T函数的圈结构特征

罗小建 胡 斌

(解放军信息工程大学电子技术学院 郑州 450004)

摘 要 T函数是n位字到n位字的一个映射,并且输出的第i位仅与第$0,1,\cdots,i$位有关,$0\leqslant i\leqslant n-1$。可逆T函数在密码学上有重要的应用。深入研究了一般可逆T函数的圈结构,利用T函数的结构和参数特性,首次从理论上证明了可逆T函数的任一圈结构的长度都是2的方幂这一重要特征,并分别从不同的角度给出了由可逆T函数$f(x) \bmod 2^k$的圈结构判定$f(x) \bmod 2^{k+1}$圈结构的两种不同判定方法。基于此进一步分析了可逆T函数的圈结构特征,提出了可逆T函数圈结构特征为$2^{n-t}\times 2^t$的判定方法。

关键词 密码学,T函数,状态转移图,圈结构,参数

中图法分类号 TN918 **文献标识码** A

Cycle Structure Characteristic of T-functions

LUO Xiao-jian HU Bin

(Electronic Technology Institute, Information Engineering University, Zhengzhou 450004, China)

Abstract T-functions is a mapping from n-bits to n-bits words in which each$(0\leqslant i\leqslant n-1)$bit i of the output depends only on bits $0,1,\cdots,i$ of the input. Invertible T-functions is essential ingredients in many cryptographic applications. By using the cycle structure and parameter, we proved that every cycle has length of powers of 2. Then we studied on the cycle structure of the invertible T-functions intensively, and gave two different methods for retrieving the cycle structure of the invertible T-functions $f(x) \bmod 2^{k+1}$ on basis of $f(x) \bmod 2^k$. Moreover, based on the retriving cycle structure method, we presented a determinant condition of the cycle structure characteristic $2^{n-t}\times 2^t$.

Keywords Cryptography, T-functions, State transfer graph, Cycle structure, Paremeter

1 引言

Klimov和Shamir提出了T函数的概念,并对其进行了一系列研究[1,2]。T函数是n位字到n位字的一个映射,并且第i位的输出仅与输入的$0,1,\cdots,i$位值有关,$0\leqslant i\leqslant n-1$。如果可逆T函数所决定的状态转移图的周期为$2^n$,则称该T函数为单圈T函数。Klimov和Shamir提出可用单圈T函数代替线性移位寄存器作为密钥发生器的驱动源的想法。在IACR发起的欧洲流密码计划Estream中,单圈T函数就被用于流密码设计。韩国学者Jin Hong提交的流密码TSC-3以T函数作为状态转移函数。另外,T函数还可用于分组密码和杂凑函数的设计中。

国外对于T函数的研究不是很多,Klimov和Shamir得到了关于T函数的一些有意义的结果。文献[1]研究了T函数的性质,通过图示方法指出任意圈结构的长度都是2的方幂,并给出了可逆T函数单圈性的充要条件。Jin Hong等给出了一类新的单圈T函数,并基于该类T函数给出了一个流密码实例[2]。目前国内对T函数的研究很少,2007年于静之等对单圈T函数的代数标准形进行了研究,给出了根据单圈T函数的连续2^{n-1}个状态写出其代数标准型的一种方法[4];2008年赵璐等给出了单圈T函数输出序列的线性复杂度及稳定性[5]。

T函数的一个重要应用是作为流密码中的状态转移函数,因此对其圈结构的研究显得尤为重要。但由于其是非线性函数,圈结构的研究难度非常大。Klimov等指出了其圈结构的一个基本特性[1],但由于T函数的非线性性和难于刻画性,他未能给出理论上的证明。而对于一般可逆T函数的圈结构分布及其判定条件目前尚无具体研究结果。本文对一般可逆T函数的圈结构进行了深入研究,利用T函数的结构和参数特性,从理论上证明了可逆T函数的任一圈结构的长度都是2的方幂这一重要特征,并分别从不同的角度给出了由可逆T函数$f(x) \bmod 2^k$的圈结构判定$f(x) \bmod 2^{k+1}$圈结构的两种不同判定方法。基于此进一步分析了可逆T函数的圈结构特征,提出了可逆T函数圈结构特征为$2^{n-t}\times 2^t$的判定方法。文献[1]中关于单圈T函数的判定条件是本方法的一个特例,为进一步研究可逆T函数的圈结构特征提供了理论基础。

2 基本定义

定义1[1] 设$f(x)$是$F_2^n\to F_2^n$上的多输出函数,记$f(x)=$

到稿日期:2010-05-12 返修日期:2010-08-29

罗小建(1985—),男,硕士生,主要研究方向为密码学与信息安全,E-mail:luojian1232@163.com;胡 斌(1971—),男,博士,副教授,硕士生导师,主要研究方向为密码学与信息安全。

$([f(x)]_{n-1},\cdots,[f(x)]_0)$，如果其输出的第 i 位$[f(x)]_i$ 仅与输入第 0 至第 i 位，即$([x]_i,\cdots,[x]_0)$有关，则称 $f(x)$为 T 函数。其中$[x]_i$，$[f(x)]_i$ 表示 n 维向量 x 和 $f(x)$的第 i 比特，$i=0,1,\cdots,n-1$。显然，根据 T 函数的定义，可将 T 函数表示为如下形式：

$$\begin{pmatrix} ([x]_{n-1},\cdots,[x]_1,[x]_0) \\ \downarrow \\ (f_{n-1}([x]_{n-1},\cdots,[x]_0),\cdots,f_0([x]_0)) \end{pmatrix} \tag{1}$$

式中，$f_i(x)=f_i([x]_i,[x]_{i-1},\cdots,[x]_0)$为布尔函数。

由 T 函数的定义知，$f(x) \bmod 2^i$ 可以看成是 $F_2^i \to F_2^i$ 的映射，$1\leqslant i\leqslant n$。

定义 2[1] 设 $f(x):F_2^n\to F_2^n$ 为 T 函数，如果$[f(x)]_i=f_i([x]_{i-1},\cdots,[x]_0)$，$i=0,1,\cdots,n-1$，其中 f_i 为布尔函数，则称 $f(x)$为参数。参数一般用 α,β,γ 表示。

显然，参数与 T 函数的区别仅在于参数输出的第 i 位仅与输入的第 0 至第 $i-1$ 位有关，而与输入的第 i 位无关。

定义 3[1] 设 $f(x):F_2^n\to F_2^n$ 为 T 函数，$[f(x)]_i=f_i([x]_i,\cdots,[x]_0)$，$i=0,1,\cdots,n-1$，$f_i$ 为布尔函数，则称$[f(x)]_i$ 为 $f(x)$的第 i 路输出。

定义 4[1] 设 $f(x):F_2^n\to F_2^n$ 是一个 T 函数，$x\in F_2^n$，令 $x^{(i)}=f^i(x)$表示 $f(x)$的一个状态，$x^{(i)}\to x^{(i+1)}$表示状态转移，$x^{(i)}$为 $x^{(i+1)}$的先导，$x^{(i+1)}$为 $x^{(i)}$的后继，则 $x^{(0)}\to x^{(1)}\to\cdots\to x^{(i)}\to\cdots\to x^{(n)}\to\cdots$称为 $f(x)$的状态转移图。特别地，周期为 T 的序列$\{x^{(0)}x^{(1)}\cdots x^{(T-1)}x^{(0)}x^{(1)}\cdots\}$，$x^{(i+T)}=x^{(i)}$的状态转移图可以形象地画成一个首尾相接的圆，如图 1 所示。此时称该状态转移图为圈，序列的周期 T 即为圈的长度。

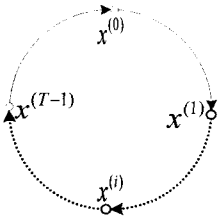

图 1 周期序列的圈结构

3 可逆 T 函数的圈结构特征

下面主要运用第 i 路输出函数和参数以及状态转移图研究可逆 T 函数的圈结构特征。

引理 1[1] 可逆 T 函数 $f(x):F_2^n\to F_2^n$ 的任一状态转移图都构成圈。

由文献[1]知，T 函数 $f(x) \bmod 2^n$ 是可逆的当且仅当对任意的 $i<n$，$f(x)$可表示为$[f(x)]_i=[x]_i\oplus\alpha$，这里 α 为一参数。对于可逆 T 函数，其圈结构特征是 T 函数的重要性质。文献[1]中讨论了可逆 T 函数的圈结构的一个基本特征，但未能给出理论上的证明，下面从理论上证明可逆 T 函数圈结构的这一基本特征。

定理 1 设 $f(x):F_2^n\to F_2^n$ 为可逆的 T 函数，如果 $f(x) \bmod 2^k$ 的状态图中有一个长度为 l 的圈，则对应地 $f(x) \bmod 2^{k+1}$的状态图中有一个长度为 $2l$ 的圈或有两个长度为 l 的圈。特别地，令$[f(x)]_k=[x]_k\oplus\alpha(x)$，则

(1)若$\bigoplus_{i=0}^{l-1}\alpha(x^{(i)})=1$，则对应地 $f(x) \bmod 2^{k+1}$有一个长度为 $2l$ 的圈；

(2)若$\bigoplus_{i=0}^{l-1}\alpha(x^{(i)})=0$，则对应地 $f(x) \bmod 2^{k+1}$有两个长度为 l 的圈。

证明：用 $x_0^{(i)}$ 表示 $f(x) \bmod 2^k$ 的状态，$i=0,1,\cdots,l-1$，$x_1^{(i)}$ 表示 $f(x) \bmod 2^{k+1}$的状态。设 $f(x) \bmod 2^k$ 的一个长度为 l 的圈结构如图 2 所示。

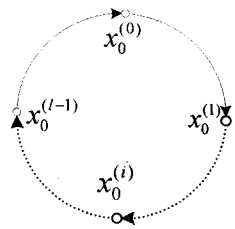

图 2 长度为 l 的圈结构

其状态转移图为 $x_0^{(0)}\to\cdots\to x_0^{(l-1)}\to x_0^{(0)}\cdots$。

在模 2^{k+1}下，考查 $f([x_1^{(j)}]_k,x_0^{(j)})$，$j=0,1,\cdots,l-1$ 的取值。由于 $f(x)$是可逆 T 函数，有

$$[f[x_1^{(j)}]_k,x_0^{(j)})]_i=[[x_1^{(j)}]_k,x_0^{(j)}]_i\oplus\alpha$$

其中 $i=0,1,\cdots,k$，α 是一个参数。

当 $0\leqslant i\leqslant k-1$ 时，

$$[f([x]_k,x_0^{(j)}) \bmod 2^{k+1}]_i=[f(x_0^{(j)}) \bmod 2^k]_i=[x_0^{(j+1)}]_i$$

因此，有 $f([x]_k,x_0^{(j)})=(a,[x_0^{(j+1)}])$，$a\in\{0,1\}$成立，即 $f(x) \bmod 2^{k+1}$时的状态转移图中其低 k 位(从第 0 到第 $k-1$ 位)与 $f(x) \bmod 2^k$ 时状态转移图是相同的，只是所增加的最高位(即第 k 位)是不确定的，于是以 $x_1^{(0)}=(0,x_0^{(0)})$为初态时，$f(x) \bmod 2^{k+1}$下的状态转移图可表示为

$$x_1^{(0)}=(0,x_0^{(0)})\to([x_1^{(1)}]_k,x_0^{(1)})\to\cdots\to([x_1^{(l-1)}]_k,x_0^{(l-1)})\to([x_1^{(l)}]_k,x_0^{(0)})\to\cdots \tag{2}$$

由于 $f(x) \bmod 2^{k+1}$的状态图与 $f(x) \bmod 2^k$ 的状态图相比，增加了一倍的点，并且由 T 函数的定义，对于 $f(x) \bmod 2^{k+1}$的状态图中的点，在不考虑其最高比特位的情形下，其低 k 位(从第 0 到第 $k-1$ 位)的对应关系完全由 $f(x) \bmod 2^k$ 的状态图中的对应关系所决定。利用状态图的这一重要特征关系，下面对初态 $x_1^{(0)}=(0,x_0^{(0)})$时，$f(x) \bmod 2^{k+1}$的状态转移图表示进行分析。

① 当$[x_1^{(l)}]_k=0$ 时，有 $x_1^{(0)}=(0,x_0^{(0)})=([x_1^{(l)}]_k,x_0^{(0)})$，于是 $x_1^{(0)}x_1^{(1)}\cdots x_1^{(l-1)}$ 构成一个周期为 l 的状态序列，即 $f(x) \bmod 2^{k+1}$的状态图表示中有一个长为 l 的圈结构，且这个圈结构的初态为 $x_1^{(0)}=(0,x_0^{(0)})$。同样地，我们考查当初态为 $x_1^{(0)}=(1,x_0^{(0)})$时状态转移图的情况，此时有 $f(1,x_0^{(0)})=f(\overline{0},x_0^{(0)})=(\overline{[x_1^{(1)}]_k},x_0^{(1)})$(如果 $f(1,x_0^{(0)})=([x_1^{(1)}]_k,x_0^{(1)})$，则 $f(1,x_0^{(0)})=f(0,x_0^{(0)})$，这与 $f(x)$的可逆性相矛盾)，于是在 $f(x) \bmod 2^{k+1}$的状态图中除有上述的一个长为 l 的圈结构外，对应地其它状态之间的关系，我们有 $f(\overline{[x_1^{(1)}]_k},x_0^{(1)})=(\overline{[x_1^{(2)}]_k},x_0^{(2)})$，$\cdots$，$f(\overline{[x_1^{(l-1)}]_k},x_0^{(l-1)})=(\overline{[x_1^{(l)}]_k},x_0^{(l)})$。故当初态为 $x_1^{(0)}=(1,x_0^{(0)})$时，对应地其余的 l 个状态所构成的状态转移图为

$$x_1^{(0)}=(1,x_0^{(0)})\to(\overline{[x_1^{(1)}]_k},x_0^{(1)})\to\cdots\to(\overline{[x_1^{(l-1)}]_k},x_0^{(l-1)})\to(\overline{[x_1^{(l)}]_k},x_0^{(0)})=(1,x_0^{(0)})$$

这显然也构成了一个长度为 l 的圈。即此时 $f(x) \bmod 2^{k+1}$的状态图对应地有两个长度为 l 的圈。

② 当$[x_1^{(l)}]_k=1$时，对应于$f(x) \bmod 2^k$的长度为l的圈，由于$f(x)$为可逆T函数，同样地利用$f(x) \bmod 2^k$的状态图与$f(x) \bmod 2^{k+1}$的状态图之间的特征关系，我们可得当初态为$x_1^{(0)}=(0,x_0^{(0)})$时$f(x) \bmod 2^{k+1}$的状态转移图可表示为

$$\begin{aligned}x_1^{(0)}=(0,x_0^{(0)})&\to([x_1^{(1)}]_k,x_0^{(1)})\to\cdots\to([x_1^{(l-1)}]_k,x_0^{(l-1)})\to\\&(1,x_0^{(0)})\to(\overline{[x_1^{(1)}]_k},x_0^{(1)})\to\cdots\to(\overline{[x_1^{(l-1)}]_k},x_0^{(l-1)})\to\\&(\overline{[x_1^{(l)}]_k},x_0^{(0)})=(0,x_0^{(0)})\to\cdots\end{aligned}\tag{3}$$

这显然构成了一个长度为$2l$的圈。

同样地，当初态为$x_1^{(0)}=(1,x_0^{(0)})$时，我们也可以得到该结论。

综上所述，当$f(x) \bmod 2^k$有一个长度为l的圈结构时，对应地$f(x) \bmod 2^{k+1}$有一个长度为$2l$的圈结构或有两个长度为l的圈结构。

由可逆T函数的性质，$f(x)$可表示为$[f(x)]_k=[x]_k \oplus \alpha(x)$，于是可得

$$\begin{aligned}[x_1^{(l)}]_k&=[f(x_1^{(l-1)})]_k=[x_1^{(l-1)}]_k \oplus \alpha(x_1^{(l-1)})\\&=[x_1^{(l-2)}]_k \oplus \alpha(x_1^{(l-2)}) \oplus \alpha(x_1^{(l-1)})\\&=\cdots\cdots\\&=[x_1^{(0)}]_k \oplus \bigoplus_{i=0}^{l-1}\alpha(x_1^{(i)})\end{aligned}$$

由上面的证明可知，当$[x_1^{(l)}]_k=[x_1^{(0)}]_k$时，$\bigoplus_{i=0}^{l-1}\alpha(x^{(i)})=0$，$f(x) \bmod 2^{k+1}$有两个长度为$l$的圈与之对应。当$[x_1^{(l)}]_k=\overline{[x_1^{(0)}]_k}$时，有$\bigoplus_{i=0}^{l-1}\alpha(x^{(i)})=1$，$f(x) \bmod 2^{k+1}$有一个长度为$2l$的圈与之对应。因此有

(1)当$\bigoplus_{i=0}^{l-1}\alpha(x^{(i)})=1$时，$f(x) \bmod 2^{k+1}$有一个长度为$2l$的圈结构。

(2)当$\bigoplus_{i=0}^{l-1}\alpha(x^{(i)})=0$时，$f(x) \bmod 2^{k+1}$有两个长度为$l$的圈结构。

定理1给出了可逆T函数的圈结构特征，也给出了由$f(x) \bmod 2^k$时的圈结构判断$f(x) \bmod 2^{k+1}$圈结构的一个判定定理。

在讨论T函数时，其圈结构特征是非常重要的一个性质。如果能掌握T函数的圈结构特征，则为在密码学中应用T函数提供了重要参考依据。下面再给出T函数的由$f(x) \bmod 2^k$时的圈结构判定$f(x) \bmod 2^{k+1}$圈结构的另一种判定形式。

定理2 如果可逆T函数$f(x) \bmod 2^k$的状态图有一个长度为l的圈，$x_0^{(0)}\to x_0^{(1)}\to\cdots\to x_0^{(l-1)}\to x_0^{(0)}$，记$N=\#\{x_0^{(i)} \mid f(0,x_0^{(i)})=(1,x_0^{(i+1)}) \bmod 2^{k+1}, i=0,\cdots,l-1\}$则(1)若$N$为奇数，则对应地$f(x) \bmod 2^{k+1}$有一个长度为$2l$的圈。(2)若$N$为偶数，则对应地$f(x) \bmod 2^{k+1}$有两个长度为$l$的圈。

这里$\#\{A\}$表示集合A中元素的个数。

证明：记$x_0^{(i)}$表示$f(x) \bmod 2^k$的状态，$x_1^{(i)}$表示$f(x) \bmod 2^{k+1}$的状态。$f(x) \bmod 2^k$的状态图$x_0^{(0)}\to x_0^{(1)}\to\cdots\to x_0^{(l-1)}\to x_0^{(0)}\to\cdots$在$f(x) \bmod 2^{k+1}$下的状态转移图根据初态的不同可分为以下两种情形：

$$\begin{aligned}x_1^{(0)}=(0,x_0^{(0)})&\to([x_1^{(1)}]_k,x_0^{(1)})\to\cdots\to([x_1^{(l-1)}]_k,x_0^{(l-1)})\to\\&([x_1^{(l)}]_k,x_0^{(0)})\to\cdots\end{aligned}\tag{4}$$

$$\begin{aligned}x_1^{(0)}=(1,x_0^{(0)})&\to(\overline{[x_1^{(1)}]_k},x_0^{(1)})\to\cdots\to(\overline{[x_1^{(l-1)}]_k},x_0^{(l-1)})\to\\&(\overline{[x_1^{(l)}]_k},x_0^{(0)})\to\cdots\end{aligned}\tag{5}$$

记状态转移图表示式(4)中

$m_1=\#\{x_0^{(i)} \mid f(0,x_0^{(i)})=(1,x_0^{(i+1)}) \bmod 2^{k+1}, i=0,1,\cdots,l-1\}$

$n_1=\#\{x_0^{(i)} \mid f(1,x_0^{(i)})=(0,x_0^{(i+1)}) \bmod 2^{k+1}, i=0,1,\cdots,l-1\}$

同样地，记状态转移图表示式(5)中

$m_2=\#\{x_0^{(i)} \mid f(0,x_0^{(i)})=(1,x_0^{(i+1)}) \bmod 2^{k+1}, i=0,1,\cdots,l-1\}$

$n_2=\#\{x_0^{(i)} \mid f(1,x_0^{(i)})=(0,x_0^{(i+1)}) \bmod 2^{k+1}, i=0,1,\cdots,l-1\}$

则有$m_1+m_2=N$。又根据$f(x) \bmod 2^k$的状态图与$f(x) \bmod 2^{k+1}$的状态图之间的特征关系知$m_2=n_1$，因此$m_1+n_1=N$，同理可得$m_2+n_2=N$。

由可逆T函数的性质知，$[f(x)]_k=[x]_k \oplus \alpha(x)$，则$[x_1^{(l)}]_k=[x_1^{(0)}]_k \oplus \bigoplus_{i=0}^{l-1}\alpha(x_1^{(i)})$。当

$x_1^{(i)} \in \{x \mid f([x]_k,x_0^{(i)})=(\overline{[x]_k},x_0^{(i+1)}), i=0,\cdots,l-1\}$

时，我们可以得到

$f(x_1^{(i)})=f([x_1^{(i)}]_k,x_0^{(i)})=(\overline{[x]_k},x_0^{(i+1)})$

再由$f(x_1^{(i)})=[x_1^{(i)}]_k \oplus \alpha(x_1^{(i)})$可得$\alpha(x_1^{(i)})=1$，于是有

$$\begin{aligned}\bigoplus_{i=0}^{l-1}\alpha(x_1^{(i)})&=\#\{x \mid f([x]_k,x_0^{(i)})\\&=(\overline{[x]_k},x_0^{(i+1)})\} \bmod 2\end{aligned}\tag{6}$$

当$f(x) \bmod 2^{k+1}$初态为$x_1^{(0)}=(0,x_0^{(0)})$时，

$\#\{x \mid f([x]_k,x_0^{(i)})=(\overline{[x]_k},x_0^{(i+1)}), i=0,\cdots,l-1\} \bmod 2$

$=(m_1+n_1) \bmod 2$

$=N \bmod 2$

当$f(x) \bmod 2^{k+1}$初态为$x_1^{(0)}=(1,x_0^{(0)})$时，

$\#\{x \mid f([x]_k,x_0^{(i)})=(\overline{[x]_k},x_0^{(i+1)}), i=0,\cdots,l-1\} \bmod 2$

$=(m_2+n_2) \bmod 2$

$=N \bmod 2$

故

$\bigoplus_{i=0}^{l-1}\alpha(x_1^{(i)})$

$=\#\{x \mid f([x]_k,x_0^{(i)})=(\overline{[x]_k},x_0^{(i+1)}), i=0,\cdots,l-1\} \bmod 2$

$=N \bmod 2$

因此，①当N为奇数时，有$\bigoplus_{i=0}^{l-1}\alpha(x_1^{(i)})=N \bmod 2=1$，于是由定理1知$f(x) \bmod 2^{k+1}$有一个长度为$2l$的圈。

②当N为偶数时，有$\bigoplus_{i=0}^{l-1}\alpha(x_1^{(i)})=N \bmod 2=0$，于是由定理2知$f(x) \bmod 2^{k+1}$有两个长度为$l$的圈。

推论1 可逆T函数$f(x):F_2^n\to F_2^n$的状态图表示中任一圈的长度都是2的方幂。

证明：当$n=1$时，$f(x) \bmod 2$的状态图表示只能是$0\to0$，$1\to1$或者是$0\to1\to0$的形式，显然是有两个长度为2^0的圈或一个长度为2^1的圈，结论成立。

假设当$n=k$时，结论成立，即$f(x) \bmod 2^k$的任一圈长度都是2的方幂。则当$n=k+1$时，由定理2知，对应于$f(x) \bmod 2^k$的状态图中一个圈长为l的圈，在$f(x) \bmod 2^{k+1}$的状态图中都演变为两个圈长为l的圈或一个圈长为$2l$的圈，显然此时无论是哪一种情形，在$f(x) \bmod 2^{k+1}$状态图中圈长只能是2的方幂，故结论成立。

定理1和定理2给出了T函数圈结构的两个判定定理，

基于此我们证明了T函数的状态图中任一圈的长度都是2的方幂。而这仅仅是刻画了T函数圈结构的一个基本特性。为了在密码算法设计中应用T函数，就必须掌握T函数的圈结构的具体分布特征。由上面的证明我们知道，参数是研究可逆T函数圈结构的一个很重要的工具，下面利用参数来进一步分析T函数的圈结构特征。

由定理1知，对 $f(x) \bmod 2^k$ 任一圈结构，其在 $f(x) \bmod 2^{k+1}$ 下的演变情况完全由参数决定。一般地，我们不妨设 $f(x) \bmod 2^k$ 的圈结构图中有 m 个圈，分别记为 $M_1, M_2, \cdots, M_m$，对应的圈长度分别为 $l_1, l_2, \cdots, l_m$，简记为 $1\times l_1+1\times l_2+\cdots+1\times l_m$（表示其状态图中有1个长为 l_1 的圈，1个长为 l_2 的圈，…，1个长为 l_m 的圈）。要考察这些圈在 $f(x) \bmod 2^{k+1}$ 下的演变情况，就必须考察 $\bigoplus_{x\in M_i}\alpha(x), i=1,\cdots,m$ 的取值变化情形。要考察其所有的取值变化情形是非常复杂的，也是很难分析的，因此我们可先考察比较特殊的情形。也就是在 $f(x) \bmod 2^k$ 的圈结构的基础上考察 $f(x) \bmod 2^{k+1}$ 时，对 $f(x) \bmod 2^k$ 的状态图中 m 个圈中的每一个圈的参数求和后结果全相等，即要么全为0，要么全为1的情形，若 $\bigoplus_{x\in M_i}\alpha(x)\equiv 0, i=1,\cdots,m$，则 $f(x) \bmod 2^k$ 的所有圈结构在 $f(x) \bmod 2^{k+1}$ 下就演变为 $2\times l_1+2\times l_2+\cdots+2\times l_m$；若 $\bigoplus_{x\in M_i}\alpha(x)\equiv 1, i=1,\cdots,m$，$f(x) \bmod 2^k$ 的所有圈结构在 $f(x) \bmod 2^{k+1}$ 下就演变为 $1\times 2l_1+1\times 2l_2+\cdots+1\times 2l_m$。

基于上述讨论，我们分析可逆T函数 $f(x) \bmod 2^n$ 的状态图中有 2^{n-t} 个圈，且每个圈的长度均相等的情况，进而给出其判定条件。

定理3 设 $f(x) \bmod 2^n$ 是一个可逆T函数，对任意的 $i<n$，有 $[f(x)]_i=[x]_i\oplus\alpha_i(x)$。设 $f(x) \bmod 2^i$ 的状态图中有 m_i 个圈，分别记为 $M_{i_1}, M_{i_2}, \cdots, M_{i_{m_i}}$，对应的圈长度分别为 $l_{i_1}, l_{i_2}, \cdots, l_{i_m}$，可简记为 $1\times l_{i_1}+1\times l_{i_2}+\cdots+1\times l_{i_m}$。如果对任意的 $i<n$，有 $\bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 0$ 或 $1, j=1,\cdots,m_i$ 且 $\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,n-1\}=t$，则 $f(x) \bmod 2^n$ 的状态图中共有 2^{n-t} 个圈，且每个圈的长度均为 2^t。特别地，当 $t=n$ 时，$f(x)$ 为单圈T函数。

证明：当 $n=1$ 时，若 $t=0$，则 $\alpha_0(0)=0$。此时 $f(x)$ 有 $0\to 0$ 和 $1\to 1$ 两个圈，即此时 $f(x)$ 的状态图可表示为 2×1（即两个长为1的圈）；若 $t=1$，则 $\alpha_0(0)=1$，此时 $f(x)$ 只有一个圈结构 $0\to 1\to 0$，即此时 $f(x)$ 的状态图可表示为 1×2，结论成立。

假设 $n=k(k\geqslant 1)$ 时，结论成立，即若

$$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k-1\}=t$$

则 $f(x) \bmod 2^k$ 的状态图中共有 2^{k-t} 个圈 $M_{k_1}, M_{k_2}, \cdots, M_{k_{2^{k-t}}}$，且每个圈的长度均为 2^t。当 $n=k+1$ 时，题设条件为

$$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k\}=t,$$

根据前 k 个参数的取值可分为两种不同情形进行讨论，即

$$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k-1\}=t-1$$

或 $$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k-1\}=t$$

下面对其分别讨论：

①若

$$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k-1\}=t-1$$

则由 $n=k$ 时的假设可知，此时 $f(x) \bmod 2^k$ 的状态图中共有 2^{k-t+1} 个圈 $M_{k_1}, M_{k_2}, \cdots, M_{k_2{}^{k-t+1}}$，且每个圈的长度均为 2^{t-1}。又由于 $\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k\}=t$，于是可得 $\bigoplus_{x\in M_{k_j}}\alpha_k(x)\equiv 1, j=1,2,\cdots,2^{k-t+1}$，因此由定理1，$f(x) \bmod 2^{k+1}$ 的状态图中有 2^{k-t+1} 个圈，且每个圈的长度为 2^t，即圈结构分布可简记为 $2^{k-t+1}\times 2^t$。此时结论成立。

②若

$$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k-1\}=t$$

则由 $n=k$ 时的假设可知 $f(x) \bmod 2^k$ 的状态图中共有 2^{k-t} 个圈 $M_{k_1}, M_{k_2}, \cdots, M_{k_2{}^{k-t}}$，且每个圈的长度均为 2^t。又由于

$$\#\{\alpha_i \mid \bigoplus_{x\in M_{i_j}}\alpha_i(x)\equiv 1, j=1,\cdots,m_i, i=0,1,\cdots,k\}=t$$

故 $\bigoplus_{x\in M_{k_j}}\alpha_k(x)\equiv 0, j=1,2,\cdots,2^{k-t}$。

因此由定理1，$f(x) \bmod 2^{k+1}$ 状态中的状态图中有 2^{k-t+1} 个圈，且每个圈的长度为 2^t，即圈结构分布可简记为 $2^{k-t+1}\times 2^t$，此时结论也成立。故当 $n=k+1$ 时，结论成立。

因此，$f(x) \bmod 2^n$ 的状态图中共有 2^{n-t} 个圈，且每个圈的长度均为 2^t，即圈结构分布为 $2^{n-t}\times 2^t$。特别地，当 $t=n$ 时，$f(x) \bmod 2^n$ 只有1个周期为 2^n 的圈，即此时 $f(x)$ 是一个单圈T函数。

文献[1]中单圈函数的判定条件：T函数 $f(x)$ 是一个单圈函数当且仅当对任意 $i<n$，有 $[f(x)]_i=[x]_i\oplus\alpha([x]_{0,\cdots,i-1}), \bigoplus_{x=0}^{2^i-1}\alpha(x)=1$ 成立。该判定方法只是定理3的一个特例。

结束语 本文研究了可逆T函数的圈结构，并从理论上证明了可逆T函数的圈结构特征，给出了由可逆T函数 $f(x) \bmod 2^k$ 的圈结构判定 $f(x) \bmod 2^{k+1}$ 圈结构的两种不同判定方法，进一步分析给出了可逆T函数的一种圈结构特征的判定条件，为进一步研究T函数状态图的圈结构特征提供了理论基础。对于任意的可逆T函数来说，其状态图中圈结构的具体分布规律如何，或满足什么样的特定条件可得到其具体圈结构分布特征，都是非常有意义的问题，值得进一步深入研究。

参考文献

[1] Klimov A, Shamir A. Applications of T-functions in Cryptography [D]. Weizmann Institute of Science: Department of Applied Mathematics and Computer Science, 2005

[2] Hong Jin, Lee D H, Yeom Yongjin. A New Class of Single Cycle T-Functions [C]// Fast Software Encryption-FSE'2005. LNCS 3018. Berlin: Springer-Verlag, 2005: 68-82

[3] Klimov A, Shamir A. New Applications of T-Functions in Block Ciphers and Hash Functions [C]// Fast Software Encryption-FSE'2005. LNCS 3018. Berlin: Springer-Verlag, 2005: 18-31

[4] 于静之，张文英. 根据连续 2^{n-1} 个状态写出单圈T函数ANF的方法[J]. 山东大学学报，2007, 42(4): 14-18

[5] 赵璐，温巧燕. 单圈T-函数输出序列的线性复杂度及稳定性[J]. 北京邮电大学学报，2008, 31(4): 62-65