一致可微 T 函数性质研究

王森鹏,刘 燕,胡 斌
(解放军信息工程大学,河南郑州 450001)

摘 要: 本文结合传统 T 函数理论与非阿基米德 T 函数理论,深入研究 T 函数的性质特点,重点讨论一致可微 T 函数的单圈性及最高位序列的保熵性. 首次利用参数的概念建立传统 T 函数理论中单字 T 函数单圈性判定条件与非阿基米德 T 函数理论中单圈性判定条件的联系,说明了两类判定条件的适用范围. 定义了对 T 函数生成序列进行压缩变换的保熵性概念,讨论了一致可微 T 函数最高位序列的保熵性,说明了一致可微的 T 函数保熵性具有传递性,给出了 T 函数最高位序列保熵性的判定条件.

关键词: T 函数; 一致可微; 参数; 保熵性
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2016)11-2676-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.11.016

On the Properties of T-functions with Uniform Differentiability

WANG Sen-peng, LIU Yan, HU Bin
(*The PLA Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: Combining conventional theory with non-Archimedean theory, we study the properties of T-functions. We focus on the criteria of single cycle T-functions and entropy preservability of the most significant bit output sequence generated by T-functions. Utilizing the parameters, the connection between criteria of single cycle T-functions in two different theories is established. The situation each criterion is suited for is cleared. On the other hand, we define the notion of entropy preservability of T-functions. We talk about the entropy preservability of most significant bit output sequences generated by T-functions with uniform differentiability. We present the condition for entropy preservability of most significant bit output sequences and show the transitivity.

Key words: T-functions; uniform differentiability; parameter; entropy preservability

1 引言

T 函数是 2002 年由 Klimov 和 Shamir 在文献[1]中提出的一类非线性函数. 由于具有计算速度快、密码学性质好、易于软硬件实现等特点,T 函数被广泛应用于序列密码、分组密码等领域. 特别是在流密码设计中,T 函数能代替线性移位寄存器(LFSR)作为初始乱源,从而克服了 LFSR 生成序列周期无法达到最大的缺陷. Klimov 和 Shamir 在文献[1~3]中利用参数的概念给出了 T 函数单圈性的判定条件,并提出基于 T 函数的流密码设计方案. 2004 后,大量基于 T 函数设计的密码算法开始涌现,如 eSTREAM 计划中提交的 TSC[4], ABC[5], Mir[6] 等密码算法均采用 T 函数,同时针对这些算法的攻击方法也成为研究的热点. 文献[7~10]对 T 函数输出序列的密码学性质进行了深入研究,包括线性复杂度、k-错线性复杂度、自相关性和非线性度等安全性指标,研究表明 T 函数具有较好的安全性.

研究 T 函数的另一重要途径是非阿基米德理论, Anashin 在 2-adic 整数环中,定义了 2-adic 距离、范数、测度等概念,阐述了 T 函数即 1-Lipchis 函数(或称为完备函数),而可逆 T 函数即可测函数,单圈 T 函数即保测函数[11]. 同时,分别利用一致可微性、马勒插值级数和 van der put 级数,给出了可逆 T 函数以及单圈 T 函数的的判定定理[12~15]. 2012 年,Tao Shi, Anashin 和 Dong-Dai Lin 等人在该理论的基础上,发现一致可微 T 函数的特定分位序列之间存在线性弱点,并提出攻击方法[16]. 2013 年,他们又利用 van der put 级数作为工具,借鉴时间存储折中的思想提出了两类快速计算 T 函数

收稿日期:2015-03-12;修回日期:2016-02-01;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61272041, No. 61502532)

的算法[17].

近年来,在 T 函数的单圈性判定方面,传统 T 函数理论与非阿基米德理论均取得了丰富的成果,其中传统理论主要是利用参数作为工具对 T 函数进行研究,而非阿基米德理论则是借助 T 函数一致可微的性质进行研究,两种理论各有特点、各有优势. 如果能将两种理论结合起来对 T 函数的性质进行研究是非常有意义的,本文从这方面出发建立起两种理论之间的联系,为 T 函数的研究提供了新的思路.

1988 年,黄民强在研究环 $Z/(p^e)$ 上序列的性质时提出了“保熵性”概念[18]. 具体地,设 $f(x)=x^n+c_{n-1}x^{n-1}+\cdots c_0$ 是 $Z/(p^e)$ 上的首一多项式,对序列 $\bar{a}=(a(t))_{t\geqslant 0}$,若满足关系式 $a(i+n)=-[c_0a(i)+c_1a(i+1)+\cdots+c_{n-1}a(i+n-1)]\pmod{p^e}$,则称 $\bar{a}$ 是环 $Z/(p^e)$ 上由 $f(x)$ 生成的 n 级线性递归序列,同时将环 $Z/(p^e)$ 上由 $f(x)$ 生成的全体序列记为 $G(f(x),p^e)$[19]. 如果将 $\bar{a}$ 的元素都进行 p-adic 展开,则可称序列 $\bar{a}_i=(a_i(t))_{t\geqslant 0}$ 为 $\bar{a}$ 的第 i 权位序列. 进一步,设 $\varphi(x_0,x_1,\cdots,x_{e-1})$ 为 $Z/(p)$ 上的 e 元多项式函数,称 $Z/(p)$ 上的序列 $\varphi(\bar{a}_0,\bar{a}_1,\cdots,\bar{a}_{e-1})=(\varphi(a_0(t),a_1(t),\cdots,a_{e-1}(t)))_{t\geqslant 0}$ 为 φ 作用在 $\bar{a}$ 上导出的权位压缩导出序列,简称权位压缩导出序列. “保熵性”概念的提出旨在刻画从 $Z/(p^e)$ 上的本原序列到其权位压缩导出序列的压缩过程中没有信息损失,从而使压缩后的权位压缩导出序列保留压缩前本原序列的所有信息,即对任意 $\bar{a},\bar{b}\in G(f(x),p^e)$,$\bar{a}=\bar{b}$ 当且仅当 $\varphi(\bar{a}_0,\bar{a}_1,\cdots,\bar{a}_{e-1})=\varphi(\bar{b}_0,\bar{b}_1,\cdots,\bar{b}_{e-1})$,文献[20,21]证明了 $Z/(p^e)$ 上的本原序列的最高权位序列是保熵的. T 函数作为一类非线性序列,基于 T 函数的密码算法常常只使用 T 函数的最高分位或最高几个分位序列,而 T 函数的最高位序列是否含有状态序列的全部信息,至今没有文献进行讨论. 本文从这方面出发给出 T 函数生成序列进行压缩变换的保熵性概念,讨论了一致可微 T 函数最高位序列的保熵性以及判定条件,揭示了一致可微 T 函数的最高位序列性质,为进一步研究 T 函数的性质提供参考.

2　基础知识

首先,给出传统意义下 T 函数的相关定义:

定义 1[1]　设 $x=(x_0,x_1,\cdots,x_{m-1})^{\mathrm{T}}\in F_2^{m\times n}$,其中 $x_i=([x_i]_{n-1},\cdots,[x_i]_0)\in F_2^n$ 为一个 n 比特字,设 $f(x)=([f(x)]_{n-1},\cdots,[f(x)]_1,[f(x)]_0)$ 为 $F_2^{m\times n}\to F_2^{l\times n}$ 上的多输出函数. 如果输出的第 i 位 $[f(x)]_i$ 仅与输入的第 0 位到第 i 位,即 $([x]_i,\cdots,[x]_1,[x]_0)$ 有关,则称 $f(x)$ 为 T 函数. 其中 $[x]_i,[f(x)]_i$ 分别表示 n 维向量 x 和 $f(x)$ 的第 i 路分量,$i=0,1,\cdots n-1$. 当 $m=l=1$ 时称为单字 T 函数,否则称为多字 T 函数.

本文的研究重点为单字 T 函数,故下文在不加说明的情况下,T 函数均指单字 T 函数.

定义 2[2]　设 $f(x)$ 为 $F_2^n\to F_2^n$ 上的 T 函数,任取 $x_0\in F_2^n$ 为初态,$x_t=f(x_{t-1})$ 为第 t 时刻状态,则序列 $\bar{x}=(x_0,x_1,x_2,\cdots)$ 称为由 $f(x)$ 生成的状态序列,其中 $x_t=(x_{t,n-1},\cdots,x_{t,1},x_{t,0})$,序列 $\bar{x}_i=(x_{0,i},x_{1,i},x_{2,i},\cdots)$ 称为由 $f(x)$ 生成的第 i 分位序列. 若序列 $\bar{x}$ 的周期为 2^n,则称 $f(x)$ 为单圈 T 函数.

定义 3[2]　设 $f(x)$ 是 $F_2^n\to F_2^n$ 上的多输出函数,记 $f(x)=([f(x)]_{n-1},\cdots,[f(x)]_1,[f(x)]_0)$,如果输出的第 i 位 $[f(x)]_i$ 仅与输入的第 0 至第 $i-1$ 位有关,则称 $f(x)$ 为参数.

定义 4[2]　若 $r(x)$ 是 $F_2^n\to F_2^n$ 上的参数,令 $B[r,n]=2^{-n}\sum_{i=0}^{2^{n-1}-1}(r(i+2^{n-1})-r(i))\pmod 2$,若存在 N_0,对任意 $n>N_0$,有 $B[r,n]=0$ 成立,则称 $r(x)$ 为偶参数;若对任意 $n>N_0$,有 $B[r,n]=1$ 成立,则称 $r(x)$ 为奇参数. 若对任意 N_0,均存在 $n_0>N_0,n_1>N_0$ 使得 $B[r,n_0]=0,B[r,n_1]=1$,则称 $r(x)$ 为非奇非偶参数.

另一方面,介绍非阿基米德理论中 T 函数的相关定义. 二元域上的任意一条序列 $\bar{x}=\cdots x_2x_1x_0$,其中 $x_j\in F_2=\{0,1\}$,可看作自然数 $\sum_{j=0}^{n-1}2^jx_j$,则任意一条二元序列均可视作由实数加法与乘法构成的 2-adic 整数环 Z_2 中的元素,而且 2-adic 整数环 Z_2 中的元素与二元域 F_2 上的序列存在一一对应关系. 另外,2-adic 整数环 Z_2 包含了分母为奇数的既约有理分数,而最终周期序列都能表示成分母为奇数的既约有理分数的形式. 所以,T 函数生成序列的相关性质可在 2-adic 整数环中进行讨论.

2-adic 整数环还有一重要性质,即关于距离构成度量空间,距离的定义如下:令 $u,v\in Z_2$,则 u,v 的距离表示为 $d_2(u,v)=|u-v|_2=\frac{1}{2^k}$,其中 $k=\min\{j|[u]_j\neq[v]_j\}$,且满足 $d_2(u,v)=0$ 当且仅当 $u=v$. 在这种定义下,当 $v=0$ 时,$d_2(u,0)=|u|_2$ 表示 u 的 2-adic 绝对值,记 $ord_2u=-\log_2|u|_2$ 表示 u 的 2-adic 估值,$ord_20=\infty$. 此时,对于任意 $a,b\in Z_2$,满足 $|a-b|_2\leqslant 2^{-k}$ 当且仅当 $a\equiv b\pmod{2^k}$.

另外,距离度量满足强三角不等式:任意 $a,b\in Z_2$,有 $|a+b|_2\leqslant\max\{|a|_2,|b|_2\}$,满足这一特性的度量又被称为超度量空间或非阿基米德度量空间. 在该度量空间中,可以讨论可微性,可导性,连续性,极限等性质. 此时,可以利用度量的概念给出 1-Lipschitz 函数的定义,即为单字 T 函数的定义.

定义 5[11]　若 $Z_2\to Z_2$ 上的函数 $f(x)$ 对于任意 u,v

$\in Z_2$,都有$|f(u)-f(v)|_2 \leqslant |u-v|_2$成立,则称$f(x)$为2-adic整数环上的1-Lipschitz函数.

定义6[11] T函数$f:Z_2\to Z_2$在点$x_0\in Z_2$称为可微的(其中$f'(x)\in Z_2$称为f在点x的导数)当且仅当对任意正整数M,存在正整数K,使得当$|h|_2\leqslant\frac{1}{2^K}$时,$f(x_0+h)\equiv f(x_0)+f'(x_0)\cdot h(\mathrm{mod}2^{ord_2h+M})$成立.

定义7[11] T函数$f:Z_2\to Z_2$称为模2^M一致可微的当且仅当存在正整数K,使得当$|h|_2\leqslant\frac{1}{2^K}$(即$h\equiv 0\mathrm{mod}2^K$)时,对任意$x\in Z_2$下式成立:

$$f(x+h)\equiv f(x)+f'(x)\cdot h(\mathrm{mod}2^{ord_2h+M})$$

具有上述特性的$K=K(M)$的最小值记为$N_M(f)$.

定义8[11] T函数$f:Z_2\to Z_2$称为一致可微的当且仅当对任意正整数$M\in N$,存在正整数K,使得当$|h|_2\leqslant\frac{1}{2^K}$时,对任意$x\in Z_2$下式均成立:

$$f(x+h)\equiv f(x)+f'(x)\cdot h(\mathrm{mod}2^{ord_2h+M})$$

给定M,具有上述特性的$K=K(M)$的最小值记为$N_M(f)$,这里$N_M(f)$的含义与定义7中的一致.

3 参数与一致可微

下面利用非阿基米德理论,对传统T函数中的参数概念进行深入研究,建立起非阿基米德理论中单圈性判定条件与传统T函数理论中单圈性判定条件之间的联系,首先,给出相关引理.

引理1[11] 设$f:Z_2\to Z_2$是模2一致可微T函数,则其是可逆的当且仅当f模$2^{N_u(f)+1}$是可逆的.

引理2[11] 设$f:Z_2\to Z_2$是模4一致可微T函数,则其是单圈的当且仅当f模$2^{N_u(f)+2}$是单圈的.

引理3[11] 设$f:Z_2\to Z_2$是模4一致可微单圈T函数,则对任意$x\in Z_2$,其导数满足$f'(x)\equiv 1(\mathrm{mod}2)$.

引理4[2] 设$r(x)$是$F_2^n\to F_2^n$上的参数,若存在整数N_0使得函数$f(x)=x+r(x)\mathrm{mod}2^{N_0}$是单圈函数,则$f(x)$是单圈T函数当且仅当对所有$n\geqslant N_0$,$r(x)$是偶参数.

引理5[2] 设$r(x)$是$F_2^n\to F_2^n$上的参数,若存在整数N_0使得函数$f(x)=x\oplus r(x)\mathrm{mod}2^{N_0}$是单圈函数,则$f(x)$是单圈T函数当且仅当对所有$n\geqslant N_0$,$r(x)$是奇参数.

引理6[2] 设$f(x)$是$F_2^n\to F_2^n$上的T函数,则$f(x)$是单圈T函数的充要条件是存在$F_2^n\to F_2^n$上的一个参数$\alpha(x)$,对所有的$i<n$,有$[f(x)]_i=[x]_i\oplus[\alpha(x)]_i$,且满足$\bigoplus_{x=0}^{2^i-1}[\alpha(x)]_i=1$.

上述引理中,引理2基于非阿基米德理论给出了判定一类T函数是否为单圈T函数的方法,引理6基于传统T函数理论给出了判定所有T函数是否为单圈T函数的方法.引理2的条件易于判定,但只对特殊的T函数成立;引理6的判定条件对所有的T函数成立,但考查其充要条件存在一定的困难.所以为了寻找更好的判定方法,我们通过研究传统理论中参数的概念在非阿基米德理论中的含义,找出不同判定条件之间的联系,给出不同判定条件的适用范围.

定理1 T函数$f(x)$为$Z_2\to Z_2$上的参数当且仅当$f(x)$模2一致可微,且对任意$x\in Z_2$,满足$f'(x)\equiv 0(\mathrm{mod}2)$.

证明 充分性:由于$f(x)$模2一致可微,则存在正整数K,使得当$|h|_2\leqslant 2^{-K}$(即$h\equiv 0\mathrm{mod}2^K$)时,对任意$x\in Z_2$,满足$f(x+h)\equiv f(x)+f'(x)\cdot h(\mathrm{mod}2^{ord_2h+1})$,又因为对任意$x\in Z_2$,有$f'(x)\equiv 0(\mathrm{mod}2)$,则当$k\geqslant K$时,令$h=2^k$,得到$f(x+2^k)\equiv f(x)(\mathrm{mod}2^{k+1})$,根据参数的定义知$f(x)$为参数.

必要性:由于$f(x)$为参数,则存在整数K,当$k\geqslant K$时,有$f(x+2^k)\equiv f(x)(\mathrm{mod}2^{k+1})$成立,即对任意$h\equiv 0\mathrm{mod}2^K$,有$f(x+h)\equiv f(x)+0\times h(\mathrm{mod}2^{k+1})$成立.则由一致可微的定义得,$f$为模2一致可微的,且对任意$x\in Z_2$,$f'(x)\equiv 0(\mathrm{mod}2)$.

定理1给出了参数在非阿基米德理论中的描述,建立了两种理论之间的联系,在此基础上,我们将讨论奇参数与偶参数的性质,并给出它们在非阿基米德理论中的描述.

定理2 若$f:Z_2\to Z_2$是模4一致可微T函数,且对任意$x\in Z_2$,有$f'(x)\equiv 0(\mathrm{mod}2)$成立,则当$k\geqslant N_2(f)+2$时,$f$为偶参数.

证明 由于f为模4一致可微的,则存在$K\in N$,使得当$|h|_2\leqslant 2^{-K}$(即$h\equiv 0\mathrm{mod}2^K$)时,对任意$x\in Z_2$,满足$f(x+h)\equiv f(x)+f'(x)\cdot h(\mathrm{mod}2^{ord_2h+2})$.令$h=2^k$,其中$k\geqslant K+1$,得$f(x+2^k)\equiv f(x)+2^k\cdot f'(x)(\mathrm{mod}2^{k+2})$.考虑$[f'(x)]_1=\frac{1}{2^{k+1}}(f(x)-f(x+2^k))(\mathrm{mod}2)$,由于$f'(x)\mathrm{mod}4$的周期为$2^K$,则$[f'(x)]_1$的周期为$2^K$,于是下式成立

$$\frac{1}{2^{k+1}}\sum_{x=0}^{2^{k-1}}(f(x)-f(x+2^k))\equiv\sum_{x=0}^{2^{k-1}}[f'(x)]_1$$
$$\equiv 2^{k-K}\sum_{x=0}^{2^K-1}[f'(x)]_1\equiv 0(\mathrm{mod}2)$$

由偶参数的定义得,当$k\geqslant N_2(f)+2$时,f为偶参数.

推论1 若T函数$f:Z_2\to Z_2$为奇参数,则f一定不是模4一致可微的.

定理1和定理2说明模4一致可微的参数一定是

偶参数,但偶参数不一定是模 4 一致可微的. 推论 1 表明奇参数一定不是模 4 一致可微的,根据奇偶参数与一致可微性的关系,结合单圈 T 函数的判定定理,得到以下结论:

推论 2　若存在正整数 K,使得 T 函数 $g(x)=x+f(x)\bmod 2^K$ 为单圈函数,则 $g(x)$ 是单圈 T 函数当且仅当 $f(x)$ 是模 4 一致可微的,且对任意 $x\in Z_2$,有 $f'(x)\equiv 0(\bmod 2)$,同时满足 $N_2(f)\leqslant K$.

定理 3　若单圈 T 函数 $f(x):Z_2\to Z_2$ 是模 4 一致可微的,则 $f(x)$ 可以表示成 $f(x)=x+r(x)$ 的形式,其中当 $k\geqslant N_2(f)+2$ 时,$r(x)$ 为偶参数.

证明　由于单圈 T 函数 $f(x):Z_2\to Z_2$ 是模 4 一致可微的,由引理 3 得 $f'(x)\equiv 1(\bmod 2)$,且当 $|h|_2\leqslant 2^{-N_2(f)}$ 时,对任意 $x\in Z_2$,下式成立:

$$f(x+h)\equiv f(x)+f'(x)\cdot h(\bmod 2^{ord_2 h+2})$$

令 $r(x)=f(x)-x$,任取 $|h|_2\leqslant 2^{-N_2(f)}$(即 $h\equiv 0\bmod 2^{N_2(f)}$),对任意 $x\in Z_2$,有:

$$r(x+h)\equiv f(x+h)-(x+h)\equiv f(x)+h\cdot f'(x)-(x+h)$$
$$\equiv r(x)+h\cdot(f'(x)-1)\equiv r(x)+h\cdot r'(x)(\bmod 2^{ord_2 h+2})$$

由 $f'(x)\equiv 1(\bmod 2)$,得到 $r'(x)\equiv 0(\bmod 2)$,且由一致可微的定义知 $r(x)$ 为模 4 一致可微的. 根据定理 2,则当 $k\geqslant N_2(f)+2$ 时,$r(x)$ 为偶参数,得证.

定理 1、定理 2 及推论 1 描述了传统 T 函数理论中参数、奇参数和偶参数等概念与非阿基米德理论中一致可微性的关系,说明了参数均是模 2 一致可微的、模 4 一致可微的参数一定是偶参数、奇参数一定不具有模 4 一致可微性,这为进一步研究 T 函数的性质提供了理论支撑. 同时,结合已有的 T 函数单圈性判定方法,发现非阿基米德理论中利用一致可微性判定 T 函数单圈性的方法,部分适用于传统理论中通过偶参数构造的 T 函数,而对基于奇参数构造的 T 函数,该判定方法不再适用,这为研究 T 函数的判定方法提供了新的工具.

4　T 函数最高分位序列保熵性研究

环 $Z/(p^e)$ 上由本原多项式 $f(x)$ 生成序列的保熵性,是为了考察该序列经过压缩变换后是否有信息丢失. 这里,我们对单圈 T 函数 $f(x)$ 的状态生成序列做压缩变换,同样考察压缩过程中是否有信息的丢失. 由于单圈 T 函数 $f(x)$ 取不同初态时的生成序列具有相同的圈结构,故此时将保熵性的定义进行拓展,称为广义保熵性. 具体地,设集合 Ω 为若干单圈 T 函数的集合,$S(\Omega)$ 为 Ω 中单圈 T 函数的状态生成序列集合,设 $\varphi(x_{n-1},\cdots,x_1,x_0)$ 为 $F_2^n\to F_2^l$ 上的映射,称序列 $\varphi(\bar{x}_{n-1},\cdots,\bar{x}_1,\bar{x}_0)=(\varphi(x_{n-1}(t),\cdots,x_1(t),x_0(t)))_{t\geqslant 0}$ 为 φ 作用在 $\bar{x}$ 上的压缩导出序列. 若对任意 $\bar{a},\bar{b}\in S(\Omega)$,$\bar{a}=\bar{b}$ 当且仅当 $\varphi(\bar{a}_{n-1},\cdots,\bar{a}_1,\bar{a}_0)=\varphi(\bar{b}_{n-1},\cdots,\bar{b}_1,\bar{b}_0)$,则称映射 φ 对 $S(\Omega)$ 是保熵的.

由于 T 函数第 i 路输出只与第 $0,\cdots,i$ 路输入有关,因此 T 函数所有输出分位序列中最高分位序列包含的输入信息最多. 本节考察单圈 T 函数输出的最高分位序列是否具有保熵性.

根据 T 函数的构造方法和结构特点,不难发现任意单圈 T 函数输出序列的最高分位序列可由多个不同的单圈 T 函数生成,故任意单圈 T 函数输出序列的最高分位序列不具有保熵性. 因此,我们将考察的范围限制到具有某一特性的单圈 T 函数.

引理 7[15]　设 $f(x):Z_2\to Z_2$ 是模 4 一致可微的 T 函数,则其导数模 4 是周期函数,且周期是 $2^{N_2(f)}$ 的因子,即 $per\{f'(x)(\bmod 4)\}\,|\,2^{N_2(f)}$.

引理 8[11]　设 $f(x):Z_2\to Z_2$ 是模 4 一致可微的单圈 T 函数,$\bar{x}=(x_0,x_1,x_2,\cdots\cdots)$ 为 $f(x)$ 生成的状态序列,x_0 为给定初态,则对任意分位 $j\geqslant N_2(f)+1$,下式成立:

$$x_{i+2^{j-1},j}=x_{i,j}\oplus x_{2^{j-1},j}\oplus x_{i,j-1}\oplus x_{0,j}\oplus x_{0,j-1}\oplus y(i)(\bmod 2)$$

其中 $y(i)$ 与分位 j 无关,且 $\mathrm{per}(\{y(i)\}_{i=0}^{\infty})=2^K$,$0\leqslant K\leqslant N_2(f)$.

从引理 8 的证明过程中,可以得到以下结论:

推论 3　设 $f(x)$ 是模 4 一致可微的单圈 T 函数,$\bar{x}=(x_0,x_1,x_2,\cdots\cdots)$ 为 $f(x)$ 生成的状态序列,其中第 i 时刻状态为 $x_i=(x_{i,n-1},x_{i,n-2},\cdots,x_{i,0})\in F_2^n$,则对任意分位 $j\geqslant N_2(f)+1$,下式成立:

$$x_{i+2^{j-1},j}=x_{i,j}\oplus x_{k+2^{j-1},j}\oplus x_{i,j-1}\oplus x_{k,j}\oplus x_{k,j-1}\oplus y(i)(\bmod 2)$$

其中 $y(i)$ 与分位 j 无关,且 $\mathrm{per}(\{y(i)\}_{i=0}^{\infty})=2^K$,$0\leqslant K\leqslant N_2(f)$.

定理 4　设集合 $\Omega=\{f(x)\,|\,f(x)$ 为模 4 一致可微的单圈 T 函数,存在 $x\in Z_2$,使得 $f'(x)\neq 1\bmod 4$,其中 $N_2(f)\leqslant K\}$,序列 $\bar{x}=(x_0,x_1,x_2,\cdots\cdots)$,$\bar{y}=(y_0,y_1,y_2,\cdots\cdots)$ 是集合 Ω 中任意 T 函数的状态生成序列,若 $\bar{x}=\bar{y}(\bmod 2^{K+2})$ 当且仅当 $\bar{x}_{K+1}=\bar{y}_{K+1}$ 成立,则对于 $n\geqslant K+2$,有 $\bar{x}=\bar{y}(\bmod 2^n)$ 当且仅当 $\bar{x}_{n-1}=\bar{y}_{n-1}$ 成立.

证明　设 $\bar{x}=(x_0,x_1,x_2,\cdots\cdots)$ 为 $f(x)\in\Omega$ 的生成序列,$\bar{y}=(y_0,y_1,y_2,\cdots\cdots)$ 为 $g(x)\in\Omega$ 的生成序列,利用归纳法进行证明:

由于序列 $\bar{x}=(x_0,x_1,x_2,\cdots\cdots)$ 与序列 $\bar{y}=(y_0,y_1,y_2,\cdots\cdots)$ 为集合 Ω 中任意 T 函数的生成序列,由条件 $\bar{x}=\bar{y}(\bmod 2^{K+2})$ 当且仅当 $\bar{x}_{K+1}=\bar{y}_{K+1}$ 成立,则当 $n=K+2$ 时,结论成立.

假设当 $n=k>K+2\geqslant N_2(f)+2$ 时,结论成立,即满足 $\bar{x}=\bar{y}(\bmod 2^k)$ 成立当且仅当 $\bar{x}_{k-1}=\bar{y}_{k-1}$ 成立.

对于序列 $\bar{x}$ 和 $\bar{y}$,当 $\bar{x}_k=\bar{y}_k$ 时,若此时存在时刻 t,使得 $x_{t,k-1}=y_{t,k-1}$,根据推论 3,对任意时刻 i 下式成立

$$x_{i+2^{k-2},k-1}=x_{i,k-1}\oplus x_{t+2^{k-2},k-1}\oplus x_{i,k-2}\oplus x_{t,k-1}\oplus x_{t,k-2}\oplus\alpha(i)\ (\mathrm{mod}2)$$

$$y_{i+2^{k-2},k-1}=y_{i,k-1}\oplus y_{t+2^{k-2},k-1}\oplus y_{i,k-2}\oplus y_{t,k-1}\oplus y_{t,k-2}\oplus\beta(i)\ (\mathrm{mod}2)$$

由假设条件 $\bar{x}_{k-1}=\bar{y}_{k-1}$ 时,有 $\bar{x}=\bar{y}\ (\mathrm{mod}2^k)$,故 $\bar{x}_{k-2}=\bar{y}_{k-2}$,所以得到对任意时刻 i,有 $\alpha(i)=\beta(i)\ (\mathrm{mod}2)$.

进一步地,当 $n=k+1$ 时,任意时刻 i 由推论 3,有

$$x_{i+2^{k-1},k}=x_{i,k}\oplus x_{t+2^{k-1},k}\oplus x_{i,k-1}\oplus x_{t,k}\oplus x_{t,k-1}\oplus\alpha(i)\ (\mathrm{mod}2)$$

$$=y_{i+2^{k-1},k}=y_{i,k}\oplus y_{t+2^{k-1},k}\oplus y_{i,k-1}\oplus y_{t,k}\oplus y_{t,k-1}\oplus\beta(i)\ (\mathrm{mod}2)$$

得到 $x_{i,k-1}\oplus x_{t,k-1}=y_{i,k-1}\oplus y_{t,k-1}\ (\mathrm{mod}2)$,而 $x_{t,k-1}=y_{t,k-1}$,所以此时 $x_{i,k-1}=y_{i,k-1}$,即 $\bar{x}_{k-1}=\bar{y}_{k-1}$,根据假设得到此时 $\bar{x}=\bar{y}\ (\mathrm{mod}2^k)$,所以 $\bar{x}=\bar{y}\ (\mathrm{mod}2^{k+1})$,故结论 $\bar{x}=\bar{y}\ (\mathrm{mod}2^{k+1})$ 成立当且仅当 $\bar{x}_k=\bar{y}_k$ 成立,即证.

若当 $\bar{x}_k=\bar{y}_k$ 时,不存在时刻 t,使得 $x_{t,k-1}=y_{t,k-1}$,即任意时刻 $i\geqslant 0$,都有 $x_{i,k-1}=y_{i,k-1}\oplus 1$,令 $\bar{y}'=(y'_0,y'_1,y'_2,\cdots\cdots)=(y_{2^{k-1}},y_{2^{k-1}+1},y_{2^{k-1}+2},\cdots\cdots)$,则 $\bar{y}'$ 为 $g(x)\in\Omega$ 的生成序列,而此时任意时刻 i 满足 $x_{i,k-1}=y_{i,k-1}\oplus 1=y_{i+2^{k-1},k-1}=y'_{i',k-1}$,即 $\bar{x}_{k-1}=\bar{y}'_{k-1}$,由假设可得此时 $\bar{x}=\bar{y}'\ (\mathrm{mod}2^k)$,又由于 $\bar{y}'=(y_{2^{k-1}},y_{2^{k-1}+1},y_{2^{k-1}+2},\cdots\cdots)=y\ (\mathrm{mod}2^{k-1})$,所以得到 $\bar{x}=\bar{y}\ (\mathrm{mod}2^{k-1})$,

由 $f(x)$ 与 $g(x)$ 为模 4 一致可微 T 函数,$\bar{x}=\bar{y}'\ (\mathrm{mod}2^k)$,而 $k\geqslant\mathrm{Max}(N_2(f)+2,N_2(g)+2)$,故 $f(x+2^{k-2}h)=f(x)+2^{k-2}hf'(x)\ (\mathrm{mod}2^k)$,$g(y+2^{k-2}h)=f(y)+2^{k-2}hf'(y)\ (\mathrm{mod}2^{k+1})$,可得 $f'(x)=g'(y)\,\mathrm{mod}4$. 另一方面,序列 $\bar{x}$ 及序列 $\bar{y}$ 满足 $\bar{x}=\bar{y}\ (\mathrm{mod}2^{k-1})$,$\bar{x}_{k-1}=\bar{y}_{k-1}\oplus 1$,$\bar{x}_k=\bar{y}_k$,则根据一致可微的定义,任意时刻 $i\geqslant 0$ 都有

$$x_{i+2^{k-1}+1}=f(x_{i+2^{k-1}})=f(x_i+(x_{i+2^{k-1}}-x_i))=f(x_i)+(x_{i+2^{k-1}}-x_i)f'(x_i)\ (\mathrm{mod}2^k)$$

$$y_{i+2^{k-1}+1}=g(y_{i+2^{k-1}})=g(y_i+(y_{i+2^{k-1}}-y_i))=g(y_i)+(y_{i+2^{k-1}}-y_i)g'(y_i)\ (\mathrm{mod}2^k)$$

其中 $x_i=y_i\,\mathrm{mod}2^K$,所以有

$$f'(x)=\frac{y_{i+2^{k-1}+1}-y_{i+1}}{y_{i+2^{k-1}}-y_i}=\frac{2(y_{i+2^{k-1}+1,k}\oplus y_{i+1,k}\oplus y_{i+1,k-1})+1}{2(y_{i+2^{k-1},k}\oplus y_{i,k}\oplus y_{i,k-1})+1}$$

$$=\frac{2(x_{i+2^{k-1}+1,k}\oplus x_{i+1,k}\oplus x_{i+1,k-1}\oplus 1)+1}{2(x_{i+2^{k-1},k}\oplus x_{i,k}\oplus y_{i,k-1}\oplus 1)+1}$$

$$=\frac{2(x_{i+2^{k-1}+1,k}\oplus x_{i+1,k}\oplus x_{i+1,k-1})+1}{2(x_{i+2^{k-1},k}\oplus x_{i,k}\oplus y_{i,k-1})+1}$$

$$=\frac{x_{i+2^{k-1}+1}-x_{i+1}}{x_{i+2^{k-1}}-x_i}=g'(y)\,\mathrm{mod}4$$

上式成立当且仅当 $x_{i+2^{k-1}+1,k}\oplus x_{i+1,k}\oplus x_{i+1,k-1}=x_{i+2^{k-1},k}\oplus x_{i,k}\oplus x_{i,k-1}$ 时,即满足任意 $x,y\in Z_2$,$f'(x)=g'(y)=1\,\mathrm{mod}4$,然而此时与条件存在 $x,y\in Z_2$,$f'(x)\neq 1\,\mathrm{mod}4$ 且 $g'(y)\neq 1\,\mathrm{mod}4$ 矛盾,故该情况不存在,即若当 $\bar{x}_k=\bar{y}_k$ 时,一定存在时刻 t,使得 $x_{t,k-1}=y_{t,k-1}$. 综上所述,当 $n=k+1$ 时,$\bar{x}=\bar{y}\ (\mathrm{mod}2^n)$ 当且仅当 $\bar{x}_{n-1}=\bar{y}_{n-1}$ 成立,即证.

定理 4 说明对于一类模 4 一致可微且具有相似结构(即相近的 $N_2(f)$ 值)的单圈 T 函数,考察其中任意两个不同的 T 函数能否生成相同的最高分位输出序列只需考察当输入规模较小时($n=N_2(f)+2$),结论是否成立.

5 小结

本文研究了一致可微的单圈 T 函数的性质,首先通过讨论参数概念在非阿基米德理论中的含义,给出了两种理论中单圈 T 函数判定条件的联系,说明了非阿基米德理论中的判定条件适用于部分由偶参数构造的 T 函数. 另一方面,考察了单圈 T 函数最高分位输出序列的保熵性,说明了一般 T 函数不具有保熵性,而对于模 4 一致可微且具有相似结构的单圈 T 函数,其最高分位序列保熵性等价于当输入规模较小时最高分位序列的保熵性,为研究具有相似结构 T 函数的多样性提供了理论基础.

参考文献

[1] A Klimov, A Shamir. A new class of invertible mappings [A]. CHES 2002 [C]. Berlin: Springer-Verlag, LNCS 2523, 2003. 470 – 483.

[2] A Klimov, A Shamir. Cryptographic applications of T-functions [A]. SAC 2003 [C]. Berlin: Springer-Verlag, LNCS 3006, 2003. 248 – 261.

[3] A Klimov, A Shamir. New cryptographic primitives based on multiword T-functions [A]. FSE 2004 [C]. Berlin: Springer-Verlag, LNCS 3017, 2004. 1 – 15.

[4] J Hong, D Lee, Y Yeom, D Han. A new class of single cycle t-functions [A]. FSE 2005 [C]. Berlin: Springer, LNCS 3557, 2005. 68 – 82.

[5] V Anashin, A Bogdanov, I Kizhvtov, S Kumar. ABC: A new fast flexible stream cipher [EB/OL]. http://www.ecrypt.eu.org/ stream, 2005.

[6] A Maximov. A new stream cipher "Mir – 1" [EB/OL]. http://www.ecrypt.eu.org/stream, 2005.

[7] N Kolokotronis. Cryptographic properties of nonlinear pseudorandom number generators [J]. Designs Codes & Cryptography, 2008, 46: 353 – 363.

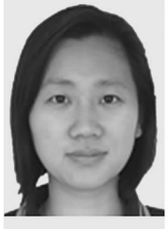
[8] N Kolokotronis. Cryptographic properties of stream ciphers based on t-functions [A]. ISIT 2006 [C]. USA: IEEE, 2006. 1604 – 1608.

[9] W Y Zhang, C K Wu. The Algebraic normal form, linear complexity and k-error linear complexity of single-cycle t-fFunction [A]. SETA 2006 [C]. Berlin: Springer, LNCS

4086,2006. 391 – 401.
[10] 游伟,戚文峰. 单圈 T 函数的 2-adic 复杂度及 1-错 2-adic 复杂度[J]. 通信学报,2014,35(3):135 – 139.
You Wei,Qi Wen-feng. The 2-adic complexity and the 1-error 2-adic complexity of single cycle T-functions[J]. Journal on Communications,2014,35(3):135 – 139. (in Chinese)
[11] V Anashin. Non-Archimedean analysis, T-functions, and cryptography [EB/OL]. http://arxiv. org/abs/cs/0612038,2006.
[12] V Anashin. Uniformly distributed sequences of p-adic integers[J]. Mathematical Notes,1994,55(2):109 – 133.
[13] V Anashin. Uniformly distributed sequences of p-adic integers,II[J]. Discrete Math Appl,2002,12(6):527 – 590.
[14] V Anashin. Pseudorandom number generation by p-adic ergodic transformations[EB/OL]. http://arxiv. org/abs/cs. CR/0401030,January 2004.
[15] V Anashin, A Khrennikov, E Yurova. T-functions revisited: New criteria for bijectivity/transitivity[J]. Designs Codes & Cryptography,2014,71(3):383 – 407.
[16] T Shi,V Anashin,D D Lin. Linear Weaknesses in T-functions[A]. SETA 2012[C]. Berlin: Springer-Verlag, LNCS 7280,2012. 279 – 290.
[17] T Shi,V Anashin,D D Lin. Fast Evaluation of T-functions via Time-Memory Trade-Offs[A]. Informations Security and Cryptology 2012[C]. Berlin: Springer, LNCS 7763, 2013. 263 – 275.
[18] Huang M Q. Analysis and cryptological evaluation of primitive sequences over an integer residue ring[D]. Beijing: Graduate School of USTC,1988.
[19] Dai Z D. Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials[J]. Journal of Cryptology,1992,5(3):193 – 207.
[20] Huang M Q,Dai Z D. Projective maps of linear recurring sequences with maximal p-adic periods[J]. Fibonacci Quart,1992,30(2):139 – 143.
[21] A S Kuzmin,A A Nechaev. Linear recurring sequences over Galois rings[J]. Algebra & Logic,1995,34(2):87 – 100.

作者简介

王森鹏　男,1990 年出生,河南商丘人. 解放军信息工程大学硕士生,主要研究方向:密码学与信息安全.
E-mail:wsp2110@126. com



刘　燕(通信作者)　女,1990 年出生,江苏无锡人,解放军信息工程大学硕士生,主要研究方向:密码学与信息安全.
E-mail:awhxxsbb@126. com