文章编号:2095-6134(2015)06-0721-07

The cardinalities of some certain Hamming constraint sets*

SONG Jia†, CHEN Yufu

(*School of Mathematical Sciences*, *University of Chinese Academy of Sciences*, *Beijing* 101408, *China*)

(Received 5 January 2015; Revised 10 April 2015)

Song J, Chen Y F. The cardinalities of some certain Hamming constraint sets[J]. Journal of University of Chinese Academy of Sciences, 2015,32(6):721-727.

Abstract It is difficult to find Boolean functions used in stream ciphers that can meet all the necessary performance criteria. Recently, two classes of Boolean functions with many good cryptographic properties have been proposed by Tu and Deng based on correctness of a combinatorial conjecture about binary strings distribution (we call it Hamming constraint set). Tu-Deng conjecture has attracted much attention from cryptographers. In this paper we give a new method to obtain the explicit formulas for the cardinalities of some certain Hamming constraint sets, which partially proves Tu-Deng conjecture.

Key words Boolean function; Tu-Deng conjecture; Hamming weight

CLC Number: O15; O29 **Document code**: A **doi**: 10.7523/j.issn.2095-6134.2015.06.001

Hamming 约束集的计数问题

宋 佳, 陈玉福

(中国科学院大学数学科学学院, 北京 101408)

摘 要 构造一个应用于流密码并且具有良好性质的布尔函数是一个非常困难的问题. 最近, Tu 和 Deng 基于一个关于二进制串分布(我们称之为 Hamming 约束集)的组合猜想的正确性, 构造了两类具有良好性质的布尔函数. 越来越多的学者致力于 Tu-Deng 猜想的证明. 本文用一种新方法给出某些 Hamming 约束集的计数公式, 从而部分地证明 Tu-Deng 猜想.

关键词 布尔函数;Tu-Deng 猜想;Hamming 重量

Boolean functions hold great importance in the design of cryptographic systems. For example, in a basic LFSR (linear feedback shift register)-based stream cipher, a Boolean function is used to combine the outputs of the register to generate a nonlinear stream of bits for the encryption[1]. Based on a long-term research, people have found that Boolean functions used in a stream cipher should be provided with some good cryptographic properties, such as bentness, balancedness, a high algebraic

* Supported by the National Natural Science Foundation of China (11271363)

†Corresponding author, E-mail: songjia10@mails.ucas.ac.cn

degree, and high nonlinearity[2-5]. For instance, in order to resist against linear cryptographic attack[6], Boolean functions must have a high nonlinearity, and in order to resist against algebraic attack[7-8] Boolean functions need a high algebraic immunity[9]. That is to say, the research work on cryptographic properties of Boolean functions is closely interconnected with the security of cryptographic systems.

However, it is difficult to find Boolean functions used in stream ciphers that can meet all the necessary criteria, which implies that the research of Boolean functions lags behind the research of cryptanalysis.

More recently, two classes of Boolean functions have been proposed by Tu and Deng[10-11] based on correctness of the following combinatorial conjecture about binary strings distribution.

Conjecture Suppose m and t are positive integers, $m > 1$ and $1 \leqslant t < 2^m - 1$. Let $S_t^m(<m) = \{(a,b) \mid a,b \in \mathbb{Z}, 0 \leqslant a,b < 2^m - 1, a + b \equiv t \bmod (2^m - 1), w(a) + w(b) < m\}$. Then $|S_t^m(<m)| \leqslant 2^{m-1}$.

One class of the functions are bent functions with maximum algebraic immunity[10,12], and the other class of the fumctions have good properties such as balancedness, maximum algebraic immunity, optimal algebraic degree, and good nonlinearity.

The Boolean functions which are constructed based on Tu-Deng conjecture have many good cryptographic properties and Tu-Deng conjecture has attracted a great deal of attention among cryptographers[11,13]. A complete proof of Tu-Deng conjecture is meaningful and significant, but it is also very difficult. More and more researchers have paid attention to the proof of Tu-Deng conjecture.

Tu and Deng[11] assumed the correctness of the conjecture and checked it for $m \leqslant 29$ by developing a transfer-matrix algorithm. Tu also investigated Tu-Deng conjecture theoretically and experimentally and obtained some general results in his doctoral dissertation[14]. Cusick et al.[15] proved the correctness of Tu-Deng conjecture under some special conditions such as $w(t) = 1,2$, and $w(t') \leqslant 2$ if t' is even, and $w(t') \leqslant 4$ if t' is odd, here $t' = 2^m - t$. They predicted that it was a challenge to obtain a general counting. Cohen and Flori[16-17] gave the proofs of a variety of Tu-Deng conjecture. Huang et al.[18] gave the proof of Tu-Deng conjecture under a few conditions by analyzing the Hamming weight of the parameter t in $S_t^m(<m)$.

In this paper, we present the explicit formulas for the cardinalities of some certain Hamming constraint sets with a new method. Based on our results, we partially prove the correctness of Tu-Deng conjecture.

1 Preliminaries

1.1 The binary expression of the nonnegative integer

A nonnegative integer a can be written as $a_{m-1}2^{m-1} + \cdots + a_1 2 + a_0$ (m is a positive integer), which is called the binary expression of a. a_i (=0 or 1) is called the ith bit value. We can simply write $a = a_{m-1}\cdots a_1 a_0$. We call it the m-bit binary expression of a when $a_{m-1} = 1$.

The Hamming weight of a, which we write as $w(a)$, is the number of 1's in the binary expression of a. Let $\tau_1(a)$ express the minimum i satisfying $a_i = 1$ when $a > 0$. Let $\tau_0(a)$ express the minimum j satisfying $a_j = 0$ when there is at least one zero among $a_{m-1}, \cdots, a_1, a_0$. We extend τ_1 and τ_0 by setting $\tau_1(\overbrace{0\cdots0}^{q}) = q$ and $\tau_0(\overbrace{1\cdots1}^{q}) = q$.

So when $a > 0$,

$\tau_0(a) = 0, \tau_1(a) > 0 \Leftrightarrow a$ is even,

$\tau_0(a) > 0, \tau_1(a) = 0 \Leftrightarrow a$ is odd.

Set $\bar{a}_i = 1 - a_i$. We call $\bar{a}_{m-1}\cdots\bar{a}_1\bar{a}_0$ the conjugation of a, which we write as $\bar{a}$. It is easy to see that $\bar{a} = 2^m - 1 - a$ and $a \equiv c \bmod (2^m - 1) \Rightarrow \bar{a} \equiv \bar{c} \bmod (2^m - 1)$.

Let m and t be positive integers. Suppose $m > 1$ and $1 \leqslant t < 2^m - 1$. The m-derivative of t is the odd integer $f(t)$ such that $2^m - 1 - t = 2^i f(t)$. It is easy to see $f(t) = 2^m - 1 - t$ when t is even and $f(t) \leqslant 2^{m-1} - 1$ when t is odd.

Let m and t be positive integers. Suppose $m > 1$ and $1 \leqslant t < 2^m - 1$. The m-integral of an odd integer t is the integer l ($0 < l < 2^m - 1$) such that $f(l) = t$. That is to say, $l = 2^m - 1 - 2^i t$, where $0 \leqslant i \leqslant 1 + \log_2(2^m - 1) - \log_2 t$.

Remark From the above definition, we can see that the m-integral l of an odd integer t is not unique. But for a fixed m, the cardinalities of $S_l^m(=m)$ (or $S_l^m(<m)$ or $S_l^m(>m)$) are the same. So we do not request the uniqueness of the m-integral of an odd integer in this paper.

1.2 The properties of Hamming weight

Lemma 1.1 Suppose a and m are positive integers. Then

1) $w(2^m \cdot a) = w(a)$;

2) $w(a-1) = w(a) + \tau_1(a) - 1$;

3) $w(a+1) = w(a) - \tau_0(a) + 1$;

4) If $1 \leqslant a \leqslant 2^m - 1$, then $w(2^m - 1 - a) = m - w(a)$, $w(2^m + a) = 1 + w(a)$;

5) If $1 \leqslant a \leqslant 2^m - 1$, then $w(2^m - 1 + a) = w(a) + \tau_1(a)$;

6) In the binary expression, the following properties are found:

$\tau_1(a_{m-1}\cdots a_{k+1}1\,a_{k-1}\cdots a_1\,a_0) = \tau_1(a_{k-1}\cdots a_1\,a_0)$,

$\tau_0(b_{m-1}\cdots b_{k+1}0\,b_{k-1}\cdots b_1\,b_0) = \tau_0(b_{k-1}\cdots b_1\,b_0)$.

1.3 Hamming constraint set

Let m and t be positive integers. Suppose $m > 1$, $1 \leqslant t < 2^m - 1$ and k is a nonnegative integer. We introduce the following notations:

$S_t^m = \{(a,b) \mid a,b \in \mathbb{Z}, 0 \leqslant a,b < 2^m - 1, a + b \equiv t \bmod (2^m - 1)\}$,

$S_t^m(\cdot k) = \{(a,b) \in S_t^m \mid w(a) + w(b) \cdot k\}$,

where "$\cdot$" represents the relation symbols $<$, $=$, $>$, $\leqslant$, $\geqslant$. We call $S_t^m(\cdot k)$ the Hamming constraint set, and we are most interested in the set $S_t^m(<m)$.

Notice that $b = t - a$ when $a \leqslant t$ and $b = 2^m - 1 - a + t$ when $a > t$. We can divide S_t^m into two parts:

$S_{t,1}^m: (0,t), (1,t-1), \cdots, (t,0)$;

$S_{t,2}^m: (t+1, 2^m - 2), (t+2, 2^m - 3), \cdots, (2^m - 2, t+1)$.

So we have

$|S_t^m| = 2^m - 1$,

$|S_{t,1}^m| = t + 1$,

$|S_{t,2}^m| = 2^m - 2 - t$.

Lemma 1.2[17] $|S_t^m(\cdot k)| = |S_{2t}^m(\cdot k)|$, where $m > 1$ and $2 \leqslant 2t < 2^m - 1$ and "$\cdot$" represents the relation symbols $<$, $=$, $>$, $\leqslant$, $\geqslant$.

Lemma 1.3 $|S_t^m(=m)| = |S_{\bar{t}}^m(=m)|$ and $|S_t^m(<m)| = |S_{\bar{t}}^m(>m)| + 2$, where $m > 1$ and $1 \leqslant t < 2^m - 1$.

Proof If $(a,b) \in S_t^m(=m)$, then $w(a) + w(b) = m$ with $a \neq 0$ and $b \neq 0$. So $w(2^m - 1 - a) + w(2^m - 1 - b) = m - w(a) + m - w(b) = m$ and $2^m - 1 - a + 2^m - 1 - b \equiv 2^m - 1 - t \bmod (2^m - 1) \Rightarrow (2^m - 1 - a, 2^m - 1 - b) \in S_{\bar{t}}^m(=m)$.

We can set up an injective mapping $\varphi: (a,b) \to (\bar{a},\bar{b})$ from $S_t^m(=m)$ to $S_{\bar{t}}^m(=m)$. So $|S_t^m(=m)| \leqslant |S_{\bar{t}}^m(=m)|$. Since $\bar{\bar{t}} = t$, we have $|S_t^m(=m)| \leqslant |S_{\bar{t}}^m(=m)|$. Thus $|S_t^m(=m)| = |S_{\bar{t}}^m(=m)|$.

If $(a,b) \in S_t^m(<m)$, then $a + b \equiv t \bmod (2^m - 1)$ and $w(a) + w(b) < m$. So $w(2^m - 1 - a) + w(2^m - 1 - b) = m - w(a) + m - w(b) > m$ and $2^m - 1 - a + 2^m - 1 - b \equiv 2^m - 1 - t \bmod (2^m - 1)$. This means $(2^m - 1 - a, 2^m - 1 - b) \in S_{\bar{t}}^m(>m)$ except $(a,b) = (0,t), (t,0)$.

We set up an injective mapping $\varphi: (a,b) \to (2^m - 1 - a, 2^m - 1 - b)$ from $S_t^m(<m) \setminus \{(0,t), (t,0)\}$ to $S_{\bar{t}}^m(>m)$. Thus $|S_t^m(<m)| - 2 \leqslant |S_{\bar{t}}^m(>m)|$.

If $(\bar{a},\bar{b}) \in S_{\bar{t}}^m(>m)$, then $w(\bar{a}) + w(\bar{b}) > m$ and $\bar{a} + \bar{b} \equiv \bar{t} \bmod (2^m - 1)$ with $\bar{a} \neq 0$ and $\bar{b} \neq 0$. So we have $w(2^m - 1 - \bar{a}) + w(2^m - 1 - \bar{b}) = m - w(\bar{a}) + m - w(\bar{b}) < 2m - m = m$ and $2^m - 1 - \bar{a} + 2^m - 1 - \bar{b} \equiv 2^m - 1 + 2^m - 1 - (\bar{a} + \bar{b}) \equiv t \bmod (2^m - 1)$. Since $\bar{a}, \bar{b} < 2^m - 1$, we have $(2^m - 1 - \bar{a}, 2^m - 1 - \bar{b}) \in S_t^m(<m) \setminus \{(0,t), (t,0)\}$.

We set up an injective mapping $\psi: (\bar{a},\bar{b}) \to (a,b)$ from $S_{\bar{t}}^m(>m)$ to $S_t^m(<m) \setminus \{(0,t), (t,0)\}$. Thus $|S_{\bar{t}}^m(>m)| \leqslant |S_t^m(<m)| - 2$. This completes our proof. □

Based on the above lemmas, we have the following lemma:

Lemma 1.4 Let $m > 1$ and $1 \leqslant t < 2^m - 1$. Then

$$|S_t^m(=m)| = |S_{f(t)}^m(=m)|,$$
$$|S_t^m(<m)| = |S_{f(t)}^m(>m)| + 2,$$
$$|S_{f(t)}^m(<m)| = |S_t^m(>m)| + 2.$$

2 The cardinalities of some Hamming constraint sets

Theorem 2.1 Suppose m is a positive integer. If $m \geqslant 4$, then

$$|S_3^m(=m)| = 5 \cdot 2^{m-4}.$$

Proof If $m \geqslant 4$ and $(a,b) \in S_3^m(=m)$, then $0 \leqslant a,b < 2^m - 1$, $a + b \equiv 3 \bmod(2^m - 1)$, and $w(a) + w(b) = m$. First we know $a > 3$. This is because if $a \leqslant 3$, we have $b = 3 - a$ and $w(a) + w(b) \leqslant 2 < m$. From $a > 3$ and $a + b \equiv 3 \bmod(2^m - 1)$, we deduce $b = 2^m - 1 - (a - 3)$. Since

$$\begin{aligned} w(a) + w(b) &= w(a) + w(2^m - 1 - (a-3)) \\ &= w(a) + m - w(a-3) \\ &= m, \end{aligned}$$

we have $w(a) = w(a-3)$.

$$\begin{aligned} w(a-3) &= w(a-2) + \tau_1(a-2) - 1 \\ &= w(a-1) + \tau_1(a-1) + \tau_1(a-2) - 2 \\ &= w(a) + \tau_1(a) + \tau_1(a-1) + \tau_1(a-2) - 3. \end{aligned}$$

So $w(a) = w(a-3)$ indicates $\tau_1(a) + \tau_1(a-1) + \tau_1(a-2) = 3$. We solve this problem in two cases:

1) Case 1: a is even.

In this case, we have $\tau_1(a) > 0$, $\tau_1(a-1) = 0$, $\tau_1(a-2) > 0$, $\tau_1(a) + \tau_1(a-2) = 3$. So we have $\tau_1(a) = 1$, $\tau_1(a-2) = 2$ or $\tau_1(a) = 2$, $\tau_1(a-2) = 1$.

1.1) When $\tau_1(a) = 1$ and $\tau_1(a-2) = 2$, the binary expression of a must have the form of $a_{m-1}\cdots a_3 110$, which means the number of a's satisfying the conditions $\tau_1(a) = 1$ and $\tau_1(a-2) = 2$ is 2^{m-3}.

1.2) When $\tau_1(a) = 2$ and $\tau_1(a-2) = 1$, the binary expression of a must have the form of $a_{m-1}\cdots a_3 100$, which means the number of a's satisfying the conditions $\tau_1(a) = 2$ and $\tau_1(a-2) = 1$ is 2^{m-3}.

2) Case 2: a is odd.

In this case, we have $\tau_1(a) = 0$, $\tau_1(a-1) > 0$, $\tau_1(a-2) = 0$, $\tau_1(a-1) = 3$. So the binary expression of a must have the form of $a_{m-1}\cdots a_4 1001$, which means the number of odd a's is 2^{m-4}.

Based on the above deduction, the cardinality of $S_3^m(=m)$ is $2 \cdot 2^{m-3} + 2^{m-4} = 5 \cdot 2^{m-4}$ when $m \geqslant 4$. □

Theorem 2.2 Suppose m is a positive integer. If $m \geqslant 4$, then

$$|S_3^m(\geqslant m)| = 7 \cdot 2^{m-4} + 2^{m-2} - 2.$$

Proof If $m = 4$, it is easy to see $S_3^m(\geqslant m) = \{(4,14),(5,13),(6,12),(7,11),(9,9),(11,7),(12,6),(13,5),(14,4)\}$. So $|S_3^m(\geqslant m)| = 9$.

If $m > 4$ and $(a,b) \in S_3^m(\geqslant m)$, then $0 \leqslant a, b < 2^m - 1$, $a + b \equiv 3 \bmod(2^m - 1)$, and $w(a) + w(b) \geqslant m$. First we know $a > 3$. This is because we have $b = 3 - a$ and $w(a) + w(b) \leqslant 2 < m$ if $a \leqslant 3$. From $a > 3$ and $a + b \equiv 3 \bmod(2^m - 1)$, we deduce $b = 2^m - 1 - (a - 3)$. Since

$$\begin{aligned} w(a) + w(b) &= w(a) + w(2^m - 1 - (a-3)) \\ &= w(a) + m - w(a-3) \\ &\geqslant m, \end{aligned}$$

we have $w(a) \geqslant w(a-3)$.

$$\begin{aligned} w(a-3) &= w(a-2) + \tau_1(a-2) - 1 \\ &= w(a-1) + \tau_1(a-1) + \tau_1(a-2) - 2 \\ &= w(a) + \tau_1(a) + \tau_1(a-1) + \tau_1(a-2) - 3. \end{aligned}$$

So $w(a) \geqslant w(a-3)$ indicates $\tau_1(a) + \tau_1(a-1) + \tau_1(a-2) \leqslant 3$.

If $\tau_1(a) \geqslant 3$, then $\tau_1(a) + \tau_1(a-1) + \tau_1(a-2) \geqslant 3 + 1 = 4$. So $\tau_1(a) = 0$ or 1 or 2 (see below).

1) $\tau_1(a) = 0$.

We know a and $a - 2$ are odd, so we have $\tau_1(a-1) \leqslant 3$.

Suppose the binary expression of a is $a_{m-1}\cdots a_3 a_2 a_1 1$. Then $a - 1 = a_{m-1}\cdots a_3 a_2 a_1 0$. Since $\tau_1(a-1) \leqslant 3$, there is at least one 1 among a_3, a_2, a_1. Thus the number of a's satisfying the condition $\tau_1(a) = 0$ is $2^{m-4} \cdot (2^3 - 1) - 2$. Here we remove the cases $a = 1\cdots 1$ and $a = 0\cdots 011 = 3$.

2) $\tau_1(a) = 1$.

Suppose the binary expression of a is $a_{m-1}\cdots a_3\, a_2 10$. Then $a - 1 = a_{m-1}\cdots a_3 a_2 01$ and $a - 2 = a_{m-1}\cdots a_3\, a_2 00$. So $\tau_1(a) + \tau_1(a-1) + \tau_1(a-2)$

$= 1 + \tau_1(a-2) \leqslant 3 \Rightarrow \tau_1(a-2) \leqslant 2$. Then we have $a_2 = 1$. Thus the number of a's satisfying the condition $\tau_1(a) = 1$ is 2^{m-3}.

3) $\tau_1(a) = 2$.

Suppose the binary expression of a is $a_{m-1}\cdots a_3 100$. Then $a-1 = a_{m-1}\cdots a_3 011$ and $a-2 = a_{m-1}\cdots a_3 010$. So $\tau_1(a)+\tau_1(a-1)+\tau_1(a-2) = 2+0+1 = 3$. Thus the number of a's satisfying the condition $\tau_1(a) = 2$ is 2^{m-3}.

Based on the above deduction, when $m > 4$, the cardinality of $S_3^m(\geqslant m)$ is

$$2^{m-4}\cdot(2^3-1) - 2 + 2\cdot 2^{m-3} = 7\cdot 2^{m-4} + 2^{m-2} - 2. \quad \square$$

Theorem 2.3 Suppose m is a positive integer. If $m \geqslant 4$, then $|S_3^m(<m)| = 5\cdot 2^{m-4} + 1$.

Proof Suppose $m \geqslant 4$. Since $|S_3^m| = 2^m - 1$, we have

$$\begin{aligned}|S_3^m(<m)| &= 2^m - 1 - |S_3^m(\geqslant m)| \\ &= 2^m - 1 - 7\cdot 2^{m-4} - 2^{m-2} + 2 \\ &= 5\cdot 2^{m-4} + 1. \quad \square\end{aligned}$$

Suppose $m \geqslant 4$. Since $f(3) = 2^{m-2} - 1$ and the m-integral of 3 is $2^m - 1 - 3\cdot 2^i$ ($0 \leqslant i \leqslant 1 + \log_2(2^m-1) - \log_2 3$), we have the following corollary.

Corollary 2.1 Suppose m and i are positive integers. If $m \geqslant 4$ and $0 \leqslant i \leqslant 1 + \log_2(2^m-1) - \log_2 3$, then

$$|S^m_{2^{m-2}-1}(=m)| = |S^m_{2^{m-1}-3\cdot 2^i}(=m)| = 5\cdot 2^{m-4},$$
$$|S^m_{2^{m-2}-1}(>m)| = |S^m_{2^{m-1}-3\cdot 2^i}(>m)| = 5\cdot 2^{m-4} - 1,$$
$$|S^m_{2^{m-2}-1}(<m)| = |S^m_{2^{m-1}-3\cdot 2^i}(<m)| = 2^{m-2} + 2^{m-3}.$$

Theorem 2.4 Suppose m is a positive integer. Then

$$|S_5^m(=m)| = \begin{cases} 2, & \text{if } m = 3, \\ 2^{m-3}, & \text{if } m \geqslant 4. \end{cases}$$

Proof If $m = 3$, it is easy to see $S_5^3(=3) = \{(3,2),(2,3)\}$. So $|S_5^3(=3)| = 2$.

If $m \geqslant 4$ and $(a,b) \in S_5^m(=m)$, then $0 \leqslant a, b < 2^m - 1$, $a + b \equiv 5 \bmod(2^m-1)$, and $w(a) + w(b) = m$. First we know $a > 5$. This is because we have $b = 5 - a$ and $w(a) + w(b) < 4 \leqslant m$ if $a \leqslant 5$. From $a > 5$ and $a + b \equiv 5 \bmod(2^m-1)$, we deduce $b = 2^m - 1 - (a-5)$. Since

$$\begin{aligned}w(a) + w(b) &= w(a) + w(2^m - 1 - (a-5)) \\ &= w(a) + m - w(a-5) \\ &= m,\end{aligned}$$

we have $w(a) = w(a-5)$.

$$\begin{aligned}w(a-5) &= w(a-4) + \tau_1(a-4) - 1 \\ &= w(a-3) + \tau_1(a-3) + \tau_1(a-4) - 2 \\ &= w(a-2) + \tau_1(a-2) + \tau_1(a-3) + \tau_1(a-4) - 3 \\ &= w(a-1) + \tau_1(a-1) + \tau_1(a-2) + \tau_1(a-3) + \tau_1(a-4) - 4 \\ &= w(a) + \tau_1(a) + \tau_1(a-1) + \tau_1(a-2) + \tau_1(a-3) + \tau_1(a-4) - 5.\end{aligned}$$

So $w(a) = w(a-5)$ indicates $\tau_1(a)+\tau_1(a-1)+\tau_1(a-2)+\tau_1(a-3)+\tau_1(a-4) = 5$.

If $\tau_1(a) \geqslant 2$, suppose the binary expression of a is $a_{m-1}\cdots a_3\, a_2 00$. Then $a-2 = a_{m-1}\cdots \bar{a}_2 10$ and $a-4 = a_{m-1}\cdots \bar{a}_2 00$. So $\tau_1(a)+\tau_1(a-1)+\tau_1(a-2)+\tau_1(a-3)+\tau_1(a-4) > 2+1+2 = 5$. This is because one of $\tau_1(a)$ and $\tau_1(a-4)$ is larger than 2. Thus $\tau_1(a) = 1$ or 0.

1) When $\tau_1(a) = 1$, a is even and $\tau_1(a-1) = \tau_1(a-3) = 0$.

When $\tau_1(a) = 1$ and $\tau_1(a-2)+\tau_1(a-4) = 4$, $\tau_1(a) = 1$ indicates $\tau_1(a-2) \geqslant 2$. If $\tau_1(a) = 1$ and $\tau_1(a-2) = 2$, then $\tau_1(a-4) = 1$, which contradicts to $\tau_1(a-2)+\tau_1(a-4) = 4$. So only $\tau_1(a) = 1, \tau_1(a-2) = 3$, and $\tau_1(a-4) = 1$ can satisfy the conditions. Thus the binary expression of a must have the form of $a_{m-1}\cdots a_4 1010$, which means the number of a's satisfying the conditions $\tau_1(a) = 1$ and $\tau_1(a-2)+\tau_1(a-4) = 4$ is 2^{m-4}.

2) When $\tau_1(a) = 0$, a is odd.

In this case, we have $\tau_1(a) = \tau_1(a-2) = \tau_1(a-4) = 0$, $\tau_1(a-1) > 0$, $\tau_1(a-3) > 0$, and $\tau_1(a-1)+\tau_1(a-3) = 5$. Since $\tau_1(a-1) = 2$ or 3 indicates $\tau_1(a-3) = 1$, which contradicts to $\tau_1(a-1)+\tau_1(a-3) = 5$, we have $\tau_1(a-1) = 1$, $\tau_1(a-3) = 4$ or $\tau_1(a-1) = 4, \tau_1(a-3) = 1$.

2.1) When $\tau_1(a-1) = 1$ and $\tau_1(a-3) = 4$, the binary expression of a must have the form of $a_{m-1}\cdots a_5 10011$, which means the number of a's satisfying the conditions $\tau_1(a-1) = 1$ and $\tau_1(a-3) = 4$ is 2^{m-5}.

2.2) When $\tau_1(a-1) = 4$ and $\tau_1(a-3) = 1$, the

binary expression of a must have the form of $a_{m-1}\cdots a_5 10001$, which means the number of a's satisfying the conditions $\tau_1(a-1)=4$ and $\tau_1(a-3)=1$ is 2^{m-5}.

Based on the above deduction, the cardinality of $S_5^m(=m)$ is $2^{m-4}+2\cdot 2^{m-5}=2^{m-3}$ when $m\geqslant 4$. □

Theorem 2.5 Suppose m is a positive integer. If $m\geqslant 3$, then $|S_5^m(\geqslant m)|=2^{m-1}+2^{m-3}-2$.

Proof If $m=3$, it is easy to see $S_5^m(\geqslant m)=\{(2,3),(3,2),(6,6)\}$. So $|S_5^m(\geqslant m)|=3$.

If $m>3$ and $(a,b)\in S_5^m(\geqslant m)$, then $0\leqslant a, b<2^m-1$, $a+b\equiv 5 \bmod(2^m-1)$, and $w(a)+w(b)\geqslant m$. First we know $a>5$. This is because we have $b=5-a$ and $w(a)+w(b)<4\leqslant m$ if $a\leqslant 5$. From $a>5$ and $a+b\equiv 5 \bmod(2^m-1)$, we deduce $b=2^m-1-(a-5)$. Since

$$\begin{aligned} w(a)+w(b) &= w(a)+w(2^m-1-(a-5)) \\ &= w(a)+m-w(a-5) \\ &\geqslant m, \end{aligned}$$

we have $w(a)\geqslant w(a-5)$.

$$\begin{aligned} w(a-5) &= w(a-4)+\tau_1(a-4)-1 \\ &= w(a-3)+\tau_1(a-3)+\tau_1(a-4)-2 \\ &= w(a-2)+\tau_1(a-2)+\tau_1(a-3)+\\ &\quad \tau_1(a-4)-3 \\ &= w(a-1)+\tau_1(a-1)+\tau_1(a-2)+\\ &\quad \tau_1(a-3)+\tau_1(a-4)-4 \\ &= w(a)+\tau_1(a)+\tau_1(a-1)+\tau_1(a-\\ &\quad 2)+\tau_1(a-3)+\tau_1(a-4)-5. \end{aligned}$$

So $w(a)\geqslant w(a-5)$ indicates $\tau_1(a)+\tau_1(a-1)+\tau_1(a-2)+\tau_1(a-3)+\tau_1(a-4)\leqslant 5$.

If $\tau_1(a)\geqslant 2$, we suppose the binary expression of a is $a_{m-1}\cdots a_3 a_2 00$. Then $a-2=a_{m-1}\cdots\bar{a}_2 10$ and $a-4=a_{m-1}\cdots\bar{a}_2 00$. So $\tau_1(a)+\tau_1(a-1)+\tau_1(a-2)+\tau_1(a-3)+\tau_1(a-4)>2+1+2=5$. This is because one of $\tau_1(a)$ and $\tau_1(a-4)$ is larger than 2. Thus $\tau_1(a)=1$ or 0.

1) When $\tau_1(a)=1$, we suppose the binary expression of a is $a_{m-1}\cdots a_3 a_2 10$. Then we have

$$\begin{aligned} a-1 &= a_{m-1}\cdots a_3 a_2 01, \\ a-2 &= a_{m-1}\cdots a_3 a_2 00, \\ a-3 &= a_{m-1}\cdots b_3\,\bar{a}_2 11, \\ a-4 &= a_{m-1}\cdots b_3\,\bar{a}_2 10, \end{aligned}$$

where $b_3=a_3$ or $b_3=\bar{a}_3$.

1.1) If $a_2=1$, the number of a's satisfying the condition $\tau_1(a)=1$ is 2^{m-3}.

1.2) If $a_2=0$, then a_3 must be 1. Thus the number of a's satisfying the condition $\tau_1(a)=1$ is 2^{m-4}.

2) When $\tau_1(a)=0$, a is odd. Suppose the binary expression of a is $a_{m-1}\cdots a_4 a_3 a_2 a_1 1$.

2.1) If $a_1=0$, then we have

$$\begin{aligned} a-1 &= a_{m-1}\cdots a_4 a_3 a_2 00, \\ a-2 &= a_{m-1}\cdots b_4 b_3\,\bar{a}_2 11, \\ a-3 &= a_{m-1}\cdots b_4 b_3\,\bar{a}_2 10, \\ a-4 &= a_{m-1}\cdots b_4 b_3\,\bar{a}_2 01, \end{aligned}$$

where $b_i=a_i$ or $b_i=\bar{a}_i$.

There is at least one 1 among a_2, a_3 and a_4. Thus the number of a's in this case is $2^{m-5}\cdot(2^3-1)-1$. Here we remove the case $a=0\cdots 0101=5$.

2.2) If $a_1=1$, then we have

$$\begin{aligned} a-1 &= a_{m-1}\cdots a_4\, a_3\, a_2 10, \\ a-2 &= a_{m-1}\cdots a_4\, a_3\, a_2 01, \\ a-3 &= a_{m-1}\cdots a_4\, a_3\, a_2 00, \\ a-4 &= a_{m-1}\cdots b_4\, b_3\,\bar{a}_2 11, \end{aligned}$$

where $b_i=a_i$ or $b_i=\bar{a}_i$.

There is at least one 1 among a_2, a_3 and a_4. Thus the number of a's in this case is $2^{m-5}\cdot(2^3-1)-1$. Here we remove the case $a=1\cdots 1$.

Based on the above deduction, when $m\geqslant 4$, the cardinality of $S_5^m(\geqslant m)$ is

$$2^{m-3}+2^{m-4}+2^{m-5}\cdot(2^3-1)-1+2^{m-5}\cdot(2^3-1)-1=2^{m-1}+2^{m-3}-2.$$ □

Theorem 2.6 Suppose m is a positive integer. If $m\geqslant 3$, then $|S_5^m(<m)|=2^{m-1}-2^{m-3}+1$.

Proof When $m\geqslant 3$, since $|S_5^m|=2^m-1$, we have

$$\begin{aligned} |S_5^m(<m)| &= 2^m-1-|S_5^m(\geqslant m)| \\ &= 2^m-1-2^{m-1}-2^{m-3}+2 \\ &= 2^{m-1}-2^{m-3}+1. \end{aligned}$$ □

Suppose $m\geqslant 4$. Since $f(5)=2^{m-1}-3$, $f^2(5)=2^{m-2}+1$, $f^3(5)=3\cdot 2^{m-3}-1$ and the m-integral of 5 is $2^m-1-5\cdot 2^i$ $(0\leqslant i\leqslant 1+\log_2(2^m-1)-\log_2 5)$, we have the following corollaries.

Corollary 2.2　Suppose m and i are positive integers. If $m \geqslant 4$ and $0 \leqslant i \leqslant 1 + \log_2(2^m - 1) - \log_2 5$, then

$$|S^m_{2^{m-1}-3}(=m)| = |S^m_{2^{m-2}+1}(=m)|$$
$$= |S^m_{3\cdot 2^{m-3}-1}(=m)| = |S^m_{2^m-1-5\cdot 2^i}(=m)| = 2^{m-3}.$$

Corollary 2.3　Suppose m and i are positive integers. If $m \geqslant 4$ and $0 \leqslant i \leqslant 1 + \log_2(2^m - 1) - \log_2 5$, then

$$|S^m_{2^{m-1}-3}(>m)| = |S^m_{3\cdot 2^{m-3}-1}(>m)|$$
$$= |S^m_{2^m-1-5\cdot 2^i}(>m)| = 2^{m-1} - 2^{m-3} - 1,$$
$$|S^m_{2^{m-1}-3}(<m)| = |S^m_{3\cdot 2^{m-3}-1}(<m)|$$
$$= |S^m_{2^m-1-5\cdot 2^i}(<m)| = 2^{m-1},$$
$$|S^m_{2^{m-2}+1}(>m)| = 2^{m-1} - 2,$$
$$|S^m_{2^{m-2}+1}(<m)| = 2^{m-1} - 2^{m-3} + 1.$$

Using the above method, we can also calculate the cardinalities of $S^m_7(=m)$, $S^m_7(\geqslant m)$, and $S^m_7(<m)$.

Corollary 2.4　Suppose m is a positive integer. If $m \geqslant 7$, then

$$|S^m_7(=m)| = 21\cdot 2^{m-6},$$
$$|S^m_7(\geqslant m)| = 2^m - 21\cdot 2^{m-6} - 2,$$
$$|S^m_7(<m)| = 21\cdot 2^{m-6} + 1.$$

3　Conclusion

In summary, Boolean functions based on Tu – Deng conjecture hold a great deal of good cryptographic properties, but it is a challenge to give a complete proof of Tu-Deng conjecture. In this paper, we present the explicit formulas for the cardinalities of some certain Hamming constraint sets using a new method. The results partially prove the correctness of Tu-Deng conjecture.

References

[1] Golomb S W, Gong G. Signal design for good correlation for wireless communication, cryptography and radar[M]. New York: Cambridge University Press, 2005.

[2] Carlet C, Ding C S. Highly nonlinear mappings[J]. Journal of Complexity, 2004, 20(2/3): 205-244.

[3] Pei D Y, Qin W L. The correlation of a Boolean function with its variables [C] // Roy B, Okamoto E. Progress in Cryptology-INDOCRYPT 2000. Springer, Berlin Heidelberg, 2000, 1977: 1-8.

[4] Siegenthaler T. Correlation immunity of non-linear combining functions for cryptographic applications [J]. IEEE Transaction on Information Theory, 1984, 30: 776-780.

[5] Katz J, Lindell Y. Introduction to modern cryptography[M]. Washington DC: CRC PRESS, 2007.

[6] Matsui M. Linear cryptanalysis method for DES cipher[C] // Helleseth T. Advances in Cryptology-EUROCRYPT 1993. Springer, Berlin Heidelberg, 1994, 765: 386-397.

[7] Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback[C] // Biham E. Advances in Cryptology-EUROCRYPT 2003. Springer, Berlin Heidelberg, 2003, 2656: 345-359.

[8] Courtois N T. Fast algebraic attacks on stream ciphers with linear feedback [C] // Boneh D. Advances inCryptology-CRYPTO 2003. Springer, Berlin Heidelberg, 2003, 2729: 176-194.

[9] Xie Y H, Hu L. A matrix construction of Boolean functions with maximum algebraic immunity [J]. Journal of Systems Science and Complexity, 2012, 25: 792-801.

[10] Tu Z R, Deng Y P. A conjucture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity [J]. Designs, Codes and Cryptography, 2011, 60: 1-14.

[11] Tu Z R, Deng Y P. Boolean functions optimizing most of the cryptographic criteria [J]. Discrete Applied Mathematics, 2012, 160: 427-435.

[12] Langevin P, Leander G. Monomial bent functions and Stickelberger's theorem [J]. Finite Fields and Their Appilications, 2008, 14: 727-742.

[13] Carlet C, Feng K Q. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity [C] // Pieprzyk J. Advances in Cryptology-ASIACRYPT 2008. Springer, Berlin Heidelberg, 2008, 5350: 425-440.

[14] Tu Z R. Design and analysis of Boolean functions under algebraic attacks[D]. Beijing: Academy of Mathematics and Systems Science, Chinese Academy of Sciences, 2009 (in Chinese).

[15] Cusick T W, Li Y, Stanica P. On a combinatorial conjecture [J/OL]. [2014-12-20]. Crypology ePrint Archive. http://eprint.iacr.org/2009/554.pdf.

[16] Flori J P, Randriam H, Cohen G, et al. On a conjecture about binary strings distribution [C] // Carlet C, Pott A. Sequences and Their Applications-SETA 2010. Springer, Berlin Heidelberg, 2010, 6338: 346-358.

[17] Cohen G, Flori J P. On a general combinatorial conjecture invovling addition mod $2^k - 1$ [J/OL]. [2014-12-20]. Cryptology ePrint Archive. http://eprint.iacr.org/2011/400.pdf.

[18] Huang K, Li C, Fu S J. Note on the Tu-Deng conjecture[J]. Computer Science, 2012, 39: 6-9 (in Chinese).