On the divisors of a typical integer

Ben Green

University of Oxford, supported by a Simons Investigator grant

Austrian Special Research Area (SFB) Online Colloquium
February 5, 2021

Introduction

Joint work with Dimitris Koukoulopoulos and Kevin Ford. *Equal sums in random sets and the concentration of divisors*, arXiv:1908.00378.

Let n be a "typical" integer (say selected at random from $[1, X]$, for large X).

What do the divisors of n look like?

We will be interested in the particular question of how concentrated they are.

Hooley's Δ-function

Obituary of Hooley by Roger Heath-Brown:
https://royalsocietypublishing.org/doi/10.1098/rsbm.2020.0027

Define

$$\Delta(n) := \max_i \#\{d|n : e^i \leqslant d \leqslant e^{i+1}\}.$$

Hooley's Δ-function

What do we expect? Trivially $\Delta(n) \geqslant 1$, but nothing else is obvious, even heuristically.

Classical: let $n \leqslant X$ be a random integer. n has $\sim (\log X)^{\log 2 + o(1)}$ divisors.

Thus, on the log scale, there are $D := \log X$ "bins" (intervals $[e^i, e^{i+1}]$) and typically $(\log X)^{\log 2 + o(1)} \approx D^{0.693}$ "balls" (divisors) to put in them.

If these balls were distributed uniformly and independently then ("birthday paradox") we would expect two in the same box, but not three.

Maier and Tenenbaum (1985, resolving a 1948 conjecture of Erdős): $\Delta(n) \geqslant 2$ a.s.

Heuristics on Hooley's Δ-function

The logs of the divisors of n have a lot of additive structure.

For example, if $n = p_1 \cdots p_k$ is squarefree (which is the generic case) then the $\log d$ are the grid $\{\varepsilon_1 \log p_1 + \cdots + \varepsilon_k \log p_k : \varepsilon_i \in \{0,1\}\}$.

This leads to far more bunching of the divisors than the naïve heuristic suggests.

Maier and Tenenbaum already obtained in 1985 the bound

$$\Delta(n) \gg (\log\log n)^{c_1+o(1)} \text{ a.s., where } c_1 = -\frac{\log 2}{\log(1-\frac{1}{\log 3})} \approx 0.288.$$

In 2009, with a much more elaborate argument, they improved this to

$$\Delta(n) \gg (\log\log n)^{c_2+o(1)}, \text{ a.s. where } c_2 = \frac{\log 2}{\log\left(\frac{1-1/\log 27}{1-1/\log 3}\right)} \approx 0.338.$$

They conjectured that this is optimal.

A new lower bound

Theorem (FGK 2019)

We have $\Delta(n) \gg (\log\log n)^{c_3+o(1)}$ *a.s., where* $c_3 = \eta \approx 0.353$.

We conjecture that *this* is optimal.

η is given by $\eta = \frac{\log 2}{\log(2/\rho)}$, where $\rho \approx 0.281$ is given in terms of a rather complicated recurrence: ρ satisfies the equation

$$\frac{1}{1-\rho/2} = \log 2 + \sum_{j=1}^{\infty} \frac{1}{2^j} \log\left(\frac{a_{j+1}+a_j^{\rho}}{a_{j+1}-a_j^{\rho}}\right),$$

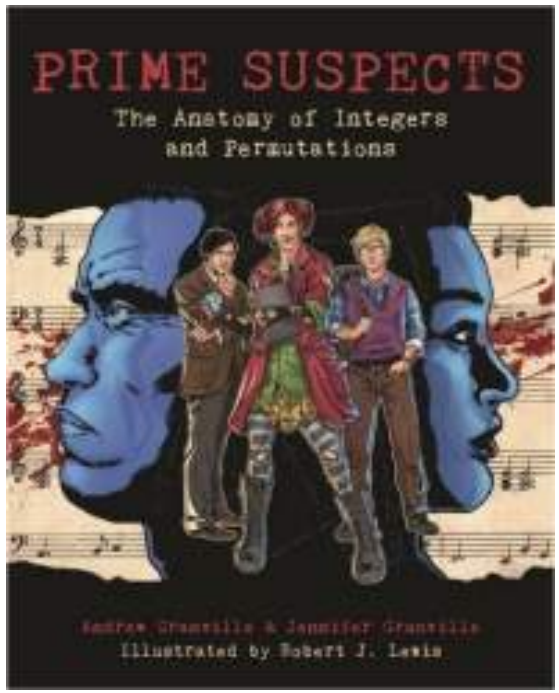
where the sequence a_j is defined by

$$a_1 = 2, \quad a_2 = 2+2^{\rho}, \quad a_j = a_{j-1}^2 + a_{j-1}^{\rho} - a_{j-2}^{2\rho} \qquad (j \geqslant 3).$$

A random model for the problem

A *logarithmic random set* A is a subset of $\mathbb{N}$ in which we select i to lie in A with probability $1/i$, these choices being independent.

Well-known principle. (Turán–Kubilius, etc) The logarithms of the prime factors of a random (squarefree) integer $n \leqslant X$ behave somewhat like $\mathrm{A} \cap [1, \dots, D]$, $D = \log X$, at least away from the edges.



A random model for the problem

A *logarithmic random set* A is a subset of $\mathbb{N}$ in which we select i to lie in A with probability $1/i$, these choices being independent.

Well-known principle. (Turán–Kubilius, etc) The logarithms of the prime factors of a random (squarefree) integer $n \leqslant X$ behave somewhat like $\mathrm{A} \cap [1, \dots, D]$, $D = \log X$, at least away from the edges.

Correspondingly, the logs of the divisors of $n \leqslant X$ should behave like the sums of elements of A in $[1, \dots, D]$.

Let $r_{\mathrm{A}}(x)$ be the number of ways of writing x as a sum of elements of A.

Model problem: what is $\max_{x \leqslant D} r_{\mathrm{A}}(x)$?

Truncated model problem

Determine β_k, the supremum of all exponents $c < 1$ for which the following is true, a.s. as $D \to \infty$:

Some x is representable in k different ways as a sum of elements of $\mathsf{A} \cap [D^c, D]$.

Lemma

$\Delta(n) \gg (\log\log n)^{\log k/\log(1/\beta_k)-o(1)}$ *a.s.*

Idea: first pass to the model problem. No explicit link between the model setting and the integer setting in the existing literature. Proof uses fairly familiar probabilistic and sieve theoretic ideas.

Model problem: "tensor trick": If x is a sum of elements of $\mathsf{A} \cap [D^c, D]$ in k ways and if y is a sum of elements of $\mathsf{A} \cap [D^{c^2}, D^c]$ in k ways then $x + y$ is a sum of elements of $\mathsf{A} \cap [D^{c^2}, D]$ in k^2 ways.

Main theorem – model problem

Last slide: β_k is the supremum of all exponents $c < 1$ for which the following is true, a.s. as $D \to \infty$: there is some x representable in k different ways as a sum of elements of $\mathrm{A} \cap [D^c, D]$, where A is a logarithmic random set.

Proposition

$\limsup_{k\to\infty} \frac{\log k}{\log(1/\beta_k)} \geqslant \eta$, *with* η *as defined before.*

Determining the exact values of the β_k is an extremely complicated problem. We do know that $\beta_2 = 1 - \frac{1}{\log 3}$, and in a future paper we will show that

$$\beta_3 = \frac{\log 3 - 1}{\log 3 + \frac{\log 3 - \log 2}{\log 2 - \log(e-1)}} \approx 0.026.$$

Further β_k values

We will also show that

$$\beta_4 = \frac{\log 3 - 1}{\log 3 + \frac{1}{\xi} + \frac{1}{\xi\lambda}} = 0.012951860913605119 18\ldots$$

where

$$\xi = \frac{\log 2 - \log(e-1)}{\log(3/2)}, \qquad \lambda = \frac{\log 2 - \log(e-1)}{1 + \log 2 - \log(e-1) - \log(1+2^{1-\xi})}.$$

β_5 appears not to have a closed form expression, but can be given numerically to high accuracy.

Flags and entropy

One of the main ideas of our paper is that β_k (essentially) coincides with what appears to be a completely different problem, to do with optimizing measures over the cube $\{0,1\}^k$. Even stating this problem requires some work.

Definition (Flags and subflags)

Let $k \in \mathbb{N}$. By an r-step *flag* we mean a nested sequence

$$\mathscr{V} : \langle 1 \rangle = V_0 \leqslant V_1 \leqslant V_2 \leqslant \cdots \leqslant V_r \leqslant \mathbb{Q}^k$$

of vector spaces. Here $1 = (1, 1, \ldots, 1) \in \mathbb{Q}^k$. Another flag

$$\mathscr{V}' : \langle 1 \rangle = V_0' \leqslant V_1' \leqslant V_2' \leqslant \cdots \leqslant V_r' \leqslant \mathbb{Q}^k$$

is said to be a *subflag* of $\mathscr{V}$ if $V_i' \leqslant V_i$ for all i. In this case we write $\mathscr{V}' \leqslant \mathscr{V}$. It is a *proper subflag* if it is not equal to $\mathscr{V}$.

Entropy of a subspace

Definition (Entropy of a subspace)

Suppose that ν is a finitely supported probability measure on $\mathbb{Q}^k$ and that $W \leqslant \mathbb{Q}^k$ is a vector subspace. Then we define

$$\mathrm{H}_\nu(W) := -\sum_x \nu(x) \log \nu(W + x).$$

Remark. This is the (Shannon) entropy of the distribution on cosets $W + x$ induced by ν.

Example: if ν is the uniform measure on $\{0,1\}^2$ and if W is the line $x_1 = x_2$ then

$$\mathrm{H}_\nu(W) = -\frac{1}{2}\log(\frac{1}{2}) - \frac{1}{4}\log(\frac{1}{4}) - \frac{1}{4}\log(\frac{1}{4}) = \frac{3}{2}\log 2.$$

Optimisation problem

Define γ_k to be the supremum of all constants c_{r+1} such that the following exist:

1. An r-step flag $\mathscr{V}$ whose members are distinct, spanned by elements of $\{0,1\}^k$ and which is nondegenerate in the sense that V_r is not contained in any subspace $\{x \in \mathbb{Q}^k : x_i = x_j\}$;
2. Parameters $1 \geqslant c_1 \geqslant c_2 \geqslant \cdots \geqslant c_{r+1} \geqslant 0$;
3. Probability measures $\mu_1, \dots, \mu_r$, with μ_i supported on $\{0,1\}^k \cap V_i$

such that we have the following *entropy condition*

$$\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V}), \tag{1}$$

for all subflags $\mathscr{V}' \leqslant \mathscr{V}$, where

$$\mathrm{e}(\mathscr{V}') := \sum_{j=1}^{r} (c_j - c_{j+1}) \mathrm{H}_{\mu_j}(V_j') + \sum_{j=1}^{r} c_j \dim(V_j'/V_{j-1}').$$

Define the variant $\tilde{\gamma}_k$ in exactly the same way, except with (**??**) replaced by the *strict entropy condition* $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$ for all proper subflags $\mathscr{V}' < \mathscr{V}$.

Equal sums in random sets again

Theorem

We have $0 < \tilde{\gamma}_k \leqslant \beta_k \leqslant \gamma_k$.

Probably, $\tilde{\gamma}_k = \beta_k = \gamma_k$, but we cannot quite prove this.

Very rough idea. Let A be a logarithmic random set. Suppose I have distinct sets $A_1, \dots, A_k \subset$ A with

$$\sum_{a \in A_1} a = \cdots = \sum_{a \in A_k} a.$$

We associate a flag as follows.

The Venn diagram of the subsets $A_1, \dots, A_k$ produces a natural partition of A into 2^k subsets, which we denote by B_ω for $\omega \in \{0,1\}^k$. Here $A_i = \sqcup_{\omega : \omega_i = 1} B_\omega$.

Associating a flag to a Venn diagram

The Venn diagram of the subsets $A_1, \dots, A_k$ produces a natural partition of A into 2^k subsets, which we denote by B_ω for $\omega \in \{0,1\}^k$. Here $A_i = \sqcup_{\omega:\omega_i=1} B_\omega$.

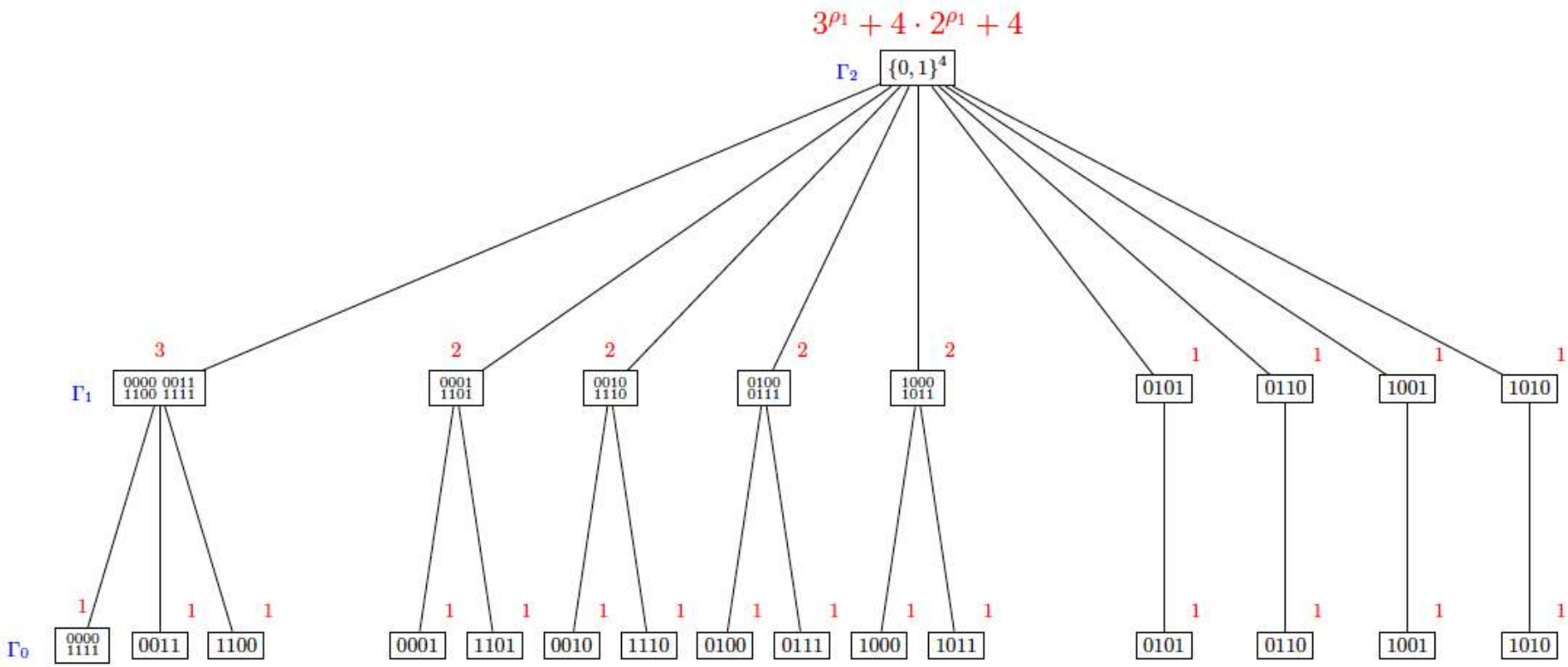
We iteratively select vectors $\omega^1, \dots, \omega^r$ to maximize $\prod_{j=1}^r (\max B_{\omega^j})$ subject to the constraint that $1, \omega^1, \dots, \omega^r$ are linearly independent over $\mathbb{Q}$.

We then define $V_j = \mathrm{Span}_{\mathbb{Q}}(1, \omega^1, \dots, \omega^j)$ for $j = 0, 1, \dots, r$. The point is that the ω^i provide the "right" basis for analysing the equal sums equations

$$\sum_{a \in A_1} a = \cdots = \sum_{a \in A_k} a.$$

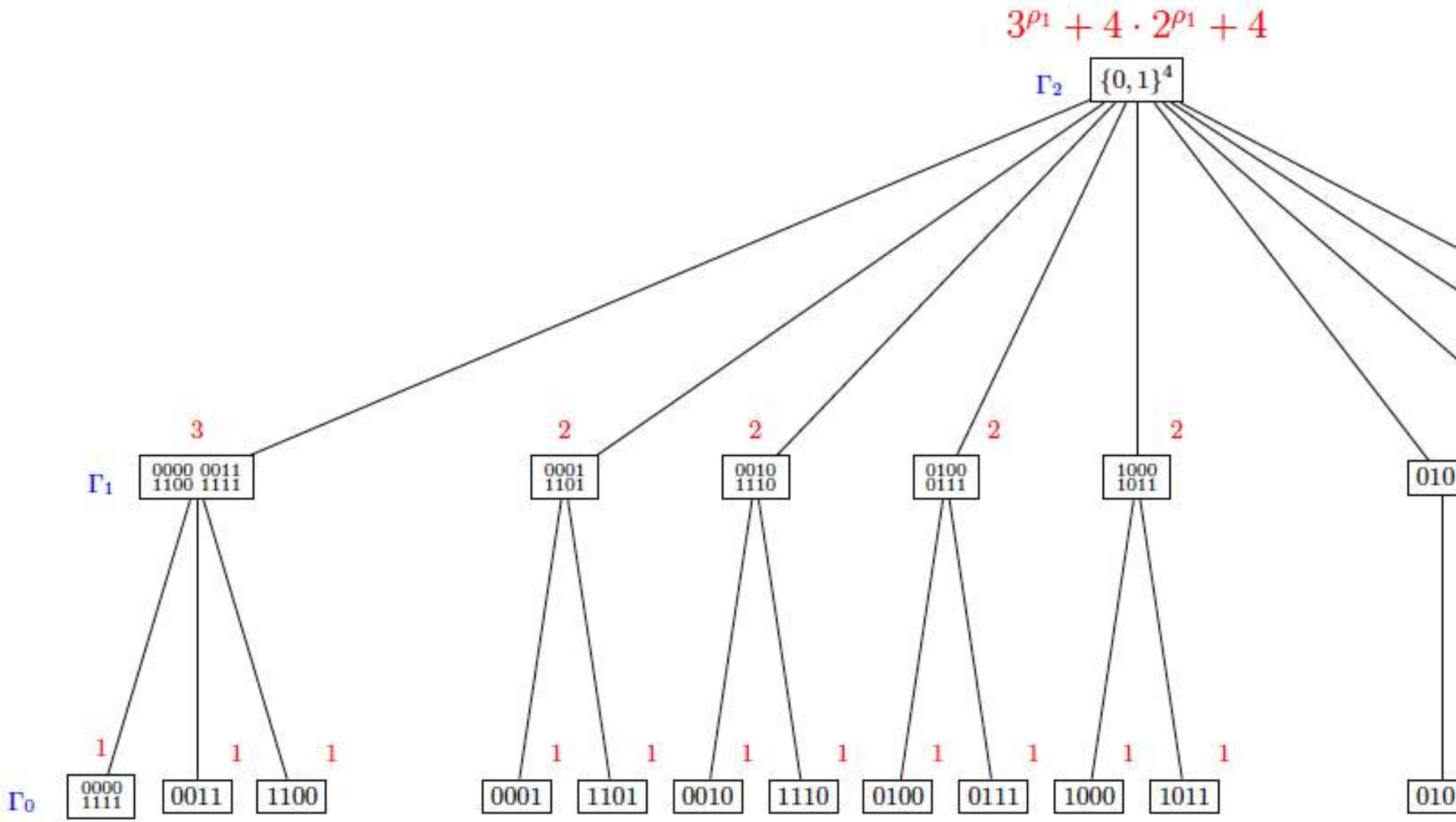
A tree recurrence

$\vec{\rho} = (\rho_0, \rho_1, \rho_2, \dots)$, $\rho_0 = 1$. Recurrence: $f^C(\rho) = \sum_{C \to C'} f^{C'}(\rho)^{\rho_{i-1}}$.



Tree of binary flag $\langle \mathbf{1} \rangle = V_0 \leq V_1 \leq V_2 = \mathbb{Q}^4$, where $V_1 := \{(x, x, y, y) : x, y \in \mathbb{Q}\}$. Values of $f^C(\rho)$ are given in red.

A tree recurrence



Solving* the optimisation problem

Theorem

Suppose that the flag $\mathscr{V}$ is fixed. Under certain conditions (satisfied in situations of interest) the optimal value of c_{r+1} in the optimisation problem is given by the formula

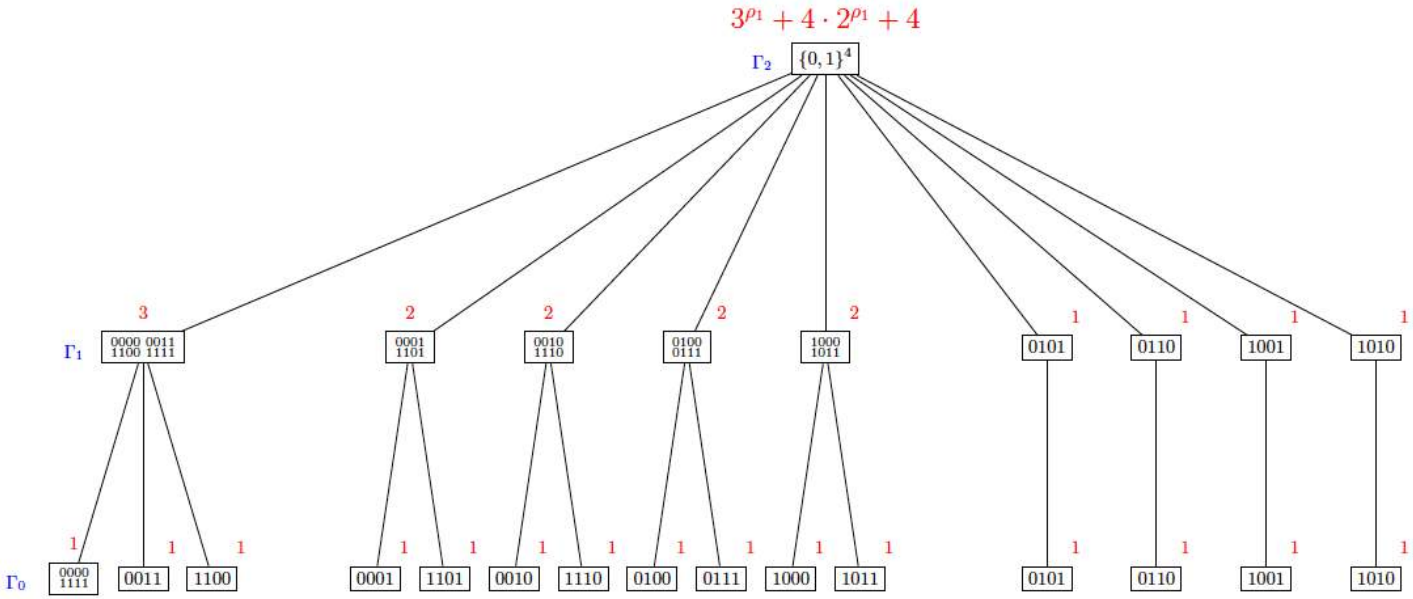
$$\tilde{\gamma}_k(\mathscr{V}) = (\log 3 - 1) \Big/ \left(\log 3 + \sum_{i=1}^{r-1} \frac{\dim(V_{i+1}/V_i)}{\rho_1 \cdots \rho_i} \right).$$

Write Γ_j for the cell at level j (that is, coset of V_j) containing $0 \in \mathbb{Q}^k$. The ρ_i satisfy the "ρ-equations" $\rho_0 = 1$ and

$$f^{\Gamma_{j+1}}(\rho) = (f^{\Gamma_j}(\rho))^{\rho_j} e^{\dim(V_{j+1}/V_j)}, \qquad j = 1, 2, \ldots, r-1,$$

where the $f^C(\rho)$ are defined by a tree recurrence as illustrated in the pictures.

Solving the optimisation problem



Tree of binary flag $\langle \mathbf{1} \rangle = V_0 \leq V_1 \leq V_2 = \mathbb{Q}^4$, where $V_1 := \{(x, x, y, y) : x, y \in \mathbb{Q}\}$. Values of $f^C(\rho)$ are given in red.

The ρ-equations consist of the single equation $f^{\Gamma_2}(\rho) = (f^{\Gamma_1}(\rho))^{\rho_1} e^2$, that is to say $3^{\rho_1} + 4 \cdot 2^{\rho_1} + 4 = 3^{\rho_1} e^2$.

This has the unique solution $\rho_1 \approx 0.306481$.

Solving the optimisation problem – sketch

Fix a flag $\mathscr{V} : \langle 1 \rangle = V_0 \leqslant V_1 \leqslant V_2 \leqslant \cdots \leqslant V_r \leqslant \mathbb{Q}^k$. Recall that γ_k is the supremum of all constants c_{r+1} such that there are

1. parameters $1 \geqslant c_1 \geqslant c_2 \geqslant \cdots \geqslant c_{r+1} \geqslant 0$, and
2. probability measures $\mu_1, \dots, \mu_r$, with μ_i supported on $\{0,1\}^k \cap V_i$

such that we have the *entropy condition* $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V})$ for all subflags $\mathscr{V}' \leqslant \mathscr{V}$, where

$$\mathrm{e}(\mathscr{V}') := \sum_{j=1}^{r} (c_j - c_{j+1}) \mathrm{H}_{\mu_j}(V_j') + \sum_{j=1}^{r} c_j \dim(V_j'/V_{j-1}').$$

Step 1. solve the problem in which the entropy condition is only required to hold for very special subflags $\mathscr{V}'$ (called "basic"): those in which $V_i' = V_i$ for $i \leqslant m$, and then $V_i' = V_m$ for $i = m+1, \dots, r$. This involves a linear programming approach.

Solving the optimisation problem – sketch

Step 2. Show that, for the parameters c_i and measures μ_i found in step 1, the more general entropy condition $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V})$ for an arbitrary subflag $\mathscr{V}'$ follows automatically from the very special case of basic flags.

Crucial idea is *symmetrisation* via repeated use of submodularity property of entropy. If σ is a permutation of coordinates preserving the flag $\mathscr{V}$, then

$$2\,\mathrm{e}(\mathscr{V}') = \mathrm{e}(\mathscr{V}') + \mathrm{e}(\sigma(\mathscr{V}')) \geqslant \mathrm{e}(\mathscr{V}' + \sigma(\mathscr{V}')) + \mathrm{e}(\mathscr{V}' \cap \sigma(\mathscr{V}')).$$

Step 3. Finally, show that one can perturb by arbitrarily small amounts to get a system satisfying the strict entropy condition $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$ (this is not as trivial as one might think).

Which flags are optimal?

Short answer: we are not quite sure.

Longer answer: based on numerical evidence and "naturality" we believe that so-called *binary* flags are (asymptotically) optimal.

Definition (Binary flags)

Let $k = 2^r$ be a power of two. Identify $\mathbb{Q}^k$ with $\mathbb{Q}^{\mathcal{P}[r]}$ (where $\mathcal{P}[r]$ means the power set of $[r] = \{1, \dots, r\}$) and define a flag $\mathscr{V}$,

$$\langle 1 \rangle = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_r = \mathbb{Q}^{\mathcal{P}[r]},$$

as follows: V_i is the subspace of all $(x_S)_{S \subset [r]}$ for which $x_S = x_{S \cap [i]}$ for all $S \subset [r]$.

ρ PARAMETERS FOR BINARY FLAGS

Given $\vec{\rho} = (\rho_0, \rho_1, \rho_2, \dots)$, $\rho_0 = 1$, set up the tree-recurrence $f^C(\rho) = 1$ for C at level 0 and then for C at level i by $f^C(\rho) = \sum_{C \to C'} f^{C'}(\rho)^{\rho_{i-1}}$ where C' runs over the children of C.

The ρ-equations:

$$f^{\Gamma_{j+1}}(\rho) = (f^{\Gamma_j}(\rho))^{\rho_j} e^{\dim(V_{j+1}/V_j)}, \qquad j = 1, 2, \dots, r-1,$$

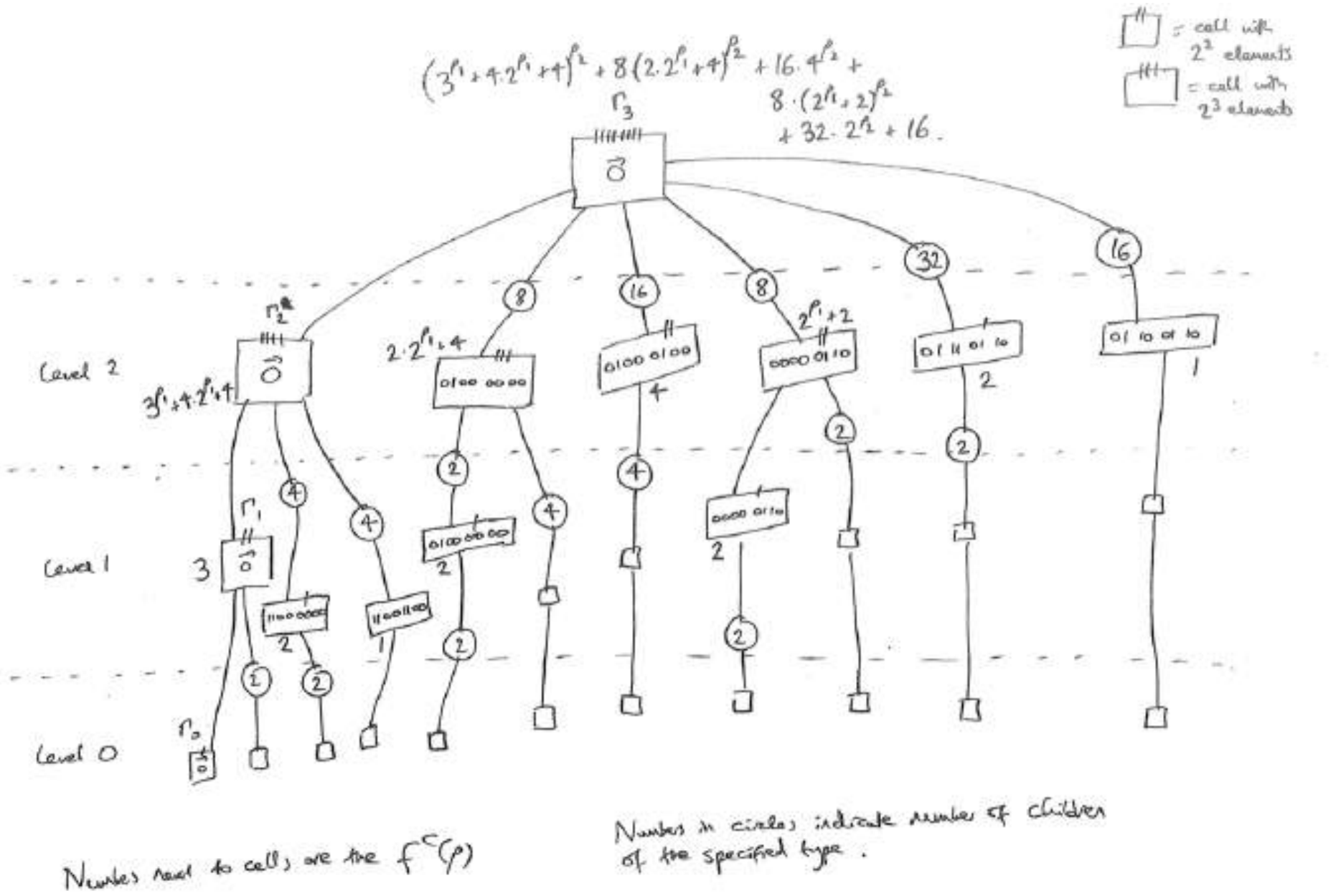
where Γ_j is the cell at level j containing 0.

We have already seen that the first nontrivial such equation is $f^{\Gamma_2}(\rho) = (f^{\Gamma_1}(\rho))^{\rho_1} e^2$, that is to say $3^{\rho_1} + 4 \cdot 2^{\rho_1} + 4 = 3^{\rho_1} e^2$.

This has the unique solution $\rho_1 \approx 0.306481$.

To write down the ρ-equation for $j = 2$, one must compute $f^{\Gamma_3}(\rho)$, and without any additional theory the only means we have to do this is to draw the full tree structure for the binary flag $\mathscr{V}$ of order 3 (on $\mathbb{Q}^8$).

ρ PARAMETERS FOR BINARY FLAGS



ρ PARAMETERS FOR BINARY FLAGS

In particular

$$f^{\Gamma_3}(\rho) = (3^{\rho_1}+4\cdot 2^{\rho_1}+4)^{\rho_2}+8(2\cdot 2^{\rho_1}+4)^{\rho_2}+16\cdot 4^{\rho_2}+8\cdot(2^{\rho_1}+2)^{\rho_2}+32\cdot 2^{\rho_2}+16.$$

The second ρ-equation is

$$f^{\Gamma_3}(\rho) = f^{\Gamma_2}(\rho)^{\rho_2} e^4,$$

which has the numerical solution $\rho_2 \approx 0.2796104\ldots$.

THEOREM

$\rho = \lim_{j\to\infty} \rho_j$ exists.

(Very) rough idea: "almost self-similarity": the cell structure on $\{0,1\}^{2^{r+1}}$ induced by the binary flag of order $r+1$ is "almost" the product of two copies of the structure on $\{0,1\}^{2^r}$. Doesn't help with computations.

Recursion relations and computations

Proposition

Define a sequence $a_{i,j}$ by the relations $a_{i,1} = 2$, $a_{i,2} = 2 + 2^{\rho_{i-1}}$ and

$$a_{i,j} = a_{i,j-1}^2 + a_{i-1,j-1}^{\rho_{i-1}} - a_{i-1,j-2}^{2\rho_{i-1}} \ (j \geqslant 3).$$

Then

$$a_{i,i+1} = a_{i-1,i}^{\rho_{i-1}} e^{2^{i-1}}.$$

Tabulating the ρ_j

j	ρ_j
1	0.3064810093305
2	0.2796104150767
3	0.2813005404710
4	0.2812067224539
5	0.2812115789381
6	0.2812113387071
7	0.2812113502101
8	0.2812113496729
9	0.2812113496974
10	0.2812113496963
11	0.2812113496964
12	0.2812113496964
13	0.2812113496964

Limit of the ρ_j

Proposition

Define a sequence a_j (depending on an arbitrary parameter $\rho \in (0,1)$) by

$$a_1 = 2, a_2 = 2 + 2^\rho, a_j = a_{j-1}^2 + a_{j-1}^\rho - a_{j-2}^{2\rho} \ \ (j \geqslant 3).$$

Then the limit $\rho = \lim_{i\to\infty} \rho_i$ satisfies the relation

$$\frac{1}{1-\rho/2} = \log 2 + \sum_{j=1}^{\infty} \frac{1}{2^j} \log\left(\frac{a_{j+1} + a_j^\rho}{a_{j+1} - a_j^\rho}\right).$$