Open Journal of Discrete Mathematics, **2013, 3, 49-52**
http://dx.doi.org/10.4236/ojdm.2013.31010 Published Online January 2013 (http://www.scirp.org/journal/ojdm)

A Note on a Combinatorial Conjecture

Guixin Deng
School of Mathematical Science, Guangxi Teachers Education University, Nanning, China
Email: dengguixin@live.com

Received October 7, 2012; revised November 7, 2012; accepted November 17, 2012

ABSTRACT

It is difficult to find Boolean functions achieving many good cryptographic properties. Recently, Tu and Deng obtained two classes of Boolean functions with good properties based on a combinatorial conjecture about binary strings. In this paper, using different approaches, we prove this conjecture is true in some cases. This conjecture has resisted different attempts of proof since it is hard to find a recursive method. In this paper we give a recursive formula in a special case.

Keywords: Binary String; Weight

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

$$w = \sum_i x_i .$$

In [1] Tu and Deng proposed the following conjecture.

Conjecture 1: Let

$$S_t = \{(a,b): 0 \le a,b \le 2^n - 2,$$
$$a + b \equiv t \pmod{2^n - 1}, w(a) + w(b) < n\},$$

where $1 \le t \le 2^n - 2$. Then the cardinality $|S_t| \le 2^{n-1}$.

Based on this conjecture, Tu and Deng [1] constructed two classes of Boolean functions with many good cryptographic properties. In this paper we always use the following bijection, where X_n is the set of binary strings of length n except the string consisting of n copies of 1.

$$Z_{2^{n-1}} \to X_n$$
$$\sum_{i \le n-1} x_i 2^i \mapsto x_0 x_1 \cdots x_{n-1}$$

We use $|t|$ to denote the length of a binary string $t = t_0 t_1 \cdots t_{n-1}$. Let $-t = (1-t_0)(1-t_1)\cdots(1-t_{n-1})$. And we use the following notation $1^k 0^m := 11\cdots 100\cdots 0$, where there are k consecutive 1 and m consecutive 0 in the string.

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

Conjecture 2: Suppose that $1 \le t \le 2^n - 2, n \ge 2$.

Let

$$S(t) = \{a: 0 \le a \le 2^n - 2, w(x) \ge w(a) + 1,$$
$$t + a \equiv x \pmod{2^n - 1}, w(a) + w(b) < n\}.$$

then $|S_t| \le 2^{n-1}$.

The following lemma is easy so we omit the proof.

Lemma 1.1 Let $t = t_0 t_1 \cdots t_{n-1}$. Then following statements are true:

1) $|S(t)| = |S(t_i t_{i+1} \cdots t_{n-1} t_0 t_1 \cdots t_{i-1})|$;

2) $w(t) + w(-t) = n$;

3) The map $\varphi: S_t \to S(-t), \varphi((a,b)) = a$ is bijective. Hence $|S_t| = |S(-t)|$.

So the authors in [3] actually showed that Conjecture 2 is true when

$$w(t) \ge |t| - 2 \text{ or } w(t) \le 4 .$$

According to Lemma 1.1. Deng and Yuan [4] show that Conjecture 2 is true if $w(t) \le 6$.

The outline of this paper is as follows. In Section 2 we introduce some notations. In Section 3, we consider what happen if we change some digit 1 into 0 in the strings. We get a recursive formula about $S(t)$ and prove a new case of the conjecture.

2. A Partition of X_n

The following lemma is about the relation between $w(t+a)$ and $w(t) + w(a)$, which is proved in [4].

Lemma 2.1 Let

$$t = t_0 t_1 \cdots t_{n-1} \in X_n, \quad a = a_0 a_1 \cdots a_{n-1} \in X_n.$$

Suppose that

$$I = \{ j : 0 \le j \le n-1, t_j = a_j \} = \{ i_1, i_2, \cdots, i_l \},$$

where $0 \le i_1 < i_2 < \cdots < i_l \le n-1$. Assume that $t + a \ne 0^n$. Then

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

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

Let

$$S(t) = \{ a \in X_n : w(t) + w(a) - w(t+a) = i \}$$

for any $t \in X_n$ and $s(t) = \dfrac{|S(t)|}{2^{|t|}}$.

Then

$$S(t) = \bigcup_{i=0}^{w(t)-1} S_i(t) \quad \text{and} \quad X_n = \bigcup_{i=0}^{|t|-1} S_i(t)$$

which are disjoin unions. We define a partition on X_n according to Lemma 2.1.

Definition 2.1 Let $t = t_0 t_1 \cdots t_{n-1}$ be a binary string of length *n*. Suppose that

$$w(t) = r, \quad \text{and} \quad t_{m_1} = t_{m_2} = \cdots = t_{m_r} = 1,$$

where $0 \le m_1 < \cdots < m_r \le n-1$. Let $a = a_0 a_1 \cdots a_{n-1}$ be a binary string. Suppose that

$$I_a = \{ j : 0 \le j \le n-1, t_j = a_j \} = \{ i_1, i_2, \cdots, i_l \},$$

where $0 \le i_1 < i_2 < \cdots < i_l \le n-1$. We set $(x_1, x_2, \cdots, x_r)^t$ to be the subset of X_n such that $a \in (x_1, x_2, \cdots, x_r)^t$ 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 $m_j \notin I_a$.

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

Definition 2.2 Let $t = t_0 t_1 \cdots t_{n-1}$ and $a = a_0 a_1 \cdots a_{n-1}$ be two given binary strings. For any $0 \le m \le n-1$, we set $a_m^t = i$, if $b_m = i$ for each $b = b_0 b_1 \cdots b_{n-1} \in a^t, i = 0,1$. We say that a_m^t is free if there are two strings b' and b'' in a^t such that $b'_m = 0$ and $b''_m = 1$.

From Definition 2.1 and Lemma 2.1 we see that

$$a^t = (x_i)^t \subseteq S_{\sum_{i=1}^{w(t)} x_i}(t) \quad \text{and} \quad |a^t| = 2^k,$$

where *k* is the number of indices such that a_i^t is free.

Example 2.1 Let

$t = 1110010010$, $a = 1100101000$, $b = 1110010110$, and

$$c = 1000110100.$$

Then

$$t_0 = t_1 = t_2 = t_5 = t_8 = 1,$$

and

$$I_a = \{0,1,3,5,7,9\},$$

$$I_b = \{0,1,2,3,4,5,6,8,9\},$$

$$I_c = \{0,3,5,6,9\}.$$

So

$a \in (1,2,0,0,0)^t$, $b \in (1,1,1,1,1)^t$ and $c \in (3,0,0,1,0)^t$.

Moreover, by Definition 2.2 $a' \in a^t$ if and only if $a' = 1100 * 0 * * 0 *$, $* = 0$ or 1. That is, a_i^t is free for $i = 4,6,7,9$. We also have $b' \in b^t$ if and only if

$$b' = 1110 * 10 * 10, \quad c' \in c^t$$

if and only if

$$c' = 1000 * 10 * 0 *, \quad * = 0 \text{ or } 1.$$

3. Main Results

If $t = 1^{r_1} 0^{s_1} 1^{r_2} 0^{s_2} \cdots 1^{r_n} 0^{s_n}$ with each $r_i \ge 1$, then we say that the block of t is n. Jean-P. Flori and H. Randriam [5] give some asymptotic results when each $s_i \ge w(t) - 1$. In particular, they show that Conjecture 2 is true if the block of *t* is smaller than 3 or each r_i is sufficient large for a fixed length of block. We give a recursive formula to show that we can restrict our attention to the case each r_i is smaller than the block of t in this situation. They also conjectured that

$$\left| S\left(1^{r_1} 0^{s_1} \cdots 1^{r_n - 1} 0^{s_n + 1}\right) \right| > \left| S\left(1^{r_1} 0^{s_1} \cdots 1^{r_n} 0^{s_n}\right) \right| \quad \text{if} \quad r_n > 3.$$

Lemma 3.1 Let

$$t = 10^{s_1} 10^{s_2} \cdots 10^{s_r}$$

and

$$T = 10^{s_1} 10^{s_2} \cdots 10^{s_{r-2}} 10^{s_{r-1} + s_r + 1}$$

with

$$s_r \ge r - 1 \quad \text{and} \quad |t| = |T| = n.$$

Let

$$m_i = \sum_{j=i}^{r-1} (s_j + 1) \quad \text{for} \quad 1 \le i \le r-1,$$

$$\chi(T) = \{ a \in X_n : a_{m_1}^T \text{ is free} \}$$

and

$$\chi_j(T) = S_j(T) \cap \chi(T).$$

Then

$$|S(T)| - |S(t)| = 2^{-r} \left(\sum_{j=0}^{r-2} 2^j |\chi_j(T)| - 2^{r-1} |\chi_{r-1}(T)| \right)$$

Proof. Note that for any $(x_1, x_2, \cdots, x_r)^t$, if $x_i \ge m_i + 1$,

then $x_j = 0$ for each $j > i$, moreover in this case we have

$$\left|\left(x_i\right)^t\right| = \left|\left(x_1, \cdots, x_{i-1}, m_i, 0, \cdots, 0, x_i - m_i\right)^t\right|.$$

Let

$$I_1 = \sum_{\sum x_i \le r-1, x_i < m_i} \left|\left(x_1, x_2, \cdots, x_r\right)^t\right|,$$

$$I_2 = \sum_{\sum x_i \le r-1, \text{one } x_i \ge m_i + 1} \left|\left(x_1, x_2, \cdots, x_r\right)^t\right|,$$

then $\left|S\left(t\right)\right| = I_1 + 2I_2$. Similarly we write

$$\left|S\left(T\right)\right| = J_1 + J_2,$$

where

$$J_1 = \sum_{\sum x_i \le r-2, x_i < m_i} \left|\left(x_1, x_2, \cdots, x_{r-1}\right)^T\right|,$$

$$J_2 = \sum_{\sum x_i \le r-2, \text{one } x_i \ge m_i} \left|\left(x_1, x_2, \cdots, x_{r-1}\right)^T\right|.$$

We observe that if $a^T = \left(x_1, x_2, \cdots, x_{r-1}\right)^T$, then $a \in \chi$ if and only if each $x_i < m_i$. Now if $x_i \ge m_i + 1$, by comparing the number of free indices we have

$$\left|\left(x_1, \cdots, x_i, 0, \cdots, 0\right)^t\right| = \frac{1}{2}\left|\left(x_1, \cdots, x_i, 0, \cdots, 0\right)^T\right|.$$

Hence, $2I_2 = J_2$. If each $x_i < m_i$, then

$$\left|\left(x_1, \cdots, x_r\right)^t\right| = 2^{-x_r - 1}\left|\left(x_1, \cdots, x_{r-1}\right)^T\right|.$$

Suppose that $\sum_{i=1}^{r-1} x_i = j \le r-1$. Then

$$\sum_{x_r=0}^{r-1-j}\left|\left(x_1, \cdots, x_r\right)^t\right| = \sum_{x_r=0}^{r-1-j} 2^{-x_r}\left|\left(x_1, \cdots, x_{r-1}, 0\right)^t\right|$$
$$= 2\left(1 - 2^{-r+j}\right)\left|\left(x_1, \cdots, x_{r-1}, 0\right)^t\right|.$$

So

$$I_1 = \sum_{j=0}^{r-1}\sum_{\sum x_i \le r-1, x_i < m_i} 2\left(1 - 2^{-r+j}\right)\left|\left(x_1, \cdots, x_{r-1}, 0\right)^t\right|$$
$$= \sum_{j=0}^{r-1}\sum_{\sum x_i \le r-1, x_i < m_i}\left(1 - 2^{-r+j}\right)\left|\left(x_1, \cdots, x_{r-1}\right)^T\right|.$$

Therefore

$$\left|S\left(T\right)\right| - \left|S\left(t\right)\right| = J_1 - I_1$$
$$\sum_{\sum x_i \le r-2, x_i < m_i}\left|\left(x_1, x_2, \cdots, x_{r-1}\right)^T\right|$$
$$-\sum_{j=0}^{r-1}\sum_{\sum x_i \le r-1, x_i < m_i}\left(1 - 2^{-r+j}\right)\left|\left(x_1, \cdots, x_{r-1}\right)^T\right|$$
$$= 2^{-r}\left(\sum_{j=0}^{r-2} 2^j\left|\chi_j\left(T\right)\right| - 2^{r-1}\left|\chi_{r-1}\left(T\right)\right|\right).$$

This finishes the proof.

Remark 3.1 Let $t = 10^{s_1}10^{s_2}\cdots 10^{s_r}$ with $s_r \ge r-1$. It is clear that

$$\left|S\left(t0^n\right)\right| = 2^n\left|S\left(t\right)\right|$$

for any $n > 0$. So we use the following notation 0^∞ means that there are sufficient consecutive 0 in the string.

We set

$$\chi_j\left(t\right) = \left\{a : a^t = \left(x_i\right)^t, x_j = 0 \text{ for } j > \sum_{i=1}^{n-1} r_i\right\}$$

for $t = 1^{r_1}0^\infty 1^{r_2}0^\infty\cdots 1^{r_n}0^\infty$.

Theorem 3.1 Let

$$t = 1^{r_1}0^\infty 1^{r_2}0^\infty\cdots 1^{r_n-1}0^\infty,\quad T = 1^{r_1}0^\infty 1^{r_2}0^\infty\cdots 1^{r_n}0^\infty,$$
$$t' = 1^{r_1-1}0^\infty 1^{r_2}0^\infty\cdots 1^{r_n}0^\infty,\quad T' = 1^{r_1-1}0^\infty 1^{r_2}0^\infty\cdots 1^{r_n+1}0^\infty,$$
$$t^* = 10^\infty 1^{r_2}0^\infty\cdots 1^{r_n-2}0^\infty,\quad T^* = 10^\infty 1^{r_2}0^\infty\cdots 1^{r_n-1}0^\infty,$$

where each $r_i \ge 1$ and $r_1 \ge 2, r_n \ge 2$. Then

$$s\left(t\right) - s\left(T\right) = s\left(t'\right) - s\left(T'\right) + 2^{-2}\left(s\left(t^*\right) - s\left(T^*\right)\right).$$

Proof. Suppose that those strings have the same length and $w\left(T\right) = \sum_{i=1}^n r_i = r$. By Lemma 3.1

$$\left|S\left(t\right)\right| - \left|S\left(T\right)\right| = 2^{-r}\left(\sum_{j=0}^{r-2} 2^j\left|\chi_j\left(t\right)\right| - 2^{r-1}\left|\chi_{r-1}\left(t\right)\right|\right)$$

$$\left|S\left(t'\right)\right| - \left|S\left(T'\right)\right| = 2^{-r}\left(\sum_{j=0}^{r-2} 2^j\left|\chi_j\left(t'\right)\right| - 2^{r-1}\left|\chi_{r-1}\left(t'\right)\right|\right)$$

$$\left|S\left(t^*\right)\right| - \left|S\left(T^*\right)\right|$$
$$= 2^{-r+r_1}\left(\sum_{j=0}^{r-r_1-2} 2^j\left|\chi_j\left(t^*\right)\right| - 2^{r-r_1-1}\left|\chi_{r-r_1-1}\left(t^*\right)\right|\right).$$

Let

$$a^t = \left(x_{11}, \cdots, x_{1r_1}, \cdots, x_{n-1,1}, \cdots, x_{n-1,r_{n-1}}, 0, \cdots, 0\right)^t.$$

If $x_{11} > 0$, by comparing the number of free indices we have

$$\left|a^t\right| = \left|\left(r_1 - 1, 0, \cdots, y, x_{21}, \cdots, x_{n-1,r_{n-1}}, 0, \cdots, 0\right)\right|^t,$$

where $y = \sum_{i=1}^{r_1} x_{1i} - r_1 + 1$. We set

$$\kappa_j\left(t\right) = \left\{a \in \chi_j\left(t\right) : a^t = \left(0, y_2, \cdots, y_{r-1}\right)^t\right\}$$

and

$$\lambda_j\left(t\right) = \left\{a \in \chi_j\left(t\right) : a^t = \left(r_1 - 1, y_2, \cdots, y_{r-1}\right)^t\right\}.$$

Then

$$\left|S\left(t\right)\right| - \left|S\left(T\right)\right| = 2^{-r}\left(\sum_{j=0}^{r-2} 2^j\left|\kappa_j\left(t\right)\right| - 2^{r-1}\left|\kappa_{r-1}\left(t\right)\right|\right)$$
$$+ 2^{-r+r_1-1}\left(\sum_{j=0}^{r-2} 2^j\left|\lambda_j\left(t\right)\right| - 2^{r-1}\left|\lambda_{r-1}\left(t\right)\right|\right)$$

Let

$$I_1 = 2^{-r}\left(\sum_{j=0}^{r-2} 2^j\left|\kappa_j\left(t\right)\right| - 2^{r-1}\left|\kappa_{r-1}\left(t\right)\right|\right),$$

and

$$I_2 = 2^{-r+r_1-1}\left(\sum_{j=0}^{r-2} 2^j \left|\lambda_j(t)\right| - 2^{r-1}\left|\lambda_{r-1}(t)\right|\right).$$

Now consider the following mapping φ and ψ. If $a \in \kappa_j(t)$ and $a^t = (0, y_2, \cdots, y_{r-1})^t$, then

$$\varphi(a^t) = (y_2, \cdots, y_{r-1}, 0)^{t'}.$$

Then

$$\left|a^t\right| = \left|\varphi(a^t)\right|.$$

So

$$\left|\kappa_j(t)\right| = \left|\chi_j(t')\right|.$$

If

$$a \in \lambda_j(t) \text{ and } a^t = (r_1 - 1, y_2, \cdots, y_{r-1})^t,$$

then

$$\psi(a^t) = (y_{r_1} - 1, y_{r_1+1}, \cdots, y_{r-1})^{t^*}.$$

It is easy to see that

$$\psi(a^t) \subseteq \chi_{j-r_1}(t^*) \text{ and } \left|a^t\right| = 2^{-r_1-1}\left|\psi(a^t)\right|.$$

By the discussion above we obtain

$$I_1 = \left|S(t')\right| - \left|S(T')\right|, \text{ and } I_2 = 2^{-2}\left(\left|S(t^*)\right| - \left|S(T^*)\right|\right).$$

This finishes the proof.

Corollary 3.1 With the same notations in Theorem 3.1. Suppose that

$$r_n \geq \#\{i : 1 \leq i \leq n, r_i \geq 2\},$$

then

$$s(t) > s(T).$$

Proof. We proof the statement by induction on

$$l = r_n \geq \#\{i : 1 \leq i \leq n, r_i \geq 2\}.$$

The case $l = 1$ implies that

$$r_1 = r_2 = \cdots = r_{n-1} = 1.$$

This was proved in [4]. Without loss of generality we can assume that $r_1 > 1$ and $r_n > l$. By induction

$$s(t^*) > s(T^*),$$

by Theorem 3.1

$$s(t) - s(T) > s(t') - s(T').$$

The proof is completed by induction on $\sum_{i=1}^{n-1} r_i$.

Corollary 3.2 Let $t = 1^{r_1}0^{\infty}1^{r_2}0^{\infty}1^{r_3}0^{\infty}$. Then

$$s(t) \leq \frac{1}{2}.$$

Proof. By Corollary 3.1 it suffice to show that case when each $r_i < 3$. So we have $w(t) \leq 6$, which is proved in [4].

REFERENCES

[1] 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*, Vol. 60, No. 1, 2010, pp. 1-14. doi:10.1007/s10623-010-9413-9

[2] G. Cohen and J.-P. Flori, "On a Generalized Combinatorial Conjecture Involving Addition Mod $2^k - 1$," *IACR Cryptology ePrint Archive*, Vol. 400, 2011, in press.

[3] T. W. Cusick, Y. Li and P. Stanica, "On a Combinatorial Conjecture," *Integers*, Vol. 11, No. 2, 2011, pp. 185-203. doi:10.1515/integ.2011.017

[4] G. Deng and P. Yuan, "On a Combinatorial Conjecture of Tu and Deng," *Integers*, Vol. 12, No. A48, 2012.

[5] J.-P. Flori and H. Randriam, "On the Number of Carries Occuring in an Addition Mod $2^k - 1$," *Integers*, Vol. 12, No. A10, 2012.

