doi:10.3969/j.issn.1000-436x.2014.03.015

单圈 T-函数的 2-adic 复杂度和 1-错 2-adic 复杂度

游伟[1]，戚文峰[2,3]

(1. 国家数字交换系统工程技术研究中心，河南 郑州 450002；2. 解放军信息工程大学 四院，河南 郑州 450002；
3. 解放军信息工程大学 数学工程与先进计算国家重点实验室，河南 郑州 450002)

摘 要：研究了由 F_2^n 上单圈 T-函数所导出权位序列的 2-adic 复杂度，设 j 为整数，$0 \leqslant j \leqslant n-1$。结论表明，第 j 权位序列 2-adic 复杂度的上界为 $\mathrm{lb}(2^{2^j}+1)$。另外，讨论了与所有单圈 T-函数所导出第 j 权位序列相对应的 2-adic 整数的分布，分布情况说明这个上界是可以达到的。最后，研究了权位序列的 1-错 2-adic 复杂度。研究结果表明对所有 $1 \leqslant j \leqslant n-1$，权位序列 $\underline{x}_j$ 的 1-错 2-adic 复杂度都与其 2-adic 复杂度相同。

关键词：序列密码；2-adic 复杂度；k -错 2-adic 复杂度；单圈 T-函数；权位序列

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2014)03-0135-05

The 2-adic complexity and the 1-error 2-adic complexity of single cycle T-functions

YOU Wei[1], QI Wen-feng[2,3]

(1. National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China;
2. Fourth Institute, PLA Information Engineering University, Zhengzhou 450002, China;
3. State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: The 2-adic complexities of the coordinate sequences derived from single cycle T-functions over F_2^n were investigated. Let j be an integer such that $0 \leqslant j \leqslant n-1$. It is shown that the 2-adic complexity of the j th coordinate sequence is upper bounded by $\mathrm{lb}(2^{2^j}+1)$. The distribution of the corresponding 2-adic number associated with the j th coordinate sequence of all single cycle T-functions was also discussed, which implies that the upper bound is attainable. Moreover, 1-error 2-adic complexity was also studied. It was proved that the 1-error 2-adic complexity of the j th coordinate sequence is equal to its 2-adic complexity except for $j=0$.

Key words: stream cipher; 2-adic complexity; k -error 2-adic complexity; single cycle T-functions; coordinate sequences

1 引言

线性反馈移位寄存器(LFSR)是序列密码设计的重要组件之一。然而，研究发现基于 LFSR 设计的序列密码体制容易受到代数攻击和相关攻击的威胁[1~3]。因此，研究利用其他结构来产生密码性质好的非线性序列就受到越来越多的关注。T-函数和带进位反馈移位寄存器(FCSR)就是 2 类重要的非线性序列生成器。

T-函数作为一类密码本原是由 Klimov 和 Shamir 提出的[4]，它非常适合用于序列密码的设计。由于使用了现代微处理器中的所有逻辑运算和大多数算术运算(包括加法、减法、乘法)，因此它是非常高效的，而它们的安全性主要依赖于这 2 类运算的混合使用。

带进位反馈移位寄存器(FCSR)是由 Klapper 和 Goresky 提出的[5]。与建立在模 2 加运算上的线性反馈移位寄存器不同，FCSR 利用进位寄存器实

收稿日期：2012-08-22；**修回日期**：2013-01-27
基金项目：国家自然科学基金资助项目(61070178)
Foundation Item: The National Natural Science Foundation of China(61070178)

现了 2-adic 整数的加法。2-adic 复杂度[6]是用来衡量生成一条二元序列 FCSR 所需要的规模。对于 2-adic 复杂度低的序列，只需序列大约两倍 2-adic 复杂度的长度有理逼近算法[6]就可以有效还原生成该序列的 FCSR。因此，2-adic 复杂度是衡量序列伪随机性的一个重要指标。

本文主要研究由单圈 T-函数所导出权位序列的 2-adic 复杂度。设 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$ 是由 F_2^n 上单圈 T-函数 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 生成的序列，$\underline{x}_j=(x_{0,j},x_{1,j},\cdots)$ 是 $\underline{\boldsymbol{x}}$ 的第 j 权位序列，其中，$0\leqslant j\leqslant n-1$。结论表明，对于所有 $0\leqslant j\leqslant n-1$，权位序列 $\underline{x}_j$ 的 2-adic 复杂度上界为 $\mathrm{lb}(2^{2^j}+1)$。此外，对于 $0\leqslant j\leqslant n-1$，设 $\alpha_j=\sum_{i=0}^{\infty}x_{i,j}\cdot 2^i$ 是与权位序列 $\underline{x}_j$ 相对应的 2-adic 整数，则若给定初态 $\boldsymbol{x}_0$，可以证明 α_j 在集合 $\{-(2p_j-x_{0,j})/(2^{2^j}+1)\,|\,1\leqslant p_j\leqslant 2^{2^j-1}\}$ 上是均匀分布的。最后，本文进一步研究了权位序列的 1-错 2-adic 复杂度，研究结果表明对于所有 $1\leqslant j\leqslant n-1$，权位序列 $\underline{x}_j$ 的 1-错 2-adic 复杂度都与其 2-adic 复杂度相同。

在本文中，用“·”和“+”分别表示常规的整数乘法和整数加法，用“⊕”表示有限域 F_2 中的加法。另外，对于一条周期为 T 的二元周期序列 $\underline{a}=(a_0,a_1,\cdots)$，记为 $\underline{a}=(a_0,a_1,\cdots,a_{T-1})^{\infty}$。

2 预备知识

2.1 T-函数

T-函数是一类有着诸多应用的密码函数[7~9]，它可以看成多输出的布尔函数，对于 $0\leqslant j\leqslant n-1$，其第 j 权位函数的表示如图 1 所示。

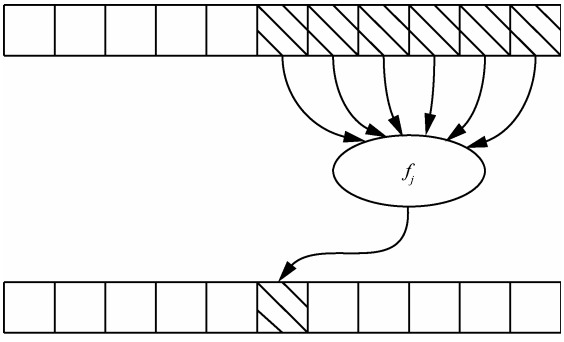

图 1 T-函数的布尔函数形式表示

记 F_2 上的 n 维向量空间为 F_2^n。字 $\boldsymbol{x}\in F_2^n$ 指的是长为 n 的向量 $\boldsymbol{x}=(x_{n-1},x_{n-2},\cdots,x_0)^{\mathrm{T}}$，其中，$x_j$ 称为 $\boldsymbol{x}$ 的第 j 比特。记 F_2^n 上单圈 T-函数的全体为 $\mathcal{T}_n$。

定义 1[4] 设 $f:\boldsymbol{x}=(x_{n-1},x_{n-2},\cdots,x_0)^{\mathrm{T}}\to\boldsymbol{y}=(y_{n-1},y_{n-2},\cdots,y_0)^{\mathrm{T}}$ 是 F_2^n 到 F_2^n 的函数。对于 $0\leqslant j\leqslant n-1$，若 $f(\boldsymbol{x})$ 的第 j 比特输出 y_j 仅与输入比特 $x_j,\cdots,x_0$ 有关，则称 $f(\boldsymbol{x})$ 是 T-函数。

定义 2[4] 设 $f:F_2^n\to F_2^n$ 是 T-函数。给定初态 $\boldsymbol{x}_0=(x_{0,n-1},x_{0,n-2},\cdots,x_{0,0})^{\mathrm{T}}\in F_2^n$，对于 $i\geqslant 0$，令 $\boldsymbol{x}_{i+1}=f(\boldsymbol{x}_i)$。记序列 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$。若序列 $\underline{\boldsymbol{x}}$ 的周期 $per(\underline{\boldsymbol{x}})=2^n$，则称 $f(\boldsymbol{x})$ 是单圈 T-函数，并称序列 $\underline{\boldsymbol{x}}$ 由单圈 T-函数 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 生成。

定义 3[7] 设 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$ 是 F_2^n 上的序列，其中，$\boldsymbol{x}_i=(x_{i,n-1},x_{i,n-2},\cdots,x_{i,0})^{\mathrm{T}}$，$i\geqslant 0$。则对于 $0\leqslant j\leqslant n-1$，称 $\underline{x}_j=(x_{0,j},x_{1,j},\cdots)$ 为 $\underline{\boldsymbol{x}}$ 的第 j 权位序列。

下面的引理 1 刻画了由单圈 T-函数所导出权位序列的周期，而引理 2 则给出了 $\mathbb{T}_2^n$ 上单圈 T-函数的计数。

引理 1[7] 设序列 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$ 由单圈 T-函数 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 生成。则对于 $0\leqslant j\leqslant n-1$，$\underline{\boldsymbol{x}}$ 的第 j 权位序列 $\underline{x}_j$ 的周期 $per(\underline{x}_j)=2^{j+1}\overset{\mathrm{dif}}{=}T_j$。另外，对于 $0\leqslant j\leqslant n-1$，序列 $\underline{x}_j$ 在一个周期中后一半恰好是前一半的补，即 $x_{i+2^j,j}=x_{i,j}\oplus 1$，$i\geqslant 0$。

引理 2[8] F_2^n 上单圈 T-函数的总数为 2^{2^n-n-1}，即 $|T_n|=2^{2^n-n-1}$。

2.2 FCSR 序列及 2-adic 复杂度

设 q 是正奇数，$q+1=q_1 2+q_2 2^2+\cdots+q_r 2^r$，$q_1,\cdots,q_{r-1}\in\{0,1\}$ 且 $q_r=1$。连接数为 q 的 FCSR 如图 2 所示。

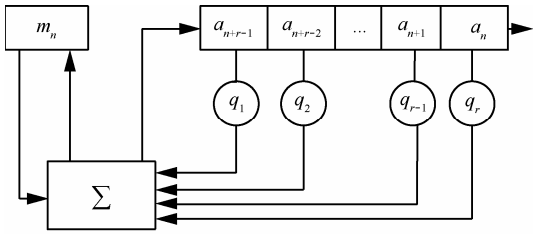

图 2 FCSR 结构

其中，Σ 表示整数加法，m_n 是进位(也称记忆)，$(m_n;a_{n+r-1},a_{n+r-2},\cdots,a_n)$ 是 FCSR 的一个状态，特别地，$(m_0;a_{r-1},a_{r-2},\cdots,a_0)$ 称为 FCSR 的初态。设 $n\geqslant 0$，则第 n 状态到第 $n+1$ 状态的更新算法如下：

1) 计算整数和 $\sigma_n=\sum_{k=1}^{r}q_k\cdot a_{n+r-k}+m_n$；

2) 主寄存器比特右移 1 bit，输出寄存器最右

端的 a_n；

3) 令 $a_{n+r}=\sigma_n \pmod 2$，放入寄存器的最左端；

4) 令 $m_{n+1}=(\sigma_n-a_{n+r})/2$。

称输出序列 $\underline{a}=(a_0,a_1,\cdots)$ 是以 q 为连接数的 FCSR 序列。

下面的结论说明了二元准周期序列与 FCSR 序列之间的对应关系。

引理 3[5]　设 $\underline{a}=(a_0,a_1,\cdots)$ 是二元准周期序列。则存在有理数 p/q，使得 $p/q=\sum_{i=0}^{\infty}a_i\cdot 2^i=\alpha$，并且 q 是生成序列 $\underline{a}$ 的 FCSR 的连接数。进一步，$\underline{a}$ 是周期的当且仅当 $-1\leqslant\alpha\leqslant 0$。

上述引理说明任意二元准周期序列都能由 FCSR 生成。若二元准周期序列 $\underline{a}$ 可以由以 q 为连接数的 FCSR 生成，则也称 q 是序列 $\underline{a}$ 的连接数，序列 $\underline{a}$ 的全体连接数中最小者称为 $\underline{a}$ 的极小连接数。

推论 1　设 $\underline{a}$ 是以 q 为极小连接数的二元周期序列，则 q' 是序列 $\underline{a}$ 的连接数当且仅当 $q\,|\,q'$。

2-adic 复杂度是用来衡量生成一条二元序列 FCSR 所需要的规模。

定义 4[6]　设 $\underline{a}=(a_0,a_1,\cdots)$ 是二元准周期序列，$\sum_{i=0}^{\infty}a_i\cdot 2^i=p/q$ 且 $\gcd(p,q)=1$。则称 $\boldsymbol{\Phi}(\underline{a})=\mathrm{lb}(\max(|p|,|q|))$ 为序列 $\underline{a}$ 的 2-adic 复杂度。

注 1　若 $\underline{a}$ 是全 0 序列，则令 $\boldsymbol{\Phi}(\underline{a})=0$。

注 2　若 $\underline{a}$ 是以 q 为极小连接数的二元周期序列，则由引理 3 可得 $\boldsymbol{\Phi}(\underline{a})=\mathrm{lb}q$。

3　单圈 T-函数的 2-adic 复杂度

定理 1　设序列 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$ 由单圈 T-函数 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 生成。则对于 $0\leqslant j\leqslant n-1$，有 $\boldsymbol{\Phi}(\underline{x}_j)\leqslant\mathrm{lb}(2^{2^j}+1)$。

特别地，若 $2^{2^j}+1$ 是素数，则等式成立。

证明　设 j 为整数，$0\leqslant j\leqslant n-1$。由引理 1 可得，对于 $0\leqslant i\leqslant T_j/2-1$，有 $x_{i+T_j/2,j}=1-x_{i,j}$，从而

$$\begin{aligned}\alpha_j&=\sum_{i=0}^{\infty}x_{i,j}\cdot 2^i\\&=-\frac{\sum_{i=0}^{T_j-1}x_{i,j}\cdot 2^i}{2^{T_j}-1}\\&=-\frac{\sum_{i=0}^{T_j/2-1}x_{i,j}\cdot 2^i+\sum_{i=0}^{T_j/2-1}x_{i+T_j/2,j}\cdot 2^{i+T_j/2}}{2^{T_j}-1}\\&=-\frac{\sum_{i=0}^{T_j/2-1}x_{i,j}\cdot 2^i+\sum_{i=0}^{T_j/2-1}(1-x_{i,j})\cdot 2^{i+T_j/2}}{2^{T_j}-1}\\&=-\frac{2^{T_j/2}\cdot(2^{T_j/2}-1)-(2^{T_j/2}-1)\cdot\sum_{i=0}^{T_j/2-1}x_{i,j}\cdot 2^i}{2^{T_j}-1}\\&=-\frac{2^{T_j/2}-\sum_{i=0}^{T_j/2-1}x_{i,j}\cdot 2^i}{2^{T_j/2}+1}\end{aligned}$$

因此，由注 2 和推论 1 可得 $\boldsymbol{\Phi}(\underline{x}_j)\leqslant\mathrm{lb}(2^{T_j/2}+1)$。另外，因为 $0<2^{T_j/2}-\sum_{i=0}^{T_j/2-1}x_{i,j}\cdot 2^i<2^{T_j/2}+1$，所以，若 $2^{T_j/2}+1$ 是素数，则 $\boldsymbol{\Phi}(\underline{x}_j)=\mathrm{lb}(2^{T_j/2}+1)$。

定理 2　给定初态 $\boldsymbol{x}_0=(x_{0,n-1},x_{0,n-2},\cdots,x_{0,0})^{\mathrm{T}}\in F_2^n$。则对于所有 $0\leqslant j\leqslant n-1$ 以及 $1\leqslant p_j\leqslant 2^{2^j-1}$，存在 $2^{2^n-2^j-n}$ 个单圈 T-函数 $f(\boldsymbol{x})$ 使得

$$\alpha_j=\sum_{i=0}^{\infty}x_{i,j}\cdot 2^i=-\frac{2p_j-x_{0,j}}{2^{2^j}+1}$$

其中，$\underline{x}_j=\{x_{i,j}\}_{i\geqslant 0}$ 是由 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 所生成序列的第 j 权位序列。

证明　由引理 2 可知 F_2^n 上单圈 T-函数的总数为 2^{2^n-n-1}。因此，给定初态 $\boldsymbol{x}_0$，由所有单圈 T-函数和相同初态 $\boldsymbol{x}_0$ 共可以生成 2^{2^n-n-1} 条不同的序列。

另一方面，由引理 1 可知对于 $0\leqslant j\leqslant n-1$，序列 $\underline{x}_j$ 是完全由它的前半周期所决定的。给定初态 $\boldsymbol{x}_0$，令

$$\begin{aligned}S_j=\{\underline{x}_j=(&x_{0,j},x_{1,j},\cdots,x_{T_j/2-1,j},x_{0,j}\oplus 1,x_{1,j}\oplus 1,\cdots,\\&x_{T_j/2-1,j}\oplus 1)\,|\,x_{i,j}\in F_2,1\leqslant i\leqslant T_j/2-1\}\end{aligned}$$

以及

$$S=\{\underline{\boldsymbol{x}}=(\underline{x}_{n-1},\underline{x}_{n-2},\cdots,\underline{x}_0)^{\mathrm{T}}\,|\,\underline{x}_j\in S_j,0\leqslant j\leqslant n-1\}$$

因此，序列 $\underline{x}_j$ 最多有 $2^{T_j/2-1}=2^{2^j-1}$ 种选择，序列 $\underline{\boldsymbol{x}}$ 则最多有 $\prod_{j=0}^{n-1}2^{2^j-1}=2^{2^n-n-1}$ 种选择。然而，因为由所有单圈 T-函数和相同初态 $\boldsymbol{x}_0$ 恰好可以生成 2^{2^n-n-1} 条不同的序列，所以集合 S 和集合 $\mathcal{T}_n$ 之间存在着一一对应关系。即是说，集合 S 中的每条序列都是由某个单圈 T-函数和初态 $\boldsymbol{x}_0$ 生成的。

对于 $0\leqslant j\leqslant n-1$，由定理 1 的证明过程可知对于每条序列 $\underline{x}_j\in S_j$，都存在正整数 p_j，$1\leqslant p_j\leqslant 2^{2^j-1}$，使得

$$\alpha_j=\sum_{i=0}^{\infty}x_{i,j}\cdot 2^i=-\frac{2^{2^j}-\sum_{i=0}^{2^j-1}x_{i,j}\cdot 2^i}{2^{2^j}+1}=-\frac{2p_j-x_{0,j}}{2^{2^j}+1}\quad(1)$$

因为集合 S_j 中共有 2^{2^j-1} 条序列，所以对于每个整数 $p_j \in \{1,2,\cdots,2^{2^j-1}\}$，集合 S_j 中都恰好有一条序列 $\underline{x}_j$ 使得式(1)成立。另外，由于共有 $\frac{|S|}{|S_j|}=\frac{2^{2^n-n-1}}{2^{2^j-1}}=2^{2^n-2^j-n}$ 个不同的单圈 T-函数满足所生成序列的第 j 权位序列是相同的，从而结论成立。

注 3 由定理 2 的证明可知，对于 $0 \leqslant j \leqslant n-1$，$\alpha_j$ 在集合 $\{-(2p_j - x_{0,j})/(2^{2^j}+1) \mid 1 \leqslant p_j \leqslant 2^{2^j-1}\}$ 上是均匀分布的。

注 4 对于奇数 $m>1$ 和整数 a，$1 \leqslant a \leqslant m-1$，若 $gcd(a,m)=1$，则 $gcd(m-a,m)=1$。因此，分别有 $\frac{1}{2}\varphi(m)$ 个偶数和 $\frac{1}{2}\varphi(m)$ 个奇数，a 满足 $1 \leqslant a \leqslant m-1$ 以及 $gcd(a,m)=1$，其中，$\varphi(\cdot)$ 是欧拉函数。

注 5 给定初态 $\boldsymbol{x}_0 \in F_2^n$，由注 4 可知对于 $0 \leqslant j \leqslant n-1$，在集合 $\{2p_j - x_{0,j} \mid 1 \leqslant p_j \leqslant 2^{2^j-1}\}$ 中存在 $\frac{1}{2}\varphi(2^{2^j}+1)$ 个整数满足 $gcd(2p_j - x_{0,j}, 2^{2^j}+1)=1$。因此，由定理 2 和定义 4 可知对于 $0 \leqslant j \leqslant n-1$，共有 $\varphi(2^{2^j}+1)\cdot 2^{2^n-2^j-n-1}$ 个单圈 T-函数 $f(\boldsymbol{x})$ 使得 $\boldsymbol{\Phi}(\underline{x}_j)=\mathrm{lb}(2^{2^j}+1)$，其中，$\underline{x}_j$ 是由 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 所生成序列的第 j 权位序列。

4 单圈 T-函数的 1-错 2-adic 复杂度

为了衡量序列 2-adic 复杂度的稳定性，文献[11]提出了 k-错 2-adic 复杂度的概念。

定义 5 设 $\underline{a}=(a_0,a_1,\cdots,a_{T-1})^\infty$ 是周期为 T 的二元周期序列，k 是整数，$0 \leqslant k \leqslant T$。则称 $\boldsymbol{\Phi}_k(\underline{a})=\min_{\underline{b}} \boldsymbol{\Phi}(\underline{b})$ 为序列 $\underline{a}$ 的 k-错 2-adic 复杂度，其中，序列 $\underline{b}=(b_0,b_1,\cdots,b_{T-1})^\infty$ 跑遍所有周期为 T 并且满足向量 $(a_0,a_1,\cdots,a_{T-1})$ 和 $(b_0,b_1,\cdots,b_{T-1})$ 之间汉明距离至多为 k 的二元周期序列。

引理 4 设 $\underline{a}=(a_0,a_1,\cdots,a_{T-1})^\infty$ 是周期为 T 的二元周期序列，T 为偶数。则 $(2^{T/2}+1) \mid \sum_{i=0}^{T-1} a_i \cdot 2^i$ 当且仅当对所有 $0 \leqslant i \leqslant T/2-1$，$a_i = a_{i+T/2}$。

证明 由于对所有 $0 \leqslant i \leqslant T/2-1$，$2^{i+T/2} = -2^i \pmod{2^{T/2}+1}$，从而有

$$\sum_{i=0}^{T-1} a_i \cdot 2^i = \sum_{i=0}^{T/2-1} a_i \cdot 2^i + \sum_{i=0}^{T/2-1} a_{i+T/2} \cdot 2^{i+T/2}$$

$$= \sum_{i=0}^{T/2-1} a_i \cdot 2^i - \sum_{i=0}^{T/2-1} a_{i+T/2} \cdot 2^i \pmod{2^{T/2}+1}$$

$$= \sum_{i=0}^{T/2-1} (a_i - a_{i+T/2}) \cdot 2^i \pmod{2^{T/2}+1}$$

因此，$\sum_{i=0}^{T-1} a_i \cdot 2^i = 0 \pmod{2^{T/2}+1}$ 当且仅当对所有 $0 \leqslant i \leqslant T/2-1$，$a_i = a_{i+T/2}$。

为了研究 k-错 2-adic 复杂度，需要介绍一下 $\boldsymbol{\Psi}_k(\underline{a})$ 的概念。对于 $1 \leqslant k \leqslant T$，$\boldsymbol{\Psi}_k(\underline{a})$ 表示的是序列 $\underline{a}$ 在每个周期内替换掉 k 个比特后所得序列 2-adic 复杂度的最小值。注意到对任意 $1 \leqslant k \leqslant T$，有 $\boldsymbol{\Phi}_k(\underline{a}) = \min\{\boldsymbol{\Phi}(\underline{a}), \boldsymbol{\Psi}_1(\underline{a}), \cdots, \boldsymbol{\Psi}_k(\underline{a})\}$。

引理 5 设序列 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$ 由单圈 T-函数 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 生成。则 $\boldsymbol{\Psi}_1(\underline{x}_0)=0$，对于 $1 \leqslant j \leqslant n-1$，存在 $2^{2^j}+1$ 的因子 $h_j (h_j>1)$ 使得

$$\boldsymbol{\Psi}_1(\underline{x}_j) = \mathrm{lb}(h_j \cdot (2^{2^j}-1))$$

特别地，若 $2^{2^j}+1$ 是素数，则

$$\boldsymbol{\Psi}_1(\underline{x}_j) = \mathrm{lb}(2^{2^{j+1}}-1)$$

证明 由引理 1 易得 $\boldsymbol{\Psi}_1(\underline{x}_0)=0$。对 $1 \leqslant j \leqslant n-1$，假设 $\underline{z}_j=(z_{0,j},z_{1,j},\cdots,z_{T_j-1,j})^\infty$ 是序列 $\underline{x}_j$ 在每个周期内替换掉 1 个比特后所得序列，且替换的位置为 k_j，$0 \leqslant k_j \leqslant T_j-1$，则

$$\beta_j = \sum_{i=0}^{\infty} z_{i,j} \cdot 2^i = -\frac{\sum_{i=0}^{T_j-1} z_{i,j} \cdot 2^i}{2^{T_j}-1}$$

$$= -\frac{\sum_{i=0}^{T_j-1} x_{i,j} \cdot 2^i + (-1)^{x_{k_j,j}} 2^{k_j}}{(2^{T_j/2}+1)(2^{T_j/2}-1)} \tag{2}$$

令 $d_j = gcd(\sum_{i=0}^{T_j-1} z_{i,j} \cdot 2^i, 2^{T_j/2}-1)$。由定理 1 的证明可知 $(2^{T_j/2}-1) \mid \sum_{i=0}^{T_j-1} x_{i,j} \cdot 2^i$，从而 $d_j \mid (-1)^{x_{k_j,j}} 2^{k_j}$，因此 $d_j=1$。

另一方面，由引理 1 可知对于 $0 \leqslant i \leqslant T_j-1$，除 $i=k_j$ 外，$z_{i,j} = z_{i+T_j/2,j} \oplus 1$，从而由引理 4 可得 $(2^{T_j/2}+1) \nmid \sum_{i=0}^{T_j-1} z_{i,j} \cdot 2^i$。因此，由式(2)可知存在 $2^{T_j/2}+1$ 的因子 h_j 使得 $\boldsymbol{\Phi}(\underline{z}_j)=\mathrm{lb}(h_j \cdot (2^{T_j/2}-1))$，且 $h_j>1$。特别地，若 $2^{T_j/2}+1$ 是素数，则 $h_j = 2^{T_j/2}+1$，$\boldsymbol{\Phi}(\underline{z}_j)=\mathrm{lb}(2^{T_j}-1)$。

定理 3 设序列 $\underline{\boldsymbol{x}}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots)$ 由单圈 T-函数 $f(\boldsymbol{x})$ 和初态 $\boldsymbol{x}_0$ 生成。则 $\boldsymbol{\Phi}_1(\underline{x}_0)=0$，对 $1 \leqslant j \leqslant n-1$，

有 $\Phi_1(\underline{x}_j)=\Phi(\underline{x}_j)$。

证明　由定理 1 和引理 5 可得 $\Phi_1(\underline{x}_0)=0$，且对于 $1\leqslant j\leqslant n-1$，有

$$\Psi_1(\underline{x}_j)=\mathrm{lb}(h_j\cdot(2^{2^j}-1))>\mathrm{lb}(2^{2^j}+1)\geqslant\Phi(\underline{x}_j)$$

因此，$\Phi_1(\underline{x}_j)=\min\{\Phi(\underline{x}_j),\Psi_1(\underline{x}_j)\}=\Phi(\underline{x}_j)$。

5　结束语

本文研究了单圈 T-函数导出权位序列的 2-adic 复杂度和 1-错 2-adic 复杂度。结论表明，除了最低权位序列，其他权位序列的 1-错 2-adic 复杂度和其 2-adic 复杂度均相同。

参考文献：

[1] COURTOIS N, MEIER W. Algebraic attacks on stream ciphers with linear feedback[A]. Cryptology- EUROCRYPT 2003[C]. Warsaw, Poland, 2003.345-359.

[2] SIEGENTHALER T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 1985, C-34(1): 81-85.

[3] MEIER W, STAFFELBACH O. Fast correlation attacks on certain stream ciphers[J]. Journal of Cryptology, 1989, 1(3): 159-176.

[4] KLIMOV A, SHAMIR A. A new class of invertible mappings[A]. Workshop on Cryptographic Hardware and Embedded Systems-CHES 2002[C]. Redwood Shores, CA, USA, 2003. 470-483.

[5] KLAPPER A, GORESKY M. 2-adic shift registers[A]. Fast Software Encryption-FSE 1993[C]. Cambridge, UK, 1993. 174-178.

[6] KLAPPER A, GORESKY M. Cryptanalysis based on 2-adic rational approximation[A]. Cryptology-CRYPTO 1995[C]. Santa Barbara, California, USA, 1995. 262-273.

[7] KLIMOV A, SHAMIR A. Cryptographic applications of T-functions[A]. Workshop on Selected Areas in Cryptography-SAC 2003[C]. Ottawa, Canada, 2004. 248-261.

[8] ZHANG W Y, WU C-K. The algebraic normal form, linear complexity and k-error linear complexity of single-cycle T-function[A]. Sequences and Their Applications-SETA 2006[C]. Beijing, China, 2006. 391-401.

[9] KLIMOV A, SHAMIR A. New cryptographic primitives based on multiword T-functions[A]. Fast Software Encryption-FSE 2004[C]. Delhi, India, 2004. 1-15.

[10] KLIMOV A, SHAMIR A. New applications of T-functions in block ciphers and hash functions[A]. Fast Software Encryption-FSE 2005[C]. Paris, France, 2005. 18-31.

[11] HU H G, FENG D G. On the 2-adic complexity and the *k*-error 2-adic complexity of periodic binary sequences[J]. IEEE Transactions on Information Theory, 2008, 54(2): 874-883.

作者简介：

游伟（1984-），男，江西丰城人，国家数字交换系统工程技术研究中心讲师，主要研究方向为密码学和信息安全。

戚文峰（1963-），男，浙江宁波人，解放军信息工程大学教授、博士生导师，主要研究方向为密码学和信息安全。