ON A COMBINATORIC CONJECTURE

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

Abstract. Recently, Tu and Deng [1] proposed a combinatorial conjecture on binary string, on the premise that the conjecture is correct they obtain two classes of Boolean functions which are both algebraic immunity optimal: the first class of functions are also bent. 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. *$S_t = \{(a,b)|a,b \in Z_{2^k-1}, a+b \equiv t \pmod{2^k-1}, w(a)+w(b) \le k-1\}$, where $1 \le t \le 2^k-2, k \ge 2$. Then $\#S_t \le 2^{k-1}$.*

They validated the conjecture by computer when $k \le 29$. Based on this conjecture, they constructed many impressive Boolean functions with many optimal cryptographic properties.

In this paper, we try to attack this conjecture from different ways. We proved the conjecture is true in many cases based on the binary weight of t. We found the distribution of the pairs in S_t is very scattered. The counting complexity increase directly with the wight of t. On the other hand, if we write t as $2^k - t'$, the counting complexity increase directly with t'. Besides, the behavior is quite different according to t' is even or odd. We also found the counting is heavily dependent on the number of solutions of the equation. $w(2^{i_1} + 2^{i_2} + ... + 2^{i_s} + x) = r + w(x)$.

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 sequel. In Section 3, we prove the conjecture is true when $w(t)$ is 1 or 2. In Section 4 we prove the conjecture when $t = 2^k - t'$, $w(t') \le 2$ and t' is even. In Section 5, we prove the conjecture when $t = 2^k - t'$, $w(t') \le 4$ and t' is odd. In Section 6, we give some open questions about the number of solutions of $w(2^{i_1} + 2^{i_2} + ... + 2^{i_s} + x) = r + w(x)$, where $0 \le x \le 2^k - 1$ and $0 \le i_1 < i_2 ... < i_s \le k-1$.

2. Preliminaries

Let x be an nonnegative integer, if $x = x_0 + x_1 2 + x_2 2^2 + ...$, where $x_i = 0, 1$. Then we write $x = (x_0 x_1 ....)$. The nonzero number of x_i will be called the weight of x and written as $w(x)$. Obviously, we have the following facts. For conveniences, we write them as lemmas.

Lemma 2.1. *$w(2^k - 1) = k$.*

Lemma 2.2. *If $0 \le x \le 2^k - 1$, then $w(2^k - 1 - x) = k - w(x)$.*

Lemma 2.3. *$w(x + 2^i) \le w(x)$ if $x_i = 1$.*

Key words and phrases. Boolean function, Binary String, Counting. MSC:14N10 06E30.

* Corresponding author.

Lemma 2.4. *Triangle inequality,* $w(x+y) \le w(x)+w(y)$. *The equation holds if and only if* $x_i + y_i \le 1$ *for any* i.

Lemma 2.5. $w(x) = w(x-1) - i + 1$, $x \equiv 2^i \pmod{2^{i+1}}$, $i = 0, 1, 2, ...$

This lemma means $w(x) = w(x-1)+1$ if x is odd, $w(x) = w(x-1)$ if $x \equiv 2 \pmod 4$, $w(x) = w(x-1)-1$ if $x \equiv 4 \pmod 8$ and etc. For two consecutive integers, the weight of the even one is never greater than that of the odd one.

Lemma 2.6. *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 $N_r^{(i,j)} = 0$ *if* $r \ge 3$.
$N_2^{(i,j)} = 2^{m-2}$.
If $r = 1$, $w(x + 2^i + 2^j) = 1 + w(x) \Leftrightarrow$
$$\begin{cases} x_i = 0 \quad x_j = 1 \quad x_{j+1} = 0 \\ or \quad x_i = 1 \quad x_{i+1} = 0 \quad x_j = 0 \quad (j > i+1) \end{cases}$$
Hence,
$$N_1^{(i,j)} = \begin{cases} 2^{m-2} + 2^{m-3} & i+1 < j = m-1 \\ 2^{m-2} & i+1 = j = m-1 \\ 2^{m-2} & i+1 < j \le m-2 \\ 2^{m-3} & i+1 = j \le m-2 \end{cases}.$$
If $r = 0$ $w(x + 2^i + 2^j) = w(x) \Leftrightarrow$
$$\begin{cases} x_i = 0 \quad x_j = 1 \quad x_{j+1} = 1 \quad x_{j+2} = 0 (j < m-1) \\ or \quad x_i = 1 \quad x_{i+1} = 1 \quad x_{i+2} = 0 \quad x_j = 0 (j > i+2) \\ or \quad x_i = 1 \quad x_{i+1} = 0 \quad x_j = 1 \quad x_{j+1} = 0 (j > i+1) \\ or \quad x_i = 1 \quad x_j = 1 \quad x_{j+1} = 0 \quad (j = i+1) \end{cases}$$
Hence,
$$N_0^{(i,j)} = \begin{cases} 2^{m-3} + 2^{m-4} & i+2 < j = m-1 \\ 2^{m-3} & i+2 = j = m-1 \\ 2^{m-2} & i+1 = j = m-1 \\ 2^{m-2} & i+2 < j = m-2 \\ 2^{m-3} + 2^{m-4} & i+2 = j = m-2 \\ 2^{m-2} & i+1 = j = m-2 \\ 2^{m-3} + 2^{m-4} & i+2 < j = m-3 \\ 2^{m-3} & i+2 = j = m-3 \\ 2^{m-3} + 2^{m-4} & i+1 = j = m-3 \end{cases}$$

The proof of the above lemma is straightforward by considering the four possible values of x_i, x_j. We omit it.

Since the b will be uniquely determined by a in S_t, we will count the number of a which satisfy the conditions of the set S_t. Actually, we have two different groups of a.

Group I: $a = 0, 1, ...t$, $b = t - a$.

Group II: $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, ...2^k - t - 2$.

3. $t = 2^i$ AND $t = 2^j + 2^i$

In this section, we prove the conjecture is true when $t = 2^i$ and $t = 2^i + 2^j$. We have

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

Proof. Case A: $0 \le i \le k-2$

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

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

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

$\Sigma = k \Leftrightarrow w(2^i+v) = w(v) \Leftrightarrow v_i = 1, v_{i+1} = 0$. There are 2^{k-2} many v between 0 and 2^k-1 such that $\Sigma = k$. When $v \geq 2^k - 2^i - 1$, $v_{i+1} = 1$. 0 is not a solution of the above equation. So, 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 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 is S_t in Group II.

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

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

Combine these two groups. We get $\#S_t = 2^{k-2} - 2^i + 2^i + 1 = 2^{k-2} + 1 \leq 2^{k-1}$.

Case B: $i = k-1$

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

$\Sigma = w(2^{k-1} + v) + k - w(v) = 1 + k$, so, Group II makes no contributions to S_t.

In Group I

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

So, $\#S_t = 1 + \frac{t}{2} = 1 + 2^{k-2} \leq 2^{k-1}$. We finish the proof of this theorem.

□

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

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

Proof. Group I: $a = 0, 1, 2..., t$, $t = 2^i + 2^j$.

Group II: $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, ..., 2^k - 2^j - 2^i - 2$.

Case A: $j \leq k-3$

In Group II

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

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

$v = 0$ 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 $\Sigma = 2 + k$.

$\Sigma = 1 + k \Leftrightarrow w(2^i + 2^j + v) = 1 + w(v) \Leftrightarrow \begin{cases} v_i = 0 \quad v_j = 1 \quad v_{j+1} = 0 \\ \text{or} \quad v_i = 1 \quad v_{i+1} = 0 \quad v_j = 0 \quad (j > i+1) \end{cases}$

by Lemma 2.6. $v = 0$ is not a solution. $v \geq 2^k - 2^j - 2^i - 1$, 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 $\begin{cases} 2^{k-2} & j > i+1 \\ 2^{k-3} & j = i+1 \end{cases}$ many a such that $\Sigma = k+1$

$\Sigma = k \Leftrightarrow w(2^i + 2^j + v) = w(v)$

It is easy to check that $v = 0$ is not a solution and $v \geq 2^k - 2^j - 2^i - 1$ do not satisfy any condition of Lemma 2.6 when $r = 0$. Hence, there are exactly $N_0^{(i,j)}$ many v such that $\Sigma = k$.

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

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

$\begin{cases} 2^{k-1}-2^j-2^i-2^{k-3} & j>i+1 \\ 2^{k-1}-2^j-2^i-2^{k-4} & j=i+1 \end{cases}$ many a such that $\Sigma \le k-1$ in Group II. Group I has only $t+1=2^j+2^i+1$ many a. So,

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

Case A has been proved.

Case B: $j=k-2$

In Group II, $v=1,2,...,2^k-2^{k-2}-2^i-2$.

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

$\Sigma = 2+k$, same to Case A, get exactly $2^{k-2}-2$ many a such that $\Sigma = 2+k$.

$\Sigma = 1+k$, same to Case A, get exactly $\begin{cases} 2^{k-2} & k-2>i+1 \\ 2^{k-3} & k-2=i+1 \end{cases}$ many a such that $\Sigma = 1+k$.

$\Sigma = k$, i.e., $w(2^{k-2}+2^i+v)=w(v)$, From Lemma 2.6($m=k$, $r=0$), the number of solutions of all the v between 0 and 2^k-1 is $\begin{cases} 2^{k-2} & i+2<j=k-2 \\ 2^{k-3}+2^{k-4} & i+2=j=k-2 \\ 2^{k-2} & i+1=j=k-2 \end{cases}$. All the v that satisfy the first condition in the Lemma 2.6 are greater than $2^k-2^{k-2}-2^i-1$. This means there are 2^{k-3}(Please note $v_{j+2}=v_k=0$ always) many v should be excluded from the solution of $\Sigma = k$. Hence, we get

$\begin{cases} 2^{k-3} & i+2<k-2 \\ 2^{k-4} & i+2=k-2 \\ 2^{k-3} & i+1=k-2 \end{cases}$ many a such that $\Sigma = k$.

In summary, the number of a that $\Sigma \ge k$ 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 in Group II that $\Sigma \le k-1$ 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. When $i+1=k-2$, let $a=2^{k-3}+1$, we get $w(a)+w(t-a)=k$. Hence, combine all the a in two Groups, we get $\#S_t \le 2^{k-1}$.

We finish the proof of Case B.

Case C: $j=k-1$

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

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

$\Sigma = 2+k$, same to Case A, there are exactly $2^{k-2}-2$ many a such that $\Sigma = 2+k$.

$\Sigma = 1+k \Leftrightarrow w(2^{k-1}+2^i+v)=1+w(v)$. Check Lemma 2.6, 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 $k-1>i+1$). $v=0$ 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 such that $\Sigma = 1+k$ (only if $k-1>i+1$).

$\Sigma = k \Leftrightarrow w(2^{k-1}+2^i+v)=w(v)$, $1 \le v \le 2^{k-1}-2^i-2$. Check Lemma 2.6, it means

$v_i=1$ $v_{i+1}=1$ $v_{i+2}=0$ $v_{k-1}=0$ ($k-1>i+2$). $v \ge 2^{k-1}-2^i-1$ is impossible. So, there are exactly 2^{k-4} many a such that $\Sigma = k$ (only if $k-1>i+2$). So, the number such that $\Sigma \ge k$ 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 that makes $\Sigma \le k-1$ is

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

In Group I

Case C1 $i=0$

$\sigma = w(a)+w(2^{k-1}+1-a) = w(a)+k-1-w(a-2) = k$ when $a \equiv 2,3 \pmod 4$. So, there are at most $2^{k-2}+2$ many a between 0 and $t=2^{k-1}+1$ such that $\sigma \le k-1$. Combine with the results in Group II, we get $\#S_t \le 2^{k-2}+2+2^{k-4}-2^0 = 2^{k-2}+2^{k-4}+1 \le 2^{k-1}$. Hence, let's assume $i \ge 1$.

Case C2: $i \ge 1$, $j = k-1 \ge i+2$

$\sigma = w(a)+w(t-a) = w(a)+w(2^{k-1}+2^i-a)$.

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 to S_t.

When $2^i+1 \le a \le 2^{k-1}+2^i$

$\sigma = w(a)+w(2^{k-1}-1-(a-2^i-1)) = w(a)+k-1-w(a-2^i-1)$

(Let $x = a-2^i-1$, $0 \le x \le 2^{k-1}-1$)

$= w(x+2^i+1)+k-1-w(x) \le 1+k$.

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

$\sigma = k \Leftrightarrow w(x+2^i+1 = 1+w(x)$, by Lemma 2.6, $(m=k-1)$

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

The number of solution of 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 that $\sigma \le k-1$ is $2^{k-1}-2^{k-3}-\begin{cases} 2^{k-3} & 1<i\le k-3 \\ 2^{k-4} & 1=i\le k-3 \end{cases} = \begin{cases} 2^{k-2} & 1<i\le k-3 \\ 2^{k-2}+2^{k-4} & 1=i\le k-3 \end{cases}$.

Totally, in Group I, the number of a in S_t is

$$\begin{cases} 2^{k-2}+2^i+1 & 1<i\le k-3 \\ 2^{k-2}+2^{k-4}+2^i+1 & 1=i\le k-3 \end{cases} \le \begin{cases} 2^{k-2}+2^{k-3}+1 & 1<i\le k-3 \\ 2^{k-2}+2^{k-3}+2^{k-4}+1 & 1=i\le k-3 \end{cases}$$ Combine these with the result in Group II, we get (in any case) $\#S_t \le 2^{k-1}$.

Case C3: $j=k-1=i+1$, i.e., $j=k-1$ and $i=k-2$

When $0 \le a \le 2^{k-2}$

$\sigma = w(a)+w(2^{k-1}+2^{k-2}-a) = w(a)+1+w(2^{k-2}-a) = w(a)+1+k-2-w(a-1) =$

$$\begin{cases} k & a \equiv 1 \pmod 2 \\ \le k-1 & a \equiv 0 \pmod 2 \end{cases}$$

So, this contributes $1+2^{k-3}$ many a to S_t.

When $2^{k-2}+1 \le a \le 2^{k-1}+2^{k-2}$

$\sigma = w(a)+k-1-w(a-2^{k-2}-1)$

(Let $x = a-2^{k-2}-1$, $0 \le x \le 2^{k-1}-1$)

$= w(x+2^{k-2}+1)+k-1-w(x) \le 1+k$.

$\sigma = k+1$, there are $2^{k-1-2}=2^{k-3}$ many x (or a)

$\sigma = k$, i.e., $w(x+b^{k-2}+1) = 1+w(x)$, same to Lemma 2.6$(m=k-1)$, we have

$x_0=0$ $x_{k-2}=1$ or

$x_0=1$ $x_1=0$ $x_{k-2}=0$

The number of solutions is $2^{k-3}+2^{k-4}$, $1<i=k-2$.
Hence, the number of a in S_t is $2^{k-1}-2^{k-3}-(2^{k-3}+2^{k-4})=2^{k-3}+2^{k-4}$, $1<k=k-2$.
Group I contributes $1+2^{k-3}+2^{k-3}+2^{k-4}=2^{k-2}+2^{k-4}+1$.
Combine those in Group II, we have
$\#S_t\le 2^{k-2}+2^{k-4}+1+2^{k-4}-2^i<2^{k-1}$.
We complete the proof of this theorem. □

4. $t=2^k-2^i$ AND $t=2^k-2^j-2^i$

In this section, we prove the conjecture is true when $t=2^k-2^i$ and $t=2^k-2^j-2^i$.

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

Proof. Group I: $a=0,1...t$.
Group II: $a=t+1,...,2^k-2$, i.e., $a=t+v$, $b=2^k-1-v$, $v=1,2,...2^i-2$.
In Group II
$\Sigma=w(a)+w(b)=w(t+v)+w(2^k-1-v)=w(2^k-2^i+v)+k-w(v)=2k-w(2^i-v-1)-w(v)=2k-i\ge k+1$. So, Group II makes no contributions to S_t.
In Group I
If a is odd, then $\sigma=w(a)+w(b)=w(a)+w(t-a)=w(a)+w(2^k-2^i-a)=w(a)+k-w(2^i+a-1)\ge w(a)+k-(1+w(a-1))=k$.
Hence, there are at most $\frac{1}{2}t+1=2^{k-1}-2^{i-1}+1\le 2^{k-1}$ many a makes $w(a)+w(b)\le k-1$, i.e., $\#S_t\le 2^{k-1}$.
We are Done. □

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

Proof. Group I: $a=0,1...t$.
Group II: $a=t+v$, $b=2^k-1-v$, $v=1,2,...2^j+2^i-2$.
In Group II
$\Sigma=w(a)+w(b)=w(t+v)+w(2^k-1-v)=w(2^k-2^j-2^i+v)+k-w(v)=2k-w(2^j+2^i-v-1)-w(v)$
If $1\le v\le 2^i-1$
$\Sigma=2k-1-w(2^i-1-v)-w(v)=2k-1-i\ge k+1$.
If $2^i\le v\le 2^j+2^i-2$
$\Sigma=2k-w(2^j-1-(v-2^i))-w(v)=2k-j+w(v-2^i)-w(v)\ge 2k-j+w(v-2^i)-(w(v-2^i)+1)=2k-j-1\ge k$. So, Group II makes no contributions to S_t.
In Group I
Case A: $i=1$
$t=2^k-2^j-2=2^k-1-2^j-1$
$\sigma=w(a)+w(t-a)=w(a)+w(2^k-1-2^j-1-a)=w(a)+k-w(2^j+1+a)\ge k-2$.
$\sigma=k-2\Leftrightarrow w(1+2^j+a)=2+w(a)$, there are at most 2^{k-2} many such a.
$\sigma=k-1\Leftrightarrow w(1+2^j+a)=1+w(a)$, there are at most 2^{k-2} many such a by Lemma 2.6.
In summary, $\#S_t\le 2^{k-1}$.
Case B: $i>1$ and $j\le k-2$.
$\sigma=w(a)+w(b)=w(a)+w(2^k-2^j-2^i-a)=w(a)+k-w(2^j+2^i+a-1)\ge w(a)+k-2-w(a-1)$.
If $a\equiv 1 \pmod 2$
$\sigma\ge k-1$.
$\sigma=k-1\Leftrightarrow w(2^j+2^i+a-1)=2+w(a-1)\Leftrightarrow (a-1)_i=(a-1)_j=0$.
Since $(a-1)_0=0$, there are at most 2^{k-3} many a belongs to S_t.
If $a\equiv 2 \pmod 4$
$\sigma\ge w(a)+k-2-w(a-1)=k-2$

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

$(a-1)_0 = 1, (a-1)_1 = 0, (a-1)_i = 0, (a-1)_j = 0$, there are at most 2^{k-4} many such a.

$\sigma = k-1 \Leftrightarrow w(2^j+2^i+a-1) = 1+w(a-1)$, by Lemma 2.6, there are at most 2^{k-4} many such a ($m=k$, $x=a-1$, $(a-1)_0=1$, $(a-1)_1=0$).

There are at most 2^{k-2} many a such that $a \equiv 0 \pmod 4$, even if all of them belong to S_t, we still get $\#S_t \le 2^{k-3}+2^{k-4}+2^{k-4}+2^{k-2} = 2^{k-1}$.

Case C: $i > 1$ and $j = k-1$

$t = 2^{k-1} - 2^i$

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

When $a \equiv 1 \pmod 2$

$\sigma \ge k-1$, $\sigma = k-1 \Leftrightarrow w(2^i+a-1) = 1+w(a-1) \Leftrightarrow (a-1)_0 = (a-1)_i = 0$. There are at most $2^{k-1-2} = 2^{k-3}$ many solutions.

When $a \equiv 2 \pmod 4$

$\sigma \ge k-2$, $\sigma = k-2 \Leftrightarrow w(2^i+a-1) = 1+w(a-1) \Leftrightarrow (a-1)_0 = 1$, $(a-1)_1 = 0$, $(a-1)_i = 1$. 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.

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

□

5. $t = 2^k - 2^i - 1$, $t = 2^k - 2^j - 2^i - 1$ AND $t = 2^k - 2^l - 2^j - 2^i - 1$

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

Proof. Group I: $0 \le a \le t$.

Group II: $a = t+v$, $b = 2^k - 1 - v$, $v = 1, ..., 2^i - 1$.

In Group II

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

In Group I

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

$\sigma = k-1 \Leftrightarrow w(a+2^i) = 1+w(a)$, there are at most 2^{k-1} many such a. Hence, $\#S_t \le 2^{k-1}$. □

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

Proof. Group I: $0 \le a \le t$.

Group II: $a = t+v$, $b = 2^k - 1 - v$, $v = 1, ..., 2^j + 2^i - 1$.

In Group II

When $1 \le v \le 2^i$

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

When $2^i+1 \le v \le 2^j+2^i-1$

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

(Let $x = v-2^i-1$, $0 \le x \le 2^j-2$)

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

If $j \le k-2$, then $\Sigma \ge k$.

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

In Group I

$0 \le a \le 2^k - 2^j - 2^i - 1$

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

Case A: $j \leq k - 2$

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

$\sigma = k - 1 \Leftrightarrow w(2^j + 2^i + a) = 1 + w(a)$, by Lemma 2.6, the number of such a is at most 2^{k-2}. Hence, $\#S_t \leq 0 + a^{k-2} + 2^{k-2} = 2^{k-1}$.

Case B: $j = k - 1$

$\sigma = k - 2$, there are at most 2^{k-2} many such a.

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

(Same to Lemma 2.6)

$a_i = 0$ $a_j = a_{k-1} = 1$ $a_{j+1} = 0$ 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 the first condition can not be satisfied. So, there are at most 2^{k-3} many such a. Combine with Group II, we have $\#S_t \leq 2^{k-3} + 2^{k-2} + 2^{k-3} = 2^{k-1}$. Done. □

We need a lemma to prove our last theorem.

Lemma 5.3. *$N_r^{(i,j,l)} = \#\{x | 0 \leq x \leq 2^m - 1, w(2^i + 2^j + 2^l + x) = r + w(x)\}$, where $0 \leq i < j < l \leq m - 1$. Then*

$r = 3$, $w(2^i + 2^j + 2^l + x) = 3 + w(x) \Leftrightarrow x_i = x_j = x_l = 0$

$N_3^{(i,j,l)} = 2^{m-3}$.

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

$x_i = 0$ $x_j = 0$ $x_l = 1$ $x_{l+1} = 0$

or $x_i = 0$ $x_j = 1$ $x_{j+1} = 0$ $x_l = 0$ $(l > j + 1)$

or $x_i = 1$ $x_{i+1} = 0$ $x_j = 0$ $x_l = 0$ $(j > i + 1)$

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

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

$x_i = 0$ $x_j = 0$ $x_l = 1$ $x_{l+1} = 1$ $x_{l+2} = 0$ $(l \leq m - 2)$

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 $x_i = 1$ $x_{i+1} = 0$ $x_j = 1$ $x_{j+1} = 0$ $x_l = 0$ $(l > j + 1, j > i + 1)$

For $l = m - 1$, we get

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

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

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

Again, we omit this straightforward and a little tedious proof.

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

Proof. Group I: $0 \le a \le t$.

Group II: $a = t + v$, $b = 2^k - 1 - v$, $v = 1, 2, ..., 2^l + 2^j + 2^i - 1$.

Case A: $l \le k-3$ ($k \ge l+3 \ge j+4 \ge i+5$)

In Group II, $\Sigma = w(a)+w(b) = w(t+v)+w(2^k-1-v) = w(2^k-1-(2^l+2^j+2^i)+v)+k-w(v)$ $= 2k - w(2^l+2^j+2^i-v) - w(v)$.

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

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

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

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

If $2^j+1 \le 2^j+2^i$

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

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

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

Hence, Group II makes no contributions to S_t.

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

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

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

$\sigma = k-2 \Leftrightarrow w(2^l+2^j+2^i+a) = 2+w(a)$, there are at most $2^{k-3}+2^{k-4}$ many such a by Lemma 5.3(Please note that $m=k$ and $l \le k-3$, $r=2$).

$\sigma = k-1 \Leftrightarrow w(2^l+2^j+2^i+a) = 1+w(a)$, there are at most $2^{k-3}+2^{k-4}$ many such a 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, we check the proof of Case A, only if $2^j+2^i+1 \le 2^l+2^j+2^i-1$, there are some a will make contributions to S_t. $\Sigma = w(a)+w(b) = 2k-w(2^l-1-(v-2^j-2^i-1))-w(v) = 2k-l+w(v-2^j-2^i-1)-w(v) = 2k-l+w(x)-w(x+2^j+2^i+1) \ge 2k-l-3 = k-1$, where $x = v-2^j-2^i-1$, $0 \le x \le 2^l-2$.

$\Sigma = k-1 \Leftrightarrow w(2^l+2^j+2^i+x) = 3+w(x)$, there are at most $2^{l-3} = 2^{k-5}$ many such a.

In Group I

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

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

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

$\sigma = k-1 \Leftrightarrow w(2^l+2^j+2^l+a) = 1+w(a)$, check Lemma 5.3, $r=1$, $m=k$, $l=k-2$, the first condition $x_i=0\ x_j=0\ x_l=1\ x_{l+1}=1\ x_{l+2}=0 \Leftrightarrow x_i=0\ x_j=0\ x_{k-2}=1\ x_{k-1}=1 \Rightarrow x \ge 2^{k-1}+2^{k-2} > t$, so, the number of solutions of $\sigma = k-1$ should not include this 2^{k-4} many, i.e., there are at most $2^{k-3}+2^{k-5}$ many a such that $\sigma = k-1$ by Lemma 5.3.

Combine Group I and II, $\#S_t \le 2^{k-5}+2^{k-3}+2^{k-3}+2^{k-4}+2^{k-3}+2^{k-5} = 2^{k-1}$. We finish the proof of Case B.

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

In Group II, we check the proof in Case A, only if $2^i+1 \le v \le 2^j$ or $2^j+2^i+1 \le v \le 2^l+2^j+2^i-1$, there are some a will make contributions to S_t.

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

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

$\Sigma = k-1 \Leftrightarrow w(v-2^i-1)-2 = w(v)$ and $j = k-2$. Let $x = v-2^i-1$, $0 \le x \le 2^j-2^i-1$. $w(x+2^i+1) = 2+w(x)$ 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 $2^j+2^i+1 \le v \le 2^l+2^j+2^i-1$

$\Sigma = w(a)+w(b) = 2k-l+w(v-2^j-2^i-1)-w(v) \ge k+1-3 = k-2$. Let $x = v-2^j-2^i-1$, $0 \le x \le 2^l-2 = 2^{k-1}-2$.

If $\Sigma = k-2$ get at most (actually, exactly)$2^{k-1-3} = 2^{k-4}$ many solutions.

$\Sigma = k-1 \Leftrightarrow w(x+2^j+2^i+1) = w(x)+2$, 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.

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

In Group I

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

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

$\sigma = k-2 \Leftrightarrow w(2^l+2^j+2^i+a) = w(a)+2$, check the first condition of Lemma 5.3($r=2$), $a_i=0\ a_j=0\ a_l=1\ a_{l+1}=0 \Leftrightarrow a_i=0\ a_j=0\ a_{k-1}=1 \Rightarrow a \geq 2^{k-1} > t$. This means 2^{k-3} many a should not be counted. So, the number of solutions of $\sigma = k-2$ is at most

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

$\sigma = k-1 \Leftrightarrow w(2^l+2^j+2^i+a) = w(a)+1$. Check Lemma 5.3($r=1$). The third condition $a_i=0\ a_j=1\ a_l=1\ a_{l+1}=0\ (l=j+1) \Leftrightarrow a_i=0\ a_j=1\ a_{k-1}=1 \Rightarrow a > 2^{k-1} > t$, so, there are 2^{k-3} many a should not be counted for $l=j+1$.

The sixth condition $\Leftrightarrow a_i=0\ a_j=1\ a_{j+1}=0\ a_{k-1}=1\ (l>j+1) \Rightarrow a>t$. There are 2^{k-4} many a should not be counted for $l>j+1$.

The seventh condition $\Leftrightarrow a_i=1\ a_{i+1}=0\ a_j=0\ a_{k-1}=1\ (j>i+1) \Rightarrow a>t$. There are 2^{k-4} many a 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 $j \neq k-2$,i.e., $j \leq k-3$

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

If $j=k-2$

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

We complete the proof of this theorem. □

6. On the equation $w(2^{i_1}+2^{i_2}+...+2^{i_s}+x) = r+w(x)$

As we see, the counting heavily depends on the following number $N_r^{(i_1,i_2,...,i_s)} = \{x | 0 \leq x \leq 2^k-1, w(2^{i_1}+2^{i_2}+...+2^{i_s}+x) = r+w(x)\}$, where $0 \leq i_1 < i_2 < ... < i_s \leq k-1$. A general formula may be hard to obtain. We ask if the upper and lower bound can be determined for given s and r. We also ask the relation of all the bounds among all the r. Obviously, we have $N_r^{(i_1,i_2,...,i_s)} = 0$ if $r > s$. We also have $N_r^{(i_1,i_2,...,i_s)} = 0$ if $r \leq -k$.

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]SUNY, Department of Math, 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