On the Number of Carries Occuring in an Addition mod $2^k - 1$

Jean-Pierre Flori* Hugues Randriam*

May 16, 2011

Abstract

In this paper we study the number of carries occurring while performing an addition modulo $2^k - 1$. For a fixed modular integer t, it is natural to expect the number of carries occurring when adding a random modular integer a to be roughly the Hamming weight of t. Here we are interested in the number of modular integers in $\mathbb{Z}/(2^k - 1)\mathbb{Z}$ producing strictly more than this number of carries when added to a fixed modular integer $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$. In particular it is conjectured that less than half of them do so. An equivalent conjecture was proposed by Tu and Deng in a different context [8].

Although quite innocent, this conjecture has resisted different attempts of proof [4, 5, 3, 2] and only a few cases have been proved so far. The most manageable cases involve modular integers t whose bits equal to `0` are sparse. In this paper we continue to investigate the properties of $P_{t,k}$, the fraction of modular integers a to enumerate, for t in this class of integers. Doing so we prove that $P_{t,k}$ has a polynomial expression and describe a closed form of this expression. This is of particular interest for computing the function giving $P_{t,k}$ and studying it analytically. Finally we bring to light additional properties of $P_{t,k}$ in an asymptotic setting and give closed forms for its asymptotic values.

1 Introduction

For a fixed modular integer $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, it is natural to expect the number of carries occurring when adding a random modular integer $a \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$ to be roughly the Hamming weight of t. Following this idea, it is of interest to study the distribution of the number of carries around this value. Quite unexpectedly the following conjecture, indicating a kind of regularity, seems to be verified:

Conjecture 1.1. *Let $S_{t,k}$ denote the following set:*

$$S_{t,k} = \left\{ a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} | r(a,t) > w(t) \right\},$$

and $P_{t,k}$ the fraction *of modular integers in $S_{t,k}$:*

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

Then:

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

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

(We are fully aware that there are only $2^k - 1$ elements in $\mathbb{Z}/(2^k-1)\mathbb{Z}$, but we will often use the abuse of terminology we made above and speak of *fraction*, *probability* or *proportion* for $P_{t,k}$.) An equivalent conjecture was originally proposed by Tu and Deng [8] in a different context. For the connection between the conjecture of Tu and Deng and the one given here, we refer the reader to [4]. Tu and Deng verified computationally the validity of their assumption for $k \leq 29$.

Up to now, different attempts [4, 5, 3, 2] were conducted and lead to partial proof of the conjecture in very specific cases. A list of the different cases proven to be true can be found in [5, Section 5]. Unfortunately a direct proof or a simple recursive one seems hard to find [5, Section 4]. What however came out of these works is that supposing that t has a high Hamming weight [3, 2] or more generally that its `0` bits are sparse [4, 5], greatly simplifies the study of $P_{t,k}$. This condition casts a more algebraic and probabilistic structure upon it.

In this paper we restrict ourselves to this class of numbers. We do not prove any further cases of the conjecture, but extend the study of $P_{t,k}$ as a function of t for this class of numbers. It is organized as follows. In the first section we recall definitions and results found in [4]. In the second section we explore the algebraic nature of $P_{t,k}$, deduce a closed-form expression for it as well as additional properties that this expression verifies. This is of particular interest for computing the function giving $P_{t,k}$ and studying it analytically. In the third section we analyse the probabilistic nature of $P_{t,k}$, find useful closed forms for the asymptotic value of $P_{t,k}$ and give relations verified by different limits.

1.1 Notations

Unless stated otherwise, we use the following notations:

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

Moreover we will assume that $t \neq 0$. The case $t = 0$ is trivial and can be found in [4, Proposition 2.1].

The Hamming (or binary) weight of a natural or modular integer is defined as follows.

Definition 1.2 (Hamming Weight)**.**

- *For $a \in \mathbb{N}$, $w(a)$ is the weight of a, i.e. the number of `1`s in its binary expansion.*
- *For $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $w(a)$ is the weight of its unique representative in $\{0, \ldots, 2^k - 2\}$.*

The number of carries is then defined as follows.

Definition 1.3. *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. By convention we set:

$$r(0,t) = k,$$

i.e. 0 behaves like the binary string $\underbrace{\texttt{1}\ldots\texttt{1}}_{k}$. We also remark that $r(-t,t) = k$.

The set $S_{t,k}$ is described as

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

We recall that t can multiplied by any power of 2 (which corresponds to rotating its binary expansion) without affecting the value of $P_{t,k}$ [4, Proposition 2.2].

1.2 A Block Splitting Pattern

To compute $P_{t,k}$, a fruitful idea is to split t in several blocks and perform the computation in each block as independently as possible. Here we recall the splitting pattern defined in [4].

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 1.4.

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

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

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

Definition 1.5.

$$t = \overbrace{1\texttt{---}1}^{\alpha_1}\overbrace{0\texttt{---}0}^{\beta_1}\ldots\overbrace{1\texttt{---}1}^{\alpha_i}\overbrace{0\texttt{---}0}^{\beta_i}\ldots\overbrace{1\texttt{---}1}^{\alpha_d}\overbrace{0\texttt{---}0}^{\beta_d},$$

$$a = \underbrace{\texttt{?10-0}}_{\gamma_1}\underbrace{\texttt{?01-1}}_{\delta_1}\ldots\underbrace{\texttt{?10-0}}_{\gamma_i}\underbrace{\texttt{?01-1}}_{\delta_i}\ldots\underbrace{\texttt{?10-0}}_{\gamma_d}\underbrace{\texttt{?01-1}}_{\delta_d},$$

i.e. γ_i is the number of `0`s in front of the end of the `1`s sub-block of t_i and δ_i is the number of `1`s in front of the end of the `0`s sub-block of t_i. One should be aware that γ_is and δ_is depend on a and are considered as variables.

Then $\alpha_i - \gamma_i$ is the number of carries occurring in the ith block, but only if no carry comes out of the previous block.

If a carry comes out of the previous block, the situation is more complicated because we must take into account the fact that it will propagate in the `0` sub-block and could even propagate into the `1` sub-block if $\delta_i = \beta_i$. Therefore we define γ'_i as follows:

- if $\delta_i \neq \beta_i$, we define $\gamma'_i = \gamma_i$ as before,
- if $\delta_i = \beta_i$, we define $\gamma'_i = 0$ (i.e. the carry coming from the previous block goes through the `0`s sub-block so the `1`s sub-block always produces α_i carries).

We define $\delta'_i = \delta_i$ for notation consistency. Then $\alpha_i - \gamma'_i + \delta'_i$ is the number of carries occurring if a carry comes out of the previous block.

Unfortunately 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 and the distributions are as follows:

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

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

Finally, for computational reasons, it will sometimes be easier to count the number of carries *not* occurring within a block. Hence we define $\epsilon_i = \gamma_i + \delta_i$ and $\epsilon'_i = \gamma'_i + \beta_i - \delta'_i$. It is the number of carries lost in the ith block depending on whether a carry comes out of the previous block or not.

1.3 The Constrained Case

It is now time to define what we understand by *sparse* `0` bits. Informally we want each of the blocks defined in the previous subsection to have a large number of `1` and only a few `0`. Mathematically we impose that t verifies the following constraint:

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

Under that hypothesis, if a is in $S_{t,k}$, then a carry has to go through each sub-block of `1`s. Therefore each block is independent of the other ones. Moreover it can be shown that we get an equivalence between $r(a,t) > w(t)$ and $\sum_{i=1}^{d} \gamma'_i < \sum_{i=1}^{d} \delta'_i$, so that:

Proposition 1.6. *[4, Proposition 3.8]*

$$P_{t,k} = P\left[\sum_d \gamma' < \sum_d \delta'\right].$$

Formulated in a different way, it also means that for such $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $a \in S_{t,k}$ is equivalent to $\sum_d \epsilon'_i < B = k - w(t)$ and we get the following proposition:

Proposition 1.7. *[4, Proposition 3.9]*

$$P_{t,k} = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} \prod_d P(e_i)$$

where $P(e_i)$ is defined by:

$$P(e_i) = P(\epsilon'_i = e_i) = \begin{cases} 2^{-\beta_i} & \text{if } e_i = 0, \\ \frac{2^{-\beta_i}}{3}(2^{e_i} - 2^{-e_i}) & \text{if } 0 < e_i < \beta_i, \\ \frac{2^{\beta_i} - 2^{-\beta_i}}{3} 2^{-e_i} & \text{if } \beta_i \leq e_i. \end{cases}$$

As soon as a given set of β_is and α_is verifies the constraint $\min_i \alpha_i \geq B - 1$, the above expression shows that the value of $P_{t,k}$ for the corresponding t and k only depends on the value of the β_is. Furthermore it does not depend on the order of the β_is and so is a symmetric function of them, whence the following definition.

Definition 1.8. *We denote by:*

$$f_d(\beta_1, \ldots, \beta_d)$$

the value of $P_{t,k}$ for any t made of d blocks, with that set of β_is and any set of of α_is such that $\min_i \alpha_i \geq B - 1$. Obviously f_d is a symmetric function of the β_is.

This function will be our main object of interest in this paper.

2 A Closed-Form Expression for $P_{t,k}$

The main goal of this section is to describe a closed-form expression of f_d and its properties.

After giving some experimental results in Subsection 2.1, we will prove that f_d has the following "polynomial" expression.

Proposition 2.1. *For any $d \geq 1$, f_d can be written in the following form:*

$$f_d(\beta_1, \ldots, \beta_d) = \sum_{I \subset \{1,\ldots,d\}} 4^{-\sum_{i\in I} \beta_i} P_d^{|I|}(\{\beta_i\}_{i\in I}),$$

where P_d^n is a symmetric multivariate polynomial in n variables of total degree $d-1$ and of degree $d-1$ in each variable if $n > 0$. If $n = 0$, then $P_d^0 = \frac{1}{2}(1 - P_d)$, the value computed in 3.12.

The proof of this result covers three subsections:

1. in Subsection 2.2, we split the expression giving f_d as a sum into smaller pieces and establish a recursion relation in d,
2. in Subsection 2.3, we study the expression of the residual term appearing in this relation,
3. in Subsection 2.4, we put the pieces back together to conclude.

Once this proposition is shown, we will be allowed to denote by $a^{d,n}_{(i_1,\ldots,i_n)}$ the coefficient of $P_d^n(x_1, \ldots, x_n)$ of multi-degree $(i_1, \ldots, i_n)$ normalized by 3^d. In Subsection 2.5 we give simple expressions for some specific values of $a^{d,n}_{(i_1,\ldots,i_n)}$ as well as the following general expression.

Proposition 2.2. *Suppose that $i_1 > \ldots > i_m \neq 0 > i_{m+1} = 0 > \ldots > i_n = 0$ and $m > 0$. Let us denote by l the sum $l = i_1 + \ldots + i_n > 0$ (i.e. the total degree of the monomial). Then*

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} b^{d,n}_{l,m},$$

with

$$b^{d,n}_{l,m} = \sum_{\mathfrak{i}=0}^{n-m} \binom{n-m}{\mathfrak{i}} \sum_{\mathfrak{j}=0}^{d-n} \binom{d-n}{\mathfrak{j}} \sum_{k_j \geq 0, j \in I \cup J, 1 \leq j \leq m} \frac{(l+S-m)!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ l+S-m \end{bmatrix} \right) \prod_{j\in J} \frac{A_{k_j}}{k_j!} \prod_{j\in I} \frac{A_{k_j} - 3_{k_j=0}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j-1}}{|k_j - 1|!}.$$

Within $b^{d,n}_{l,m}$, the following notations are used:

- $I = \{m+1, \ldots, m+\mathfrak{i}\}$;
- $J = \{n+1, \ldots, n+\mathfrak{j}\}$;
- $S = \sum_{j\in I\cup J, 1\leq j\leq m} k_j$;
- $h = d - m - \mathfrak{j} - \mathfrak{i}$;

and

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & \text{if } j > 0, \\ -\frac{13}{6} & \text{if } j = 0, \\ 1 & \text{if } j = -1. \end{cases}$$

Here A_i is a sum of Eulerian numbers and B_i a Bernoulli number which are described in Subsection 2.3.

Finally, we prove in Subsection 2.6 an additional property predicted experimentally.

Proposition 2.3. *For* $0 < j \leq i$,

$$a^{d,n}_{(i,j,\ldots)} = \frac{i+1}{j} a^{d,n}_{(i+1,j-1,\ldots)};$$

i.e. the value of $b^{d,n}_{l,m}$ *does not depend on* m.

2.1 Experimental Results

For $d = 1$, by [4, Theorem 3.6], we have:

$$f_1(\beta_1) = \frac{2}{3} 4^{-\beta_1} + \frac{1}{3}.$$

The case $d = 2$ has been treated in [4, Proposition 3.12] and leads to a similar expression:

$$\begin{aligned} f_2(\beta_1, \beta_2) = \frac{11}{27} &+ 4^{-\beta_1} \left(\frac{2}{9}\beta_1 - \frac{2}{27} \right) \\ &+ 4^{-\beta_2} \left(\frac{2}{9}\beta_2 - \frac{2}{27} \right) + 4^{-\beta_1-\beta_2} \left(\frac{20}{27} - \frac{2}{9}(\beta_1 + \beta_2) \right). \end{aligned}$$

In both these case, f_d has the correct form and has been shown to verify Conjecture 1.1.

The tables in Appendix A give the coefficients of the multivariate polynomials P^n_d for the first few ds. Graphs of some functions derived from f_d are given in Figures 2.1 and 2.1. All of this data was computed using Sage [7], Pynac [10] and Maxima [9].

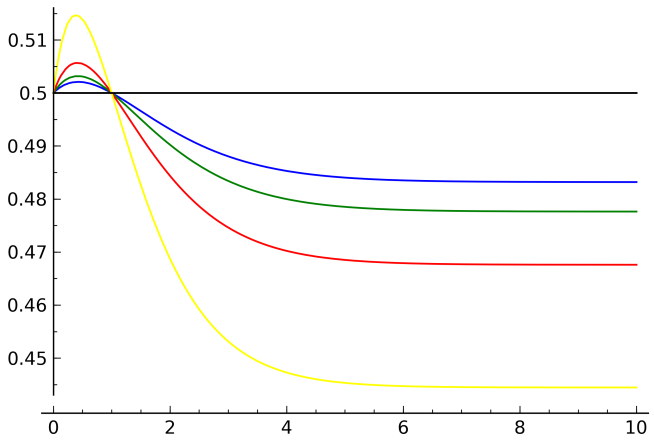

Figure 1: $f_d(\beta_i)$ for $\beta_i = 1$, $i \neq 1$.

Moreover looking at the tables in Appendix A, some additional properties seem to be verified. Here are some examples. The value of $a^{d,d}_{(1,\ldots,1,0)}$ is easy to predict:

$$a^{d,d}_{(1,\ldots,1,0)} = (-1)^{d+1} 2;$$

we prove this in 2.20. There is a recursion relation between coefficients with different ds:

$$a^{d,n+1}_{(i_1,\ldots,i_n,0)} + a^{d,n}_{(i_1,\ldots,i_n)} = 3a^{d-1,n}_{(i_1,\ldots,i_n)};$$

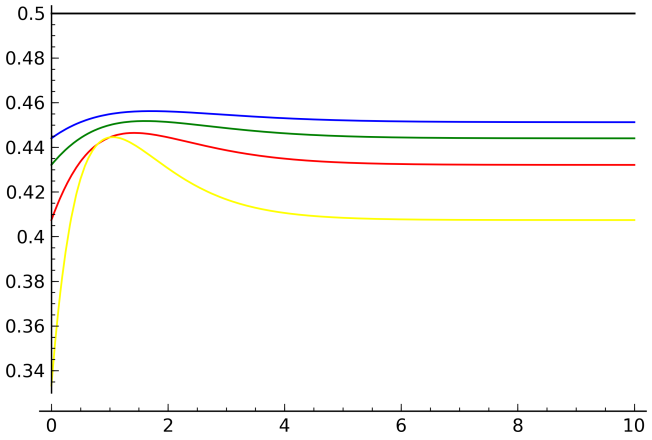

Figure 2: $f_d(\beta_i)$ for $\beta_i = 10$, $i \neq 1$.

this is Corollary 2.19. There is a relation between coefficients with a given d:

$$a^{d,n}_{(i,j,\ldots)} = \frac{i+1}{j} a^{d,n}_{(i+1,j-1,\ldots)};$$

this is Proposition 2.3. All of these results will be proved in the next subsections.

It should also be noted that we already know the value of $f_d(1,\ldots,1)$.

Theorem 2.4. *[4, Theorem 4.14] For $d \geq 1$:*

$$f_d(1,\ldots,1) = \frac{1}{2}.$$

2.2 Splitting the Sum into Atomic Parts

We consider a general $d \geq 1$. From Proposition 1.7:

$$f_d(\beta_1,\ldots,\beta_d) = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} \prod_d P(e_i),$$

where $P(e_i)$ has three different expressions according to the value of e_i:

$$P(e_i) = \begin{cases} 2^{-\beta_i} & \text{if } e_i = 0, \\ \frac{2^{-\beta_i}}{3}(2^{e_i} - 2^{-e_i}) & \text{if } 0 < e_i < \beta_i, \\ \frac{2^{\beta_i} - 2^{-\beta_i}}{3} 2^{-e_i} & \text{if } \beta_i \leq e_i. \end{cases}$$

Let us denote for a vector $X \in \{0,1,2\}^d$:

- the ith coordinate by X_i with $1 \leq i \leq d$;
- $j_k = w_k(X) = |\{i | X_i = k\}|$ for $0 \leq k \leq 2$;
- $B_{0,1} = \sum_{\{i|X_i \neq 2\}} \beta_i$;

- $E_1 = \sum_{\{i|X_i=1\}} e_i$.

We can now define subsets S_X^d of the sum in Proposition 1.7 where each $P(e_i)$ has a specific behavior given by the value of the ith coordinate of such a vector X.

$$S_X^d = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ e_i=0 \text{ if } X_i=0 \\ 0<e_i<\beta_i \text{ if } X_i=1 \\ \beta_i \le e_i \text{ if } X_i=2}} \prod_{i=1}^{n} P(e_i)$$

$$= \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ e_i=0 \text{ if } X_i=0 \\ 0<e_i<\beta_i \text{ if } X_i=1 \\ \beta_i \le e_i \text{ if } X_i=2}} \left(\prod_{\{i|X_i=0\}} 2^{-\beta_i} \prod_{\{i|X_i=1\}} \frac{2^{-\beta_i}}{3}(2^{e_i} - 2^{-e_i}) \prod_{\{i|X_i=2\}} \frac{2^{\beta_i} - 2^{-\beta_i}}{3} 2^{-e_i} \right),$$

so that

$$f_d(\beta_1, \ldots, \beta_d) = \sum_{X \in \{0,1,2\}^d} S_X^d.$$

Here we drop the dependency in the β_is for concision. S_X^d has already some properties of f_d.

Lemma 2.5. *S_X^d is symmetric for each set $\{i|X_i = k\}$ where $k \in \{0,1,2\}$. To compute S_Y where Y is any permutation of X, one has just to permute the β_is accordingly.*

The previous lemma shows that it is enough to study the Xs such that $X = (\overbrace{0, \ldots, 0}^{j_0}, \overbrace{1, \ldots, 1}^{j_1}, \overbrace{2, \ldots, 2}^{j_2})$. The following lemma is obvious.

Lemma 2.6. *$S_{(0,\ldots,0)} = 2^{-\sum_{i=1}^d \beta_i}$ and $S_{(2,\ldots,2)} = 0$.*

And when $j_2 = 0$, S_X^d has a simple expression.

Proposition 2.7. *If $j_2 = 0$ and $X = (\overbrace{0, \ldots, 0}^{j_0}, \overbrace{1, \ldots, 1}^{j_1})$, then*

$$S_X^d = \frac{2^{-\sum_{i=1}^{j_0} \beta_i}}{3^{j_1}} \prod_{i=j_0+1}^{d} (1 + 2 \cdot 4^{-\beta_i} - 3 \cdot 2^{-\beta_i}).$$

Proof This is a simple consequence of the fact that we can sum up in each e_i independently.

$$S_X^d = \frac{2^{-B}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1 \le i \le d}} \prod_{i=j_0+1}^{d} (2^{e_i} - 2^{-e_i}) = \frac{2^{-B}}{3^{|j_1|}} \prod_{i=j_0+1}^{d} \sum_{0<e_i<\beta_i} (2^{e_i} - 2^{-e_i})$$

$$= \frac{2^{-B}}{3^{j_1}} \prod_{i=j_0+1}^{d} (2^{\beta_i} + 2 \cdot 2^{-\beta_i} - 3)$$

$$= 2^{-\sum_{i=1}^{j_0} \beta_i} \prod_{i=j_0+1}^{d} \frac{1 + 2 \cdot 4^{-\beta_i} - 3 \cdot 2^{-\beta_i}}{3}.$$

□

The next proposition is the key to our demonstration. It exhibits a recursion relation between S_X^d for different values of d and will reduce the demonstration of Proposition 2.1 to the case $j_2 = 0$ and the study of a residual term denoted T_X^d.

Proposition 2.8. *For $j_2 \geq 1$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$, we have*

$$S_X^d = 2\frac{1-4^{-\beta_d}}{3}S_X^{d-1} - 2T_X^d,$$

where

$$T_X^d = \frac{4^{-B_{0,1}}}{3^{j_1+j_2}}\prod_{i=j_0+j_1+1}^{d}(1-4^{-\beta_i})\sum_{\substack{0<e_i<\beta_i\\ j_0+1\leq i\leq j_0+j_1}}\prod_{i=j_0+1}^{j_0+j_1}(4^{e_i}-1)\sum_{\substack{0\leq e_i,\sum e_i<B_{0,1}-E_1\\ j_0+j_1+1\leq i\leq d-1}}1.$$

Proof Replacing $P(e_i)$ by its expression, we get

$$\begin{aligned}S_X^d &= \prod_{i=1}^{j_0}2^{-\beta_i}\sum_{\substack{0<e_i<\beta_i\\ j_0+1\leq i\leq j_0+j_1}}\prod_{i=j_0+1}^{j_0+j_1}\frac{2^{-\beta_i}}{3}(2^{e_i}-2^{-e_i})\sum_{\substack{\beta_i\leq e_i,\sum e_i<B-E_1\\ j_0+j_1+1\leq i\leq d}}\prod_{i=j_0+j_1+1}^{d}\frac{2^{\beta_i}-2^{-\beta_i}}{3}2^{-e_i}\\ &= \frac{2^{-B_{0,1}}}{3^{j_1+j_2}}\prod_{i=j_0+j_1+1}^{d}(1-4^{-\beta_i})\sum_{\substack{0<e_i<\beta_i\\ j_0+1\leq i\leq j_0+j_1}}\prod_{i=j_0+1}^{j_0+j_1}(2^{e_i}-2^{-e_i})\sum_{\substack{0\leq e_i,\sum e_i<B_{0,1}-E_1\\ j_0+j_1+1\leq i\leq d}}\prod_{i=j_0+j_1+1}^{d}2^{-e_i},\end{aligned}$$

letting $e_i = e_i - \beta_i$ for $j_0 + j_1 + 1 \leq i \leq d$. We now explicitly compute the sum on e_d:

$$\begin{aligned}S_X^d &= \frac{2^{-B_{0,1}}}{3^{j_1+j_2}}\prod_{i=j_0+j_1+1}^{d}(1-4^{-\beta_i})\sum_{\substack{0<e_i<\beta_i\\ j_0+1\leq i\leq j_0+j_1}}\prod_{i=j_0+1}^{j_0+j_1}(2^{e_i}-2^{-e_i})\\ &\qquad\sum_{\substack{0\leq e_i,\sum e_i<B_{0,1}-E_1\\ j_0+j_1+1\leq i\leq d-1}}\prod_{i=j_0+j_1+1}^{d-1}2^{-e_i}\left(2\left(1-2^{-B_{0,1}+E_1+\sum_{i=j_0+j_1+1}^{d-1}e_i}\right)\right)\\ &= 2\frac{1-4^{-\beta_d}}{3}S_X^{d-1} - 2\frac{4^{-B_{0,1}}}{3^{j_1+j_2}}\prod_{i=j_0+j_1+1}^{d}(1-4^{-\beta_i})\sum_{\substack{0\leq e_i,\sum e_i<B_{0,1}-E_1\\ j_0+j_1+1\leq i\leq d-1}}1\\ &= 2\frac{1-4^{-\beta_d}}{3}S_X^{d-1} - 2T_X^d.\end{aligned}$$

□

2.3 The Residual Term T_X^d

We now study the term T_X^d for $j_2 \geq 1$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$ and show that f_d has the following expression.

Proposition 2.9. *For $j_2 \geq 1$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$,*

$$T_X^d = \frac{1}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i})\Sigma_X^d$$

where

$$\Sigma_X^d = \frac{4^{-\sum_{i=1}^{j_0}\beta_i}}{3^{j_1}(j_2-1)!} \sum_{l=0}^{j_2-1} \begin{bmatrix} j_2-1 \\ l \end{bmatrix} \sum_{k+k_{j_0+1}+\dots+k_{j_0+j_1}=l} \binom{l}{k,k_{j_0+1},\dots,k_{j_0+j_1}} \left(\sum_{i=1}^{j_0}\beta_i\right)^k \Pi_X^d$$

and

$$\Pi_X^d = \prod_{\{j_0\leq j\leq j_0+j_1 | k_j=0\}} \frac{1-4^{-\beta_j}-3\beta_j 4^{-\beta_j}}{3}$$
$$\prod_{\{j_0\leq j\leq j_0+j_1 | k_j\neq 0\}} \left(A_{k_j}(1-4^{-\beta_j}) - \left(\frac{1}{k_j+1}\beta_j^{k_j+1} + \frac{5}{6}\beta_j^{k_j} + \sum_{i=1}^{k_j-1} \binom{k_j}{i} \left(A_i + \frac{B_{i+1}}{i+1}\right)\beta^{k_j-i} \right) 4^{-\beta_j} \right).$$

Σ_X^d is a sum for $I \subset \{j_0+1,\dots,j_0+j_1\}$ of terms of the form $4^{-\sum_{i=1}^{j_0}\beta_i - \sum_{i\in I}\beta_i}$ multiplied by a multivariate polynomial of degree in β_i exactly j_2 if $i \in I$, j_2-1 if $1 \leq i \leq j_0$, 0 otherwise, and of total degree $j_2+|I|-1$.

The end of this subsection is devoted to the proof of this proposition. This is a quite technical part, but it is also of great interest to prove Proposition 2.2.

We denote by R_X^d the sum at the end of T_X^d:

$$R_X^d = \sum_{\substack{0\leq e_i, \sum e_i < B_{0,1}-E_1 \\ j_0+j_1+1\leq i\leq d-1}} 1,$$

this is simply the number of j_2-1-tuples of natural integers such that their sum is strictly less than $B_{0,1}-E_1$; and by Σ_X^d the sum on the e_is for $j_0+1 \leq i \leq j_0+j_1$:

$$\Sigma_X^d = \frac{4^{-B_{0,1}}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\leq i\leq j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (4^{e_i}-1) R_X^d,$$

so T_X^d is given by:

$$T_X^d = \frac{1}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i})\Sigma_X^d.$$

We first check the proposition for $j_2 = 1$. Then $R_X^d = 1$ and the sum Σ_X^d to compute is:

$$\Sigma_X^d = \frac{4^{-B_{0,1}}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\leq i\leq j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (4^{e_i}-1) = \frac{4^{-B_{0,1}}}{3^{j_1}} \prod_{i=j_0+1}^{j_0+j_1} \frac{4^{\beta_i}-1-3\beta_i}{3}$$
$$= \frac{4^{-\sum_{i=0}^{j_0}\beta_i}}{3^{j_1}} \prod_{i=j_0+1}^{j_0+j_1} \frac{1-4^{-\beta_i}-3\beta_i 4^{-\beta_i}}{3},$$

so T_X^d becomes:

$$T_X^d = \frac{1}{3}(1-4^{-\beta_d})\frac{4^{-\sum_{i=0}^{j_0}\beta_i}}{3^{j_1}}\prod_{i=j_0+1}^{j_0+j_1}\frac{1-4^{-\beta_i}-3\beta_i 4^{-\beta_i}}{3}$$

which is what the proposition states.

Let us now proceed to a general $j_2 \geq 1$. In what follows B_i is a Bernoulli number [6, Formula 6.78] (here $B_1 = 1/2$) and $\begin{bmatrix} i \\ j \end{bmatrix}$ is an unsigned Stirling number of the first kind [6, Section 6.1]. We recall that the sum of the n first kth powers is given as a polynomial in n by:

$$\sum_{i=0}^{n} i^k = \frac{1}{k+1}\sum_{i=0}^{k}\binom{k+1}{i}B_i n^{k+1-i}.$$

Here is a classical combinatorial lemma.

Lemma 2.10. *For $n \geq 1$ and $m > 0$, the number of n-tuples of natural integers such that their sum is strictly less than m is given by:*

$$\sum_{\substack{0\leq i_j, 1\leq j\leq n \\ \sum_{j=1}^{n} i_j < m}} 1 = \binom{n+m-1}{n}$$

$$= \frac{1}{n!}\sum_{l=1}^{n}\begin{bmatrix} n \\ l \end{bmatrix} m^l.$$

Proof This is indeed the same thing as the number of $n+1$-tuples of natural integers such that their sum is exactly $m-1$. □

Then the sum R_X^d in T_X^d for $j_2 \geq 1$, which counts the number of $j_2 - 1$-tuples of natural integers such that their sum is strictly less than $B_{0,1} - E_1$, is given by the following expression:

$$R_X^d = \frac{1}{(j_2-1)!}\sum_{l=0}^{j_2-1}\begin{bmatrix} j_2-1 \\ l \end{bmatrix}(B_{0,1}-E_1)^l$$

$$= \frac{1}{(j_2-1)!}\sum_{l=0}^{j_2-1}\begin{bmatrix} j_2-1 \\ l \end{bmatrix}\sum_{k+k_{j_0+1}+\ldots+k_{j_0+j_1}=l}\binom{l}{k, k_{j_0+1}, \ldots, k_{j_0+j_1}}\left(\sum_{i=1}^{j_0}\beta_i\right)^k\prod_{i=j_0+1}^{j_0+j_1}(\beta_i - e_i)^{k_i}.$$

And Σ_X^d becomes:

$$\Sigma_X^d = \frac{4^{-B_{0,1}}}{3^{j_1}}\sum_{\substack{0<e_i<\beta_i \\ j_0+1\leq i\leq j_0+j_1}}\prod_{i=j_0+1}^{j_0+j_1}(4^{e_j}-1)R_X^d$$

$$= \frac{4^{-\sum_{i=1}^{j_0}\beta_i}}{3^{j_1}(j_2-1)!}\sum_{l=0}^{j_2-1}\begin{bmatrix} j_2-1 \\ l \end{bmatrix}\sum_{k+k_{j_0+1}+\ldots+k_{j_0+j_1}=l}\binom{l}{k, k_{j_0+1}, \ldots, k_{j_0+j_1}}\left(\sum_{i=1}^{j_0}\beta_i\right)^k\Pi_X^d,$$

where Π_X^d is defined as:

$$\Pi_X^d = 4^{-\sum_{i=j_0+1}^{j_0+j_1}\beta_i} \prod_{i=j_0+1}^{j_0+j_1} \sum_{e_i=1}^{\beta_i-1} (\beta_i - e_i)^{k_i}(4^{e_i}-1).$$

We now study the different sums on e_i according to the value of k_i. We drop the subscripts for clarity.

If $k = 0$, then the sum is simply

$$\sum_{e=1}^{\beta-1}(4^e-1) = \sum_{e=0}^{\beta-1}(4^e-1) = \frac{4^\beta - 1 - 3\beta}{3}.$$

When $k \geq 1$, we do the change of summation variable $e = \beta - e$, so that the sum becomes

$$\begin{aligned}\sum_{e=1}^{\beta-1}(\beta-e)^k(4^e-1) &= 4^\beta \sum_{e=1}^{\beta-1}(\beta-e)^k(1/4)^{\beta-e} - \sum_{e=1}^{\beta-1}(\beta-e)^k \\ &= 4^\beta \sum_{e=1}^{\beta-1} e^k 4^{-e} - \sum_{e=1}^{\beta-1} e^k.\end{aligned}$$

The second part of this difference is related to the sum of the n first kth powers. Here we sum up to $\beta - 1$ so the formula is slightly different:

$$\sum_{e=0}^{\beta-1} e^k = \frac{1}{k+1}\sum_{i=0}^{k}(-1)^{1_{i=1}}\binom{k+1}{i}B_i\beta^{k+1-i}.$$

For the first part, the sum $\sum_{i=1}^n i^k z^i$ is a multivariate polynomial in n, z and z^n of degree exactly k in n and 1 in z^n. More precisely the series $\sum_{i=0}^\infty i^k z^i$ is related to the Eulerian numbers $\left\langle {k \atop i} \right\rangle$ [6, Section 6.2] defined by:

$$\begin{aligned}\left\langle {0 \atop i} \right\rangle &= 1_{i=0}, \\ \left\langle {k \atop i} \right\rangle &= (i+1)\left\langle {k-1 \atop i} \right\rangle + (k-i)\left\langle {k-1 \atop i-1} \right\rangle \text{ for } k > 0,\end{aligned}$$

and expressed in closed form as [6, Formula 6.38]:

$$\left\langle {k \atop i} \right\rangle = \sum_{j=0}^{i}(-1)^j\binom{k+1}{j}(i+1-j)^k.$$

The series is then given by the following classical formula for $k \geq 1$ and $|z| < 1$:

$$\sum_{i=1}^\infty i^k z^i = \frac{\sum_{j=0}^k \left\langle {k \atop j} \right\rangle z^{j+1}}{(1-z)^{k+1}}.$$

The formula for the truncated sum is slightly more involved as stated in the next lemma.

Lemma 2.11. *For $k \geq 1$ and $|z| \neq 1$:*

$$\sum_{i=1}^{n} i^k z^i = \frac{\sum_{j=0}^{k} A_0(k,j) z^{j+1}}{(1-z)^{k+1}} - \frac{\left(\sum_{i=0}^{k} \binom{k}{i} \left(\sum_{j=0}^{k} A_i(k,j) z^{j+1}\right) n^i\right) z^n}{(1-z)^{k+1}},$$

where $A_i(k,j)$ is defined by the same recursion relation as $\left\langle {k \atop j} \right\rangle$ and the initial conditions:

$$A_i(i,j) = A_i(i+1,j) = (-1)^j \binom{i}{j}.$$

In particular, $A_0(k,j) = \left\langle {k \atop j} \right\rangle$ and we have the simple recursion formula for $i \geq 1$:

$$A_i(k,j) = A_{i-1}(k-1,j) - A_{i-1}(k-1,j-1).$$

We are interested in the case where $z = 1/4$, $n = \beta - 1$ and $1 \leq k \leq j_2 - 1$, which is written as (beware that we are summing up to $\beta - 1$ and not β, so the expression is slightly different from the one above):

$$\sum_{e=1}^{\beta-1} e^k 4^{-e} = \frac{\sum_{j=0}^{k} A_0(k,j) 4^{-j-1}}{(3/4)^{k+1}} - \frac{\left(\sum_{i=0}^{k-1} \binom{k}{i} \left(\sum_{j=0}^{k} A_i(k,j) 4^{-j-1}\right) \beta^i\right) 4^{-\beta}}{(3/4)^{k+1}} - \frac{\left(\sum_{j=0}^{k} A_k(k,j) 4^{-j}\right) \beta^k 4^{-\beta}}{(3/4)^{k+1}}.$$

Moreover we have the identity:

Lemma 2.12. *For $0 \leq i \leq k$*

$$3 \sum_{j=0}^{k} A_i(k,j) 4^{-j} = 4 \sum_{j=0}^{k+1} A_{i+1}(k+1,j) 4^{-j}.$$

Proof Indeed,

$$\begin{aligned}
4 \sum_{j=0}^{k+1} A_{i+1}(k+1,j) 4^{-j} &= 4 \sum_{j=0}^{k+1} (A_i(k,j) - A_i(k,j-1)) 4^{-j} \\
&= 4 \sum_{j=0}^{k} A_i(k,j) 4^{-j} - 4 \sum_{j=1}^{k+1} A_i(k,j-1) 4^{-j} \\
&= 4 \sum_{j=0}^{k} A_i(k,j) 4^{-j} - 4 \sum_{j=0}^{k} A_i(k,j) 4^{-j-1} \\
&= 3 \sum_{j=0}^{k} A_i(k,j) 4^{-j}.
\end{aligned}$$

□

Whence the definition:

Definition 2.13. *For $i \geq 0$, let us denote by A_i the quantity:*

$$A_i = \frac{\sum_{j=0}^{i} A_0(i,j)4^{-j-1}}{(3/4)^{i+1}} = \frac{\sum_{j=0}^{i} \left\langle {i \atop j} \right\rangle 4^{-j-1}}{(3/4)^{i+1}}.$$

The few first values for A_i are given in Table 1.

Table 1: A_i for $0 \leq i \leq 7$

$i =$	0	1	2	3	4	5	6	7
$A_i =$	1/3	4/9	20/27	44/27	380/81	4108/243	17780/243	269348/729

Then the following corollary of Lemmas 2.11 and 2.12 give a simple expression of the sum.

Corollary 2.14.

$$\sum_{e=1}^{\beta-1} e^k 4^{-e} = A_k - \left(\sum_{i=0}^{k-1} \binom{k}{i} A_{k-i} \beta^i \right) 4^{-\beta} - 4A_0 \beta^k 4^{-\beta}.$$

So for $k \geq 1$, the sum becomes

$$\begin{aligned}
\sum_{e=1}^{\beta-1} (\beta - e)^k (4^e - 1) &= A_k 4^\beta - \sum_{i=0}^{k-1} \binom{k}{i} A_{k-i} \beta^i - 4A_0\beta^k - \frac{1}{k+1} \sum_{i=0}^{k} (-1)^{1_{i=1}} \binom{k+1}{i} B_i \beta^{k+1-i} \\
&= A_k 4^\beta - \sum_{i=1}^{k} \binom{k}{i} A_k \beta^{k-i} - 4A_0\beta^k - \frac{1}{k+1}\beta^{k+1} + \frac{1}{2}\beta^k - \sum_{i=2}^{k} \binom{k+1}{i} B_i \beta^{k+1-i} \\
&= A_k(4^\beta - 1) - \frac{1}{k+1}\beta^{k+1} - \frac{5}{6}\beta^k - \sum_{i=1}^{k-1} \binom{k}{i} \left(A_i + \frac{B_{i+1}}{i+1} \right) \beta^{k-i}.
\end{aligned}$$

According to the above discussion about the different sums on e_i, Π_X^d can be expressed as:

$$\begin{aligned}
\Pi_X^d &= 4^{-\sum_{i=j_0+1}^{j_0+j_1} \beta_i} \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j = 0\}} \frac{4^{\beta_j} - 1 - 3\beta_j}{3} \\
&\quad \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j \neq 0\}} \left(A_{k_j}(4^{\beta_j} - 1) - \frac{1}{k_j+1}\beta_j^{k_j+1} - \frac{5}{6}\beta_j^{k_j} - \sum_{i=1}^{k_j-1} \binom{k_j}{i} \left(A_i + \frac{B_{i+1}}{i+1} \right) \beta^{k_j-i} \right) \\
&= \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j = 0\}} \frac{1 - 4^{-\beta_j} - 3\beta_j 4^{-\beta_j}}{3} \\
&\quad \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j \neq 0\}} \left(A_{k_j}(1 - 4^{-\beta_j}) - \left(\frac{1}{k_j+1}\beta_j^{k_j+1} + \frac{5}{6}\beta_j^{k_j} + \sum_{i=1}^{k_j-1} \binom{k_j}{i} \left(A_i + \frac{B_{i+1}}{i+1} \right) \beta^{k_j-i} \right) 4^{-\beta_j} \right),
\end{aligned}$$

Hence Π_X^d, Σ_X^d and T_X^d are all as stated in the proposition. The values of the degrees of the multivariate polynomials follow from the above expressions.

2.4 A Polynomial Expression

We can now prove a first step toward Proposition 2.1. We show that S_X^d is a product of exponentials in basis 2 and 4 (but not only 4 !) by multivariate polynomials.

Proposition 2.15. *For $j_2 > 0$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$,*

$$S_X^d = \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^d \right),$$

where

$$\begin{aligned}\Xi_X^d &= \sum_{i=0}^{j_2-1} 2^{-i} \Sigma_X^{d-j_2+1+i} \\ &= \frac{4^{-\sum_{i=1}^{j_0}\beta_i}}{3^{j_1}} \sum_{l=0}^{j_2-1} \left(\sum_{i=l}^{j_2-1} \frac{2^{-i}}{i!} \begin{bmatrix} i \\ l \end{bmatrix} \right) \sum_{k+k_{j_0+1}+\dots+k_{j_0+j_1}=l} \binom{l}{k, k_{j_0+1}, \dots, k_{j_0+j_1}} \left(\sum_{i=1}^{j_0} \beta_i \right)^k \Pi_X^d.\end{aligned}$$

Ξ_X^d is a sum for $I \subset \{j_0+1,\dots,j_0+j_1\}$ of terms of the form $4^{-\sum_{i=1}^{j_0}\beta_i - \sum_{i\in I}\beta_i}$ multiplied by a multivariate polynomial of degree in β_i exactly j_2 if $i \in I$, $j_2 - 1$ if $1 \le i \le j_0$, 0 otherwise, and of total degree $j_2 + |I| - 1$.

Proof The proof goes by induction on $j_2 \ge 1$.

For $j_2 = 1$, this is Proposition 2.8.

Suppose now that $j_2 > 1$. From Proposition 2.8,

$$S_X^d = 2\frac{1-4^{-\beta_d}}{3} S_X^{d-1} - 2T_X^d;$$

by induction hypothesis on j_2

$$\begin{aligned}S_X^d &= 2\frac{1-4^{-\beta_d}}{3} \frac{2^{j_2-1}}{3^{j_2-1}} \prod_{i=j_0+j_1+1}^{d-1} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d-1} \right) - 2T_X^d \\ &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d-1} \right) - 2T_X^d;\end{aligned}$$

using Proposition 2.9, we have

$$T_X^d = \frac{1}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \Sigma_X^d,$$

so that

$$\begin{aligned}S_X^d &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d-1} - 2^{-j_2+1}\Sigma_X^d \right) \\ &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d} \right),\end{aligned}$$

whence the proposition. □

In fact as soon as we know that S_X^d is a sum of exponentials multiplied by multivariate polynomials, we know which β_is can appear in the multivariate polynomials. Indeed, as a fraction of f_d we know that S_X^d is finite and even bounded between 0 and 1 for every tuple of β_is, so that S_X^d would explode as β_i goes to infinity whereas the other ones are fixed if this β_i appeared in a multivariate polynomial, but not in the exponential.

We can now prove the final step toward Proposition 2.1. We claim that for $I \subset \{1, \dots, d\}$, S_I^d that we define as

$$S_I^d = \sum_{\{X | X_i = 2 \text{ if } i \in I, X_i \neq 2 \text{ if } i \notin I\}} S_X$$

already has an appropriate form, whence Proposition 2.1 because

$$f_d(\beta_1, \dots, \beta_d) = \sum_{I \subset \{1,\dots,d\}} S_I^d.$$

For $I, J \subset \{1, \dots, d\}$ such that $I \cap J = \emptyset$, we define $X(I, J)$ as the only vector in $\{0, 1, 2\}^d$ such that

$$X_i = \begin{cases} 2 & \text{if } i \in I, \\ 1 & \text{if } i \in J, \\ 0 & \text{otherwise.} \end{cases}$$

We denote $S^d_{X(I,J)}$ simply by $S^d_{I,J}$ so that

$$S_I^d = \sum_{J \subset I^c} S_{I,J}^d.$$

We define in the same way $T^d_{I,J}$ and T^d_I and so on when $I \neq \emptyset$.

Proposition 2.16. *S_I^d is a symmetric function in the β_is such that $i \notin I$, as well as in the β_is such that $i \in I$.*

For $I = \emptyset$, we have:

$$S_\emptyset^d = \frac{1}{3^d} \sum_{J \subset \{1,\dots,d\}} 2^{|J|} 4^{-\sum_{j \in J} \beta_j},$$

and for $\{d\} \subset I = \{j_0 + j_1 + 1, \dots, d\}$,

$$S_I^d = \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1 - 4^{-\beta_i}) \left(S_\emptyset^{d-j_2} - \Xi_I^d \right).$$

For $\{d\} \subset I = \{j_0 + j_1 + 1, \dots, d\}$, Ξ_I^d is a sum for $J \subset I^c$ of terms of the form $4^{-\sum_{j \in J} \beta_j}$ multiplied by a multivariate polynomial of degree in β_j exactly $|I|$ if $j \in J$, 0 otherwise, and of total degree $\min(d - 1, |I| \cdot |J|)$.

Proof This assertion does not depend on the exact value of I, but only of $|I|$, even if the value of S_I^d does: one has to permute the β_is to deduce one from another. Hence we can assume that $I = \{j_0 + j_1 + 1, \dots, d\}$. The symmetry of S_I^d in each subset of variables follows from its definition. The proof goes by induction on $j_2 = |I|$.

Suppose first that $j_2 = 0$, i.e. $I = \emptyset$. We go by induction on d. For $d = 1$:

$$S_\emptyset^1 = S_{(0)}^1 + S_{(1)}^1 = f_1(\beta_1) = \frac{2}{3} 4^{-\beta_1} + \frac{1}{3}.$$

Suppose now that $d > 1$:

$$\begin{aligned}
S^d_\emptyset &= \sum_{J\subset\{1,\dots,d\}} S^d_{\emptyset,J} = \sum_{J\subset\{1,\dots,d-1\}} S^d_{\emptyset,J} + \sum_{\{d\}\subset J\subset\{1,\dots,d\}} S^d_{\emptyset,J} \\
&= 2^{-\beta_d} S^{d-1}_\emptyset + 2^{-\beta_d}\frac{2^{\beta_d} + 2\cdot 2^{-\beta_d} - 3}{3} S^{d-1}_\emptyset \\
&= \frac{2\cdot 4^{-\beta_d}+1}{3}\frac{1}{3^{d-1}} \sum_{J\subset\{1,\dots,d-1\}} 2^{|J|} 4^{-\sum_{j\in J}\beta_j} \\
&= \frac{1}{3^d} \sum_{J\subset\{1,\dots,d\}} 2^{|J|} 4^{-\sum_{j\in J}\beta_j}.
\end{aligned}$$

using the induction hypothesis on d which proves the proposition for $I = \emptyset$.

Suppose now that $I = \{j_0 + j_1 + 1, \dots, d\}$ is not empty. It implies that $d > 1$.

$$\begin{aligned}
S^d_I &= \sum_{J\subset\{1,\dots,j_0+j_1\}} S^d_{I,J} \\
&= \sum_{J\subset\{1,\dots,j_0+j_1\}} \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S^{d-j_2}_{I,J} - \Xi^d_{I,J} \right) \\
&= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(\sum_{J\subset\{1,\dots,j_0+j_1\}} S^{d-j_2}_{I,J} - \sum_{J\subset\{1,\dots,j_0+j_1\}} \Xi^d_{I,J} \right) \\
&= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S^{d-j_2}_\emptyset - \Xi^d_I \right).
\end{aligned}$$

□

Proposition 2.1 is a simple corollary to the last proposition and hence is finally proven.

2.5 The Coefficients $a^{d,n}_{(i_1,\dots,i_n)}$

We can now properly define the coefficients appearing in the multivariate polynomials.

Definition 2.17. *We denote by $a^{d,n}_{(i_1,\dots,i_n)}$ the coefficient of $P^n_d(x_1,\dots,x_n)$ of multi-degree $(i_1,\dots,i_n)$ normalized by 3^d.*

It should be remembered that d is the index of the function f_d, n represents the number of β_is appearing in the exponential in front of the polynomial and the i_j the degree (potentially 0) in each of these β_is of a monomial appearing in P^n_d. This does not depend on the order of the i_j because P^n_d is symmetric, so we can suppose that $(i_1 > \ldots > i_n)$. Moreover $a^{d,n}_{(i_1,\dots,i_n)} = 0$ as soon as $\sum_{j=1}^n i_j \geq d-1$.

Lemma 2.18. *For $d \geq 1$:*

$$f_{d+1}(\beta_1,\dots,\beta_d,0) = f_d(\beta_1,\dots,\beta_d).$$

Proof This is obvious from the expression of $f_d(\beta_1,\dots,\beta_d)$ as a sum. □

Hence we obtain a simple recursion relation on the coefficients of P^n_d.

Corollary 2.19. *For $d \geq 2$ and $0 \leq n < d$:*

$$a^{d,n+1}_{(i_1,\ldots,i_n,0)} + a^{d,n}_{(i_1,\ldots,i_n)} = 3a^{d-1,n}_{(i_1,\ldots,i_n)}.$$

We now give closed-form expressions for the coefficients $a^{d,n}_{(i_1,\ldots,i_n)}$.
Here is a simple proposition proving an experimental observation.

Proposition 2.20. $a^{d,d}_{(1,\ldots,1,0)} = (-1)^{d+1}2$ *and* $a^{d,d-1}_{(1,\ldots,1)} = (-1)^d 2$.

Proof From Propositions 2.16 and 2.15, the monomial of multi-degree $(1,\ldots,1,0)$ in P_d^{d-1} and P_d^d comes from $S^d_{\{d\}}$, within it from $S^d_{(1,\ldots,1,2)}$. Moreover

$$S^d_{(1,\ldots,1,2)} = \frac{2}{3}(1-4^{-\beta_d})\left(S^{d-1}_{(1,\ldots,1)} - \Xi^d_{(1,\ldots,1,2)}\right),$$

so it is clear that $a^{d,d}_{(1,\ldots,1,0)} = -a^{d,d-1}_{(1,\ldots,1)}$. The coefficient $a^{d,d-1}_{(1,\ldots,1,0)}$ must come from $\Xi^d_{(1,\ldots,1,2)}$:

$$\Xi^d_{(1,\ldots,1,2)} = \frac{1}{3^{d-1}}\Pi^d_{(1,\ldots,1,2)} = \frac{1}{3^{d-1}}\prod_{i=0}^{d-1}\frac{1-(1+3\beta_i)4^{-\beta_i}}{3},$$

and finally

$$a^{d,d-1}_{(1,\ldots,1,0)} = -3^d\frac{2}{3}\frac{1}{3^{d-1}}(-1)^{d-1} = (-1)^d 2.$$

□

More generally, we have the following expression for a monomial of total degree $d-1$.

Proposition 2.21. *Suppose that $i_1 + \ldots + i_n = d-1$. Then:*

$$a^{d,n}_{(i_1,\ldots,i_n)} = 2\frac{(-1)^{n+1}}{i_1!\ldots i_n!}.$$

Proof We can suppose that $i_1 > \ldots > i_{j_1} \neq 0 > i_{j_1+1} = 0 > \ldots > i_n$. These notations are coherent because the different constraints on the degrees show that such a monomial can only appear in S^d_X when $j_1 = |\{i_j | i_j \neq 0\}|$ and $j_2 = d - j_1$, so that this coefficient only comes from

$$S^d_{(1,\ldots,1,2,\ldots,2)} = \frac{2^{j_2}}{3^{j_2}}\prod_{i=j_1+1}^{d}(1-4^{-\beta_i})\left(S^{d-j_2}_{(1,\ldots,1)} - \Xi^d_{(1,\ldots,1,2,\ldots,2)}\right).$$

Moreover within $\Xi^d_{(1,\ldots,1,2,\ldots,2)}$ it can only appear in $\Sigma^{d-i}_{(1,\ldots,1,2,\ldots,2)}$ when $i = 0$. Looking at the expression of Π^d_X, we have the following expression

$$\begin{aligned}
a^{d,n}_{(i_1,\ldots,i_n)} &= (-1)^{n-j_1}(-2)\frac{(-1)^{j_1}}{(j_2-1)!}\begin{bmatrix} j_2-1 \\ d-1-j_1 \end{bmatrix}\binom{d-1-j_1}{i_1-1,\ldots,i_{j_1}-1}\prod_{j=1}^{j_1}\frac{1}{(i_j-1)+1} \\
&= 2\frac{(-1)^{n+1}}{(j_2-1)!}\begin{bmatrix} j_2-1 \\ j_2-1 \end{bmatrix}\binom{j_2-1}{i_1-1,\ldots,i_{j_1}-1}\prod_{j=1}^{j_1}\frac{1}{(i_j-1)+1} \\
&= 2\frac{(-1)^{n+1}}{i_1!\ldots i_{j_1}!} = 2\frac{(-1)^{n+1}}{i_1!\ldots i_n!}.
\end{aligned}$$

□

As a corollary, we get the dependence relation:

Corollary 2.22. *For $0 \leq n \leq l \leq d-1$, and $\sum_{j=1}^{n} i_j = l$,*

$$\sum_{j=0}^{d-l} \binom{d-l}{j} a^{d,n+j}_{i_1,\ldots,i_n,0,\ldots,0} = 0.$$

Proof The proof goes by induction on $d-1-l$. For $l = d-1$, this is the previous proposition. For $l < d-1$, one uses the induction hypothesis and Corollary 2.19. □

Finally here is the general expression for $a^{d,n}_{(i_1,\ldots,i_n)}$.

Proposition 2.2. *Suppose that $i_1 > \ldots > i_m \neq 0 > i_{m+1} = 0 > \ldots > i_n$ and $m > 0$. Let us denote by l the sum $l = i_1 + \ldots + i_n > 0$ (i.e. the total degree of the monomial). Then*

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} b^{d,n}_{l,m},$$

with

$$b^{d,n}_{l,m} = \sum_{\mathfrak{i}=0}^{n-m} \binom{n-m}{\mathfrak{i}} \sum_{\mathfrak{j}=0}^{d-n} \binom{d-n}{\mathfrak{j}} \sum_{k_j \geq 0, j \in I \cup J, 1 \leq j \leq m} \frac{(l+S-m)!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ l+S-m \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j} - 3_{k_j=0}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j-1}}{|k_j-1|!}.$$

Within $b^{d,n}_{l,m}$, the following notations are used:

- $I = \{m+1, \ldots, m+\mathfrak{i}\}$;
- $J = \{n+1, \ldots, n+\mathfrak{j}\}$;
- $S = \sum_{j \in I \cup J, 1 \leq j \leq m} k_j$;
- $h = d - m - \mathfrak{j} - \mathfrak{i}$;

and

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & \text{if } j > 0, \\ -\frac{13}{6} & \text{if } j = 0, \\ 1 & \text{if } j = -1. \end{cases}$$

Proof If $X_j = 2$, then the degree of β_j in S^d_X is zero. If $X_j = 0$, then $4^{-\beta_j}$ can be factored out of S^d_X and β_j will appear in every exponential. Therefore we can consider only Xs which verify the following constraints to compute $a^{d,n}_{(i_1,\ldots,i_n)}$:

$$X_j = \begin{cases} 0, 1 & \text{if } 1 \leq j \leq m, \\ 0, 1, 2 & \text{if } m+1 \leq j \leq n, \\ 1, 2 & \text{if } n+1 \leq j \leq d. \end{cases}$$

From Proposition 2.15,

$$S^d_X = \frac{2^{j_2}}{3^{j_2}} \prod_{\{j | X_j = 2\}} (1 - 4^{-\beta_j}) \left(S^{d-j_2}_X - \Xi^d_X \right),$$

and the monomials of non-zero degree only comes from Ξ_X^d.

Moreover Ξ_X^d can be written as

$$\Xi_X^d = \frac{1}{3^{j_1}} \sum_{k_j \geq 0, \{j|X_j \neq 2\}} \left(\sum_{k=0}^{j_2-1} \frac{2^{-k}}{k!} \begin{bmatrix} k \\ \sum_{\{j|X_j \neq 2\}} k_j \end{bmatrix} \right) \frac{\left(\sum_{\{j|X_j \neq 2\}} k_j\right)!}{\prod_{\{j|X_j \neq 2\}} k_j!} \left(\prod_{\{j|X_j=0\}} \beta_j^{k_j} 4^{-\beta_j} \right) \Pi_X^d.$$

So to get a multinomial of multi-degree $(i_1, \ldots, i_n)$, different choices can be made for the k_js.

- If $X_j = 0$, then we must take $k_j = i_j$. This happens for $1 \leq j \leq n$.
- If $X_j = 1$, then we can take any $k_j \geq \min(i_j - 1, 0)$ and take into account the correct coefficient in Π_X^d. This happens for $1 \leq j \leq d$
- If $X_j = 2$, then there is no choice to make. This happens for $m + 1 \leq j \leq d$.

In the following sum, we gathered the contributions of all Xs. We denote by I the set of indices $m + 1 \leq j \leq n$ such that $X_j = 0, 1$ (the other ones are such that $X_j = 2$) and by J the set of indices $n + 1 \leq j \leq d$ such that $X_j = 1$ (the other ones are such that $X_j = 2$).

The summation variables k_j where j is in $I \cup J$ or $[1, m]$ are to be understood as the degree we choose in the above expression of Ξ_X^d. Following the above discussion on the choice of the k_js:

- If $j \in J$, we can choose any positive degree k_j and extract the constant coefficient A_{k_j}.
- If $j \in I$, we can choose any positive degree k_j and we extract the constant coefficient A_{k_j} as above if $k_j > 0$, and $A_0 - 3$ if $k_j = 0$ (the -3 comes from the choice $X_j = 0$ which gives $1 = 3 \cdot 1/3$).
- Finally if $1 \leq j \leq m$, we have to choose $k_j \geq i_j - 1$, and the corresponding coefficient is $\frac{1}{k_j+1} = \frac{1}{i_j}$ if $k_j = i_j - 1$, $5/6 - 3 = -13/6$ if $k_j = i_j$ (as above the -3 comes from the choice $X_j = 0$) and $\binom{k_j}{i_j} \left(A_{k_j - i_j} + \frac{B_{k_j - i_j + 1}}{k_j - i_j + 1} \right)$ if $k_j > i_j$. We denote that coefficient by D_{k_j, i_j}.

We denote S and h the quantities $S = \sum_{j \in I \cup J, 1 \leq j \leq m} k_j$ and $h = d - m - |J| - |I|$. Then $a^{d,n}_{(i_1,\ldots,i_n)}$ can be expressed as:

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \sum_{\substack{I \subset \{m+1,\ldots,n\} \\ J \subset \{n+1,\ldots,d\}}} \sum_{\substack{k_j \geq 0, j \in I \cup J \\ k_j \geq i_j - 1, 1 \leq j \leq m}} \frac{S!}{\prod_{j \in I \cup J} k_j! \prod_{j=1}^m k_j!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) \prod_{j \in J} A_{k_j} \prod_{j \in I} \left(A_{k_j} - 3_{k_j = 0} \right) \prod_{j=1}^m D_{k_j, i_j}$$

Extracting the binomial coefficient of D_{k_j, i_j}, we can factor out the multinomial coefficient $\binom{l}{i_1, \ldots, i_n}$ (remember that l was defined as $l = \sum_{j=1}^n i_j$):

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} \sum_{\substack{I \subset \{m+1,\ldots,n\} \\ J \subset \{n+1,\ldots,d\}}} \sum_{\substack{k_j \geq 0, j \in I \cup J \\ k_j \geq i_j - 1, 1 \leq j \leq m}} \frac{S!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j} - 3_{k_j = 0}}{k_j!} \prod_{j=1}^m \frac{C_{k_j - i_j}}{|k_j - i_j|!},$$

where

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & \text{if } j > 0 \\ -\frac{13}{6} & \text{if } j = 0 \\ 1 & \text{if } j = -1 \end{cases}.$$

The exact value of I and J is not important, only their cardinalities, so defining $I = \{m+1, \ldots, m+\mathfrak{i}\}$ and $J = \{n+1, \ldots, n+\mathfrak{j}\}$,

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1}\binom{l}{i_1,\ldots,i_n}\sum_{\mathfrak{i}=0}^{n-m}\binom{n-m}{\mathfrak{i}}\sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}}\sum_{\substack{k_j\geq 0, j\in I\cup J\\ k_j\geq i_j-1, 1\leq j\leq m}}\frac{S!}{l!}$$
$$\left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix}h-k\\ S\end{bmatrix}\right)\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j\in I}\frac{A_{k_j}-3_{k_j=0}}{k_j!}\prod_{j=1}^{m}\frac{C_{k_j-i_j}}{|k_j-i_j|!}.$$

We finally make the change of summation variables $k_j = k_j - i_j + 1$:

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1}\binom{l}{i_1,\ldots,i_n}\sum_{\mathfrak{i}=0}^{n-m}\binom{n-m}{\mathfrak{i}}\sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}}\sum_{k_j\geq 0, j\in I\cup J, 1\leq j\leq m}\frac{(l+S-m)!}{l!}$$
$$\left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix}h-k\\ l+S-m\end{bmatrix}\right)\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j\in I}\frac{A_{k_j}-3_{k_j=0}}{k_j!}\prod_{j=1}^{m}\frac{C_{k_j-1}}{|k_j-1|!}$$
$$= (-1)^{n+1}\binom{l}{i_1,\ldots,i_n}b^{d,n}_{l,m}.$$

□

2.6 An Additional Relation

In this subsection we prove the following experimental fact.

Proposition 2.3. *For $0 < j \leq i$,*

$$a^{d,n}_{(i,j,\ldots)} = \frac{i+1}{j}a^{d,n}_{(i+1,j-1,\ldots)};$$

i.e. the value of $b^{d,n}_{l,m}$ does not depend on m.

Proof From Proposition 2.2,

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1}\binom{l}{i_1,\ldots,i_n}b^{d,n}_{l,m},$$

where $b^{d,n}_{l,m}$ only depends on d, n, l and m. Therefore if $j > 1$, this value does not vary and the theorem is a simple corollary of Proposition 2.2.

If there is some degree equal to zero in $(i, j, \ldots)$, i.e. if $n > m$, then we can use the result of Corollary 2.19:

$$a^{d,n}_{(i,j,\ldots,0)} + a^{d,n-1}_{(i,j,\ldots)} = 3a^{d-1,n-1}_{(i,j,\ldots)};$$

hence we can restrict ourselves to the study of tuples where $n = m$.

Finally the only tuples we must treat are the ones such that $i > j = 1$ and $n = m$. We write the degree $i \neq 0$ in first position even if it not the greatest one. Then

$$a^{d,n}_{(i,\dots,1)} = (-1)^{n+1}\binom{l}{i,\dots,1} b^{d,n}_{l,n},$$
$$a^{d,n}_{(i+1,\dots,0)} = (-1)^{n+1}\binom{l}{i+1,\dots,0} b^{d,n}_{l,n-1},$$

so it suffices to show that $b^{d,n}_{l,n} = b^{d,n}_{l,n-1}$.

We use the same notations as in Proposition 2.2 except that S and h denote the quantities $S = l + \sum_{j\in I\cup J, 1\leq j\leq n-1} k_j - n$ and $h = d - n - \mathfrak{j}$. For $b^{d,n}_{l,n}$, I must be empty:

$$\begin{aligned} b^{d,n}_{l,n} &= \sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in J, 1\leq j\leq n} \frac{(S+k_n)!}{l!} \\ &\qquad \left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix} h-k \\ S+k_n\end{bmatrix}\right)\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j=1}^{n}\frac{C_{k_j-1}}{|k_j-1|!} \\ &= \sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in J, 1\leq j\leq n-1} \frac{1}{l!}\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j=1}^{n-1}\frac{C_{k_j-1}}{|k_j-1|!} \\ &\qquad \sum_{k_n\geq 0}(S+k_n)!\left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix} h-k \\ S+k_n\end{bmatrix}\right)\frac{C_{k_n-1}}{|k_n-1|!}; \end{aligned}$$

whereas for $b^{d,n}_{l,n-1}$, I can contain n:

$$\begin{aligned} b^{d,n}_{l,n-1} &= \sum_{\mathfrak{i}=0}^{1}\binom{1}{\mathfrak{i}}\sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in I\cup J, 1\leq j\leq n-1} \frac{(S+1)!}{l!} \\ &\qquad \left(\sum_{k\geq 1}\frac{2^k}{(h+1-k-\mathfrak{i})!}\begin{bmatrix} h+1-k-\mathfrak{i} \\ S+1\end{bmatrix}\right)\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j\in I}\frac{A_{k_j}-3_{k_j=0}}{k_j!}\prod_{j=1}^{n-1}\frac{C_{k_j-1}}{|k_j-1|!} \\ &= \sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in J, 1\leq j\leq n-1} \frac{1}{l!}\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j=1}^{n-1}\frac{C_{k_j-1}}{|k_j-1|!} \\ &\qquad \left[(S+1)!\left(\sum_{k\geq 1}\frac{2^k}{(h+1-k)!}\begin{bmatrix} h+1-k \\ S+1\end{bmatrix}\right)\right. \\ &\qquad\quad \left. + \sum_{k_n\geq 0}(S+k_n+1)!\left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix} h-k \\ S+k_n+1\end{bmatrix}\right)\frac{A_{k_n}-3_{k_n=0}}{|k_n-1|!}\right]. \end{aligned}$$

The sums on $\mathfrak{j}$ and k_j for $j \in J$ and $1 \leq j \leq n-1$ are identical, so it is sufficient to show the

equality of the remaining terms, or that Δ defined as

$$\Delta = \sum_{k_n \geq 0} \frac{(S+k_n)!}{|k_n-1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) C_{k_n-1} - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$- \sum_{k_n \geq 0} \frac{(S+k_n+1)!}{|k_n-1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n+1 \end{bmatrix} \right) (A_{k_n} - 3_{k_n=0})$$

is zero. We split out the two first terms of the first sum on k_n:

$$S! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) - \frac{13}{6}(S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right),$$

and the first one of the second sum on k_n:

$$(S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right) \left(\frac{1}{3} - 3 \right),$$

so that Δ becomes:

$$\Delta = \sum_{k_n \geq 2} \frac{(S+k_n)!}{|k_n-1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) \left(A_{k_n-1} + \frac{B_{k_n}}{k_n} \right)$$
$$+ S! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) + \frac{1}{2}(S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right)$$
$$- (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right) - \sum_{k_n \geq 1} \frac{(S+k_n+1)!}{|k_n-1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n+1 \end{bmatrix} \right) A_{k_n}.$$

Making the change of summation variable $k_n = k_n + 1$ in the second sum on k_n, the terms in A_{k_n} cancel out between the two sums on k_n and we get:

$$\Delta = \sum_{k_n \geq 2} \frac{(S+k_n)!}{k_n!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) B_{k_n} + B_0 S! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right)$$
$$+ B_1 (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right) - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$= \sum_{k_n \geq 0} \frac{(S+k_n)!}{k_n!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) B_{k_n} - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$= S! \sum_{k \geq 1} \frac{2^k}{(h-k)!} \left(\sum_{k_n \geq 0} \binom{S+k_n}{S} B_{k_n} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$= S! \sum_{k \geq 1} \frac{2^k}{(h-k)!} \left(\sum_{k_n \geq 0} \binom{S+k_n}{S} B_{k_n} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} - \frac{S+1}{h+1-k} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right).$$

The difference in parenthesis is shown to be zero using Lemma 2.23, so that $\Delta = 0$. $\square$

Lemma 2.23. *For $n \geq k \geq 0$,*

$$\sum_{l=0}^{n-k} \binom{k+l}{k} B_l \begin{bmatrix} n \\ k+l \end{bmatrix} = \frac{k+1}{n+1} \begin{bmatrix} n+1 \\ k+1 \end{bmatrix}.$$

Proof Let us fix $k \geq 0$. We first recall classical results about exponential generating functions:

$$\sum_{n\geq 0} B_n \frac{z^n}{n!} = \frac{z}{1-e^{-z}},$$
$$\sum_{n\geq 0} \begin{bmatrix} n \\ k \end{bmatrix} \frac{z^n}{n!} = \frac{(-\log(1-z))^k}{k!}.$$

We now form the exponential generating function of the coefficients of interest:

$$\begin{aligned}
\sum_{n\geq 0} \left(\sum_{l=k}^{n} \binom{l}{k} B_{l-k} \begin{bmatrix} n \\ l \end{bmatrix} \right) \frac{z^n}{n!} &= \sum_{l\geq k} \sum_{n\geq l} \binom{l}{k} B_{l-k} \begin{bmatrix} n \\ l \end{bmatrix} \frac{z^n}{n!} = \sum_{l\geq k} \binom{l}{k} B_{l-k} \sum_{n\geq l} \begin{bmatrix} n \\ l \end{bmatrix} \frac{z^n}{n!} \\
&= \sum_{l\geq k} \binom{l}{k} B_{l-k} \frac{(-\log(1-z))^l}{l!} \\
&= \frac{(-\log(1-z))^k}{k!} \sum_{l\geq k} B_{l-k} \frac{(-\log(1-z))^{l-k}}{(l-k)!} \\
&= \frac{(-\log(1-z))^k}{k!} \sum_{l\geq 0} B_l \frac{(-\log(1-z))^l}{l!} \\
&= \frac{(-\log(1-z))^k}{k!} \frac{-\log(1-z)}{1-e^{\log(1-z)}} = \frac{k+1}{z} \frac{(-\log(1-z))^{k+1}}{(k+1)!} \\
&= \frac{k+1}{z} \sum_{n\geq 0} \begin{bmatrix} n \\ k+1 \end{bmatrix} \frac{z^n}{n!} = \sum_{n\geq 0} \frac{k+1}{n+1} \begin{bmatrix} n+1 \\ k+1 \end{bmatrix} \frac{z^n}{n!},
\end{aligned}$$

whence the identity of the lemma. □

3 Asymptotic Behavior

In this section, we study the behavior of $P_{t,k}$ when a given number of β_is go to infinity. To this end, we take advantage of its probabilistic nature:

$$P_{t,k} = P\left[\sum_d \gamma' < \sum_d \delta' \right].$$

In Subsection 3.1, we study the behavior of f_d when all of the β_is and give useful closed forms for the value toward which it converges, as well as its monotony in d. In Subsection 3.2, we consider a more general setting and give relations involving the limit of f_d when a β_i is set to 1 while the other ones go to infinity.

3.1 The Limit $f_d(\infty, \ldots, \infty)$

We first consider the limit of f_d when all the β_is go to infinity. We now denote this limit by $f_d(\infty, \ldots, \infty)$. This is also the value of the constant term in the expression of f_d given in Proposition 2.1.

We remark that as all 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 (which we denote by $Geo(1/2)$), 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 $d > 0$ and proves the conjecture *asymptotically.*

Definition 3.1. *Let X_d be the random variable*

$$X_d = \sum_d Geo(1/2) - \sum_d Geo(1/2),$$

and P_d denote

$$P_d = P\left[X_d = 0\right].$$

With these notations,

$$f_d(\infty, \ldots, \infty) = \frac{1}{2}(1 - P_d),$$

and the importance of the random variable X_d becomes obvious.

It is readily seen that X_d is symmetric, i.e. $P\left[X_d = k\right] = P\left[X_d = -k\right]$ and the following lemma is easy:

Lemma 3.2.

$$P\left[\sum_d Geo(1/2) = j\right] = \binom{d-1+j}{d-1}\frac{1}{2^{j+1}}.$$

The following proposition gives an expression of $P\left[X_d = k\right]$ as a power series and a hypergeometric series:

Proposition 3.3. *For $d \geq 1$ and $k \geq 0$:*

$$\begin{aligned} P\left[X_d = k\right] &= \frac{1}{4^d}\frac{1}{2^k}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\binom{d-1+k+j}{d-1}\frac{1}{4^j} \\ &= \frac{1}{4^d}\frac{1}{2^k}\binom{d-1+k}{d-1}{}_2F_1(d, d+k; k+1; 1/4), \end{aligned}$$

so that:

$$P_d = P\left[X_d = 0\right] = \frac{1}{4^d}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}^2\frac{1}{4^j} = \frac{1}{4^d}{}_2F_1(d, d; 1; 1/4).$$

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

Proof

$$\begin{aligned} P\left[X_d = k\right] &= \sum_{j=0}^{\infty} P\left[\sum_d Geo(1/2) = j\right] P\left[\sum_d Geo(1/2) = j + k\right] \\ &= \sum_{j=0}^{\infty} P\left[\sum_d Geo(1/2) = j\right] P\left[\sum_d Geo(1/2) = j + k\right] \\ &= \frac{1}{4^d}\frac{1}{2^k}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\binom{d-1+k+j}{d-1}\frac{1}{4^j}. \end{aligned}$$

Suppose now that $k = 0$. We bound the sum of squares from below by:

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

and from above by:

$$\begin{aligned}\frac{1}{4^d}\left(1+\sum_{j=1}^{\infty}\binom{d-1+j}{d-1}\frac{2^{d-2+j}}{4^j}\right) &= \frac{1}{4^d}+\frac{2^{d-2}}{4^d}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\frac{1}{2^j}-\frac{2^{d-2}}{4^d}\\ &= \frac{1+4^{d-1}-2^{d-2}}{4^d} = \frac{1+3\cdot 2^{d-2}}{4^d}.\end{aligned}$$

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

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

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

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

□

When the number of blocks, d, goes as well to infinity, $f_d(\infty,\ldots,\infty)$ converges toward $1/2$. Indeed $\frac{1}{3^d} \le P_d \le \frac{1}{4^d}+\frac{3}{4}\frac{1}{2^d}$ converges towards 0 as d goes to infinity. As we show below, it does so decreasingly so that $f_d(\infty,\ldots,\infty)$ goes to $1/2$ increasingly.

The following expression of the distribution for $d = 1$ is easily computed:

Lemma 3.4. *For $d = 1$:*

$$P[X_1 = k] = \frac{1}{3\cdot 2^{|k|}}.$$

Proof Indeed, for $k \ge 0$:

$$\begin{aligned}P[X_1 = k] &= P[Geo(1/2) = k + Geo(1/2)]\\ &= \sum_{i=0}^{\infty}P[Geo(1/2) = i]\,P[Geo(1/2) = k+i]\\ &= \sum_{i=0}^{\infty}\frac{1}{2^{i+1}}\frac{1}{2^{k+i+1}} = \frac{1}{2^{k+2}}\sum_{i=0}^{\infty}\frac{1}{4^i}\\ &= \frac{1}{2^{k+2}}\frac{4}{3} = \frac{1}{3}\frac{1}{2^k}.\end{aligned}$$

□

Lemma 3.5. *For $d \geq 1$ and $k \neq 0$:*

$$P[X_d = k] < P[X_d = 0].$$

Proof This is a simple consequence of the Cauchy-Schwarz inequality because $P[X_d = k]$ is a scalar product of the distribution of $\sum_d Geo(1/2)$ with itself shifted by k. □

Combining Lemmas 3.4 and 3.5, we get the monotony of P_d in d:

Proposition 3.6. *For $d \geq 1$:*

$$P_d > P_{d+1}.$$

Proof

$$\begin{aligned} P_{d+1} &= P[X_{d+1} = 0] = P[X_1 + X_d = 0] \\ &= \sum_{k=-\infty}^{+\infty} P[X_1 = -k] P[X_d = k] \\ &= \sum_{k=-\infty}^{+\infty} \frac{1}{3 \cdot 2^{|k|}} P[X_d = k] \\ &< \sum_{k=-\infty}^{+\infty} \frac{1}{3 \cdot 2^{|k|}} P[X_d = 0] \\ &< P[X_d = 0] = P_d. \end{aligned}$$

□

Corollary 3.7. *$f_d(\infty, \ldots, \infty)$ goes to $\frac{1}{2}$ increasingly as d goes to infinity.*

In fact there are several other expressions for the distribution of X_d which can be obtained via hypergeometric transformations. Here is a first one of particular interest.

Proposition 3.8.

$$\begin{aligned} P[X_d = k] &= \frac{2^k}{3^{2d+2k}} \binom{d-1+k}{d-1} {}_2F_1(k+1/2, d+k; 2k+1; 8/9), \\ &= 3^{-2d} \sum_{j=k}^{\infty} \binom{d-1+j}{j} \binom{2j}{k+j} 2^j 3^{-2j}. \end{aligned}$$

Proof It follows directly from the quadratic transformation [1, Formula 15.3.27]:

$${}_2F_1(a, b; a-b+1; z) = (1+\sqrt{z})^{-2a} {}_2F_1\left(a, a-b+\frac{1}{2}; 2a-2b+1; \frac{4\sqrt{z}}{(1+\sqrt{z})^2}\right),$$

valid for $|z| < 1$. We obtain the following expression where we shift the summation index j by k:

$$\begin{aligned} P[X_d = k] &= \frac{2^k}{3^{2d+2k}} \sum_{j=0}^{\infty} \binom{d-1+k+j}{d-1} \binom{2k+2j}{j} 2^j 3^{-2j} \\ &= 3^{-2d} \sum_{j=k}^{\infty} \binom{d-1+j}{j} \binom{2j}{k+j} 2^j 3^{-2j}, \end{aligned}$$

□

Using it we deduce a stronger result about X_d.

Corollary 3.9. *For $d \geq 1$, X_d follows a unimodal distribution centered in 0, i.e. $P[X_d = k]$ is increasing for $k \leq 0$ and decreasing for $k \geq 0$.*

Proof Indeed, $P[X_d = k]$ is an even function of k and for a fixed j and $k \geq 0$ each summand of the previous expression is decreasing in k. □

And we deduce another useful expression for P_d where d appears only twice.

Corollary 3.10. *For $d \geq 1$:*

$$P_d = 3^{-2d} \sum_{j=0}^{\infty} \binom{d-1+j}{j} \binom{2j}{j} 2^j 3^{-2j}.$$

Here are other closed forms for $P[X_d = k]$ deduced using linear transformations. They are of particular interest for actual computation because they express $P[X_d = k]$ as a finite sum.

Proposition 3.11. *For $d \geq 1$ and $0 \leq k$:*

1.
$$\begin{aligned} P[X_d = k] &= \frac{4^{d-1}}{2^k 3^{2d-1}} \binom{d-1+k}{d-1} {}_2F_1(k+1-d, 1-d; k+1; 1/4) \\ &= \begin{cases} \frac{2^k}{3^{2d-1}} \sum_{j=0}^{d-1-k} \binom{d-1-k}{j} \binom{d-1+k}{j+k} 4^j & \text{if } 0 \leq k \leq d-1 \\ \frac{4^{d-1}}{2^k 3^{2d-1}} \sum_{j=0}^{d-1} (-1)^j \binom{d-1+k}{k+j} \binom{k-d+j}{k-d} 4^{-j} & \text{if } d-1 < k \end{cases}; \end{aligned}$$

2.
$$\begin{aligned} P[X_d = k] &= \frac{2^k}{3^{d+k}} \binom{d-1+k}{d-1} {}_2F_1(k+1-d, k+d; k+1; -1/3) \\ &= \begin{cases} \frac{2^k}{3^{d+k}} \sum_{j=0}^{d-1-k} \binom{d-1+k+j}{d-1} \binom{d-1-k}{j} 3^{-j} & \text{if } 0 \leq k \leq d-1 \\ \frac{2^k}{3^{d+k}} \sum_{j=0}^{\infty} (-1)^j \binom{d-1+k+j}{d-1} \binom{k-d+j}{k-d} 3^{-j} & \text{if } d-1 < k \end{cases}; \end{aligned}$$

3.
$$\begin{aligned} P[X_d = k] &= \frac{1}{2^k 3^d} \binom{d-1+k}{d-1} {}_2F_1(d, 1-d; k+1; -1/3) \\ &= \frac{1}{2^k 3^d} \sum_{j=0}^{d-1} \binom{d-1+j}{d-1} \binom{d-1+k}{k+j} 3^{-j}. \end{aligned}$$

Proof The first expression comes from Euler's transformation [1, Formula 15.3.3]:

$${}_2F_1(a, b; c; z) = (1-z)^{c-a-b} {}_2F_1(c-a, c-b; c; z).$$

The second one from Pfaff's transformation [1, Formula 15.3.5]:

$${}_2F_1(a, b; c; z) = (1-z)^{-b} {}_2F_1(c-a, b; c; z/(z-1)).$$

The third one from the other Pfaff's transformation [1, Formula 15.3.4]:

$$ {}_2F_1(a,b;c;z) = (1-z)^{-a}\,{}_2F_1(a,c-b;c;z/(z-1)). $$

□

We finally deduce different expressions for P_d as a finite sum.

Corollary 3.12. *For $d \geq 1$:*

$$ \begin{aligned} P_d &= \frac{1}{3^{2d-1}}\,{}_2F_1(1-d,1-d;1;4) = \frac{1}{3^{2d-1}}\sum_{j=0}^{d-1}\binom{d-1}{j}^2 4^j \\ &= \frac{1}{3^d}\,{}_2F_1(1-d,d;1;-1/3) = \frac{1}{3^d}\sum_{j=0}^{d-1}\binom{d-1+j}{d-1}\binom{d-1}{j}3^{-j}. \end{aligned} $$

It can be verified elementary that both expressions for P_d are equal writing $4 = 1+3$, using the binomial theorem and the identity:

$$ \binom{2n+k}{n+k} = \sum_{j=0}^{n}\binom{n}{j}\binom{n+k}{j+k}, $$

deduced from Chu-Vandermonde identity.

3.2 The Limit $f_d(1,\infty,\ldots,\infty)$

In the previous subsection we studied the behavior of $P_{t,k} = f_d(\beta_1,\ldots,\beta_d)$ as all the β_is go to infinity.

In fact if for some $i \in \{1,\ldots,d\}$, we set $\beta_i = 1$ and α_i still goes to infinity, then $\epsilon'_i = \gamma'_i + \beta_i - \delta'_i$ has a similar behavior to the one of γ'_i and δ'_i: its law converges towards the law of an independent geometrically distributed variable with parameter $1/2$ (denoted by $Geo(1/2)$). Then we have a probabilistic interpretation for $\lim_{\beta_j\to\infty, j>i} f_d(\overbrace{1,\ldots,1}^{i},\overbrace{\beta_{i+1},\ldots,\beta_d}^{d-i})$ which we denote by $f_d(\overbrace{1,\ldots,1}^{i},\overbrace{\infty,\ldots,\infty}^{d-i})$.

$$ \begin{aligned} f_d(\overbrace{1,\ldots,1}^{i},\overbrace{\infty,\ldots,\infty}^{d-i}) &= \lim_{\beta_j\to\infty, j>i} P\left[\sum_d \gamma' < \sum_d \delta'\right] \\ &= \lim_{\beta_j\to\infty, j>i} P\left[\sum_i \epsilon' + \sum_{d-i}\gamma' < i + \sum_{d-i}\delta'\right] \\ &= P\left[\sum_d Geo(1/2) < i + \sum_{d-i} Geo(1/2)\right] \\ &= P\left[X_{d-i} + \sum_i Geo(1/2) < i\right]. \end{aligned} $$

The few first values of such expressions computed using explicit expressions for f_d are given in Table 2.

We now give some results about these values.

Table 2: $f_d(1,\dots,1,\infty,\dots,\infty)$ for $d \geq 1$

$i=$	d	$d-1$	$\dots$				
$d=1$	1/2	1/3					
$d=2$	1/2	4/9	11/27				
$d=3$	1/2	101/216	4/9	35/81			
$d=4$	1/2	619/1296	112/243	328/729	971/2187		
$d=5$	1/2	15029/31104	10969/23328	112/243	2984/6561	8881/19683	
$d=6$	1/2	90829/186624	2777/5832	1024/2187	9104/19683	9028/19683	2993/6561

Proposition 3.13. *For $d \geq 2$:*

$$f_d(1,\infty,\dots,\infty) = \frac{3}{2} f_d(\infty,\dots,\infty) - \frac{1}{2} f_{d-1}(\infty,\dots,\infty).$$

Proof We equivalently show that:

$$f_d(\infty,\dots,\infty) = \frac{1}{3} f_{d-1}(\infty,\dots,\infty) + \frac{2}{3} f_d(1,\infty,\dots,\infty),$$

i.e. written in a probabilistic way:

$$P\left[0 < X_d\right] = \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{2}{3} P\left[X_{d-1} < 1 - Geo(1/2)\right].$$

$$\begin{aligned}
P\left[0 < X_d\right] = P\left[0 < X_{d-1} + X_1\right] &= \sum_{i=-\infty}^{+\infty} P\left[X_1 = i\right] P\left[-i < X_{d-1}\right] \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(P\left[i < X_{d-1}\right] + P\left[-i < X_{d-1}\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(P\left[i < X_{d-1}\right] + P\left[X_{d-1} < i\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(P\left[X_{d-1} \neq i\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(1 - P\left[X_{d-1} = i\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \left(1 - \sum_{i=1}^{\infty} \frac{1}{2^i} P\left[X_{d-1} = i\right]\right).
\end{aligned}$$

It is now enough to show that:

$$2P\left[X_{d-1} < 1 - Geo(1/2)\right] = 1 - \sum_{i=1}^{\infty} \frac{1}{2^i} P\left[X_{d-1} = i\right],$$

which follows from:

$$\begin{aligned}
P\left[X_{d-1} < 1 - Geo(1/2)\right] &= \sum_{i=0}^{\infty} \frac{1}{2^{i+1}} P\left[X_{d-1} < 1 - i\right] \\
&= \frac{1}{2} P\left[X_{d-1} < 1\right] + \frac{1}{4} \sum_{i=0}^{\infty} \frac{1}{2^i} P\left[X_{d-1} < -i\right] \\
&= \frac{1}{2} \left(1 - P\left[1 \leq X_{d-1}\right]\right) + \frac{1}{4} \sum_{i=0}^{\infty} \frac{1}{2^i} P\left[i < X_{d-1}\right] \\
&= \frac{1}{2} - \frac{1}{2} \sum_{i=1}^{\infty} P\left[X_{d-1} = i\right] + \frac{1}{4} \sum_{i=1}^{\infty} \left(\sum_{j=0}^{i-1} \frac{1}{2^j} \right) P\left[X_{d-1} = i\right] \\
&= \frac{1}{2} - \frac{1}{2} \sum_{i=1}^{\infty} P\left[X_{d-1} = i\right] + \frac{1}{2} \sum_{i=1}^{\infty} \left(1 - \frac{1}{2^i}\right) P\left[X_{d-1} = i\right] \\
&= \frac{1}{2} - \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^i} P\left[X_{d-1} = i\right].
\end{aligned}$$

□

Corollary 3.14. *For $d \geq 2$:*

$$f_d(1, \infty, \ldots, \infty) > f_d(\infty, \infty, \ldots, \infty);$$

Proof This is a consequence of the above proposition and of the monotony of P_d. □

References

[1] Milton Abramowitz and Irene A. Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964.

[2] Claude Carlet. Private communication, 2009.

[3] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică. On a combinatorial conjecture. *Integers*, 11(2):185–203, May 2011.

[4] 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.

[5] Jean-Pierre Flori, Hugues Randriam, Gérard Cohen, and Sihem Mesnager. On a conjecture about binary strings distribution. Cryptology ePrint Archive, Report 2010/170, 2010. `http://eprint.iacr.org/`.

[6] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[7] William Stein. *Sage: Open Source Mathematical Software (Version 4.6.2)*. The Sage Group, 2011. `http://www.sagemath.org`.

[8] Ziran Tu and Yingpu Deng. A conjecture about binary strings and its applications on constructing boolean functions with optimal algebraic immunity. *Designs, Codes and Cryptography*, pages 1–14, 2010. 10.1007/s10623-010-9413-9.

[9] `Maxima.sourceforge.net`. *Maxima, a Computer Algebra System (Version 5.23.2)*, 2011. `http://maxima.sourceforge.net`.

[10] `Pynac.sagemath.net`. *Pynac, symbolic computation with Python objects (Version 0.2.2)*, 2011. `http://pynac.sagemath.org`.

A Coefficients of f_d

In the following tables, 4^n means an exponential where the exponent is the opposite of the sum of n different β_is. The following n-tuples indicate the multi-exponent of the monomial and the corresponding coefficient. The total degree of the multivariate polynomial is exactly $d-1$, except for $n = 0$. The omitted coefficients are obtained from the previous ones by permuting the β_is. These coefficients were obtained using Sage [7], Pynac [10] and Maxima [9].

Table 3: $d = 1$, $(1/3) = (1/3^1)*$

4^ 1	4^ 0
(0,) 2	() 1

Table 4: $d = 2$, $(1/9) = (1/3^2)*$

4^ 2	4^ 1	4^ 0
(1, 0) −2	(1,) 2	
(0, 0) 20/3	(0,) −2/3	() 11/3

Table 5: $d = 3$, $(1/27) = (1/3^3)*$

4^ 3	4^ 2	4^ 1	4^ 0
(2, 0, 0) 1 (1, 1, 0) 2	(2, 0) −1 (1, 1) −2	(2,) 1	
(1, 0, 0) −11	(1, 0) 5	(1,) 1	
(0, 0, 0) 64/3	(0, 0) −4/3	(0,) −2/3	() 35/3

Table 6: $d = 4$, $(1/81) = (1/3^4)*$

4^	4	4^	3	4^	2	4^	1	4^	0
$(3,0,0,0)$	$-1/3$	$(3,0,0)$	$1/3$	$(3,0)$	$-1/3$	$(3,)$	$1/3$		
$(2,1,0,0)$	-1	$(2,1,0)$	1	$(2,1)$	-1				
$(1,1,1,0)$	-2	$(1,1,1)$	2						
$(2,0,0,0)$	$23/3$	$(2,0,0)$	$-14/3$	$(2,0)$	$5/3$	$(2,)$	$4/3$		
$(1,1,0,0)$	$46/3$	$(1,1,0)$	$-28/3$	$(1,1)$	$10/3$				
$(1,0,0,0)$	$-416/9$	$(1,0,0)$	$119/9$	$(1,0)$	$16/9$	$(1,)$	$11/9$		
$(0,0,0,0)$	$1808/27$	$(0,0,0)$	$-80/27$	$(0,0)$	$-28/27$	$(0,)$	$-26/27$	$()$	$971/27$

Table 7: $d = 5$, $(1/243) = (1/3^5)*$

4^	5	4^	4	4^	3	4^	2	4^	1	4^	0
$(4,0,0,0,0)$	$1/12$	$(4,0,0,0)$	$-1/12$	$(4,0,0)$	$1/12$	$(4,0)$	$-1/12$	$(4,)$	$1/12$		
$(3,1,0,0,0)$	$1/3$	$(3,1,0,0)$	$-1/3$	$(3,1,0)$	$1/3$	$(3,1)$	$-1/3$				
$(2,2,0,0,0)$	$1/2$	$(2,2,0,0)$	$-1/2$	$(2,2,0)$	$1/2$	$(2,2)$	$-1/2$				
$(2,1,1,0,0)$	1	$(2,1,1,0)$	-1	$(2,1,1)$	1						
$(1,1,1,1,0)$	2	$(1,1,1,1)$	-2								
$(3,0,0,0,0)$	$-59/18$	$(3,0,0,0)$	$41/18$	$(3,0,0)$	$-23/18$	$(3,0)$	$5/18$	$(3,)$	$13/18$		
$(2,1,0,0,0)$	$-59/6$	$(2,1,0,0)$	$41/6$	$(2,1,0)$	$-23/6$	$(2,1)$	$5/6$				
$(1,1,1,0,0)$	$-59/3$	$(1,1,1,0)$	$41/3$	$(1,1,1)$	$-23/3$						
$(2,0,0,0,0)$	$161/4$	$(2,0,0,0)$	$-69/4$	$(2,0,0)$	$13/4$	$(2,0)$	$7/4$	$(2,)$	$9/4$		
$(1,1,0,0,0)$	$161/2$	$(1,1,0,0)$	$-69/2$	$(1,1,0)$	$13/2$	$(1,1)$	$7/2$				
$(1,0,0,0,0)$	$-9421/54$	$(1,0,0,0)$	$1933/54$	$(1,0,0)$	$209/54$	$(1,0)$	$79/54$	$(1,)$	$119/54$		
$(0,0,0,0,0)$	$16832/81$	$(0,0,0,0)$	$-560/81$	$(0,0,0)$	$-160/81$	$(0,0)$	$-92/81$	$(0,)$	$-142/81$	$()$	$8881/81$