ON A COMBINATORIAL CONJECTURE

THOMAS W. CUSICK[1], YUAN LI[2*] AND PANTELIMON STĂNICĂ[3]

ABSTRACT. Recently, Tu and Deng [1] proposed a combinatorial conjecture on binary string, and, on the premise that the conjecture is correct they obtain two classes of Boolean functions which are both algebraic immunity optimal, the first of which are also bent functions. The second class are balanced functions, which have optimal algebraic degree and the best nonlinearity up to now. In this paper, from three different sides, we prove this conjecture is true in many cases with different counting strategies. We also propose some problems about the weight equations which is related to this conjecture. Because of the scattered distribution, we predict that a general counting is difficult to obtain.

1. INTRODUCTION

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

Conjecture 1.1. $S_t = \{(a,b)|a,b \in Z_{2^k-1}, a+b \equiv t \pmod{2^k-1}, w(a)+w(b) \leq k-1\}$, *where* $1 \leq t \leq 2^k-2, k \geq 2$. *Then, the cardinality* $\#S_t \leq 2^{k-1}$.

They validated the conjecture by computer for $k \leq 29$. Based on this conjecture, they constructed some classes of Boolean functions with many optimal cryptographic properties.

In this paper, we attack this conjecture, and prove it for many parameters, based on 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 $w(2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} + x) = r + w(x)$.

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 $t = 2^k - t'$, $w(t') \leq 2$ and t' is even. In Section 5, we prove the conjecture when $t = 2^k - t'$, $w(t') \leq 4$ 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 $0 \leq i_1 < i_2 < \ldots < i_s \leq k-1$.

2. PRELIMINARIES

Let x be an nonnegative integer, if the binary expansion of x is $x = x_0 + x_1 2 + x_2 2^2 + \cdots$, where $x_i \in \mathbb{F} = \{0,1\}$. Then we write $x = (x_0 x_1 ....)$. 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.

Key words and phrases. Boolean functions, Binary Strings, Hamming weights, Enumeration.
Mathematics Subject Classification: 14N10, 06E30.
* Corresponding author.

Lemma 2.1. *The following statements are true:*

$$w(2^k-1-x)=k-w(x),\ 0\le x\le 2^k-1;$$
$$w(x+2^i)\le w(x),\ \text{if } x_i=1;$$
$$w(x+y)\le w(x)+w(y),\ \text{with equality if and only if } x_i+y_i\le 1,\ \text{for any } i;$$
$$w(x)=w(x-1)-i+1, x\equiv 2^i \pmod{2^{i+1}},\ i=0,1,2,\ldots.$$

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 2.2. *When $0\le x\le 2^m-1$ and $0\le i<j\le m-1$, We have:*

(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 straightforward by considering the four possible values of x_i, x_j. □

The previous lemma can be used to show

Lemma 2.3. *Given a positive integer m, let*

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

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

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

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

Since integers b will be uniquely determined by a in S_t, we will count the number of such a's. We have two different groups of integers a, which will show up in the next few sections:
Group I: $a=0,1,\ldots,t$, $b=t-a$;
Group II: $a=t+v$, $b=2^k-1-v$, $v=1,2,\ldots,2^k-t-2$.

3. The conjecture is true for $t=2^i$ and $t=2^j+2^i$

We have

Theorem 3.1. *We have $\#S_t\le 2^{k-1}$, $t=2^i$, $0\le i\le k-1$.*

Proof. We split our analysis in two cases.
We first assume that $0 \le i \le k-2$. Look at Group II, $1 \le v \le 2^k - 2^i - 2$. Let

$$\Sigma := w(a) + w(b) = w(t+v) + w(2^k - 1 - v) = w(2^i + v) + k - w(v) \le 1 + k.$$

Then

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

There are 2^{k-1} many $0 \le v \le 2^k - 1$ with $v_i = 0$. When $v > 2^k - 2^i - 1$ then $v_i \neq 0$. Thus, $v = 2^k - 2^i - 1$ and $v = 0$ are two solutions of the above equation. Hence, there are $2^{k-1} - 2$ many v (or a) such that $\Sigma = 1 + k$.

Now,

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

There are 2^{k-2} many $0 \le v \le 2^k - 1$ such that $\Sigma = k$. When $v \ge 2^k - 2^i - 1$, $v_{i+1} = 1$, and 0 is not a solution of the above equation. Therefore, all the v 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} many a's such that $\Sigma = k$.

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

In Group I, $a = 0, 1, ..., t$. Let

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

which gives $\sigma \le k-1$. Combining these two groups, we get $\#S_t = 2^{k-2} - 2^i + 2^i + 1 = 2^{k-2} + 1 \le 2^{k-1}$.

We next assume that $i = k-1$. Group II ($1 \le v \le 2^{k-1} - 2$) makes no contributions to S_t, since

$$\Sigma = w(2^{k-1} + v) + k - w(v) = 1 + k.$$

In Group I,

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

Consequently, $\#S_t = 1 + \frac{t}{2} = 1 + 2^{k-2} \le 2^{k-1}$, and the proof of the theorem is done. □

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

Theorem 3.2. *We have $\#S_t \le 2^{k-1}$ when $t = 2^i + 2^j$, $0 \le i < j \le k-1$, $k \ge 4$.*

Proof. Recall that: Group I: $a = 0, 1, 2..., t$, $t = 2^i + 2^j$;
Group II: $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, ..., 2^k - 2^j - 2^i - 2$.

We first assume that $j \le k-3$ (Case A). In Group II, let

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

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 $2^{k-2} - 2$ many v (or a) such that $\Sigma = 2 + k$. Next, $\Sigma = 1 + k \Leftrightarrow$

$w(2^i+2^j+v)=1+w(v) \Leftrightarrow \left\{\begin{array}{ll} v_i=0 \quad v_j=1 \quad v_{j+1}=0 \\ \text{or,} \quad v_i=1 \quad v_{i+1}=0 \quad v_j=0 \quad (j>i+1)\end{array}\right.$ by Lemma 2.3.
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 $\left\{\begin{array}{ll} 2^{k-2}, & j>i+1 \\ 2^{k-3}, & j=i+1\end{array}\right.$ many a's such that $\Sigma=k+1$.

Further, $\Sigma=k \Leftrightarrow w(2^i+2^j+v)=w(v)$. 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 2.3 when $r=0$. Hence, there are exactly $N_0^{(i,j)}$ many v such that $\Sigma=k$, where

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

Hence, there are at most $\left\{\begin{array}{ll} 2^k-2^j-2^i-2-(2^{k-2}-2)-2^{k-2}-2^{k-3}, & j>i+1 \\ 2^k-2^j-2^i-2-(2^{k-2}-2)-2^{k-3}-(2^{k-3}+2^{k-4}), & j=i+1\end{array}\right.$
$=\left\{\begin{array}{ll} 2^{k-1}-2^j-2^i-2^{k-3} & j>i+1 \\ 2^{k-1}-2^j-2^i-2^{k-4} & j=i+1\end{array}\right.$ many a's such that $\Sigma \leq k-1$ in Group II. In Group I there are only $t+1=2^j+2^i+1$ many a. Thus,

$$\#S_t \leq \left\{\begin{array}{ll} 2^{k-1}-2^{k-3}+1, & j>i+1 \\ 2^{k-1}-2^{k-4}+1, & j=i+1\end{array}\right. \leq 2^{k-1}.$$

Case A has been proved.

Assume next that $j=k-2$ (Case B). In Group II, $v=1,2,\ldots,2^k-2^{k-2}-2^i-2$. 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 $2^{k-2}-2$ many a's such that $\Sigma=2+k$. Secondly, if $\Sigma=1+k$, as in Case A, we get exactly $\left\{\begin{array}{ll} 2^{k-2} & k-2>i+1 \\ 2^{k-3} & k-2=i+1\end{array}\right.$ many a's such that $\Sigma=1+k$. If $\Sigma=k$, that is, $w(2^{k-2}+2^i+v)=w(v)$, from Lemma 2.3($m=k$, $r=0$), then the number of solutions of all the v between 0 and 2^k-1 is

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

All the integers v satisfying the first condition in Lemma 2.3 are greater than $2^k-2^{k-2}-2^i-1$. This means that there are 2^{k-3} (please note that always $v_{j+2}=v_k=0$) many v that should be excluded from the solutions of $\Sigma=k$. Hence, we get

$$\left\{\begin{array}{ll} 2^{k-3} & i+2<k-2 \\ 2^{k-4} & i+2=k-2 \\ 2^{k-3} & i+1=k-2.\end{array}\right.$$

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

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

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

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 $t+1=2^j+2^i+1$ many 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 proved.

Next, we assume that $j=k-1$ (Case C). Look at 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, there are exactly $2^{k-2}-2$ many a's such that $\Sigma = 2+k$. Next, $\Sigma = 1+k \Leftrightarrow w(2^{k-1}+2^i+v)=1+w(v)$. By Lemma 2.3, 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} many 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 2.3, 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} many 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 solution 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 $2^{k-2}+2$ many 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 $\sigma = w(a)+w(t-a)=w(a)+w(2^{k-1}+2^i-a)$. 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 many 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 $2^{k-1-2}=2^{k-3}$ many x's (or a's). If $\sigma = k \Leftrightarrow w(x+2^i+1=1+w(x)$, by Lemma 2.3 ($m=k-1$), 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 solution 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 that $\sigma \le k-1$ 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 $1+2^{k-3}$ many 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 $2^{k-1-2}=2^{k-3}$ many x (or a). Next, $\sigma=k$, that is, $w(x+b^{k-2}+1)=1+w(x)$, and as in Lemma 2.3($m=k-1$), we have $x_0=0$, $x_{k-2}=1$; or, $x_0=1$, $x_1=0$, $x_{k-2}=0$. which gives that the number of solutions is $2^{k-3}+2^{k-4}$, if $1<i=k-2$.

Hence, 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 $1+2^{k-3}+2^{k-3}+2^{k-4}=2^{k-2}+2^{k-4}+1$ many 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 $t=2^k-2^j-2^i$

Theorem 4.1. *We have $\#S_t\le 2^{k-1}$, $t=2^k-2^i$, $1\le i\le k-1$.*

Proof. Under our assumption, Group I includes $a=0,1,\ldots,t$; and Group II includes $a=t+1,\ldots,2^k-2$, that is, $a=t+v$, $b=2^k-1-v$, $v=1,2,\ldots,2^i-2$.

In Group II,

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

so, Group II makes no contributions to S_t.

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

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

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

Theorem 4.2. *We have* $\#S_t \le 2^{k-1}$, $t = 2^k - 2^j - 2^i$, $1 \le i < j \le k-1$.

Proof. Under our assumption, Group I includes $a = 0, 1, \ldots, t$; and Group II includes $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, \ldots, 2^j + 2^i - 2$.

In Group II,

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

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

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

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

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

If $\sigma = k - 2 \Leftrightarrow w(1 + 2^j + a) = 2 + w(a)$, there are at most 2^{k-2} many such a's. If $\sigma = k - 1 \Leftrightarrow w(1 + 2^j + a) = 1 + w(a)$, there are at most 2^{k-2} many such a's by Lemma 2.3. Consequently, $\#S_t \le 2^{k-1}$.

Case B: $i > 1$ and $j \le k - 2$. Then

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

If $a \equiv 1 \pmod 2$, then $\sigma \ge k - 1$. 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} many a's belongs to S_t.

If $a \equiv 2 \pmod 4$, then $\sigma \ge w(a)+k-2-w(a-1) = k-2$. 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} many 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 2.3, there are at most 2^{k-4} many such a's ($m = k$, $x = a - 1$, $(a-1)_0 = 1$, $(a-1)_1 = 0$).

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

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

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

When $a \equiv 1 \pmod 2$, $\sigma \ge k - 1$, 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 $2^{k-1-2} = 2^{k-3}$ many solutions to contribute to S_t.

When $a \equiv 2 \pmod 4$, $\sigma \ge k-2$, 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 $2^{k-1-3} = 2^{k-4}$ many solutions.

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

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

5. The conjecture is true for $t = 2^k - 2^i - 1$, $t = 2^k - 2^j - 2^i - 1$ and $t = 2^k - 2^l - 2^j - 2^i - 1$

Since the proofs require many counting arguments we split our result in several theorems.

Theorem 5.1. *We have* $\#S_t \le 2^{k-1}$, *if* $t = 2^k - 2^i - 1$, $0 \le i \le k - 1$.

Proof. Recall that Group I includes $0 \le a \le t$; Group II includes $a = t + v$, $b = 2^k - 1 - v$, $v = 1, \ldots, 2^i - 1$.

For Group II, $\Sigma = w(t+v)+k-w(v) = w(2^k-1-(2^i-v))+k-w(v) = 2k-w(2^i-v)-w(v) = 2k - i + w(v-1) - w(v) \ge 2k - i - 1 \ge k$.

For Group I, $\sigma = w(a)+w(t-a) = w(a)+w(2^k-1-(a+2^i)) = w(a)+k-w(a+2^i) \ge k-1$. Next, if $\sigma = k-1 \Leftrightarrow w(a+2^i) = 1 + w(a)$, then there are at most 2^{k-1} many such a's. Hence, $\#S_t \le 2^{k-1}$. □

Theorem 5.2. *We have $\#S_t \le 2^{k-1}$, if $t = 2^k - 2^j - 2^i - 1$, $1 \le i < j \le k-1$.*

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

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

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

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

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

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

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

Case A: $j \le k-2$; Then $\sigma = k-2 \Leftrightarrow w(2^j + 2^i + a) = 2 + w(a)$, and so, there are at most 2^{k-2} many a's. Next, $\sigma = k-1 \Leftrightarrow w(2^j + 2^i + a) = 1 + w(a)$, and by Lemma 2.3, the number of such a's is at most 2^{k-2}. Hence, $\#S_t \le 0 + a^{k-2} + 2^{k-2} = 2^{k-1}$.

Case B: $j = k-1$; Then $\sigma = k-2$, and there are at most 2^{k-2} many such a's. Next, $\sigma = k-1 \Leftrightarrow w(2^j + 2^i + a) = 1 + w(a) \Leftrightarrow$ (as in Lemma 2.3) $a_i = 0$, $a_j = a_{k-1} = 1$, $a_{j+1} = 0$ 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} many such a's. Combining this estimate with the one from Group II, we have $\#S_t \le 2^{k-3} + 2^{k-2} + 2^{k-3} = 2^{k-1}$, and the proof is done. □

Before proving our last theorem, we need a lemma.

Lemma 5.3. *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,

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

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

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

Proof. We omit this straightforward and slightly tedious proof. □

Theorem 5.4. *We have* $\#S_t \le 2^{k-1}$, $t = 2^k - 2^l - 2^j - 2^i - 1$, $1 \le i < j < l \le k-1$.

Proof. Under our assumptions, Group I includes $0 \le a \le t$; and Group II includes $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, \ldots, 2^l + 2^j + 2^i - 1$. We consider several cases.

Case A: $l \le k-3$ ($k \ge l+3 \ge j+4 \ge i+5$). In Group II,

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

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

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

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

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

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

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

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

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

Hence, Group II has no contributions to S_t.

In Group I, $\sigma = w(a) + w(t-a) = w(a) + k - w(2^l + 2^j + 2^i + a) \ge k - 3$. First, if $\sigma = k - 3 \Leftrightarrow w(2^l + 2^j + 2^i + a) = 3 + w(a)$, there are at most 2^{k-3} many such a's. Next, if $\sigma = k - 2 \Leftrightarrow w(2^l + 2^j + 2^i + a) = 2 + w(a)$, there are at most $2^{k-3} + 2^{k-4}$ many such a's by Lemma 5.3 (please 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 $2^{k-3} + 2^{k-4}$ many such a's by Lemma 5.3($r = 1$, $l \le k-3$).

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: $l = k-2$ ($k = l+2 \ge j+3 \ge i+4$). 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

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

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 $2^{l-3} = 2^{k-5}$ many such a's.

In Group I, $\sigma = w(a) + w(t-a) = w(a) + k - w(2^l + 2^j + 2^i + a) \ge k - 3$. If $\sigma = k-3$, there are at most 2^{k-3} many such a's. If $\sigma = k-2$, there are at most $2^{k-3} + 2^{k-4}$ many such a's. If $\sigma = k-1 \Leftrightarrow w(2^l + 2^j + 2^l + a) = 1 + w(a)$, by Lemma 5.3, with $r = 1$, $m = k$, $l = k-2$, we get $x_i = 0$, $x_j = 0$, $x_l = 1$, $x_{l+1} = 1$, $x_{l+2} = 0 \Leftrightarrow x_i = 0$, $x_j = 0$ $x_{k-2} = 1$, $x_{k-1} = 1$ $\Rightarrow x \ge 2^{k-1} + 2^{k-2} > t$, so, the number of solutions of $\sigma = k-1$ should not include this 2^{k-4} many. That is, there are at most $2^{k-3} + 2^{k-5}$ many a's such that $\sigma = k-1$ by Lemma 5.3.

Combine Groups I and II, and 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 in Case A, there are some a's 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 $2^i + 1 \le v \le 2^j$,

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

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 $2^{j-2} = 2^{k-4}$ many solutions, so $\Sigma = k-1$ has at most 2^{k-4} many solutions if $j = k-2$.

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

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

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 at most (in fact, exactly) $2^{k-1-3} = 2^{k-4}$ many solutions. If $\Sigma = k-1$ then $w(x + 2^j + 2^i + 1) = w(x) + 2$, by Lemma 5.3 ($m = k-1$), we get exactly $N_2^{(0,i,j)}$ many 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,

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

If $\sigma = k-3$, there are at most (in fact, exactly) 2^{k-3} many solutions. If $\sigma = k-2$, then $w(2^l + 2^j + 2^i + a) = w(a) + 2$, and the first condition of Lemma 5.3 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} many 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 5.3 ($r = 1$), 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} many a's which should not be counted for $l = j+1$.

The sixth condition of Lemma 5.3 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} many a's which should not be counted for $l > j+1$.

The seventh condition of Lemma 5.3 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} many 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

As we see, the counting heavily depends on the following quantity

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

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.

References

[1] Ziran Tu and Yingpu Deng, A Conjecture on Binary String and Its Application on Constructing Boolean Functions of Optimal Algebraic Immunity, http://eprint.iacr.org/2009/272.pdf

[1]State University of New York, Department of Mathematics, Buffalo, NY 14260, USA; Email: cusick@buffalo.edu

[2]Mathematics Department, WSSU, NC 27110,USA; Email: yuanli7983@gmail.com

[3]Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA; Email: pstanica@nps.edu