On a conjecture about binary strings distribution

Jean-Pierre Flori* Hugues Randriambololona*
Gérard Cohen* Sihem Mesnager†

March 31, 2010

Abstract

It is a difficult challenge to find Boolean functions used in stream ciphers achieving all of the necessary criteria and the research of such functions has taken a significant delay with respect to cryptanalyses. A lot of attacks has led to design criteria for these functions; mainly: balancedness, a high algebraic degree, a high nonlinearity, a good behavior against Fast Algebraic Attacks and also a high algebraic immunity (which is now an absolutely necessary criterion (but not sufficient) for cryptographic Boolean functions).

Very recently, an infinite class of Boolean functions has been proposed by Tu and Deng having many good cryptographic properties under the assumption that the following combinatorial conjecture about binary strings is true:

Conjecture 0.1. *Let $S_{t,k}$ be the following set:*

$$S_{t,k} = \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a+b=t \text{ and } w(a)+w(b)<k \right\}.$$

Then:

$$|S_{t,k}| \leq 2^{k-1}.$$

The main contribution of the present paper is the reformulation of the problem in terms of *carries* which gives more insight on it than simple counting arguments. Successful applications of our tools include explicit formulas of $|S_{t,k}|$ for numbers whose binary expansion is made of one block (see theorem 3.8), a proof that the conjecture is *asymptotically* true (see theorem 3.12) and a proof that a family of numbers (whose binary expansion has a high number of 1s and isolated 0s) reaches the bound of the conjecture (see theorem 3.17). We also conjecture that the numbers in that family are the only ones reaching the bound (see conjecture 3.20).

1 Introduction

Symmetric cryptosystems are commonly used for encrypting and decrypting owing to their efficiency. A classical model of symmetric cryptosystem are stream

*Institut Télécom, Télécom ParisTech, CNRS LTCI, 46 rue Barrault, F-75634 Paris Cedex 13, France

†LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, 2 rue de la liberté, 93526 Saint-Denis Cedex, France

ciphers. They are composed of one or several Linear Feedback Shift Register (LFSR) combined or filtered by a Boolean function. These cryptosystems have been the objects of a lot of cryptanalyses and several design criteria have been proposed concerning the filtering or combining functions, mainly: balancedeness, a high algebraic degree, a high nonlinearity. Moreover, because of the recent algebraic attacks of Courtois and Meier [5], which have received a lot of attention in cryptographic literature, the notion of algebraic immunity has been introduced. Given a Boolean function f on n variables, a nonzero Boolean function g is called an annihilator of f if $f \star g = 0$ (where "$\star$" is the multiplication of functions). The algebraic immunity of f is the minimum value of d such that f or its complement $1 + f$ admits an annihilator function of algebraic degree d. (Recall that the algebraic degree of a Boolean function f is the degree of its unique representation as a multivariate polynomial over the finite field of two elements $\mathbb{F}_2$.) In view of algebraic attacks, the study of the set of annihilators of a Boolean function is very important. Indeed, it has been shown that Boolean functions used in cryptosystems should not have annihilators of low algebraic degree. The best possible algebraic immunity of n-variable functions is $\lceil \frac{n}{2} \rceil$ [5]. A high algebraic immunity is now an absolutely necessary (but not sufficient for resisting the Fast Algebraic Attacks introduced by Courtois [4]) property for Boolean functions used in stream ciphers. Since the introduction of this parameter, several constructions of Boolean functions with high algebraic immunity have been provided but very few of them are of optimal algebraic immunity. More importantly, those having other good cryptographic properties, as bentness, balancedness or high nonlinearity for instance, are even rarer.

In 2008, Carlet and Feng [3] proposed for the first time an infinite class of functions which seems able to satisfy all of the main criteria for being used as a filtering function in a stream cipher. Their functions are balanced with optimal algebraic degree, optimal algebraic immunity, good immunity to Fast Algebraic Attacks and good nonlinearity. Very recently, it has been revealed by Tu and Deng in [10] that there may be Boolean functions of optimal algebraic immunity in a classical class of Partial Spread functions due to Dillon [7] provided that conjecture 0.1 is correct.

The authors of [10] assume the validity of the conjecture and checked it for $k \leq 29$. They also proved that, if the conjecture is true, then one can get in even dimension balanced Boolean functions of optimal algebraic immunity and of high nonlinearity (better than that of the function proposed in [3]). The approach of the authors was to identify annihilators of the Boolean functions in n variables that they consider with codewords of BCH codes. The role of the conjecture is then to deduce from the BCH bound that those codewords are equal to zero if the algebraic degree of the corresponding annihilator is less than $\lceil \frac{n}{2} \rceil$. Very recently, Carlet [1] has observed that the function introduced by Tu and Deng is weak against Fast Algebraic Attacks and tried to repair its weakness. Any possibility of a real repair of this weakness (or an alternative function sharing all the properties of the Tu-Deng function but not having this weakness) should give an infinite class of balanced functions having a good behavior against Fast Algebraic Attacks, optimal algebraic immunity, optimal algebraic degree and good nonlinearity; that is, the best construction of an infinite class of Boolean functions proposed in the literature.

In the present paper we attack this conjecture. It is organized as follows. In section 2, we prove several *simple* properties and reformulate the problem in

terms of *carries*. In section 3 we apply our new formulation in different situations. In particular we compute in subsection 3.3 exact formulas of $|S_{t,k}|$for numbers made of only one block. We then introduce a constraint in subsection 3.4 which greatly simplifies calculations. It leads us to a proof that the conjecture is *asymptotically* true in subsection 3.5 and to a proof that a family of numbers reaches the bound (we believe they are the only ones to do so) in subsection 3.7. In section 4 we use an inductive approach which allows us to prove that $|S_{t,k}|$ has a good asymptotic behavior. In section 5 we discuss results and strategies found in other papers. The most important notations are given in definitions 3.1, 3.2 and 3.4.

2 Reformulation and first results

2.1 Notations

Unless stated otherwise, we use the following notations:

- $k \in \mathbb{N}$ the number of bits (or length of binary strings) we are currently working on.
- $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ a fixed modular integer.

We use the following function of natural (or modular) integers (or binary strings).

Definition 2.1 (Weight)**.** *For $t \in \mathbb{N}$, $w(t)$ is the binary (or Hamming) weight of t, i.e. the number of* `1`*s of its binary expansion. For $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $w(t)$ is the binary (or Hamming) weight of the representative of t in $\{0,\dots,2^k-2\}$.*

We now define the sets we are interested in.

Definition 2.2.

- $C_{t,k} = \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a+b=t\right\}$*, the modular integers whose sum is t.*
- $C_{t,k,i} = \{(a,b) \in C_{t,k} | w(a)+w(b) = k+i\}$*, the modular integers whose sum is t and whose sum of weights is $k+i$ for $i \in \mathbb{Z}$.*
- $S_{t,k}$*, the modular integers whose sum is t and whose sum of weights is strictly less than k; i.e. $S_{t,k} = \bigsqcup_{i<0} C_{t,k,i}$.*
- $T_{t,k}$*, the modular integers whose sum is t and whose sum of weights is strictly more than k; i.e. $S_{t,k} = \bigsqcup_{i>0} C_{t,k,i}$.*
- $E_{t,k}$*, the modular integers whose sum is t and whose sum of weights equals k; i.e. $E_{t,k} = C_{t,k,0}$.*

The following lemma is obvious:

Lemma 2.3.

$$C_{t,k} = S_{t,k} \sqcup E_{t,k} \sqcup T_{t,k}.$$

2.2 Mean

For $t \neq t'$, $S_{t,k} \cap S_{t',k} = \varnothing$, so that:

$$\begin{aligned} S &= \bigsqcup_{t=0}^{2^k-2} S_{t,k} \\ &= \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | w(a)+w(b) \leq k-1\right\}, \end{aligned}$$

and summing up according to the value of $w(a)+w(b)$, we compute:

$$\begin{aligned} |S| &= \sum_{i=0}^{k-1} \binom{2k}{i} \\ &= 2^{2k-1} - \frac{1}{2}\binom{2k}{k}. \end{aligned}$$

The following proposition shows that the bound of the conjecture is sharp.

Proposition 2.4.

$$E_t\left(|S_{t,k}|\right) = 2^{k-1}\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right).$$

Proof Using Stirling's approximation, we have:

$$\binom{2k}{k} = \frac{2k!}{k!^2} \sim \frac{2^{2k}}{\sqrt{\pi k}},$$

and we compute:

$$\begin{aligned} E_t\left(|S_{t,k}|\right) &= \frac{|S|}{2^k-1} \\ &= \frac{2^{2k-1} - \frac{1}{2}\binom{2k}{k}}{2^k-1} \\ &= \frac{2^{2k-1} - \frac{1}{2}\frac{2^{2k}}{\sqrt{\pi k}} + o\left(\frac{2^{2k}}{\sqrt{k}}\right)}{2^k-1} \\ &= \frac{2^{2k-1}}{2^k-1}\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right) \\ &= 2^{k-1}\left(1 + \frac{1}{2^k} + o\left(\frac{1}{2^k}\right)\right)\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right) \\ &= 2^{k-1}\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right). \end{aligned}$$

□

2.3 Negation

Definition 2.5. *We define $\overline{a}^k$ as the modular integer whose binary expansion is the binary not on k bits of the binary expansion of the canonical representative of a. We write it down $\overline{a}$ when there is no ambiguity about the value of k.*

Lemma 2.6. *Let $a \neq 0 \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, then $-a = \overline{a}$ and $w(-a) = k - w(a)$.*

Proof Indeed $a + \overline{a} = \sum_{i=0}^{k-1} 2^i = 2^k - 1 = 0$. □

We are able to deal with the pathological case $t = 0$:

Proposition 2.7. *For all k:*

$$S_{0,k} = \{(0,0)\}.$$

Proof Indeed $(a,b) \in S_{0,k}$ iff $b = -a$ and $w(a) + w(-a) = k$ iff $a \neq 0$ so that:

$$S_{0,k} = \{(0,0)\}.$$

□

Corollary 2.8. *For all k:*

$$|S_{0,k}| = 1.$$

From now on we suppose $t \neq 0$.

2.4 Rotation

In this subsection we prove that $|S_{t,k}|$ is invariant by *rotation* of t.

Lemma 2.9. *For all $i \in \mathbb{Z}$ and $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, we have:*

$$w(2^i a) = w(a).$$

Proof We are working in $\mathbb{Z}/(2^k-1)\mathbb{Z}$ so that $2^k = 1$ and multiplying a modular integer in $\mathbb{Z}/(2^k-1)\mathbb{Z}$ by 2 is just rotating its representation as a binary string on k bits by one bit to the left. □

Proposition 2.10. *For $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ and $i \in \mathbb{Z}$:*

$$S_{2^i t,k} = 2^i S_{t,k} = \left\{(2^i a, 2^i b) | (a,b) \in S_{t,k}\right\}.$$

We say that for any $i \in \mathbb{Z}$, $2^i t$ and t are equivalent and we write $t \simeq 2^i t$.

Proof Indeed for $(a,b) \in S_{t,k}$, $2^i a + 2^i b = 2^i t$ and $w(2^i a) + w(2^i b) = w(a) + w(b) < k$. □

Corollary 2.11. *For $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ and $i \in \mathbb{Z}$:*

$$|S_{t,k}| = \left|S_{2^i t,k}\right|.$$

2.5 Parity

The function swap : $(a,b) \mapsto (b,a)$ is an involution of $C_{t,k,i}$, so that we prove the following statement:

Proposition 2.12. *$S_{t,k}$ is odd iff $0 \leq w(t) \leq \frac{k-1}{2}$.*

Proof Indeed $(b,a) \in S_{t,k}$ iff $(a,b) \in S_{t,k}$ and $(b,a) \neq (a,b)$ unless $a = b$, i.e. $a = b = t/2$. Moreover $(t/2, t/2) \in S_{t,k}$ iff $2w(t/2) \leq k-1$, i.e. $w(t) = w(t/2) \leq \frac{k-1}{2}$. □

2.6 Carries

We now define the main tool used in this paper:

Definition 2.13. *For $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $a \neq 0$, we set:*

$$r(a,t) = w(a) + w(t) - w(a+t),$$

i.e. $r(a,t)$ is the number of carries occurring while performing the addition. We set:

$$r(0,t) = "r(2^k - 1 = \underbrace{\texttt{1...1}}_{k}, t)" = k,$$

*which could seem unnatural, but fits our following definitions and propositions.*0 *is considered to produce k carries, i.e. 0 behaves like the $\underbrace{\texttt{1...1}}_{k}$ binary string. We also remarks that $r(-t,t) = k$.*

The following proposition is fundamental. It brings to light the importance of the number of carries occuring during the addition.

Proposition 2.14.

$$C_{t,k,i} = \{(a, t-a) | r(-a,t) = w(t) - i\}.$$

Proof For $(a,b) \in C_{t,k,i}$ we have $a + b = t$ so $b = t - a$ If $a \neq 0$, using 2.6, our condition for $C_{t,k,i}$ becomes:

$$\begin{aligned} w(a) + w(t-a) = k + i &\Leftrightarrow w(-(-a)) + w(-a+t) = k + i \\ &\Leftrightarrow k - w(-a) + w(-a+t) = k + i \\ &\Leftrightarrow r(-a,t) = w(t) - i. \end{aligned}$$

We also have $r(-0 = 0, t) = k = w(t) - (w(t) - k)$ and $(0,t) \in C_{t,k,w(t)-k}$. □

Corollary 2.15.

$$|S_{t,k}| = |\{a | r(a,t) > w(t)\}|.$$

The following lemma allows us to prove some relations between $S_{t,k}$, $T_{t,k}$ and $S_{-t,k}$.

Lemma 2.16. *If $a \neq 0, -t$, then:*

$$r(a,t) = k - r(-a,-t).$$

If $a = 0, -t$, then:

$$r(a,t) = r(-a,-t) = k.$$

Proof If $a \neq 0, -t$, going back to the definition of $r(a,t)$, we have:

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

□

Definition 2.17. *We define:*

$$S^*_{t,k} = S_{t,k} \setminus \{(0,t),(t,0)\}.$$

Proposition 2.18.

$$T_{t,k} = -S^*_{-t,k}.$$

Proof Indeed if $(a, t-a) \in T_{t,k}$, then $a \neq 0, t$ and $r(-a,t) < w(t)$, so that $r(a,-t) > w(-t)$ and $(-a,-t+a) \in S^*_{-t,k}$.

Conversly if $(a,-t-a) \in S^*_{-t,k}$, then $(-a,t+a) \in T_{t,k}$. □

Proposition 2.19.

$$T_{t,k} = t + S^*_{-t,k}.$$

Proof If $(a,-t-a) \in S_{-t,k}$ and $a \neq 0,-t$, then:

$$r(-a,-t) = w(-a) + w(-t) - w(-a-t) < w(-t) = k - w(t).$$

Moreover:

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

so that $r(-t-a,-t) > w(t)$ and $t + (a,-t-a) \in T_{t,k}$.

Conversely, if $(a,t-a) \in T_{t,k}$, then $a \neq 0,t$ and $a - t \in S^*_{-t,k}$.

We could also have used the swap function and the previous corollary. □

Corollary 2.20. *If $2t \neq -t$:*

$$|S_{t,k}| + |S_{-t,k}| \leq 2^k - 1.$$

Otherwise:

$$|S_{t,k}| + |S_{-t,k}| \leq 2^k.$$

Proof We already know that $S_{t,k} \sqcup T_{t,k} \subset C_{t,k}$ so that $|S_{t,k}| + |S{-}t,k| \leq 2^k + 1$. But in fact $w(t+t) = w(2t) = w(t)$ so that $(2t,-t)$ and $(-t,2t)$ are in $E_{t,k}$, i.e. neither in $S_{t,k}$ nor in $T_{t,k}$ and:

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

if $2t \neq -t$, and:

$$|S_{t,k}| + |S_{-t,k}| \leq 2^k$$

if $2t = t$. □

We can prove the conjecture in the specific case where $t \simeq -t$:

Theorem 2.21. *If $t \simeq -t$, then:*

$$|S_{t,k}| \leq 2^{k-1} - 1$$

if $2t \neq -t$, and:

$$|S_{t,k}| \leq 2^{k-1}$$

otherwise.

Proof $t \simeq -t$ so that $|S_{-t,k}| = |S_{t,k}|$. If $2t \neq -t$, the corollary 2.20 becomes:

$$|S_{t,k}| \leq 2^{k-1} - \frac{1}{2}.$$

But $|S_{t,k}| \in \mathbb{N}$ so the following inequality holds:

$$|S_{t,k}| \leq 2^{k-1} - 1.$$

If $2t = -t$, only the following one is true:

$$|S_{t,k}| \leq 2^{k-1}.$$

□

2.7 A combinatorial proposition of independent interest

In the next sections we use the following quantities and want to compare them:

Definition 2.22.

- $\Sigma(d,n) = \sum_{l=0}^{n} 2^{-l}\binom{l+d}{d}$
- $\Delta(d,n) = 2^{-n}\binom{n+d+1}{d}\frac{d-n}{2d+2}$

Proposition 2.23. *For any d, n and e positive,*

$$\Sigma(d+e, n+e) = 2^e\Sigma(d,n) + \sum_{l=1}^{e} 2^{e-l}\Delta(d+l-1, n+l-1).$$

Proof For $e = 1$ and d and n fixed, we compute:

$$\begin{aligned}
\Sigma(d+1, n+1) &= \sum_{l=0}^{n+1} 2^{-l}\binom{l+d+1}{d+1} \\
&= \sum_{l=0}^{n+1} 2^{-l}\left(\binom{l+d}{d} + \binom{l+d}{d+1}\right) \\
&= \sum_{l=0}^{n} 2^{-l}\binom{l+d}{d} + 2^{-n-1}\binom{n+d+1}{d} \\
&\quad + \frac{1}{2}\left(\sum_{l=0}^{n+2} 2^{-(l-1)}\binom{(l-1)+d+1}{d+1}\right) \\
&\quad - \frac{1}{2}2^{-n-1}\binom{n+d+2}{d+1} \\
&= \Sigma(d,n) + 2^{-n-1}\binom{n+d+1}{d} \\
&\quad + \frac{1}{2}\Sigma(d+1, n+1) - \frac{1}{2}2^{-n-1}\binom{n+d+2}{d+1} \\
&= \Sigma(d,n) + \frac{1}{2}\Sigma(d+1, n+1) \\
&\quad + 2^{-n-1}\binom{n+d+1}{d}\left(1 - \frac{n+d+2}{2d+2}\right) \\
&= \Sigma(d,n) + \frac{1}{2}\Sigma(d+1, n+1) + \frac{1}{2}\Delta(d,n).
\end{aligned}$$

The result follows by induction. □

Corollary 2.24. *For any $d \geq 0$ and $e \geq 0$,*

$$\Sigma(d+e, n+e) \geq 2^e \Sigma(d, n)$$

iff $n \leq d$.

Proof Indeed $\Delta(d+e, n+e) \geq 0$ iff $n \leq d$. □

As a byproduct we get the following well-known formula [8, formula 5.20]:

Corollary 2.25. *For any d positive,*

$$\Sigma(d, d) = 2^d.$$

Proof When $n = d$ and $e = 1$ the proposition becomes:

$$\Sigma(d+e, d+e) = 2^e \Sigma(0, 0) = 2^e.$$

□

When $n \to \infty$, the sum converges and we get the classical result:

Proposition 2.26.

$$\Sigma(d, "n = \infty") = 2^{d+1}.$$

Proof It follows from the classical identity:

$$\frac{1}{(1-z)^{n+1}} = \sum_{k=0}^{\infty} \binom{n+k}{n} z^k.$$

□

3 A block splitting pattern

3.1 General situation

In this section, we often compute $P_{t,k} = 2^{-k} |S_{t,k}|$ rather than $|S_{t,k}|$. Therefore we use the words *proportion* or *probability* in place of *cardinality*.

We split $t(\neq 0)$ (once correctly rotated, i.e. we multiply it by a correct power of 2 so that its binary expansion on k bits begins with a `1` and ends with a `0`) in blocks of the form $[1^*0^*]$ (i.e. as many `1`s as possible followed by as many `0`s as possible) and write it down:

Definition 3.1.

$$t = \underbrace{\overbrace{1\cdots}^{\alpha_1}\overbrace{0\cdots}^{\beta_1}}_{t_1} \cdots \underbrace{\overbrace{1\cdots}^{\alpha_i}\overbrace{0\cdots}^{\beta_i}}_{t_i} \cdots \underbrace{\overbrace{1\cdots}^{\alpha_d}\overbrace{0\cdots}^{\beta_d}}_{t_d}$$

with d the number of blocks, α_i and β_i the numbers of `1`s and `0`s of the ith block t_i. We define $A = \sum_{i=1}^{d} \alpha_i = w(t)$ and $B = \sum_{i=1}^{d} \beta_i = k - w(t)$.

We define corresponding values for a (a number to be added to t) as follows:

Definition 3.2.

$$t = \overbrace{\texttt{1---1}}^{\alpha_1}\overbrace{\texttt{0---0}}^{\beta_1}\ldots\overbrace{\texttt{1---1}}^{\alpha_i}\overbrace{\texttt{0---0}}^{\beta_i}\ldots\overbrace{\texttt{1---1}}^{\alpha_d}\overbrace{\texttt{0---0}}^{\beta_d},$$
$$a = \underbrace{\texttt{?10-0}}_{\gamma_1}\underbrace{\texttt{?01-1}}_{\delta_1}\ldots\underbrace{\texttt{?10-0}}_{\gamma_i}\underbrace{\texttt{?01-1}}_{\delta_i}\ldots\underbrace{\texttt{?10-0}}_{\gamma_d}\underbrace{\texttt{?01-1}}_{\delta_d},$$

i.e. γ_i *is the number of* `0`*s in front of the end of the* `1`*s subblock of* t_i *and* δ_i *is the number of* `1`*s in front of the end of the* `0`*s subblock of* t_i*. We define* $\Gamma = \sum_{i=1}^{d} \gamma_i$ *and* $\Delta = \sum_{i=1}^{d} \delta_i$*.*

We first *approximate* $r(a,t)$ by $\sum_{i=0}^{d} \alpha_i - \gamma_i + \delta_i$ ignoring the two following facts:

- if a carry goes out of the $i-1$st block (we say that it *overflows*) and $\delta_i = \beta_i$, the `1`s subblock produces α_i carries, whatever value γ_i takes,
- and if no carry goes out of the $i-1$st block (we say that it is *inert*), the `0`s subblock produces no carries, whatever value β_i.

Then $r(a,t) > w(t)$ becomes *approximately* $\sum_{i=1}^{d} \gamma_i < \sum_{i=1}^{d} \delta_i$ and we have the following distributions for γ_i and δ_i:

$\gamma_i =$	0	1	$\ldots$	γ_i	$\ldots$	$\alpha_i - 1$	α_i	$\alpha_i + 1$	$\ldots$
$P(\gamma_i)$	$1/2 - 1/2^k$	$1/4$	$\ldots$	$1/2^{\gamma_i+1}$	$\ldots$	$1/2^{\alpha_i}$	$1/2^{\alpha_i}$	0	$\ldots$

$\delta_i =$	0	1	$\ldots$	δ_i	$\ldots$	$\beta_i - 1$	β_i	$\beta_i + 1$	$\ldots$
$P(\delta_i)$	$1/2$	$1/4$	$\ldots$	$1/2^{\delta_i+1}$	$\ldots$	$1/2^{\beta_i}$	$1/2^{\beta_i} - 1/2^k$	0	$\ldots$

Moreover all the γ_is and δ_is are independent.

We modify γ_i and δ_i to take the first fact into account:

- if $\delta_i \neq \beta_i$, we define $\delta'_i = \delta_i$ and $\gamma'_i = \gamma_i$ as before,
- if $\delta_i = \beta_i$, we define $\delta'_i = \beta_i$ and $\gamma'_i = 0$.

γ'_i and δ'_i follow the distributions:

$\gamma'_i =$	0	1	$\ldots$	γ'_i	$\ldots$	$\alpha_i - 1$	α_i	$\alpha_i + 1$	$\ldots$
$P(\gamma'_i)$	$\frac{1+1/2^{\beta_i}}{2} - \frac{1}{2^k}$	$\frac{1-1/2^{\beta_i}}{4}$	$\ldots$	$\frac{1-1/2^{\beta_i}}{2^{\gamma'_i+1}}$	$\ldots$	$\frac{1-1/2^{\beta_i}}{2^{\alpha_i}}$	$\frac{1-1/2^{\beta_i}}{2^{\alpha_i}}$	0	$\ldots$

$\delta'_i =$	0	1	$\ldots$	δ'_i	$\ldots$	$\beta_i - 1$	β_i	$\beta_i + 1$	$\ldots$
$P(\delta'_i)$	$1/2$	$1/4$	$\ldots$	$1/2^{\delta'_i+1}$	$\ldots$	$1/2^{\beta_i}$	$1/2^{\beta_i} - 1/2^k$	0	$\ldots$

The γ'_is and δ'_is are no longer pairwise independent. Indeed within the same block, γ'_i and δ'_i are correlated. However each block remains independent of the other ones.

Taking the second fact into account is more difficult, and we do it in an iterative way.

We first take care of the as such that $r(a,t) = k$:

- if $\forall i, \delta_i = \beta_i$, then $\delta''_i = \delta_i$ and $\gamma''_i = \gamma'_i = 0$.

We now suppose that there exists i_0 such that $\delta_{i_0} \neq \beta_{i_0}$. We first define γ''_{i_0}, then δ''_{i_0+1}, γ''_{i_0+1}, ... and finally δ''_{i_0}:

- set $\gamma''_{i_0} = \gamma_{i_0}$, $i = i_0 + 1$,
- do:
  - $\delta''_i = \delta_i$ if $\gamma_{i-1} \neq \alpha_{i-1}$, 0 otherwise,
  - $\gamma''_i = \gamma_i$ if $\delta''_i \neq \beta_i$, 0 otherwise,
  - $i = i + 1$

  while $i \neq i_0 + 1$

The γ''_is and δ''_is are no longer pairwise independent, even between different blocks, but $r(a,t) = \sum_d \alpha_i - \gamma''_i + \delta''_i$ and the following proposition is true:

Proposition 3.3. *$a \in S_{t,k}$ iff $\sum_d \gamma''_i < \sum_d \delta''_i$.*

Most of the time t is considered to be fixed so that the α_is and the β_is are considered to be constants, whereas the other quantities defined in this section depend on a which ranges over $\mathbb{Z}/(2^k-1)\mathbb{Z}$ and will be considered as variables, whence the vocabulary we use. However we sometimes use their names to denote a fixed value to lighten notations.

3.2 Combining variables

In the previous section we defined two variables for each block. However we are only really interested in the number of carries, so one should suffice, that is why we also define:

Definition 3.4.

$$t = \overbrace{\texttt{1---1}}^{\alpha_1}\overbrace{\texttt{0---0}}^{\beta_1}\texttt{...}\overbrace{\texttt{1---1}}^{\alpha_i}\overbrace{\texttt{0---0}}^{\beta_i}\texttt{...}\overbrace{\texttt{1---1}}^{\alpha_d}\overbrace{\texttt{0---0}}^{\beta_d},$$
$$a = \texttt{?}\underbrace{\texttt{10-0?01-1}}_{\epsilon_1}\texttt{...?}\underbrace{\texttt{10-0?01-1}}_{\epsilon_i}\texttt{...?}\underbrace{\texttt{10-0?01-1}}_{\epsilon_d},$$

i.e. $\epsilon_i = \gamma_i + \beta_i - \delta_i$ is approximately *the number of carries that do not occur in the ith block. We define $E = \sum_{i=1}^{d} \epsilon_i$.*

As in the previous section, we define $\epsilon'_i = \gamma'_i + \beta_i - \delta'_i$ and $\epsilon''_i = \gamma''_i + \beta_i - \delta''_i$. Proposition 3.3 becomes:

Proposition 3.5. *$a \in S_{t,k}$ iff $\sum_d \epsilon''_i < \sum_d \beta_i = B = k - w$.*

The first value we are interested in is $P(\epsilon''_i | \gamma''_{i-1} \neq \alpha_{i-1})$, i.e. the proportion of modular integers for which we lose ϵ''_i in the ith block and the $i-1$st block overflows. However this value is difficult to express because of the circular dependency between the blocks. That is why we compute $P_+(\epsilon''_i)$ the proportion of modular integers where we lose ϵ''_i in the ith block if we suppose that the $i-1$st block *always* overflows, a kind of equivalent when the blocks are pairwise independent. It is exactly $P(\epsilon'_i = \epsilon''_i)$ (i.e. the probability that the *variable* ϵ'_i takes the *value* ϵ''_i) for suitable values of ϵ''_i.

We are also interested in $P(\epsilon''_i | \gamma''_{i-1} = \alpha_{i-1})$. For the same reason as above we only compute $P_-(\epsilon''_i)$ the proportion of modular integers for which we lose ϵ''_i in the ith block if we suppose that the $i-1$st block is *always* inert. It is not directly linked to the variables we defined before.

Theorem 3.6.

$$\begin{aligned} P_+(\epsilon_i'') &= "P(\epsilon_i''|\gamma_{i-1}'' \neq \alpha_{i-1})" \\ &= P_0(\epsilon_i'') + P_1(\epsilon_i''), \end{aligned}$$

where:

$$\begin{aligned} P_0(\epsilon_i'') &= "P(\epsilon_i''|\gamma_{i-1}'' \neq \alpha_{i-1}, \gamma_i'' \neq \alpha_i)" \\ &= \begin{cases} 2^{-\beta_i} & \epsilon_i'' = 0 \\ 2^{-|\epsilon_i'' - \beta_i|} \frac{1-4^{M-m}}{3} & \epsilon_i'' \neq 0 \end{cases} \end{aligned}$$

i.e. if the block itself overflows,

$$\begin{aligned} P_1(\epsilon_i'') &= "P(\epsilon_i''|\gamma_{i-1}'' \neq \alpha_{i-1}, \gamma_i'' = \alpha_i)" \\ &= 2^{\epsilon_i'' - 2\alpha_i - \beta_i - 1} \end{aligned}$$

i.e. if it is inert, with:

$$\begin{aligned} m &= \min(\epsilon_i'', \alpha_i), \\ M &= \max(0, \epsilon_i'' - \beta_i); \end{aligned}$$

and

$$\begin{aligned} P_-(\epsilon_i'') &= "P(\epsilon_i''|\gamma_{i-1}'' = \alpha_{i-1})" \\ &= 2^{\beta_i - \epsilon_i'' - 1_{\epsilon_i'' \neq \alpha_i + \beta_i}} - 2^{-k}. \end{aligned}$$

Proof We first compute $P_0(\epsilon_i'') = "P(\epsilon_i''|\gamma_{i-1}'' \neq \alpha_{i-1}, \gamma_i'' \neq \alpha_i)"$.

That situation is described below:

$$\begin{aligned} t &= \ldots \overset{\leftarrow}{\overbrace{\texttt{1---1}}^{\alpha_i}} \overbrace{\texttt{0---0}}^{\beta_i} \overset{\leftarrow}{\ldots}, \\ a &= \ldots \underbrace{\texttt{?10-0?01-1}}_{\epsilon_i''} \ldots \end{aligned}$$

A carry comes out of the previous block and one goes out of this one.

We remark that if $\delta_i = \beta_i$, then $\gamma_i'' = 0$ and $\epsilon_i'' = 0$ whatever value γ_i takes. Therefore:

$$\begin{aligned} P_0(\epsilon_i'' = 0) &= P(\delta_i = \beta_i) + 2^{-k} \\ &= 2^{-\beta_i}. \end{aligned}$$

We must add 2^{-k} for the modular integer 0.

We now suppose that $\delta_i \neq \beta_i$. Then $\epsilon_i'' = \epsilon_i = \gamma_i + \beta_i - \delta_i$ and $0 \leq \epsilon_i'' \leq \alpha_i + \beta_i - 1$. To get such an ϵ_i'', we must have:

$$0 \leq \gamma_i \leq \alpha_i - 1,$$

$$0 \leq \delta_i \leq \beta_i - 1,$$

but $\delta_i = \beta_i + \gamma_i - \epsilon_i''$ so γ_i must be bounded as follows:

$$M = \max(0, \epsilon_i'' - \beta_i) \leq \gamma_i \leq m - 1 = \min(\epsilon_i'', \alpha_i) - 1.$$

And $P_0(\epsilon_i'')$ is computed below:

$$\begin{aligned}
P_0(\epsilon_i'') &= \sum_{\gamma_i=\max(0,\epsilon_i''-\beta_i)}^{\min(\epsilon_i'',\alpha_i)-1} 2^{-\gamma_i-\delta_i-2} \\
&= \sum_{\gamma_i=M}^{m-1} 2^{\epsilon_i''-\beta_i-2\gamma_i-2} \\
&= 2^{\epsilon_i''-\beta_i-2M-2} \sum_{\gamma_i=0}^{m-M-1} 2^{-2\gamma_i} \\
&= 2^{-|\epsilon_i''-\beta_i|-2} \frac{1-(1/4)^{m-M}}{3/4} \\
&= 2^{-|\epsilon_i''-\beta_i|} \frac{1-4^{M-m}}{3}.
\end{aligned}$$

We then compute $P_1(\epsilon_i'') =$ "$P(\epsilon_i''|\gamma_{i-1}'' \neq \alpha_{i-1}, \gamma_i'' = \alpha_i)$".
We describe it below:

$$\begin{aligned}
t &= \ldots \overset{\times}{\overbrace{\texttt{1---1}}^{\alpha_i}} \overbrace{\texttt{0---0}}^{\beta_i} \overset{\leftarrow}{\ldots}, \\
a &= \ldots \underbrace{\texttt{0---0?01}}_{\epsilon_i''} \texttt{-1}\ldots.
\end{aligned}$$

A carry comes out of the previous block, but none goes out from this one.

In that case, we must have $\gamma_i = \alpha_i$ and $\delta_i \neq \beta_i$, so that $1 \leq \epsilon_i'' \leq \alpha_i + \beta_i$, $\epsilon_i'' = \alpha_i + \beta_i - \delta_i$ and only the value of $\delta_i'' = \delta_i$ is relevant:

$$\begin{aligned}
P_1(\epsilon_i'') &= P(\gamma_i = \alpha_i) P(\delta_i) \\
&= 2^{-\alpha_i} 2^{\beta_i - \delta_i - 1} \\
&= 2^{\epsilon_i'' - 2\alpha_i - \beta_i - 1}.
\end{aligned}$$

We finish with $P_-(\epsilon_i'') =$ "$P(\epsilon_i''|\gamma_{i-1}'' = \alpha_{i-1})$".
Schematically it looks like below:

$$\begin{aligned}
t &= \ldots \overbrace{\texttt{1---1}}^{\alpha_i} \overbrace{\texttt{0---0}}^{\beta_i} \overset{\times}{\ldots}, \\
a &= \ldots \texttt{?}\underbrace{\texttt{10-0?---?}}_{\epsilon_i''}\ldots.
\end{aligned}$$

No carry comes out of the previous block.

In that case, $\delta_i'' = 0$ whatever value δ_i takes, so that $\epsilon_i'' = \gamma_i'' + \beta_i$, $\beta_i \leq \epsilon_i'' \leq \alpha_i + \beta_i$ and only the value of $\gamma_i'' = \gamma_i$ is relevant:

$$\begin{aligned}
P_-(\epsilon_i'') &= P(\gamma_i) \\
&= 2^{-\gamma_i - 1_{\gamma_i \neq \alpha_i}} - 2^{-k} \\
&= 2^{\beta_i - \epsilon_i'' - 1_{\epsilon_i'' \neq \alpha_i + \beta_i}} - 2^{-k}.
\end{aligned}$$

We must substract 2^{-k}, because 0 is considered to make every block overflow.
□

3.3 One block: $d = 1$

If t is made of only one block, the situation is quite simple and theorem 3.6 gives us closed forms for $|C_{t,k,j}| = 2^k P(\epsilon'' = k - j)$ for all j.

Such a t (or an equivalent one) is written $t = 2^k - 2^{k-\alpha}$ ($\simeq 2^\alpha - 1$, i.e. $t = \underbrace{1\ldots1}_{\alpha}\underbrace{0\ldots0}_{\beta=k-\alpha}$) and its weight is $w(t) = \alpha$ with $\alpha \geq 1$.

Proposition 3.7.

$$P(\epsilon'') = \begin{cases} 2^{-\beta} & \epsilon'' = 0 \\ 2^{-|\epsilon''-\beta|}\frac{1-4^{M-m}}{3} & 1 \leq \epsilon'' \leq k-1 \\ 2^{-\alpha} - 2^{-k} & \epsilon'' = k \end{cases},$$

with:

$$\begin{aligned} m &= \min(\epsilon'', \alpha), \\ M &= \max(0, \epsilon'' - \beta). \end{aligned}$$

Proof There is indeed only one block, so that it is its own previous block.

If $\delta = \beta$, then $\gamma'' = 0$ and $\epsilon'' = 0$, so that:

$$P(\epsilon'' = 0) = P_0(\epsilon'' = 0) = 2^{-\beta}.$$

If $\delta \neq \beta$ and $\gamma \neq \alpha$, we have that $0 < \epsilon'' < k$ and:

$$P(\epsilon'') = P_0(\epsilon'') = 2^{-|\epsilon''-\beta|}\frac{1-4^{M-m}}{3}.$$

Finally if $\delta \neq \beta$ and $\gamma = \alpha$, $\epsilon'' = k$ and:

$$P(\epsilon'' = k) = P_-(\epsilon'' = k) = 2^{-\alpha} - 2^{-k}.$$

□

Summing up the above formulas, we get the following theorem:

Theorem 3.8.

$$P_{t,k} = \begin{cases} 2^{-\alpha-\beta}\frac{1-2^{-2\alpha}}{3}, & 1 \leq \alpha \leq \frac{k-1}{2} \\ \frac{1+2^{-2\beta+1}}{3}, & \frac{k-1}{2} \leq \alpha \leq k-1 \end{cases}.$$

For $\alpha = 1$, it reads $S_{1,k} = 2^{k-2} + 1$ and for $\alpha = k-1$, it reads $S_{-1,k} = 2^{k-1}$.

Proof $\beta - 1 < k$ so that:

$$P_{t,k} = \sum_{\epsilon''=0}^{\beta-1} P_0(\epsilon'').$$

Moreover $\beta - \epsilon''$ is always positive so that $|\beta - \epsilon''| = \beta - \epsilon''$ and $M = 0$. Finally $m = \epsilon''$ as long as $\epsilon'' \leq \alpha$ which is always true iff $\beta - 1 \leq \alpha$ or equivalently $\frac{k-1}{2} \leq \alpha$.

If $0 < \alpha < \frac{k-1}{2}$, the computation is:

$$\begin{aligned}
P_{t,k} &= 2^{-\beta} + \sum_{\epsilon''=1}^{\alpha-1} 2^{\epsilon''-\beta}\frac{1-4^{-\epsilon''}}{3} + \sum_{\epsilon''=\alpha}^{\beta-1} 2^{\epsilon''-\beta}\frac{1-4^{-\alpha}}{3} \\
&= 2^{-\beta} + \frac{2^{-\beta}}{3}\sum_{\epsilon''=1}^{\alpha-1}(2^{\epsilon''} - 2^{-\epsilon''}) + \frac{2^{-\beta}(1-4^{-\alpha})}{3}\sum_{\epsilon''=\alpha}^{\beta-1} 2^{\epsilon''} \\
&= 2^{-\beta} + \frac{2^{-\beta}}{3}\left((2^{\alpha}-1) + 2.(2^{-\alpha}-1)\right) + \frac{2^{-\beta}(1-4^{-\alpha})}{3}2^{\alpha}(2^{\beta-\alpha}-1) \\
&= 2^{-\beta} + \frac{2^{\alpha-\beta} - 2^{-\beta} + 2^{-\alpha-\beta+1} - 2^{-\beta+1}}{3} + \frac{1 - 2^{-2\alpha} - 2^{\alpha-\beta} + 2^{-\alpha-\beta}}{3} \\
&= 2^{-\beta} + \frac{1 - 3.2^{-\beta} - 3.2^{-\alpha-\beta} - 2^{-2\alpha}}{3} \\
&= 2^{-\alpha-\beta}\frac{1-2^{-2\alpha}}{3}.
\end{aligned}$$

If $\frac{k-1}{2} \leq \alpha < k$, the calculation is somewhat easier:

$$\begin{aligned}
P_{t,k} &= 2^{-\beta} + \sum_{\epsilon''=1}^{\beta-1} 2^{\epsilon''-\beta}\frac{1-4^{-\epsilon''}}{3} \\
&= 2^{-\beta} + \frac{2^{-\beta}}{3}\sum_{\epsilon''=1}^{\beta-1}(2^{\epsilon''} - 2^{-\epsilon''}) \\
&= 2^{-\beta} + \frac{2^{-\beta}}{3}\left((2^{\beta}-1) + 2.(2^{-\beta}-1)\right) \\
&= 2^{-\beta} + \frac{1 - 2^{-\beta} + 2^{-2\beta+1} - 2^{-\beta+1}}{3} \\
&= \frac{1 + 2^{-2\beta+1}}{3}.
\end{aligned}$$

□

3.4 A helpful constraint: $\min_i(\alpha_i) \geq B - 1$

Until the end of this section we add the following constraint on t:

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d}\beta_i - 1 = B - 1 = k - w(t) - 1.$$

That condition tells us that, if a is in $S_{t,k}$, a carry has to go through each subblock of 1s, i.e. $\gamma_i'' \neq \alpha_i$. Indeed, if $\gamma_i'' = \alpha_i$, then $\delta_i'' < \beta_i$ and $\epsilon_i'' = \gamma_i'' + \beta_i - \delta_i'' \geq \alpha_i + 1 \geq B$, so that $a \notin S_{t,k}$. So if $a \in S_{t,k}$, each block overflows and we are in a situation where they are kind of independent.

In fact, if $\forall i$, $\gamma_i'' \neq \alpha_i$, then $\gamma_i'' = \gamma_i'$ and $\delta_i'' = \delta_i'$.

If $\forall i$, $\delta_i'' = \beta_i$, then $\gamma_i'' = \gamma_i' = 0$ and $\delta_i'' = \delta_i' = \beta_i$.

If there are a $\delta_i'' \neq \beta_i$ and a $\gamma_i'' = \alpha_i$, then $\sum_{i=1}^d \gamma_i'' \geq B > \sum_{i=1}^d \delta_i''$. Moreover $\sum_{i=1}^d \gamma_i' \geq \sum_{i=1}^d \gamma_i''$ and $B > \sum_{i=1}^d \delta_i'$, so that $\sum_{i=1}^d \gamma_i' \geq \sum_{i=1}^d \delta_i'$.

Finally, we have an equivalence between $r(a,t) > w(t)$ and $\sum_{i=1}^d \gamma_i' < \sum_{i=1}^d \delta_i'$.

Proposition 3.9.

$$P_{t,k} = \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} 2^{-\Delta-\Gamma-2d} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} 2^{2|\{i|\delta_i=\beta_i\}|} 1_{\delta_i'=\beta_i,\gamma_i'=0}.$$

Proof

$$\begin{aligned}
P_{t,k} &= P\left[\sum_d \gamma' < \sum_d \delta'\right] \\
&= \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} P(\gamma',\delta') \\
&= \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} \prod_d P(\gamma_i',\delta_i') \\
&= \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} \prod_d P(\delta_i')P(\gamma_i'|\delta_i') \\
&= \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} 2^{-\Delta-d+|\{i|\delta_i=\beta_i\}|} \prod_d P(\gamma_i'|\delta_i') \\
&= \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} 2^{-\Delta-\Gamma-2d+2|\{i|\delta_i=\beta_i\}|} 1_{\delta_i'=\beta_i,\gamma_i'=0} \\
&= \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} 2^{-\Delta-\Gamma-2d} \sum_{\substack{\sum_d \gamma_i'=\Gamma \\ 0\le\gamma_i'}} \sum_{\substack{\sum_d \delta_i'=\Delta \\ 0\le\delta_i'\le\beta_i}} 2^{2|\{i|\delta_i=\beta_i\}|} 1_{\delta_i'=\beta_i,\gamma_i'=0}.
\end{aligned}$$

□

We also have that $a \in S_{t,k}$ is equivalent to $\sum_d \epsilon_i' < B$ so that we get the following proposition:

Proposition 3.10.

$$P_{t,k} = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d \epsilon_i''=E \\ 0\le\epsilon_i''}} \prod_d P_0(\epsilon_i'')$$

where:

$$P_0(\epsilon_i'') = \begin{cases} 2^{-\beta_i} & \epsilon_i'' = 0 \\ 2^{-\left|\epsilon_i''-\beta_i\right|} \frac{1-4^{M-m}}{3} & \epsilon_i'' \neq 0 \end{cases},$$

with:

$$m = \min(\epsilon_i'', \alpha_i),$$
$$M = \max(0, \epsilon_i'' - \beta_i).$$

Proof Indeed we cannot have $\gamma_i'' = \alpha_i$ so that each block overflows and:

$$P_{t,k} = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d \epsilon_i'' = E \\ 0 \leq \epsilon_i''}} \prod_d P_0(\epsilon_i'').$$

□

3.5 Asymptotic behavior: $\beta_i \to \infty$

As the β_is go to infinity, the laws of the γ_i's and the δ_i's converge towards laws of independent geometrically distributed variables with parameter $1/2$, so that $P_{t,k} = P\left[\sum \gamma' < \sum \delta'\right]$ converges towards:

$$P\left[\sum_d Geo(1/2) < \sum_d Geo(1/2)\right] = \frac{1}{2}\left(1 - P\left[\sum_d Geo(1/2) = \sum_d Geo(1/2)\right]\right)$$

which is strictly lower than $1/2$ for any $d > 0$.

Proposition 3.11. *For $d \geq 1$:*

$$P_d = P\left[\sum_d Geo(1/2) = \sum_d Geo(1/2)\right] = \frac{1}{4^d} \sum_{S=0}^{\infty} \frac{1}{4^S} \binom{S+d-1}{d-1}^2.$$

In particular $\frac{1}{3^d} \leq P_d \leq \frac{1+3.2^{d-2}}{4^d}$. Moreover $P_1 = 1/3$ and $P_2 = 5/27$.

Proof The computation is quite the same as in the previous subection, but without constraints:

$$\begin{aligned}
P_d = P\left[\sum_d Geo(1/2) = \sum_d Geo(1/2)\right] &= \sum_{S=0}^{\infty} \sum_{\substack{\sum_d \gamma_i = S \\ 0 \leq \gamma_i}} \sum_{\substack{\sum_d \delta_i = S \\ 0 \leq \delta_i}} P(\gamma, \delta) \\
&= \sum_{S=0}^{\infty} \sum_{\substack{\sum_d \gamma_i = S \\ 0 \leq \gamma_i}} \sum_{\substack{\sum_d \delta_i = S \\ 0 \leq \delta_i}} \prod_d P(\gamma_i) \prod_d P(\delta_i) \\
&= \sum_{S=0}^{\infty} \sum_{\substack{\sum_d \gamma_i = S \\ 0 \leq \gamma_i}} \sum_{\substack{\sum_d \delta_i = S \\ 0 \leq \delta_i}} \frac{1}{2^{S+d}} \frac{1}{2^{S+d}} \\
&= \frac{1}{4^d} \sum_{S=0}^{\infty} \frac{1}{4^S} \sum_{\substack{\sum_d \gamma_i = S \\ 0 \leq \gamma_i}} \binom{S+d-1}{d-1} \\
&= \frac{1}{4^d} \sum_{S=0}^{\infty} \frac{1}{4^S} \binom{S+d-1}{d-1}^2.
\end{aligned}$$

We bound the sum of squares from below by:

$$\frac{1}{4^d}\sum_{S=0}^{\infty}\frac{1}{4^S}\binom{S+d-1}{d-1} = \frac{1}{4^d}\frac{1}{(1-1/4)^d}$$
$$= \frac{1}{3^d},$$

and from above by:

$$\frac{1}{4^d}\left(1+\sum_{S=1}^{\infty}\frac{2^{S+d-2}}{4^S}\binom{S+d-1}{d-1}\right) = \frac{1}{4^d}+\frac{2^{d-2}}{4^d}\sum_{S=0}^{\infty}\frac{1}{2^S}\binom{S+d-1}{d-1} - \frac{2^{d-2}}{4^d}$$
$$= \frac{1+4^{d-1}-2^{d-2}}{4^d}$$
$$= \frac{1+3.2^{d-2}}{4^d}.$$

Finally, for $d=1$, $\binom{S+d-1}{d-1}=1$ and the sum becomes:

$$P_1 = \frac{1}{4}\frac{1}{1-1/4} = \frac{1}{3};$$

and for $d=2$, $\binom{S+d-1}{d-1}=S+1$ so that:

$$P_2 = \frac{1}{4^2}\sum_{S=0}^{\infty}\frac{(S+1)^2}{4^S}$$
$$= \frac{1}{4}\sum_{S=0}^{\infty}\frac{S^2}{4^S}$$
$$= \frac{1}{4}\left(\frac{2\frac{1}{4^2}}{\left(1-\frac{1}{4}\right)^3}+\frac{\frac{1}{4}}{\left(1-\frac{1}{4}\right)^2}\right)$$
$$= \frac{2}{27}+\frac{1}{9} = \frac{5}{27}.$$

□

We have proved the following theorem:

Theorem 3.12. *Let d be a strictly positive integer. There exists a constant K_d such that if:*

- $\forall i,\ \beta_i \geq K_d$ *and*
- $\min_i \alpha_i \geq B-1$,

then:

$$P_{t,k} < \frac{1}{2}.$$

When the number of blocks, d, goes as well to infinity, $P_{t,k}$ converges toward $1/2$. Indeed $\frac{1}{3^d} \leq P_d \leq \frac{1}{4^d}+\frac{3}{4}\frac{1}{2^d}$ converges towards 0 as d goes to infinity.

3.6 Analytic study: $d = 2$

It is possible to compute the exact value of $|S_{t,k}|$ for a given d and a corresponding set of β_is. It is also worth noting that the order of the β_is does not matter because each subblock behaves the same when a is in $S_{t,k}$, i.e. it overflows.

We did the computation for $d = 2$ where the symmetry of the problem leads to only one situation and gives a quite general result.

Definition 3.13.

$$\begin{aligned} f(x,y) =& \frac{11}{27} + 4^{-x}\left(\frac{2}{9}x - \frac{2}{27}\right) \\ &+ 4^{-y}\left(\frac{2}{9}y - \frac{2}{27}\right) + 4^{-x-y}\left(\frac{20}{27} - \frac{2}{9}(x+y)\right). \end{aligned}$$

Proposition 3.14.

$$P_{t,k} = f(\beta_1, \beta_2).$$

Proof According to proposition 3.10:

$$\begin{aligned} P_{t,k} =& \sum_{E=0}^{B-1} \sum_{\substack{\epsilon_1''+\epsilon_2''=E \\ 0\le\epsilon_1'',\epsilon_2''}} P_0(\epsilon_1'')P_0(\epsilon_2'') \\ =& 2^{-\beta_1-\beta_2}\big(\Sigma_{\epsilon_1''\neq 0,\epsilon_2''\neq 0} \\ &+ \Sigma_{\epsilon_1''=0,\epsilon_2''\neq 0} + \Sigma_{\epsilon_1''\neq 0,\epsilon_2''=0} + \Sigma_{\epsilon_1''=0,\epsilon_2''=0}\big), \end{aligned}$$

where:

$$\begin{aligned} \Sigma_{\epsilon_1''\neq 0,\epsilon_2''\neq 0} =& \sum_{\epsilon_1''=0}^{\beta_1-1} \frac{2^{\epsilon_1''} - 2^{-\epsilon_1''}}{3} \left(\sum_{\epsilon_2''=0}^{\beta_2-1} \frac{2^{\epsilon_2''} - 2^{-\epsilon_2''}}{3} + \sum_{\epsilon_2''=\beta_2}^{\beta_1+\beta_2-1-\epsilon_1''} 2^{-\epsilon_2''} \frac{4^{\beta_2}-1}{3} \right) \\ &+ \sum_{\epsilon_1''=\beta_1}^{\beta_1+\beta_2-1} 2^{-\epsilon_1''} \frac{4^{\beta_1}-1}{3} \sum_{\epsilon_2''=0}^{\beta_1+\beta_2-1-\epsilon_1''} \frac{2^{\epsilon_2''} - 2^{-\epsilon_2''}}{3} \\ \Sigma_{\epsilon_1''=0,\epsilon_2''\neq 0} =& \sum_{\epsilon_2''=0}^{\beta_2-1} \frac{2^{\epsilon_2''} - 2^{-\epsilon_2''}}{3} + \sum_{\epsilon_2''=\beta_2}^{\beta_1+\beta_2-1} 2^{-\epsilon_2''} \frac{4^{\beta_2}-1}{3} \\ \Sigma_{\epsilon_1''\neq 0,\epsilon_2''=0} =& \sum_{\epsilon_1''=0}^{\beta_1-1} \frac{2^{\epsilon_1''} - 2^{-\epsilon_1''}}{3} + \sum_{\epsilon_1''=\beta_1}^{\beta_1+\beta_2-1} 2^{-\epsilon_1''} \frac{4^{\beta_1}-1}{3} \\ \Sigma_{\epsilon_1''=0,\epsilon_2''=0} =& 1. \end{aligned}$$

An easy but quite lengthy and error-prone calculation, which can be checked with a symbolic calculus software, leads to the desired expression. □

The graph of f, computed with Maple™ [9], is given in figures 1 and 2.

Proposition 3.15. *$\forall x, y \geq 1$ in $\mathbb{N}$:*

$$f(x,y) \leq \frac{1}{2}.$$

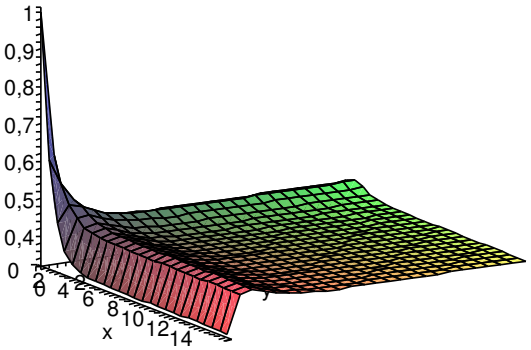

Figure 1: $f(x, y)$ for $0 \leq x, y \leq 15$.

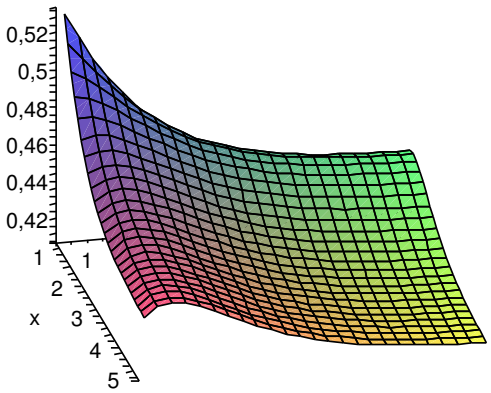

Figure 2: $f(x, y)$ for $1 \leq x, y \leq 5$.

Proof

$$\begin{aligned}\frac{\partial f}{\partial x}(x,y) =& \frac{2}{9}4^{-x}\ln 4(4^{-y}-1)x \\ &+ \frac{2}{9}4^{-x}\left(4^{-y}\ln 4\left(y-\frac{10}{3}\right)-4^{-y}+\frac{1}{3}\ln 4+1\right),\end{aligned}$$

so that for $y>0$, $\frac{\partial f}{\partial x}(x,y)\geq 0$ is equivalent to:

$$x \leq \frac{(\frac{1}{3}+\frac{1}{2\ln 2})4^y + y - \frac{1}{2\ln 2} - \frac{10}{3}}{4^y-1}.$$

We denote the left side of that inequality by $h(y)$. Unfortunately it happens that $h(y)>1$ when $y\geq 1$. However $f(\max(1,h(y)),y)\leq \frac{1}{2}$ for $y\geq 1$, so that $f(x,y)\leq\frac{1}{2}$ for $x,y\geq 1$ in $\mathbb{R}$. We do not prove that here for the sake of simplicity, but only that $f(x,y)\leq\frac{1}{2}$ for $x,y\geq 1$ in $\mathbb{N}$ which is the case we are interested in.

Let $g(x)=4^{-x}\left(x-\frac{1}{3}\right)$.

$$g'(x)=\left(1+\frac{\ln 4}{3}-\ln 4x\right)4^{-x}$$

so that for $x\geq 0$, $g'(x)\geq 0 \Leftrightarrow x\leq \frac{1}{2\ln 2}+\frac{1}{3}=x_{\max}$.

Moreover $1<x_{\max}\approx 1.054<2$ so that

$$g(x)\leq \max(g(1),g(2))=g(1)=\frac{1}{6}.$$

Then

$$f(x,y)\leq \frac{11}{27}+\frac{1}{27}+\frac{1}{27}+\frac{1}{54}=\frac{1}{2}.$$

□

We remark that $f(x,y)\to\frac{11}{27}$ when $x,y\to\infty$ which confirms our previous result for $d=2$.

We have proved:

Theorem 3.16. *If t verifies the following constraint:*

- $d=2$,
- $\alpha_1,\alpha_2\geq B-1$,

then:

$$|S_{t,k}|\leq 2^{k-1}.$$

3.7 Extremal value: $\beta_i=1$

We add another constraint:

$$\forall i,\beta_i=1.$$

The previous one becomes:

$$\min_i(\alpha_i)\geq B-1=d-1.$$

Theorem 3.17. *Let t verify the two following constraints:*

- $\forall i, \beta_i = 1$,
- $\min_i(\alpha_i) \geq B - 1 = d - 1$.

Then:

$$|S_{t,k}| = 2^{k-1}.$$

Proof We equivalently show that $P_{t,k} = 1/2$.

$$\begin{aligned} P_{t,k} &= \sum_{\Delta=1}^{d} \sum_{\Gamma=0}^{\Delta-1} 2^{-\Gamma+\Delta-2d} \sum_{\substack{\sum_d \delta'_i = \Delta \\ \delta'_i = 0,1}} \sum_{\substack{\sum_d \gamma'_i = \Gamma \\ 0 \leq \gamma'_i}} 1_{\delta'_i=1, \gamma'_i=0} \\ &= 2^{-2d} \sum_{\Gamma=0}^{d-1} 2^{-\Gamma} \sum_{\Delta=\Gamma+1}^{d} 2^{\Delta} \binom{d}{\Delta} \binom{\Gamma + d - \Delta - 1}{d - \Delta - 1}. \end{aligned}$$

The above sum is difficult to evaluate but could be of interest for comparison with other cases. Using $\epsilon'_i = \gamma'_i + (1 - \delta'_i)$, $P_{t,k}$ becomes:

$$\begin{aligned} P_{t,k} &= \sum_{E=0}^{d-1} 2^{-E-d} \sum_{\substack{\sum_d \epsilon'_i = E \\ 0 \leq \epsilon'_i}} 1 \\ &= 2^{-d} \sum_{E=0}^{d-1} 2^{-E} \binom{E + d - 1}{d - 1} \\ &= \frac{2^{d-1}}{2^d} \\ &= \frac{1}{2}. \end{aligned}$$

In that case we can also see $\epsilon'_i = \gamma'_i + (1 - \delta'_i) = \gamma_i(1 - \delta_i)$ as the number of `0`s at the end of each block:

$$\begin{aligned} t &= \texttt{1--10...1--10...1--10}, \\ a &= \texttt{?}\underbrace{\texttt{10-0}}_{\epsilon_1}\texttt{...?}\underbrace{\texttt{10-0}}_{\epsilon_i}\texttt{...?}\underbrace{\texttt{10-0}}_{\epsilon_d}, \end{aligned}$$

and directly compute $P(\epsilon'_i) = 2^{-\epsilon'_i - 1}$. □

As a byproduct we get the interesting combinatorial equality:

Corollary 3.18.

$$\sum_{\Gamma=0}^{d-1} 2^{-\Gamma} \sum_{\Delta=\Gamma+1}^{d} 2^{\Delta} \binom{d}{\Delta} \binom{\Gamma + d - \Delta - 1}{d - \Delta - 1} = 2^{2d-1}.$$

And using corollary 2.20, we prove the conjecture in the following case:

Corollary 3.19. *Let t verify the two following constraints:*

- $\forall i, \beta_i = 1$,
- $\min_i(\alpha_i) \geq B - 1 = d - 1$.

Then:

$$|S_{-t,k}| \leq 2^{k-1}.$$

Proof According to 2.20, $|S_{t,k}| + |S_{-t,k}| \leq 2^k$ so that $|S_{-t,k}| \leq 2^{k-1}$. □

We conjecture that the converse of theorem 3.17 is also true, i.e. those numbers are the only ones reaching the bound of the original conjecture 0.1.

Conjecture 3.20. *$S_{t,k} = 2^{k-1}$ iff t verifies the two following constraints:*

- $\forall i, \beta_i = 1$,
- $\min_i(\alpha_i) \geq B - 1 = d - 1$.

4 An inductive approach

The idea of this section is to fix $t \in \mathbb{N}$ and to study the behavior of $S_{t,k}$ as k grows. Obviously as long as $2^k < t$, the binary expansion of $t \mod 2^k - 1$ has an inconsistent behavior. Therefore we define:

Definition 4.1 (Length)**.** *Let t be a natural integer. Its binary length is defined to be the smallest integer k such that $t \leq 2^k$. We denote it by $l(t)$.*

Indeed for $k \geq l(t)$, the binary expansion of t on $k+1$ bits is that of t on k bits with a `0` prepended.

4.1 Overflow and inertia

We split $C_{t,k,i}$ according to the value of the sum $a + t$ in $\mathbb{Z}$.

Definition 4.2.
- $I_{t,k,i} = \left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} | r(a,t) = w(t) - i, a + t < 2^k - 1 \text{ in } \mathbb{Z}\right\}$, *the* inert *modular integers.*
- $O_{t,k,i} = \left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} | r(a,t) = w(t) - i, a + t \geq 2^k - 1 \text{ in } \mathbb{Z}\right\}$, *the* overflowing *modular integers.*

Remember that $r(0,t) = k$, so that $0 \in O_{t,k,w(t)-k}$.
We define $I_{t,k} = \bigsqcup_{i \in \mathbb{Z}} I_{t,k,i}$ and $O_{t,k} = \bigsqcup_{i \in \mathbb{Z}} O_{t,k,i}$.

Lemma 4.3.

$$|C_{t,k,i}| = |I_{t,k,i}| + |O_{t,k,i}|.$$

We want to increase k when t is fixed. Considering the binary string associated with a modular integer, we write down $0a$ and $1a$ for the binary strings on $k+1$ bits associated with a and $2^k + a$ (i.e. the binary string on k bits of a with a `0` or a `1` prepended). We note that $2^k - 1$ which is equal to 0 in $\mathbb{Z}/(2^k - 1)\mathbb{Z}$ but not in $\mathbb{Z}/(2^{k+1} - 1)\mathbb{Z}$ can not be described as $0a$ or $1a$ for $a \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$.

If $k \geq l(t)$ and $a \in I_{t,k,i}$, then $0a$ and $1a$ are in $I_{t,k+1,i}$.

Unfortunately the situation is more complicated for $O_{t,k,i}$; if $a \neq 0, -t \in O_{t,k,i}$, then $1a$ is in $O_{t,k+1,i-1}$ and $0a$ is in $I_{t,k+1,j}$ with $j \geq i$.

If $a = 0$, then $a \in O_{t,k,w(t)-k}$, $0a = 0 \in O_{t,k+1,w(t)-k-1}$ and $1a = 2^k \in I_{t,k+1,w(t)}$.

If $a = -t$, then $a \in O_{t,k,w(t)-k}$, $0a = \bar{t}^k \in I_{t,k+1,w(t)}$ and $1a = -t \in O_{t,k+1,w(t)-k-1}$.

Finally, $2^k - 1 = 0\underbrace{\texttt{1}\ldots\texttt{1}}_{=k} \in I_{t,k,w(t)-k}$.

The following lemma summarizes the above discussion:

Lemma 4.4.

$$O_{t,k+1,i-1} = \begin{cases} 1O_{t,k,i} & \text{if } i < w(t) - k \\ 1\left(O_{t,k,i} \setminus \{0\}\right) \sqcup \{0\} & \text{if } i = w(t) - k \end{cases},$$
$$I_{t,k+1,i} \supset 0I_{t,k,i} \sqcup 1I_{t,k,i}.$$

4.2 Asymptotic behavior

Lemma 4.5. *For $k \geq w(t) + l(t)$, if $i \geq 0$, then $O_{t,k,i} = \varnothing$.*

Proof Indeed $t = \underbrace{\texttt{0}\ldots\texttt{0}}_{\geq w(t)}\ldots$, so $a = {}^{\leftarrow}\underbrace{\texttt{1}\ldots\texttt{1}}_{\geq w(t)}{}^{\leftarrow}\ldots$ and $r(a,t) > w(t)$. □

Theorem 4.6. *For $k \geq w(t) + l(t)$:*

$$|S_{t,k+1}| = 2\,|S_{t,k}| - 1.$$

Proof Since $k \geq w(t) + l(t)$, $O_{t,k,i} = \varnothing$ for $i \geq 0$ so that:

$$I_{t,k+1,i} = \begin{cases} 0I_{t,k,i} \sqcup 1I_{t,k,i} & \text{for } 0 \leq i < w(t) \\ 0I_{t,k,i} \sqcup 1I_{t,k,i} \sqcup \left\{2^k, \bar{t}^k\right\} & \text{for } i = w(t) \end{cases},$$

and:

$$\begin{aligned} |E_{t,k+1} \sqcup T_{t,k+1}| &= \sum_{i \geq 0} |I_{t,k+1,i}| + |O_{t,k+1,i}| \\ &= \sum_{i \geq 0} |I_{t,k+1,i}| \\ &= 2\sum_{i \geq 0} |I_{t,k,i}| + 2 \\ &= 2\,|E_{t,k} \sqcup T_{t,k}| + 2. \end{aligned}$$

Then:

$$\begin{aligned} |S_{t,k+1}| &= 2^{k+1} - 1 - |E_{t,k+1} \sqcup T_{t,k+1}| \\ &= 2(2^k - 1 - |E_{t,k} \sqcup T_{t,k}|) - 1 \\ &= 2\,|S_{t,k}| - 1. \end{aligned}$$

□

Unfortunately that equality is not true for $l(t) \leq k < l(t) + w(t)$, and it can even happen that $|S_{t,k+1}| > 2\,|S_{t,k}|$. However experimental results suggest that as soon as $k \geq l(t) + 2$ the following inequality is true:

Conjecture 4.7. *For $k \geq l(t) + 2$:*

$$|S_{t,k+1}| \leq 2\,|S_{t,k}|\,.$$

5 Other works

We now compare our results with those of Cusick, Li and Stanica [6], and those of Carlet [2].

5.1 Cusick et al.

In [6], Cusick et al. prove the conjecture in some specific cases:

- $w(t) = 1, 2$,
- $t = 2^k - t'$ with $w(t') \leq 2$ and t' even,
- $t = 2^k - t'$ with $w(t') \leq 4$ and t' odd.

by splitting each case in several subcases and using specific counting arguments for each one. We compare their results with ours.

The first case is treated by different theorems:

- $w(t) = 1$ iff $t \simeq 1$, so this case is taken care of by theorem 3.8.
- $w(t) = 2$ iff $t \simeq 3$ which is included in theorem 3.8 or $d = 2$ and $\alpha_1 = \alpha_2 = 1$ which is included in the corollary of theorem 3.17.

The second one reads $t = 2^k - t' = \overline{t'}$ with $w(t') \leq 2$ and t' even, i.e. $w(t) \geq k - 2$ and $t = 1 \mod 2$. So t is either made of one block which is included in theorem 3.8, or two blocks with $\beta_1 = \beta_2 = 1$ which is included in theorem 3.17.

The last one reads $t = 2^k - t' = \overline{t'}$ with $w(t') \leq 4$ and t' odd, i.e. $w(t) \geq k-4$ and $t = 0 \mod 2$. The subcases $w(t) = k-1, k-2$ are included in our theorems just like in the previous case. The only subcases not directly included in our theorems 3.8, 3.16 and 3.17 when $w(t) = k - 3$ are:

- when $w(t) = k - 3, d = 2$:
  - `10010` but it is taken care of by the corollary of theorem 3.17,
  - `001101` and `110010` wich can be directly computed,
- when $w(t) = k - 3, d = 3$:
  - `101010` but it is taken care of by theorem 2.21,
  - one or two, but not three, α_is equal 1, which is not treated by our theorems.

We also miss several subcases when $w(t) = k - 4$.

Their approach kind of lacks a general strategy to tackle the conjecture, but points out the importance of what we call $r(a, t)$, the number of carries.

5.2 Carlet

In [2], Carlet proves the conjecture in the following cases:

- $w(t) = 0, 1$ and
- $t = 2^i - 2^j$,

using affine functions and multisets. Both these results deal with numbers made of one block and are included in theorem 3.8.

6 Toward a complete proof

The numbers for which $P_{t,k}$ is the nearest to the bound of the conjecture seem to be the ones which verify the constraint $\min(\alpha_i) \geq B - 1$, and especially the ones which also verify $\forall i,\ \beta_i = 1$. Moreover puncturing a `1` of a binary string seems to make $P_{t,k}$ smaller most of the time.

We consequently hope to be able to completely solve the conjecture using one of the following strategies:

- Show that any number gives a smaller set than an *extremal* one by induction (i.e. by puncturing `1`s, even so that different blocks merge) and by comparing different expressions of $P_{t,k}$.
- Show that the conjecture is true for every number which verifies the constraint $\min(\alpha_i) \geq B - 1$ and then that the numbers which do not, give smaller sets by induction (i.e. by puncturing `1`s, but without merging different blocks) and by comparing different expressions of $P_{t,k}$.

References

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

[2] Claude Carlet. Private communication, 2009.

[3] Claude Carlet and Keqin Feng. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In *Advances in Cryptology - ASIACRYPT 2008*, pages 425–440. Springer-Verlag, 2008.

[4] Nicolas Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - CRYPTO 2003*, pages 176–194. Springer-Verlag, 2003.

[5] Nicolas Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology — EUROCRYPT 2003*, pages 345–359. Springer-Verlag, 2003.

[6] T. W. Cusick, Yuan Li, and Pantelimon Stanica. On a combinatoric conjecture. Cryptology ePrint Archive, Report 2009/554, 2009. `http://eprint.iacr.org/`.

[7] J.F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.

[8] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Professional, 2 edition, March 1994.

[9] Michael B. Monagan, Keith O. Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005.

[10] Ziran Tu and Yingpu Deng. A conjecture on binary string and its applications on constructing boolean functions of optimal algebraic immunity. Cryptology ePrint Archive, Report 2009/272, 2009. http://eprint.iacr.org/.