A Note on the Tu-Deng Conjecture*

CHENG Kaimin · HONG Shaofang · ZHONG Yuanming

DOI: 10.1007/s11424-015-2240-3
Received: 8 November 2012 / Revised: 1 July 2014
©The Editorial Office of JSSC & Springer-Verlag Berlin Heidelberg 2015

Abstract Let $k$ be a positive integer. For any positive integer $x = \sum_{i=0}^{\infty} x_i 2^i$, where $x_i = 0, 1$, we define the weight $w(x)$ of $x$ by $w(x) = \sum_{i=0}^{\infty} x_i$. For any integer $t$ with $0 < t < 2^k - 1$, let $S_t := \{(a, b) \in \mathbb{Z}_2 | a + b \equiv t \pmod{2^k - 1}, w(a) + w(b) < k, 0 \leq a, b \leq 2^k - 2\}$. This paper gives explicit formulas for cardinality of $S_t$ in the cases of $w(t) \leq 3$ and an upper bound for cardinality of $S_t$ when $w(t) = 4$. From this one then concludes that a conjecture proposed by Tu and Deng in 2011 is true if $w(t) \leq 4$.

Keywords 2-adic valuation, Tu-Deng conjecture, weight.

1 Introduction

Let $m$ and $k$ be arbitrary given positive integers. For any integer $x$, by $\langle x \rangle_m$ we denote the least nonnegative residue of $x$ modulo $m$. That is, $x \equiv \langle x \rangle_m \pmod{m}$ and $0 \leq \langle x \rangle_m \leq m - 1$. For convenience, we always let $\langle x \rangle := \langle x \rangle_{2^k - 1}$ if $m = 2^k - 1$. One may write $\langle x \rangle = \sum_{i=0}^{k-1} x_i 2^i$, where $x_i \in \{0, 1\}$. Then the weight $w(x)$ of $x$ is defined by $w(x) := \sum_{i=0}^{k-1} x_i$.

Boolean functions are important topics in the area of cryptography algorithm[1, 2]. In 2011, Tu and Deng[1] constructed two classes of Boolean functions: One is balanced and the other is bent. In the meantime, they proposed the following interesting conjecture.

Conjecture 1 (see [1]) Let $k > 1$ be an integer. For any integer $0 < t < 2^k - 1$, let $S_t := \{(a, b) \in \mathbb{Z}_2 | (a + b) = t, w(a) + w(b) < k, 0 \leq a, b \leq 2^k - 2\}$. Then $|S_t| \leq 2^{k-1}$.

Tu and Deng[1] confirmed their own conjecture by computer for $k \leq 29$. Based on this conjecture, they constructed some classes of Boolean functions with many optimal cryptographic properties.

CHENG Kaimin
Mathematical College, Sichuan University, Chengdu 610064, China; Department of Mathematics, Sichuan University Jinjiang College, Pengshan 620860, China. Email: ckm200126.com.

HONG Shaofang (Corresponding author) · ZHONG Yuanming
Mathematical College, Sichuan University, Chengdu 610064, China. Email: sfhong@scu.edu.cn.

*The research was supported partially by the National Science Foundation of China under Grant No. 11371260 and the Youth Foundation of Sichuan University Jinjiang College under Grant No. QJ141308.

○This paper was recommended for publication by Editor HU Lei.
Our main goal in this paper is to investigate the above conjecture. In particular, we will show that the Tu-Deng conjecture is true when \( w(t) \leq 4 \). Actually, we give explicit formulas for cardinality of \( S_t \) in the cases of \( w(t) \leq 3 \) and give an upper bound for cardinality of \( S_t \) when \( w(t) = 4 \). That is, we have the following main result.

**Theorem 2**  Let \( k \geq 30 \) be an integer. Then the following are true.

(i) If \( t = 2^i, 0 \leq i \leq k - 1 \), then \( |S_t| = 2^{k-2} + 1 \).

(ii) If \( t = 2^i + 2^j, 0 \leq i < j \leq k - 1 \), then \( |S_t| = 2^{k-2} + 2^{k-3} + 1 \) if \( j - i = k - 2 \) or \( 2 \), and \( |S_t| = 2^{k-2} + 2^{k-4} + 1 \) otherwise.

(iii) If \( t = 2^i + 2^j + 2^l, 0 \leq i < j < l \leq k - 1 \), then

\[
|S_t| = \begin{cases} 
2^{k-2} + 2^{k-4} + 2^{k-5} + 1, & \text{if } (j - i, l - i) = (1, 2), (1, e_1)(5 \leq e_1 \leq k - 4), (e_2, e_2 + 1) \\
& (4 \leq e_2 \leq k - 2), (e_3, f_3)(e_3 \geq 4, e_3 + 4 \leq f_3 \leq k - 4), \\
& (e_4, k - 2)(4 \leq e_4 k - 6), (e_5, k - 1)(4 \leq e_5 \leq k - 5); \\
2^{k-2} + 2^{k-3} + 2^{k-5} + 1, & \text{if } (j - i, l - i) = (1, 3), (2, 3)(1, k - 2), (2, k - 1); \\
2^{k-2} + \sum_{i=1}^{3} 2^{k-3-i} + 1, & \text{if } (j - i, l - i) = (1, 4), (1, k - 3), (2, e_1)(6 \leq e_1 \leq k - 4), \\
& (3, e_2)(7 \leq e_2 \leq k - 4), (e_3, k - 3)(4 \leq e_3 \leq k - 7), \\
& (3, 4), (e_4, f_4)(e_4 \geq 4, e_4 + 1 \leq f_4 \leq e_4 + 2, f_4 \leq k - 1); \\
2^{k-2} + 2^{k-4} + 2^{k-6} + 1, & \text{if } (j - i, l - i) = (1, k - 1), (k - 2, k - 1); \\
2^{k-2} + 2^{k-3} + 1, & \text{if } (j - i, l - i) = (2, 5), (2, k - 3), (3, 5), (3, 6), (3, k - 2). 
\end{cases}
\]

(iv) If \( t = 2^i + 2^j + 2^l + 2^q, 0 \leq i < j < l < q \leq k - 1 \), then \( |S_t| \leq 2^{k-1} - 2^{k-8} + 1 \).

From Theorem 2, we deduce immediately the following result.

**Corollary 3**  Conjecture 1 holds for any positive integer \( t \) with \( w(t) \leq 4 \).

The paper is organized as follows. In Section 2, we introduce a class of sets of pairs of nonnegative integers and present some important lemmas which are needed in proving Theorem 2. In Section 3, we give the proof of Theorem 2.

## 2 Preliminaries

In this section, we first define a class of sets of pairs of nonnegative integers and then give some lemmas which play important roles in proving Theorem 2.

For any nonzero integer \( x \), let \( v_2(x) \) be the 2-adic valuation of \( x \), i.e., \( v_2(x) \) is the highest power of 2 which divides \( x \). Evidently we can write any integer \( a \geq 0 \) as \( a = \sum_{i=0}^{\infty} a_i 2^i \) where \( a_i \in \{0, 1\} \). For any integer \( r \) with \( 0 \leq r \leq k - 1 \), we define a set \( M_r \) as follows:

\[
M_r := \{(a, b) \in \mathbb{Z}^2 | 0 \leq a, b \leq 2^k - 2, v_2(a) = v_2(b) = r, a_i + b_i = 1 \text{ with } r < i < k\}.
\]

Clearly if \((a, b) \in M_r\), then

\[
a_j = b_j = 0, \quad a_r = b_r = 1, \quad a_i + b_i = 1, \quad \text{where } 0 \leq j \leq r - 1 \text{ and } r < i < k - 1.
\]

From (1), the following lemma follows.