂度反映了序列由 FCSR 生成的级数. 通过分析单圈 T 函数生成的第 k 位序列和状态序列各位之间的关系，利用 Fermat 数理论，给出了这 2 种序列低位序列的 2-adic 复杂度的值和高位序列 2-adic 复杂度的估值，从 FCSR 生成的角度，揭示了单圈 T 函数序列的特性. 结果表明，与文献[6,12]的结果对比，尽管单圈 T 函数生成序列达到了最大周期并具有高的线性复杂度，但远没有达到最大 2-adic 复杂度，不是 l 序列.

参考文献：

[1] Lenstra A K, Lenstra H W, JR. Manasse M S, et al. The factorization of the ninth Fermat number [J]. Mathematics of Computation, 1993, 61(203): 319-349.

[2] Brent R P. Factorization of the tenth and eleventh Fermat numbers [J]. Mathematics of Computation, 2000, 68 (154): 627-630.

[3] 贾耿华. 关于费马数的研究 [D]. 成都：成都理工大学, 2006.

[4] Klapper A, Goresky M. 2-adic shift registers [C]// Fast Software Encryption. Leuven: Springer, 1994: 174-178.

[5] Klapper A, Goresky, M. Feedback shift registers, 2-adic span, and combiners with memory [J]. Journal of Cryptology, 1997, 10(2): 111-147.

[6] Tian Tian, Qi Wenfeng. 2-adic complexity of binary m-sequences [J]. IEEE Transactions on Information Theory, 2010, 56(1): 450-454.

[7] Klimov A, Shamir A. A new class of invertible mappings [C]// CHES 2002. London: Springer, 2003: 470-483.

[8] Klimov A, Shamir A. Cryptographic applications of T-functions [C]// SAC 2003. Ottawa: Springer, 2003: 248-261.

[9] Klimov A, Shamir A. New cryptographic primitives based on multiword T functions [C]// FSE 2004. Delhi: Springer, 2004: 1-15.

[10] Klimov A. Applications of T-functions in cryptography [D]. Rehovot: Weizmann Institute of Science, 2005.

[11] Kolokotronis N. Cryptographic properties of nonlinear pseudorandom number generators [J]. Designs, Codes and Cryptography, 2008, 46(3): 353-363.

[12] Wang Yan, Hu Yupu, Li Shunbo, et al. Linear complexity of sequences produced by single cycle T-function [J]. The Journal of China Universities of Posts and Telecommunications, 2011, 18(4): 123-128.