ON A COMBINATORIAL CONJECTURE OF TU AND DENG

Guixin Deng
School of Mathematical Sciences, Guangxi Teachers Education University, Nanning, P.R.China
dengguixin@live.com

Pingzhi Yuan
School of Mathematics, South China Normal University, Guangzhou, P.R.China
mcsypz@mail.sysu.edu.cn

Received: 12/22/11, Revised: 4/2/12, Accepted: 8/19/12, Published: 9/3/12

Abstract

Recently, Tu and Deng obtained two classes of Boolean functions with nice properties based on a combinatorial conjecture about binary strings. In this paper, using different approaches, we prove this conjecture is true in several cases.

1. Introduction

Let x be a nonnegative integer. If the binary expansion of x is $x = \sum_i x_i 2^i$, then the Hamming weight of x is $w(x) = \sum_i x_i$. In [7] Tu and Deng proposed the following conjecture.

Conjecture 1. Let $S_t = \{(a, b) \mid a, b \in \mathbb{Z}_{2^n-1},\ a+b \equiv t \pmod{2^{n-1}},\ w(a)+w(b) \leq n-1\}$, where $1 \leq t \leq 2^n - 2$, $n \geq 2$. Then $|S_t| \leq 2^{n-1}$.

Based on this conjecture, the authors in [7] constructed some classes of Boolean functions with many nice cryptographic properties.

In this paper we make use of the following bijection from $\mathbb{Z}_{2^n-1}$ onto X_n, where X_n is the set of binary strings of length n except the string consisting of n copies of 1:

$$\mathbb{Z}_{2^n-1} \to X_n, \quad \sum_{i=0}^{n-1} x_i 2^i \mapsto x_0 x_1 \ldots x_{n-1}.$$

We use $|t|$ to denote the length of a binary string $t = t_0 t_1 \ldots t_{n-1}$. Let $-t = \bar{t}_0 \bar{t}_1 \ldots \bar{t}_{n-1}$, where $\bar{t}_i = 1 - t_i$. We also use the notation $1^k 0^m := \underbrace{11\ldots1}_{k\ times}\underbrace{00\ldots0}_{m\ times}$.

In [7], Tu and Deng construct an algorithm which they used it to show that the conjecture above is true when $n \leq 29$. Cusick, Li and Stanica [2] show that Conjecture 1 is true when $w(t) \leq 2$, or $w(t) \geq |t| - 4$. In this paper, we will consider the following conjecture, which is equivalent to Conjecture 1.

Conjecture 2. Let $1 \leq t \leq 2^n - 2$, $n \geq 2$. Let $S(t) = \{a \mid a \in \mathbb{Z}_{2^n-1},\ w(x) \geq w(a) + 1,\ t + a \equiv x \pmod{2^{n-1}}\}$. Then $|S(t)| \leq 2^{n-1}$.

Lemma 3. *Let $t = t_0t_1 \ldots t_{n-1}$. The following statements are true:*
(i) $|S(t)| = |S(t_it_{i+1} \ldots t_{n-1}t_0 \ldots t_{i-1})|$ for any i;
(ii) $w(t) + w(-t) = |t|$;
(iii) The map $\varphi :\ S_t \to S(-t)$, $\quad \varphi((a, b)) = a$, is bijective. Hence $|S_t| = |S(-t)|$.

Proof. The assertions (i) and (ii) are trivial. If $(a, b) \in S_t$, then $w(-t + a) = w(-b) = n - w(b) \geq w(a) + 1$. Hence $a \in S(-t)$. The map φ is well-defined and injective. Conversely, if $a \in S(-t)$, then $w(-t + a) \geq w(a) + 1$ so that

$$\begin{aligned} w(a) + w(t - a) &= w(a) + n - w(-t + a) \\ &\leq w(a) + n - w(a) - 1 = n - 1. \end{aligned}$$

Thus $(a, t - a) \in S_t$, and therefore φ is also surjective. □

Note that the authors in [3] actually showed that Conjecture 2 is true when $w(t) \geq |t| - 2$, or $w(t) \leq 4$ according to Lemma 3.

The remainder of this paper is organized as follows. In Section 2 we construct a partition on the set of binary strings of fixed length. The partition guarantees us to compute a class of $S(t)$, which reaches the bound of Conjecture 2. In Section 3 we compare $|S(t)|$ and $|S(t0^m)|$ based on the partition, and we show that Conjecture 2 is true for some other classes.

2. The Partition $\sim_t$ of X_n

We begin with a lemma.

Lemma 4. *Let $t = t_0t_1 \ldots t_{n-1} \in X_n$, $a = a_0a_1 \ldots a_{n-1} \in X_n$. Suppose that $I = \{j \mid 0 \leq j \leq n - 1, t_j = a_j\} = \{i_1, i_2, \ldots, i_l\}$, where $0 \leq i_1 < i_2 < \cdots < i_l \leq n - 1$. Assume that $t + a \neq 0^n$. Then*

$$w(t + a) = w(a) + w(t) - \sum_{s \in I, t_{i_s} = 1} (i_{s+1} - i_s),$$

where we set $i_{l+1} = i_1 + n$.

Proof. It is clear that $I = \emptyset$ if and only if $t + a = 0^n$. Suppose that $t + a = x_0x_1 \ldots x_{n-1}$. If $j \notin I$, then $j < i_1$ or there exists an $s \geq 1$ such that $i_s < j < i_{s+1}$.

If $i_s < j < i_{s+1}$, by a simple computation we obtain $x_j = 1 - t_{i_s}$. If $j < i_1$, then $x_j = 1 - t_{i_l}$. On the other hand, if $j = i_s \in I$, then $x_j = t_{i_{s-1}}$ if $s > 1$, and $x_j = t_{i_l}$ if $s = 1$. Let $I_j = \{i_s \mid 1 \leq s \leq l, t_{i_s} = a_{i_s} = j\}$, $j = 0, 1$. Then

$$\begin{aligned} w(t) + w(a) - w(t+a) &= (n + |I_1| - |I_0|) - (\sum_{i_s \in I_0} (i_{s+1} - i_s - 1) + |I_1|) \\ &= n - \sum_{i_s \in I_0} (i_{s+1} - i_s) \\ &= \sum_{i_s \in I} (i_{s+1} - i_s) - \sum_{i_s \in I_0} (i_{s+1} - i_s) \\ &= \sum_{i_s \in I_1} (i_{s+1} - i_s). \end{aligned}$$

□

Let $S_i(t) = \{a \in X_n \mid w(t) + w(a) - w(t+a) = i\}$ for any $t \in X_n$. Then $S(t) = \cup_{i=0}^{w(t)-1} S_i(t)$ and $X_n = \cup_{i=0}^{n-1} S_i(t)$ are both disjoint unions. We construct a partition $\sim_t$ on X_n according to Lemma 4.

Definition 5. Let $t = t_0 t_1 \ldots t_{n-1}$ be a binary string of length n. Suppose that $w(t) = r$, and $t_{m_1} = t_{m_2} = \cdots = t_{m_r} = 1$, where $0 \leq m_1 < m_2 < \cdots < m_r \leq n-1$. Let $a = a_0 a_1 \ldots a_{n-1}$ be a binary string. Suppose that $I_a = \{0 \leq j \leq n-1 : a_j = t_j\} = \{i_1, i_2, \ldots, i_l\}$, where $0 \leq i_1 < i_2 < \cdots < i_l \leq n-1$ and set $i_{l+1} = i_1 + n$. We define $(x_1, x_2, \ldots, x_r)^t$ to be the subset of X_n such that $a \in (x_1, x_2, \ldots, x_r)^t$ if and only if the following two conditions hold

(i) $x_j = i_{s+1} - i_s$ if $m_j = i_s \in I_a$;

(ii) $x_j = 0$ if $m_j \notin I_a$.

Moreover, we will use the notation $a^t := (x_1, x_2, \ldots, x_r)^t$ if $a \in (x_1, x_2, \ldots, x_r)^t$.

Remark 6. The idea of this partition comes from the "carries" in [5]. It is a refinement of the partition $X_n = \cup_i S_i(t)$. So we can obtain more information about the structure of $S(t)$.

Definition 7. Let $t = t_0 t_1 \ldots t_{n-1}$, $a = a_0 a_1 \ldots a_{n-1}$ be two given binary strings of length n. For any $0 \leq m \leq n-1$, we set $a_m^t = i$, if $b_m = i$ for all $b \in a^t$, $i = 0, 1$. Moreover, we say that a_m^t is free if there exist two strings b' and b'' in a^t such that $b'_m = 0$ and $b''_m = 1$.

Example 8. Let $t = 010010010$, $a = 011000011$, $b = 110110110$, and $c = 100110111$. Then $t_1 = t_4 = t_7 = 1$, and $I_a = \{0, 1, 3, 5, 6, 7\}$, $I_b = \{1, 2, 4, 5, 7, 8\}$, and $I_c = \{2, 4, 5, 7\}$. So $a \in (2, 0, 2)^t$, $b \in (1, 1, 1)^t$, and $c \in (0, 1, 4)^t$.

Moreover, by definition 5 $a' \in a^t$ if and only if $a' = 01100{*}{*}11$, where $* = 0$ or 1. That is, a_5^t and a_6^t are both free and $|a^t| = 4$. Moreover, $b' \in b^t$ if and only if $b' = {*}10{*}10{*}10$, $c' \in c^t$ if and only if $c' = 100{*}10{*}11$, where $* = 0$ or 1.

It follows that $a^t = (x_i)^t \subseteq S_{\sum_{i=1}^r x_i}(t)$ from Definition 5 and Lemma 4. Moreover, if k is the number of indices such that a_i^t is free, then $|a^t| = 2^k$. Let

$$a_i(j) = \sharp\{(x_1, x_2, \ldots, x_j) \mid x_j \in \mathbb{N},\ \sum_{k=1}^{j} x_k = i\} = \binom{i+j-1}{i}.$$

The proof of the following lemma is easy so we omit it.

Lemma 9. *For any $r \geq 1$,*

$$\sum_{i=0}^{l} c_i a_i(r) = \sum_{i=0}^{l} (c_i - \sum_{j=i+1}^{l} c_j) a_i(r+l-i+1).$$

In particular, $\sum_{i=0}^{l} 2^{-i} a_i(r) = 2^{-l} \sum_{i=0}^{l} a_i(r+l-i+1)$.

The results of Theorem 10 and Lemma 11 have been proved in [5]. Here we give another proof.

Theorem 10. *Let $t = 10^{s_1}10^{s_2}\ldots 10^{s_r}$, where $s_i \geq r-1$ and $w(t) = r$. Then $|S(t)| = 2^{|t|-1}$.*

Proof. Suppose that $|t| = n$, $a \in (x_1, x_2, \ldots, x_r)^t$ and $\sum_{i=1}^{r} x_i \leq r-1$. Then a is of the form

$$*_1 \underbrace{11\ldots1}_{k_1} 00\ldots0 *_2 \underbrace{11\ldots1}_{k_2} 00\ldots0 \ldots\ldots *_r \underbrace{11\ldots1}_{k_r} 00\ldots0,$$

where $*_i = 1$ and $k_i = x_i$ if $x_i > 0$, and $*_i = 0, k_i = 0$ if $x_i = 0$. Observe that there are exactly $n - r - \sum_{i=1}^{r} x_i$ free indices of $(x_1, x_2, \ldots, x_r)^t$ if $x_i \leq s_i$. Since $S(t) = \cup_{i=0}^{r-1} S_i(t)$ is a disjoint union, one has

$$\begin{aligned} |S(t)| = \sum_{i=0}^{r-1} |S_i(t)| = \sum_{i=0}^{r-1} \sum_{\sum_{j=1}^{r} x_j = i} |(x_1, x_2, \ldots, x_r)^t| &= \sum_{i=0}^{r-1} 2^{n-r-i} a_i(r) \\ &= 2^{n-2r+1} \sum_{i=0}^{r-1} \binom{2r-1}{i} \\ &= 2^{n-2r+1} \cdot 2^{2r-2} \\ &= 2^{n-1}. \end{aligned}$$

$\square$

Lemma 11. *Let $t = 1^k 0^m$. Then $|S_j(t)| = b_j 2^{m-j}$, where*

$$b_j = \begin{cases} 1, & j = 0 \\ \frac{4^j - 1}{3}, & 1 \leq j \leq k \\ \frac{4^k - 1}{3}, & k < j \leq m \end{cases}$$

Proof. The case $j = 0$ is trivial. In fact for any $1 < j \leq m$,

$$\begin{aligned}
|S_j(t)| &= \sum_{\sum_{i=1}^{k} x_i = j} |(x_1, x_2, \ldots, x_k)^t| \\
&= \sum_{i=k-j+1}^{k} \sum_{x_i > 0, \sum_i x_i = j} |(0, \ldots, 0, x_i, x_{i+1}, \ldots, x_k)^t| \\
&= \sum_{i=k-j+1}^{k} 2^{k-i} \cdot 2^{m-j+k-i} \\
&= 2^{m-j} \sum_{i=k-j+1}^{k} 2^{2(k-i)} \\
&= b_j 2^{m-j}.
\end{aligned}$$

□

Theorem 12. *Let $t = 1^k 0^{s_1} 10^{s_2} \ldots 10^{s_{r-k+1}}$, where $w(t) = r$, $k \geq 1$ and $s_i \geq r - 1$. Then $|S(t)| \leq 2^{|t|-1}$.*

Proof. Suppose that $t' = 1^k 0^{s_1}$, $t'' = 10^{s_2} \ldots 10^{s_{r-k+1}}$ such that $|t'| = n_1$, $|t''| = n_2$, and $|t| = n$. Let b_j satisfy $|S_j(t')| = b_j 2^{n_1-k-j}$. Then

$$\begin{aligned}
|S(t)| &= \sum_{i=1}^{r-1} |S_i(t)| \\
&= \sum_{i=0}^{r-1} \sum_{j=0}^{r-i-1} |S_{i-j}(t'')||S_j(t')| \\
&= 2^{n-r} [\sum_{i=0}^{r-1} \sum_{j=0}^{r-i-1} b_j 2^{-i-j} a_i(r-k)] \\
&= 2^{n-r} [\sum_{i=0}^{r-1} c_i a_i(r-k)] \\
&= 2^{n-r} [\sum_{i=0}^{r-k-1} 2^{k-i-1} a_i(r-k+1) + \sum_{i=r-k}^{r-2} 2^{r-2i-2} a_i(r-k+1) \\
&\quad + 2^{-r+1} a_{r-1}(r-k+1)],
\end{aligned}$$

where $c_i = 2^{k-i} - \frac{2^{-r+2k+1} - 2^{-r+1}}{3}$ if $0 \leq i \leq r-k-1$, and $c_i = \frac{2^{r-2i} + 2^{-r+1}}{3}$ if $r - k \leq i \leq r - 1$.

Let $T = 1^{k-1}0^{s_1}10^{s_2}\dots 10^{s_{r-k+1}+1}$. Then $|T| = n$ and $w(T) = r-1$. Similarly,

$$\begin{aligned}
|S(T)| &= 2^{n-r+1}[\sum_{i=0}^{r-k-1} 2^{k-i-2}a_i(r-k+1) + \sum_{i=r-k}^{r-3} 2^{r-2i-3}a_i(r-k+1) \\
&\quad + 2^{-r+2}a_{r-2}(r-k+1)] \\
&= 2^{n-r}[\sum_{i=0}^{r-k-1} 2^{k-i-1}a_i(r-k+1) + \sum_{i=r-k}^{r-3} 2^{r-2i-2}a_i(r-k+1) \\
&\quad + 2^{-r+3}a_{r-2}(r-k+1)].
\end{aligned}$$

Therefore,

$$\begin{aligned}
|S(T)| - |S(t)| &= 2^{n-2r+1}[2a_{r-2}(r-k+1) - a_{r-1}(r-k+1)] \\
&= 2^{n-2r+1}[2\binom{2r-k-2}{r-2} - \binom{2r-k-1}{r-1}] \\
&= \frac{k-1}{r-1}\binom{2r-k-2}{r-2}2^{n-2r+1} > 0.
\end{aligned}$$

It follows by induction that $|S(t)| \le |S(10^{s_1+k-1}10^{s_2}\dots 10^{s_{r-k+1}+k-1})| = 2^{n-1}$. $\square$

3. A Comparison Lemma and its Application

It was conjectured in [5] that the converse of Theorem 10 is true. Let $t = t_0t_1\dots t_{n-1}$ and $T = t0^{N-n}$ be two binary strings, where $N - n \ge w(t) - 1$. Another question is whether $|S(T)| \ge 2^{N-n}|S(t)|$. We cannot prove that, but we have the following result based on the partition on X_n. We consider what happens if we add some $0's$ in the string.

Lemma 13. *Let* $t = 10^{s_1}\dots 10^{s_u}10^{s_{u+1}}\dots 10^{s_r}$, $T = 10^{s_1}\dots 10^{s_u}10^{r-1}10^{r-1}\dots 10^{s'_r}$ *such that* $|t| = |T| = n$, $w(t) = w(T) = r$. *Suppose that* $s_i \ge r-1$ *for any* $i \ge u+2$, $s'_r \ge r-1$. *Let* $m_l = \sum_{i=l}^{u+1}(s_i+1)$ *for any* $1 \le l \le u+1$. *Then*

$$\begin{aligned}
|S(T)| - |S(t)| &= \sum_{l=1}^{u+1}\sum_{j=0}^{r-1}\sum_{\sum_{i=1}^{l} x_i = j} 2^{-r+j+1}[a_{r-j-1}(r-u-1) - a_{r-j-2}(r-u)] \\
&\quad \times |(x_1,\dots,x_{l-1},x_l = m_l,0,\dots,0)^T|.
\end{aligned}$$

Proof. Suppose that $l \le u+1$ and $x_l < m_l$. By comparing the free indices the cardinality of $(x_1,\dots,x_l,0,\dots,0,x_{u+2},x_{u+3},\dots,x_r)^t$ is equal to the cardinality of $(x_1,\dots,x_l,0,\dots,0,x_{u+2},x_{u+3},\dots,x_r)^T$. Let

$$I_1 = \sum_{l=1}^{u+1}\sum_{x_l \ge m_l, \sum_i x_i \le r-1} |(x_1,\dots,x_l,0,\dots,0,x_{u+2},x_{u+3},\dots,x_r)^T|,$$

$$I_2 = \sum_{l=1}^{u+1} \sum_{x_l \geq m_l, \sum_i x_i \leq r-1} |(x_1, \ldots, x_l, 0, \ldots, 0, x_{u+2}, x_{u+3}, \ldots, x_r)^t|.$$

Then $\Delta = |S(T)| - |S(t)| = I_1 - I_2$.

For any given $(x_1, x_2, \ldots, x_l, 0, \ldots, 0, x_{u+2}, x_{u+3}, \ldots, x_r)^t$ such that $x_l \geq m_l$, one has $x_{u+2} = 0$ if $x_l > m_l$, $x_{u+2} > 0$ if $x_l = m_l$. Moreover, if $x_l > m_l$, the cardinality of $(x_1, \ldots, x_l, 0, \ldots, 0, x_{u+2}, x_{u+3}, \ldots, x_r)^t$ is equal to the cardinality of $(x_1, \ldots, x_{l-1}, m_l, 0, \ldots, 0, x_{u+2} = x_l - m_l, x_{u+3}, \ldots, x_r)^t$. So

$$\begin{aligned}
I_2 &= 2\sum_{l=1}^{u+1} \sum_{x_l = m_l, x_{u+2} > 0, \sum_{i=1}^r x_i \leq r-1} |(x_1, \ldots, x_l, 0, \ldots, 0, x_{u+2}, \ldots, x_r)^t| \\
&= 4\sum_{l=1}^{u+1} \sum_{x_{u+2} > 0, \sum_{i=1}^r x_i \leq r-1} |(x_1, \ldots, x_l = m_l, 0, \ldots, 0, x_{u+2}, \ldots, x_r)^T| \\
&= 4\sum_{l=1}^{u+1} \sum_{j=0}^{r-2} \sum_{\sum_{i=1}^l x_i = j} \sum_{\sum_{i=u+2}^r x_i \leq r-j-1, x_{u+2} > 0} |(x_1, \ldots, x_l = m_l, 0, \ldots, 0, x_{u+2}, \ldots, x_r)^T| \\
&= 4\sum_{l=1}^{u+1} \sum_{j=0}^{r-2} \sum_{\sum_{i=1}^l x_i = j} \sum_{k=0}^{r-j-2} 2^{-1-k} a_k(r-u-1) |(x_1, \ldots, x_l = m_l, 0, \ldots, 0)^T|.
\end{aligned}$$

Similarly,

$$\begin{aligned}
I_1 &= \sum_{l=1}^{u+1} \sum_{x_l \geq m_l, \sum_{i=1}^l x_i \leq r-1} |(x_1, \ldots, x_l, 0, \ldots, 0, x_{u+2}, \ldots, x_r)^T| \\
&= \sum_{l=1}^{u+1} \sum_{j=0}^{r-1} \sum_{\sum_{i=1}^{l-1} x_i + m_l = j} \sum_{y + \sum_{i=u+2}^r \leq r-j-1} |(x_1, \ldots, m_l + y, 0, \ldots, 0, x_{u+2}, \ldots, x_r)^T| \\
&= \sum_{l=1}^{u+1} \sum_{j=0}^{r-1} \sum_{\sum_{i=1}^l x_i = j} \sum_{k=0}^{r-j-1} 2^{-k} a_k(r-u) |(x_1, \ldots, x_{l-1}, x_l = m_l, 0, \ldots, 0)^T|.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\Delta &= I_1 - I_2 \\
&= \sum_{l=1}^{u+1} \sum_{j=0}^{r-1} \sum_{\sum_{i=1}^l x_i = j} [\sum_{k=0}^{r-j-1} 2^{-k} a_k(r-u) - \sum_{k=0}^{r-j-2} 2^{1-k} a_k(r-u-1)] \\
&\quad \times |(x_1, \ldots, x_{l-1}, x_l = m_l, 0, \ldots, 0)^T| \\
&= \sum_{l=1}^{u+1} \sum_{j=0}^{r-1} \sum_{\sum_{i=1}^l x_i = j} 2^{-r+j+1} [a_{r-j-1}(r-u-1) - a_{r-j-2}(r-u)] \\
&\quad \times |(x_1, \ldots, x_{l-1}, x_l = m_l, 0, \ldots, 0)^T|.
\end{aligned}$$

This finishes the proof. $\square$

Theorem 14. *Let $t = 10^{s_1}10^{s_2}\dots 10^{s_{r-1}}10^{s_r}$, where $s_i \geq i-2$. Then $|S(t)| \leq 2^{|t|-1}$. In particular, $|S(t)| \leq 2^{|t|-1}$ if $s_1 < s_2 < \cdots < s_r$.*

Proof. It is clear that $2^m|S(t)| \leq |S(t0^m)| = 2^{m-1}|S(t0)|$ for any $m \geq 1$ since $s_r \geq r-2$. So we can assume that s_r is sufficiently large. We set

$$t^{(i)} = 10^{s_1}10^{s_2}\dots 10^{s_i}10^{r-1}10^{r-1}\dots 10^{s_{r,i}},$$

such that $|t^{(i)}| = n$, $w(t^i) = r$, and $s_{r,i} \geq r-1$. Let $m_{l,u+1} = \sum_{i=l}^{u+1}(s_i+1)$ for any $l \leq u+1 \leq r-1$. By Lemma 13,

$$\begin{aligned} \Delta_u &= |S(t^{(u)})| - |S(t^{(u+1)})| \\ &= \sum_{l=1}^{u+1}\sum_{j=0}^{r-1}\sum_{\sum_{i=1}^{l} x_i = j} 2^{-r+j+1}[a_{r-j-1}(r-u-1) - a_{r-j-2}(r-u)] \\ &\qquad \times |(x_1,\dots,x_{l-1},x_l = m_{l,u+1},0,\dots,0)^{t^{(u)}}|. \end{aligned}$$

Suppose that $(x_1,\dots,x_{l-1},x_l = m_{l,u+1},0,\dots,0)^{t^{(u)}} \neq \emptyset$, where $\sum_{i=1}^{l} x_i = j \leq r-1$ and $m_{l,u+1} \geq s_{u+1}+1$. Then $r-j-1 \leq r-s_{u+1}-2 \leq r-u-1$ since $s_{u+1} \geq u-1$. It follows that $a_{r-j-1}(r-u-1) - a_{r-j-2}(r-u) \geq 0$ and $\Delta_u \geq 0$. By induction $|S(t)| \leq |S(t^{(r-2)})| \leq |S(t^{(r-3)})| \leq \cdots \leq |S(t^{(0)})| = 2^{n-1}$. $\square$

Theorem 15. *Let $t = 10^{s_1}10^{s_2}\dots 10^{s_{r-1}}10^{s_r}$. Suppose that $s_i + s_j \geq r-2$ for any $1 \leq i,j \leq r$. Then $|S(t)| \leq 2^{|t|-1}$.*

Proof. We can assume that $s_r < r-1$. Let $T = 10^{s_1}10^{s_2}\dots 10^{s_{r-1}}10^{r-1}$. Suppose that $|T| = N$, $|t| = n$. It suffice to show that $|S(T)| \geq 2^{N-n}|S(t)|$. Similar to the proof of Lemma 13, one has

$$\begin{aligned} |S(T)| - 2^{N-n}|S(t)| &= \sum_{\sum x_i \leq r-1, x_r \geq s_r+1} |(x_1,x_2,\dots,x_r)^T| \\ &\quad - 2^{N-n+1}\sum_{\sum x_i \leq r-1, x_1>0} |(x_1,x_2,\dots,x_r = s_r+1)^t|. \end{aligned}$$

But

$$I_1 = \sum_{\sum x_i \leq r-1} |(x_1,x_2,\dots,x_r \geq s_r+1)^T| = \sum_{j=0}^{r-s_r-2} 2^{N-r-j-s_r-1}a_j(r),$$

$$I_2 = 2\sum_{\sum x_i \leq r-1, x_1>0} |(x_1,x_2,\dots,x_r = s_r+1)^t| = \sum_{j=0}^{r-s_r-3} 2^{N-r-s_r-j}a_j(r-1).$$

Thus,

$$\begin{aligned}|S(T)| - 2^{N-n}|S(t)| &= I_1 - I_2 \\ &= 2^{N-r-s_r-1}[\sum_{j=0}^{r-s_r-2} a_j(r) - \sum_{j=0}^{r-s_r-3} 2^{1-j}a_j(r-1)] \\ &= 2^{N-r-s_r-1}[a_{r-s_r-2}(r-1) - a_{r-s_r-3}(r)] \geq 0.\end{aligned}$$

The proof is completed. □

Corollary 16. $|S(t)| \leq 2^{|t|-1}$ *if* $w(t) \leq 6$.

Proof. We only treat the case $w(t) = 6$. Suppose that $t = 10^{s_1}10^{s_2}10^{s_3}10^{s_4}10^{s_5}10^{s_6}$. Let $t' = 10^{r_1}10^{r_2}10^{r_3}10^{r_4}10^{r_5}10^{r_6}$, where $r_i = \min\{s_i, 5\}$. Then $(x_1, x_2, x_3, x_4, x_5, x_6)^t \mapsto (x_1, x_2, x_3, x_4, x_5, x_6)^{t'}$ is a bijection between $\frac{S(t)}{\sim_t}$ and $\frac{S(t')}{\sim_{t'}}$. Moreover, by comparing the number of free indices $|(x_1, x_2, x_3, x_4, x_5, x_6)^t| = 2^{|t|-|t'|}|(x_1, x_2, x_3, x_4, x_5, x_6)^{t'}|$. Therefore, $|S(t)| = 2^{|t|-|t'|}|S(t')|$.

It remains to show that $|S(t')| \leq 2^{n'-1}$. We can assume that $|t'| \geq 30$. If $\min_{1\leq i\leq 6}\{r_i\} \geq 2$, then $r_i + r_j \geq w(t) - 2 = 4$ for any $1 \leq i, j \leq 6$. If $\min_{1\leq i\leq 6}\{r_i\} = r_1 = 1$, then $\min_{2\leq i\leq 6}\{r_i\} \geq 3$. If $\min_{1\leq i\leq 6}\{r_i\} = r_1 = 0$, then $\min_{2\leq i\leq 6}\{r_i\} \geq 4$. We have $r_i + r_j \geq w(t) - 2 = 4$ for any $1 \leq i, j \leq 6$. The corollary follows from Theorem 15. □

References

[1] C. Carlet, On a weakness of the Tu-Deng functions and its repair. IACR Crypotology ePrint Archive **606** (2009).

[2] G. Cohen, Jean-P. Flori, On a generalized combinatorial conjecture involving addition mod $2^k - 1$. IACR Cryptology ePrint Archive **400** (2011).

[3] T. W. Cusick, Y. Li, and P. Stănică, On a combinatorial conjecture. Integers **11** (2011), 185−203.

[4] Jean-P. Flori, H. Randriam, G. Cohen, and S. Mesnager, On a conjecture about binary strings distribution. Sequences and Their Applications SETA 2010, LNCS **6338** (2010), 346−358.

[5] Jean-P. Flori, H. Randriam, G. Cohen, and S. Mesnager, On a conjecture about binary strings distribution. IACR Cryptology ePrint Archive **170** (2010).

[6] Jean-P. Flori, H. Randriam, On the number of carries occuring in an addition mod $2^k - 1$. Integers **12** (2012).

[7] Z. Tu and Y. Deng, A conjecture on binary string and its application on constructing Boolean Functions of optimal algebraic immunity. Designs, Codes and Cryptography **60** (2010), 1−14.

[8] Z. Tu and Y. Deng, A class of 1−Resilient function with high nonlinearity and algebraic immunity. IACR Cryptology ePrint Archive **179** (2010).