On a generalized combinatorial conjecture involving addition mod $2^k - 1$

Jean-Pierre Flori

Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg
75700 Paris SP 07
France
E-mail: `jean-pierre.flori@ssi.gouv.fr`

Gérard Cohen

Télécom ParisTech
46, rue Barrault
F-75634 Paris cedex 1,
France
E-mail: `cohen@enst.fr`

Abstract In this note, we give a simple proof of the combinatorial conjecture proposed by Tang, Carlet and Tang, based on which they constructed two classes of Boolean functions with many good cryptographic properties. We also give more general properties about the generalization of the conjecture they propose.

Keywords: Combinatorics; Boolean functions; Tu-Deng conjecture

Biographical notes: Jean-Pierre Flori received a PhD from Télécom ParisTech in 2012. He is currently working for the Agence nationale de la sécurité des systèmes d'information. His main fields of interest are cryptograhpy and number theory.

Gérard Cohen received the Engineer's degree from École Nationale Supérieure des Télécommunications (ENST) in 1973 and Doctorat d'État ès Sciences in Mathematics in 1980 from University Paris 6. He is currently Professor at Télécom ParisTech (ex ENST) and has taught at various Universities, including École Normale Supérieure de Paris (Ulm), Paris 6 and supervised a dozen of PhD students. He has held a few visiting positions in Universities abroad (Waterloo, Syracuse, Technion, Tel Aviv, . . .). His main fields of interest are coding theory, combinatorics information theory and cryptography. Gérard Cohen has written over 150 papers in international journals and co-authored 3 books. He is a IEEE Fellow, chairman and founder of the IEEE French Chapter in Information Theory in 1993, and was associate editor from 2009 to 2012 of the IT-Transactions. He is also a member of SMF, AMS and SIAM.

1 Introduction

Inspired by a previous work of Tu and Deng [6], Tang, Carlet and Tang [5] constructed an infinite family of Boolean functions with many good cryptographic properties depending on the validity of the following combinatorial property:

Conjecture 1: *$\forall k \geq 2$, the following inequality is verified:*

$$\max_{t \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^*} \# \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid a - b = t; w(a) + w(b) \leq k-1 \right\} \leq 2^{k-1} \ .$$

They verified it experimentally for $k \leq 29$, as well as the following generalized property for $k \leq 15$ where $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ is such that $\gcd(u, 2^k-1) = 1$:

Conjecture 2: *$\forall k \geq 2$, the following inequality is verified:*

$$\max_{t \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^*} \# \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua \pm b = t; w(a) + w(b) \leq k-1 \right\} \leq 2^{k-1} \ .$$

This generalized conjecture includes the original conjecture proposed by Tu and Deng [6].

In this note, we prove Conjecture 1 which is sufficient to validate Tang, Carlet and Tang construction of Boolean functions, but also give some additional results about the properties of the sets involved.

In the following, $S_{k,t,\pm,u}$ will always denote the quantity of interest:

$$S_{k,t,\pm,u} = \# \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua \pm b = t; w(a) + w(b) \leq k-1 \right\} \ .$$

2 General properties

Here we follow the approach of the previous attempts to prove the original conjecture of Tu and Deng [2, 1].

We recall the elementary results:

Lemma 3: *For $k \geq 1$,*

- *$\forall a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $w(2a) = w(a)$;*
- *$\forall a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $w(-a) = k - w(a)$.*

We first remark that for a given $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, b must be equal to $\pm(t - ua)$, whence the following lemma.

Lemma 4: *For $k \geq 2$,*

$$S_{k,t,\pm,u} = \# \left\{ a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(\pm(t - ua)) \leq k-1 \right\} \ .$$

We now show that is enough to study the conjecture for one t, but also one u, in each cyclotomic class.

Lemma 5: *For $k \geq 2$,*

$$S_{k,t,\pm,u} = S_{k,2t,\pm,u} \quad .$$

Proof: Indeed $a \mapsto 2a$ is a permutation of $\mathbb{Z}/(2^k-1)\mathbb{Z}$ so that

$$\begin{aligned} S_{k,2t,\pm,u} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(\pm(2t - ua)) \leq k-1\right\} \\ &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(2a) + w(\pm 2(t - ua)) \leq k-1\right\} \\ &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(\pm(t - ua)) \leq k-1\right\} \\ &= S_{k,t,\pm,u} \quad . \end{aligned}$$

□

Lemma 6: *For $k \geq 2$,*

$$S_{k,t,\pm,u} = S_{k,t,\pm,2u} \quad .$$

Proof: Using the previous lemma:

$$\begin{aligned} S_{k,t,\pm,2u} &= S_{k,2t,\pm,2u} \\ &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(\pm(2t - 2ua)) \leq k-1\right\} \\ &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(\pm(t - ua)) \leq k-1\right\} \\ &= S_{k,t,\pm,u} \quad . \end{aligned}$$

□

We now show a more elaborate relation.

Lemma 7: *For $k \geq 2$ and $\gcd(u, 2^k - 1) = 1$,*

$$S_{k,t,\pm,u} = S_{k,\pm u^{-1}t,\pm,u^{-1}} \quad .$$

Proof: We use the fact that $a \mapsto u^{-1}(\mp a + t)$ is a permutation of $\mathbb{Z}/(2^k-1)\mathbb{Z}$.

$$\begin{aligned} S_{k,t,\pm,u} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(\pm(t - ua)) \leq k-1\right\} \\ &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(u^{-1}(\mp a + t)) + w(a) \leq k-1\right\} \\ &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(\pm(\pm u^{-1}t - u^{-1}a)) + w(a) \leq k-1\right\} \\ &= S_{k,\pm u^{-1}t,\pm,u^{-1}} \quad . \end{aligned}$$

□

3 Proof of the conjecture

We now prove Conjecture 1, and so its extension for u equal to any power of 2, that is Conjecture 2 for $u = 2^i$ and the sign $-$, according to Lemma 6.

First, we note that for $u = 1$ and the sign $-$, Lemma 7 becomes

$$S_{k,t,-,1} = S_{k,-t,-,1} \ .$$

Second, for the specific values of $a = 0$, t, we have that

- $w(0) + w(-t) = w(-t) \le k - 1$,
- and $w(t) + w(0) = w(t) \le k - 1$,

so that we always have

$$\{0, t\} \subset \left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid w(a) + w(-(t - a)) \le k - 1\right\} \ .$$

Finally, for $a \ne 0$, t, we have that

$$\begin{aligned} w(a) + w(-(t-a)) &= k - w(-a) + k - w(t-a) \\ &= 2k - (w(-a) + w(t-a)) \ . \end{aligned}$$

Then using the fact that $a \mapsto -a$ is a permutation of $\mathbb{Z}/(2^k - 1)\mathbb{Z}$:

$$\begin{aligned} S_{k,t,-,1} &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \setminus \{0, t\} \mid w(a) + w(-(t-a)) \le k - 1\right\} \\ &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \setminus \{0, t\} \mid w(-a) + w(t-a) \ge k + 1\right\} \\ &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid w(-a) + w(t-a) \ge k + 1\right\} \\ &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid w(a) + w(t+a) \ge k + 1\right\} \\ &= 2 + (2^k - 1 - \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid w(a) + w(t+a) \le k\right\}) \\ &\le 2 + (2^k - 1 - \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid w(a) + w(t+a) \le k - 1\right\}) \\ &\le 2^k + 1 - S_{k,-t,-,1} \\ &\le 2^k + 1 - S_{k,t,-,1} \ . \end{aligned}$$

Hence

$$2S_{k,t,-,1} \le 2^k + 1 \ ,$$

but we know that $S_{k,t,-,1}$ is an integer, which concludes the proof of Conjecture 1.

We also note that for $t = 0$,

$$\begin{aligned} S_{k,0,-,1} &= \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid 2w(a) \le k - 1\right\} \\ &= \sum_{w=0}^{\lfloor \frac{k-1}{2} \rfloor} \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid w(a) = w\right\} \\ &= \sum_{w=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{w} \ , \end{aligned}$$

which is equal to $2^{k-1} - \binom{k}{(k+1)/2}$ if k is odd, and $2^{k-1} - \binom{k}{k/2-1} - \binom{k/2}{k}/2$ if k is even. Therefore the conjecture can be naturally extended to include the case $t = 0$.

4 Computing the exact gap

If we rewrite the above reasoning more carefully, we find that

$$S_{k,t,-,1} = 2^{k-1} + (1 - \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w(a) + w(t+a) = k\right\})/2 \ .$$

It is an interesting problem to find a closed-form formula for the value of

$$\begin{aligned} M_{k,t} &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid w(a) + w(t+a) = k\right\} \ , \\ M_k &= \min_{t \in \mathbb{Z}/(2^k-1)\mathbb{Z}} M_{k,t} \ . \end{aligned}$$

We denote by Δ_k the following value

$$\Delta_k = \frac{M_k - 1}{2} \ ,$$

so that $S_{k,t,-,1} = 2^{k-1} - \Delta_k$.

The experimental results of Tang, Carlet and Tang suggest that the following recursive formula is verified:

$$\Delta_{k+1} = \begin{cases} 2\Delta_k + 1 & \text{if } k \text{ even,} \\ 2\Delta_k + 1 - \Gamma_{(k-1)/2} & \text{if } k \text{ odd,} \end{cases}$$

where

$$\Gamma_n = 1 + \sum_{w=0}^{n-1} C_w$$

and $C_w = \binom{2w}{w}/(w+1)$ is the w-th Catalan number. Γ_n is the sequence A155587 in OEIS [3].

Further experimental investigations made with Sage [4] show that the minimal value M_k seems to be attained for $t = 1$ if k is even and $t = 3$ if k is odd. In fact, the next proposition gives explicit formulae for $M_{k,1}$ and $M_{k,3}$.

We recall that $r(a,t) = w(a+t) - w(a) - w(t)$ can be interpreted as the number of carries occurring while adding a and t. Then we can describe $M_{k,t}$ as

$$\begin{aligned} M_{k,t} &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid w(a) + w(t+a) = k\right\} \\ &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid 2w(a) + w(t) - r(a,t) = k\right\} \\ &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid r(a,t) = -k + w(t) + 2w(a)\right\} \ . \end{aligned}$$

Proposition 8: *For $k \geq 2$,*

$$M_{k,1} = \sum_{w=1}^{\lfloor (k+1)/2 \rfloor} \binom{2w-2}{w-1} \ .$$

Proof: We know that $M_{k,1} = M_{k,-1}$, so we enumerate the set of a's verifying $r(a,-1) = 2w(a) - 1$ according to $w(a)$ or equivalently $r(a,-1)$. The binary expansion of -1 is `1---10`.

First, for any number $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$, $0 \leq r(a,t) \leq k$, so we deduce that a must verify $1 \leq w(a) \leq \lfloor (k+1)/2 \rfloor$.

Second, for a given number of carries r, a number a verifying $r(a,-1) = r$ must be of the following form

$$\begin{aligned} -1 &= \texttt{1---1---10} \ , \\ a &= \underbrace{\texttt{????1}}_{r}\texttt{0---0} \ . \end{aligned}$$

Such a description is valid even if $r(a,-1) = k$. So, for a given weight w, a number a verifying $w(a) = w$ and $r(a,-1) = 2w - 1$ must be of the following form

$$\begin{aligned} -1 &= \texttt{1---1---10} \ , \\ a &= \underbrace{\texttt{????1}}_{2w-1}\texttt{0---0} \ , \end{aligned}$$

with the other $w - 1$ bits equal to `1` anywhere among the $2w - 2$ first bits. Hence there are $\binom{2w-2}{w-1}$ differents a's of weight w verifying $r(a,-1) = 2w - 1$.

Finally, summing up on $1 \leq w \leq \lfloor (k+1)/2 \rfloor$, we get that $M_{k,1} = \sum_{w=1}^{\lfloor (k+1)/2 \rfloor} \binom{2w-2}{w-1}$. □

Proposition 9: *For $k \geq 3$,*

$$M_{k,3} = 1 + 2 \sum_{w=1}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} \ .$$

Proof: We proceed as in the proof of Proposition 8. The arguments are only slightly more technical.

We know that $M_{k,3} = M_{k,-3}$, so we enumerate the set of a's verifying $r(a,-3) = 2w(a) - 2$ according to $w(a)$ or equivalently $r(a,-3)$. The binary expansion of -3 is `1---100`.

First, from $r(a,-3) = 2w(a) - 2$, we deduce that $1 \leq w \leq \lfloor k/2 \rfloor + 1$.

Second, for a given number of carries r, there are now different possibilities.

For any $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$, there are exactly $\sum_{w=0}^{k-w(t)-1} \binom{k-w(t)}{w}$ different a's producing no carries. Indeed, such a's are characterized by the facts that they have no bits equal to `1` in front of any bit of t equal to `1` and that they can not have only `1`'s in front of the bits of t equal to `0`. For $t = -3$, the such a's are exactly 0, 1 and 2 and both 1 and 2 have weight 1.

Then, for a given number of carries $1 \leq r < 2\lfloor k/2 \rfloor$, a number a verifying $r(a,-3) = r$ cannot have its two last bits (in front of the two bits of -3 equal to `0`) equal to `1`. Otherwise it would produce k carries. So it must be of one of the following forms

$$\begin{aligned} -3 &= \texttt{1---1---100} \ , \\ a &= \underbrace{\texttt{????1}}_{r}\texttt{0--0?0} \ , \\ a &= \underbrace{\texttt{???1}}_{r-1}\texttt{0----01} \ . \end{aligned}$$

So for a given weight w, a number a verifying $w(a) = w$ and $r(a, -3) = 2w - 2$ must be of one of the following forms

$$\begin{aligned} -3 &= \texttt{1---1---100} \ , \\ a &= \underbrace{\texttt{????}}_{2w-2}\texttt{10--0?0} \ , \\ a &= \underbrace{\texttt{???}}_{2w-3}\texttt{10----01} \ , \end{aligned}$$

with the other $w - 1$ bits set to `1` anywhere among the $2w - 2$ remaining bits in the first case, and the other $w - 2$ bits set to `1` anywhere among the $2w - 4$ first bits in the second one. Hence there are $\binom{2w-2}{w-1} + \binom{2w-4}{w-2}$ differents a's of weight w.

Finally, if k is odd and $w(a) = \lfloor k/2 \rfloor + 1$, then $r(a, t) = k - 1$ and a must be of the following form

$$\begin{aligned} -3 &= \texttt{1---100} \ , \\ a &= \texttt{????101} \ . \end{aligned}$$

There are $\binom{2w-4}{w-2}$ different such a's. And, if k is even and $w(a) = \lfloor k/2 \rfloor + 1$, then $r(a, t) = k$ and a must be of the following form

$$\begin{aligned} -3 &= \texttt{1---100} \ , \\ a &= \texttt{?????11} \ . \end{aligned}$$

There are also $\binom{2w-4}{w-2}$ different such a's.

Therefore, we find that

$$\begin{aligned} M_{k,3} &= 2 + \sum_{w=2}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} + \sum_{w=2}^{\lfloor k/2 \rfloor + 1} \binom{2w-4}{w-2} \\ &= 1 + 2 \sum_{w=1}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} \ . \end{aligned}$$

□

We now prove recurrence relations for $M_{k,1}$ and $M_{k,3}$.

Corollary 10: *If k is even, then*

$$2M_{k,1} + 1 = M_{k+1,3} \ .$$

If k is odd, then

$$M_{k,3} - \Gamma_{(k-1)/2} = (M_{k+1,1} - 1)/2 \ .$$

Proof: The first equality is a simple consequence of the fact $\lfloor k/2 \rfloor = \lfloor (k+1)/2 \rfloor$ when k is even.

For the second one, we write

$$\begin{aligned}
M_{k,3} - \Gamma_{(k-1)/2} &= 1 + 2 \sum_{w=1}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} - 1 - \sum_{w=0}^{(k-3)/2} \binom{2w}{w} / (w+1) \\
&= 2 \sum_{w=1}^{(k-1)/2} \binom{2w-2}{w-1} - \sum_{w=0}^{(k-3)/2} \binom{2w}{w} / (w+1) \\
&= 1 + \sum_{w=1}^{(k-3)/2} (2 - 1/(w+1)) \binom{2w}{w} \ ,
\end{aligned}$$

and

$$\begin{aligned}
(M_{k+1,1} - 1)/2 &= \sum_{w=2}^{\lfloor k/2 \rfloor + 1} \binom{2w-2}{w-1} / 2 \\
&= \sum_{w=1}^{(k-1)/2} \binom{2w}{w} / 2 \ ,
\end{aligned}$$

so that we can equivalently show that

$$\binom{k-1}{(k-1)/2} - 2 = \sum_{w=1}^{(k-3)/2} (3 - 2/(w+1)) \binom{2w}{w} \ ,$$

which follows from a simple induction. For $k = 3$, this reduces to $0 = 0$ which is indeed true; for $k > 3$ odd, we have

$$\begin{aligned}
\binom{k+1}{(k+1)/2} - 2 &= 4k/(k+1) \binom{k-1}{(k-1)/2} - 2 \\
&= (4 - 1/(k+1)) \binom{k-1}{(k-1)/2} - 2 \ ,
\end{aligned}$$

and

$$\sum_{w=1}^{(k-1)/2} (3 - 2/(w+1)) \binom{2w}{w} = \left[\sum_{w=1}^{(k-3)/2} (3 - 2/(w+1)) \binom{2w}{w} \right] + (3 - 1/(k+1)) \binom{k-1}{(k-1)/2} \ .$$

$\square$

To conclude this section, let us note that $M_{k,1} \leq M_{k,3}$ if k is even and $M_{k,3} \leq M_{k,1}$ if k is odd. So, if we assume that these are indeed the minimal values M_k according to the parity of k, then Δ_k is given by

$$\Delta_k = \begin{cases} (M_{k,1} - 1)/2 \text{ if } k \text{ even,} \\ (M_{k,3} - 1)/2 \text{ if } k \text{ odd,} \end{cases}$$

and the recursive formulae are proved.

References

[1] Jean-Pierre Flori and Hugues Randriam. On the number of carries occurring in an addition mod $2^k - 1$. *Integers*, 12, 2012.

[2] Jean-Pierre Flori, Hugues Randriam, Gérard D. Cohen, and Sihem Mesnager. On a conjecture about binary strings distribution. In Claude Carlet and Alexander Pott, editors, *SETA*, volume 6338 of *Lecture Notes in Computer Science*, pages 346–358. Springer, 2010.

[3] The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`.

[4] William Stein. *Sage: Open Source Mathematical Software (Version 4.7.0)*. The Sage Group, 2011. `http://www.sagemath.org`.

[5] Deng Tang, Claude Carlet, and Xiaohu Tang. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. *IEEE Trans. Information Theory*, 59(1):653–664, 2013.

[6] Ziran Tu and Yingpu Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Des. Codes Cryptography*, 60(1):1–14, 2011.