ON A COMBINATORIAL CONJECTURE

Thomas W. Cusick
Department of Mathematics, University at Buffalo, Buffalo, New York
cusick@buffalo.edu

Yuan Li[1]
Department of Mathematics, Winston-Salem State University, Winston-Salem, North Carolina
yuanli7983@gmail.com

Pantelimon Stănică
Applied Mathematics Department, Naval Postgraduate School, Monterey, California
pstanica@nps.edu

Received: 4/6/10, Revised: 11/30/10, Accepted: 12/30/10, Published: 2/4/11

Abstract

Recently, Tu and Deng proposed a combinatorial conjecture about binary strings, and, on the assumption that the conjecture is correct, they obtained two classes of Boolean functions which are both algebraic immunity optimal, the first of which are also bent functions. The second class gives balanced functions, which have optimal algebraic degree and the best nonlinearity known up to now. In this paper, using three different approaches, we prove this conjecture is true in many cases with different counting strategies. We also propose some problems about the weight equations which are related to this conjecture. Because of the scattered distribution, we predict that an exact count is difficult to obtain, in general.

1. Introduction

In [3], Tu and Deng proposed the following combinatorial conjecture.

Conjecture 1. Let $S_t = \{(a,b) \,|\, a,b \in \mathbb{Z}_{2^k-1}, a+b \equiv t \pmod{2^k-1}, w(a)+w(b) \leq k-1\}$, where $1 \leq t \leq 2^k-2, k \geq 2$, and $w(x)$ is the Hamming weight of x. Then, the cardinality $\#S_t \leq 2^{k-1}$.

They validated the conjecture by computer for $k \leq 29$. Based on this conjecture, Tu and Deng [3] constructed some classes of Boolean functions with many optimal

[1] Corresponding author

cryptographic properties. It is perhaps worth mentioning that these functions (under some slight modifications) have the best collection of cryptographic properties currently known for a Boolean function.

In this paper we attack this conjecture and prove it for many parameters, dependent upon the binary weight of t. We found out that the distribution of the pairs in S_t is very scattered. With our method, the counting complexity increases directly with the weight of t, or t', where $t' = 2^k - t$. Our counting approach is heavily dependent on the number of solutions of the equation $w(2^{i_1}+2^{i_2}+\cdots+2^{i_s}+x) = r+w(x)$, where $2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} = t$ or t'.

This paper is organized as follows. In Section 2, we introduce some notations and basic facts about the binary weight functions which will be frequently used in the rest of the paper. In Section 3, we prove that the conjecture is true when $w(t) = 1, 2$. In Section 4 we prove the conjecture when $t = 2^k - t'$, $w(t') \leq 2$. In Section 5, we prove the conjecture when $t = 2^k - t'$, $3 \leq w(t') \leq 4$ and t' is odd. In Section 6, we give some open questions about the number of solutions of $w(2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} + x) = r + w(x)$, where $0 \leq x \leq 2^k - 1$ and $0 \leq i_1 < i_2 < \ldots < i_s \leq k-1$.

Since our purpose is to attack the previous combinatorial conjecture, we will not discuss the cryptographic significance of functions constructed assuming the above conjecture. Since we first wrote the paper and posted it on ePrint, several other works have been published [1, 2, 4] on this important class of functions. Our method of attacking the conjecture is somewhat ad-hoc, and covers several cases, which are not covered by the more recent paper [2]. In turn, the paper [2], also gives several results, which are not covered by our approach.

2. Preliminaries

If x is an nonnegative integer with binary expansion $x = x_0 + x_1 2 + x_2 2^2 + \cdots$ ($x_i \in \mathbb{F}_2 = \{0, 1\}$), we write $x = (x_0 x_1 x_2 \ldots.)$. The (*Hamming*) *weight* (sometimes called the sum of digits) of x is $w(x) = \sum_i x_i$. The following lemma is well known and easy to show.

Lemma 2. *The following statements are true:*

$$w(2^k - 1 - x) = k - w(x),\ 0 \leq x \leq 2^k - 1;$$
$$w(x + 2^i) \leq w(x),\ \textit{if } x_i = 1;$$
$$w(x + y) \leq w(x) + w(y),\ \textit{with equality if and only if } x_i + y_i \leq 1,\ \textit{for any } i;$$
$$w(x) = w(x-1) - i + 1, x \equiv 2^i \pmod{2^{i+1}},\ \textit{i.e., the first nonzero digit is } x_i.$$

The last statement implies that: $w(x) = w(x-1)+1$ if x is odd; $w(x) = w(x-1)$ if $x \equiv 2 \pmod 4$; $w(x) = w(x-1) - 1$ if $x \equiv 4 \pmod 8$, etc., and so, for two consecutive integers, the weight of the even integer is never greater than the weight of the odd integer.

Lemma 3. *If* $0 \le x \le 2^m - 1$ *and* $0 \le i < j \le m-1$*, then:*

1. $w(x + 2^i + 2^j) = 1 + w(x)$ *if and only if*
   $x_i = 0, x_j = 1, x_{j+1} = 0,$
   or, $x_i = 1, x_{i+1} = 0, x_j = 0\,(j > i+1)$*;*
2. $w(x + 2^i + 2^j) = w(x)$ *if and only if*
   $x_i = 0, x_j = 1, x_{j+1} = 1, x_{j+2} = 0\ (j < m-1)$*;*
   $x_i = 1, x_{i+1} = 1, x_{i+2} = 0, x_j = 0\ (j > i+2)$*;*
   $x_i = 1, x_{i+1} = 0, x_j = 1, x_{j+1} = 0\ (j > i+1)$*;*
   or, $x_i = 1, x_j = 1, x_{j+1} = 0\ (j = i+1)$*.*

Proof. The proof of the above lemma is rather straightforward, and we sketch below the argument for the solutions of $w(x + 2^i + 2^j) = 1 + w(x)$. We look at the binary sum $x + 2^i + 2^j$, where

$$\begin{array}{rcl} 2^i + 2^j & = & \dots 0\overset{i}{1}0 \dots 0\overset{j}{1}0 \dots \\ x & = & \dots\ x_i\ \dots x_j\, x_{j+1} \dots \end{array}$$

and we consider four cases:

`Case 1:` $x_i = 0$, $x_j = 0$; this is impossible, since then, $w(x + 2^i + 2^j) = 2 + w(x)$.

`Case 2:` $x_i = 0$, $x_j = 1$; in this case, it is obvious that one needs $x_{j+1} = 0$.

`Case 3:` $x_i = 1$, $x_j = 0$; as in Case 2, we have $x_{i+1} = 0$ and $j > i+1$.

`Case 4:` $x_i = 1$, $x_j = 1$; this case is impossible by the second item of Lemma 2.

The second part of the lemma can be proved similarly. □

The previous result can be used to show the next lemma, whose straightforward proof is omitted.

Lemma 4. *Given a positive integer m, let*

$N_r^{(i,j)} = \#\{x \,|\, 0 \le x \le 2^m - 1, w(2^i + 2^j + x) = r + w(x)\}$*, where* $0 \le i < j \le m-1$*.*

Then $N_2^{(i,j)} = 2^{m-2}, N_r^{(i,j)} = 0$ *if* $r \ge 3$*. Further, if* $r = 1$*, then*

$$N_1^{(i,j)} = \begin{cases} 2^{m-2} + 2^{m-3}, & i+1 < j = m-1 \\ 2^{m-2}, & i+1 = j = m-1 \\ 2^{m-2}, & i+1 < j \le m-2 \\ 2^{m-3}, & i+1 = j \le m-2. \end{cases}$$

Finally, if $r = 0$*, then* $N_0^{(i,j)} = \begin{cases} 2^{m-3}+2^{m-4}, & i+2<j=m-1 \\ 2^{m-3}, & i+2=j=m-1 \\ 2^{m-2}, & i+1=j=m-1 \\ 2^{m-2}, & i+2<j=m-2 \\ 2^{m-3}+2^{m-4}, & i+2=j=m-2 \\ 2^{m-2}, & i+1=j=m-2 \\ 2^{m-3}+2^{m-4}, & i+2<j\le m-3 \\ 2^{m-3}, & i+2=j\le m-3 \\ 2^{m-3}+2^{m-4}, & i+1=j\le m-3. \end{cases}$

Similarly, as in the previous two lemmas, we have the next case.

Lemma 5. *Let* $N_r^{(i,j,l)} = \#\{x \,|\, 0 \le x \le 2^m-1, w(2^i+2^j+2^l+x) = r + w(x)\}$*, where* $0 \le i < j < l \le m-1$*. The following hold:*

1. *If* $r = 3$*,* $w(2^i+2^j+2^l+x) = 3+w(x) \Leftrightarrow x_i = x_j = x_l = 0$*; Further,* $N_3^{(i,j,l)} = 2^{m-3}$*.*

2. *If* $r = 2$*,* $w(2^i+2^j+2^l+x) = 2+w(x) \Leftrightarrow$

   $x_i = 0,\ x_j = 0,\ x_l = 1,\ x_{l+1} = 0$*;*
   or, $x_i = 0,\ x_j = 1,\ x_{j+1} = 0,\ x_l = 0\ (l > j+1)$*;*
   or, $x_i = 1,\ x_{i+1} = 0,\ x_j = 0,\ x_l = 0\ (j > i+1)$*.*

   Further, $N_2^{(i,j,l)} = \begin{cases} 2^{m-2}, & i+2<j+1<l=m-1 \\ 2^{m-3}+2^{m-4}, & i+2=j+1<l=m-1 \\ 2^{m-3}+2^{m-4}, & i+2<j+1=l=m-1 \\ 2^{m-3}, & i+2=j+1=l=m-1 \\ 2^{m-3}+2^{m-4}, & i+2<j+1<l\le m-2 \\ 2^{m-3}, & i+2=j+1<l\le m-2 \\ 2^{m-3}, & i+2<j+1=l\le m-2 \\ 2^{m-4}, & i+2=j+1=l\le m-2. \end{cases}$

3. *If* $r = 1$*,* $w(2^i+2^j+2^l+x) = 1+w(x) \Leftrightarrow$

   $x_i = 0,\ x_j = 0,\ x_l = 1,\ x_{l+1} = 1,\ x_{l+2} = 0\ (l \le m-2)$*;*
   or, $x_i = 0,\ x_j = 1,\ x_{j+1} = 1,\ x_{j+2} = 0,\ x_l = 0\ (l > j+2)$*;*
   or, $x_i = 0,\ x_j = 1,\ x_l = 1,\ x_{l+1} = 0\ (l = j+1)$*;*
   or, $x_i = 1,\ x_{i+1} = 1,\ x_{i+2} = 0,\ x_j = 0,\ x_l = 0\ (j > i+2)$*;*
   or, $x_i = 1,\ x_j = 0,\ x_{j+1} = 0,\ x_l = 0\ (j = i+1, l > j+1)$*;*
   or, $x_i = 0,\ x_j = 1,\ x_{j+1} = 0,\ x_l = 1,\ x_{l+1} = 0\ (l > j+1)$*;*
   or, $x_i = 1,\ x_{i+1} = 0,\ x_j = 0,\ x_l = 1,\ x_{l+1} = 0\ (j > i+1)$*;*
   or, $x_i = 1,\ x_{i+1} = 0,\ x_j = 1,\ x_{j+1} = 0,\ x_l = 0\ (l > j+1, j > i+1)$*.*

   Further,

$$N_1^{(i,j,m-1)} = \begin{cases} 2^{m-3}+2^{m-4}+2^{m-5}, & i+4<j+2<l=m-1 \\ 2^{m-3}+2^{m-4}, & i+4=j+2<l=m-1 \\ 2^{m-3}+2^{m-5}, & i+3=j+2<l=m-1 \\ 2^{m-3}+2^{m-4}, & i+4<j+2=l=m-1 \\ 2^{m-3}+2^{m-5}, & i+4=j+2=l=m-1 \\ 2^{m-3}, & i+3=j+2=l=m-1 \\ 2^{m-3}+2^{m-4}+2^{m-5}, & i+3<j+1=l=m-1 \\ 2^{m-3}+2^{m-4}, & i+3=j+1=l=m-1 \\ 2^{m-3}, & i+2=j+1=l=m-1 \end{cases}$$

$$N_1^{(i,j,m-2)} = \begin{cases} 2^{m-3}+2^{m-4}+2^{m-5}, & i+4<j+2<l=m-2 \\ 2^{m-3}+2^{m-4}, & i+4=j+2<l=m-2 \\ 2^{m-3}+2^{m-4}, & i+3=j+2<l=m-2 \\ 2^{m-3}+2^{m-4}, & i+4<j+2=l=m-2 \\ 2^{m-3}+2^{m-5}, & i+4=j+2=l=m-2 \\ 2^{m-3}+2^{m-5}, & i+3=j+2=l=m-2 \\ 2^{m-3}+2^{m-4}, & i+3<j+1=l=m-2 \\ 2^{m-3}+2^{m-5}, & i+3=j+1=l=m-2 \\ 2^{m-3}, & i+2=j+1=l=m-2, \end{cases}$$

$$N_1^{(i,j,l)} = \begin{cases} 2^{m-3}+2^{m-4}, & i+4<j+2<l\le m-3 \\ 2^{m-3}+2^{m-5}, & i+4=j+2<l\le m-3 \\ 2^{m-3}+2^{m-5}, & i+3=j+2<l\le m-3 \\ 2^{m-3}+2^{m-5}, & i+4<j+2=l\le m-3 \\ 2^{m-3}, & i+4=j+2=l\le m-3 \\ 2^{m-3}, & i+3=j+2=l\le m-3 \\ 2^{m-3}+2^{m-5}, & i+3<j+1=l\le m-3 \\ 2^{m-3}, & i+3=j+1=l\le m-3 \\ 2^{m-4}+2^{m-5}, & i+2=j+1=l\le m-3. \end{cases}$$

Since integers b will be uniquely determined by a in S_t, we will count the number of such a's. When $a \le t$, the counting strategy is different from that of $a > t$. Hence, we will partition the set of a's into two subsets:
Group I: $a = 0, 1, \ldots, t$, $b = t - a$;
Group II: $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, \ldots, 2^k - t - 2$.

In the following three sections, we will find the number of a's which satisfy $w(a) + w(b) \le k - 1$. For ease in writing and to distinguish between the above two groups, we let $\sigma := w(a) + w(t - a)$ corresponding to Group I, and we let $\Sigma := w(t + v) + w(2^k - 1 - v)$, corresponding to Group II. So, in Group II, the number of a will be equal to the number of v. The equation $\Sigma = k \pm r$ or $\sigma = k \pm r$ will usually be reduced to some cases of $w(2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} + x) = r + w(x)$ which have been discussed in this section (but we will consider the solutions only in Group I or II). In both groups, sometimes we directly count the number of solutions in S_t. Oftentimes, though, we get the number of solutions $\Sigma = k + r$ (or $\sigma = k + r$), $r \ge 0$, then subtract it from the corresponding group cardinality.

3. The Conjecture is True for $t = 2^i$ and $t = 2^j + 2^i$

Theorem 6. *We have* $\#S_t \leq 2^{k-1}$, $t = 2^i$, $0 \leq i \leq k-1$.

Proof. In Group II, $1 \leq v \leq 2^k - 2^i - 2$. So,

$$\Sigma = w(2^i + v) + k - w(v) \leq 1 + k.$$

Then

$$\Sigma = k + 1 \Leftrightarrow w(2^i + v) = 1 + w(v) \Leftrightarrow v_i = 0.$$

There are 2^{k-1} v, $0 \leq v \leq 2^k - 1$, with $v_i = 0$. When $v > 2^k - 2^i - 1$ then $v_i \neq 0$. Moreover, $v = 2^k - 2^i - 1$ and $v = 0$ are two solutions of the above equation. Hence, there are $2^{k-1} - 2$ v (or a) in Group II such that $\Sigma = 1 + k$. So, if $i = k - 1$, Group II makes no contributions to S_t (since all the $2^{k-1} - 2$ v's (or a's) make $\Sigma = 1 + k$). When $i \leq k - 2$,

$$\Sigma = k \Leftrightarrow w(2^i + v) = w(v) \Leftrightarrow v_i = 1, v_{i+1} = 0.$$

There are 2^{k-2} v, $0 \leq v \leq 2^k - 1$, such that $\Sigma = k$. When $v \geq 2^k - 2^i - 1$, $v_{i+1} = 1$, and 0 is not a solution of the above equation. Therefore, all v's such that $v_i = 1$ and $v_{i+1} = 0$ must be between 1 and $2^k - 2^i - 2$. Hence, there are 2^{k-2} a's such that $\Sigma = k$.

In summary, there are exactly $2^k - 2^i - 2 - (2^{k-1} - 2) - 2^{k-2} = 2^{k-2} - 2^i$ a's in S_t belonging to Group II when $i \leq k - 2$.

In Group I, $0 \leq a \leq t$. Let

$$\sigma = w(a) + w(2^i - 1 - (a - 1)) = w(a) + i - w(a - 1)$$
$$\begin{cases} = i + 1 & \text{if } a \equiv 1 \pmod 2 \\ \leq i & \text{if } a \equiv 0 \pmod 2, \end{cases}$$

which gives $\sigma \leq i + 1 \leq k - 1$ when $i \leq k - 2$. So when $i \leq k - 2$, All a's in Group I belong to S_t. But Group I contributes only $1 + \frac{t}{2} = 1 + 2^{k-2}$ to S_t if $i = k - 1$. Combining these two groups, we get $S_t = 1 + 2^{k-2} \leq 2^{k-1}$, always. $\square$

When the weight of t is increased by 1, the counting complexity increases significantly.

Theorem 7. *We have* $\#S_t \leq 2^{k-1}$ *when* $t = 2^i + 2^j$, $0 \leq i < j \leq k - 1$, $k \geq 4$.

Proof. We consider three cases:
`Case A`: $j \leq k - 3$.

In Group II ($1 \leq v \leq 2^k - 2^j - 2^i - 2$), let

$$\Sigma = w(2^i + 2^j + v) + w(2^k - 1 - v) = w(2^i + 2^j + v) + k - w(v) \leq 2 + k.$$

Further,

$$\Sigma = 2 + k \Leftrightarrow w(2^i + 2^j + v) = 2 + w(v) \Leftrightarrow v_i = v_j = 0.$$

Then, $v = 0$ and $v = 2^k - 2^j - 2^i - 1$ are two solutions. When $v > 2^k - 2^j - 2^i - 1$, then $v_i = 1$ or $v_j = 1$. Hence, we get $2^{k-2} - 2$ v (or a) such that $\Sigma = 2 + k$. (Note: This result will be reused in Case C). Next,

$$\Sigma = 1 + k \text{ if and only if } w(2^i + 2^j + v) = 1 + w(v),$$

if and only if

$$\begin{cases} v_i = 0 \quad v_j = 1 \quad v_{j+1} = 0 \\ \text{or,} \quad v_i = 1 \quad v_{i+1} = 0 \quad v_j = 0 \quad (j > i + 1) \end{cases}$$

by Lemma 4. Certainly, $v = 0$ is not a solution. If $v \geq 2^k - 2^j - 2^i - 1$, then v does not satisfy any of the above conditions. In other words, all solutions are between 1 and $2^k - 2^j - 2^i - 2$. Hence, there are exactly $\begin{cases} 2^{k-2}, & j > i + 1 \\ 2^{k-3}, & j = i + 1 \end{cases}$ a's such that $\Sigma = k + 1$.

Further, $\Sigma = k$ if and only if $w(2^i + 2^j + v) = w(v)$. It is easy to check that $v = 0$ is not a solution and any $v \geq 2^k - 2^j - 2^i - 1$ does not satisfy any condition of Lemma 4 when $r = 0$. Hence, there are exactly $N_0^{(i,j)}$ v such that $\Sigma = k$, where

$$N_0^{(i,j)} \geq \begin{cases} 2^{k-3} & j > i + 1 \\ 2^{k-3} + 2^{k-4} & j = i + 1. \end{cases}$$

It follows that there are at most

$$\begin{cases} 2^k - 2^j - 2^i - 2 - (2^{k-2} - 2) - 2^{k-2} - 2^{k-3}, & j > i + 1 \\ 2^k - 2^j - 2^i - 2 - (2^{k-2} - 2) - 2^{k-3} - (2^{k-3} + 2^{k-4}), & j = i + 1 \end{cases}$$

$= \begin{cases} 2^{k-1} - 2^j - 2^i - 2^{k-3}, & j > i + 1 \\ 2^{k-1} - 2^j - 2^i - 2^{k-4}, & j = i + 1 \end{cases}$ a's such that $\Sigma \leq k - 1$ in Group II.

In Group I there are only $t + 1 = 2^j + 2^i + 1$ a's. Thus,

$$\#S_t \leq \begin{cases} 2^{k-1} - 2^{k-3} + 1, & j > i + 1 \\ 2^{k-1} - 2^{k-4} + 1, & j = i + 1, \end{cases}$$

and so, $\#S_t \leq 2^{k-1}$, and case A is shown.

`Case B`: $j = k - 2$.

In Group II, $1 \leq v \leq 2^k - 2^{k-2} - 2^i - 2$. Let

$$\Sigma := w(2^{k-2} + 2^i + v) + k - w(v) \leq 2 + k.$$

First, if $\Sigma = 2+k$, then, as in Case A, we get exactly $2^{k-2} - 2$ a's such that $\Sigma = 2+k$. Secondly, if $\Sigma = 1 + k$, as in Case A, we get exactly $\begin{cases} 2^{k-2} & k - 2 > i + 1 \\ 2^{k-3} & k - 2 = i + 1 \end{cases}$ a's such that $\Sigma = 1 + k$.

If $\Sigma = k$, that is, $w(2^{k-2} + 2^i + v) = w(v)$, from Lemma 4 ($m = k$, $r = 0$), then the number of solutions with $0 \le v \le 2^k - 1$ is

$$\begin{cases} 2^{k-2}, & i+2 < j = k-2 \\ 2^{k-3} + 2^{k-4}, & i+2 = j = k-2 \\ 2^{k-2}, & i+1 = j = k-2. \end{cases}$$

The integers v satisfying the first condition in Lemma 4 are greater than $2^k - 2^{k-2} - 2^i - 1$. This means that there are 2^{k-3} many v (note that always $v_{j+2} = v_k = 0$) that should be excluded from the solutions of $\Sigma = k$. Hence, we get

$$\begin{cases} 2^{k-3}, & i+2 < k-2 \\ 2^{k-4}, & i+2 = k-2 \\ 2^{k-3}, & i+1 = k-2 \end{cases}$$

a's such that $\Sigma = k$.

In summary, the number of a's with $\Sigma \ge k$ is

$$\begin{cases} 2^{k-2} - 2 + 2^{k-2} + 2^{k-3}, & i+2 < k-2 \\ 2^{k-2} - 2 + 2^{k-2} + 2^{k-4}, & i+2 = k-2 \\ 2^{k-2} - 2 + 2^{k-3} + 2^{k-3}, & i+1 = k-2 \end{cases} = \begin{cases} 2^{k-1} - 2 + 2^{k-3}, & i+2 < k-2 \\ 2^{k-1} - 2 + 2^{k-4}, & i+2 = k-2 \\ 2^{k-1} - 2, & i+1 = k-2. \end{cases}$$

So, the number of a's in Group II with $\Sigma \le k-1$ is

$$\begin{cases} 2^k - 2^j - 2^i - 2 - (2^{k-1} - 2 + 2^{k-3}) = 2^{k-1} - 2^j - 2^i - 2^{k-3}, & i+2 < k-2 \\ 2^k - 2^j - 2^i - 2 - (2^{k-1} - 2 + 2^{k-4}) = 2^{k-1} - 2^j - 2^i - 2^{k-4}, & i+2 = k-2 \\ 2^k - 2^j - 2^i - 2 - (2^{k-1} - 2) = 2^{k-1} - 2^j - 2^i, & i+1 = k-2. \end{cases}$$

In Group I, there are only $t + 1 = 2^j + 2^i + 1$ a's. When $i + 1 = k - 2$, and $a = 2^{k-3} + 1$, we get $w(a) + w(t - a) = k$. Hence, combining all the a's in the Groups I and II, we get $\#S_t \le 2^{k-1}$, and Case B is shown.

`Case C`: $j = k - 1$.

In Group II, $1 \le v \le 2^{k-1} - 2^i - 2$. Let $\Sigma = w(2^{k-1} + 2^i + v) + k - w(v) \le 2 + k$.

If $\Sigma = 2 + k$, as in Case A, Group II, there are exactly $2^{k-2} - 2$ a's such that $\Sigma = 2 + k$.

Next, $\Sigma = 1 + k \Leftrightarrow w(2^{k-1} + 2^i + v) = 1 + w(v)$. By Lemma 4, we must have $k - 1 > i + 1$ (since $v_j = v_{k-1} = 1$ is impossible due to $v \le 2^k - 2^j - 2^i - 2 < 2^j$) and $v_i = 1$, $v_{i+1} = 0$, $v_{k-1} = 0$ (if $k - 1 > i + 1$). Certainly, $v = 0$ is not a solution. If $v \ge 2^k - 2^{k-1} - 2^i - 1 = (2^{k-1} - 1) - 2^i$, then v does not satisfy $v_i = 1$,$v_{i+1} = 0$, $v_{k-1} = 0$. So, there are exactly 2^{k-3} a's such that $\Sigma = 1 + k$ (only if $k - 1 > i + 1$).

Further, $\Sigma = k \Leftrightarrow w(2^{k-1} + 2^i + v) = w(v)$, $1 \le v \le 2^{k-1} - 2^i - 2$. By Lemma 4, we infer that $v_i = 1$, $v_{i+1} = 1$, $v_{i+2} = 0$, $v_{k-1} = 0$ ($k - 1 > i + 2$). $v \ge 2^{k-1} - 2^i - 1$ is impossible. So, there are exactly 2^{k-4} a's such that $\Sigma = k$ (only if $k - 1 > i + 2$). So, the number of a's with $\Sigma \ge k$ is

$$\begin{cases} 2^{k-2} - 2 + 2^{k-3} + 2^{k-4}, & i+2 < k-1 \\ 2^{k-2} - 2 + 2^{k-3}, & i+2 = k-1 \\ 2^{k-2} - 2, & i+1 = k-1. \end{cases}$$

In Group II, the number of a's that makes $\Sigma \le k-1$ is

$$\begin{cases} 2^{k-1}-2^i-2-(2^{k-2}-2+2^{k-3}+2^{k-4}) = 2^{k-4}-2^i, & i+2<k-1 \\ 2^{k-1}-2^i-2-(2^{k-2}-2+2^{k-3}) = 0, & i+2=k-1 \\ 2^{k-1}-2^i-2-(2^{k-2}-2) = 0, & i+1=k-1. \end{cases}$$

We now look at solutions from Group I. If $i = 0$ (call it, Case C_1), then $\sigma = w(a)+w(2^{k-1}+1-a) = w(a)+k-1-w(a-2) = k$ when $a \equiv 2, 3 \pmod 4$. So, there are at most $2^{k-2}+2$ a's between 0 and $t = 2^{k-1}+1$ such that $\sigma \le k-1$. Combining with the results in Group II, we get $\#S_t \le 2^{k-2}+2+2^{k-4}-2^0 = 2^{k-2}+2^{k-4}+1 \le 2^{k-1}$.

Now, we assume $i \ge 1$. If $i \ge 1$, $j = k-1 \ge i+2$ (Case C_2), then $\sigma = w(a)+w(2^{k-1}+2^i-a)$. When $0 \le a \le 2^i$, $\sigma = w(a)+1+w(2^i-a) = w(a)+1+i-w(a-1) \le i+2 \le k-1$. So, this contributes 2^i+1 a's to S_t. When $2^i+1 \le a \le 2^{k-1}+2^i$, then (let $x = a-2^i-1$, $0 \le x \le 2^{k-1}-1$)

$$\begin{aligned} \sigma &= w(a)+w(2^{k-1}-1-(a-2^i-1)) \\ &= w(a)+k-1-w(a-2^i-1) \\ &= w(x+2^i+1)+k-1-w(x) \le 1+k. \end{aligned}$$

First, if $\sigma = k+1 \Leftrightarrow w(x+2^i+1) = 2+w(x)$, there are exactly $2^{k-1-2} = 2^{k-3}$ x's (or a's).

If $\sigma = k \Leftrightarrow w(x+2^i+1) = 1+w(x)$, by Lemma 4 ($m = k-1$), then

$$\begin{cases} x_0 = 0, x_i = 1, x_{i+1} = 0 \\ x_0 = 1, x_1 = 0, x_i = 0 \ (i > 1). \end{cases}$$

The number of solutions x (or a) is $\begin{cases} 2^{k-3}, & 1 < i \le k-3 \\ 2^{k-4}, & 1 = i \le k-3 \end{cases}$. Hence, the number of a's with $\sigma \le k-1$ is

$$2^{k-1}-2^{k-3}-\begin{cases} 2^{k-3} & 1<i\le k-3 \\ 2^{k-4} & 1=i\le k-3 \end{cases} = \begin{cases} 2^{k-2}, & 1<i\le k-3 \\ 2^{k-2}+2^{k-4}, & 1=i\le k-3. \end{cases}$$

Putting all this together, in Group I, the number of a's in S_t is

$$\begin{cases} 2^{k-2}+2^i+1, & 1<i\le k-3 \\ 2^{k-2}+2^{k-4}+2^i+1, & 1=i\le k-3 \end{cases} \le \begin{cases} 2^{k-2}+2^{k-3}+1, & 1<i\le k-3 \\ 2^{k-2}+2^{k-3}+2^{k-4}+1, & 1=i\le k-3. \end{cases}$$

Combining these estimates with the ones from Group II, we get (in any case) $\#S_t \le 2^{k-1}$.

Finally, we assume that $j = k-1 = i+1$, that is, $j = k-1$ and $i = k-2$ (Case

C_3). When $0 \le a \le 2^{k-2}$, then

$$\begin{aligned}
\sigma &= w(a) + w(2^{k-1} + 2^{k-2} - a) \\
&= w(a) + 1 + w(2^{k-2} - a) \\
&= w(a) + 1 + k - 2 - w(a-1) \\
&= \begin{cases} k & a \equiv 1 \pmod 2 \\ \le k-1 & a \equiv 0 \pmod 2, \end{cases}
\end{aligned}$$

which contributes $1 + 2^{k-3}$ a's to S_t.

When $2^{k-2} + 1 \le a \le 2^{k-1} + 2^{k-2}$, then (let $x = a - 2^{k-2} - 1$, $0 \le x \le 2^{k-1} - 1$)

$$\begin{aligned}
\sigma &= w(a) + k - 1 - w(a - 2^{k-2} - 1) \\
&= w(x + 2^{k-2} + 1) + k - 1 - w(x) \le 1 + k.
\end{aligned}$$

First, as before, when $\sigma = k+1$, there are $2^{k-1-2} = 2^{k-3}$ x (or a).

Next, $\sigma = k$, that is, $w(x + 2^{k-2} + 1) = 1 + w(x)$, and as in Lemma 4 ($m = k-1$), we have $x_0 = 0$, $x_{k-2} = 1$; or, $x_0 = 1$, $x_1 = 0$, $x_{k-2} = 0$. Hence, the number of solutions is $2^{k-3} + 2^{k-4}$, if $1 < i = k-2$. Therefore, the number of a's in S_t is $2^{k-1} - 2^{k-3} - (2^{k-3} + 2^{k-4}) = 2^{k-3} + 2^{k-4}$, $1 < i = k-2$. Group I contributes $1 + 2^{k-3} + 2^{k-3} + 2^{k-4} = 2^{k-2} + 2^{k-4} + 1$ solutions to S_t.

Combining these estimates with the ones from Group II, we have

$$\#S_t \le 2^{k-2} + 2^{k-4} + 1 + 2^{k-4} - 2^i < 2^{k-1},$$

and this completes the proof of this theorem. □

4. The Conjecture is True for $t = 2^k - 2^i$ and $t = 2^k - 2^j - 2^i$

When $t = 2^k - 2^i$, i must be at least 1.

Theorem 8. *We have $\#S_t \le 2^{k-1}$, $t = 2^k - 2^i$, $1 \le i \le k-1$.*

Proof. In Group II, $1 \le v \le 2^i - 2$.

$$\begin{aligned}
\Sigma &= w(2^k - 2^i + v) + k - w(v) \\
&= 2k - w(2^i - v - 1) - w(v) = 2k - i \\
&\ge k + 1,
\end{aligned}$$

so, Group II makes no contributions to S_t.

We now look at Group I. If a is odd, then

$$\begin{aligned}
\sigma &= w(a) + w(2^k - 2^i - a) = w(a) + k - w(2^i + a - 1) \\
&\ge w(a) + k - (1 + w(a-1)) = k.
\end{aligned}$$

Hence, there are at most $\frac{1}{2}t + 1 = 2^{k-1} - 2^{i-1} + 1 \le 2^{k-1}$ a's with $w(a) + w(b) \le k-1$, and so, $\#S_t \le 2^{k-1}$. The proof is done. □

Theorem 9. *We have* $\#S_t \leq 2^{k-1}$, $t = 2^k - 2^j - 2^i$, $0 \leq i < j \leq k-1$.

Proof. In Group II, $1 \leq v \leq 2^j + 2^i - 2$.

$$\begin{aligned} \Sigma &= w(2^k - 2^j - 2^i + v) + k - w(v) \\ &= 2k - w(2^j + 2^i - v - 1) - w(v). \end{aligned}$$

If $1 \leq v \leq 2^i - 1$, then $\Sigma = 2k - 1 - w(2^i - 1 - v) - w(v) = 2k - 1 - i \geq k + 1$. If $2^i \leq v \leq 2^j + 2^i - 2$, then $\Sigma = 2k - w(2^j - 1 - (v - 2^i)) - w(v) = 2k - j + w(v - 2^i) - w(v) \geq 2k - j + w(v - 2^i) - (w(v - 2^i) + 1) = 2k - j - 1 \geq k$. Thus, Group II has no contributions to S_t.

We now look at Group I, and consider several cases.

`Case A`: $i = 0$.

$$\sigma = w(a) + w(2^k - 1 - (a + 2^j)) = w(a) + k - w(a + 2^j) \geq k - 1.$$

Next, if $\sigma = k - 1 \Leftrightarrow w(a + 2^j) = 1 + w(a)$, then there are at most 2^{k-1} such a's. Hence, $\#S_t \leq 2^{k-1}$.

`Case B`: $i = 1$. So, $t = 2^k - 2^j - 2 = 2^k - 1 - 2^j - 1$. Thus,

$$\sigma = w(a) + w(2^k - 1 - 2^j - 1 - a) = w(a) + k - w(2^j + 1 + a) \geq k - 2.$$

If $\sigma = k - 2 \Leftrightarrow w(1 + 2^j + a) = 2 + w(a)$, there are at most 2^{k-2} such a's.

If $\sigma = k - 1 \Leftrightarrow w(1 + 2^j + a) = 1 + w(a)$, there are at most 2^{k-2} such a's by Lemma 4. Consequently, $\#S_t \leq 2^{k-1}$.

`Case C`: $i > 1$ and $j \leq k - 2$. Then

$$\begin{aligned} \sigma &= w(a) + w(2^k - 2^j - 2^i - a) \\ &= w(a) + k - w(2^j + 2^i + a - 1) \\ &\geq w(a) + k - 2 - w(a - 1). \end{aligned}$$

If $a \equiv 1 \pmod 2$, then $\sigma \geq k - 1$.

Next, $\sigma = k - 1 \Leftrightarrow w(2^j + 2^i + a - 1) = 2 + w(a - 1) \Leftrightarrow (a-1)_i = (a-1)_j = 0$. Since $(a-1)_0 = 0$, there are at most 2^{k-3} a's that belong to S_t.

If $a \equiv 2 \pmod 4$, then $\sigma \geq w(a) + k - 2 - w(a - 1) = k - 2$.

Next, $\sigma = k - 2 \Leftrightarrow w(2^j + 2^i + a - 1) = 2 + w(a - 1)$, which is equivalent to $(a-1)_0 = 1, (a-1)_1 = 0, (a-1)_i = 0, (a-1)_j = 0$. Thus, there are at most 2^{k-4} such a's for a contribution to S_t.

Further, $\sigma = k - 1 \Leftrightarrow w(2^j + 2^i + a - 1) = 1 + w(a - 1)$, and by Lemma 4, there are at most 2^{k-4} such a's ($m = k$, $x = a - 1$, $(a-1)_0 = 1$, $(a-1)_1 = 0$).

Consequently, there are at most 2^{k-2} a's such that $a \equiv 0 \pmod 4$, even if all of them belong to S_t, and so, we obtain $\#S_t \leq 2^{k-3} + 2^{k-4} + 2^{k-4} + 2^{k-2} = 2^{k-1}$.

`Case D`: $i > 1$ and $j = k-1$, and so, $t = 2^{k-1} - 2^i$. Then

$$\begin{aligned} \sigma &= w(a) + w(2^{k-1} - 2^i - a) \\ &= w(a) + k - 1 - w(2^i + a - 1) \\ &\geq w(a) + k - 2 - w(a-1). \end{aligned}$$

When $a \equiv 1 \pmod 2$, $\sigma \geq k-1$, and $\sigma = k-1 \Leftrightarrow w(2^i + a - 1) = 1 + w(a-1) \Leftrightarrow (a-1)_0 = (a-1)_i = 0$. Therefore, there are at most $2^{k-1-2} = 2^{k-3}$ solutions to contribute to S_t.

When $a \equiv 2 \pmod 4$, $\sigma \geq k-2$, and
$\sigma = k-2 \Leftrightarrow w(2^i+a-1) = 1+w(a-1) \Leftrightarrow (a-1)_0 = 1$, $(a-1)_1 = 0$, $(a-1)_i = 1$. Therefore, there are at most $2^{k-1-3} = 2^{k-4}$ solutions.

Further, $\sigma = k-1 \Leftrightarrow w(2^i + a - 1) = w(a-1) \Leftrightarrow (a-1)_0 = 0$, $(a-1)_1 = 1$, $(a-1)_i = 1$, $(a-1)_{i+1} = 0$. There are at most $2^{k-1-4} = 2^{k-5}$ solutions to contribute to S_t.

Finally, there are at most 2^{k-2} $a \equiv 0 \pmod 4$, even if all of them belong to S_t, we still obtain $\#S_t \leq 2^{k-3} + 2^{k-4} + 2^{k-5} + 2^{k-2} < 2^{k-1}$. □

5. The Conjecture is True for $t = 2^k - 2^j - 2^i - 1$ and $t = 2^k - 2^l - 2^j - 2^i - 1$

Since the proofs require many counting arguments we split our result into two theorems.

Theorem 10. *We have $\#S_t \leq 2^{k-1}$, if $t = 2^k - 2^j - 2^i - 1$, $1 \leq i < j \leq k-1$.*

Proof. As before, for Group II, when $1 \leq v \leq 2^i$, then

$$\begin{aligned} \Sigma &= w(t+v) + k - w(v) = 2k - w(2^j + 2^i - v) - w(v) \\ &= 2k - (1 + w(2^i - v)) - w(v) \\ &= 2k - 1 - (i - w(v-1)) - w(v) \\ &= 2k - i - 1 + w(v-1) - w(v) \\ &\geq 2k - i - 1 - 1 \geq k. \end{aligned}$$

When $2^i + 1 \leq v \leq 2^j + 2^i - 1$, then (with $x = v - 2^i - 1$, $0 \leq x \leq 2^j - 2$)

$$\begin{aligned} \Sigma &= 2k - w(2^j + 2^i - v) - w(v) \\ &= 2k - w(2^j - 1 - (v - 2^i - 1)) - w(v) \\ &= 2k - j + w(x) - w(x + 2^i + 1) \\ &\geq 2k - j - 2. \end{aligned}$$

If $j \leq k-2$, then $\Sigma \geq k$.

If $j = k-1$, then $\Sigma \geq k-1$, $\Sigma = k-1$ if and only if $w(x+2^i+1) = 2+w(x)$. Thus, there are at most $2^{j-2} = 2^{k-3}$ many such x (v or a) contributing to S_t.

In Group I, $0 \leq a \leq 2^k - 2^j - 2^i - 1$, and

$$\sigma = w(a) + w(2^k - 2^j - 2^i - 1 - a) = w(a) + k - w(2^j + 2^i + a) \geq k-2.$$

`Case A`: $j \leq k-2$. Then $\sigma = k-2$ if and only if $w(2^j+2^i+a) = 2+w(a)$, and so, there are at most 2^{k-2} a's.

Next, $\sigma = k-1$ if and only if $w(2^j+2^i+a) = 1+w(a)$, and by Lemma 4, the number of such a's is at most 2^{k-2} and hence, $\#S_t \leq 0 + a^{k-2} + 2^{k-2} = 2^{k-1}$.

`Case B`: $j = k-1$. Then $\sigma = k-2$, and there are at most 2^{k-2} such a's.

Next, $\sigma = k-1 \Leftrightarrow w(2^j+2^i+a) = 1+w(a) \Leftrightarrow$ (as in Lemma 4) $a_i = 0$, $a_j = a_{k-1} = 1$, $a_{j+1} = 0$ or $a_i = 1$, $a_{i+1} = 0$, $a_j = 0$, ($j > i+1$). But $j = k-1$, $t < 2^{k-1}$, hence $a_j = 0$. It means that the first condition cannot be satisfied. So, there are at most 2^{k-3} such a's. Combining this estimate with the one from Group II, we have $\#S_t \leq 2^{k-3} + 2^{k-2} + 2^{k-3} = 2^{k-1}$, and the proof is done. $\square$

Theorem 11. *We have* $\#S_t \leq 2^{k-1}$, $t = 2^k - 2^l - 2^j - 2^i - 1$, $1 \leq i < j < l \leq k-1$.

Proof. We consider several cases.
<u>Case A</u>: $l \leq k-3$ ($k \geq l+3 \geq j+4 \geq i+5$).
In Group II, $1 \leq v \leq 2^l + 2^j + 2^i - 1$, and

$$\begin{aligned}
\Sigma &= w(t+v) + w(2^k - 1 - v) \\
&= w(2^k - 1 - (2^l + 2^j + 2^i) + v) + k - w(v) \\
&= 2k - w(2^l + 2^j + 2^i - v) - w(v).
\end{aligned}$$

If $1 \leq v \leq 2^i$, then

$$\begin{aligned}
\Sigma &= 2k - (2 + w(2^i - v)) - w(v) \\
&= 2k - 2 - w((2^i - 1) - (v-1)) - w(v) \\
&= 2k - 2 - i + w(v-1) - w(v) \\
&\geq 2k - 2 - i - 1 \geq k+2.
\end{aligned}$$

If $2^i + 1 \leq v \leq 2^j$, then

$$\begin{aligned}
\Sigma &= 2k - (1 + w(2^j + 2^i - v)) - w(v) \\
&= 2k - 1 - w(2^j - 1 - (v - 2^i - 1)) - w(v) \\
&= 2k - 1 - j + w(v - 2^i - 1) - w(v) \\
&\geq 2k - 1 - j - 2 \geq k+1.
\end{aligned}$$

If $2^j + 1 \le v \le 2^j + 2^i$, then

$$\begin{aligned}\Sigma &= 2k - (1 + w(2^j + 2^i - v)) - w(v) \\ &= 2k - 1 - w(2^i - 1 - (v - 2^j - 1)) - w(v) \\ &= 2k - 1 - i + w(v - 2^j - 1) - w(v) \\ &\geq 2k - 1 - i - 2 \geq k + 2.\end{aligned}$$

If $2^j + 2^i + 1 \le v \le 2^l + 2^j + 2^i - 1$, then

$$\begin{aligned}\Sigma &= 2k - w(2^l - 1 - (v - 2^j - 2^i - 1)) - w(v) \\ &= 2k - l + w(v - 2^j - 2^i - 1) - w(v) \\ &\geq 2k - l - 3 \geq k.\end{aligned}$$

Hence, Group II has no contributions to S_t.

In Group I, $\sigma = w(a) + k - w(2^l + 2^j + 2^i + a) \geq k - 3$.

First, if $\sigma = k - 3 \Leftrightarrow w(2^l + 2^j + 2^i + a) = 3 + w(a)$, there are at most 2^{k-3} such a's.

Next, if $\sigma = k - 2 \Leftrightarrow w(2^l + 2^j + 2^i + a) = 2 + w(a)$, there are at most $2^{k-3} + 2^{k-4}$ such a's by Lemma 5 (note that $m = k$ and $l \le k - 3$, $r = 2$).

Finally, if $\sigma = k - 1 \Leftrightarrow w(2^l + 2^j + 2^i + a) = 1 + w(a)$, there are at most $2^{k-3} + 2^{k-4}$ such a's by Lemma 5 ($r = 1$, $l \le k - 3$).

In summary, $\#S_t \le 2^{k-3} + 2^{k-3} + 2^{k-4} + 2^{k-3} + 2^{k-4} = 2^{k-1}$.

`Case B`: $l = k - 2$ ($k = l + 2 \geq j + 3 \geq i + 4$).

In Group II, by the proof of Case A, there are some a's which will contribute to S_t only if $2^j + 2^i + 1 \le v \le 2^l + 2^j + 2^i - 1$. Then

$$\begin{aligned}\Sigma &= 2k - w(2^l - 1 - (v - 2^j - 2^i - 1)) - w(v) \\ &= 2k - l + w(v - 2^j - 2^i - 1) - w(v) \\ &= 2k - l + w(x) - w(x + 2^j + 2^i + 1) \\ &\geq 2k - l - 3 = k - 1,\end{aligned}$$

where $x = v - 2^j - 2^i - 1$, $0 \le x \le 2^l - 2$. If $\Sigma = k - 1 \Leftrightarrow w(2^l + 2^j + 2^i + x) = 3 + w(x)$, there are at most $2^{l-3} = 2^{k-5}$ such a's.

In Group I, $\sigma = w(a) + k - w(2^l + 2^j + 2^i + a) \geq k - 3$.

If $\sigma = k - 3$, there are at most 2^{k-3} such a's.

If $\sigma = k - 2$, there are at most $2^{k-3} + 2^{k-4}$ such a's.

If $\sigma = k - 1 \Leftrightarrow w(2^l + 2^j + 2^l + a) = 1 + w(a)$, by Lemma 5, with $r = 1$, $m = k$, $l = k - 2$, we get $x_i = 0$, $x_j = 0$, $x_l = 1$, $x_{l+1} = 1$, $x_{l+2} = 0 \Leftrightarrow x_i = 0$, $x_j = 0$ $x_{k-2} = 1$, $x_{k-1} = 1 \Rightarrow x \geq 2^{k-1} + 2^{k-2} > t$, so, the number of solutions of $\sigma = k - 1$ should not include this 2^{k-4} many. That is, there are at most $2^{k-3} + 2^{k-5}$ a's such that $\sigma = k - 1$ by Lemma 5.

Combining Groups I and II, we get $\#S_t \le 2^{k-5} + 2^{k-3} + 2^{k-3} + 2^{k-4} + 2^{k-3} + 2^{k-5} = 2^{k-1}$.

Case C: $l = k-1$ $(k = l+1 \ge j+2 \ge i+3)$.

In Group II, by the proof of Case A, there are some a's which will make contributions to S_t, only if $2^i+1 \le v \le 2^j$ or $2^j+2^i+1 \le v \le 2^l+2^j+2^i-1$. If $2^i+1 \le v \le 2^j$,

$$\Sigma = 2k-1-j+w(v-2^i-1)-w(v) \ge 2k-1-j-2 \ge k-1.$$

First, $\Sigma = k-1$ implies that $w(v-2^i-1)-2 = w(v)$ and $j = k-2$. Let $x = v-2^i-1$, $0 \le x \le 2^j-2^i-1$. Then $w(x+2^i+1) = 2+w(x)$ has at most $2^{j-2} = 2^{k-4}$ solutions, so $\Sigma = k-1$ has at most 2^{k-4} solutions if $j = k-2$.

If $2^j+2^i+1 \le v \le 2^l+2^j+2^i-1$, then

$$\Sigma = 2k-l+w(v-2^j-2^i-1)-w(v) \ge k+1-3 = k-2.$$

Let $x = v-2^j-2^i-1$, $0 \le x \le 2^l-2 = 2^{k-1}-2$. If $\Sigma = k-2$ we get exactly $2^{k-1-3} = 2^{k-4}$ solutions. If $\Sigma = k-1$ then $w(x+2^j+2^i+1) = w(x)+2$, by Lemma 5 $(m = k-1)$, we get exactly $N_2^{(0,i,j)}$ solutions since 2^l-1 is not a solution. Recall that

$$N_2^{(0,i,j)} = \begin{cases} 2^{k-3}, & 2 < i+1 < j = k-2 \\ 2^{k-4}+2^{k-5}, & 2 = i+1 < j = k-2 \\ 2^{k-4}+2^{k-5}, & 2 < i+1 = j = k-2 \\ 2^{k-4}, & 2 = i+1 = j = k-2 \\ 2^{k-4}+2^{k-5}, & 2 < i+1 < j \le k-3 \\ 2^{k-4}, & 2 = i+1 < j \le k-3 \\ 2^{k-4}, & 2 < i+1 = j \le k-3 \\ 2^{k-5}, & 2 = i+1 = j \le k-3. \end{cases}$$

In Group I,

$$\sigma = w(a)+k-w(2^l+2^j+2^i+a) \ge k-3.$$

If $\sigma = k-3$, there are at most (in fact, exactly) 2^{k-3} solutions.

If $\sigma = k-2$, then $w(2^l+2^j+2^i+a) = w(a)+2$, and the first condition of Lemma 5 is satisfied $(r = 2)$, and we get $a_i = 0$, $a_j = 0$, $a_l = 1$, $a_{l+1} = 0 \Leftrightarrow a_i = 0$, $a_j = 0$, $a_{k-1} = 1 \Rightarrow a \ge 2^{k-1} > t$. That means 2^{k-3} a's should not be counted. So, the number of solutions of $\sigma = k-2$ is at most

$$\begin{cases} 2^{k-3}, & i+2 < j+1 < l = k-1 \\ 2^{k-4}, & i+2 = j+1 < l = k-1 \\ 2^{k-4}, & i+2 < j+1 = l = k-1 \\ 0, & i+2 = j+1 = l = k-1. \end{cases}$$

If $\sigma = k-1$, then $w(2^l+2^j+2^i+a) = w(a)+1$. By Lemma 5 $(r = 1)$, we obtain $a_i = 0$, $a_j = 1$, $a_l = 1$, $a_{l+1} = 0$ $(l = j+1) \Leftrightarrow a_i = 0$, $a_j = 1$, $a_{k-1} = 1 \Rightarrow a > 2^{k-1} > t$, so, there are 2^{k-3} a's which should not be counted for $l = j+1$.

The sixth condition of Lemma 5 implies $a_i = 0$, $a_j = 1$, $a_{j+1} = 0$, $a_{k-1} = 1$ $(l > j+1) \Rightarrow a > t$. There are 2^{k-4} a's which should not be counted for $l > j+1$.

The seventh condition of Lemma 5 implies $a_i = 1$, $a_{i+1} = 0$, $a_j = 0$, $a_{k-1} = 1$ $(j > i+1) \Rightarrow a > t$. There are 2^{k-4} a's which should not be counted for $j > i+1$. In summary, we get the number of solutions of $\sigma = k-1$ is at most

$$\begin{cases} 2^{k-4} + 2^{k-5}, & i+4 < j+2 < l = k-1 \\ 2^{k-4}, & i+4 = j+2 < l = k-1 \\ 2^{k-4} + 2^{k-5}, & i+3 = j+2 < l = k-1 \\ 2^{k-4}, & i+4 < j+2 = l = k-1 \\ 2^{k-5}, & i+4 = j+2 = l = k-1 \\ 2^{k-4}, & i+3 = j+2 = l = k-1 \\ 2^{k-5}, & i+3 < j+1 = l = k-1 \\ 0, & i+3 = j+1 = l = k-1 \\ 0, & i+2 = j+1 = l = k-1. \end{cases}$$

If $j \neq k-2$,that is, $j \leq k-3$, then

$$\#S_t \leq 2^{k-4} + 2^{k-4} + 2^{k-5} + 2^{k-3} + 2^{k-3} + 2^{k-4} + 2^{k-5} = 2^{k-1}.$$

If $j = k-2$, then

$$\#S_t \leq 2^{k-4} + 2^{k-4} + 2^{k-3} + 2^{k-3} + 2^{k-4} + 2^{k-5} = 2^{k-2} + 2^{k-3} + 2^{k-4} + 2^{k-5} < 2^{k-1}.$$

This completes the proof of our theorem. □

6. Further Remarks

We observe from our analysis that the counting heavily depends on the following quantity

$$N_r^{(i_1,i_2,\ldots,i_s)} = \#\{x \mid 0 \leq x \leq 2^k - 1, w(2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} + x) = r + w(x)\},$$

where $0 \leq i_1 < i_2 < \ldots < i_s \leq k-1$. Obviously, we have $N_r^{(i_1,i_2,\ldots,i_s)} = 0$ if $r > s$. We also have $N_r^{(i_1,i_2,\ldots,i_s)} = 0$ if $r \leq -k$. A general formula may be hard to obtain, but it could be interesting if a good upper and lower bound can be determined for given s and r.

Acknowledgement. The authors appreciate the referee's insightful and thorough comments which greatly improved the presentation of this paper.

References

[1] C. Carlet, *On a weakness of the Tu-Deng function and its repair*, Cryptology ePrint Archive, Report 2009/606, http://eprint.iacr.org/2009/606.pdf, 2009.

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

[3] Ziran Tu and Yingpu Deng, *A Conjecture on Binary String and Its Application on Constructing Boolean Functions of Optimal Algebraic Immunity*, Designs, Codes and Cryptography, to appear.

[4] Ziran Tu and Yingpu Deng, *A Class of* 1*–Resilient Function with High Nonlinearity and Algebraic Immunity*, Cryptology ePrint Archive, Report 2010/179, http://eprint.iacr.org/2010/179.pdf, 2010.