EQUAL SUMS IN RANDOM SETS AND THE CONCENTRATION OF DIVISORS

KEVIN FORD, BEN GREEN, AND DIMITRIS KOUKOULOPOULOS

ABSTRACT. We study the extent to which divisors of a typical integer n are concentrated. In particular, defining the Erdős-Hooley Δ-function by $\Delta(n) := \max_t \#\{d|n, \log d \in [t, t+1]\}$, we show that $\Delta(n) \geqslant (\log\log n)^{0.35332277\ldots}$ for almost all n, a bound we believe to be sharp. This disproves a conjecture of Maier and Tenenbaum. We also prove analogs for the concentration of divisors of a random permutation and of a random polynomial over a finite field.

Most of the paper is devoted to a study of the following much more combinatorial problem of independent interest. Pick a random set $\mathbf{A} \subset \mathbb{N}$ by selecting i to lie in $\mathbf{A}$ with probability $1/i$. What is the supremum of all exponents β_k such that, almost surely as $D \to \infty$, some integer is the sum of elements of $\mathbf{A} \cap [D^{\beta_k}, D]$ in k different ways?

We characterise β_k as the solution to a certain optimisation problem over measures on the discrete cube $\{0,1\}^k$, and obtain lower bounds for β_k which we believe to be asymptotically sharp.

CONTENTS

2010 *Mathematics Subject Classification.* Primary 11N25; Secondary 05A05,11S05.

PART I. MAIN RESULTS AND OVERVIEW OF THE PAPER

1. INTRODUCTION

1.1. The Erdős-Hooley Δ-function

Given an integer n, we define the Erdős-Hooley Δ-function

$$\Delta(n) := \max_t \#\{d|n, \log d \in [t, t+1]\},$$

that is to say the maximum number of divisors n has in any interval of logarithmic length 1. Its normal order (almost sure behaviour) has proven quite mysterious, and indeed it was a celebrated achievement of Maier and Tenenbaum [20], answering a question of Erdős from 1948 [11], to show that $\Delta(n) > 1$ for almost every n.

Work on the distribution of Δ began with Erdős [7], Erdős and Nicolas [9, 10] and Hooley [17] in the 1970s. Further work on the normal and average behavior of Δ can be found in the papers of Tenenbaum [23, 24], Hall and Tenenbaum [13, 14, 15], and of Maier and Tenenbaum [20, 21, 22]. See also [16, Ch. 5,6,7]. Tenenbaum's survey paper [26, p. 652–658] includes a history of the function Δ and description of many applications in number theory.

The best bounds for $\Delta(n)$ for "normal" n currently known were obtained in a more recent paper of Maier and Tenenbaum [22].

Theorem MT (Maier–Tenenbaum [22]) *For almost all integers n we have*

$$(\log\log n)^{c_1-o(1)} \leqslant \Delta(n) \leqslant (\log\log n)^{\log 2+o(1)},$$

where

$$c_1 = \frac{\log 2}{\log\left(\frac{1-1/\log 27}{1-1/\log 3}\right)} \approx 0.33827.$$

It is conjectured in [22] that the lower bound is optimal.

One of the main results of this paper is a disproof of this conjecture.

Theorem 1. *For almost all integers n we have*

$$\Delta(n) \geqslant (\log\log n)^{\eta-o(1)},$$

where $\eta = 0.35332772701323467 11\ldots$.

The constant η, which we believe to be sharp, is described in relation (1.1) below, just after the statement of Theorem 2.

1.2. Random sets and equal sums

For most of the paper we do not talk about integers and divisors, but rather about the following model setting. Throughout the paper, $\mathbf{A}$ will denote a random set of positive integers in which i is included in $\mathbf{A}$ with probability $1/i$, these choices being independent for different is. We refer to $\mathbf{A}$ as a *logarithmic random set*. We have

$$\mathbb{E}\#(\mathbf{A} \cap I) = \sum_{i\in I} 1/i$$

for any interval I, and later we will show that with high probability, $\mathbf{A}$ has close to this expected number of elements in all "large" intervals I.

A large proportion of our paper will be devoted to understanding conditions under which there is an integer which can be represented as a sum of elements of $\mathbf{A}$ in (at least) k different ways. In particular, we wish to obtain bounds on the quantities β_k defined in the following problem.

Problem 1.1. Let $k \geqslant 2$ be an integer. Determine β_k, the supremum of all exponents $c < 1$ for which the following is true, a.s. as $D \to \infty$: there are distinct sets $A_1, \cdots, A_k \subset \mathbf{A} \cap [D^c, D]$ with $\sum_{a \in A_1} a = \cdots \sum_{a \in A_k} a$.

The main result of this paper is an asymptotic lower bound on β_k.

Theorem 2. *For each integer $r \geqslant 1$ there is a constant θ_r, defined in Definition 9.6 in terms of the solution to certain equations arising from a nonlinear recurrence on a particular tree, such that the following hold:*

(a) *For each r, we have $\beta_{2^r} \geqslant \theta_r$.*

(b) *The limit $\lim_{r\to\infty} \theta_r^{1/r}$ exists and equals $\rho/2$, where $\rho = 0.28121134969637466015\ldots$ This ρ satisfies the equation*

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

where the sequence a_j is defined by

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

In terms of ρ, the constant η in Theorem 1 is given by

$$\eta = \frac{\log 2}{\log(2/\rho)}. \tag{1.1}$$

We conjecture that our lower bounds on β_k are asymptotically sharp.

Conjecture 1. *Define*

$$\zeta = \limsup_{k\to\infty} \frac{\log k}{\log(1/\beta_k)}. \tag{1.2}$$

Then $\zeta = \eta = 0.3533227\ldots$.

We believe that our bounds are not *strictly* sharp for any $r \geqslant 2$, that is to say $\beta_{2^r} > \theta_r$ for all $r \geqslant 2$. We will address the exact values of β_k in a future paper; in particular, we will show that

$$\beta_3 = \frac{\log 3 - 1}{\log 3 + \frac{1}{\xi}} = 0.026162187973169651 33\ldots$$

and

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

where

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

The proof of Theorem 2 will occupy the bulk of this paper. Parts (a) and (b) are quite independent of one another, with the proof of (a) (given in subsection 9.2) being by far the longer of the two. The definition of θ_r, while somewhat complicated, is fairly self-contained: see Definition 9.6. Part

(b) is then a problem of an analytic and combinatorial flavour which can be addressed largely independently of the main arguments of the paper.

1.3. **Application to divisors of integers, permutations and polynomials**

The link between Problem 1.1 and the concentration of divisors is given by the following Theorems. The proofs are relatively straightforward and given in the next section. Recall from (1.2) the definition of ζ.

Theorem 3. *For almost every n, we have*

$$\Delta(n) \gg (\log\log n)^{\zeta-o(1)}.$$

The same probabilistic setup allows us to quickly make similar conclusions about the distribution of divisors (product of cycles) of permutations and of polynomials over finite fields.

Theorem 4. *For a permutation σ on S_n, denote by*

$$\Delta(\sigma) := \max_r \#\{d|\sigma : \mathrm{length}(d) = r\},$$

where d denotes a generic divisor of σ; that is, d is the product of a subset of the cycles of σ. Then, for all but $o_{n\to\infty}(n!)$ of the permutations $\sigma \in S_n$, we have

$$\Delta(\sigma) \geqslant (\log n)^{\zeta-o(1)}.$$

Theorem 5. *Let q be any prime power. For a polynomial $f \in \mathbb{F}_q[t]$, let*

$$\Delta(f) = \max_r \#\{g|f : \deg(g) = r\}.$$

If f is a random monic polynomial of degree n, then with probability $\to 1$ as $n \to \infty$,

$$\Delta(f) \geqslant (\log n)^{\zeta-o(1)}.$$

Conjecture 2. *The lower bounds given in Theorems 3, 4 and 5 are sharp. That is, $\Delta(n) = (\log\log n)^{\zeta+o(1)}$ for almost all n, $\Delta(\sigma) = (\log\sigma)^{\zeta+o(1)}$ for $(1+o(1))n!$ of the permutations $\sigma \in S_n$, and $\Delta(f) = (\log n)^{\zeta+o(1)}$ for almost all polynomials of degree n over $\mathbb{F}_q$. Here, $o(1)$ refers to functions of n tending to 0 as $n \to \infty$.*

If both Conjectures 1 and 2 hold, then we deduce that the optimal exponent in the above Theorems is equal to η.

Remark. The optimal exponent in Theorems 3, 4 and 5 depends only on accurate asymptotics for β_k as $k \to \infty$. In this work, however, we develop a framework for determining β_k exactly for each k.

The quantity β_k is also closely related to the densest packing of k divisors of a typical integer. To be specific, we define α_k be the supremum of all real numbers α such that for almost every $n \in \mathbb{N}$, n has k divisors $d_1 < \cdots < d_k$ with $d_k \leqslant d_1(1 + (\log n)^{-\alpha})$. In 1964, Erdős [6] conjectured that $\alpha_2 = \log 3 - 1$, and this was confirmed by Erdős and Hall [8] (upper bound) and Maier and Tenenbaum [20] (lower bound). The best bounds on α_k for $k \geqslant 3$ are given by Maier and Tenenbaum [22], who showed that

$$\alpha_k \leqslant \frac{\log 2}{k+1} \qquad (k \geqslant 3)$$

and (this is not stated explicitly in [22])

$$\alpha_k \geqslant \frac{(\log 3 - 1)^m 3^{m-1}}{(3\log 3 - 1)^{m-1}} \qquad (2^{m-1} < k \leqslant 2^m, m \in \mathbb{N}). \tag{1.3}$$

See also [26, p. 655–656][1]. In particular, it is not known if $\alpha_3 > \alpha_4$, although Tenenbaum [26] conjectures that the sequence $(\alpha_k)_{k\geqslant 2}$ is strictly decreasing.

We can quickly deduce a lower bound for α_k in terms of β_k.

Theorem 6. *for all $k \geqslant 2$ we have $\alpha_k \geqslant \beta_k/(1-\beta_k)$.*

In particular,

$$\alpha_3 \geqslant \frac{\beta_3}{1-\beta_3} = 0.0268650\ldots,$$

which is substantially larger than the bound from (1.3), which is $\alpha_3 \geqslant 0.0127069\ldots$.

Combining Theorem 6 with the bounds on β_k given in Theorem 2, we have improved the lower bounds (1.3) for large k (in fact, our bounds are better than (1.3) for all $k \geqslant 3$).

The upper bound on α_k is more delicate, and a subject which we will return to in a future paper. For now, we record our belief that the lower bound in Theorem 6 is sharp.

Conjecture 3. *For all $k \geqslant 2$ we have $\alpha_k = \beta_k/(1-\beta_k)$.*

Acknowledgements. This collaboration began at the MSRI program on Analytic Number Theory, which took place in the first half of 2017 and which was supported by the National Science Foundation under Grant No. DMS-1440140. All three authors are grateful to MSRI for allowing us the opportunity to work together.

The project was completed during a visit of KF and DK to Oxford in the first half of 2019. Both authors are grateful to the University of Oxford for its hospitality.

KF is supported by the National Science Foundation Grants DMS-1501982 and DMS-1802139. In addition, his stay at Oxford in early 2019 was supported by a Visiting Fellowship at Magdalen College Oxford. BG is supported by a Simons Investigator Grant, which also funded DK's visit to Oxford. DK is also supported by the Natural Sciences and Engineering Research Council of Canada (Discovery Grant 2018-05699) and by the Fonds de recherche du Québec - Nature et technologies (projet de recherche en équipe - 256442).

2. Application to random integers, random permutations and random polynomials

In this section we prove Theorems 3, 4, 5 and 6.

The two main ingredients in the proof are a simple combinatorial device (Lemma 2.1), of a type often known as a "tensor power trick", used for building a large collection of equal subset sums, and transference results (Lemmas 2.2, 2.3 and 2.4) giving a correspondence between the random set $\mathbf{A}$ and prime factors of a random integer, the cycle structure of a random permutation and the factorization of a random polynomial over a finite field. In the integer setting, this is a well-known principle following, e.g. from the Kubilius model of the integers (Kubilius, Elliott [4, 5], Tenenbaum [25]). We give a self-contained (modulo using the sieve) proof below.

Throughout this section, $\mathbf{A}$ denotes a logarithmic random set.

[1]The factor 3^{m-1} is missing in the stated lower bounds for α_k in [26].

2.1. **A "tensor power" argument**

In this section we give a simple combinatorial argument, first used in a related context in the work of Maier-Tenenbaum [20], which shows how to use equal subsums in multiple intervals $((D')^c, D']$ to create many more common subsums in $\mathcal{A}$.

Lemma 2.1. *Let $k \geqslant 1$ be an integer. Let D_1, D_2 be parameters depending on D with $1 \leqslant D_1 < D_2 \leqslant D$, $\log\log D_1 = o(\log\log D)$ and $\log\log D_2 = (1-o(1))\log\log D$ as $D \to \infty$. Then, with probability $\to 1$ as $D \to \infty$, there are distinct $A_1, \dots, A_M \subset \mathbf{A} \cap [D_1, D_2]$ with $\sum_{a\in A_1} a = \cdots = \sum_{a\in A_M} a$ and $M \geqslant (\log D)^{(\log k)/\log(1/\beta_k)-o(1)}$.*

Remark. In particular, the result applies when $D_1 = 1$ and $D_2 = D$, in which case it has independent combinatorial interest, giving a (probably tight) lower bound on the growth of the representation function for a random set.

Proof. Since increasing the value of D_1 only makes the proposition stronger, we may assume that $D_1 \to \infty$. Let $\varepsilon > 0$, and set $\alpha := \beta_k - \varepsilon$. Set

$$m := \Big\lfloor \frac{\log\log D_2 - \log\log D_1}{-\log(\beta_k - \varepsilon)} \Big\rfloor$$

and consider the intervals $[D_2^{\alpha^{i+1}}, D_2^{\alpha^i})$, $i = 0, 1, \dots, m-1$. Due to the choice of m, these all lie in $[D_1, D_2]$.

Let E_i, $i = 0, 1, 2, \dots$ be the event that there are distinct $A_1^{(i)}, \dots, A_k^{(i)} \subset [D_2^{\alpha^{i+1}}, D_2^{\alpha^i})$ with $\sum_{a\in A_1^{(i)}} a = \cdots = \sum_{a\in A_k^{(i)}} a$. Then, by the definition of β_k and the fact that $D_1 \to \infty$, we have $\mathbb{P}(E_i) = 1 - o_{\varepsilon,k}(1)$, uniformly in i. These events E_i are all independent. The Law of Large Numbers then implies that, with probability $1 - o_{\varepsilon,k}(1)$, at least $(1 - o_{\varepsilon,k}(1))m$ of them occur, let us say for $i \in I$, $|I| = (1 - o_{\varepsilon,k}(1))m$.

From the above discussion, we have found $M := k^{|I|} = k^{(1-o_{\varepsilon,k}(1))m}$ distinct sets $B_{\boldsymbol{j}} = \bigcup_{i\in I} A_{j_i}^{(i)}$, $\boldsymbol{j} \in [k]^I$, such that all of the sums $\sum_{a\in B_{\boldsymbol{j}}} a$ are the same. Note that

$$M = k^{(1+O_k(\varepsilon)+o_{\varepsilon,k}(1))\log\log D/\log(1/\beta_k)}.$$

Taking $\varepsilon \to 0$, the result follows. □

2.2. **Modeling prime factors with a logarithmic random set**

Let X be a large parameter, suppose that

$$1 \leqslant K \leqslant (\log X)^{1/2}, \tag{2.1}$$

and let $I = [i_1, i_2] \cap \mathbb{N}$, where

$$i_1 = \big\lfloor K(\log\log X)^3 \big\rfloor, \quad i_2 = \left\lfloor \frac{K\log X}{2\log\log\log X} \right\rfloor. \tag{2.2}$$

For a uniformly random positive integer $\mathbf{n} \leqslant X$, let $\mathbf{n} = \prod_p p^{v_p}$ be the the prime factorization of $\mathbf{n}$, where the product is over all primes. Let $\mathscr{P}_i$ be the set of primes in $(e^{i/K}, e^{(i+1)/K}]$, and define the random set

$$\mathbf{B} = \{i \in I : b_i \geqslant 1\}, \quad b_i = \sum_{p\in\mathscr{P}_i} v_p \tag{2.3}$$

that is, the set of i for which $\mathbf{n}$ has a prime factor in $\mathscr{P}_i$. By the sieve, it is known that the random variables v_p are nearly independent for $p = X^{o(1)}$, and thus the probability that $b_i \geqslant 1$ is roughly

$$R_i := \sum_{p \in \mathscr{P}_i} \frac{1}{p} \approx \frac{1}{i}.$$

The next lemma makes this precise.

Lemma 2.2. *Uniformly for any collection $\mathscr{I}$ of subsets of I, we have*

$$\mathbb{P}(\mathbf{A} \cap I \in \mathscr{I}) = \mathbb{P}(\mathbf{B} \in \mathscr{I}) + O(1/\log\log X).$$

Proof. Recall the definition (2.2) of i_1, i_2. By the Prime Number Theorem with classical error term [27, Theorem II.4.1], we have for $i \in I$

$$R_i = \log\Big(\frac{i+1}{K}\Big) - \log\Big(\frac{i}{K}\Big) + O(e^{-(1/100)(i/K)^{1/2}}) = \frac{1}{i} + O\Big(\frac{1}{i^2}\Big). \tag{2.4}$$

For any $B \subset I$,

$$\mathbb{P}(\mathbf{A} \cap I = B) = \prod_{i \in B} \frac{1}{i} \prod_{i \in I \setminus B} \Big(1 - \frac{1}{i}\Big) = \prod_{i \in I} \Big(1 - \frac{1}{i}\Big) \prod_{i \in B} \frac{1}{i-1} = (1 + O(1/i_1)) \frac{i_1}{i_2} \prod_{i \in B} \frac{1}{i}.$$

Hence,

$$\mathbb{P}(\mathbf{A} \cap I \in \mathscr{I}) = (1 + O(1/i_1)) \frac{i_1}{i_2} \sum_{B \in \mathscr{I}} \prod_{i \in B} \frac{1}{i}. \tag{2.5}$$

Now we estimate $\mathbb{P}(\mathbf{B} \in \mathscr{I})$. Throughout, we set

$$Z = \exp\{i_1/K\} \quad \text{and} \quad Y = \exp\{(i_2+1)/K\}.$$

Firstly, the probability that some b_i is at least 2 is

$$\ll \sum_{i \in I} \prod_{p,p' \in \mathscr{P}_i} \frac{1}{pp'} \leqslant \sum_{i \in I} R_i^2 \ll \frac{1}{i_1}.$$

Next, fix a set B and, for every $i \in B$, fix a choice of a prime $p_i \in \mathscr{P}_i$ and define $Q = \prod_{i \in B} p_i$. Firstly, assume that B has the property

$$\sum_{i \in B} (i+1) > \frac{K \log X}{2}. \tag{2.6}$$

This implies

$$Q \geqslant \prod_{i \in B} e^{i/K} = e^{-|B|/K} \prod_{i \in B} e^{(i+1)/K} \geqslant X^{1/2} e^{-(i_2 - i_1 + 1)/K} \geqslant X^{1/3}.$$

Standard bounds on smooth numbers [27, Theorem III.5.1] imply that (2.6) occurs with probability $e^{-\log X/\log Y} \ll 1/\log\log X$.

Now suppose that (2.6) does not hold. Then $Q \leqslant X^{1/2}$. By the fundamental lemma of the sieve [12, Lemma 6.11], the probability that $Q|\mathbf{n}$ and $\mathbf{n}/Q$ has no prime factors in $(Z, Y]$ is equal to

$$(1 + O(e^{-\log X/\log Y})) \cdot \frac{1}{Q} \prod_{Z < p \leqslant Y} \Big(1 - \frac{1}{p}\Big).$$

Now $Y \ll X^{1/\log\log\log X}$ and thus summing over all choices of the p_i, we see that

$$\mathbb{P}\big((\mathbf{B}=B)\wedge(b_i\leqslant 1 \text{ for } i\in I)\big) = (1+O(1/\log\log X))\prod_{Z<p\leqslant Y}\Big(1-\frac{1}{p}\Big)\prod_{i\in B}\sum_{p_i\in\mathscr{P}_i}\frac{1}{p_i-1}.$$

Since

$$\sum_{p_i\in\mathscr{P}_i}\frac{1}{p_i-1} = R_i + O(e^{-i/K}) = \frac{1}{i}+O\Big(\frac{1}{i^2}\Big),$$

by (2.4) and the choice of K, we infer that

$$\mathbb{P}\big((\mathbf{B}=B)\wedge(b_i\leqslant 1 \text{ for } i\in I)\big) = (1+O(1/\log\log X))\frac{i_1}{i_2}\prod_{i\in B}\frac{1}{i}.$$

Summing over all $B\in\mathscr{I}$, and recalling (2.5), we conclude that

$$\mathbb{P}(\mathbf{A}\in\mathscr{I}) = (1+O(1/\log\log X))\cdot\mathbb{P}(\mathbf{B}\in\mathscr{I})+O(1/\log\log X). \qquad \square$$

2.3. **The concentration of divisors of integers**

In this section we prove Theorems 3 and 6. Recall from (1.2) the definition of ζ.

Proof of Theorem 3. Let X be large, and let $\mathbf{n}\leqslant X$ be a uniformly sampled random integer. Generate a logarithmic random set $\mathbf{A}$. Set $K=10\log\log X$, $D_1=i_1$, $D=D_2=i_2$, where i_1 and i_2 are defined by (2.2). With our choice of parameters, the hypotheses of Lemma 2.1 hold and hence, with probability $1-o(1)$, there are distinct sets $A_1,\dots,A_M\subset\mathbf{A}\cap[D_1,D_2]$ with $\sum_{a\in A_1}a=\cdots=\sum_{a\in A_M}a$ and $M\geqslant(\log\log X)^{\zeta-o(1)}$. Also with probability $1-o(1)$,

$$|A_i|\leqslant|\mathbf{A}\cap[D_1,D_2]|\leqslant 2\log D_2\leqslant 2\log\log X+2\log K$$

for all i. Write F for the event that both of these happen.

By Lemma 2.2, the corresponding event F' for the random set $\mathbf{B}$ also holds with probability $1-o(1)$; that is, F' is the event that $|\mathbf{B}\cap[D_1,D_2]|\leqslant 2\log D$ and that there are distinct subsets $B_1,\dots,B_M$ with equal sums. If we are in the event F' and $\mathbf{n}$ is divisible by $\prod_{i\in\mathbf{B}}p_i$, where $p_i\in\mathscr{P}_i$ for each i, then

$$\begin{aligned}\Big|\sum_{b\in B_i}\log p_b-\sum_{b\in B_j}\log p_b\Big| &\leqslant \frac{|B_i|+|B_j|}{K}+\frac{1}{K}\Big|\sum_{b\in B_i}b-\sum_{b\in B_j}b\Big|\\ &\leqslant \frac{4\log\log X+4\log K}{K}<\frac{1}{2}.\end{aligned}$$

Writing $d_i:=\prod_{b\in B_i}p_b$ for each i, we thus see that the d_i are all divisors of $\mathbf{n}$ and their logarithms all lie in an interval of length 1. It follows that $\mathbb{P}(\Delta(\mathbf{n})\geqslant M)=1-o(1)$, as required for Theorem 3. $\square$

Proof of Theorem 6. Fix $0<c<\frac{\beta_k}{1-\beta_k}$, let X be large and set $K=(\log X)^c$. Define i_1,i_2 by (2.2), let $D=i_2$ and define c' by $D^{c'}=i_1$. Let n be a random integer chosen uniformly in $[1,X]$. By assumption,

$$c'\sim\frac{c}{c+1}$$

and therefore $c'\leqslant\beta_k-\delta$ for some $\delta>0$, which depends only on c. By the definition of β_k and Lemma 2.2, it follows that with probability $1-o(1)$, the set $\mathbf{B}$ defined in (2.3) has k distinct subsets $B_1,\dots,B_k$ with equal sums. Thus, with probability $1-o(1)$, there are primes $p_i\in\mathscr{P}_i$

($i \in \mathbf{B}$) such that for any i, j we have

$$\Big|\sum_{b\in B_i}\log p_b - \sum_{b\in B_j}\log p_b\Big| \leqslant \frac{|B_i|+|B_j|}{K} \ll \frac{\log\log X}{(\log X)^c}.$$

Thus, setting $d_i = \prod_{b\in B_i} p_b$, we see that $\max(d_j) \leqslant \min(d_j)\exp O(\frac{\log\log x}{(\log X)^c})$. Since c is arbitrary subject to $c < \beta_k/(1-\beta_k)$, we conclude that $\alpha_k \geqslant \beta_k/(1-\beta_k)$. □

2.4. **Permutations and polynomials over finite fields**

The connection between random logarithmic sets, random permutations and random polynomials is more straightforward, owing to the well-known approximations of these objects by a vector of Poisson random variables.

For each j, let Z_j be a Poisson random variable with parameter $1/j$, and such that $Z_1, Z_2, \dots,$ are independent. Recall the notion of *total variation distance* $d_{\mathrm{TV}}(X,Y)$ between two discrete real random vectors X, Y defined on the same probability space:

$$d_{\mathrm{TV}}(X,Y) = \max_A |\mathbb{P}(X\in A) - \mathbb{P}(Y\in A)|.$$

We recall the easy inequality

$$d_{\mathrm{TV}}((X_1,\dots,X_k),(Y_1,\dots,Y_k)) \leqslant \sum_{j=1}^k d_{\mathrm{TV}}(X_j,Y_j), \tag{2.7}$$

provided that X_j, Y_j live on the same space for each j, that $X_1,\dots,X_k$ are independent, and $Y_1,\dots,Y_k$ are independent. Also, recall the identity

$$d_{\mathrm{TV}}(X,Y) = \frac{1}{2}\sum_t |\mathbb{P}(X=t) - \mathbb{P}(Y=t)|. \tag{2.8}$$

The next proposition states that, apart from the very longest cycles, the cycle lengths of a random permutation have a joint Poisson distribution.

Lemma 2.3. *For a random permutation $\sigma \in S_n$, let $C_j(\sigma)$ denote the number of cycles in σ of length j. Then for $r = o(n)$ as $n\to\infty$ we have*

$$d_{\mathrm{TV}}\Big((C_1(\sigma),\dots,C_r(\sigma)),(Z_1,\dots,Z_r)\Big) = o(1).$$

Proof. In fact there is a bound $\ll e^{-n/r}$ uniformly in n and r; see [3]. □

The next proposition states a similar phenomenon for the degrees of the irreducible factors of a random polynomial over $\mathbb{F}_q$, except that now one must also exclude the very smallest degrees as well.

Lemma 2.4. *Let q be a prime power. Let f be a random, monic polynomial in $\mathbb{F}_q[t]$ of degree n. Let $Y_d(f)$ denote the number of monic, irreducible factors of f which have degree d. Suppose that $10\log n \leqslant r \leqslant s \leqslant \frac{n}{10\log n}$. Then*

$$d_{\mathrm{TV}}\Big((Y_r(f),\dots,Y_s(f)),(Z_r,\dots,Z_s)\Big) = o(1)$$

as $n\to\infty$.

Proof. For $r \leqslant i \leqslant s$, let $\hat{Z}_i$ be a negative binomial random variable $\mathrm{NB}(\frac{1}{i}\sum_{j|i}\mu(i/j)q^j, q^{-i})$. Corollary 3.3 in [2] implies that

$$d_{\mathrm{TV}}\Big((Y_r(f),\dots,Y_s(f)),(\hat{Z}_r,\dots,\hat{Z}_s)\Big) \ll 1/n. \tag{2.9}$$

Note that $\frac{1}{i}\sum_{j|i}\mu(i/j)q^j = \frac{1}{i}q^i(1+O(q^{-i/2})) = \frac{1}{i}q^i(1+O(1/n))$ since $r \geqslant 10\log n$. A routine if slightly lengthy calculation with (2.8) gives

$$d_{\mathrm{TV}}(Z_i,\hat{Z}_i) \ll 1/n.$$

Combining this with (2.7), we arrive at

$$d_{\mathrm{TV}}((Z_r,\cdots,Z_s),(\hat{Z}_r,\dots,\hat{Z}_s)) \ll s/n = o(1).$$

The conclusion follows from this, (2.9) and the triangle inequality. □

Finally we record a simple lemma quantifying the (minimal) difference between a logarithmic random set $\mathbf{A}$ and a set $\tilde{\mathbf{A}}$ generated in the obvious way by Poisson random variables.

Lemma 2.5. *Define a random set $\tilde{\mathbf{A}} = \{j : Z_j \geqslant 1\}$. Then, uniformly for u, v with $v \geqslant u \geqslant 1$ we have*

$$d_{\mathrm{TV}}(\mathbf{A}\cap(u,v], \tilde{\mathbf{A}}\cap(u,v]) \ll 1/u.$$

Proof. Let W_j be a Bernoulli random variable with $\mathbb{P}(W_j = 1) = 1/j$ and $\mathbb{P}(W_j = 0) = 1 - 1/j$, with $W_1, W_2, \dots$ independent. The desired inequality is immediate from (2.7) and the simple inequality $d_{\mathrm{TV}}(Z_j, W_j) \ll 1/j^2$ which follows from (2.8). □

Proof of Theorem 4. Let $u = \log n$ and $v = n/\log n$. For a random permutation $\sigma \in S_n$, let $\mathbf{C} = \{j : C_j(\sigma) \geqslant 1\}$, and as in Lemma 2.5 define the random set $\tilde{\mathbf{A}} = \{j : Z_j \geqslant 1\}$. By Lemma 2.3, Lemma 2.5, and the triangle inequality, we have

$$\begin{aligned} d_{\mathrm{TV}}(\mathbf{A}\cap(u,v], \mathbf{C}\cap(u,v]) &\leqslant d_{\mathrm{TV}}(\mathbf{A}\cap(u,v], \tilde{\mathbf{A}}\cap(u,v]) + d_{\mathrm{TV}}(\tilde{\mathbf{A}}\cap(u,v], \mathbf{C}\cap(u,v]) \\ &= o(1) \end{aligned}$$

as $n \to \infty$. By Lemma 2.1, with probability $\to 1$ as $n \to \infty$, $\mathbf{A}\cap(u,v]$ has M distinct subsets $A_1,\dots,A_M$ with equal sums, where $M = (\log n)^{\zeta - o(1)}$. Hence, $\mathbf{C}$ has distinct subsets $S_1,\dots,S_M$ with equal sums with probability $\to 1$ as $n \to \infty$. Each subset S_j corresponds to a distinct divisor of σ, the size of the divisor being the sum of elements of S_j. □

Proof of Theorem 5. The proof is essentially the same as that of Theorem 4, except now we take $u = 10\log n$, $v = \frac{n}{10\log n}$, $\mathbf{C} = \{j : Y_j(f) \geqslant 1\}$ and use Lemma 2.4 in place of Lemma 2.3. □

3. Overview of the paper

The purpose of this section is to explain the main ideas that go into the proof of Theorem 2 in broad strokes, as well as to outline the structure of the rest of the paper. The remainder of the paper splits into three parts, and we devote a subsection to each of these. Finally, in subsection 3.4, we make some brief comments about the relationship of our work to previous work of Maier and Tenenbaum [20, 22]. Further comments on this connection are made in Appendix C.

3.1. **Part II: Equal sums and the optimization problem.**

Part II provides a very close link between the key quantity β_k (which is defined in Problem 1.1 and appears in all four of Theorems 2, 3, 4 and 5) and a quantity γ_k, which on the face of it appears to be of a completely different nature, being the solution to a certain optimization problem (Problem 3.7 below) involving the manner in which linear subspaces of $\mathbb{Q}^k$ intersect the cube $\{0,1\}^k$.

At the heart of this connection is a fairly simple way of associating to k disjoint sets $A_1,\dots,A_k \subset A$ a *flag*, where A is a given set of integers (that we typically generate logarithmically).

Definition 3.1 (Flags)**.** Let $k \in \mathbb{N}$. By an r-step *flag* we mean a nested sequence

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

of vector spaces.[2] Here $\mathbf{1} = (1,1,\dots,1) \in \mathbb{Q}^k$. A flag is *complete* if $\dim V_{i+1} = \dim V_i + 1$ for $i = 0,1,\dots,r-1$.

To each choice of distinct sets $A_1,\dots,A_k \subset A$, 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 $A_i = \sqcup_{\omega:\omega_i=1} B_\omega$. We iteratively select vectors $\omega^1,\dots,\omega^r$ to maximize $\prod_{j=1}^r (\max B_{\omega^j})$ subject to the constraint that $\mathbf{1},\omega^1,\dots,\omega^r$ are linearly independent over $\mathbb{Q}$. We then define $V_j = \mathrm{Span}_{\mathbb{Q}}(\mathbf{1},\omega^1,\dots,\omega^j)$ for $j = 0,1,\dots,r$.

The purpose of making this construction is difficult to describe precisely in a short paragraph. However, the basic idea is that the vectors $\omega^1,\dots,\omega^r$ and the flag $\mathscr{V}$ provide a natural frame of reference for studying the equal sums equation

$$\sum_{a\in A_1} a = \cdots = \sum_{a\in A_k} a. \tag{3.1}$$

Suppose now that $A_1,\dots,A_k \subset [D^c, D]$. Then the construction just described naturally leads, in addition to the flag $\mathscr{V}$, to the following further data: thresholds c_j defined by $\max B_{\omega^j} \approx D^{c_j}$, and measures μ_j on $\{0,1\}^k$, which capture the relative sizes of the sets $B_\omega \cap (D^{c_{j+1}}, D^{c_j}]$, $\omega \in \{0,1\}^k$. Full details of these constructions are detailed in Section 4.

The above discussion motivates the following definition, which will be an important one in our paper.

Definition 3.2 (Systems)**.** Let $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ be a triple such that:

(a) $\mathscr{V}$ is an r-step flag whose members V_j are distinct and spanned by elements of $\{0,1\}^k$;
(b) $\mathscr{V}$ is *nondegenerate*, which means that V_r is not contained in any of the subspaces $\{x \in \mathbb{Q}^k : x_i = x_j\}$, $i \neq j$;
(c) $\mathbf{c} = (c_1,\dots,c_r,c_{r+1})$ with $1 \geqslant c_1 \geqslant \cdots \geqslant c_{r+1} \geqslant 0$;
(d) $\boldsymbol{\mu} = (\mu_1,\dots,\mu_r)$ is an r-tuple of probability measures;
(e) $\mathrm{Supp}(\mu_i) \subset V_i \cap \{0,1\}^k$ for all i.

Then we say that $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ is a *system*. We say that a system is complete if its underlying flag is, in the sense of Definition 3.1.

[2] In the literature, the term "flag" means that the inclusions are proper, i.e., $\dim(V_{i+1}) > \dim V_i$ for all i. In this paper, we will use the term more broadly to refer to an arbitrary nested sequence of subspaces.

Remark. The nondegeneracy condition (b) arises naturally from the construction described previously, provided one assumes the sets $A_1, \dots, A_k$ are distinct.

We have sketched how a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ may be associated to any k distinct sets $A_1, \dots, A_k \subset [D^c, D]$. Full details are given in subsection 4.1. There is certainly no canonical way to reverse this and associate sets A_i to a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$. However, given a set $\mathbf{A} \subset [D^c, D]$ (which, in our paper, will be a logarithmic random set) and a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, there is a natural *probabilistic* way to construct subsets $A_1, \dots, A_k \subset \mathbf{A}$ via their Venn diagram $(B_\omega)_{\omega \in \{0,1\}^k}$: if $a \in \mathbf{A} \cap (D^{c_{j+1}}, D^{c_j}]$ then we put a in B_ω with probability $\mu_j(\omega)$, these choices being independent for different as.

This will be indeed be roughly our strategy for constructing, given a logarithmic random set $\mathbf{A} \subset [D^c, D]$, distinct subsets $A_1, \dots, A_k \subset \mathbf{A} \cap [D^c, D]$ satisfying the equal sums condition (3.1). Very broadly speaking, we will enact this plan in two stages, described in Sections 5 and 6 respectively. In Section 5, which is by far the deeper part of the argument, we will show that (almost surely in $\mathbf{A}$) the distribution of tuples $(\sum_{a \in A_i} a)_{i=1}^k$ is dense in a certain box adapted to the flag $\mathscr{V}$, as the A_i range over the random choices just described. Then, in Section 6, we will show that (almost surely) one of these tuples can be "corrected" to give the equal sums condition (3.1). This general mode of argument has its genesis in the paper [20] of Maier and Tenenbaum, but the details here will look very different. In addition to the fact that linear algebra and entropy play no role in Maier and Tenenbaum's work, they use a second moment argument which does not work in our setting. Instead we use an ℓ^p estimate with $p \approx 1$, building on ideas in [18, 19].

In analysing the distribution of tuples $(\sum_{a \in A_i} a)_{i=1}^k$ in Section 5, the notation of entropy comes to the fore.

Definition 3.3 (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

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

Remark. This the (Shannon) entropy of the distribution on cosets $W + x$ induced by ν. Entropy will play a key role in our paper, and basic definitions and properties of it are collected in Appendix B.

More important than the entropy itself will be a certain quantity $\mathrm{e}(\mathscr{V}')$, assigned to *subflags* of $\mathscr{V}$. We give the relevant definitions now.

Definition 3.4 (Subflags)**.** Suppose that

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

is a flag. Then another flag

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

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 $\mathscr{V}$.

Definition 3.5 (e-value)**.** Let $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ be a system, and let $\mathscr{V}' \leqslant \mathscr{V}$ be a subflag. Then we define the *e-value*

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

Remark. Note that

$$\mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) = \sum_{j=1}^{r} c_j \dim(V_j/V_{j-1}), \tag{3.2}$$

since condition (e) of Definition 3.2 implies that $\mathbb{H}_{\mu_j}(V_j) = 0$ for $1 \leqslant j \leqslant r$.

Definition 3.6 (Entropy condition)**.** Let $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ be a system. We say that this system satisfies the *entropy condition* if

$$\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V}) \qquad \text{for all subflags } \mathscr{V}' \text{ of } \mathscr{V}. \tag{3.3}$$

and the *strict entropy condition* if

$$\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V}) \qquad \text{for all proper subflags } \mathscr{V}' \text{ of } \mathscr{V}. \tag{3.4}$$

We cannot give a meaningful discussion of exactly why these definitions are the right ones to make in this overview. Indeed, it took the authors over a year of working on the problem to arrive at them. Let us merely say that

- If a random logarithmic set $\mathbf{A} \cap [D^c, D]$ almost surely admits distinct subsets $A_1, \dots, A_k$ satisfying the equal sums condition (3.1), then some associated system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ satisfies the entropy condition (3.3). For detailed statements and proofs, see Section 4.
- If a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ satisfies the strict entropy condition (3.4) then the details of the construction of sets $A_1, \dots, A_k$ satisfying the equal sums condition, outlined above, can be made to work. For detailed statements and proofs, see Sections 5 and 6.

With the above definitions and discussion in place, we are finally ready to introduce the key optimization problem, the study of which will occupy a large part of our paper.

Problem 3.7 (The optimisation problem)**.** Determine the value of γ_k, defined to be the supremum of all constants c for which there is a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ such that $c_{r+1} = c$ and the entropy condition (3.3) holds.

Similarly, determine $\tilde{\gamma}_k$, defined to be the supremum of all constants c for which there is a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ such that $c_{r+1} = c$ and the strict entropy condition (3.4) holds.

The precise content of the two bullet points above, and the main result of Part II of the paper, is then the following theorem.

Theorem 7. *For every $k \geqslant 2$, we have*

$$\tilde{\gamma}_k \leqslant \beta_k \leqslant \gamma_k.$$

Remark 3.1. (a) Presumably $\gamma_k = \beta_k = \tilde{\gamma}_k$. Indeed, it is natural to think that any system satisfying (3.3) can be perturbed an arbitrarily small amount to satisfy (3.4). However, we have not been able to show that this is possible in general.

(b) In the definition of γ_k, the supremum is attained. This can be established by an easy compactness and continuity argument, the details of which are left to the reader – the crucial point is that there are only finitely many choices of the flag $\mathscr{V}$.

(c) If $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ is an "optimal system", in the sense that $\gamma_k = c_{r+1}$, then it might be the case that some of the thresholds c_j are equal. In this case we can, if desired, remove the "unused" subspaces, measures and c_j's, without changing $\mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$. Thus, there is always a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ that solves the first part of Problem 3.7 and has $1 = c_1 > c_2 > \cdots > c_{r+1}$. We leave the details of this observation, which will not play an explicit role in the paper, to the reader.

3.2. **Part III: The optimization problem**

Part III of the paper is devoted to the study of Problem 3.7 in as much generality as we can manage. Unfortunately we have not yet been able to completely resolve this problem, and indeed numerical experiments suggest that a complete solution, for all k, could be very complicated.

The main achievement of Part III is to provide a solution of sorts when the flag $\mathscr{V}$ is fixed, but one is free to choose $\boldsymbol{\mu}$ and $\mathbf{c}$. Write $\gamma_k(\mathscr{V})$ (or $\tilde{\gamma}_k(\mathscr{V})$) for the solution to this problem.

Our solution applies only to rather special flags $\mathscr{V}$, but this is unsurprising: for "generic" flags $\mathscr{V}$, one would not expect there to be any choice of $\boldsymbol{\mu}$, $\mathbf{c}$ for which $c_{r+1} > 0$, and so $\gamma_k(\mathscr{V}) \leqslant 0$ in these cases. Such flags are of no interest in this paper.

We begin, in Section 7, by solving an even more specific problem in which the entropy condition (3.3) is only required to hold for certain very special subflags $\mathscr{V}'$ of $\mathscr{V}$, which we call *basic flags*. These are flags of the form

$$\mathscr{V}'_{\mathrm{basic}(m)} : \langle \mathbf{1} \rangle = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_{m-1} \leqslant V_m = V_m = \cdots = V_m.$$

We call this the *restricted entropy condition*; to spell it out, this is the condition that

$$e(\mathscr{V}'_{\mathrm{basic}(m)}, \mu, \mathbf{c}) \geqslant e(\mathscr{V}, \mu, \mathbf{c}) \tag{3.5}$$

for $m = 0, 1, \dots, r-1$ (the case $m = r$ being vacuous).

We write $\gamma_k^{\mathrm{res}}(\mathscr{V})$ for the maximum value of c_{r+1} (over all choices of $\mathbf{c}$ and $\boldsymbol{\mu}$ such that $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ is a system) subject to this condition. Clearly

$$\gamma_k^{\mathrm{res}}(\mathscr{V}) \geqslant \gamma_k(\mathscr{V}). \tag{3.6}$$

The main result of Section 7 is Proposition 7.7, which states that under certain conditions we have

$$\gamma_k^{\mathrm{res}}(\mathscr{V}) = \frac{\log 3 - 1}{\log 3 + \sum_{i=1}^{r-1} \frac{\dim(V_{i+1}/V_i)}{\rho_1 \cdots \rho_{r-1}}}, \tag{3.7}$$

for certain parameters $\rho_1, \cdots, \rho_{r-1}$ depending on the flag $\mathscr{V}$.

To define these, one considers the "tree structure" on $\{0,1\}^k \cap V_r$ induced by the flag $\mathscr{V}$: the "cells at level j" are simply intersections with cosets of V_j, and we join a cell C at level j to a "child" cell C' at level $j-1$ iff $C' \subset C$. The ρ_i are then defined by setting up a certain recursively-defined function on this tree and then solving what we term the *ρ-equations*. The details may be found in subsection 7.2. Proposition 7.7 also describes the measures $\boldsymbol{\mu}$ and the parameters $\mathbf{c}$ for which this optimal value is attained.

In Section 8, we relate the restricted optimisation problem to the real one, giving fairly general conditions under which we in fact have equality in (3.6), that is to say $\gamma_k^{\mathrm{res}}(\mathscr{V}) = \gamma_k(\mathscr{V})$. The basic strategy of this section is to show that for the $\mathbf{c}$ and $\boldsymbol{\mu}$ which are optimal for the restricted optimisation problem, the full entropy condition (3.3) is in fact a consequence of the restricted condition (3.5).

The arguments of this section make heavy use of the submodularity inequality for entropy, using this to drive a kind of "symmetrisation" argument. In this way one can show that an arbitrary $\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu})$ is greater than or equal to one in which $\mathscr{V}'$ is *almost* a basic flag; these "semi-basic" flags are then dealt with by hand.

To add an additional layer of complexity, we build a perturbative device into this argument so that our results also apply to $\tilde{\gamma}_k(\mathscr{V})$.

3.3. **Part IV: Binary systems**

The final part of the paper is devoted to a discussion of a particular type of flag $\mathscr{V}$, the *binary flags*, and the associated optimal systems $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, which we call *binary systems*.

Definition 3.8 (Binary flag of order r)**.** 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 an r-step flag $\mathscr{V}$, $\langle \mathbf{1} \rangle = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_r = \mathbb{Q}^{\mathcal{P}[r]}$, as follows: V_i is the subspace of all $(x_S)_{S \subset [r]}$ for which $x_S = x_{S \cap [i]}$ for all $S \subset [r]$.

Whilst the definition is, in hindsight, rather simple and symmetric, it was motivated by extensive numerical experiment. We believe these flags to be asymptotically optimal for Problem 3.7, though we currently lack a proof.

There are two main tasks in Part IV. First, we must verify that the various conditions necessary for the results of Part III hold for the binary flags. This is accomplished in Section 10, the main statements being given in Section 9. At the end of Section 9 we give the proof (and complete statement) of Theorem 2(a), conditional upon the results of Section 10. This is the deepest result in the paper.

Following this we turn to Theorem 2(b). There are two tasks here. First, we prove that the parameters ρ_i for the binary flags (which do not depend on r) tend to a limit ρ. This is not at all straightforward, and is accomplished in Section 11.

After that, in Section 12, we describe this limit in terms of certain recurrence relations, which also provide a useful means of calculating it numerically. Theorem 2(b) is established at the very end of the paper.

Most of Part IV could, if desired, be read independently of the rest of the paper.

3.4. **Relation to previous work**

Previous lower bounds for the a.s. behaviour of the Erdős–Hooley Δ-function are contained in two papers of Maier and Tenenbaum [20, 22]. Both of these bounds can be understood within the framework of our paper.

The main result of [20] follows from the fact that

$$\tilde{\gamma}_2 \geqslant 1 - \frac{1}{\log 3}. \tag{3.8}$$

Indeed by Theorem 7 it then follows that $\beta_2 \geqslant 1 - \frac{1}{\log 3}$, and then from Theorem 3 it follows that for almost every n we have

$$\Delta(n) \gg (\log\log n)^{-\log 2/\log(1-\frac{1}{\log 3})+o(1)}. \tag{3.9}$$

The exponent appearing here is $0.28754048957\dots$ and is exactly the one in [20, Theorem 2].

The bound (3.8) is very easy to establish, and a useful exercise in clarifying the notation we have set up. Take $k = 2$, $r = 1$ and let $\mathscr{V}$ be the flag $\langle \mathbf{1} \rangle = V_0 \leqslant V_1 = \mathbb{Q}^2$. Let $\mathbf{c} = (c_1, c_2)$ with $c_1 = 1$ and

$$c_2 < 1 - \frac{1}{\log 3}. \tag{3.10}$$

Let μ_1 be the measure which assigns weight $\frac{1}{3}$ to the points $\mathbf{0} = (0,0)$, $(0,1)$ and $(1,0)$ in $\{0,1\}^2$ (this being a pullback of the uniform measure on $\{0,1\}^2/V_0$).

There are only two subflags $\mathscr{V}'$ of $\mathscr{V}$, namely $\mathscr{V}$ itself and the basic flag $\mathscr{V}'_{\mathrm{basic}(0)} : \langle \mathbf{1} \rangle = V_0' \leqslant V_1'$ with $V_0' = V_1' = V_0 = \langle \mathbf{1} \rangle$. The entire content of the strict entropy condition (3.4) is therefore that

$$\mathrm{e}(\mathscr{V}'_{\mathrm{basic}(0)}, \mathbf{c}, \boldsymbol{\mu}) > \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}),$$

which translates to

$$(c_1 - c_2)\mathbb{H}_{\mu_1}(V_0) > c_1.$$

We have $\mathbb{H}_{\mu_1}(V_0) = \log 3$ and $c_1 = 1$, and so this translates to precisely condition (3.10).

Remark. (a) With very little more effort (appealing to Lemma B.2) one can show that $\gamma_2 = \beta_2 = \tilde{\gamma}_2 = 1 - \frac{1}{\log 3}$.

(b) This certainly does not provide a shorter proof of Theorem 3.9 than the one Maier and Tenenbaum gave, since our deductions are reliant on the material in Sections 5 and 6, which constitute a significant elaboration of the ideas from [20].

The main result of [22] (Theorem 1.4 there) follows from the lower bound

$$\tilde{\gamma}_{2^r} \geqslant \Big(1 - \frac{1}{\log 3}\Big)\Big(\frac{1 - 1/\log 3}{1 - 1/\log 27}\Big)^{r-1}, \tag{3.11}$$

which of course includes (3.8) as the special case $r = 1$. Applying Theorem 7 and Theorem 3, then letting $r \to \infty$, we recover [22, Theorem 1.4] (quoted as Theorem MT in Section 1), namely the bound

$$\Delta(n) \geqslant (\log\log n)^{\frac{\log 2}{\log \frac{1-1/\log 27}{1-1/\log 3}} - o(1)}$$

for almost all n. The exponent here is $0.33827824168\ldots$.

To explain how (3.11) may be seen within our framework requires a little more setting up. Since it is not directly relevant to our main arguments, we defer this to Appendix C.

PART II. EQUAL SUMS AND THE OPTIMISATION PROBLEM

4. THE UPPER BOUND $\beta_k \leqslant \gamma_k$

In this section we establish the bound in the title. The reader may wish to begin by recalling the definitions of β_k (Problem 1.1) and γ_k (Problem 3.7).

4.1. Venn diagrams and linear algebra

Let $0 < c < 1$ be some fixed quantity, and let D be a real number, large in terms of c. Suppose that $A_1, \dots, A_k \subset [D^c, D]$ are distinct sets. In this section we show that there is a rather natural way to associate a complete system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ (in the sense of Definition 3.2) to these sets. This system encodes the "linear algebra of the Venn diagram of the A_i" in a way that turns out to be extremely useful.

The Venn diagram of the A_i has 2^k cells, indexed by $\{0,1\}^k$ in a natural way. Thus for each $\omega = (\omega_1, \dots, \omega_k) \in \{0,1\}^k$, we define

$$B_\omega := \bigcap_{i\,:\,\omega_i = 1} A_i \bigcap_{i\,:\,\omega_i = 0} (A_i)^c, \tag{4.1}$$

The flag $\mathscr{V}$. Set $\Omega := \{\omega : B_\omega \neq \emptyset\}$. We may put a total order $\prec$ on Ω by writing $\omega' \prec \omega$ if and only if $\max B_{\omega'} < \max B_\omega$. We now select r special vectors $\omega^1, \dots, \omega^r \in \Omega$, with $r \leqslant k-1$, in the following manner. Let $\omega^1 = \max_\prec(\Omega \setminus \{\mathbf{0}, \mathbf{1}\})$. Assuming we have chosen $\omega^1, \dots, \omega^j$ such that $\mathbf{1}, \omega^1, \dots, \omega^j$ are linearly independent over $\mathbb{Q}$, let $\omega^{j+1} = \max(\Omega \setminus \mathrm{Span}(\mathbf{1}, \omega^1, \dots, \omega^j))$, as long as such a vector exists.

Let $\mathbf{1}, \omega^1, \cdots, \omega^r$ be the set of vectors produced when this algorithm terminates. By construction, $\Omega \subset \mathrm{Span}_{\mathbb{Q}}(\mathbf{1}, \omega^1, \dots, \omega^r)$, or in other words $B_\omega = \emptyset$ whenever

$$\omega \in \{0,1\}^k \setminus \mathrm{Span}_{\mathbb{Q}}(\mathbf{1}, \omega^1, \dots, \omega^r).$$

Now define an r-step flag $\mathscr{V} : \langle \mathbf{1} \rangle = V_0 < V_1 < \cdots < V_r$ by setting $V_j := \mathrm{Span}_{\mathbb{Q}}(\mathbf{1}, \omega^1, \cdots, \omega^j)$ for $1 \leqslant j \leqslant r$.

The parameters $\mathbf{c}$. Now we construct the parameters $\mathbf{c} : 1 \geqslant c_1 \geqslant c_2 \geqslant \cdots \geqslant c_{r+1}$. For $j = 1, \dots, r$, we define

$$c_j = 1 + \frac{\lceil \log \max B_{\omega^j} - \log D \rceil}{\log D}. \tag{4.2}$$

Thus

$$\max B_{\omega^j} \in (\frac{1}{e} D^{c_j}, D^{c_j}] \tag{4.3}$$

for $j = 1, \dots, r$. Also set $c_{r+1} = c$. (The presence of the ceiling function $\lceil \cdot \rceil$ does not look very natural. Its purpose is to produce a "coarse" or discretised set of possible thresholds c_i, suitable for use in a union bound later on; see Lemma 4.2 below. The offset of $-\log D$ is to ensure that $c_1 \leqslant 1$.)

The measures $\boldsymbol{\mu}$. Set

$$B'_\omega := \begin{cases} B_\omega \setminus \max B_{\omega^j} & \omega = \omega^j \text{ for some } j \\ B_\omega & \text{otherwise.} \end{cases} \tag{4.4}$$

Define

$$\mu_j(\omega) := \frac{\#\big(B'_\omega \cap (D^{c_{j+1}}, D^{c_j}]\big)}{\sum_\omega \#\big(B'_\omega \cap (D^{c_{j+1}}, D^{c_j}]\big)}, \tag{4.5}$$

with the convention that if the denominator vanishes then $\mu_j(\omega) = 1_{\omega=\mathbf{0}}$.

Remark. It is important that we use the B'_ω here, rather than the B_ω, for technical reasons that will become apparent in the proof of Proposition 4.4 below.

Lemma 4.1. *$(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ is a complete system (in the sense of Definition 3.2).*

Proof. We need to check that $\mathrm{Supp}(\mu_j) \subset V_j$ for $j = 1, \dots, r$. By definition, if $\mu_j(\omega) > 0$ then $B_\omega \cap (D^{c_{j+1}}, D] \neq \emptyset$. This implies that $\max B_\omega > D^{c_{j+1}}$. By (4.3), $D^{c_{j+1}} \geqslant \max B_{\omega^{j+1}}$. Thus $\max B_\omega > \max B_{\omega^{j+1}}$ which, by the construction of the ω^i, means that $\omega \in \mathrm{Span}(\mathbf{1}, \omega^1, \cdots, \omega^j) = V_j$.

We also need to check that $\mathscr{V}$ is nondegenerate, also in the sense of Definition 3.2, that is to say V_r is not contained in any hyperplane $\{\omega \in \mathbb{Q}^k : \omega_i = \omega_j\}$. This follows immediately from the fact that the A_i are distinct. Since

$$A_i \triangle A_j = \bigcup_{\substack{\omega \in \{0,1\}^k \\ \omega_i \neq \omega_j}} B_\omega,$$

and so there is certainly some ω with $\omega_i \neq \omega_j$ and $B_\omega \neq \emptyset$. □

Note that, in addition to the system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, the procedure described above outputs a sequence $\omega^1, \cdots, \omega^r$ of elements of $\{0,1\}^k$. We call the ensemble consisting of the system and the ω^i the *linear data* associated to $A_1, \cdots, A_k$.

Lemma 4.2. *The number of different types of linear data arising from sets $A_1, \cdots, A_k \subset [D^c, D]$ with $|\bigcup_i A_i| \leqslant 10 \log D$ is $\ll (\log D)^{O(1)}$.*

Proof. The number of choices for $\omega^1, \cdots, \omega^r$ is $O(1)$. The thresholds c_j are drawn from a fixed set of size $\log D$, and the numerators and denominators of the $\mu_j(\omega)$ are all integers $\leqslant 10 \log D$. □

Remark 4.1. The $O(1)$ and the $\ll$ here both depend on k. However we regard k as fixed here and do not indicate this dependence explicitly. If one is more careful then one can obtain results that are effective up to about $k \sim \log\log D$.

4.2. **A local-to-global estimate**

Our next step towards establishing the bound $\beta_k \leqslant \gamma_k$ is to pass from the "local" event that a random logarithmic set $\mathbf{A}$ possesses a k-tuple of equal subsums $(\sum_{a \in A_1} a, \dots, \sum_{a \in A_k} a)$ to the "global" distribution of such subsums (with the subtlety that we must mod out by $\mathbf{1}$). The latter is controlled by the set $\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(\mathbf{A})$ defined below.

Definition 4.3. Given a set of integers A and a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, we write $\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A)$ for the set of vectors

$$\sum_{\omega \in \{0,1\}^k} \omega \sum_{a \in B_\omega} a \pmod{\mathbf{1}},$$

where $(B_\omega)_{\omega \in \{0,1\}^k}$ runs over all partitions of A such that

$$\mu_j(\omega) = \frac{\#\big(B_\omega \cap (D^{c_{j+1}}, D^{c_j}]\big)}{\#\big(A \cap (D^{c_{j+1}}, D^{c_j}]\big)} \tag{4.6}$$

for $1 \leqslant j \leqslant r, \omega \in \{0,1\}^k$.

Proposition 4.4. *Fix an integer k and a parameter $0 < c < 1$. Let D be large in terms of c, and let $\mathbf{A} \subset [D^c, D]$ be a logarithmic random set. Let $\mathcal{E}$ be any subset of the event that $|\mathbf{A}| \leqslant 10 \log D$, and*

$$\tilde{\mathcal{E}} = \{A' : \text{ for some } A \in \mathcal{E}, A' \subset A \text{ and } |A'| \geqslant |A| - k\}. \tag{4.7}$$

Then we have

$$\mathbb{P}_{\mathbf{A}}\Big(\exists \text{ distinct } A_1, \dots, A_k \subseteq \mathbf{A} \text{ such that } \sum_{a \in A_1} a = \cdots = \sum_{a \in A_k} a\Big)$$
$$\leqslant (\log D)^{O(1)} \sup_{(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})} D^{-(c_1 + \cdots + c_r)} \mathbb{E}_{\mathbf{A}}\big[1_{\tilde{\mathcal{E}}}(\mathbf{A}) |\mathscr{L}_{\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}}(\mathbf{A})|\big] + \mathbb{P}_{\mathbf{A}}(\mathcal{E}^c).$$

Here, the supremum is over all complete systems $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ with $c_{r+1} = c$.

Proof. Fix linear data $\{(\mathscr{V}, \mathbf{c}, \mu), \omega^1, \dots, \omega^r\}$. Then let $\mathscr{S}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}, (\omega^i))$ be the collection of all sets $A \subset (D^c, D]$ with $|A| \leqslant 10 \log D$ and such that there are distinct subsets $(A_1, \dots, A_k)$ of A satisfying

(a) We have
$$\sum_{a \in A_1} a = \cdots = \sum_{a \in A_k} a; \tag{4.8}$$
(b) The linear data associated to $(A_1, \dots, A_k)$ is $\{(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}), \omega^1, \cdots, \omega^r\}$;

Then the probability we are interested in is bounded above by

$$\mathbb{P}_{\mathbf{A}}(\mathcal{E}^c) + \sum_{\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}, (\omega^i)} \sum_{A \in \mathscr{S}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}, (\omega^i))} \mathbb{P}(\mathbf{A} = A).$$

Abbreviate $\mathscr{S}$ for $\mathscr{S}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$. An elementary probability calculation gives

$$E(\mathscr{S}) := \sum_{A \in \mathscr{S}} \mathbb{P}(\mathbf{A} = A) = \sum_{A \in \mathscr{S}} \prod_{D^c < a \leqslant D} \Big(1 - \frac{1}{a}\Big) \prod_{a \in A} \frac{1}{a - 1}. \tag{4.9}$$

For each A, fix a choice of $(A_1, \dots, A_k)$ satisfying (1), (2) above (if one exists). Let B_ω be the cells of the Venn diagram corresponding to the A_i, as in (4.1), and then define the B'_ω as in (4.4). Recall that (4.5) holds, and define $K_j = \max B_{\omega^j}$ for $1 \leqslant j \leqslant r$. In particular, $K_1 > \cdots > K_r$. Let $A' = A \setminus \{K_1, \dots, K_r\}$. We now invoke (4.8). Note that

$$\sum_{a \in A_i} a = \sum_{\omega \in \{0,1\}^k} \omega_i \sum_{a \in B_\omega} a.$$

Therefore, relation (4.8) is equivalent to

$$\sum_{\omega \in \{0,1\}^k} \omega \sum_{a \in B_\omega} a = (\mathrm{mod}\ \mathbf{1}),$$

and hence

$$\sum_{j=1}^{r} K_j \omega^j = -\sum_{\omega} \omega \sum_{a' \in B'_\omega} a' (\mathrm{mod}\ \mathbf{1}). \tag{4.10}$$

Since $\mathbf{1}, \omega^1, \cdots, \omega^r$ are linearly independent, the value of the right-hand side of (4.10) uniquely determines the numbers K_j, which themselves uniquely determine A in terms of the sets B'_ω.

Moreover by (4.3) we have $K_j > \frac{1}{e} D^{c_j}$ for every j, and therefore

$$\prod_{a\in A} \frac{1}{a-1} \ll D^{-(c_1+\cdots+c_r)} \prod_{a\in A'} \frac{1}{a-1}.$$

Now $A' \in \tilde{\mathcal{E}}$, since $A \in \mathcal{E}$. For any $A' \in \tilde{\mathcal{E}}$ and vector x, if the right side of (4.8) is $-x$, then the numbers K_j are uniquely determines and hence so is the set $A = A' \cup \{K_1, \dots, K_r\}$. Hence, given A', the number of possible sets A which induce A' is at most the number possibilities for the right side of (4.8), which by Definition (4.3) equals $|\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A')|$. We sum over A', and reinterpret the product on the right side of (4.9) in terms of $\mathbb{P}_{\mathbf{A}}(\mathbf{A} = A')$. This gives

$$\begin{aligned} E(\mathscr{S}) &\ll D^{-(c_1+\cdots+c_r)} \sum_{A'\in\tilde{\mathcal{E}}} |\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A')| \prod_{D^c<a\leqslant D} \Big(1-\frac{1}{a}\Big) \prod_{a\in A'} \frac{1}{a-1} \\ &= D^{-(c_1+\cdots+c_r)} \sum_{A'\in\tilde{\mathcal{E}}} |\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A')| \cdot \mathbb{P}_{\mathbf{A}}(\mathbf{A} = A') \\ &= D^{-(c_1+\cdots+c_r)} \mathbb{E}_{\mathbf{A}} \big[1_{\tilde{\mathcal{E}}}(\mathbf{A}) \cdot |\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(\mathbf{A})|\big]. \end{aligned}$$

By Lemma 4.2 there are $(\log D)^{O(1)}$ possible choices for the data $\{(\mathscr{V}, \mathbf{c}, \mu), \omega^1, \dots, \omega^r\}$, and the proof is complete. □

4.3. **Upper bounds in terms of entropies**

Having established Proposition 4.4, we turn to the study of the sets $\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A)$. We will bound their cardinality in terms of the quantities

$$\mathrm{e}(\mathscr{V}') = \mathrm{e}(\mathscr{V}', \mathbf{c}, \mu) = \sum_{j=1}^{r} (c_j - c_{j+1}) \mathbb{H}_{\mu_j}(V_j') + \sum_{j=1}^{r} \dim(V_j'/V_{j-1}') c_j, \tag{4.11}$$

with $\mathscr{V}'$ a subflag of $\mathscr{V}$.

Lemma 4.5. *Let $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ be a system and let $A \subset [D^c, D]$ satisfy the condition*

$$\big|\#(A \cap (D^\alpha, D^\beta]) - (\beta-\alpha)\log D\big| \leqslant 2\log^{3/4} D \tag{4.12}$$

whenever $c \leqslant \alpha \leqslant \beta \leqslant 1$. Then, for any subflag $\mathscr{V}'$ of $\mathscr{V}$,

$$|\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A)| \ll_{\mathscr{V}'} e^{O(\log^{3/4} D)} D^{\mathrm{e}(\mathscr{V}',\mathbf{c},\mu)}. \tag{4.13}$$

Remark. The condition (4.12) will be satisfied for a random logarithmic set $\mathbf{A}$ with very high probability, as we shall see later. The implied constant in the $\ll_{\mathscr{V}'}$ could be made explicit if desired (in terms of the quantitative rationality of a basis for the spaces in $\mathscr{V}'$) but we have no need to do this.

Proof of Lemma 4.5. Given a set $X \subset [D^c, D]$, write $X^{(j)} := X \cap (D^{c_{j+1}}, D^{c_j}]$ for $j = 1, \dots, r$. Throughout the proof, we will assume that A is a set of integers and that $(B_\omega)_{\omega\in\{0,1\}^k}$ runs over all partitions of A such that (4.6) is satisfied. In our new notation, this may be rewritten as

$$|A^{(j)}| = \mu_j(\omega)|B_\omega^{(j)}|, \quad j = 1, \dots, r, \ \ \omega \in \{0,1\}^k. \tag{4.14}$$

Recall that we are given a subflag $\mathscr{V}'$. For each j, $1 \leqslant j \leqslant r$, fix a linear projection $P_j : V_j \to V_j'$, and set $Q_j := \mathrm{id}_{V_j} - P_j$. Set

$$\mathscr{L}^P(A) := \Big\{ \sum_{j=1}^{r} \sum_{\substack{\omega \in \{0,1\}^k \\ \omega \in V_j}} P_j(\omega) \sum_{a \in B_\omega^{(j)}} a \pmod{\mathbf{1}} : (4.14) \text{ is satisfied} \Big\}$$

and

$$\mathscr{L}^Q(A) := \Big\{ \sum_{j=1}^{r} \sum_{\substack{\omega \in \{0,1\}^k \\ \omega \in V_j}} Q_j(\omega) \sum_{a \in B_\omega^{(j)}} a \pmod{\mathbf{1}} : (4.14) \text{ is satisfied} \Big\}.$$

Since

$$\sum_{\omega \in \{0,1\}^k} \omega \sum_{a \in B_\omega} a = \sum_{j=1}^{r} \sum_{\substack{\omega \in \{0,1\}^k \\ \omega \in V_j}} P_j(\omega) \sum_{a \in B_\omega^{(j)}} a + \sum_{j=1}^{r} \sum_{\substack{\omega \in \{0,1\}^k \\ \omega \in V_j}} Q_j(\omega) \sum_{a \in B_\omega^{(j)}} a,$$

it follows immediately from the definition of $\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A)$ (Definition 4.3) that

$$|\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A)| \leqslant |\mathscr{L}^P(A)| \cdot |\mathscr{L}^Q(A)|, \tag{4.15}$$

We claim that

$$|\mathscr{L}^P(A)| \ll_{\mathscr{V}'} (\log D)^r D^{\sum_{j=1}^r c_j \dim(V_j'/V_{j-1}')} \tag{4.16}$$

and that

$$|\mathscr{L}^Q(A)| \leqslant e^{O(\log^{3/4} D)} D^{\sum_{j=1}^r (c_j - c_{j+1}) \mathbb{H}_{\mu_j}(V_j')}. \tag{4.17}$$

These bounds, substituted into (4.15), immediately imply Lemma 4.5.

It remains to establish (4.16) and (4.17), which are proven in quite different ways. We begin with (4.17), which is a "combinatorial" bound, in that there cannot be too many choices for the data making up the sums in $\mathscr{L}^Q(A)$. For this, observe that Q_j vanishes on V_j' and hence is constant on cosets of V_j'. Therefore the elements of $\mathscr{L}^Q(A)$ are determined by the sets $\bigcup_{\omega \in v_j + V_j'} B_\omega^{(j)}$, over all $v_j \in V_j/V_j'$ and $1 \leqslant j \leqslant r$. By (4.14),

$$\Big| \bigcup_{\omega \in v_j + V_j'} B_\omega^{(j)} \Big| = \mu_j(v_j + V_j') |A^{(j)}|,$$

and by Lemma B.1 the number of ways of partitioning $A^{(j)}$ into sets of these sizes is bounded above by $e^{\mathbb{H}(\mathbf{p}^{(j)})|A^{(j)}|}$, where $\mathbf{p}^{(j)} = (\mu_j(v_j + V_j'))_{v_j \in V_j/V_j'}$. By Definition 3.3, $\mathbb{H}(\mathbf{p}^{(j)}) = \mathbb{H}_{\mu_j}(V_j')$. Taking the product over $j = 1, \dots, r$ gives

$$|\mathscr{L}^Q(A)| \leqslant e^{\sum_{j=1}^r \mathbb{H}_{\mu_j}(V_j')|A^{(j)}|}.$$

From the assumption (4.12) we have

$$|A^{(j)}| = (c_j - c_{j+1}) \log D + O(\log^{3/4} D).$$

Using this, and the trivial bound $\mathbb{H}_{\mu_j}(V_j') \leqslant \log |\operatorname{Supp}(\mu_j)| \leqslant \log(2^k)$, (4.17) follows.

Now we prove (4.16), which is a "metric" bound, the point being that none of the sums in $\mathscr{L}^P(A)$ can be too large in an appropriate sense. Pick a basis for $\mathbb{Q}^k$ adapted to $\mathscr{V}'$: that is, a basis $e_1, \dots, e_k$ such that $V_j' = \operatorname{Span}_{\mathbb{Q}}(e_1, \dots, e_{\dim V_j'})$ for each j, and $e_1 = \mathbf{1}$. There are positive

integers $M, N = O_{\mathscr{V}',\mathscr{V}}(1)$ such that, in this basis, the e_i-coordinates of $P_j(\omega)$ are all rationals with denominator M and absolute value at most N.

Now for fixed j and ω, if D is large then

$$\sum_{a\in B_\omega^{(j)}} a \leqslant D^{c_j}\log D,$$

since $B_\omega^{(j)} \subset (D^{c_{j+1}}, D^{c_j}]$ and by the assumption (4.12). Thus

$$\sum_{\substack{\omega\in\{0,1\}^k\\ \omega\in V_j}} P_j(\omega) \sum_{a\in B_\omega^{(j)}} a \in \Big\{ \sum_{1\leqslant i\leqslant \dim(V_j')} x_i e_i \in \mathbb{Q}^k : Mx_i\in\mathbb{Z},\ |x_i|\leqslant rND^{c_j}\log D\ \forall i\Big\},$$

and so

$$\sum_{j=1}^r \sum_{\substack{\omega\in\{0,1\}^k\\ \omega\in V_j}} P_j(\omega) \sum_{a\in B_\omega^{(j)}} a \in \Big\{ \sum_{1\leqslant i\leqslant k} x_i e_i \in \mathbb{Q}^k :\ \begin{array}{l} Mx_i\in\mathbb{Z} \text{ and } |x_i|\leqslant r^2ND^{c_j}\log D\\ \text{for } \dim V_{j-1}' < i \leqslant \dim V_j' \text{ and } 1\leqslant j\leqslant r\end{array}\Big\}.$$

We are interested in the number of different values that the expression $\sum_{i=1}^k x_i e_i$ can take mod $\mathbf{1}$ when the coefficients $x_1,\dots,x_k$ are as above. Since $e_1 = \mathbf{1}$, we only need to know the reduction of x_1 mod 1. Using the restriction $Mx_1\in\mathbb{Z}$, we find that there are M possibilities for x_1 mod 1. In addition, there are

$$\ll (\log D)^r D^{\sum_{j=1}^r c_j \dim(V_j'/V_{j-1}')}$$

possibilities for $x_2,\dots,x_k$, thereby concluding the proof of (4.16) and hence of Lemma 4.5. □

Corollary 4.6. *Let $(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$ be a system and suppose that $A\subset[D^c,D]$ satisfies (4.12). Then*

$$|\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(A)| \ll e^{O(\log^{3/4} D)} \min_{\mathscr{V}'\leqslant\mathscr{V}} D^{\mathrm{e}(\mathscr{V}',\mathbf{c},\mu)}.$$

Proof. At first sight this is a trivial consequence of Lemma 4.5, but this is not quite so on account of the $\mathscr{V}'$-dependence in the implied constant in (4.13). However, while there are infinitely many choices for $\mathscr{V}'$, we can say that two subflags $\mathscr{V}',\mathscr{V}''$ are *equivalent* if V_j', V_j'' have the same intersection with $\{0,1\}^k$ and $\dim V_j' = \dim V_j''$, for all $j=1,\dots,r$. There are clearly only $O_k(1)$ equivalence classes, and so we may pick a complete set of representatives for them such that the implied constants $\ll_{\mathscr{V}'}$ in Lemma 4.5 are uniformly bounded (as a function of k, which could be made explicit if truly desired). Since $\mathrm{e}(\mathscr{V}',\mathbf{c},\boldsymbol{\mu}) = \mathrm{e}(\mathscr{V}'',\mathbf{c},\boldsymbol{\mu})$ when $\mathscr{V}'$ and $\mathscr{V}''$ are equivalent, the corollary follows (and the minimum really *is* a minimum and not just an inf). □

4.4. **The upper bound in Theorem 7**

We can now establish the upper bound in Theorem 7, that is to say the inequality $\beta_k\leqslant\gamma_k$.

We start by applying Proposition 4.4, taking $\mathcal{E}$ to be the event that

$$\big|\#(\mathbf{A}\cap(D^\alpha,D^\beta]) - (\beta-\alpha)\log D\big| \leqslant \log^{3/4} D \tag{4.18}$$

whenever $c\leqslant\alpha\leqslant\beta\leqslant 1$. Then, by Lemma A.5, we have

$$\mathbb{P}_{\mathbf{A}}(\mathcal{E}^c) \ll e^{-\frac14\log^{1/2} D}.$$

It follows that

$$\mathbb{P}_{\mathbf{A}}\Big(\exists \text{ distinct } A_1,\dots,A_k \subseteq \mathbf{A}\cap(D^c,D] \text{ such that } \sum_{a\in A_1} a = \dots = \sum_{a\in A_k} a\Big)$$
$$\leqslant (\log D)^{O(1)} \sup_{(\mathscr{V},\mathbf{c},\boldsymbol{\mu})} D^{-\mathrm{e}(\mathscr{V},\mathbf{c},\boldsymbol{\mu})}\mathbb{E}_{\mathbf{A}} 1_{\tilde{\mathcal{E}}}(\mathbf{A})|\mathscr{L}_{\mathscr{V},\mathbf{c},\boldsymbol{\mu}}(\mathbf{A})| + O(e^{-\frac{1}{4}\log^{1/2} D}).$$

Here, the sup is over complete systems $(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$ with $c_{r+1}=c$, and we made the observation that for such systems we have

$$\mathrm{e}(\mathscr{V},\mathbf{c},\boldsymbol{\mu}) = c_1+\dots+c_r,$$

an immediate consequence of (4.11) and the fact that $\mathbb{H}_{\mu_j}(V_j)=0$ for all j and that $\dim V_j = j+1$.

Note also that $\tilde{\mathcal{E}}$ (as defined at (4.7)) is contained in the event

$$\mathcal{E}_*: \quad \big|\#(\mathbf{A}\cap(D^\alpha,D^\beta]) - (\beta-\alpha)\log D\big| \leqslant 2\log^{3/4} D \qquad \text{whenever} \quad c\leqslant\alpha\leqslant\beta\leqslant 1.$$

Thus we may apply Corollary 4.6 (with $u_1=\dots=u_k=0$), concluding that

$$\mathbb{P}_{\mathbf{A}}\Big(\exists \text{ distinct } A_1,\dots,A_k \subseteq \mathbf{A}\cap(D^c,D] \text{ such that } \sum_{a\in A_1} a = \dots = \sum_{a\in A_k} a\Big)$$
$$\leqslant (\log D)^{O(1)} e^{O(\log^{3/4} D)} \sup_{(\mathscr{V},\mathbf{c},\boldsymbol{\mu})} \min_{\mathscr{V}'\leqslant\mathscr{V}} D^{\mathrm{e}(\mathscr{V}',\mathbf{c},\boldsymbol{\mu})-\mathrm{e}(\mathscr{V},\mathbf{c},\boldsymbol{\mu})} + O(e^{-\frac{1}{4}\log^{1/2} D}). \tag{4.19}$$

Here the sup is over all complete systems $(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$ with $c_{r+1}=c$, and the minimum is over all subflags $\mathscr{V}'\leqslant\mathscr{V}$.

Fix some $c<\beta_k$. If D is large enough, by the definition of β_k (cf. Definition 1.1) we must have

$$\mathbb{P}_{\mathbf{A}}\Big(\exists \text{ distinct } A_1,\dots,A_k \subseteq \mathbf{A}\cap(D^c,D] \text{ such that } \sum_{a\in A_1} a = \dots = \sum_{a\in A_k} a\Big) \geqslant \frac{1}{2}.$$

Comparing with (4.19), and taking D arbitrarily large, we have

$$\sup_{(\mathscr{V},\mathbf{c},\boldsymbol{\mu}):\, c_{r+1}=c} \min_{\mathscr{V}'\leqslant\mathscr{V}} \big(\mathrm{e}(\mathscr{V}',\mathbf{c},\boldsymbol{\mu}) - \mathrm{e}(\mathscr{V},\mathbf{c},\boldsymbol{\mu})\big) \geqslant 0. \tag{4.20}$$

Now the space of systems $(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$ is compact, since there are only $O_k(1)$ choices for $\mathscr{V}$ (the spaces V_j are spanned by elements of $\{0,1\}^k$) and the $\mathbf{c}$, $\boldsymbol{\mu}$ range over compact subsets of Euclidean space. Moreover, the functional

$$(\mathscr{V},\mathbf{c},\boldsymbol{\mu}) \mapsto \min_{\mathscr{V}'\leqslant\mathscr{V}} \big(\mathrm{e}(\mathscr{V}',\mathbf{c},\boldsymbol{\mu}) - \mathrm{e}(\mathscr{V},\mathbf{c},\boldsymbol{\mu})\big)$$

is continuous, noting here that the min is effectively over $O_k(1)$ different subflags $\mathscr{V}'$ by the proof of Corollary 4.6.

It follows that the supremum in (4.20) is realised for some system $(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$ with $c_{r+1}=c$, and so for this system

$$\mathrm{e}(\mathscr{V}',\mathbf{c},\boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$$

for all $\mathscr{V}'\leqslant\mathscr{V}$. Consequently (recalling the definition of γ_k in Problem 3.7) $c\leqslant\gamma_k$. Since $c<\beta_k$ was arbitrary, it follows immediately that $\beta_k\leqslant\gamma_k$.

Remark. An examination of the proof makes it clear that in fact $(\mathscr{V},\mathbf{c},\boldsymbol{\mu})$ is a *complete* system. However, for other aspects of our problem it is not natural to focus on the completeness condition, for which reason we omit it from the definition of β_k.

5. THE LOWER BOUND $\beta_k \geqslant \tilde{\gamma}_k$

5.1. Introduction and simple reductions

The aim of this section and the next is to establish the lower bound $\beta_k \geqslant \tilde{\gamma}_k$. We begin, in Lemma 5.2 below, by showing that we may restrict our attention to certain systems satisfying some additional regularity conditions.

We isolate a "folklore" lemma from the proof for which it is not easy to find a good reference. The authors thank Carla Groenland for a helpful conversation on this topic.

Lemma 5.1. *Let V be a subspace of $\mathbb{Q}^k$. Then $\#(V \cap \{0,1\}^k) \leqslant 2^{\dim V}$.*

Proof. We outline two quite different short proofs. Let $d := \dim V$.

Proof 1. We claim that there is a projection from $\mathbb{Q}^k$ onto some set of d coordinates which is injective on V. From this, the result is obvious, since the image of $\{0,1\}^k$ under any such projection has size 2^d. To prove the claim, let $e_1, \dots, e_n$ denote the standard basis on $\mathbb{Q}^n$. Note that if $W \leqslant \mathbb{Q}^n$ and if none of the quotient maps $\mathbb{Q}^n \mapsto \mathbb{Q}^n/\langle e_i \rangle$ is injective on W, then W must contain a multiple of each e_i, and therefore $W = \mathbb{Q}^n$. Thus if W is a proper subspace of $\mathbb{Q}^n$ then there is a projection onto some set of $(n-1)$ coordinates which is injective on W. Repeated use of this fact establishes the claim.

Proof 2. Suppose that $\#(V \cap \{0,1\}^k)$ contains $2^d + 1$ points. These are all distinct under the natural ring homomorphism $\pi : \mathbb{Z}^k \to \mathbb{F}_2^k$, and so their images cannot lie in a subspace (over $\mathbb{F}_2$) of dimension d. Hence there are $v_1, \dots, v_{d+1} \in V$ such that $\pi(v_1), \dots, \pi(v_{d+1})$, are linearly independent over $\mathbb{F}_2$. The $(d+1) \times k$ matrix formed by these $\pi(v_i)$ therefore has a $(d+1) \times (d+1)$-subminor which is nonzero in $\mathbb{F}_2$. The corresponding subminor of the matrix formed by the v_i is therefore an odd integer, and in particular not zero. This means that $v_1, \dots, v_{d+1}$ are linearly independent over $\mathbb{Q}$, contrary to the assumption that $\dim(V) = d$. □

Lemma 5.2. *The number $\tilde{\gamma}_k$ is the supremum of all c for which there is a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ such that:*

(a) $\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) > \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ *for every proper subflag $\mathscr{V}' < \mathscr{V}$;*
(b) $1 = c_1 > c_2 > \cdots > c_{r+1} = c$*;*
(c) *For $j = 1, \dots, r$, $\bigcup_{i=1}^{j} \mathrm{Supp}(\mu_i)$ spans V_j ;*
(d) $\dim(V_1/V_0) = 1$*;*
(e) *For all j and ω, $\mu_j(\omega) = \mu_j(\mathbf{1} - \omega)$.*

Proof. Recall that, by definition (Problem 3.7), $\tilde{\gamma}_k$ is the supremum of all c for which there is a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ such that just (a) is satisfied. Given such a system, we must show that there is another system which is equally good (i.e. with the same value of $c = c_{r+1}$) which additionally satisfies (b), (c), and (d) and (e). To do this, we introduce the following auxillary condition:

$$c_j > c_{j+1} \qquad \text{and} \qquad \mathbb{H}_{\mu_j}(V_{j-1}) > \dim(V_j/V_{j-1}) \quad \text{for } j = 1, \dots, r. \tag{5.1}$$

We then prove the following claims, in order.

Claim 1. Any system satisfying (a) also satisfies (5.1);

Claim 2. Any system satisfying (a) also satisfies (d);

Claim 3. Any system satisfying (a) also satisfies (c);

Claim 4. Given a system satisfying (a), there is an equally good system satisfying both (a) and (b);

Claim 5. Given a system satisfying (a) and (b), there is an equally good system satisfying (a), (b) and (d).

These five claims together give Lemma 5.2. Indeed, apply Claims 4 and 5 to get an equally good system satisfying (a), (b) and (d), and then apply Claims 2 and 3 to conclude that this system also satisfies (c) and (e).

Proof of Claim 1. Consider the inequality in (a) with the choice of subflag $\mathscr{V}' : \langle \mathbf{1} \rangle = V_0' \leqslant V_1' \leqslant \cdots \leqslant V_r'$, where $V_i' = V_i$ for $i \neq j$, and $V_j' = V_{j-1}$; that is, $\mathscr{V}'$ has two consecutive copies of V_{j-1}. Then

$$\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) - \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) = (c_j - c_{j+1})\big(\mathbb{H}_{\mu_j}(V_{j-1}) - \dim(V_j/V_{j-1})\big) > 0.$$

Since $c_j \geqslant c_{j+1}$, (5.1) follows immediately.

Proof of Claim 2. By Claim 1, (a) implies (5.1), and so in particular

$$\mathbb{H}_{\mu_1}(V_0) > \dim(V_1/V_0) =: d. \tag{5.2}$$

On the other hand, by Lemma 5.1 we have $|V_1 \cap \{0,1\}^k| \leqslant 2^{\dim V_1} = 2^{d+1}$ and hence μ_1 is supported on at most $2^{d+1} - 1$ cosets of V_0 (since $\mathbf{1} \in V_0$, the points $\mathbf{0}$ and $\mathbf{1}$ lie in the same coset). In particular, by Lemma B.2, $\mathbb{H}_{\mu_1}(V_0) \leqslant \log(2^{d+1} - 1)$. Comparing with (5.2) gives

$$d < \log(2^{d+1} - 1),$$

which immediately implies that $d = 1$, which is exactly statement (e).

Proof of Claim 3. By Claims 1 and 2, (e) and (5.1) both hold.. Condition (e) implies that for any subflag $\mathscr{V}'$ of $\mathscr{V}$, $V_1' \in \{V_0, V_1\}$. Hence, we have two possibilities for the coefficient of c_1 in the expression $\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) - \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$: if $V_1' = V_1$, then it is zero, whereas if $V_1' = V_0$ it equals $\mathbb{H}_{\mu_1}(V_0) - \dim(V_1/V_0)$, which is positive by (5.1). We conclude that the system $(\mathscr{V}, \tilde{\mathbf{c}}, \boldsymbol{\mu})$, where $\tilde{c}_1 = 1$ and $\tilde{c}_j = c_j$ for $j > 1$, still satisfies (a). It also satisfies (b) by construction and by the second clause of (5.1).

Proof of Claim 4. Suppose that (a) holds. By Claim 1, we also have (5.1). Consider the flag $\mathscr{V}' : \langle \mathbf{1} \rangle \leqslant V_1' \leqslant \cdots \leqslant V_r'$, where

$$V_j' = \mathrm{Span}\left(\bigcup_{i=1}^{j} \mathrm{Supp}(\mu_j)\right) \qquad (1 \leqslant j \leqslant r).$$

It is easy to see from the definition of a system (Definition 3.2) that $\mathscr{V}'$ is a subflag of $\mathscr{V}$. Suppose that (c) fails: then $\mathscr{V}'$ is a proper subflag of $\mathscr{V}$. We have $\mathbb{H}_{\mu_j}(V_j') = 0$ for all j, and hence

$$\begin{aligned}
\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) &= \sum_{i=1}^{r} c_i \dim(V_i'/V_{i-1}') \\
&= -c_1 + c_r \dim(V_r') + \sum_{i=1}^{r-1} (c_i - c_{i+1}) \dim(V_i') \\
&< -c_1 + c_r \dim(V_r) + \sum_{i=1}^{r-1} (c_i - c_{i+1}) \dim(V_i) = \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}),
\end{aligned}$$

where in the strict inequality we used the first clause of (5.1) and the fact that $\mathscr{V}' \neq \mathscr{V}$. This contradicts (a), and so our assumption that (c) fails was wrong.

Proof of Claim 5. Assume that the system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ satisfies (a) and (b). For every j and $\omega \in V_j$, we define

$$\tilde{\mu}_j(\omega) = \frac{\mu_j(\omega) + \mu_j(\mathbf{1} - \omega)}{2}.$$

We then consider the system $(\mathscr{V}, \mathbf{c}, \tilde{\boldsymbol{\mu}})$, which clearly satisfies (b) and (d). We show that it also satisfies (a). For this, it is enough to show that

$$\mathbb{H}_{\tilde{\mu}_j}(V_j') \geqslant \mathbb{H}_{\mu_j}(V_j') \tag{5.3}$$

for all j. Indeed, we then have

$$\mathrm{e}(\mathscr{V}', \mathbf{c}, \tilde{\boldsymbol{\mu}}) \geqslant \mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) = \mathrm{e}(\mathscr{V}, \mathbf{c}, \tilde{\boldsymbol{\mu}}).$$

To prove (5.3), write

$$\mathbb{H}_{\mu_j}(V_j') = \sum_C L(\mu_j(C)), \quad \mathbb{H}_{\tilde{\mu}_j}(V_j') = \sum_C L(\tilde{\mu}_j(C)),$$

where the sum is over all cosets C of V_j' and $L(t) = -t \log t$. Thus, since $-C$ runs over all cosets as C does,

$$\mathbb{H}_{\mu_j}(V_j') = \frac{1}{2} \sum_C \big[L(\mu_j(C)) + L(\mu_j(-C))\big] \tag{5.4}$$

and

$$\mathbb{H}_{\tilde{\mu}_j}(V_j') = \frac{1}{2} \sum_C \big[L(\tilde{\mu}_j(C)) + L(\tilde{\mu}_j(-C))\big]. \tag{5.5}$$

However, by definition we have

$$\tilde{\mu}_j(C) = \tilde{\mu}_j(-C) = \frac{1}{2}(\mu_j(C) + \mu_j(-C)).$$

Therefore the claim (5.3) follows from (5.4), (5.5) and the concavity of L. □

In view of Lemma 5.2, the lower bound $\beta_k \geqslant \tilde{\gamma}_k$ follows from the following proposition. As usual, $\mathbf{A}$ is a logarithmic random set.

Proposition 5.3. *Let $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ be a system with $c_{r+1} = c$ and which satisfies the entropy condition*

$$\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) + \varepsilon \tag{5.6}$$

for all subflags $\mathscr{V}'$ of $\mathscr{V}$ with $\mathscr{V}' \neq \mathscr{V}$, and also satisfies conditions (b)-(d) of Lemma 5.2. Then, a.s. as $D \to \infty$, there are distinct $A_1, \dots, A_k \subset \mathbf{A} \cap [D^c, D]$ with

$$\sum_{a \in A_1} a = \cdots = \sum_{a \in A_k} a. \tag{5.7}$$

Remark. The strict condition (5.6) automatically implies the uniform condition $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon$, for some $\varepsilon > 0$. Indeed, in view of Remark 3.1 (b), the quantity $\mathrm{e}(\mathscr{V}')$ admits finitely many values.

Unlike the situation in Section 4, the system is first fixed and then we let $D \to \infty$. That is, the flag $\mathscr{V}$, constants c_j and measures μ_j do not vary with D.

The proof of Proposition 5.3 is perhaps the most difficult part of this paper, and will occupy this and the next section.

The main result, which we will prove in this section and the next, is Proposition 5.5 below.

Definition 5.4 (Nondegenerate maps)**.** Let X be any set. Then a map $\psi : X \to \{0,1\}^k$ is said to be *nondegenerate* if the image of ψ is not contained in any of the subspaces $\{x \in \mathbb{Q}^k : x_i = x_j\}$.

The map ψ is a "Venn diagram selection function", that is, the value of $\psi(b)$ specifies which piece of the Venn diagram of k subsets $X_1, \dots, X_k$ of X that b belongs to. In the notation (4.5) of the previous section, $\psi(a) = \omega$ means that $a \in B_\omega$. The condition that ψ is nondegenerate is equivalent to $X_1, \dots, X_k$ being distinct, and is similar to the property of a flag $\mathscr{V}$ being nondegenerate.

Proposition 5.5. *Let $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ be a system with $c_{r+1} = c$, and let $\delta > 0$. Suppose that the entropy gap condition (5.6) holds, and conditions (b), (c) in Lemma 5.2 hold. Then, if D is sufficiently large in terms of δ, ε and the system, with probability at least $1 - \delta$ there is a nondegenerate map $\psi : \mathbf{A} \cap (D^c, D] \to \{0,1\}^k$ such that $\sum_{a \in \mathbf{A}} a\psi(a) \in \langle \mathbf{1} \rangle$.*

The map ψ will be constructed using the data from the system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$. Before we embark on the proof of this result, we show to deduce Proposition 5.3 from it.

Proof of Proposition 5.3, assuming Proposition 5.5. By Proposition 5.5, we know that with probability $1 - o_{D\to\infty}(1)$ there is nondegenerate map $\psi : \mathbf{A} \cap (D^c, D] \to \{0,1\}^k$ such that $\sum_{a\in\mathbf{A}} a\psi(a)$ lies in $\langle \mathbf{1} \rangle$, that is to say, it is a constant vector. We will show that this map induces k distinct subsets of $\mathbf{A}$ satisfying (5.7).

Let $\psi_i : \mathbf{A} \cap (D^c, D] \to \mathbb{Q}$, $i = 1, \dots, k$, denote the projection of ψ onto the i-th coordinate of $\mathbb{Q}^k$, so that $\psi = (\psi_1, \dots, \psi_k)$. Define $A_i := \{a \in \mathbf{A} : \psi_i(a) = 1\}$. These sets are distinct because if $A_i = A_j$, then the image of ψ would take values in the hyperplane $\{\mathbf{x} \in \mathbb{Q}^k : x_i = x_j\}$, contrary to the fact that ψ is nondegenerate. Moreover, for all i, j we have

$$\sum_{a\in A_i} a - \sum_{a\in A_j} a = \sum_{a\in\mathbf{A}} a\psi_i(a) - \sum_{a\in\mathbf{A}} a\psi_j(a) = 0,$$

and so (5.7) does indeed hold. □

5.2. Many values of $\sum_{a\in\mathbf{A}} a\psi(a)$, and a moment bound

We turn now to the task of proving Proposition 5.5. We will fix the system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ throughout. We will divide the proof of Proposition 5.5 into two parts. The first and more difficult part, which we prove in this section, states that (with high probability) $\sum_{a\in\mathbf{A}} a\psi(a)$ takes many different values modulo $\langle \mathbf{1} \rangle$ as ψ ranges over all nondegenerate maps $\psi : \mathbf{A} \cap (D^c, D] \to \{0,1\}^k$. The precise statement is Proposition 5.7 below. The deduction of Proposition 5.5 from Proposition 5.7 will occupy Section 6.

Let $\kappa > 0$ be a small quantity, which may depend on D. Let

$$\mathbf{A}^j = \{a \in \mathbf{A} : D^{c_{j+1}+\kappa} < a \leqslant D^{c_j}/e\} \qquad (1 \leqslant j \leqslant r), \quad \mathbf{A}' := \bigcup_{j=1}^{r} \mathbf{A}^j. \tag{5.8}$$

The purpose of working with $\mathbf{A}'$ rather than $\mathbf{A}$ is to ensure that some gaps are left for the subsequent argument in the next section (based on ideas of Maier and Tenenbaum [20]), in which we show that one of the many sums $\sum_{a\in\mathbf{A}'} a\psi(a)$ guaranteed by Proposition 5.7 may be modified, using the elements of $\mathbf{A} \setminus \mathbf{A}'$, to be in $\langle \mathbf{1} \rangle$.

Definition 5.6 (Compatible functions)**.** Fix a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$. We say that a map $\psi : \mathbf{A}' \to \{0,1\}^k$ is *compatible* (with respect to the system) if, for all j, if $a \in \mathbf{A}^j$ then $\psi(a) \in \mathrm{Supp}(\mu_j)$.

Setting $B_\omega^{(j)} = \{a \in \mathbf{A}^j : \psi(a) = \omega\}$, we see that ψ being compatible is equivalent to $B_\omega^{(j)} \neq \emptyset$ only if $\mu_j(\omega) > 0$, and is consistent with earlier notation (4.5).

Proposition 5.7. *There exist real numbers $\kappa^* > 0$, $p > 1$ and $t > 0$ so that the following is true. Let $\delta > 0$ and suppose that D is sufficiently large as a function of δ. Uniformly for $0 \leqslant \kappa \leqslant \kappa^*$, we have with probability at least $1-\delta$, that $\sum_{a\in\mathbf{A}'} a\psi(a)$ takes at least*

$$(t\delta)^{\frac{1}{p-1}} D^{\sum_j c_j \dim(V_j/V_{j-1})}$$

different values modulo $\langle \mathbf{1}\rangle$, as ψ ranges over all nondegenerate, compatible maps.

Remark. By (5.8), it clearly suffices to prove Proposition (5.7) for $\kappa = \kappa^*$.

We will deduce Proposition 5.7 from a moment bound. Firstly, define the representation function $r_{\mathbf{A}} : \mathbb{Q}^k/\langle \mathbf{1}\rangle \to \mathbb{R}$ by

$$r_{\mathbf{A}}(x) := \sum_{\substack{\psi:\mathbf{A}'\to\{0,1\}^k \\ \sum_{a\in\mathbf{A}'} a\psi(a)-x\in\langle \mathbf{1}\rangle}} w_{\mathbf{A}}(\psi),$$

where the summation is over all maps $\psi : \mathbf{A}' \to \{0,1\}^k$, and where

$$w_{\mathbf{A}}(\psi) := \prod_{j=1}^{r} \prod_{a\in\mathbf{A}^j} \mu_j(\psi(a)).$$

This weight function is chosen so that it is large only when ψ is *balanced*, that is, when for all j and ω, the set $\mathbf{A}^j$ has about $\mu_j(\omega)|\mathbf{A}_j|$ elements a with $\psi(a) = \omega$. Observe that if $\psi(a) \notin \mathrm{Supp}(\mu_j)$ for some j and some $a \in \mathbf{A}^j$, then $w_{\mathbf{A}}(\psi) = 0$, and thus only compatible ψ contribute to the sum $r_{\mathbf{A}}(x)$.

The crucial moment bound for the deduction of Proposition 5.7 is given below.

Proposition 5.8. *Fix a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ which satisfies the entropy gap condition (5.6). There is a $p > 1$ so that uniformly for $0 \leqslant \kappa \leqslant \kappa^*$ we have the moment bound*

$$\mathbb{E}\Big[\sum_x r_{\mathbf{A}}(x)^p\Big] \ll D^{-(p-1)\sum_j c_j \dim(V_j/V_{j-1})};$$

the implied constant depends on the underlying system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, as well as on κ and on p, but not *on the parameter D.*

Proof of Proposition 5.7, assuming Proposition 5.8. Define also

$$r'_{\mathbf{A}}(x) := \sum_{\substack{\psi:\mathbf{A}'\to\{0,1\}^k \\ \psi \text{ is compatible and nondegenerate} \\ \sum_{a\in\mathbf{A}'} a\psi(a)-x\in\langle \mathbf{1}\rangle}} w_{\mathbf{A}}(\psi).$$

We have

$$\sum_x r_{\mathbf{A}}(x) = \prod_{j=1}^{r} \Big(\sum_{\omega} \mu_j(\omega)\Big)^{|\mathbf{A}^j|} = \prod_{j=1}^{r} 1 = 1$$

for any $\mathbf{A}$. On the other hand, when ψ is non-compatible then $w_{\mathbf{A}}(\psi) = 0$. Also, Lemma 5.2 (c) implies that $\cup_j \mathrm{Supp}(\mu_j)$ spans V_r. Thus, if ψ is degenerate, then for some j and $\omega \in \mathrm{Supp}(\mu_j)$, ω is not in the support of ψ. Therefore,

$$\sum_x (r_{\mathbf{A}}(x) - r'_{\mathbf{A}}(x)) \leqslant \sum_{j=1}^{r} \sum_{\omega\in\mathrm{Supp}(\mu_j)} (1-\mu_j(\omega))^{|\mathbf{A}^j|}.$$

Also, by Lemma A.5, $|\mathbf{A}^j| \geqslant \frac{1}{2}(c_j - c_{j+1})\log D$ for all j with probability $> 1 - O(e^{-(1/4)\log^{1/2} D})$, and thus the right side above is $o(1)$ with this same probability. Now fix a small $\delta > 0$. Therefore, with probability at least $1 - \delta/2$ (for D sufficiently large),

$$\sum_x r'_{\mathbf{A}}(x) \geqslant \frac{1}{2}. \tag{5.9}$$

Thus, by Markov's inequality and Proposition 5.8, we also have, with probability at least $1-\delta/2$,

$$\sum_x r'_{\mathbf{A}}(x)^p \leqslant \sum_x r_{\mathbf{A}}(x)^p \ll \delta^{-1} D^{-(p-1)\sum_j c_j \dim(V_j/V_{j-1})}. \tag{5.10}$$

By Hölder's inequality,

$$\sum_x r'_{\mathbf{A}}(x) \leqslant |\operatorname{Supp}(r'_{\mathbf{A}})|^{1-1/p}\Big(\sum_x r'_{\mathbf{A}}(x)^p\Big)^{1/p}. \tag{5.11}$$

With probability at least $1 - \delta$, both (5.9) and (5.10) hold, and in this case (5.11) gives

$$|\operatorname{Supp}(r'_{\mathbf{A}})| \gg_p \delta^{\frac{1}{p-1}} D^{\sum_j c_j \dim(V_j/V_{j-1})}.$$

This completes the proof of Proposition 5.7. □

The rest of the section is devoted to the proof of Proposition 5.8.

5.3. **An entropy condition for adapted systems**

Throughout the remainder of this section, $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ will be a fixed system satisfying (5.6). We do not assume the conditions (b)-(e) in Lemma 5.2.

For reasons that will become apparent, in the proof of Proposition 5.8 we will need to apply the entropy gap condition not only with subflags $\mathscr{V}'$ of $\mathscr{V}$, but with a more general type of system.

Definition 5.9 (Adapted system)**.** Given a system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, the pair $(\mathscr{W}, \mathbf{b})$ is *adapted* to $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ if $\mathscr{W} : \langle \mathbf{1} \rangle = W_0 \leqslant W_1 \leqslant \cdots \leqslant W_s$ is a complete flag with $W_s \leqslant V_r$, and $\mathbf{b} = (b_1, \dots, b_s)$ satisfies the condition

$$W_i \leqslant V_j \qquad \text{whenever} \qquad b_i > c_{j+1}.$$

We say that $(\mathscr{W}, \mathbf{b})$ is *saturated* if $s = \dim(V_r) - 1$ and for all $j \leqslant r$, there are exactly $\dim V_j - 1$ values of i with $b_i > c_{j+1}$. Otherwise, we call $(\mathscr{W}, \mathbf{b})$ *unsaturated*.

Remark. For the definition of complete flag, see Definition 3.1. We make a few comments to motivate the term *saturated*. Let

$$m_j = \#\{i : b_i > c_{j+1}\} \qquad (0 \leqslant j \leqslant r), \tag{5.12}$$

so that the b_i's belonging to the interval $(c_{j+1}, c_j]$ are precisely $b_{m_{j-1}+1}, \dots, b_{m_j}$. Since $W_i \leqslant V_j$ whenever $b_i > c_{j+1}$, we infer that

$$W_{m_j} \leqslant V_j \qquad (1 \leqslant j \leqslant r). \tag{5.13}$$

Since $\mathscr{W}$ is complete, we know that $\dim(W_i) = i + 1$, and thus $m_j \leqslant \dim(V_j) - 1$. In particular, $(\mathscr{W}, \mathbf{b})$ is saturated if, and only if, we have equality in (5.13) for all j. □

We need some further notation, which reflects that $\mathbf{A}'$ is supported on intervals with gaps. For $1 \leqslant j \leqslant r$, let

$$I_j = (c_{j+1}, c_j], \qquad I'_j = (c_{j+1} + \kappa, c_j]. \tag{5.14}$$

Also, if $(\mathscr{W}, \mathbf{b})$ is an adapted system for $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$, we set

$$G_i = G_i(\mathbf{b}) = (b_{i+1}, b_i], \tag{5.15}$$

There is a natural analogue of $\mathrm{e}()$ (cf. Definition 3.5) for adapted systems.

Definition 5.10. Given an adapted system $(\mathscr{W}, \mathbf{b})$, we define

$$\mathrm{e}(\mathscr{W}, \mathbf{b}) = \mathrm{e}(\mathscr{W}, \mathbf{b}; \mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) := \sum_{i,j} \lambda(G_i \cap I_j)\mathbb{H}_{\mu_j}(W_i) + \sum_i b_i,$$

where λ denotes Lebesgue measure on $\mathbb{R}$. For technical reasons (to do with needing to "leave gaps" for later parts of the argument) we also define the variant

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}) := \sum_{i,j} \lambda(G_i \cap I'_j)\mathbb{H}_{\mu_j}(W_i) + \sum_i b_i. \tag{5.16}$$

Finally, we define

$$\delta(\mathbf{b}) = \max_{i,j}\{c_j - b_i : b_i \in I'_j\}, \tag{5.17}$$

that is to say $\delta(\mathbf{b})$ is the smallest non-negative real number with the property that

$$c_j - \delta(\mathbf{b}) \leqslant b_i \leqslant c_j \qquad (1 \leqslant j \leqslant r,\ i \in I'_j).$$

Adapted systems $(\mathscr{W}, \mathbf{b})$ can, in a certain sense, be interpreted in terms of convex superpositions of pairs $(\mathscr{V}', \mathbf{c})$, $\mathscr{V}' \leqslant \mathscr{V}$ a subflag. As a consequence, their $\mathrm{e}()$-values can all be shown to be at least $\mathrm{e}(\mathscr{V})$. The next lemma elaborates this point, obtaining a strict inequality analogous to (5.6) unless $\mathscr{W}$ is saturated and has a small value of $\delta(\mathbf{b})$, which corresponds to the convex superposition which gives rise to $(\mathscr{W}, \mathbf{b})$ having weight ≈ 1 on the trivial subflag $(\mathscr{V}, \mathbf{c})$. To complicate matters, we must also work with e' in place of e.

Lemma 5.11. *Suppose that $(\mathscr{W}, \mathbf{b})$ is an adapted system such that b_i lies in some set I'_j for each i. Suppose, further, that κ is small enough in terms of ε.*

(a) *If $(\mathscr{W}, \mathbf{b})$ is unsaturated, then $\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon/2$.*
(b) *If $(\mathscr{W}, \mathbf{b})$ is a saturated, then $\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon\delta(\mathbf{b})/2$.*

Proof. We treat both parts together for most of the proof. Let m_j be defined by (5.12). Note that $\max_{i \in I'_j}(c_j - b_i) = c_j - b_{m_j}$, and let j_0 be such that

$$\delta(\mathbf{b}) = c_{j_0} - b_{m_{j_0}}.$$

Without loss of generality, we may assume that $b_{m_{j_0}} < c_{j_0}$; the case $b_{m_{j_0}} = c_{j_0}$ will then follow by continuity.

Set $b = b_{m_{j_0}}$ and note that

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \min\left\{ \mathrm{e}'(\mathscr{W}, \mathbf{b}') : \begin{array}{l} b'_i \in [c_{j+1} + \kappa, c_j] \text{ when } i \in (m_{j-1}, m_j] \text{ and } j \neq j_0, \\ b'_i \in [b, c_{j_0}] \text{ when } i \in (m_{j_0-1}, m_{j_0}),\ b'_{m_{j_0}} = b, \\ b'_1 \geqslant b'_2 \geqslant \cdots \geqslant b'_s \end{array} \right\}.$$

The quantity $\mathrm{e}'(\mathscr{W}, \mathbf{b}')$ is linear in each variable b'_i and the region over which we consider the above minimum is a polytope. As a consequence, the minimum of $\mathrm{e}'(\mathscr{W}, \mathbf{b}')$ must occur at one of the

vertices of the polytope. In particular, there are indices $\ell_j \in (m_{j-1}, m_j]$ for $j = 1, \dots, r$ such that

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}'(\mathscr{W}, \mathbf{b}^*), \qquad \text{where} \qquad b_i^* = \begin{cases} c_j & \text{if } m_{j-1} < i \leqslant \ell_j, \\ c_{j+1} + \kappa & \text{if } \ell_j < i \leqslant m_j,\ j \neq j_0, \\ b & \text{if } \ell_{j_0} < i \leqslant m_{j_0}. \end{cases} \tag{5.18}$$

In fact, note that we must have $\ell_{j_0} < m_{j_0}$ because $b^*_{m_{j_0}} = b$ and we have assumed that $b < c_{j_0}$.

Using the linearity of $\mathrm{e}'(\mathscr{W}, \cdot)$ once again, we find that

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}^*) = \frac{c_{j_0} - b}{c_{j_0} - c_{j_0+1} - \kappa} \mathrm{e}'(\mathscr{W}, \mathbf{b}^{(1)}) + \frac{b - c_{j_0+1} + \kappa}{c_{j_0} - c_{j_0+1} - \kappa} \mathrm{e}'(\mathscr{W}, \mathbf{b}^{(2)}), \tag{5.19}$$

where $b_i^{(1)} = b_i^{(2)} = b_i^*$ for $i \in \{1, \dots, s\} \setminus (\ell_{j_0}, m_{j_0}]$, $b_i^{(1)} = c_{j_0+1} + \kappa$ for $i \in (\ell_{j_0}, m_{j_0}]$ and $b_i^{(2)} = c_{j_0}$ for $i \in (\ell_{j_0}, m_{j_0}]$.

Fix $\mathbf{b}' \in \{\mathbf{b}^{(1)}, \mathbf{b}^{(2)}\}$. In addition, define the indices $i_1, \dots, i_r$ by letting $i_j = \ell_j$ when $j \neq j_0$ or $\mathbf{b}' = \mathbf{b}^{(1)}$, while letting $i_{j_0} = m_{j_0}$ when $\mathbf{b}' = \mathbf{b}^{(2)}$. We then have

$$b_i' = \begin{cases} c_j & \text{if } m_{j-1} < i \leqslant i_j, \\ c_{j+1} + \kappa & \text{if } i_j < i \leqslant m_j. \end{cases}$$

A straightforward calculation implies that

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}') = \mathrm{e}(\mathscr{V}') + S\kappa, \tag{5.20}$$

where $\mathscr{V}'$ is the subflag of $\mathscr{V}$ with $V_j' = W_{i_j}$ and

$$S = \sum_{j=1}^{r} \big(m_j - i_j - \mathbb{H}_{\mu_j}(W_{i_j})\big).$$

(Note that $\mathscr{V}'$ is indeed a subflag since $W_{i_j} \leqslant W_{m_j} \leqslant V_j$ by (5.13).)

If $\mathscr{V}' = \mathscr{V}$, we must have that $W_{i_j} = V_j$ for all j. Since $W_{i_j} \leqslant W_{m_j} \leqslant V_j$, we infer that $W_{m_j} = V_j$, as well as that $i_j = m_j$ for all j. In particular, the flag $(\mathscr{W}, \mathbf{b})$ we started with must be saturated and $S = 0$ (since $i_j = m_j$ and $\mathbb{H}_{\mu_j}(W_{i_j}) = \mathbb{H}_{\mu_j}(V_j) = 0$ for all j).

We are now ready to complete the proof of both parts of the lemma.

(a) By the above discussion, if $(\mathscr{W}, \mathbf{b})$ is unsaturated, then $\mathscr{V}' \neq \mathscr{V}$. Therefore, $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon$, whence $\mathrm{e}'(\mathscr{W}, \mathbf{b}') \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon$ for $\mathbf{b}' \in \{\mathbf{b}^{(1)}, \mathbf{b}^{(2)}\}$. Inserting this inequality into (5.19) implies that $\mathrm{e}'(\mathscr{W}, \mathbf{b}^*) \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon + O(\kappa)$. Since $\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}'(\mathscr{W}, \mathbf{b}^*)$, the proof of part (a) is complete by assuming that κ is small enough in terms of ε.

(b) Assume that $(\mathscr{W}, \mathbf{b})$ is saturated. We can only have that $\mathscr{V}' = \mathscr{V}$ if $i_{j_0} = m_{j_0}$. Since $\ell_{j_0} < m_{j_0}$, this can only happen when $\mathbf{b}' = \mathbf{b}^{(2)}$. As a consequence, assuming again that κ is small enough in terms of ε, we have that

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}') \geqslant \begin{cases} \mathrm{e}(\mathscr{V}) + \varepsilon/2 & \text{if } \mathbf{b}' = \mathbf{b}^{(1)}, \\ \mathrm{e}(\mathscr{V}) & \text{if } \mathbf{b}' = \mathbf{b}^{(2)}. \end{cases}$$

Inserting this into (5.19) yields the inequality

$$\mathrm{e}'(\mathscr{W}, \mathbf{b}^*) \geqslant \mathrm{e}(\mathscr{V}) + \frac{c_{j_0} - b}{c_{j_0} - c_{j_0+1} - \kappa} \cdot \frac{\varepsilon}{2}.$$

Since $b = c_{j_0} - \delta(\mathbf{b})$, $c_{j_0} - c_{j_0+1} - \kappa \leqslant 1$, and $\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}'(\mathscr{W}, \mathbf{b}^*)$, we find that $\mathrm{e}'(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon\delta(\mathbf{b})/2$. This completes the proof of part (b) of the lemma. □

5.4. **Proof of the moment bound**

In this subsection we prove Proposition 5.8. For a vector $\mathbf{n} = (n_0, n_1, n_2, \dots, n_r)$ with

$$0 = n_0 \leqslant n_1 \leqslant \cdots \leqslant n_r,$$

define the event

$$S(\mathbf{n}) = \{\mathbf{A}' : \#\mathbf{A}_j = n_j - n_{j-1} \quad (1 \leqslant j \leqslant r)\}.$$

When $\mathbf{A}'$ lies in $S(\mathbf{n})$, we write

$$\mathbf{A}' = \{a_1, a_2, \dots, a_{n_r}\}, \qquad a_1 > a_2 > \dots > a_{n_r},$$

so that

$$a_t \in \mathbf{A}^j \qquad \text{if and only if} \qquad n_{j-1} < t \leqslant n_j. \tag{5.21}$$

We may define, for any compatible ψ, the auxilliary function

$$\theta : [n_r] \to \Omega \cup \{\mathbf{0}\} \qquad \text{such that} \qquad \theta(t) = \psi(a_t). \tag{5.22}$$

The salient property of θ is that it is determined by the ordering of the elements in $\mathbf{A}^j$ and not by the elements themselves. We denote by $\mathbf{\Theta_n}$ the set of compatible functions θ, that is, those functions satisfying

$$\theta(t) \in \mathrm{Supp}(\mu_j) \qquad \text{whenever} \qquad t \leqslant n_j, \quad 1 \leqslant j \leqslant r\,. \tag{5.23}$$

In the event $S(\mathbf{n})$, if ψ is an compatible function and θ is defined by (5.22), we have

$$w_{\mathbf{A}}(\psi) = w_{\mathbf{n}}(\theta) := \prod_{j=1}^{r} \prod_{n_{j-1} < t \leqslant n_j} \mu_j(\theta(t)), \tag{5.24}$$

where the notation $w_{\mathbf{n}}$ (in place of $w_{\mathbf{A}}$) reflects the fact that w only depends on θ, and not otherwise on $\mathbf{A}$. In this notation,

$$r_{\mathbf{A}}(x) = \sum_{\substack{\theta \in \mathbf{\Theta_n} \\ \sum_t \theta(t) a_t - x \in \langle \mathbf{1} \rangle}} w_{\mathbf{n}}(\theta).$$

Writing $r_{\mathbf{A}}^p = r_{\mathbf{A}}^{p-1} r_{\mathbf{A}}$ and interchanging the order of summation, it follows that if $S(\mathbf{n})$ then

$$\begin{aligned} \sum_x r_{\mathbf{A}}(x)^p &= \sum_{\theta \in \mathbf{\Theta_n}} \Big(r_{\mathbf{A}}\Big(\sum_t a_t \theta(t) \Big) \Big)^{p-1} w_{\mathbf{n}}(\theta) \\ &= \sum_{\theta \in \mathbf{\Theta_n}} \Big(\sum_{\substack{\theta' \in \mathbf{\Theta_n} \\ \text{(5.26)}}} w_{\mathbf{n}}(\theta') \Big)^{p-1} w_{\mathbf{n}}(\theta), \end{aligned} \tag{5.25}$$

where the inner summation is over all compatible functions θ' satisfying

$$\sum_t a_t(\theta'(t) - \theta(t)) \in \langle \mathbf{1} \rangle. \tag{5.26}$$

Similar to the argument in subsection 4.2, we find a flag $\mathscr{W}$ and special values of i which have the effect of isolating terms in the relation (5.26). With $\theta, \theta', \mathbf{n}$ fixed, let

$$\Omega = \Omega(\theta, \theta') = \{\theta'(t) - \theta(t) : 1 \leqslant t \leqslant n_r\}$$

and

$$s = \dim_{\mathbb{Q}} \big(\mathrm{Span}(\mathbf{1}, \Omega) \big) - 1.$$

We now choose a special basis of $\mathrm{Span}(\mathbf{1}, \Omega)$. For each $\omega \in \Omega$, let

$$K_\omega = \min\{t : \theta'(t) - \theta(t) = \omega\},$$

and place a total ordering on Ω by saying that $\omega \prec \omega'$ if $K_\omega < K_{\omega'}$. Let ω^1 be the minimum element in $\Omega \setminus \langle \mathbf{1} \rangle$, $\omega^2 = \min(\Omega \setminus \mathrm{Span}(\mathbf{1}, \omega^1)), \dots, \omega^s = \min(\Omega \setminus \mathrm{Span}(\mathbf{1}, \omega^1, \dots, \omega^{s-1}))$, where s is such that $\Omega \subset \mathrm{Span}(\mathbf{1}, \omega^1, \dots, \omega^s)$. Finally, let

$$W_j = \mathrm{Span}(\mathbf{1}, \omega^1, \dots, \omega^j), \qquad \tau_j = K_{\omega^j} \qquad (1 \leqslant j \leqslant s),$$
$$\boldsymbol{\tau}(\theta, \theta', \mathbf{n}) = (\tau_1, \dots, \tau_s),$$

and form the flag

$$\mathscr{W} = \mathscr{W}(\theta, \theta', \mathbf{n}) \ : \ W_0 \leqslant W_1 \leqslant \cdots \leqslant W_s.$$

We note that in the special case $\theta = \theta'$, we have $s = 0$ and $\mathscr{W}$ is a trivial flag with only one space W_0.

Now we divide up the sample space of $\mathbf{A}'$ into events describing the rough size of the critical elements a_{τ_j}. By construction,

$$a_{\tau_j} = \max\{a_t \in \mathbf{A}' : \theta'(t) - \theta(t) = \omega^j\}.$$

Similarly to Section 4, for $1 \leqslant i \leqslant s$ let

$$b_i = \frac{\lceil \log a_{\tau_i} \rceil}{\log D} \qquad \text{so that} \quad a_{\tau_i} \in (D^{b_i}/e, D^{b_i}]. \tag{5.27}$$

From subsection 4.2 we may also assume that $c_j \log D \in \mathbb{N}$ for all j. To formalize this, we assume that all c_j and b_i lie in the lattice $\Gamma = \{m/\log D : m \in \mathbb{N}\}$.

The definition of $\mathbf{A}'$ implies that for each i, there is some j with $b_i \in I_j' = (c_{j+1} + \kappa, c_j]$. Moreover, we have the implications

$$b_i > c_{j+1} \quad \Longrightarrow \quad \tau_i \leqslant n_j \quad \Longrightarrow \quad \omega^i = \theta(\tau_i) - \theta'(\tau_i) \in V_j,$$

where we used (5.23) to obtain the second implication. Since $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_i$, we infer the stronger relation

$$b_i > c_{j+1} \qquad \Longrightarrow \qquad W_i \leqslant V_j. \tag{5.28}$$

Therefore, the pair $(\mathscr{W}, \mathbf{b})$ is adapted to $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$.

Using the inequality $(x+y)^{p-1} \leqslant x^{p-1} + y^{p-1}$ repeatedly, we may partition (5.25) according to the values of $\mathscr{W}(\theta, \theta')$ and $\boldsymbol{\tau}(\theta, \theta')$, obtaining (still assuming $S(\mathbf{n})$)

$$\sum_x r_{\mathbf{A}}(x)^p \leqslant \sum_{\mathscr{W}, \boldsymbol{\tau}, \theta} \Bigg(\sum_{\substack{\theta' \in \boldsymbol{\Theta}_{\mathbf{n}},\ (5.26) \\ \mathscr{W}(\theta,\theta',\mathbf{n}) = \mathscr{W},\ \boldsymbol{\tau}(\theta,\theta',\mathbf{n}) = \boldsymbol{\tau}}} w_{\mathbf{n}}(\theta') \Bigg)^{p-1} w_{\mathbf{n}}(\theta).$$

We need to separately consider other elements of $\mathbf{A}'$ that lie in the intervals $(D^{b_i}/e, D^{b_i}]$, and so we define

$$\mathcal{B} = \{b_i : 1 \leqslant i \leqslant s\} \qquad \text{and} \qquad \boldsymbol{\ell} = (\ell_b)_{b \in \mathcal{B}}, \qquad \text{where} \qquad \ell_b = \#\big(\mathbf{A}' \cap (D^b/e, D^b]\big).$$

By assumption, $\sum_b \ell_b \geqslant s$. It may happen that $b_i = b_{i+1}$ for some i, in which case $|\mathcal{B}| < s$. With $\mathbf{n}, \boldsymbol{\tau}, \mathbf{b}, \boldsymbol{\ell}$ all fixed, consider the event

$$E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})$$

defined as the intersection of

- $S(\mathbf{n})$;
- $\tau_i \in (D^{b_i}/e, D^{b_i}]$ for all i;
- $|\mathbf{A}' \cap (D^b/e, D^b]| = \ell_b$ for all $b \in \mathcal{B}$.

Under $S(\mathbf{n})$, the event $E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})$ must occur for some $\mathbf{b}, \boldsymbol{\tau}, \boldsymbol{\ell}$. The event $E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})$ fixes the *number* of elements of $\mathbf{A}$ in various sets, but otherwise does not specify any of the elements themselves.

Taking expectations over $\mathbf{A}$, we get

$$\mathbb{E}\Big[1_{S(\mathbf{n})} \sum_x r_{\mathbf{A}}(x)^p\Big]$$
$$\leqslant \mathbb{E}\Big[\sum_{\mathscr{W}, \boldsymbol{\tau}, \mathbf{b}, \theta, \boldsymbol{\ell}} w_{\mathbf{n}}(\theta) \Big(\sum_{\substack{\theta' \in \boldsymbol{\Theta}_{\mathbf{n}},\ (5.26) \\ \mathscr{W}(\theta,\theta',\mathbf{n}) = \mathscr{W},\ \boldsymbol{\tau}(\theta,\theta',\mathbf{n}) = \boldsymbol{\tau}}} w_{\mathbf{n}}(\theta') \Big)^{p-1} 1_{E(\mathbf{b},\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell})} \Big].$$

By Hölder's inequality with exponents $\frac{1}{p-1}$, $\frac{1}{2-p}$, this implies that

$$\mathbb{E}\Big[1_{S(\mathbf{n})} \sum_x r_{\mathbf{A}}(x)^p\Big] \leqslant \sum_{\mathscr{W}, \boldsymbol{\tau}, \mathbf{b}, \theta, \boldsymbol{\ell}} w_{\mathbf{n}}(\theta) \mathbb{P}(E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell}))^{2-p} \times$$
$$\times \Big\{ \sum_{\substack{\theta' \in \boldsymbol{\Theta}_{\mathbf{n}} \\ \mathscr{W}(\theta,\theta',\mathbf{n}) = \mathscr{W} \\ \boldsymbol{\tau}(\theta,\theta',\mathbf{n}) = \boldsymbol{\tau}}} w_{\mathbf{n}}(\theta') \mathbb{P}\big[E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell}) \wedge (5.26)\big] \Big\}^{p-1}. \tag{5.29}$$

Claim. We have

$$\mathbb{P}\big((5.26) \,\big|\, E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})\big) \ll D^{-(b_1+\cdots+b_s)} e^{\sum_b \ell_b}. \tag{5.30}$$

Proof of Claim. We argue as in the proof of Proposition (4.4). Relation (5.26) implies

$$\sum_{i=1}^s \omega^i a_{\tau_i} + \sum_{t \notin \{\tau_1, \dots, \tau_s\}} a_t(\theta'(t) - \theta(t)) = a_0 \mathbf{1}$$

for some $a_0 \in \mathbb{Z}$. Since $\mathbf{1}, \omega^1, \dots, \omega^s$ are linearly independent, this uniquely determines their coefficients $a_0, a_{\tau_1}, \dots, a_{\tau_s}$ in terms of the other a_i's. For each $b \in \mathcal{B}$, let

$$m_b = \#\{i : b_i = b\} \quad \text{and} \quad N_b = \#\big(\mathbb{Z} \cap (D^b/e, D^b]\big) = (1 - 1/e)D^b + O(1).$$

Then, given $\mathbf{A}^* = \mathbf{A}' \setminus G$ and $b \in \mathcal{B}$, there are at most

$$\binom{N_b}{\ell_b - m_b} \leqslant \frac{N_b^{\ell_b - m_b}}{(\ell_b - m_b)!} \ll \ell_b^{m_b} \cdot \frac{((1-1/e)D)^{b(\ell_b - m_b)}}{\ell_b!} \ll \frac{D^{b(\ell_b - m_b)}}{\ell_b!}$$

choices for $\tilde{\mathbf{A}}_b = \mathbf{A}' \cap (D^b, eD^b]$, where we used that $\ell_b^{m_b} \leqslant \ell_b^k \ll (1-1/e)^{-\ell_b}$. In addition, Lemma A.4 implies that the probability of occurrence of a set $X_b \subset \mathbb{Z} \cap (D^b, eD^b]$ as the set $\tilde{\mathbf{A}}_b$, conditionally to the event that $\#\tilde{\mathbf{A}}_b = \ell_b$, is

$$\ll \frac{\ell_b!}{(\sum_{D^b/e < m \leqslant D^b} 1/(m-1))^{\ell_b}} \prod_{x \in X_b} \frac{1}{x} \prod_{D^b/e < m \leqslant D^b} \Big(1 - \frac{1}{m}\Big) \ll \frac{\ell_b!}{(D^b/e)^{\ell_b}}.$$

Putting the above estimates together, we conclude that

$$\mathbb{P}\big((5.26) \bigm| E(\mathbf{b},\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell})\big) \ll \prod_{b\in\mathcal{B}} \frac{e^{\ell_b}}{D^{bm_b}} = D^{-(b_1+\cdots+b_s)} e^{\sum_b \ell_b},$$

upon noticing that $\sum_{b\in\mathcal{B}} m_b b = \sum_i b_i$. This proves our claim that (5.30) holds. □

In the light of (5.30), relation (5.29) becomes

$$\mathbb{E}\Big[1_{S(\mathbf{n})} \sum_x r_{\mathbf{A}}(x)^p\Big]$$
$$\ll \sum_{\mathscr{W},\boldsymbol{\tau},\mathbf{b},\boldsymbol{\ell}} D^{-(p-1)\sum_j b_j} e^{\sum_b \ell_b} \mathbb{E}\Big[\sum_{\theta\in\boldsymbol{\Theta}_{\mathbf{n}}} w_{\mathbf{n}}(\theta)\Big(\sum_{\substack{\theta'\in\boldsymbol{\Theta}_{\mathbf{n}}\\ \mathscr{W}(\theta,\theta',\mathbf{n})=\mathscr{W}\\ \boldsymbol{\tau}(\theta,\theta',\mathbf{n})=\boldsymbol{\tau}}} w_{\mathbf{n}}(\theta')\Big)^{p-1} 1_{E(\mathbf{b},\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell})}\Big]. \tag{5.31}$$

To evaluate the bracketed expression, first recall the definition (5.24) of $w_{\mathbf{n}}(\theta')$, and note that the conditions $\mathscr{W}(\theta,\theta',\mathbf{n}) = \mathscr{W}$, $\boldsymbol{\tau}(\theta,\theta',\mathbf{n}) = \boldsymbol{\tau}$ together imply that

$$\theta'(t) - \theta(t) \in W_i \qquad (1 \leqslant t < \tau_{i+1},\ 0 \leqslant i \leqslant s),$$

where we have defined $\tau_{s+1} := n_r + 1$. For brevity, write

$$T_{i,j} = (n_{j-1}, n_j] \cap [\tau_i, \tau_{i+1}) \cap \mathbb{N}, \qquad (1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant r).$$

Some of these sets are empty. In any case, we have

$$\sum_{\substack{\theta'\in\boldsymbol{\Theta}_{\mathbf{n}}\\ \mathscr{W}(\theta,\theta',\mathbf{n})=\mathscr{W}\\ \boldsymbol{\tau}(\theta,\theta',\mathbf{n})=\boldsymbol{\tau}}} w_{\mathbf{n}}(\theta') \leqslant \prod_{\substack{0\leqslant i\leqslant s\\ 1\leqslant j\leqslant r}} \prod_{t\in T_{i,j}} \mu_j(\theta(t) + W_i). \tag{5.32}$$

From (5.24), and the fact that the discrete intervals $T_{i,j}$ are disjoint and cover $[n_r]$, we have

$$w_{\mathbf{n}}(\theta) = \prod_{i,j} \prod_{t\in T_{i,j}} \mu_j(\theta(t)).$$

With these observations, we conclude that

$$\sum_{\theta\in\boldsymbol{\Theta}_{\mathbf{n}}} w_{\mathbf{n}}(\theta)\Big(\sum_{\substack{\theta'\in\boldsymbol{\Theta}_{\mathbf{n}}\\ \mathscr{W}(\theta,\theta',\mathbf{n})=\mathscr{W}\\ \boldsymbol{\tau}(\theta,\theta',\mathbf{n})=\boldsymbol{\tau}}} w_{\mathbf{n}}(\theta')\Big)^{p-1} \leqslant \sum_{\theta\in\boldsymbol{\Theta}_{\mathbf{n}}} \prod_{i,j} \prod_{t\in T_{i,j}} \mu_j(\theta(t))\mu_j(W_i + \theta(t))^{p-1}$$
$$= \prod_{i,j} \eta(i,j,p,\mathscr{W})^{|T_{i,j}|}, \tag{5.33}$$

where

$$\eta(i,j,p,\mathscr{W}) := \sum_{\omega\in\Omega} \mu_j(\omega)\mu_j(W_i+\omega)^{p-1}. \tag{5.34}$$

Substituting into (5.31), and summing over $\mathbf{n}$, we get

$$\mathbb{E}\Big[\sum_x r_{\mathbf{A}}(x)^p\Big] \ll \sum_{\mathscr{W},\mathbf{b}} D^{-(p-1)\sum_j b_j} \sum_{\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell}} e^{\sum_b \ell_b} \mathbb{E}\Big[1_{E(\mathbf{b},\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell})} \prod_{i,j} \eta(i,j,p,\mathscr{W})^{|T_{i,j}|}\Big]. \tag{5.35}$$

If $V_j \leqslant W_i$, then $\mu_j(W_i+\omega) = 1$ for all ω and thus $\eta(i,j,p,\mathscr{W}) = 1$. For all $i,j,p,\mathscr{W}$ we have $\eta(i,j,p,\mathscr{W}) \leqslant 1$. Thus, we require lower bounds on $|T_{i,j}|$ in the case $V_j \not\leqslant W_i$.

Claim. Assume that $E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})$ holds. Given i such that $b_{i+1} < b_i$ and $j \in \{1, \dots, r\}$, define

$$M_{i,j} := (D^{c_{j+1}+\kappa}, D^{c_j}] \cap (D^{b_{i+1}}, D^{b_i}/e]$$

Then

$$\{t : a_t \in M_{i,j}\} \subset T_{i,j}. \tag{5.36}$$

Proof of Claim. Let t be such that $a_t \in M_{i,j}$. In particular, $D^{b_{i+1}} < t \leqslant D^{b_i}/e$. This relation and the definition of b_i in (5.27) imply that $a_{\tau_{i+1}} < a_t < a_{\tau_i}$ and hence $\tau_i < t < \tau_{i+1}$, where we used that $a_1 > a_2 > \cdots > a_{n_r}$. In addition, since $D^{c_{j+1}+\kappa} < a_t \leqslant D^{c_j}$, we have that $a_t \in \mathbf{A}^j$. Thus, $n_{j-1} < t \leqslant n_j$ by (5.21). This completes the proof of the claim. □

A direct consequence of (5.36) is that

$$|T_{i,j}| \geqslant \big|\mathbf{A} \cap M_{i,j}\big|.$$

Combining this inequality with (5.35), we get

$$\mathbb{E}\Big[\sum_x r_{\mathbf{A}}(x)^p\Big] \ll \sum_{\mathscr{W},\mathbf{b}} D^{-(p-1)\sum_j b_j} \sum_{\mathbf{n},\boldsymbol{\tau},\boldsymbol{\ell}} e^{\sum_b \ell_b} \mathbb{E}\Big[1_{E(\mathbf{b},\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell})} \prod_{i,j} \eta(i,j,p,\mathscr{W})^{|\mathbf{A}\cap M_{i,j}|}\Big].$$

Given $\mathscr{W}$ and $\mathbf{b}$, and knowledge that $E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})$ holds, this uniquely determines $\mathbf{n}$ and $\boldsymbol{\ell}$, but not necessarily $\boldsymbol{\tau}$. However, the number of choices of $\boldsymbol{\tau}$ is at most $\prod_b \ell_b \leqslant e^{\sum_b \ell_b}$. Since the event $E(\mathbf{b}, \boldsymbol{\tau}, \mathbf{n}, \boldsymbol{\ell})$ contains the event $S(\mathbf{n})$, it follows that

$$\begin{aligned}&\sum_{\mathbf{n},\boldsymbol{\tau},\boldsymbol{\ell}} e^{\sum_b \ell_b} \mathbb{E}\Big[1_{E(\mathbf{b},\boldsymbol{\tau},\mathbf{n},\boldsymbol{\ell})} \eta(i,j,p,\mathscr{W})^{|\mathbf{A}\cap M_{i,j}|}\Big]\\ &\qquad \leqslant \sum_{\mathbf{n},\boldsymbol{\ell}} e^{2\sum_b \ell_b} \mathbb{E}\Big[1_{S(\mathbf{n})} 1_{E'(\boldsymbol{\ell})} \prod_{i,j} \eta(i,j,p,\mathscr{W})^{|\mathbf{A}\cap M_{i,j}|}\Big],\end{aligned}$$

where $E'(\boldsymbol{\ell})$ is the event that $\#\tilde{\mathbf{A}}_b = \ell_b$ for all $b \in \mathcal{B}$. Since the events $S(\mathbf{n})$ are mutually disjoint, we arrive at the inequality

$$\mathbb{E}\Big[\sum_x r_{\mathbf{A}}(x)^p\Big] \leqslant \sum_{\mathscr{W},\mathbf{b}} D^{-(p-1)\sum_j b_j}\, \mathbb{E}\Big[\prod_{b\in\mathcal{B}} e^{2|\tilde{\mathbf{A}}_b|} \prod_{i,j} \eta(i,j,p,\mathscr{W})^{|\mathbf{A}\cap M_{i,j}|}\Big]. \tag{5.37}$$

Next, we estimate the right hand side of (5.37). The intervals $M_{i,j}$ and $(D^b/e, D^b]$ are mutually disjoint by (5.36), hence the quantities $|\mathbf{A} \cap M_{i,j}|$ and $|\tilde{\mathbf{A}}_b|$ are independent. Using Lemma A.3, we obtain

$$\begin{aligned}&\mathbb{E}\Big[\prod_{b\in\mathcal{B}} e^{2|\tilde{\mathbf{A}}_b|} \prod_{i,j} \eta(i,j,p,\mathscr{W})^{|\mathbf{A}\cap M_{i,j}|}\Big]\\ &\leqslant \exp\Big\{\sum_{b\in\mathcal{B}} \sum_{D^b/e<m\leqslant D^b} \frac{2e-1}{m} + \sum_{i,j} \big(\eta(i,j,p,\mathscr{W})-1\big) \sum_{m\in M_{i,j}} \frac{1}{m}\Big\}\\ &\ll \exp\Big\{\sum_{i,j} \big(\eta(i,j,p,\mathscr{W})-1\big) \sum_{m\in M_{i,j}} \frac{1}{m}\Big\}.\end{aligned}$$

Recall that

$$I_j' = (c_{j+1}+\kappa, c_j] \qquad \text{and} \qquad G_i = G_i(\mathbf{b}) = (b_{i+1}, b_i],$$

as defined in (5.14) and (5.15), and that λ denotes the Lebesgue measure on $\mathbb{R}$. Then, by (5.36),

$$\sum_{m\in M_{i,j}} \frac{1}{m} = \lambda(I_j'\cap G_i)\log D + O(1).$$

Substituting into (5.37), and recalling the definition (5.16) of $\mathrm{e}'()$, this gives

$$\mathbb{E}\Big[\sum_x r_{\mathbf{A}}(x)^p\Big] \ll \sum_{\mathscr{W},\mathbf{b}} D^{-E(p,\mathscr{W},\mathbf{b})}, \tag{5.38}$$

where

$$\begin{aligned} E(p,\mathscr{W},\mathbf{b}) &:= (p-1)\sum_j b_j - \sum_{i,j}\sum \big(\eta(i,j,p,\mathscr{W})-1\big)\lambda(I_j'\cap G_i)\\ &= (p-1)\mathrm{e}'(\mathscr{W},\mathbf{b}) - \sum_{i,j}\sum \big[\eta(i,j,p,\mathscr{W})-1+(p-1)\mathbb{H}_{\mu_j}(W_i)\big]\lambda(I_j'\cap G_i). \end{aligned}$$

Recall the definition (5.34) of $\eta(i,j,p,\mathscr{W})$. If $W_i \geqslant V_j$, then $\mu_j(W_i+x)=1$ whenever $x\in\mathrm{Supp}(\mu_j)$, and so in this case $\eta(i,j,p,\mathscr{W})=1$. Since $\mathbb{H}_{\mu_j}(W_i)=0$ in this case, we have

$$\eta(i,j,p,\mathscr{W})-1+(p-1)\mathbb{H}_{\mu_j}(W_i)=0 \qquad (V_j\leqslant W_i). \tag{5.39}$$

For any fixed $i,j,\mathscr{W}$, we have

$$\frac{\mathrm{d}}{\mathrm{d}p}\eta(i,j,p,\mathscr{W})\Big|_{p=1} = -\mathbb{H}_{\mu_j}(W_i),$$

and so

$$\eta(i,j,p,\mathscr{W})-1+(p-1)\mathbb{H}_{\mu_j}(W_l) \ll (p-1)^2 \qquad (V_j\not\leqslant W_i). \tag{5.40}$$

We deduce from (5.38), (5.39) and (5.40) that

$$E(p,\mathscr{W},\mathbf{b}) = (p-1)\mathrm{e}'(\mathscr{W},\mathbf{b}) - \sum_{i,j:\ V_j\not\leqslant W_i}\sum \lambda(I_j'\cap G_i)O((p-1)^2). \tag{5.41}$$

To continue, we separate two cases.

Case 1. $(\mathscr{W},\mathbf{b})$ is unsaturated.

In the above case, Lemma 5.11(a) implies that $\mathrm{e}'(\mathscr{W},\mathbf{b})\geqslant \mathrm{e}(\mathscr{V})+\varepsilon/2$. Consequently,

$$E(p,\mathscr{W},\mathbf{b}) \geqslant (p-1)\mathrm{e}(\mathscr{V}) + \frac{(p-1)\varepsilon}{2} + O((p-1)^2) \geqslant (p-1)\mathrm{e}(\mathscr{V}) + \frac{(p-1)\varepsilon}{4},$$

provided that $p-1$ is small enough in terms of ε (and k).

Since there are $O(1)$ choices for $\mathscr{W}$ and $\log^{O(1)} D$ choices for $\mathbf{b}$, the contribution of such flags to the right hand side of (5.38) is

$$\sum_{(\mathscr{W},\mathbf{b})\ \text{unsaturated}} D^{-E(p,\mathscr{W},\mathbf{b})} \ll D^{-(p-1)\mathrm{e}(\mathscr{V})}. \tag{5.42}$$

Case 2. $(\mathscr{W},\mathbf{b})$ is saturated. (Recall from Definition 5.9 that $(\mathscr{W},\mathbf{b})$ is called saturated when $s=\dim(V_r)-1$ and for all $j\leqslant r$, there are exactly $\dim V_j - 1$ values of i with $b_i > c_{j+1}$.)

Fix for the moment a pair (i,j) such that

$$V_j\not\leqslant W_i \qquad \text{and} \qquad \lambda(I_j'\cap G_i)>0. \tag{5.43}$$

The second condition is equivalent to knowing that

$$b_i > c_{j+1} \qquad \text{and} \qquad b_{i+1} < c_j.$$

In particular, we have $W_i \leqslant V_j$ by (5.28). Note though that we have assumed $V_j \nleqslant W_i$. Therefore, $W_i < V_j$. Since $\dim(W_i) = i+1$, we infer that

$$i \leqslant \dim(V_j) - 2.$$

Since we have assumed that $(\mathscr{W}, \mathbf{b})$ is saturated, the above inequality implies that $b_{i+1} > c_{j+1}$. Recalling the definition (5.17) of $\delta(\mathbf{b})$, we conclude that

$$b_{i+1} \geqslant c_j - \delta(\mathbf{b}).$$

This implies that $G_i \cap I_j' \subset [c_j - \delta(\mathbf{b}), c_j]$ for any pair (i,j) satisfying (5.43). As a consequence,

$$\sum_{i:\ V_j \nleqslant W_i} \lambda(I_j' \cap G_i) \leqslant \delta(\mathbf{b}) \qquad (1 \leqslant j \leqslant r).$$

Since we also have that $\mathrm{e}(\mathscr{W}, \mathbf{b}) \geqslant \mathrm{e}(\mathscr{V}) + \varepsilon\delta(\mathbf{b})/2$ by Lemma (5.11)(b), it follows that

$$E(p, \mathscr{W}, \mathbf{b}) \geqslant (p-1)\mathrm{e}(\mathscr{V}) + \varepsilon\delta(\mathbf{b})/2 + O((p-1)^2\delta(\mathbf{b})) \geqslant (p-1)\mathrm{e}(\mathscr{V}) + \varepsilon\delta(\mathbf{b})/4, \quad (5.44)$$

provided that $p-1$ is small enough compared to ε.

Using (5.44), we see that the contribution of saturated flags to the right hand side of (5.38) is

$$\sum_{(\mathscr{W},\mathbf{b})\ \text{saturated}} D^{-E(p,\mathscr{W},\mathbf{b})} \ll D^{-(p-1)\mathrm{e}(\mathscr{V})} \sum_{s=0}^{r} \sum_{b_1,\dots,b_s} D^{-(p-1)\varepsilon\delta(\mathbf{b})/4},$$

where we used that there are $O(1)$ choices for $\mathscr{W}$. Recall that the numbers b_i and c_j are restricted to the set $\Gamma = \{m/\log D : m \in \mathbb{N}\}$. Thus the number of $\mathbf{b}$ with $\delta(\mathbf{b}) = m/\log D$ is at most $(m+1)^s$ and

$$\sum_{s=0}^{r} \sum_{b_1,\dots,b_s} D^{-(p-1)\varepsilon\delta(\mathbf{b})/4} \leqslant \sum_{s=0}^{r} \sum_{m \geqslant 0} (m+1)^s e^{-(p-1)(\varepsilon/4)m} \ll_{\varepsilon,p} 1.$$

We thus conclude that

$$\sum_{(\mathscr{W},\mathbf{b})\ \text{saturated}} D^{-E(p,\mathscr{W},\mathbf{b})} \ll D^{-(p-1)\mathrm{e}(\mathscr{V})}.$$

If we combine the above inequality with (5.42) and (5.38), we establish Proposition (5.8). □

6. An argument of Maier and Tenenbaum

The aim of this section is to prove Proposition 5.5. The reader may care to recall the statement of that proposition now, as well as the definition of a compatible map (Definition 5.6). As in the previous section, the system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ is fixed, and satisfies the entropy gap condition (5.6) as well as the conditions (b)-(e) of Lemma 5.2. We recall two of these conditions:

$$\text{(c)} \qquad \mathrm{Span}\Big(\bigcup_{i=1}^{j} \mathrm{Supp}(\mu_i)\Big) = V_j \qquad \text{for } j = 1, \dots, r; \quad (6.1)$$

$$\text{(e)} \qquad \mu_j(\omega) = \mu_j(\mathbf{1} - \omega) \qquad \text{for } j = 1, \dots, r \text{ and for } \omega \in V_j. \quad (6.2)$$

We also fix a basis $\{\mathbf{1}, \omega^1, \dots, \omega^d\}$ of V_r such that $V_j = \mathrm{Span}(\mathbf{1}, \omega^1, \dots, \omega^{\dim(V_j)-1})$ for each j. By (6.1), we may choose the basis so that $\omega^i \in \mathrm{Supp}(\mu_j)$ whenever $1 \leqslant j \leqslant r$ and $\dim(V_{j-1}) \leqslant$

$i \leqslant \dim(V_j) - 1$. As before, denote

$$\Omega := \bigcup_{j=1}^{r} \mathrm{Supp}(\mu_j).$$

We begin with an observation related to the solvability of (4.10). Let Λ denote the $\mathbb{Z}$-span of $\mathbf{1}, \omega^1, \dots, \omega^d$ (that is, the lattice generated by $\mathbf{1}, \omega^1, \dots, \omega^d$), and as before set $\Omega = \bigcup_{j=1}^{r} \mathrm{Supp}(\mu_j)$. Every vector $\omega \in \Omega$ is a rational combination of the basis elements $\mathbf{1}, \omega^1, \dots, \omega^d$. Hence, there is some $M \in \mathbb{N}$ such that $M\omega \in \Lambda$ for each $\omega \in \Omega$. In particular, note that the right hand side of (4.10) is in the lattice $\Lambda/M = \{x/M : x \in \Lambda\}$.

In this section, implied constants in $O()$ and $\ll$ notations may depend on the system $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ and basis $\omega^1, \dots, \omega^d$; in particular, on k, d and M.

6.1. The sets $\mathscr{L}_i(\mathbf{A})$ and lower bounds for their size

The main statement of this subsection, Proposition 6.2, is a variant of Proposition 5.7, where we stipulate that every element lies in Λ.

Fix $\kappa > 0$ satisfying $\kappa \leqslant \frac{\kappa^*}{2}$, where κ^* is the constant from Proposition 5.7. In particular, $\kappa \leqslant 1/2$. We introduce the sets

$$I_i(D) := \bigcup_{j=1}^{r} (D^{c_{j+1}}, D^{c_j(1-\kappa/i)}], \qquad i = 1, 2, \cdots. \tag{6.3}$$

Thus each $I_i(D)$ is simply a union of r intervals in Λ, and we have the nesting

$$I_1(D) \subset I_2(D) \subset \cdots \subset (D^c, D].$$

For any $\omega \in V_r$ we denote by $\overline{\omega}$ the projection onto $\overline{V}_r = V_r/\langle \mathbf{1} \rangle = \mathrm{Span}\{\omega^1, \dots, \omega^j\}$. In addition let $\overline{\psi}(a) = \overline{\psi(a)}$ for $a \in \mathbf{A}$.

The reader may wish to recall the definition of nondegenerate (Definition 5.4) and compatible (Definition 5.6) maps.

Definition 6.1. Write $\mathscr{L}_i(\mathbf{A})$ for the set of all $\sum_{a \in \mathbf{A}} a\overline{\psi}(a)$ that lie in Λ, where ψ ranges over all nondegenerate, compatible maps supported on $I_i(D)$.

Proposition 6.2. *Let $\delta > 0$ and $i \in \mathbb{N}$, and let D be sufficiently large in terms of δ. Then with probability at least $1 - \delta$ in the choice of $\mathbf{A} \cap I_i(D)$,*

$$|\mathscr{L}_i(\mathbf{A})| \gg \delta^{\alpha} D^{(1-\kappa/i)\sum_j c_j \dim(V_j/V_{j-1})}, \tag{6.4}$$

where α is a positive constant depending at most on $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$.

Proof. Let

$$I_i'(D) = \bigcup_{j=1}^{r} (D^{(c_{j+1}+\kappa^*)(1-\kappa/i)}, D^{c_j(1-\kappa/i)}] \subset \bigcup_{j=1}^{r} (D^{c_{j+1}(1+\kappa/2)}, D^{c_j(1-\kappa/i)}] \subset I_i(D),$$

where the first inclusion follows by noticing that $(c_{j+1} + \kappa^*)(1 - \kappa/i) \geqslant c_{j+1}(1 + \kappa/2)$ for $c_{j+1} \in [0, 1]$ and $0 \leqslant \kappa \leqslant \kappa^*/2 \leqslant 1/2$. Write $\mathscr{L}_i'(\mathbf{A})$ for the set of all $\sum_{a \in \mathbf{A}} a\overline{\psi}(a)$, where ψ ranges over all nondegenerate, compatible maps supported on $I_i'(D)$, but without the stipulation that the sum is in Λ. We now apply Proposition 5.7 with D replaced by $D^{1-\kappa/i}$ and δ replaced by $\delta/2$ to conclude

that

$$|\mathscr{L}_i'(\mathbf{A})| \gg \delta^\alpha D^{(1-\kappa/i)\sum_j c_j \dim(V_j/V_{j-1})}$$

with probability at least $1-\delta/2$, where $\alpha = 10/(p-1)$ with p as in Proposition 5.7.

We now use the elements of $\mathbf{A} \cap (I_i(D) \setminus I_i'(D))$ to create many sums $\sum_{a\in\mathbf{A}} \overline{\psi}(a)$ which do lie in Λ. For $1 \leqslant j \leqslant r$, let $G_j := (D^{c_{j+1}(1-\kappa/i)}, \delta^{-1}D^{c_{j+1}(1-\kappa/i)}]$, which is a subset of $I_i(D) \setminus I_i'(D)$. Let $\mathcal{E}$ be the event that for every $1 \leqslant j \leqslant r$, $\mathbf{A}\cap G_j$ contains a set $\mathcal{K}_j$ which has exactly 2^k elements that are $\equiv m \pmod M$ for each $m \in \{1,\dots,M\}$. Lemma A.2 (applied with $B = \{b \in \mathbb{Z}\cap G_j : b \equiv m \pmod M\}$ and $\varepsilon = 1/3$) implies that if δ is sufficiently small then $\mathbb{P}(\mathcal{E}) \geqslant 1-\delta/2$.

Assume now that we are in the event $\mathcal{E}$. Take any nondegenerate, compatible function $\psi : \mathbf{A} \to \mathbb{Q}^d$ supported on $I_i'(D)$, and write

$$\sum_{a\in I_i'(D)} a\psi(a) = \sum_{\omega\in\Omega} \omega N_\omega.$$

For each $\omega \in \Omega$, pick an index j such that $\omega \in \mathrm{Supp}(\mu_j)$ and an element $a_\omega \in \mathcal{K}_j$ satisfying $a_\omega \equiv -N_\omega \pmod M$. Setting $\psi_0(a_\omega) = \omega$ for each ω, and $\psi_0(a) = \psi(a)$ for $a \in I_i'(D)$, we have

$$\sum_{a\in I_i(D)} a\psi_0(a) = \sum_{\omega\in\Omega} (a_\omega + N_\omega)\omega \in \Lambda,$$

since $M|(a_\omega + N_\omega)$ for all ω. Moreover, ψ_0 is nondegenerate and compatible by construction. Consequently, $\sum_a a\overline{\psi}_0(a) \in \Lambda$ (by removing the coefficient of $\mathbf{1}$). Since there are at most $2^{\sum_j |\mathcal{K}_j|} \leqslant 2^{rM2^k}$ choices for $\{a_\omega : \omega \in \Omega\}$, the map from $\sum_{a\in I_i'(D)} a\overline{\psi}(a)$ to $\sum_{a\in I_i(D)} a\overline{\psi}_0(a)$ is at most $2^{\sum_j |\mathcal{K}_j|}$-to-1.We conclude that with probability $\geqslant 1-\delta$,

$$|\mathscr{L}_i(\mathbf{A})| \geqslant 2^{-rM2^k}|\mathscr{L}_i'(\mathbf{A})| \gg \delta^\alpha D^{(1-\kappa/i)\sum_j c_j \dim(V_j/V_{j-1})},$$

the implied constant only depending on k, M and α, which are all fixed. □

6.2. **Putting $\mathscr{L}_i(\mathbf{A})$ in a box**

In the last section, we showed that (with high probability) $\mathscr{L}_i(\mathbf{A})$ is large. In this section we show that with high probability it is contained in a box (in coordinates $\omega^1,\dots,\omega^d$); putting these results together one then sees that $\mathscr{L}_i(\mathbf{A})$ occupies a positive proportion of lattice points in the box, the bound being independent of D.

Set

$$N_j^{(i)} := \delta^{-1}\|\mu\|_\infty D^{(1-\kappa/i)c_j} \qquad \text{and} \qquad N^{(i)} := \prod_{t=1}^d N_{j(t)}^{(i)}. \tag{6.5}$$

where $\|\mu\|_\infty$ is the largest coordinate of any element in $\bigcup_{j=1}^r \mathrm{Supp}(\mu_j)$ when written with respect to the base $\mathbf{1}, \omega^1, \dots, \omega^d$.

For $t \in \{1,\dots,d\}$, write $j(t)$ for the unique j such that $\dim V_{j-1} < t \leqslant \dim V_j$.

Lemma 6.3. *Assume $\delta > 0$ is small enough so that $de^{-2/\delta} \leqslant \delta$. Then, we have*

$$\mathscr{L}_i(\mathbf{A}) \subset \bigoplus_{t=1}^d \big[-N_{j(t)}^{(i)}, N_{j(t)}^{(i)}\big]\omega^t \tag{6.6}$$

with probability at least $1-\delta$ in the choice of $\mathbf{A}\cap I_i(D)$.

Proof. This follows quickly from the fact that ψ is compatible and by Lemma A.6, the latter implying that

$$\sum_{a\in\mathbf{A}\cap[2,D^{(1-\kappa/i)c_j}]} a \leqslant \delta^{-1}D^{(1-\kappa/i)c_j} \qquad (1\leqslant j\leqslant d)$$

with probability $\geqslant 1-de^{-2/\delta}\geqslant 1-\delta$. □

Proposition 6.4. *Let δ and α be as in Proposition 6.2 and in Lemma 6.3. With probability at least $1-\delta$ in the choice of $\mathbf{A}\cap I_i(D)$, $\mathscr{L}_i(\mathbf{A})$ is a subset of the box $\bigoplus_{t=1}^d[-N^{(i)}_{j(t)},N^{(i)}_{j(t)}]\omega^t$ of size $\gg \delta^{d+\alpha}N^{(i)}$.*

Proof. This follows immediately upon combining Proposition 6.2 and Lemma 6.3 (applied with δ replaced by $\delta/2$). □

6.3. **Zero sums with positive probability**

Lemma 6.5. *Let $i\in\mathbb{Z}\cap[1,(\log D)^{1/3}]$. In addition, let $S\subset\bigoplus_{t=1}^d[-N^{(i)}_{j(t)},N^{(i)}_{j(t)}]\omega^t$ with $|S|\gg\delta^\beta N^{(i)}$ and with $S\subset\Lambda$. Then*

$$\mathbb{P}\big(0\in\mathscr{L}_{i+1}(\mathbf{A})\,\big|\,\mathscr{L}_i(\mathbf{A})=S\big)\gg\delta^{2d\beta}.$$

Proof. We condition on a fixed choice of $\mathbf{A}\cap I_i(D)$ for which $\mathscr{L}_i(\mathbf{A})=S$. Then it is enough to show that with probability $\gg\delta^{2\beta d}$, the set $\mathbf{A}\cap(I_{i+1}(D)\setminus I_i(D))$ contains $2d$ distinct elements a_t and a_t', $1\leqslant t\leqslant d$, such that

$$\sum_t (a_t'-a_t)\omega^t\in S. \tag{6.7}$$

To see why this is sufficient, let $s=\sum_t(a_t'-a_t)\omega^t$, which we know belongs to $S=\mathscr{L}_i(\mathbf{A})$. In particular, there is an compatible map ψ supported on $I_i(D)$ such that $\sum_{a\in\mathbf{A}}a\overline{\psi}(a)=s$. Now, consider the function $\psi':\mathbf{A}\cap I_{i+1}(D)\to\Omega$ with $\psi'(a)=\psi(a)$ for $a\in\mathbf{A}\cap I_i(D)$, $\psi'(a_t')=\mathbf{1}-\omega^t$ and $\psi'(a_t)=\omega^t$ for $1\leqslant t\leqslant d$. This is possible in virtue of (6.2). It is now clear that $0\in\mathscr{L}_{i+1}(\mathbf{A})$. Hence, if the conditional probability that (6.7) holds is $\gg\delta^{2\beta d}$, so is the probability that $0\in\mathscr{L}_{i+1}(\mathbf{A})$.

To find a_t and a_t' satisfying (6.7), let

$$n:=\big\lceil d2^{d+2}N^{(i)}/|S|\big\rceil\ll\delta^{-\beta}.$$

The number of elements $\sum_t s_t\omega^t\in S$ with $n|s_t$ for some t is

$$\leqslant\sum_{t=1}^d\big(2N^{(i)}_{j(t)}/n+1\big)\prod_{t'\neq t}\big(2N^{(i)}_j(t')+1\big)\leqslant d2^{d+1}N^{(i)}/n\leqslant|S|/2$$

for large D. Thus, there is a subset $S'\subset S$ of size at least $|S|/2$ and with $n\nmid s_t$ for all t. We will choose the sets $\{a_t:1\leqslant t\leqslant d\}$ and $\{a_t':1\leqslant t\leqslant d\}$ independently, by selecting $a_t\equiv 0\pmod n$ and $a_t'\not\equiv 0\pmod n$.

Note that

$$I_{i+1}(D)\setminus I_i(D)=\bigcup_{j=1}^r(D^{(1-\kappa/i)c_j},D^{(1-\kappa/(i+1))c_j}]\supset\bigcup_{j=1}^r[N^{(i)}_j,100dN^{(i)}_j]$$

provided that $i \leqslant (\log D)^{1/3}$. For each given t, i and j, the probability that the interval $[4tN_j^{(i)}, (4t+2)N_j^{(i)}]$ contains no element $a_t \equiv 0 \pmod n$ of $\mathbf{A}$ equals

$$\prod_{\substack{4tN_j^{(i)} \leqslant a \leqslant (4t+2)N_j^{(i)} \\ a \equiv 0 \pmod n}} (1 - 1/a) \leqslant 1 - \gamma/n$$

for some small positive constant $\gamma = \gamma(d)$. Thus, the probability that, for each $t = 1, 2, \dots, d$, the set $\mathbf{A}$ contains some $a_t \equiv 0 \pmod n$ in the interval $[4tN_j^{(i)}, (4t+2)N_j^{(i)}]$ is $\gg 1/n^d \gg \delta^{d\beta}$.

Fix a choice of $a_1, \dots, a_d$ as described above, and set

$$X := \{(a_1 + s_1, \dots, a_d + s_d) : s_1\omega^1 + \cdots + s_d\omega^d \in S'\}. \tag{6.8}$$

By construction, every coordinate of $x \in X$ is $\not\equiv 0 \pmod n$. Also,

$$X \subset \prod_{t=1}^{d} \big[(4t-1)N_{j(t)}^{(i)}, (4t+3)N_{j(t)}^{(i)}\big]. \tag{6.9}$$

Now the intervals on the right side above are disjoint, and

$$|X| \geqslant \frac{|S|}{2} \gg \delta^{\beta} \prod_{t=1}^{d} N_{j(t)}^{(i)}.$$

Thus, by Lemma A.7, with probability $\gg (\delta^{\beta})^d$, there are $a_1', \dots, a_d' \in \mathbf{A}$ such that $(a_1', \dots, a_t') \in X$. The relation (6.7) follows for such a_t, a_t', which exist with probability $\gg \delta^{d\beta} \cdot \delta^{d\beta}$. □

6.4. **An iterative argument**

To complete the proof of Proposition 5.5, we apply Lemma 6.5 iteratively. Let $\mathscr{S}$ be the set of sets S satisfying the assumptions of Lemma 6.5. We say that $\mathscr{L}_i(\mathbf{A})$ is *large* if it satisfies the conclusions of Proposition 6.4, or equivalently if $\mathscr{L}_i(\mathbf{A}) = S$ with $S \in \mathscr{S}$. Thus Lemma 6.5 implies that

$$\begin{aligned}\mathbb{P}\big(0 \in \mathscr{L}_{i+1}(\mathbf{A}) \setminus \mathscr{L}_i(\mathbf{A}),\ \mathscr{L}_i(\mathbf{A}) \text{ large}\big) &= \sum_{\substack{S \text{ large} \\ 0 \notin S}} \mathbb{P}(\mathscr{L}_i(\mathbf{A}) = S) \cdot \mathbb{P}\big(0 \in \mathscr{L}_{i+1}(\mathbf{A}) \,\big|\, \mathscr{L}_i(\mathbf{A}) = S\big) \\ &\gg \delta^{2d\alpha} \mathbb{P}\big(\mathscr{L}_i(\mathbf{A}) \text{ large},\ 0 \notin \mathscr{L}_i(\mathbf{A})\big).\end{aligned}$$

We conclude there is some $\varepsilon = \delta^{O(1)}$ such that

$$\mathbb{P}\big(0 \in \mathscr{L}_{i+1}(\mathbf{A}) \,\big|\, \mathscr{L}_i(\mathbf{A}) \text{ large}, 0 \notin \mathscr{L}_i(\mathbf{A})\big) \geqslant \varepsilon. \tag{6.10}$$

Moreover, Proposition 6.4 implies that

$$\mathbb{P}(\mathscr{L}_i(\mathbf{A}) \text{ large}) \geqslant 1 - \delta. \tag{6.11}$$

For brevity, write E_i for the event that $0 \notin \mathscr{L}_i(\mathbf{A})$, and F_i for the event that $\mathscr{L}_i(\mathbf{A})$ is large. Since $\mathscr{L}_1(\mathbf{A}) \subset \mathscr{L}_2(\mathbf{A}) \subset \cdots$, we have $E_1 \supset E_2 \supset \cdots$.

We claim that there is some $i \leqslant I := \lfloor (\log D)^{1/3} \rfloor$ such that $\mathbb{P}(E_i) < 2\delta$. Indeed, for each $i \leqslant I$, we have

$$\begin{aligned}\mathbb{P}(E_{i+1}) &= \mathbb{P}(E_{i+1}|E_i \cap F_i)\mathbb{P}(E_i \cap F_i) + \mathbb{P}(E_{i+1}|E_i \cap F_i^c)\mathbb{P}(E_i \cap F_i^c)\\ &\leqslant (1-\varepsilon)\mathbb{P}(E_i \cap F_i) + \mathbb{P}(E_i \cap F_i^c) \qquad \text{by (6.10)}\\ &= \mathbb{P}(E_i) - \varepsilon\mathbb{P}(E_i \cap F_i)\\ &\leqslant \mathbb{P}(E_i) - \varepsilon(\mathbb{P}(E_i) - \delta) \qquad \text{by (6.11)}.\end{aligned}$$

It follows that if $\mathbb{P}(E_i) \geqslant 2\delta$, then $\mathbb{P}(E_{i+1}) \leqslant (1-\varepsilon/2)\mathbb{P}(E_i)$. If this were true for each $i \leqslant I$, we would infer that $\mathbb{P}(E_I) \leqslant (1-\varepsilon/2)^{I-1} < 2\delta$, which is a contradiction. We conclude that there is some $i^* \leqslant I$ for which $\mathbb{P}(\mathbb{E}_{i^*}) \leqslant 2\delta$. Redefining δ to $\delta/2$, this completes the proof of Proposition 5.5.

PART III. THE OPTIMISATION PROBLEM

7. THE OPTIMISATION PROBLEM – BASIC FEATURES

In this section we consider Problem 3.7, the optimisation problem on the cube, which is a key feature of our paper. We will give some kind of a solution to this for a fixed nondegenerate flag $\mathscr{V}$, leaving aside the question of how to choose $\mathscr{V}$ optimally.

Let us refresh ourselves on the main elements of the setup of Problem 3.7. We have a flag

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

of distinct vector spaces. We wish to find probability measures $\mu_1, \dots, \mu_r$ on $\{0,1\}^k$ satisfying $\mathrm{Supp}(\mu_j) \subset V_j$, and thresholds $1 = c_1 > c_2 > \cdots > c_{r+1} = c$ such that the entropy condition (3.3) holds, that is to say

$$\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) \tag{7.1}$$

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

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

By Lemma 5.2 (e), we may restrict our attention to systems such that $\dim(V_1/V_0) = 1$, which we henceforth assume. The aim is to find the maximum possible value of c, and this we denote by $\gamma_k(\mathscr{V})$.

7.1. A restricted optimisation problem

It turns out to be very useful to consider a restricted variant of the problem in which the entropy condition (7.1) is only required to be satisfied for certain "basic" subflags $\mathscr{V}'$, rather than all of them.

Definition 7.1 (Basic subflag)**.** Given a flag $\mathscr{V} : \langle \mathbf{1} \rangle = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_r$, the basic subflags $\mathscr{V}'_{\mathrm{basic}(m)}$ are the ones in which $V_i' = V_{\min(m,i)}$, for $m = 0, 1, \dots, r-1$ (note that when $m = r$ we recover $\mathscr{V}$ itself).

Here is the restricted version of Problem 3.7. Recall that a flag is non-degenerate if the top space V_r is not contained in any of the subspaces $\{x \in \mathbb{R}^k : x_i = x_j\}$. The restriction to nondegenerate flags ensures that the subsets $A_1, \dots, A_k$ in our main problem are distinct.

Problem 7.2. Let $\mathscr{V}$ be a nondegenerate flag of distinct spaces in $\mathbb{Q}^k$. Define $\gamma_k^{\mathrm{res}}(\mathscr{V})$ to be the supremum of all constants c for which we can construct the data $\mu_1, \dots, \mu_r$, $\mathrm{Supp}(\mu_i) \subset V_i$, and $1 = c_1 > \cdots > c_{r+1} = c$ such that the restricted entropy condition

$$\mathrm{e}(\mathscr{V}'_{\mathrm{basic}(m)}; \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}; \mathbf{c}, \boldsymbol{\mu}) \tag{7.2}$$

holds for all $m = 0, 1, \dots, r-1$.

It is clear that

$$\gamma_k^{\mathrm{res}}(\mathscr{V}) \geqslant \gamma_k(\mathscr{V}). \tag{7.3}$$

In general there is absolutely no reason to suppose that the two quantities are equal, since after all the restricted entropy condition (7.2) apparently only captures a small portion of the full condition (7.1).

Our reason for studying the restricted problem is that we do strongly believe that

$$\sup_{\mathscr{V}\text{ nondegenerate}} \gamma_k^{\text{res}}(\mathscr{V}) = \sup_{\mathscr{V}\text{ nondegenerate}} \gamma_k(\mathscr{V}) = \gamma_k.$$

One might think of this unproven assertion, on an intuitive level, in two (roughly equivalent) ways:

- for those flags optimal for Problem 3.7, the critical cases of (7.1) are those for which $\mathscr{V}'$ is basic;
- for those flags optimal for Problem 3.7, and for the critical choice of the c_i, μ_i, the restricted condition (7.2) in fact implies the more general condition (7.1).

7.2. **The ρ-equations, optimal measures and optimal parameters**

The definitions and constructions of this section will appear unmotivated at first sight. They are forced upon us by the analysis of subsection 7.5 below.

Let the flag $\mathscr{V}$ be fixed.

It is convenient to call the intersection of a coset $x+V_i$ with the cube $\{0,1\}^k$ a *cell at level* i, and to denote the cells at various levels by the letter C. (The terminology comes from the fact it can be useful to think of V_i defining a σ-algebra (partition) on $\{0,1\}^k$, the equivalence relation being given by $\omega \sim \omega'$ iff $\omega - \omega' \in V_i$: however, we will not generally use the language of σ-algebras in what follows.)

If C is a cell at level i then it will be a union of cells C' at level $i-1$. These cells we call the children of C, and we write $C \to C'$.

Let $\boldsymbol{\rho} = (\rho_1, \dots, \rho_{r-1})$ be real parameters in $(0,1)$, and for each cell C define functions $f^C(\boldsymbol{\rho})$ by the following recursive recipe:

- If C has level 0, then $f^C(\boldsymbol{\rho}) = 1$;
- If C has level i, then

$$f^C(\boldsymbol{\rho}) = \sum_{C \to C'} f^{C'}(\boldsymbol{\rho})^{\rho_{i-1}}, \tag{7.4}$$

with the convention that $\rho_0 = 0$.

Write

$$\Gamma_i = V_i \cap \{0,1\}^k$$

for the cell at level i which contains $\mathbf{0}$. Note that

$$\Gamma_0 \subset \Gamma_1 \subset \cdots \subset \Gamma_r.$$

Figure 7.2 on the next page illustrates these definitions for the so-called *binary flag* in $\mathbb{Q}^4$, which will be a key object of study from Section 9 onwards. Here $V_1 = \{x_1x_2x_3x_4 \in \{0,1\}^4 : x_1 = x_2, x_3 = x_4\}$ and $V_2 = \mathbb{Q}^4$.

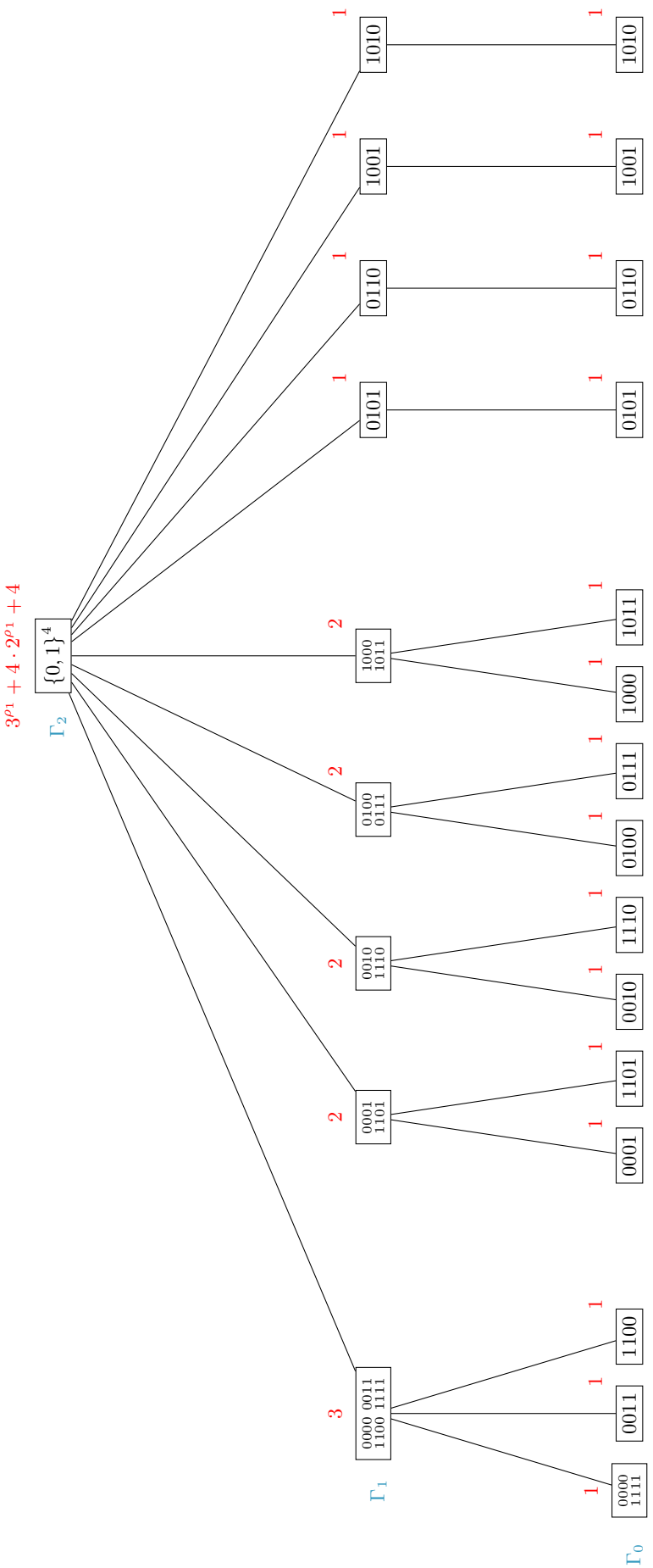


Figure: the tree structure corresponding to the binary flag $\langle \mathbf{1} \rangle = V_0 \leqslant V_1 \leqslant V_2 \leqslant \mathbb{Q}^4$. Values of $f^C(\rho)$ are given in red.

Definition 7.3 (ρ-equations)**.** The ρ-equations are the system of equations

$$f^{\Gamma_{j+1}}(\boldsymbol{\rho}) = (f^{\Gamma_j}(\boldsymbol{\rho}))^{\rho_j} e^{\dim(V_{j+1}/V_j)}, \qquad j = 1, 2, \dots, r-1. \tag{7.5}$$

We say that they have a solution if they are satisfied with $\rho_1, \dots, \rho_{r-1} \in (0,1)$.

Example. For the binary flag on $\mathbb{Q}^4$, as illustrated in Figure 7.2, 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 $\rho_1 \approx 0.306481$.

In general the ρ-equations may or may not have a solution, but for flags $\mathscr{V}$ of interest to us, it turns out that they have a unique such solution. In this case, we make the following definition.

Definition 7.4 (Optimal measures)**.** Suppose that $\mathscr{V}$ is a flag for which the ρ-equations have a solution. Then the corresponding *optimal measure on* μ^* *on* $\{0,1\}^k$ *with respect to* $\mathscr{V}$ is defined as follows: we set $\mu^*(\Gamma_r) = 1$, and

$$\frac{\mu^*(C')}{\mu^*(C)} = \frac{f^{C'}(\boldsymbol{\rho})^{\rho_{i-1}}}{f^C(\boldsymbol{\rho})} \tag{7.6}$$

for any cell C at level $i \geqslant 1$ and any child $C \to C'$. We also set $\mu^*(\mathbf{1}) = 0$. Lastly, we define the restrictions $\mu_j^*(\omega) := \mu^*(\Gamma_j)^{-1}\mu^*(\omega)1_{\omega \in \Gamma_j}$ for $j = 1, 2, \dots, r$ (thus $\mu_r^* = \mu^*$). We call these[3] *optimal measures* (on $\{0,1\}^k$, with respect to $\mathscr{V}$). Finally, we write $\boldsymbol{\mu}^* = (\mu_1^*, \mu_2^*, \dots, \mu_r^*)$.

Remark. (a) By taking telescoping products of (7.6) for $i = r, r-1, \cdots, 0$, we see that μ^* is uniquely defined on all cells at level 0, and these are the cell $\{\mathbf{0}, \mathbf{1}\}$ and singletons $\{\omega\}$ for all $\omega \in \{0,1\}^k$, $\omega \neq \mathbf{0}, \mathbf{1}$. Since we also specified $\mu^*(\mathbf{1}) = 0$ (an arbitrary choice) we see that $\mu^*(\omega)$ is completely and uniquely determined by these rules, for all ω. In particular, the ρ-equations (7.5) imply that

$$\mu_j(\Gamma_m) = e^{-\dim(V_j/V_m)} \qquad (j \geqslant m \geqslant 0). \tag{7.7}$$

(b) At the moment, the term "optimal measure" is just a name. We will establish the sense in which (in situations of interest) the measures μ_j^* are optimal in Proposition 7.7 below.

(c) Note that $\boldsymbol{\mu}^*$ and μ^* are two different (but closely related) objects. The former is an r-tuple of measures μ_j^*, all of which are induced from the single measure μ^*.

Definition 7.5 (Optimal parameters)**.** Suppose that $\mathscr{V}$ is a flag for which the ρ-equations have a solution. Let μ^* be the corresponding optimal measure on $\{0,1\}^k$ with respect to $\mathscr{V}$. Suppose additionally that

$$\mathbb{H}_{\mu_{m+1}^*}(V_m) \neq \dim(V_{m+1}/V_m) \tag{7.8}$$

for $m = 0, 1, \dots, r-1$. Then the corresponding *optimal parameters* with respect to $\mathscr{V}$ and the solution $\boldsymbol{\rho}$ are the unique choice of $\mathbf{c}^* : 1 = c_1^* > c_2^* > \cdots > c_{r+1}^* > 0$, if it exists, such that

$$\mathrm{e}(\mathscr{V}'_{\mathrm{basic}(m)}, \mu^*, \mathbf{c}^*) = \mathrm{e}(\mathscr{V}, \mu^*, \mathbf{c}^*) \qquad \text{for } m = 0, 1, \dots, r-1. \tag{7.9}$$

Remark 7.1. By Lemma 5.2 (b), a stronger form of the condition (7.8) is required in order for the entropy gap condition to hold, and so in practice this assumption is not at all restrictive. The equations to be satisfied are, written out in full,

$$\sum_{j=m+1}^{r} (c_j^* - c_{j+1}^*)\mathbb{H}_{\mu_j^*}(V_m) = \sum_{j=m+1}^{r} c_j^* \dim(V_j/V_{j-1}) \qquad m = 0, 1, \dots, r-1. \tag{7.10}$$

[3]Note that we have not said that the ρ_i are unique. However, in cases of interest to us this will turn out to be the case.

By (7.8), there are constants $\lambda_{j,\mathscr{V},\mu^*}$ such that if $c^*_{r+1} = t$ then, computing in turn using (7.10) for $m = r-1, \cdots, 0$, we get $c^*_r = \lambda_{r,\mathscr{V}} t, \cdots, c^*_1 = \lambda_{1,\mathscr{V}} t$. Thus the optimal parameters exist if and only if $\lambda_{1,\mathscr{V}} > \cdots > \lambda_{r,\mathscr{V}} > 0$, and in this case we should take $t := \lambda^{-1}_{1,\mathscr{V}}$.

We conclude this subsection with a characterization of the optimal measure μ^* and parameters $\mathbf{c}^*$. Given an r-step flag $\mathscr{V}$, there is an associated rooted tree $\mathscr{T}(\mathscr{V})$, which captures the structure of the cells at different levels $0, \dots, r-1$. In particular, this tree always has exactly $2^k - 1$ leaves at level 0, corresponding to the cell $\Gamma_0 = \{\mathbf{0}, \mathbf{1}\}$ and the singletons $\{\omega\}$ for each $\omega \in \{0,1\}^k \setminus \{\mathbf{0}, \mathbf{1}\}$.

Lemma 7.6. *The optimal constant $\gamma^{res}_k(\mathscr{V})$, associated measures $\mu^*_i(C)$ and optimal parameters c^*_i depend only on the tree $\mathscr{T}(\mathscr{V})$ and the sequence of dimensions $\dim(V_j)$, $0 \leqslant j \leqslant r$.*

Proof. Let $\mathscr{V}$ and $\widetilde{\mathscr{V}}$ be different flags with the same tree structure, that is, $\mathscr{T}(\mathscr{V})$ is isomorphic to $\mathscr{T}(\widetilde{\mathscr{V}})$. By an easy induction on the level and the definition of $f^C(\boldsymbol{\rho})$, if $C \in \mathscr{T}(\mathscr{V})$ and $\tilde{C} \in \mathscr{T}(\widetilde{\mathscr{V}})$ correspond, we find that $f^C(\boldsymbol{\rho}) = f^{\tilde{C}}(\boldsymbol{\rho})$. The statements now follow from Definitions 7.4 and 7.5. □

7.3. **Solution of the optimisation problem: statement**

Here is the main result of this section, which explains the introduction of the various concepts above, as well as their names.

Proposition 7.7. *Suppose that $\mathscr{V} : \mathbf{1} = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_r \leqslant \mathbb{Q}^k$, is a proper flag such that the ρ-equations have a solution. Let μ^* be the corresponding optimal measures, and suppose that the corresponding optimal parameters $\mathbf{c}^*$ exist. Then*

$$\gamma^{\mathrm{res}}_k(\mathscr{V}) = (\log 3 - 1) \Big/ \Big(\log 3 + \sum_{i=1}^{r-1} \frac{\dim(V_{i+1}/V_i)}{\rho_1 \cdots \rho_i} \Big). \tag{7.11}$$

Moreover, the optimal measures μ^* and optimal parameters $\mathbf{c}^*$ provide the solution to Problem 7.2; in particular, c^*_{r+1} is precisely the right-hand side of (7.11).

For this result to be of any use, we need methods for establishing, for flags $\mathscr{V}$ of interest, that the ρ-equations have a solution, and also that the optimal parameters exist. The former is a very delicate matter, highly dependent on the specific structure of the flags of interest. Once this is sorted out, the latter problem is less serious, at least in situations relevant to us.

7.4. **Linear forms in entropies**

In the next section we will prove Proposition 7.7. In this section we isolate some lemmas from the proof.

Let $\mathscr{V} : \langle \mathbf{1} \rangle = V_0 \leqslant \cdots \leqslant V_r \leqslant \mathbb{Q}^k$ be a flag. We use the terminology of cells C at level i, introduced at the beginning of subsection 7.2.

Lemma 7.8. *Let $\mathbf{y} = (y_0, \cdots, y_{r-1})$ be real numbers with the property that all the partial sums $y_{<i} := y_0 + \cdots + y_{i-1}$ are positive. If C is a cell (at some level i), then we write*

$$h^C(\mathbf{y}) := \sup_{\mathrm{Supp}(\mu_C) \subset C} \Big(\sum_{0 \leqslant m < r} y_m \mathbb{H}_{\mu_C}(V_m) \Big), \tag{7.12}$$

where the supremum is over all probability measures μ_C supported on C. Then the quantities $h^C(\mathbf{y})$ are completely determined by the following rules:

- *If C has level 0, then $h^C(\mathbf{y}) = 0$;*
- *If C has level i, then*

$$h^C(\mathbf{y}) = y_{<i} \log\Big(\sum_{C' \colon C \to C'} e^{h^{C'}(\mathbf{y})/y_{<i}}\Big), \tag{7.13}$$

Then, for any C, the maximum in (7.12) occurs for a unique measure $\mu^*_{C,\mathbf{y}}$. Furthermore, all of the $\mu^*_{C,\mathbf{y}}$ are restrictions of the "top" measure $\mu^*_{\mathbf{y}} := \mu^*_{\Gamma_r,\mathbf{y}}$, that is to say $\mu^*_{C,\mathbf{y}}(x) = \mu^*_{\mathbf{y}}(x)/\mu^*_{\mathbf{y}}(C)$ for all $x \in C$, and

$$\frac{\mu^*_{\mathbf{y}}(C')}{\mu^*_{\mathbf{y}}(C)} = \frac{e^{h^{C'}(\mathbf{y}/y_{<i})}}{e^{h^C(\mathbf{y}/y_{<i})}}. \tag{7.14}$$

Remark. As will be apparent from the proof, we do not use the linear structure of the cells C (that is, the fact that they come from cosets). We leave it to the reader to formulate a completely general version of this lemma in which the cells at level i are the atoms in a σ-algebra $\mathscr{F}_i$, with $\mathscr{F}_i$ being a refinement of $\mathscr{F}_{i+1}$ for all i.

Proof. Let us temporarily write $\tilde{h}^C(\mathbf{y})$ for the function defined by (7.13), thus the aim is to prove that $h^C(\mathbf{y}) = \tilde{h}^C(\mathbf{y})$. We do this by induction on i, the $i = 0$ case being trivial since, in this case, all the entropies $\mathbb{H}_{\mu_C}(V_m)$ are zero. Suppose, then, that we know the result for cells of level $i-1$.

Note that both h^C and $\tilde{h}^C$ satisfy a homogeneity property

$$\tilde{h}^C(t\mathbf{y}) = t\tilde{h}^C(\mathbf{y}), \qquad h^C(t\mathbf{y}) = th^C(\mathbf{y}).$$

This is obvious for h^C, and can be proven very easily for $\tilde{h}^C$ by induction. Therefore we may assume that $y_{<i} = 1$. This does not affect the measure $\mu^*_{\mathbf{y}}$, which does not depend on the scaling of the parameters y_m.

Suppose that C is a cell at level i. A probability measure μ_C on C is completely determined by probability measures $\mu_{C'}$ on the children C' of C (at level $i-1$) together with the probabilities $\mu_C(C')$, which must sum to 1, with the relation being that $\mu_{C'}(x) = \mu_C(x)/\mu_C(C')$ for $x \in C'$.

Suppose that $0 \leqslant m < i$. Let the random variables X, Y be random cosets of V_m, V_{i-1} respectively, sampled according to the measure μ_C. Then X determines Y and so, by Lemma B.5, $\mathbb{H}(X,Y) = \mathbb{H}(X)$. The chain rule for entropy, Lemma B.4, then yields

$$\mathbb{H}(X) = \mathbb{H}(Y) + \sum_y \mathbb{P}(Y = y)\mathbb{H}(X|Y = y).$$

Translated back to the language we are using, this implies that

$$\mathbb{H}_{\mu_C}(V_m) = \mathbb{H}_{\mu_C}(V_{i-1}) + \sum_{C'} \mu_C(C')\mathbb{H}_{\mu_{C'}}(V_m).$$

Therefore

$$\sum_{0\leqslant m<i} y_m \mathbb{H}_{\mu_C}(V_m) = \mathbb{H}_{\mu_C}(V_{i-1}) + \sum_{C'} \mu_C(C') \sum_{0\leqslant m<i} y_m \mathbb{H}_{\mu_{C'}}(V_m).$$

(Here we used our assumption that $y_{<i}=1$.) Since $\mathbb{H}_{\mu_C}(V_m)=0$ for $m\geqslant i$, and $\mathbb{H}_{\mu_{C'}}(V_m)=0$ for $m\geqslant i-1$, we may extend the sums over all $m\in\{0,1,\dots,r-1\}$ thereby obtaining

$$\sum_{0\leqslant m<r} y_m\mathbb{H}_{\mu_C}(V_m)=\mathbb{H}_{\mu_C}(V_{i-1})+\sum_{C'}\mu_C(C')\sum_{0\leqslant m<r} y_m\mathbb{H}_{\mu_{C'}}(V_m).$$

Since the $\mu_{C'}$ can be arbitrary probability measures, and $\mathbb{H}_{\mu_C}(V_{i-1})$ depends only on the value of $\mu_C(C')$, it follows from the inductive hypothesis that

$$h^C(\mathbf{y})=\sup_{\mu_C}\Big(\sum_{0\leqslant m<r} y_m\mathbb{H}_{\mu_C}(V_m)\Big) \tag{7.15}$$

$$=\sup_{\mu_C(C'),\mu_{C'}}\Big(\mathbb{H}_{\mu_C}(V_{i-1})+\sum_{C'}\mu_C(C')\sum_{0\leqslant m<r} y_m\mathbb{H}_{\mu_{C'}}(V_m)\Big) \tag{7.16}$$

$$=\sup_{\mu_C(C')}\Big(\mathbb{H}_{\mu_C}(V_{i-1})+\sum_{C'}\mu_C(C')\tilde{h}^{C'}(\mathbf{y})\Big), \tag{7.17}$$

with equality when going from (7.16) to (7.17) when $\mu_{C'}=\mu^*_{C',\mathbf{y}}$ for all C'. Applying Lemma B.3 with the p_j being the $\mu_C(C')$ and the a_j being the $\tilde{h}^{C'}(\mathbf{y})$, and noting that $\mathbb{H}_{\mu_C}(V_{i-1})=\mathbb{H}(\mathbf{p})$ (where $\mathbf{p}=(p_1,p_2,\dots)$), it follows that

$$\sup_{\mu_C(C')}\Big(\mathbb{H}_{\mu_C}(V_{i-1})+\sum_{C'}\mu_C(C')\tilde{h}^{C'}(\mathbf{y})\Big)=\log\Big(\sum_{C'\colon C\to C'} e^{\tilde{h}^{C'}(\mathbf{y})}\Big)=\tilde{h}^C(\mathbf{y}). \tag{7.18}$$

In addition, Lemma B.3 implies that equality occurs in (7.18) precisely when $p_j=e^{a_j}/\sum_i e^{a_i}$, that is to say when

$$\mu_C(C')=\frac{e^{h^C(\mathbf{y})}}{\sum_{C'\colon C\to C'} e^{h^C(\mathbf{y})}}=\frac{\mu^*_{\mathbf{y}}(C')}{\mu^*_{\mathbf{y}}(C)}.$$

(Here we used again that $y_{<i}=1$.) Recalling that $\mu_{C'}=\mu^*_{C',\mathbf{y}}$ for all C', we see that the measure μ_C for which equality occurs in (7.15) is the restriction of $\mu^*_{\mathbf{y}}=\mu^*_{\Gamma_r,\mathbf{y}}$ to C. This completes the inductive step. □

7.5. **Solution of the optimisation problem: proof**

This section is devoted to the proof of Proposition 7.7. Strictly speaking, for our main theorems we only need a lower bound on $\gamma_k^{\mathrm{res}}(\mathscr{V})$, and for this it suffices to show that c^*_{r+1} is given by the right-hand side of (7.11). This could, in principle, be phrased as a calculation, but it would look complicated and unmotivated. Instead, we present it in the way we discovered it, by showing that the RHS of (7.11) is an *upper* bound on $\gamma_k^{\mathrm{res}}(\mathscr{V})$, and then observing that equality does occur when $\mu=\mu^*$ is the optimal measure (Definition 7.4) and $\mathbf{c}=\mathbf{c}^*$ the optimal parameters (Definition 7.5). We establish this upper bound using the duality argument from linear programming and Lemma 7.8.

To ease the notation, we use the shorthand $d_i:=\dim(V_i)$ throughout this subsection. Let us, then, consider the restricted optimisation problem, namely Problem 7.2. The condition (7.2) may be rewritten as

$$\sum_{j=m+1}^{r}(c_j-c_{j+1})(\mathbb{H}_{\mu_j}(V_m)+d_m-d_j)\geqslant c_{r+1}(d_r-d_m)\qquad(0\leqslant m\leqslant r-1). \tag{7.19}$$

This holds for $m = 0, 1, \ldots, r-1$. Therefore for any choice of "dual variables" $\mathbf{y} = (y_0, y_1, \ldots, y_{r-1})$, $y_0, \cdots, y_{r-1} \geqslant 0$, we have

$$\sum_{m=0}^{r-1} y_m \sum_{j=m+1}^{r} (c_j - c_{j+1})(\mathbb{H}_{\mu_j}(V_m) + d_m - d_j) \geqslant c_{r+1} \sum_{m=0}^{r-1} y_m (d_r - d_m), \tag{7.20}$$

which, rearranging, gives

$$\sum_{j=1}^{r} (c_j - c_{j+1}) E_j(\mathbf{y}) + c_{r+1} E_{r+1}(\mathbf{y}) \geqslant c_{r+1}. \tag{7.21}$$

where

$$E_j(\mathbf{y}) := \sum_{m=0}^{j-1} y_m (\mathbb{H}_{\mu_j}(V_m) + d_m - d_j)$$

for $j = 1, \ldots, r$, and

$$E_{r+1}(\mathbf{y}) := 1 - \sum_{m=0}^{r-1} y_m (d_r - d_m).$$

Since the $c_j - c_{j+1}$, $j = 1, \ldots, r$, and c_{r+1} are nonnegative and sum to 1, this implies that

$$c_{r+1} \leqslant \min_{y_i \geqslant 0 \ \forall i} \max\{E_1(\mathbf{y}), \cdots, E_r(\mathbf{y}), E_{r+1}(\mathbf{y})\}. \tag{7.22}$$

By Lemma 7.8, this implies that

$$c_{r+1} \leqslant \min_{y_i \geqslant 0 \ \forall i} \max\{E'_1(\mathbf{y}), \cdots E'_r(\mathbf{y}), E_{r+1}(\mathbf{y})\}, \tag{7.23}$$

where

$$E'_j(\mathbf{y}) := h^{\Gamma_j}(\mathbf{y}) + \sum_{m=0}^{j-1} y_m (d_m - d_j) = \sum_{m=0}^{j-1} y_m (\mathbb{H}_{\mu^*_{\Gamma_j, \mathbf{y}}}(V_m) + d_m - d_j), \tag{7.24}$$

for $j = 1, \ldots, r$, and $\mu^*_{\Gamma_j, \mathbf{y}}$ is the measure ν supported on $\Gamma_j = V_j \cap \{0,1\}^k$ for which the sum $\sum_m y_m \mathbb{H}_\nu(V_m)$ is maximal, as defined in Lemma 7.8.

Now we specify a choice of $\mathbf{y}$. To do this, we make a change of variables, defining $\rho_i = y_{<i}/y_{<i+1}$. Note that for fixed $y_0 > 0$, choices of $y_1, \cdots, y_{r-1} > 0$ are in one-to-one correspondence with choices of $\rho_1, \cdots, \rho_{r-1}$ with $0 < \rho_i < 1$. We must then have that

$$\log f^C(\boldsymbol{\rho}) = h^C(\mathbf{y}/y_{<i}) = \frac{1}{y_{<i}} h^C(\mathbf{y}) = \frac{\rho_1 \cdots \rho_{i-1}}{y_0} h^C(\mathbf{y}) \tag{7.25}$$

for the cells C at level i, which may easily be proven by induction on the level i, using the defining equations for the h^C and f^C (see (7.13), (7.4) respectively).

Now choose the ρ_i to satisfy the ρ-equations (7.5). In virtue of (7.25), the j-th ρ-equation

$$f^{\Gamma_{j+1}}(\boldsymbol{\rho}) = (f^{\Gamma_j}(\boldsymbol{\rho}))^{\rho_j} e^{d_{j+1} - d_j}$$

with $j \in \{1, 2, \ldots, r-1\}$ is equivalent to

$$E'_j(\mathbf{y}) = E'_{j+1}(\mathbf{y}), \tag{7.26}$$

with $E'_j(\mathbf{y})$ defined as in (7.24) above.

Recall that $d_1 - d_0 = \dim(V_1/V_0) = 1$. Thus, if we choose

$$y_0 := 1\Big/\Big(\log 3 + \sum_{i=1}^{r-1} \frac{d_{i+1}-d_i}{\rho_1\cdots\rho_i}\Big),$$

a short calculation confirms that

$$E_{r+1}(\mathbf{y}) = E_1'(\mathbf{y}) = y_0(\log 3 - 1). \tag{7.27}$$

With this choice of $\mathbf{y}$ we therefore have, from (7.26) with $j = 1, \dots, r-1$, (7.27) and (7.23),

$$c_{r+1} \leqslant E_1'(\mathbf{y}) = (\log 3 - 1)\Big/\Big(\log 3 + \sum_{i=1}^{r-1} \frac{d_{i+1}-d_i}{\rho_1\cdots\rho_i}\Big). \tag{7.28}$$

In the above analysis, the μ_i and the c_i were arbitrary subject to the conditions of Problem 7.2, thus $\mathrm{Supp}(\mu_i) \subset V_i$ and $1 = c_1 > c_2 > \cdots > c_{r+1}$. Therefore, recalling the definition of $\gamma_k^{\mathrm{res}}(\mathscr{V})$ (see Problem 7.2), we have proven that

$$\gamma_k(\mathscr{V}) \leqslant \gamma_k^{\mathrm{res}}(\mathscr{V}) \leqslant (\log 3 - 1)\Big/\Big(\log 3 + \sum_{i=1}^{r-1} \frac{d_{i+1}-d_i}{\rho_1\cdots\rho_i}\Big).$$

Proposition 7.7 asserts that equality occurs in this bound when $c_j = c_j^*$ and $\mu_j = \mu_j^*$, where $\mathbf{c}^* = (c_1^*, \cdots, c_{r+1}^*)$ are the optimal parameters defined in Definition 7.5, and μ^* and its restrictions μ_j^* are the optimal measures defined in Definition 7.4. To establish this, we must go back through the argument showing that equality occurs at every stage with these choices.

First note that (7.19) is equivalent (as we stated at the time) to $\mathrm{e}(\mathscr{V}'_{\mathrm{basic}(m)}, \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$. The fact that equality occurs here when $\mathbf{c} = \mathbf{c}^*$ and $\boldsymbol{\mu} = \boldsymbol{\mu}^*$ is essentially the definition of the optimal parameters $\mathbf{c}^*$ (Definition 7.5). That equality occurs in (7.20) and (7.21) is then automatic.

Working from the other end of the proof, the choice of $\mathbf{y}$ was made so that $E_1'(\mathbf{y}) = \cdots = E_r'(\mathbf{y}) = E_{r+1}(\mathbf{y})$. We claim that, with this choice of $\mathbf{y}$,

$$\mu^* = \mu^*_{\mathbf{y}}. \tag{7.29}$$

By (7.14), it suffices to check that

$$\frac{\mu^*(C')}{\mu^*(C)} = \frac{e^{h^{C'}(\mathbf{y}/y_{<i})}}{e^{h^{C}(\mathbf{y}/y_{<i})}}.$$

This follows immediately from (7.6) and (7.25).

Since μ_j^* is defined to be the restriction of μ^* to Γ_j, it follows from (7.29) that $\mu_j^* = \mu^*_{\Gamma_j,\mathbf{y}}$, and hence that $E_j(\mathbf{y}) = E_j'(\mathbf{y})$ for $j = 1, \dots, r$.

Thus all $2r+1$ of the quantities $E_j'(\mathbf{y})$ $(j = 1, \dots, r)$ and $E_j(\mathbf{y})$ $(j = 1, \dots, r+1)$ are equal. It follows from this and the fact that equality occurs in (7.21) that equality occurs in (7.22), (7.23) and (7.28) as well. This concludes the proof of Proposition 7.7. □

8. The strict entropy condition

8.1. Introduction

Fix an r-step flag $\mathscr{V}$. In the previous section, we studied a restricted optimization problem (Problem 7.2) asking for the supremum of c_{r+1} when ranging over all systems $(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ satisfying

the "restricted entropy condition"

$$\mathrm{e}(\mathscr{V}'_{\mathrm{basic}(m)}, \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) \qquad (m = 0, 1, \dots, r-1). \tag{8.1}$$

The aim of the present section is two-fold: we wish to establish, under general conditions, that an "optimal system" with respect to (8.1) satisfies the more general entropy condition

$$\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) \geqslant \mathrm{e}(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu}) \qquad (\text{all } \mathscr{V}' \leqslant \mathscr{V}). \tag{8.2}$$

In addition, we want to show that if we slightly perturb such a system, we may guarantee a version of (8.2) with strict inequalities for all proper subflags $\mathscr{V}'$ of $\mathscr{V}$.

Before stating our result, we need to define the notion of the automorphism group of a flag.

Definition 8.1 (Automorphism group)**.** For a permutation $\sigma \in S_k$ and $\omega = (\omega_1, \dots, \omega_k) \in \mathbb{Q}^k$, denote by $\sigma\omega$ the usual coordinate permutation action $\sigma\omega = (\omega_{\sigma(1)}, \dots, \omega_{\sigma(k)})$. The *automorphism group* $\mathrm{Aut}(\mathscr{V})$ is the group of all σ that satisfy $\sigma V_i = V_i$ for all i.

Proposition 8.2. *Let $\mathscr{V}$ be an r-step, nondegenrate flag of distinct spaces. Assume that the ρ-equations (7.5) have a solution, and define the optimal measures $\boldsymbol{\mu}^*$ on $\{0,1\}^k$ as in Definition 7.4. Furthermore, assume that:*

(a) *no intermediate subspace is fixed by $\mathrm{Aut}(\mathscr{V})$, that is to say there is no space W that is invariant under the action of $\mathrm{Aut}(\mathscr{V})$ and such that $V_{i-1} < W < V_i$ (the inclusions being strict);*
(b) *the optimal parameters $\mathbf{c}^*$ exist, that is to say the system of equations (7.10) has a unique solution $\mathbf{c}^*$ satisfying $1 = c_1^* > c_2^* > \cdots > c_{r+1}^*$;*
(c) *the following "positivity inequalities" hold:*
  (i) $\mathbb{H}_{\mu^*_{m+1}}(V_m) > \dim(V_{m+1}/V_m)$ *for* $0 \leqslant m \leqslant r-1$;
  (ii) $\mathbb{H}_{\mu^*_i}(V_{m-1}) - \mathbb{H}_{\mu^*_i}(V_m) < \dim(V_m/V_{m-1})$ *for* $1 \leqslant m < i \leqslant r$.

Then there are arbitrarily small perturbations $\tilde{\mathbf{c}}$ of $\mathbf{c}^*$ such that $1 = \tilde{c}_1 > \tilde{c}_2 > \cdots > \tilde{c}_{r+1}$ and such that we have the strict entropy condition

$$\mathrm{e}(\mathscr{V}', \tilde{\mathbf{c}}, \boldsymbol{\mu}^*) > \mathrm{e}(\mathscr{V}, \tilde{\mathbf{c}}, \boldsymbol{\mu}^*) \qquad \textit{for all proper subflags } \mathscr{V}' \leqslant \mathscr{V}. \tag{8.3}$$

We assume throughout the rest of the section that (a), (b) and (c) of Proposition 8.2 are satisfied, and we now fix the system $(\mathscr{V}, \mathbf{c}^*, \boldsymbol{\mu}^*)$. For notational brevity in what follows, we write

$$\mathrm{e}(\mathscr{V}') := \mathrm{e}(\mathscr{V}', \mathbf{c}^*, \boldsymbol{\mu}^*).$$

Our strategy is as follows. First, we show the weaker "unperturbed" statement that

$$\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V}) \qquad \text{for all subflags } \mathscr{V}' \leqslant \mathscr{V}, \tag{8.4}$$

noting that we have strict inequality for certain subflags $\mathscr{V}'$ along the way. Then, in subsection 8.8, we show how to perturb $\mathbf{c}^*$ to $\tilde{\mathbf{c}}$ so that the strict inequality (8.3) is satisfied. We also sketch a second way of effecting the perturbation which is in a sense more robust, but which in essence requires a perturbation of the whole proof of (8.4).

8.2. **Analysis of non-basic flags**

We turn now to the task of proving (8.4). We will prove it for progressively wider sets of subflags $\mathscr{V}'$, each time using the previous statement. In order, we will prove it for subflags $\mathscr{V}'$ which we call:

(a) *semi-basic*: flags $V_1 \leqslant V_2 \leqslant \cdots \leqslant V_{m-1} \leqslant V_{m-1} \leqslant \cdots \leqslant V_m \leqslant \cdots \leqslant V_m$ with $m \geqslant 1$ (that is, $\mathscr{V}'$ is like a basic flag, but there can be more than one copy of V_{m-1});
(b) *standard*: each V_i' is one of the spaces V_j;
(c) *invariant*: this means that $\sigma V_i' = V_i'$ for all automorphisms $\sigma \in \mathrm{Aut}(\mathscr{V})$ and all i;
(d) general subflags, i.e. we assume no restriction on the V_i' other than that $V_i' \leqslant V_i$.

Note that a semi-basic flag is standard, a standard flag is invariant, and of course an invariant flag is general.

We introduce some notation for standard flags. Let $J \subset \mathbb{N}_0^r$ be the set of all r-tuples $\boldsymbol{j} = (j_1, \cdots, j_r)$ such that $j_1 \leqslant \cdots \leqslant j_r$ and $j_i \leqslant i$ for all i. Then we define the flag $\mathscr{V}'_{\boldsymbol{j}} = \mathscr{V}'_{(j_1,\dots,j_r)}$ to be the one with $V_i' = V_{j_i}$. This is a standard flag, and conversely every standard flag is of this form. If we define

$$\mathrm{basic}(m) := (1, 2, \dots, m-1, m, \dots, m)$$

then $\mathrm{basic}(m) \in J$, and $\mathscr{V}'_{\mathrm{basic}(m)}$ agrees with our previous notation.

8.3. **Semi-basic subflags**

In this subsection we prove the following result, establishing that (8.4) holds for semi-basic subflags, and with strict inequality for those which are not basic.

Lemma 8.3. *(Assuming that (a), (b) and (c) of Proposition 8.2 hold) we have* $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$ *for all non-basic, semi-basic flags* $\mathscr{V}'$.

We begin by setting a small amount of notation for semi-basic flags. We note that the idea of a semi-basic flag, which looks rather *ad hoc*, will only be used here and in subsection 8.5.

Definition 8.4 (Semi-basic flags that are not basic)**.** Suppose that $1 \leqslant m \leqslant r-1$ and that $m \leqslant s \leqslant r-1$. Then we define the element $\mathrm{semi}(m,s) \in J$ to be $\boldsymbol{j} = (1, 2, \dots, m-1, m-1, \dots, m, \dots, m)$ such that $j_i = i$ for $i \leqslant m-1$, $j_i = m-1$ for $m \leqslant i \leqslant s$ and $j_i = m$ for $i > s$.

It is convenient and natural to extend the notation to $s = m-1$ and $s = r$, by defining

$$\mathrm{semi}(m, r) = \mathrm{basic}(m-1), \qquad \mathrm{semi}(m, m-1) = \mathrm{basic}(m). \tag{8.5}$$

One can think of the semi-basic flags as interpolating between the basic flags.

Example. When $r = 3$ there are three semi-basic flags $\mathscr{V}_{\boldsymbol{j}}$ that are not basic, corresponding to

$$\begin{aligned} \boldsymbol{j} &= \mathrm{semi}(1,1) = (0,1,1), \\ \boldsymbol{j} &= \mathrm{semi}(1,2) = (0,0,1), \\ \boldsymbol{j} &= \mathrm{semi}(2,2) = (1,1,2). \end{aligned}$$

Proof of Lemma 8.3. Assume that $\mathscr{V}'$ is semi-basic but not basic. We will show that

$$\mathrm{e}(\mathscr{V}'_{\mathrm{semi}(m,s)}) > \mathrm{e}(\mathscr{V}'_{\mathrm{semi}(m,s+1)}) \tag{8.6}$$

for $m \leqslant s \leqslant r-1$. Since $\mathscr{V}'_{\mathrm{semi}(m,r)} = \mathscr{V}'_{\mathrm{basic}(m-1)}$ is basic, this establishes Lemma 8.3.

To prove (8.6), we simply compute that

$$\mathrm{e}(\mathscr{V}'_{\mathrm{semi}(m,s)}) - \mathrm{e}(\mathscr{V}'_{\mathrm{semi}(m,s+1)}) = (c^*_{s+1} - c^*_{s+2})\big[\mathbb{H}_{\mu_{s+1}}(V_m) - \mathbb{H}_{\mu_{s+1}}(V_{m-1}) + \dim(V_m/V_{m-1})\big]$$

when $m \leqslant s \leqslant r-2$, and

$$\mathrm{e}(\mathscr{V}'_{\mathrm{semi}(m,r-1)}) - \mathrm{e}(\mathscr{V}'_{\mathrm{semi}(m,r)}) = (c_r^* - c_{r+1}^*)\big[\mathbb{H}_{\mu_r}(V_m) - \mathbb{H}_{\mu_r}(V_{m-1}) + \dim(V_m/V_{m-1})\big] + \dim(V_m/V_{m-1})c_{r+1}^*.$$

In both cases, the result follows from condition (c) (ii) of Proposition 8.2. □

8.4. **Submodularity inequalities**

To proceed further, we make heavy use of a submodularity property of the expressions $\mathrm{e}()$.

Suppose that $\mathscr{V}', \tilde{\mathscr{V}}'$ are two subflags of $\mathscr{V}$. We can define the *sum* $\mathscr{V}' + \tilde{\mathscr{V}}'$ and *intersection* $\mathscr{V}' \cap \tilde{\mathscr{V}}'$ by

$$(\mathscr{V}' + \tilde{\mathscr{V}}')_i := V_i' + \tilde{V}_i'$$

and

$$(\mathscr{V}' \cap \tilde{\mathscr{V}}')_i := V_i' \cap \tilde{V}_i'.$$

Both of these are indeed subflags of $\mathscr{V}$.

Lemma 8.5. *We have*

$$\mathrm{e}(\mathscr{V}') + \mathrm{e}(\tilde{\mathscr{V}}') \geqslant \mathrm{e}(\mathscr{V}' + \tilde{\mathscr{V}}') + \mathrm{e}(\mathscr{V}' \cap \tilde{\mathscr{V}}').$$

Proof. We first note that the entropies $\mathbb{H}_\mu(W)$ satisfy a submodularity inequality. Namely, if W_1, W_2 are subspaces of $\mathbb{Q}^k$ and μ is a probability measure then

$$\mathbb{H}_\mu(W_1) + \mathbb{H}_\mu(W_2) \geqslant \mathbb{H}_\mu(W_1 \cap W_2) + \mathbb{H}_\mu(W_1 + W_2). \tag{8.7}$$

To prove this, consider the following three random variables:

- X is a random coset of $W_1 + W_2$, sampled according to the measure μ;
- Y is a random coset of W_1, sampled according to the measure μ;
- Z is a random coset of W_2, sampled according to the measure μ.

Then, more-or-less by definition,

$$\mathbb{H}(X) = \mathbb{H}_\mu(W_1 + W_2), \quad \mathbb{H}(Y) = \mathbb{H}_\mu(W_1), \quad \mathbb{H}(Z) = \mathbb{H}_\mu(W_2).$$

Note also that Y determines X and so $\mathbb{H}(Y) = \mathbb{H}(X, Y)$, and similarly $\mathbb{H}(Z) = \mathbb{H}(X, Z)$. Finally, (Y, Z) uniquely defines a random coset of $W_1 \cap W_2$, and so

$$\mathbb{H}_\mu(W_1 \cap W_2) = \mathbb{H}(Y, Z) = \mathbb{H}(X, Y, Z).$$

The inequality to be proven, (8.7) is therefore equivalent to

$$\mathbb{H}(X, Y) + \mathbb{H}(X, Z) \geqslant \mathbb{H}(X, Y, Z) + \mathbb{H}(X),$$

which is a standard entropy inequality (Lemma B.6; usually known as "submodularity of entropy" or "Shannon's inequality" in the literature).

Lemma 8.5 is essentially an immediate consequence of (8.7) and the formula

$$\dim(W_1) + \dim(W_2) = \dim(W_1 \cap W_2) + \dim(W_1 + W_2).$$

(It is very important that this formula holds with *equality*, as compared to (8.7), which holds only with an inequality.) □

This has the following immediate corollary when applied to standard subflags. Here, the $\max$ and $\min$ are taken coordinatewise.

Corollary 8.6. *Suppose that $\boldsymbol{j}_1, \boldsymbol{j}_2 \in J$. Then*

$$\mathrm{e}(\mathscr{V}'_{\boldsymbol{j}_1}) + \mathrm{e}(\mathscr{V}'_{\boldsymbol{j}_2}) \geqslant \mathrm{e}(\mathscr{V}'_{\max(\boldsymbol{j}_1,\boldsymbol{j}_2)}) + \mathrm{e}(\mathscr{V}'_{\min(\boldsymbol{j}_1,\boldsymbol{j}_2)})$$

8.5. **Standard subflags**

Now we extend the result of the subsection 8.3 to all standard subflags.

Lemma 8.7. *(Assuming that (a), (b) and (c) of Proposition 8.2 hold) we have $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$ for all standard, non-basic subflags $\mathscr{V}' \leqslant \mathscr{V}$.*

Proof. Let $\boldsymbol{j} \in J$ with $\boldsymbol{j}$ non-basic, and let $\mathscr{V}' = \mathscr{V}'_{\boldsymbol{j}}$. Then $r \geqslant 3$, since when $r \leqslant 2$ all standard flags are basic. We proceed by induction on $\|\boldsymbol{j}\|_\infty$, the case $\|\boldsymbol{j}\|_\infty = 1$ being trivial, since then $\mathscr{V}$ is semibasic and we invoke may Lemma 8.3. Now suppose we have proved $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$ for all non-basic standard flags $\mathscr{V}' = \mathscr{V}'_{\boldsymbol{j}}$ with $\|\boldsymbol{j}\|_\infty < m$, and let $\boldsymbol{j} \in J$ with $\|\boldsymbol{j}\|_\infty = m$. We apply Corollary 8.6 with $\boldsymbol{j}_1 = \boldsymbol{j}$ and $\boldsymbol{j}_2 = \mathrm{basic}(j_r - 1)$. Noting that $\max(\boldsymbol{j}, \mathrm{basic}(j_r - 1)) = \mathrm{semi}(j_r, s)$, where s is the largest index in $\boldsymbol{j}$ such that $j_s < j_r$, we see that

$$\mathrm{e}(\mathscr{V}'_{\boldsymbol{j}}) + \mathrm{e}(\mathscr{V}'_{\mathrm{basic}(j_r-1)}) \geqslant \mathrm{e}(\mathscr{V}'_{\boldsymbol{j}_*}) + \mathrm{e}(\mathscr{V}'_{\mathrm{semi}(j_r,s)}). \tag{8.8}$$

where

$$\boldsymbol{j}_* := \min(\boldsymbol{j}, \mathrm{basic}(j_r - 1)).$$

Suppose that both of the flags on the right of (8.8) are basic. If $\mathrm{semi}(j_r, s)$ is basic then it must be $\mathrm{basic}(j_r)$, which means that $s = j_r - 1$. But then $\boldsymbol{j}_* = (j_1, \dots, j_s, j_r - 1, \cdots j_r - 1)$ which, if it is basic, must be $\mathrm{basic}(j_r - 1)$; this then implies that $j_i = i$ for $1 \leqslant i \leqslant s$, and hence that $\boldsymbol{j} = \mathrm{basic}(j_r)$, a contradiction. Thus, at least one of the two flags $\boldsymbol{j}_*, \mathrm{semi}(j_r, s)$ on the right of (8.8) is not basic. Since $\|\boldsymbol{j}_*\|_\infty < \|\boldsymbol{j}\|_\infty = m$, the induction hypothesis together with Lemma 8.3 implies that $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$, as desired. □

8.6. **Invariant subflags**

Now we extend our results to all invariant flags, but now without the strict inequality.

Lemma 8.8. *(Assuming that (a), (b) and (c) of Proposition 8.2 hold) we have $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V})$ for all invariant subflags $\mathscr{V}' \leqslant \mathscr{V}$.*

Proof. We associate a pair (i, ℓ), $i \geqslant \ell$, of positive integers to $\mathscr{V}'$, which we call the *signature*, in the following manner. If $\mathscr{V}'$ is standard, then set $(i, \ell) = (-1, -1)$. Otherwise, let i be maximal so that V'_i is not a standard space V_t, and then let ℓ be minimal such that $V'_i \leqslant V_\ell$. The fact that $\ell \leqslant i$ is immediate from the definition of a subflag. We put an ordering on signatures as follows: $(i', \ell') \preceq (i, \ell)$ iff $i' < i$, or if $i' = i$ and $\ell' \leqslant \ell$. We proceed by induction on the pair (i, ℓ) with respect to this ordering, the case $(i, \ell) = (-1, -1)$ handled by Lemma 8.7.

For the inductive step, suppose $\mathscr{V}'$ is nonstandard with signature (i, ℓ). By submodularity,

$$\mathrm{e}(\mathscr{V}') + \mathrm{e}(\mathscr{V}'_{\mathrm{basic}(\ell-1)}) \geqslant \mathrm{e}(\mathscr{V}_1) + \mathrm{e}(\mathscr{V}_2), \tag{8.9}$$

where

$$\mathscr{V}_1 = \mathscr{V}' \cap \mathscr{V}'_{\mathrm{basic}(\ell-1)}, \qquad \mathscr{V}_2 = \mathscr{V}' + \mathscr{V}'_{\mathrm{basic}(\ell-1)}.$$

Suppose that $\mathscr{V}_1, \mathscr{V}_2$ have signatures $(i_1, \ell_1), (i_2, \ell_2)$, respectively. We show that

$$(i_1, \ell_1) \precneqq (i, \ell) \quad \text{and} \quad (i_2, \ell_2) \precneqq (i, \ell). \tag{8.10}$$

Both $\mathscr{V}_1$ and $\mathscr{V}_2$ are invariant flags Thus, if (8.10) holds, then both flags on the right-hand side of (8.9) have strictly smaller signature than $\mathscr{V}'$, and the lemma follows by induction.

Finally, we prove (8.10). Note that if $j > i$, then V_j' is a standard space V_m and thus so are $(\mathscr{V}_1)_j$ and $(\mathscr{V}_2)_j$. In particular, $i_1 \leqslant i$ and $i_2 \leqslant i$. We have that $(\mathscr{V}_2)_i$ contains $V_{\ell-1}$, is not equal to $V_{\ell-1}$, and is contained in V_ℓ. But $(\mathscr{V}_2)_i$ is invariant, and hence by our assumption that (a) of Proposition 8.2 holds, $(\mathscr{V}_2)_i = V_\ell$. Consequently, $i_2 < i$ if $\mathscr{V}_2$ is nonstandard. In the case that $\mathscr{V}_1$ is nonstandard, we also have that $\ell_1 < \ell$ because every space in the flag $\mathscr{V}_1$ is contained in $V_{\ell-1}$. This proves (8.10). □

8.7. **General subflags**

In this section we establish (8.4), that is to say the inequality $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V})$ for *all* subflags $\mathscr{V}'$, of course subject to our standing assumption that (a), (b) and (c) of Proposition 8.2 hold. We need a simple lemma about the action of the automorphism group $\mathrm{Aut}(\mathscr{V})$ on subflags.

Lemma 8.9. *Let $\sigma \in \mathrm{Aut}(\mathscr{V})$ and let $\mathscr{V}'$ be a subflag of $\mathscr{V}$. Then one may define a new subflag $\sigma(\mathscr{V}')$, setting $\sigma(\mathscr{V}')_i := \sigma(V_i')$. Moreover, $\mathrm{e}(\sigma(\mathscr{V}')) = \mathrm{e}(\mathscr{V}')$.*

Proof. Since $\mathscr{V}'$ is a subflag, $V_i' \leqslant V_i$. Applying σ, and recalling that V_i is invariant under σ, we see that $\sigma(V_i') \leqslant V_i$. Therefore $\sigma(\mathscr{V}')$ is also a subflag. To see that $\mathrm{e}(\sigma(\mathscr{V}')) = \mathrm{e}(\mathscr{V}')$, recall Lemma 7.6, which implies that μ_i is invariant under σ, since the trees $\mathscr{T}(\mathscr{V}')$ and $\mathscr{T}(\sigma(\mathscr{V}'))$ are isomorphic. It follows that, for any subspace $W \leqslant \mathbb{Q}^k$,

$$\begin{aligned}\mathbb{H}_{\mu_i}(\sigma(W)) &= -\sum_x \mu_i(x) \log \mu_i(\sigma(W) + x) \\ &= -\sum_y \mu_i(\sigma(y)) \log \mu_i(\sigma(W + y)) \\ &= -\sum_y \mu_i(y) \log \mu_i(W + y) \\ &= \mathbb{H}_{\mu_i}(W).\end{aligned}$$

This completes the proof of the lemma. □

Proof of (8.4). Let m be the minimum of $\mathrm{e}(\mathscr{V}')$ over all subflags $\mathscr{V}' \leqslant \mathscr{V}$, and among the flags with $\mathrm{e}(\mathscr{V}') = m$, take the one with $\sum_i \dim V_i'$ minimal. Let $\sigma \in \mathrm{Aut}(\mathscr{V})$ be an arbitrary automorphism. By Lemma 8.9, $\mathrm{e}(\mathscr{V}') = \mathrm{e}(\sigma(\mathscr{V}'))$, and hence submodularity implies that

$$2\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V}' + \sigma(\mathscr{V}')) + \mathrm{e}(\mathscr{V}' \cap \sigma(\mathscr{V}')). \tag{8.11}$$

In particular, we have $\mathrm{e}(\mathscr{V} \cap \sigma(\mathscr{V}')) = m$ (and also $\mathrm{e}(\mathscr{V}' + \sigma(\mathscr{V}')) = \mathrm{e}(\mathscr{V})$, but we will not need this). Moreover, by the minimality of $\sum_i \dim V_i'$,

$$\sum_i \dim(V_i' \cap \sigma(V_i')) = \sum_i \dim V_i',$$

which means that $\mathscr{V}'$ is invariant. Invoking Lemma 8.8, we conclude that $m \geqslant \mathrm{e}(\mathscr{V})$. □

8.8. **The strict entropy condition**

In this section we complete the proof of Proposition 8.2 by showing how to perturb (8.4) to the desired strict inequality (8.3).

First argument. Consider first the collection $\mathcal{U}$ of all subflags $\mathscr{V}'$ which satisfy, for some $1 \leqslant j \leqslant r-1$, the relations

$$V_i' = V_i \ \ (i \neq j), \quad V_{j-1} \leqslant V_{j'} < V_j.$$

These are flags which differ from $\mathscr{V}$ in exactly one space. Our first task will be to establish the *strict* inequality

$$\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V}) \tag{8.12}$$

for all $\mathscr{V}' \in \mathcal{U}$, by elaborating upon the argument of the previous subsection. We already know that $\mathrm{e}(\mathscr{V}') \geqslant \mathrm{e}(\mathscr{V})$, so suppose as a hypothesis for contradiction that $\mathrm{e}(\mathscr{V}') = \mathrm{e}(\mathscr{V})$ for some $\mathscr{V}' \in \mathcal{U}$. Amongst all such flags, take one with minimal $\sum \dim(V_i')$. By submodularity, we have (8.11) and hence $\mathrm{e}(\mathscr{V}' \cap \sigma(\mathscr{V}')) = \mathrm{e}(\mathscr{V})$ for any automorphism $\sigma \in \mathrm{Aut}(\mathscr{V})$. But

$$\mathscr{V}' \cap \sigma(\mathscr{V}') = (V_1, \dots, V_{j-1}, V_j' \cap \sigma(V_j'), V_{j+1}, \dots, V_r)$$

is evidently in $\mathcal{U}$ as well, and by our minimality assumption it follows that $\dim(V_j' \cap \sigma(V_j')) = \dim(V_j')$. Thus, $\mathscr{V}'$ is invariant, and by assumption (a) of Proposition 8.2, it follows that $V_j' = V_{j-1}$. Thus, $\mathscr{V}'$ is a standard flag, which is not basic since $j \leqslant r-1$. Hence, $\mathrm{e}(\mathscr{V}') > \mathrm{e}(\mathscr{V})$ by Lemma 8.7. This contradition establishes (8.12).

Let $1 \leqslant j \leqslant r-1$ and let V be a space satisfying $V_{j-1} \leqslant V < V_j$. Let $\mathscr{V}'$ be the subflag $\langle \mathbf{1} \rangle = V_0 \leqslant \dots V_{j-1} \leqslant V \leqslant V_{j+1} \leqslant \dots \leqslant V_r$. Then one easily computes that

$$\mathrm{e}(\mathscr{V}') - \mathrm{e}(\mathscr{V}) = (c_j - c_{j+1})\big(\mathbb{H}_{\mu_j}(V) - \dim(V_j/V)\big),$$

and so (8.12) implies that

$$\mathbb{H}_{\mu_j}(V) > \dim(V_j/V). \tag{8.13}$$

Now let $\varepsilon > 0$ be sufficiently small and consider the pertubation $\tilde{\mathbf{c}}$ given by

$$\tilde{c}_1 = 1, \quad \tilde{c}_j = c_j^* - \frac{1}{2}\sum_{\ell=1}^{j-1} \varepsilon^\ell \quad (2 \leqslant j \leqslant r+1).$$

Evidently, $1 = \tilde{c}_1 > \tilde{c}_2 > \dots > \tilde{c}_{r+1} \geqslant c_{r+1}^* - \varepsilon$. For any proper subflag $\mathscr{V}' \leqslant \mathscr{V}$, we compute

$$\begin{aligned}
&\mathrm{e}(\mathscr{V}', \tilde{\mathbf{c}}, \boldsymbol{\mu}^*) - \mathrm{e}(\mathscr{V}, \tilde{\mathbf{c}}, \boldsymbol{\mu}^*) \\
&= \mathrm{e}(\mathscr{V}') - \mathrm{e}(\mathscr{V}) + \frac{1}{2}\sum_{j=1}^{r} \varepsilon^j \big(\mathbb{H}_{\mu_j}(V_j') - \dim(V_j/V_j')\big) + \frac{1}{2}(\varepsilon + \varepsilon^2 + \dots + \varepsilon^{r-1}) \dim(V_r/V_r').
\end{aligned}$$

Let $J = \min\{j : V_j' \neq V_j\}$. If $J = r$, then $\dim(V_r/V_r') \geqslant 1$ and the right side above is at least $\varepsilon/2 + O(\varepsilon^r)$, which is positive for small enough ε. If $J \leqslant r-1$, then $V_{J-1} \leqslant V_J' < V_J$ and we see that the right side above is at least

$$\mathrm{e}(\mathscr{V}') - \mathrm{e}(\mathscr{V}) + \varepsilon^J \big(\mathbb{H}_{\mu_J}(V_J') - \dim(V_J/V_J')\big) + O(\varepsilon^{J+1}),$$

which is also positive for sufficiently small ε by (8.4) and (8.12).

Second argument. We now sketch a second approach to the proof of Proposition 8.2. The idea is to introduce a small perturbation of our fundamental quantity $\mathrm{e}()$, namely

$$\mathrm{e}_\lambda(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) := \lambda \sum_{j=1}^{r} (c_{j+1} - c_j)\mathbb{H}_{\mu_j}(V_j') + \sum_{j=1}^{r} c_j \dim(V_j'/V_{j-1}'),$$

where $\lambda \approx 1$. Note that $\mathrm{e}_1(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}) = \mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu})$, and also that $\mathrm{e}_\lambda(\mathscr{V}, \mathbf{c}, \boldsymbol{\mu})$ does not depend on λ, since all the entropies $\mathbb{H}_{\mu_j}(V_j)$ vanish. Define the λ-perturbed optimal parameters $\mathbf{c}^*(\lambda)$,

$1 = c_1^*(\lambda) > c_2^*(\lambda) > \cdots > c_{r+1}^*(\lambda)$ to be the unique solution to the λ-perturbed version of (7.9), that is to say the equations $\mathrm{e}_\lambda(\mathscr{V}'_{\mathrm{basic}(m)}, \mathbf{c}^*(\lambda), \boldsymbol{\mu}) = \mathrm{e}_\lambda(\mathscr{V}, \mathbf{c}^*(\lambda), \boldsymbol{\mu})$, $m = 0, 1, \dots, r-1$. By a continuity argument these exist for λ sufficiently close to 1 and that $\lim_{\lambda\to 1} \mathbf{c}^*(\lambda) = \mathbf{c}^*(1) = \mathbf{c}^*$.

Now observe that the proof of (8.4) holds verbatim for these λ-perturbed quantities, allowing one to conclude that

$$\mathrm{e}_\lambda(\mathscr{V}', \mathbf{c}^*(\lambda), \boldsymbol{\mu}) \geqslant \mathrm{e}_\lambda(\mathscr{V}, \mathbf{c}^*(\lambda), \boldsymbol{\mu})$$

for all subflags $\mathscr{V}'$ of $\mathscr{V}$.

Now suppose that $\lambda < 1$. Then we have

$$\mathrm{e}(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}^*) \geqslant \mathrm{e}_\lambda(\mathscr{V}', \mathbf{c}, \boldsymbol{\mu}^*),$$

with equality if and only if $\mathscr{V}' = \mathscr{V}$. Therefore if $\mathscr{V}'$ is a proper subflag of $\mathscr{V}$ we have

$$\mathrm{e}(\mathscr{V}', \mathbf{c}^*(\lambda), \boldsymbol{\mu}^*) > \mathrm{e}_\lambda(\mathscr{V}', \mathbf{c}^*(\lambda), \boldsymbol{\mu}^*) \geqslant \mathrm{e}_\lambda(\mathscr{V}, \mathbf{c}^*(\lambda), \boldsymbol{\mu}^*) = \mathrm{e}(\mathscr{V}, \mathbf{c}^*(\lambda), \boldsymbol{\mu}^*).$$

Taking $\tilde{\mathbf{c}} = \mathbf{c}^*(\lambda)$ for λ sufficiently close to 1, Proposition 8.2 follows.

PART IV. BINARY SYSTEMS

9. BINARY SYSTEMS AND A LOWER BOUND FOR β_k

In this section we define certain special flags $\mathscr{V}$ on $\mathbb{Q}^k$, $k = 2^r$, which we call the *binary systems of order* r. It is these systems which lead to the lower bound on β_k given in Theorem 2, which is one of the main results of the paper.

In this section we will define these flags (which is easy) and state their basic properties. The proofs of these properties, some of which are quite lengthy, are deferred to Section 10.

We are then in a position to prove part of one of our main theorems, Theorem 2 (a), which we do in subsection 9.2.

9.1. Binary flags and systems: definitions and properties

Definition 9.1 (Binary flag of order r)**.** 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 $\mathscr{V}$, $\langle \mathbf{1} \rangle = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_r = \mathbb{Q}^{\mathcal{P}[r]}$, as follows: V_i is the subspace of all $(x_S)_{S \subset [r]}$ for which $x_S = x_{S \cap [i]}$ for all $S \subset [r]$.

Remark. We have $\dim(V_i) = 2^i$, and $V_r = \mathbb{Q}^{\mathcal{P}[r]}$, so the system is trivially nondegenerate. Note that we have been using the letter r to denote the number of V_i in the flag $\mathscr{V}$, throughout the paper. It just so happens that, in this example, this is the same r as in the definition of $k = 2^r$.

One major task is to show that optimal measures and optimal parameters, as described in Section 7, may be defined on the binary flags. Since we will be seeing them so often, let us write down the ρ-equations (7.5) for the binary flags explicitly:

$$f^{\Gamma_{j+1}}(\boldsymbol{\rho}) = f^{\Gamma_j}(\boldsymbol{\rho})^{\rho_j} e^{2^j}, \quad j = 1, 2, \dots. \tag{9.1}$$

Proposition 9.2. *Let $\mathscr{V}$ be the binary flag of order r. Then*

(a) *the ρ-equations (9.1) have a solution with $0 < \rho_i < 1$ for $i \geqslant 1$, and consequently we may define the optimal measures $\boldsymbol{\mu}^*$ on $\{0,1\}^k$ as in Definition 7.4;*
(b) *the optimal parameters $\mathbf{c}^*$ (in the sense of Definition 7.5) exist.*

We call the binary flag $\mathscr{V}$ (of order r) together with the additional data of the optimal measures $\mu = \mu^*$ and optimal parameters $\mathbf{c} = \mathbf{c}^*$, the binary *system* (of order r). We caution that for fixed i (such as $i = 2$) the parameters c_i do depend on r, although not very much.

The second major task is to show that the binary systems satisfy the entropy condition (3.3), or more accurately that arbitrarily small perturbations of them satisfy the strict entropy condition (3.4). In the last section we provided a tool for doing this in somewhat general conditions, namely Proposition 8.2. That proposition has four conditions, (a), (b), (c)(i) and (c)(ii) which must be satisfied. Of these, (b) (the existence of the optimal parameters $\mathbf{c}^*$) has already been established. We state the other three conditions separately as lemmas.

Lemma 9.3. *Suppose that $V_{i-1} \leqslant W \leqslant V_i$ and that W is invariant under $\mathrm{Aut}(\mathscr{V})$. Then W is either V_{i-1} or V_i. Thus, the binary flags satisfy Proposition 8.2 (a).*

Lemma 9.4. *We have $\mathbb{H}_{\mu^*_{m+1}}(V_m) > 2^m$ for $0 \leqslant m \leqslant r-1$. Thus, the binary flags satisfy Proposition 8.2 (c)(i).*

Lemma 9.5. *We have* $\mathbb{H}_{\mu_i^*}(V_{m-1}) - \mathbb{H}_{\mu_i^*}(V_m) < 2^{m-1}$ *for* $1 \leqslant m < i \leqslant r$. *Thus, the binary flags satisfy Proposition 8.2 (c)(ii).*

The proofs of these various facts are given in Section 10.

9.2. **Proof of Theorem 2 (a)**

We are now in a position to complete the proof of Theorem 2 (a), modulo the results stated above. First, we define the constants θ_r.

Definition 9.6. Let $\rho_1, \rho_2, \dots$ be the solution to the ρ-equations (9.1) for the binary flag. Then we define

$$\theta_r := (\log 3 - 1) \Big/ \Big(\log 3 + \sum_{i=1}^{r-1} \frac{2^i}{\rho_1 \cdots \rho_i} \Big).$$

Proof of Theorem 2 (a). By Proposition 7.7, θ_r is equal to c^*_{r+1}, where $\mathbf{c}^*$ are the optimal parameters on the binary flag $\mathscr{V}$ of order r, the existence of which is Proposition 9.2 (b) above.

By Proposition 8.2 (the hypotheses of which are satisfied by Lemma 9.3, Proposition 9.2 (b) and Lemmas 9.4 and 9.5), arbitrarily small perturbations of $(\mathscr{V}, \mathbf{c}^*, \boldsymbol{\mu}^*)$ satisfy the strict entropy condition (3.4).

Hence, by the definition of $\tilde{\gamma}_k$ (Problem 3.7) we have $\tilde{\gamma}_k \geqslant \tilde{\gamma}_k(\mathscr{V}) \geqslant \theta_r$ (and in fact equality holds in the second inequality here).

Theorem 2 now follows immediately from the inequality $\tilde{\gamma}_k \leqslant \beta_k$, which is (part of) Theorem 7. □

9.3. **Remarks on Theorem 2 (b)**

Theorem 2 (b) is a problem of a combinatorial and analytic nature which can be considered more-or-less completely independently of the first three parts of the paper.

To get a feel for it, and a sense of why it is difficult, let us write down the first two ρ-equations for the binary flags. The equation with $j = 1$ is

$$f^{\Gamma_2}(\rho) = f^{\Gamma_1}(\rho)^{\rho_1} e^2. \tag{9.2}$$

This has the numerical 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 $\mathbb{Q}^8$). This is a tractable exercise and one may confirm that

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

The ρ-equation with $j = 2$ is then

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

where (recall from Figure 7.2) $f^{\Gamma_2}(\rho) = 3^{\rho_1} + 4 \cdot 2^{\rho_1} + 4$. This may be solved numerically, with the value $\rho_2 \approx 0.2796104\dots$, using Mathematica.

Such a numerical procedure, however, is already quite an unappetising prospect if one wishes to compute ρ_3.

Consequently, we must develop more theory to understand the ρ_i and to prove Theorem 2 (b). This is the task of the last two sections of the paper.

10. Binary systems: proofs of the basic properties

In this section, we prove the various statements in subsection 9.1.

We begin, in subsection 10.2, by proving Lemma 9.3. This is a relatively simple and self-contained piece of combinatorics.

In subsection 10.3 we introduce the concept of *genotype*, which allows us to describe the tree structure induced on $\{0,1\}^k$ by the binary flag $\mathscr{V}$. In subsection 10.4 we show how to compute the quantities $f^C(\boldsymbol{\rho})$ in terms of the genotype.

We are then, in subsection 10.5, in a position to prove Proposition 9.2 (a), guaranteeing that the ρ_i exist and allowing us to define the optimal measures $\boldsymbol{\mu}^*$.

In subsection 10.6 we establish the two entropy inequalities, Lemmas 9.4 and 9.5.

Finally, in subsection 10.7 we prove Proposition 9.2 (b), which confirms the existence of the optimal parameters $\mathbf{c}^*$.

10.1. Basic terminology

Throughout the section, $\mathscr{V}$ will denote the binary flag or order r, as defined in Definition 9.1. That is, we take $k = 2^r$, identify $\mathbb{Q}^k$ with $\mathbb{Q}^{\mathcal{P}[r]}$, and take V_i to be the subspace of all $(x_S)_{S\subset\mathcal{P}[r]}$ for which $x_S = x_{S\cap[i]}$ for all $S \subset [r]$.

In addition, we will write $\mathbf{0}_j, \mathbf{1}_j$ for the vectors in $\{0,1\}^{\mathcal{P}[j]}$ consisting of all 0's (respectively all $1's$). We call these (or any multiples of them) *constant* vectors.

Finally, we introduce the notion of a *block* of a vector $x = (x_S)_{S\subset[r]} \in \mathbb{Q}^{\mathcal{P}[r]}$. For each $A \subset [i]$ we consider the 2^{r-i}-tuple

$$x(A,i) := (x_{A\cup A'})_{A'\subset\{i+1,\cdots,r\}}.$$

We call these the *i-blocks* of x.

Remark 10.1. (a) One should note carefully that the i-blocks are strings of length 2^{r-i}. In this language, V_i is the space of vectors x, all of whose i-blocks are constant.

(b) If we put together the coordinates of the i-blocks $x(A,i)$ and $x(A\triangle\{i\},i)$, then we obtain the $(i-1)$-block $x(A\cap[i-1], i-1)$.

In order to visualize the structure of the flag $\mathscr{V}$ and of the partition of $\{0,1\}^{\mathcal{P}[r]}$ by the cosets of V_j, it will be often useful to write elements of $\{0,1\}^{\mathcal{P}[r]}$ as strings of 0s and 1s of length 2^r. When we do this we use the *reverse binary order*, which is the one induced from $\mathbb{N}$ via the map $f(S) = \sum_{s\in S} 2^{r-s}$.

Example 10.2. For concreteness, let us consider the case $r = 3$. In this case, the ordering of the coordinates of x is

$$(x_\emptyset, x_{\{3\}}, x_{\{2\}}, x_{\{2,3\}}, x_{\{1\}}, x_{\{1,3\}}, x_{\{1,2\}}, x_{[3]}). \tag{10.1}$$

If $x = 01001110$ then its 2-blocks are $01, 00, 11, 10$, and its 1-blocks are $0100, 1110$.

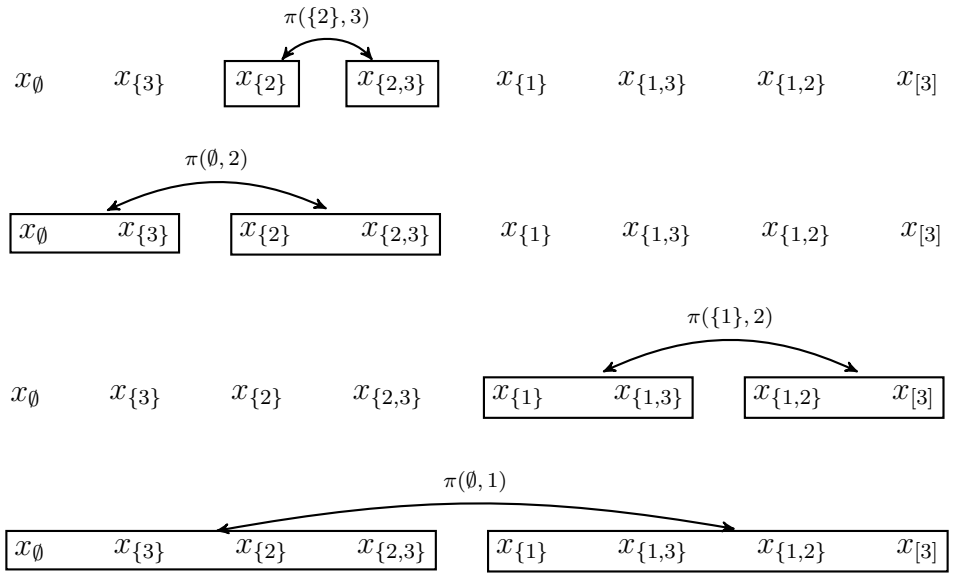
10.2. Automorphisms of the binary system

Proof of Lemma 9.3. We begin by defining some permutations of $\mathcal{P}[r]$ for which, we claim, the corresponding coordinate permutations give elements of $\mathrm{Aut}(\mathscr{V})$. Suppose that $1 \leqslant j \leqslant r$ and

that $A \subset [j-1]$. Then we may consider the permutation $\pi(A,j)$ defined by

$$\pi(A,j)(S) = \begin{cases} S\triangle\{j\} & \text{if } S \cap [j-1] = A, \\ S & \text{otherwise.} \end{cases}.$$

To visualize the action of this permutation on the coordinates of a vector x, it is useful to order its coordinates as we explained above. The action of $\pi(A,j)$ is then to permute the two adjacent j-blocks $x(A,j)$ and $x(A \sqcup \{j\}, j)$, which together form the $(j-1)$-block $x(A, j-1)$, as per Remark 10.1(b). More concretely, below are some examples of the action of the permutations $\pi(A,j)$ in the setting of Example 10.2:



If the readers wish, they may translate the arguments below in the above more visual language.

Claim. $\pi(A,j)$ preserves V_i for all i, and therefore $\pi(A,j) \in \mathrm{Aut}(\mathscr{V})$.

Proof. Suppose that $x = (x_S)_{S \subset [r]} \in V_i$ and let us write for simplicity π instead of $\pi(A,j)$.

Suppose first that $j > i$. Then $\pi(S) \cap [i] = S \cap [i]$ for all S, and so

$$x_{\pi(S)} = x_{\pi(S)\cap[i]} = x_{S\cap[i]} = x_S.$$

where the first and last steps used the fact that $\mathbf{x} \in V_i$. Thus the claim follows in this case.

Suppose now that $j \leqslant i$. Let $t > i$. Then the conditions $(S\triangle\{t\})\cap[j-1] = A$ and $S\cap[j-1] = A$ are equivalent. Hence, if $S \cap [j-1] = A$, then we find that

$$x_{\pi(S\triangle\{t\})} = x_{S\triangle\{t\}\triangle\{j\}} = x_{S\triangle\{j\}} = x_{\pi(S)},$$

where we used that $\mathbf{x} \in V_i$ and that $t > i$ at the second step. Similarly, if $S \cap [j-1] \neq A$, then

$$x_{\pi(S\triangle\{t\})} = x_{S\triangle\{t\}} = x_S = x_{\pi(S)}.$$

In all cases, we have found that $x_{\pi(S\triangle\{t\})} = x_{\pi(S)}$. Since this is true for all $t > i$, $\pi(x)$ indeed lies in V_i. This completes the proof of the claim. □

Suppose now that W is an invariant subspace of $\mathscr{V}$ satisfying the inclusions $V_{i-1} < W \leqslant V_i$. We want to conclude that $W = V_i$. To accomplish this, we introduce some auxiliary notation.

For each $A \subset [i-1]$, we consider the vector $y^A = (y^A_S)_{S\subset[r]} \in V_i$ that is uniquely determined by the relations $y^A_A = 1$, $y^A_{A\cup\{i\}} = -1$ and $y^A_S = 0$ for all other $S \subset [i]$. There are 2^{i-1} such vectors y^A. They are mutually orthogonal, hence linearly independent. In addition, together with V_{i-1}, they generate all of V_i.

Now, it is easy to check that for any $j < i$ and any $A \subset [i-1]$, we have

$$\pi(A \cap [j-1], j)y^A = y^{A\triangle\{j\}}.$$

From the above relation and the invariance of W under $\mathrm{Aut}(\mathscr{V})$, it is clear that if W contains at least one vector y^A with $A \subset [i-1]$, then it contains all such vectors. Since we also know that $V_{i-1} \leqslant W \leqslant V_i$, we must have that $W = V_i$, which is what we need to complete the proof of Lemma 9.3.

It remains to exhibit a vector y^A lying in W. Since we have assumed that $W \neq V_{i-1}$, there is some $x \in W$ and some $A \subset [i-1]$ such that $a = x_A \neq x_{A\cup\{i\}} = b$. It is then easy to check that $(a-b)^{-1}\big(x - \pi(A,i)(x)\big) = y^A$. The vector of the left hand side is in W by our assumptions that $x \in W$ and that W is invariant. Thus, $y^A \in W$ as well. This completes the proof of Lemma 9.3. □

Remark. A minor elaboration of the above argument in fact allows one to show that the subspaces of $\mathbb{Q}^{\mathcal{P}[r]}$ invariant under $\mathrm{Aut}(\mathscr{V})$ are the V_i, the orthogonal complements of V_{i-1} in V_i, and all direct sums of these spaces. However, we will not need the classification in this explicit form.

10.3. **Cell structure and genotype**

The cosets of V_i partition $\{0,1\}^{\mathcal{P}[r]}$ into sets which we call the *cells at level* i. Our first task is to describe these explicitly.

Consider $\omega, \omega' \in \{0,1\}^{\mathcal{P}[r]}$. It is easy to see that $\omega - \omega' \in V_i$ (and so ω, ω' lie in the same cell at level i) if and only if for every $A \subset [i]$ one of the following is true:

(a) Both $\omega(A,i)$ and $\omega'(A,i)$ are constant blocks (that is, they both lie in $\{\mathbf{0}_{r-i}, \mathbf{1}_{r-i}\}$).
(b) $\omega(A,i) = \omega'(A,i)$, and neither of these blocks is constant (that is, neither is $\mathbf{0}_{r-i}$ nor $\mathbf{1}_{r-i}$).

Thus a cell at level i is completely specified by the *positions* A of its constant i-blocks, and the *values* $\omega(A,i)$ (for an arbitrary $\omega \in C$) of its non-constant i-blocks.

Example. With $r = 3$ and $\omega = 01001110$, the level 2 cell that contains ω is the set

$$\{\omega, 01111110, 01000010, 01000010\}.$$

Its constant 2-blocks are at $A = \{2\}$ and $A = \{1\}$. Its non-constant 2-blocks are at $A = \emptyset$ (taking the value $\omega(A,2) = 01$) and at $A = \{1,2\}$ (taking the value $\omega(A,2) = 10$). The level 1 cell containing ω is just $\{\omega\}$.

The positions of the constant i-blocks play an important role, and we introduce the name *genotype* to describe these[4].

Definition 10.1 (Genotype)**.** If C is a cell at level i, its *genotype* $g(C) \subset \mathcal{P}[i]$ is defined to be the collection of $A \subset [i]$ for which $\omega(A,i)$ is constant, where $\omega \in C$ is any element. Note that, by the preceding dicussion, it does not matter which $\omega \in C$ we choose. We refer to any subset of $\mathcal{P}[i]$ as an *i-genotype*. If g, g' are two i-genotypes then we write $g \leqslant g'$ to mean the same as $g \subseteq g'$. We write $|g|$ for the cardinality of g.

[4]The term genotype is appropriate, as each component in g acts like recessive gene with respect to child cells.

Example. If C is the cell at level 2 containing $\omega = 01001110$, the genotype $g(C)$ is equal to $\big\{\{2\},\{1\},\{1,2\}\big\}$. (We have listed these sets in the reverse binary ordering once again.)

Definition 10.2 (Consolidations)**.** If g is an i-genotype, then its *consolidation* is the $(i-1)$-genotype g^* defined by $g^* := \{A' \subset [i-1] : A' \in g, A' \cup \{i\} \in g\}$ (cf. Remark 10.1 (b)).

Let us pause to note the easy inequality

$$\frac{1}{2}|g| \geqslant |g^*| \geqslant |g| - 2^{i-1}, \tag{10.2}$$

valid for all i-genotypes.

The genotype is intimately connected to the cell structure on $\{0,1\}^k$ induced by $\mathscr{V}$, as the following lemma shows.

Lemma 10.3. *We have the following statements.*

(a) *If C is a cell, we have $|C| = 2^{|g(C)|}$.*
(b) *Suppose that g is an i-genotype. There are $(2^{2^{r-i}}-2)^{2^i-|g|}$ cells (at level i) with $g(C) = g$;*
(c) *If $g(C) = g$, and if C' is a child of C, then $g(C') \leqslant g^*$. In particular, $|g(C')| \leqslant \frac{1}{2}|g(C)|$;*
(d) *Suppose that $g(C) = g$. Suppose that g' is an $(i-1)$-genotype and that $g' \leqslant g^*$. Then number of children C' of C with $g(C') = g'$ is $2^{|g|-|g^*|-|g'|}$;*
(e) *Suppose that C is a cell at level i with $g(C) = g$. Then the number of children of C (at level $i-1$) is $2^{|g|-2|g^*|}3^{|g^*|}$.*

Proof. (a) This is almost immediate: for each of the $A \subset g(C)$ of constant blocks, the are two choices ($\mathbf{0}_{r-i}$ or $\mathbf{1}_{r-i}$) for $\omega(A,i)$.

(b) To determine C completely (given g), one must specify the value of each of $2^i - |g|$ non-constant i-blocks. For each such block, there are $2^{2^{r-i}} - 2$ possible non-constant values.

(c) A set $A' \subset [i-1]$ can only possibly be the position of a constant block in some child cell of C if both A' and $A' \cup \{i\}$ are the positions of constant blocks in C, or in other words $A', A' \cup \{i\} \in g$, which is precisely what it means for A' to lie in g^*.

Note that the child cell C' containing ω only *does* have a constant $(i-1)$-block at position A' if $\omega(A',i) = \omega(A' \cup \{i\}, i)$, which may or may not happen.

The second statement is an immediate consequence of the first and (10.2).

(d) Let $A \in g$. We say that A is *productive* if $A' := A \cap [i-1] \in g^*$, or equivalently if A' and $A' \cup \{i\}$ both lie in g (or, more succinctly, $A \triangle \{i\} \in g$). These are the positions which can give rise to constant $(i-1)$-blocks in children of C. There are $2|g^*|$ such positions, coming in $|g^*|$ pairs. To create a child C' with genotype g', we have a binary choice at $|g^*| - |g'|$ of these pairs: at each of them either $\omega(A',i) = \mathbf{0}_{r-i}$ and $\omega(A' \cup \{i\}, i) = \mathbf{1}_{r-i}$, or the other way around. There are $|g| - 2|g^*|$ non-productive positions $A \in g$, and for each of these there is also a binary choice, either $\omega(A,i) = \mathbf{0}_{r-i}$ or $\omega(A,i) = \mathbf{1}_{r-i}$. The total number of choices is therefore $2^{|g^*|-|g'|} \times 2^{|g|-2|g^*|}$, which is exactly as claimed.

(e) is immediate from part (d), upon summing over $g' \subseteq g^*$. □

10.4. The $f^C(\rho)$ and genotype

We begin by recalling from (7.4) the definition of the functions $f^C(\boldsymbol{\rho})$. Here $\boldsymbol{\rho} = (\rho_1, \cdots, \rho_{r-1})$ is a sequence of parameters, and we define $\rho_0 = 0$. If C has level 0, we set $f^C(\boldsymbol{\rho}) = 1$, whilst for C at level $i \geqslant 1$ we apply the recursion

$$f^C(\boldsymbol{\rho}) = \sum_{C \to C'} f^{C'}(\boldsymbol{\rho})^{\rho_{i-1}}.$$

Proposition 10.4. *The quantities f^C depend only on the genotype of C, and thus for any i-genotype g we may define $F(g) := f^C(\boldsymbol{\rho})$, where C is any cell with $g(C) = g$. We have the recursion*

$$F(g) = \sum_{g' \leqslant g^*} 2^{|g|-|g^*|-|g'|} F(g')^{\rho_{i-1}}. \tag{10.3}$$

Remark. The $F(g)$ depend on $\boldsymbol{\rho}$, as well as on i (where g is an i-genotype) but we suppress explicit mention of this. For example, it should be clear from context that g on the left is an i-genotype, but the sum on the right is over $(i-1)$-genotypes, since g^* is an $(i-1)$ genotype by definition.

Proof. This is a simple induction on the level i using the definition of the $f^C(\boldsymbol{\rho})$, and parts (c) and (d) of Lemma 10.3. □

Let us pause to record two corollaries which we will need later.

Corollary 10.5. *Suppose that g_1, g_2 are two i-genotypes with $g_1 \leqslant g_2$. Then $F(g_1) \leqslant F(g_2)$.*

Proof. Note that $g_1^* \leqslant g_2^*$, and also that $|g_1| - |g_1^*| \leqslant |g_2| - |g_2^*|$, since $|g| - |g^*| = \#\{A \subset \mathcal{P}[i-1] : \#(\{A, A \cup \{i\}\} \cap g) = 1\}$. Hence, by two applications of Proposition 10.4,

$$F(g_1) = 2^{|g_1|-|g_1^*|} \sum_{g' \leqslant g_1^*} 2^{-|g'|} F(g')^{\rho_{i-1}} \leqslant 2^{|g_2|-|g_2^*|} \sum_{g' \leqslant g_2^*} 2^{-|g'|} F(g')^{\rho_{i-1}} = F(g_2).$$ □

Recall that Γ_i is the cell at level i containing $\mathbf{0}$. Note that $g(\Gamma_i) = \mathcal{P}[i]$.

Corollary 10.6. *If $C \neq \Gamma_i$ is a cell of level i, then $f^C(\boldsymbol{\rho}) < f^{\Gamma_i}(\boldsymbol{\rho})$.*

Proof. This is simply the special case $g_2 = \mathcal{P}[i]$ of the preceding corollary. The inequality is strict because if $g < \mathcal{P}[i]$, then $g^* < \mathcal{P}[i-1]$. □

10.5. Existence of the ρ_i

In this section we prove Proposition 9.2 (a), which asserts that for the binary flags there is a unique solution $\boldsymbol{\rho} = (\rho_1, \rho_2, \dots)$ to the ρ-equations (9.1). In fact, we will prove the following more general fact which treats the jth ρ-equation in isolation, irrespective of whether the earlier ones have already been solved.

Proposition 10.7. *Let $\rho_1, \dots, \rho_{j-1} \in (0,1)$. Then there is a unique $\rho_j \in (0,1)$ such that the jth ρ-equation for the binary flag, $f^{\Gamma_{j+1}}(\boldsymbol{\rho}) = e^{2^j} f^{\Gamma_j}(\boldsymbol{\rho})^{\rho_j}$, is satisfied.*

Remark. We will prove in the next section (Lemma 11.2) that for the solution $\rho_1, \rho_2, \dots$ to the full set of ρ-equations we have $\rho_j \leqslant \rho_1 = 0.30648\dots$ for all j. For a table of numerical values of the ρ_j, see Table 1 in Section 12.

Before beginning the proof of Proposition 10.7, we isolate a lemma.

Lemma 10.8. *Fix a $(j-1)$-genotype g'. Then*

$$\sum_{g\colon g^*\geqslant g'} 2^{-|g^*|} = \left(\frac{1}{2}\right)^{2^{j-1}} 7^{2^{j-1}-|g'|},$$

where the sum is over all j-genotypes g.

Proof. Assume that $g^* \geqslant g'$ and fix $A \subset [j-1]$. If $A \in g'$, then $A \in g^*$ and hence both $A \in g$ and $A \cup \{j\} \in g$. If $A \notin g'$, then either $A \in g^*$ (whence $A \in g$ and $A \cup \{j\} \in g$) or $A \notin g^*$ (whence at most one of A and $A \cup \{j\}$ is in g). Therefore,

$$\sum_{g\colon g^*\geqslant g'} 2^{-|g^*|} = \prod_{A\in g'} 2^{-1} \prod_{A\notin g'} (2^{-1} + 3\cdot 2^0) = \left(\frac{1}{2}\right)^{2^{j-1}} 7^{2^{j-1}-|g'|}. \qquad \square$$

Proof of Proposition 10.7. For $j = 1$, the equation to be satisfied is $3^{\rho_1} + 4\cdot 2^{\rho_1} + 4 = e^2 3^{\rho_1}$. It may easily be checked numerically that this has a unique solution $\rho_1 \approx 0.306481\ldots$ in $(0,1)$. One may also proceed analytically as follows. Define

$$G(x) = G_1(x) := e^2 3^x - (3^x + 4\cdot 2^x + 4) = 3^x\big(e^2 - (1 + 4\cdot(2/3)^x + 4/3^x)\big),$$

In particular, the roots of G are in correspondence with the roots of $H(x) = e^2 - (1 + 4\cdot(2/3)^x + 4/3^x)$. This is clearly a continuous and strictly increasing function. In addition, $H(0) = e^2 - 9 < 0$ and $H(1) = e^2 - 5 > 0$. Thus, H has a unique root $\rho_1 \in (0,1)$, and so does G.

Now assume $j \geqslant 2$. It turns out that much the same argument works, although the details are more elaborate. Assume that $0 < \rho_i < 1$ for $1 \leqslant i < j$. Define

$$G(x) := G_j(x) = e^{2^j}(f^{\Gamma_j}(\boldsymbol{\rho}))^x - f^{\Gamma_{j+1}}(\rho_1,\ldots,\rho_{j-1},x).$$

Proposition 10.4 implies that

$$\begin{aligned} G(x) &= e^{2^j}(F(\mathcal{P}[j]))^x - \sum_g 2^{2^j-|g|}F(g)^x \qquad (10.4)\\ &= F(\mathcal{P}[j])^x \cdot H(x), \end{aligned}$$

where

$$H(x) = e^{2^j} - 2^{2^j}\sum_g 2^{-|g|}\big(F(g)/F(\mathcal{P}[j])\big)^x$$

and the sums over g run over all genotypes $g \subset \mathcal{P}[j]$ at level j. Since (by an easy induction) $F(\mathcal{P}[j]) > 0$, it follows that G and H have the same roots. The latter is a continuous and strictly increasing function because Corollary 10.5 implies that $F(g)/F(\mathcal{P}[j]) \leqslant 1$. Moreover, $H(0) = e^{2^j} - 3^{2^j} < 0$. Therefore to complete the proof it suffices to show that $H(1) > 0$.

To show this, we use (10.4). First note that

$$F(\mathcal{P}[j]) = (\sqrt{2})^{2^j}\sum_{g'} 2^{-|g'|}F(g')^{\rho_{j-1}}, \qquad (10.5)$$

where the sum is over all genotypes g' of level $(j-1)$. Next, by Proposition 10.4 and Lemma 10.8 we have

$$\begin{aligned}\sum_{g\subset\mathcal{P}[j]} 2^{-|g|}F(g) &= \sum_{g} 2^{-|g^*|}\sum_{g'\leqslant g^*} 2^{-|g'|}F(g')^{\rho_{j-1}}\\ &= \sum_{g'\subset\mathcal{P}[j-1]} 2^{-|g'|}F(g')^{\rho_{j-1}}\sum_{g:\, g^*\geqslant g'} 2^{-|g^*|}\\ &= (7/2)^{2^{j-1}}\sum_{g'} 14^{-|g'|}F(g')^{\rho_{j-1}}. \end{aligned} \tag{10.6}$$

Putting (10.4), (10.5) and (10.6) together we obtain

$$H(1)\cdot F(\mathcal{P}[j]) = (e\sqrt{2})^{2^j}\sum_{g'} 2^{-|g'|}F(g')^{\rho_{j-1}} - (\sqrt{14})^{2^j}\sum_{g'} 14^{-|g'|}F(g')^{\rho_{j-1}}.$$

Since $e^2>7$, $\sqrt{14}<e\sqrt{2}$ and it follows that indeed $H(1)>0$. This completes the proof. □

10.6. **Entropy inequalities for the binary systems**

We begin with a lemma which will be used a few times in what follows.

Lemma 10.9. *Let C' be one of the children of Γ_i, thus C' is a cell at level $(i-1)$. Then*

$$\mu_i(C') \leqslant \mu_i(\Gamma_{i-1}) = e^{-2^{i-1}},$$

and equality occurs only when $C'=\Gamma_{i-1}$.

Proof. We showed in Corollary 10.6 that $f^{C'}(\boldsymbol{\rho}) < f^{\Gamma_{i-1}}(\boldsymbol{\rho})$, for any choice of $\boldsymbol{\rho}=(\rho_1,\dots,\rho_{r-1})$, and for any child C' of Γ_i with $C'\neq\Gamma_{i-1}$. Now that we know that the ρ-equations have a solution, it follows immediately from the definition of the optimal measures $\boldsymbol{\mu}^*$ in (7.6), applied with $C=\Gamma_i$, that $\mu_i(C')<\mu_i(\Gamma_{i-1})$, again for any child C' of Γ_i with $C'\neq\Gamma_{i-1}$. Finally, observe that $\mu_i(\Gamma_{i-1})=e^{-2^{i-1}}$ by (7.7). □

Proof of Lemma 9.4. This follows almost immediately from Lemma 10.9 with $i=m+1$. Indeed since $\mu_{m+1}(C)\leqslant e^{-2^m}$ for all cells C at level m, with equality only for $C=\Gamma_m$, we have

$$\mathbb{H}_{\mu_{m+1}}(V_m) = \sum_C \mu_{m+1}(C)\log\frac{1}{\mu_{m+1}(C)} > 2^m\sum_C \mu_{m+1}(C) = 2^m.$$

This concludes the proof. □

Proof of Lemma 9.5. Let $\mu=\mu_i$ with $i>m$. By the definition of entropy, Lemma 10.3 (e), and the concavity of $L(x)=-x\log x$ we find that

$$\begin{aligned}\mathbb{H}_\mu(V_{m-1}) - \mathbb{H}_\mu(V_m) &= \sum_C \mu(C)\sum_{C'} L\left(\frac{\mu(C')}{\mu(C)}\right)\\ &\leqslant \sum_C \mu(C)\log(\#C')\\ &\leqslant \sum_C \mu(C)\log\left[2^{|g(C)|}(3/4)^{|g(C)^*|}\right], \end{aligned} \tag{10.7}$$

where here the sum is over cells C at level m and their children C' at level $(m-1)$, and the notations $g(C)$ and $g(C)^*$ refers to the genotype of C and its consolidation, as defined in Definitions 10.1 and 10.2.

Now by (10.2) we have $|g(C)^*| \geqslant |g(C)| - 2^{m-1}$, whence

$$2^{|g(C)|}(3/4)^{|g(C)^*|} \leqslant 2^{|g(C)|}(3/4)^{|g(C)|-2^{m-1}} = (3/2)^{|g(C)|}(4/3)^{2^{m-1}}. \tag{10.8}$$

Since we also have that $|g(C)| \leqslant 2^m$, we infer that

$$2^{|g(C)|}(3/4)^{|g(C)^*|} \leqslant 3^{2^{m-1}}. \tag{10.9}$$

This and (10.7) already imply the bound

$$\mathbb{H}_\mu(V_{m-1}) - \mathbb{H}_\mu(V_m) \leqslant 2^{m-1}\log 3,$$

which is only very slightly weaker than Lemma 9.5.

To make the crucial extra saving, write S for the union of all cells C at level m with $|g(C)| > \frac{3}{4}2^m$. We claim that

$$\mu(S) < \frac{1}{2}. \tag{10.10}$$

We postpone the proof of this inequality momentarily and show how to use it to complete the proof of Lemma 9.5.

Observe that if C is not one of the cells making up S, that is to say if $|g(C)| \leqslant \frac{3}{4}2^m$, then

$$\begin{aligned}\log\left[2^{|g(C)|}(3/4)^{|g(C)^*|}\right] &\leqslant \log\left[(3/2)^{|g(C)|}(4/3)^{2^{m-1}}\right]\\ &\leqslant \left(\frac{3}{2}\log(3/2) + \log(4/3)\right)2^{m-1}\\ &\leqslant 0.9\cdot 2^{m-1},\end{aligned}$$

where we used (10.8) to obtain the first inequality. Assuming the claim (10.10), it follows from this, (10.7) and (10.9) that

$$\mathbb{H}_\mu(V_{m-1}) - \mathbb{H}_\mu(V_m) \leqslant 2^{m-1}(\log 3)\mu(S) + 0.9\cdot 2^{m-1}(1-\mu(S)) < 2^{m-1},$$

which is the statement of Lemma 9.5.

It remains to prove (10.10). Recall that $1 \leqslant m < i \leqslant r$.

If $1 \leqslant m \leqslant 2$, there is only one cell C with $|g(C)| > \frac{3}{4}2^m$, namely Γ_m. Since we have $\mu(\Gamma_m) = e^{2^m - 2^i} \leqslant e^{-1}$ by (7.7), our claim (10.10) follows in this case.

Assume now that $m \geqslant 3$. Let $\tilde{S}$ be the union of all children $\tilde{C}$ of Γ_i (thus these are cells at level $i-1 \geqslant m$) which contain a cell C in S. By repeated applications of Lemma 10.3 (c) we have $|g(\tilde{C})| > 2^{i-1-m}(\frac{3}{4}2^{m-1}) = \frac{3}{4}2^{i-1}$ for any such $\tilde{C}$. Lemma 10.3 (d), applied with $C = \Gamma_i$, implies that the number of such cells $\tilde{C}$ is at most

$$\sum_{h > (3/4)2^{i-1}} \binom{2^{i-1}}{h} 2^{2^{i-1}-h} \leqslant 2^{\frac{1}{4}2^{i-1}} 2^{2^{i-1}} = 2^{(5/4)2^{i-1}}.$$

By Lemma 10.9 it follows that

$$\mu(S) \leqslant \mu(\tilde{S}) \leqslant (2^{5/4}/e)^{2^{i-1}} < 0.35,$$

using that $i - 1 \geqslant m \geqslant 3$. This completes the proof of the claim (10.10) and hence of Lemma 9.5. □

10.7. Existence of the optimal parameters $\mathbf{c}^*$

Proof of Proposition 9.2 (b). Observe that $\mathrm{Supp}(\mu_j) \subset V_j \cap \{0,1\}^k$, and hence $|\mathrm{Supp}(\mu_j)| \leqslant 2^{2^j}$ by Lemma 5.1. By Lemma B.2, when $j \geqslant m+2$ we deduce the inequality

$$\mathbb{H}_{\mu_j}(V_m) \leqslant \log|\mathrm{Supp}(\mu_j^*)| \leqslant 2^j \log 2 < 2^j - 2^m. \tag{10.11}$$

Now recall (Definition 7.5) that the optimal parameters should satisfy the conditions (7.10) (which are the fully written out version of (7.9)). We wish to show that there is a solution with $1 = c_1^* > c_2^* > \cdots > c_{r+1}^* > 0$. Rearranging (7.10) and recalling $\dim(V_j) = 2^j$, we find that

$$\begin{aligned}(c_{m+1}^* - c_{m+2}^*)\big(\mathbb{H}_{\mu_{m+1}}(V_m) - 2^m\big) \\ = \sum_{j=m+2}^{r} \big(2^j - 2^m - \mathbb{H}_{\mu_j}(V_m)\big)(c_j^* - c_{j+1}^*) + (2^r - 2^m)c_{r+1}^*\end{aligned}$$

for $0 \leqslant m \leqslant r-1$. By Lemma 9.4 and (10.11), we may apply a downwards induction on $m = r-1, r-2, \cdots$ to solve these equations with $0 < c_{r+1}^* < c_r^* < \cdots < c_1^*$. Rescaling, we may additionally ensure that $c_1^* = 1$. □

11. The limit of the ρ_i

In the last section we showed that there is a unique solution $\boldsymbol{\rho} = (\rho_1, \rho_2, \ldots)$ to the $\boldsymbol{\rho}$-equations (9.1) for the binary system with $0 < \rho_j < 1$ for all j. In this section, we show that the limit $\lim_{j\to\infty} \rho_j$ exists.

Proposition 11.1. *$\rho = \lim_{j\to\infty} \rho_j$ exists.*

11.1. ρ_1 is the largest ρ_j

The estimates required in the proof of Proposition 11.1 are rather delicate, and to make them usable for our purposes we need the following *a priori* bound on the ρ_j.

Lemma 11.2. *For all j, $\rho_j \leqslant \rho_1 = 0.30648\ldots$*

The reader should recall the notion of genotype g (Definition 10.1) and of the function $F(g)$ (Proposition 10.4).

The next lemma is a stronger version of Corollary 10.5, whose proof uses that result as an ingredient.

Lemma 11.3. *For any j and $g_1 \leqslant g_2$ at level j, we have*

$$\frac{F(g_1)}{F(g_2)} \leqslant \left(\frac{1}{2}\right)^{|g_2|-|g_1|} \left(\frac{4}{3}\right)^{|g_2^*|-|g_1^*|}.$$

Proof. Applying Proposition 10.4 to g_2, followed by Corollary 10.5, followed by an application of the binomial theorem, followed by an application of Proposition 10.4 to g_1, we obtain

$$\begin{aligned} F(g_2) &= 2^{|g_2|-|g_2^*|}\sum_{g\leqslant g_1^*} 2^{-|g|}\sum_{g'\leqslant g_2^*\setminus g_1^*} 2^{-|g'|}F(g\cup g')^{\rho_{j-1}} \\ &\geqslant 2^{|g_2|-|g_2^*|}\sum_{g\leqslant g_1^*} 2^{-|g|}\sum_{g'\leqslant g_2^*\setminus g_1^*} 2^{-|g'|}F(g)^{\rho_{j-1}} \\ &= 2^{|g_2|-|g_2^*|}\sum_{g\leqslant g_1^*} 2^{-|g|}F(g)^{\rho_{j-1}}(3/2)^{|g_2^*|-|g_1^*|} \\ &= F(g_1)2^{|g_2|-|g_1|}(3/4)^{|g_2^*|-|g_1^*|} \end{aligned}$$

This concludes the proof. □

Proof of Lemma 11.2. We begin by observing that

$$\sum_{g\leqslant \mathcal{P}[j]} c_1^{|g|}c_2^{|g^*|} = \prod_{A\subset[j-1]}\Big(\sum_{a,b\in\{0,1\}} c_1^{a+b}c_2^{ab}\Big) = (1+2c_1+c_1^2c_2)^{2^{j-1}}. \tag{11.1}$$

The ρ-equations (9.1), translated into the language of genotype, are $F(\mathcal{P}[j+1]) = e^{2^j}F(P[j])^{\rho_j}$. Therefore, by Proposition 10.4 (with $g=\mathcal{P}[j+1]$) followed by Lemma 11.3 (with $g_2=\mathcal{P}[j]$) we have

$$\begin{aligned} e^{2^j}F(\mathcal{P}[j])^{\rho_j} = F(\mathcal{P}[j+1]) &= 2^{2^j}\sum_{g\leqslant\mathcal{P}[j]} 2^{-|g|}F(g)^{\rho_j} \\ &\leqslant 2^{2^j}\sum_{g\leqslant\mathcal{P}[j]} 2^{-|g|}F(\mathcal{P}[j])^{\rho_j}\Big[(1/2)^{2^j-|g|}(4/3)^{2^{j-1}-|g^*|}\Big]^{\rho_j}. \end{aligned}$$

Dividing through by $F(\mathcal{P}[j])^{\rho_j}$, and applying (11.1) with $c_1 = 2^{\rho_j-1}$ and $c_2=(3/4)^{\rho_j}$, we find that

$$\begin{aligned} e^{2^j} &\leqslant 2^{2^j}(1/3)^{2^{j-1}\rho_j}\sum_{g\leqslant P[j]} 2^{(\rho_j-1)|g|}(3/4)^{\rho_j|g^*|} \\ &= (4/3^{\rho_j})^{2^{j-1}}\big(1+2^{\rho_j}+2^{2\rho_j-2}(3/4)^{\rho_j}\big)^{2^{j-1}} \\ &= \big(1+4(2/3)^{\rho_j}+4\cdot 3^{-\rho_j}\big)^{2^{j-1}}. \end{aligned}$$

Therefore

$$3^{\rho_j}e^2 \leqslant 3^{\rho_j}+4\cdot 2^{\rho_j}+4.$$

However, the first ρ-equation (9.2) is precisely that

$$3^{\rho_1}e^2 = 3^{\rho_1}+4\cdot 2^{\rho_1}+4.$$

The result follows immediately (using the monotonicity of the function $1+4(2/3)^t+4(1/3)^t$). □

11.2. **Preamble to the proof**

In this section, we set up some notation and structure necessary for the proof of Proposition 11.1. It is convenient to reverse the indices in f^C. Specifically, let $\mathbf{x}=(x_1,x_2,\ldots)$, where $0\leqslant x_i\leqslant 1$. If C is a cell at level j then we define

$$\psi^C(\mathbf{x}) := \log f^C(x_{j-1},\ldots,x_1).$$

In the special case $C = \Gamma_j$ we define also the normalised version

$$\phi_j(\mathbf{x}) = 2^{-j}\psi^{\Gamma_j}(\mathbf{x}) = 2^{-j}\log f^{\Gamma_j}(x_{j-1}, \cdots, x_1).$$

Thus $\phi_1(\mathbf{x}) = \frac{1}{2}\log 3$, $\phi_2(\mathbf{x}) = \frac{1}{4}\log(3^{x_1} + 4\cdot 2^{x_1} + 4)$.

Note that ψ^C, ϕ_j are non-decreasing in each variable. Moreover we have the following simple bounds.

Lemma 11.4 (Simple bounds)**.** *We have* $\frac{1}{2}\log 3 \leqslant \phi_j(\mathbf{x}) < \log 2$.

Proof. For the upper bound, note that $f^{\Gamma_j}(\mathbf{x}) \leqslant f^{\Gamma_j}(\mathbf{1})$. By the definition of f^C (see (7.4)), we have that $f^{\Gamma_j}(\mathbf{1})$ is equal to the number of children of Γ_j at level 0, which, in turn, is equal to $2^{2^j} - 1$. This proves the claimed upper bound on $\phi_j(\mathbf{x})$.

For the lower bound, observe that $f^{\Gamma_j}(\mathbf{x}) \geqslant f^{\Gamma_j}(\mathbf{0})$. Using again the definition of f^C, we find that $f^{\Gamma_j}(\mathbf{0})$ equals the number of children of Γ_j at level $j-1$. Thus $f^{\Gamma_j}(\mathbf{0}) = 3^{2^{j-1}}$ by Lemma 10.3. This proves the claimed lower bound of $\phi_j(\mathbf{x})$, thus completing the proof of the lemma. □

The ρ-equations (9.1) may be expressed in terms of the ϕ_j in the following simple form:

$$\phi_{j+1}(\rho_j, \rho_{j-1}, \ldots) = \frac{1}{2}\big(\rho_j\phi_j(\rho_{j-1}, \rho_{j-2}, \ldots) + 1\big). \tag{11.2}$$

11.3. **Product structure of cells and self-similarity of the functions** ϕ_j

There is a natural bijection $\pi : \mathbb{Q}^{\mathcal{P}[r-1]} \times \mathbb{Q}^{\mathcal{P}[r-1]} \to \mathbb{Q}^{\mathcal{P}[r]}$ defined by $\pi((x, x')) = y$, where $y_A = x_{A-1}$ and $y_{\{1\}\cup A} = x'_{A-1}$, for all $A \subset \{2, \ldots, r\}$. Here, we write $A - 1$ for the set $\{a - 1 : a \in A\}$. In coordinates, this can be thought of as a concatenation map.

Now one may easily check that $\pi(V_{j-1}^{(r-1)} \times V_{j-1}^{(r-1)}) = V_j^{(r)}$, where the $V_j^{(s)}$'s are as in the definition of binary system of step s. This holds for $j = 1, \ldots, r$.

Therefore if C_1, C_2 are two cells at level $(j-1)$ in the binary system of step $(r-1)$, then $\pi(C_1 \times C_2)$ is a cell at level j in the binary system of step r, and conversely every cell is of this form. The children C' of C are precisely $\pi(C_1' \times C_2')$ where $C_1 \to C_1'$, $C_2 \to C_2'$.

The product structure established above manifests itself in a self-similarity property $\phi_j \approx \phi_{j-1}$. In this section, we will establish the following precise version of this.

Proposition 11.5. *Let* $\alpha \in (0, 1]$ *and consider a vector* $\mathbf{x} = (x_1, x_2, \ldots)$ *such that* $0 \leqslant x_i \leqslant \alpha$ *for all* $i \geqslant 1$*. In addition, let* $C = \pi(C_1 \times C_2)$ *be a cell of level* $j \geqslant 2$*. Then we have*

$$\psi^{C_1}(\mathbf{x}) + \psi^{C_2}(\mathbf{x}) \leqslant \psi^{C}(\mathbf{x}) \leqslant \psi^{C_1}(\mathbf{x}) + \psi^{C_2}(\mathbf{x}) + \alpha^{j-1}\log 2. \tag{11.3}$$

In particular, taking $C = \Gamma_j = \pi(\Gamma_{j-1} \times \Gamma_{j-1})$*, we have*

$$\phi_{j-1}(\mathbf{x}) \leqslant \phi_j(\mathbf{x}) \leqslant \phi_{j-1}(\mathbf{x}) + (\alpha/2)^j\frac{\log 2}{\alpha}. \tag{11.4}$$

Proof. We give the proof of the upper bound in (11.3), the lower bound being very similar. We proceed by induction on j. When $j = 2$, we proceed by hand. There are six different types of cells $C = \pi(C_1 \times C_2)$ corresponding to the six possibilities for the unordered pair $\{|C_1|, |C_2|\}$.

Five of these cases are essentially trivial; for example, when $|C_1| = 2$ and $|C_2| = 3$ we have $f^C(\mathbf{x}) = 2\cdot 2^x + 4$, $f^{C_1} = 2$, $f^{C_2} = 3$ and so the desired inequality is $\log(2\cdot 2^x + 4) \leqslant \log 6 + x\log 2$, which is immediately seen to be true for all $x \geqslant 0$.

A little trickier is the case $|C_1| = |C_2| = 3$, corresponding to $C = \Gamma_2 = \pi(\Gamma_1 \times \Gamma_1)$. In this case $f^C(\mathbf{x}) = 3^x + 4 \cdot 2^x + 4$, $f^{C_1} = f^{C_2} = 3$, so the desired inequality is $\log(3^x + 4 \cdot 2^x + 4) \leqslant 2\log 3 + x \log 2$. To prove that this is true for $0 \leqslant x \leqslant 1$, set $f(x) := 5 \cdot 2^x - 3^x - 4$, and note that $f(0) = 0$ and that $f'(x) = 5\log 2 \cdot 2^x - \log 3 \cdot 3^x > 0$ (since $\frac{5\log 2}{\log 3} > \frac{3}{2}$). Thus $f(x) \geqslant 0$ for $0 \leqslant x \leqslant 1$, which is equivalent to the desired inequality.

Now suppose that $j \geqslant 3$, and assume the result is true for cells at level $(j-1)$. By the recursive definition of f^C, if C is a cell at level j, we have the recurrence

$$e^{\psi^C(\mathbf{x})} = \sum_{C \to C'} e^{x_1 \psi^{C'}(T\mathbf{x})}, \tag{11.5}$$

where $T\mathbf{x}$ denotes the *shift operator*

$$T\mathbf{x} = (x_2, x_3, \dots).$$

Therefore we have

$$\begin{aligned} e^{\psi^C(\mathbf{x})} = \sum_{C \to C'} e^{x_1 \psi^{C'}(T\mathbf{x})} &\leqslant \sum_{\substack{C_1 \to C_1' \\ C_2 \to C_2'}} e^{x_1(\psi^{C_1'}(T\mathbf{x}) + \psi^{C_2'}(T\mathbf{x}) + \alpha^{j-2}\log 2)} \\ &\leqslant 2^{\alpha^{j-1}} \Big(\sum_{C_1 \to C_1'} e^{x_1 \psi^{C_1'}(T\mathbf{x})} \Big) \Big(\sum_{C_2 \to C_2'} e^{x_1 \psi^{C_2'}(T\mathbf{x})} \Big) \\ &= 2^{\alpha^{j-1}} e^{\psi^{C_1}(\mathbf{x})} e^{\psi^{C_2}(\mathbf{x})}. \end{aligned}$$

The result follows. □

11.4. **Derivatives and the limit of the ρ_i.**

The self-similarity property (11.4) is not enough for us by itself. We will also require the following (rather ad hoc) derivative bounds.

Here, and in what follows, $\partial_m F(y_1, \dots, y_m) := \frac{\partial F}{\partial y_m}(y_1, \dots, y_m)$, that is to say the derivative of the function F with respect to its mth variable. Thus, for instance,

$$\partial_m \psi^C(T\mathbf{x}) = \frac{\partial}{\partial x_{m+1}} \big[\psi^C(T\mathbf{x})\big]. \tag{11.6}$$

Proposition 11.6. *Set* $\Delta_m := \sup_{j \geqslant 2} \sup_{0 \leqslant x_i \leqslant 0.31} |\partial_m \phi_j(\mathbf{x})|$. *Then* $\Delta_1 < 0.17$, $\Delta_2 < 0.05$, $\sum_{m \geqslant 3} \Delta_m < 0.01$ *and* $\Delta_m \ll 0.155^m$.

The proof of this proposition is given in subsection 11.5. Let us now show how this proposition, together with (11.4), implies Proposition 11.1.

Proof of Proposition 11.1. Write $\varepsilon_i := \rho_{i+1} - \rho_i$, $i = 1, 2, 3, \dots$ The ρ-equation at level $(j+1)$ is, by (11.2),

$$\phi_{j+2}(\rho_{j+1}, \rho_j, \dots) = \frac{1}{2}\big(\rho_{j+1}\phi_{j+1}(\rho_j, \rho_{j-1}, \dots) + 1\big).$$

By two applications of (11.4) (with $\alpha = 0.31$), this implies that

$$\phi_{j+1}(\rho_{j+1}, \rho_j, \dots) = \frac{1}{2}\big(\rho_{j+1}\phi_j(\rho_j, \rho_{j-1}, \dots) + 1\big) + O(0.155^j).$$

Subtracting (11.2), the ρ-equation at level j, from this gives

$$\begin{aligned}\phi_{j+1}(\rho_{j+1},\rho_j,\dots)-\phi_{j+1}(\rho_j,\rho_{j-1},\dots)\\ =\frac{\rho_{j+1}}{2}\big(\phi_j(\rho_j,\rho_{j-1},\dots)-\phi_j(\rho_{j-1},\rho_{j-2},\dots)\big)+\frac{\varepsilon_j}{2}\phi_j(\rho_j,\rho_{j-1},\dots)+O(0.155^j).\end{aligned}\tag{11.7}$$

Now by the mean value theorem,

$$|\phi_{j+1}(\rho_{j+1},\rho_j,\dots)-\phi_{j+1}(\rho_j,\rho_{j-1},\dots)|\leqslant\Delta_1|\varepsilon_j|+\cdots+\Delta_j|\varepsilon_1|\tag{11.8}$$

and

$$|\phi_j(\rho_j,\rho_{j-1},\dots)-\phi_j(\rho_{j-1},\rho_{j-2},\dots)|\leqslant\Delta_1|\varepsilon_{j-1}|+\cdots+\Delta_{j-1}|\varepsilon_1|.\tag{11.9}$$

Therefore, from (11.7), the triangle inequality and the fact that $\frac{\rho_{j+1}}{2}\leqslant\frac{\rho_1}{2}\leqslant 0.155$ (cf. Lemma 11.2), we have

$$\begin{aligned}|\varepsilon_j|\Big(\frac{1}{2}\phi_j(\rho_j,\rho_{j-1},\dots)-\Delta_1\Big)\leqslant(\Delta_2+0.155\Delta_1)|\varepsilon_{j-1}|+(\Delta_3+0.155\Delta_2)|\varepsilon_{j-2}|+\cdots\\ +O(0.155^j).\end{aligned}\tag{11.10}$$

Now by Lemma 11.4 and Proposition 11.6,

$$\frac{1}{2}\phi_j(\rho_j,\rho_{j-1},\dots)-\Delta_1>\frac{1}{4}\log 3-0.17>0.104.$$

Also, by Proposition 11.6 we have

$$(\Delta_2+0.155\Delta_1)+(\Delta_3+0.155\Delta_2)+\cdots<0.096.$$

Therefore (11.10) implies a bound

$$|\varepsilon_j|\leqslant c_1|\varepsilon_{j-1}|+c_2|\varepsilon_{j-2}|+\cdots+c_{j-1}|\varepsilon_1|+2^{-j},\tag{11.11}$$

for all $j\geqslant j_0$, where $c_1,c_2,\dots$ are fixed nonnegative constants with $\sum_i c_i<\frac{0.096}{0.104}<0.93$ and, by Proposition 11.6, $c_i\leqslant 2^{-i}$ for all $i\geqslant i_0$ for some i_0. It is convenient to assume that $i_0,j_0\geqslant 10$, which we clearly may.

We claim that (11.11) implies exponential decay of the ε_j, which of course immediately implies Theorem 11.1. To see this, take $\delta\in(0,\frac{1}{4})$ so small that $0.94(1-\delta)^{-i_0}<0.99$, and then take $A\geqslant 100$ large enough that $|\varepsilon_j|\leqslant A(1-\delta)^j$ for all $j\leqslant j_0$. We claim that the same bound holds for all j, which follows immediately by induction using (11.11) provided one can show that

$$\sum_{i\geqslant 1}c_i(1-\delta)^{-i}+\frac{1}{A}\Big(\frac{1}{2(1-\delta)}\Big)^j<1\tag{11.12}$$

for $j\geqslant j_0$. Since $\delta<\frac{1}{2}$ and $A\geqslant 100$, it is enough to show that $\sum_{i\geqslant 1}c_i(1-\delta)^{-i}<0.99$. The contribution to this sum from $i\leqslant i_0$ is at most $0.93(1-\delta)^{-i_0}$, whereas the contribution from $i>i_0$ is (by summing the geometric series) at most $\sum_{i>i_0}2^{-i}(1-\delta)^{-i}<2\cdot 2^{-i_0}(1-\delta)^{-i_0}<0.01(1-\delta)^{-i_0}$. Therefore the desired bound follows from our choice of δ. □

11.5. **Self-similarity for derivatives**

Our remaining task is to prove the derivative bounds in Proposition 11.6. Once again we use self-similarity properties of the ϕ_j, but now for their derivatives, the key point being that $\partial_m\phi_j\approx\partial_m\phi_{j-1}$. Here is a precise statement.

Proposition 11.7. *Suppose that $C = \pi(C_1 \times C_2)$ is cell at level j. Let $\alpha \in [0,1)$ and $m \geqslant 1$, and suppose that $0 \leqslant x_i \leqslant \alpha$ for all i. Then we have*

$$0 \leqslant \partial_m \psi^C(\mathbf{x}) \leqslant 2^{\sum_{i=1}^m \alpha^{j-i}} \big(\partial_m \psi^{C_1}(\mathbf{x}) + \partial_m \psi^{C_2}(\mathbf{x}) + \alpha^{j-2}\log 2\big).$$

In particular, taking $C = \Gamma_j = \pi(\Gamma_{j-1} \times \Gamma_{j-1})$, we have

$$0 \leqslant \partial_m \phi_j(\mathbf{x}) \leqslant 2^{\sum_{i=1}^m \alpha^{j-i}} \Big(\partial_m \phi_{j-1}(\mathbf{x}) + \Big(\frac{\alpha}{2}\Big)^j \frac{\log 2}{\alpha^2}\Big). \tag{11.13}$$

Proof. The lower bound follows by noticing that ψ^C is increasing in each variable. Now, we turn to the upper bound. First observe that we may assume that $m \leqslant j-1$, for when $m \geqslant j$, $\partial_m \phi_j(\mathbf{x})$ is identically zero. We proceed by induction on m, first establishing the case $m = 1$. Differentiating (11.5) gives

$$e^{\psi^C(\mathbf{x})} \partial_1 \psi^C(\mathbf{x}) = \sum_{C \to C'} \psi^{C'}(T\mathbf{x}) e^{x_1 \psi^{C'}(T\mathbf{x})}.$$

By two applications of the upper bound in Proposition 11.5 (to $C' = \pi(C_1' \times C_2')$), we obtain

$$e^{\psi^C(\mathbf{x})} \partial_1 \psi^C(\mathbf{x}) \leqslant 2^{\alpha^{j-1}} \sum_{\substack{C_1 \to C_1' \\ C_2 \to C_2'}} \big(\psi^{C_1'}(T\mathbf{x}) + \psi^{C_2'}(T\mathbf{x}) + \alpha^{j-2}\log 2\big) e^{x_1(\psi^{C_1'}(T\mathbf{x}) + \psi^{C_2'}(T\mathbf{x}))}. \tag{11.14}$$

On the other hand, for $i = 1, 2$ we get by differentiating the recurrence

$$e^{\psi^{C_i}(\mathbf{x})} = \sum_{C_i \to C_i'} e^{x_1 \psi^{C_i'}(T\mathbf{x})} \tag{11.15}$$

with respect to x_1 that

$$e^{\psi^{C_i}(\mathbf{x})} \partial_1 \psi^{C_i}(\mathbf{x}) = \sum_{C_i \to C_i'} \psi^{C_i'}(T\mathbf{x}) e^{x_1 \psi^{C_i'}(T\mathbf{x})}. \tag{11.16}$$

Substituting (11.15) and (11.16) into (11.14) gives

$$e^{\psi^C(\mathbf{x})} \partial_1 \psi^C(\mathbf{x}) \leqslant 2^{\alpha^{j-1}} \big(\partial_1 \psi^{C_1}(\mathbf{x}) + \partial_1 \psi^{C_2}(\mathbf{x}) + \alpha^{j-2}\log 2\big) e^{\psi^{C_1}(\mathbf{x}) + \psi^{C_2}(\mathbf{x})}.$$

Finally, Proposition 11.5 implies that $e^{\psi^{C_1}(\mathbf{x}) + \psi^{C_2}(\mathbf{x})} \leqslant e^{\psi^C(\mathbf{x})}$. Dividing both sides by $e^{\psi^C(\mathbf{x})}$ gives the result when $m = 1$.

Now we turn to the cases $m \geqslant 2$. Differentiating (11.5) with respect to x_m and applying (11.6) gives

$$e^{\psi^C(\mathbf{x})} \partial_m \psi^C(\mathbf{x}) = \sum_{C \to C'} x_1 e^{x_1 \psi^{C'}(T\mathbf{x})} \partial_{m-1} \psi^{C'}(T\mathbf{x}). \tag{11.17}$$

By the inductive hypothesis, if $C' = \pi(C_1' \times C_2')$ we have

$$\partial_{m-1} \psi^{C'}(T\mathbf{x}) \leqslant 2^{\sum_{i=2}^m \alpha^{j-i}} \Big(\partial_{m-1} \psi^{C_1'}(T\mathbf{x}) + \partial_{m-1} \psi^{C_2'}(T\mathbf{x}) + \alpha^{j-3}\log 2\Big). \tag{11.18}$$

Also, by the upper bound in Proposition 11.5, we have

$$\psi^{C'}(T\mathbf{x}) \leqslant \psi^{C_1'}(T\mathbf{x}) + \psi^{C_2'}(T\mathbf{x}) + \alpha^{j-2}\log 2. \tag{11.19}$$

Substituting (11.18) and (11.19) into (11.17) and using the assumption that $0 \leqslant x_1 \leqslant \alpha$ gives

$$e^{\psi^C(\mathbf{x})}\partial_m\psi^C(\mathbf{x}) \leqslant 2^{\sum_{i=1}^m \alpha^{j-i}} \times \sum_{\substack{C_1\to C_1'\\ C_2\to C_2'}} x_1\Big[\partial_{m-1}\psi^{C_1'}(T\mathbf{x}) + \partial_{m-1}\psi^{C_2'}(T\mathbf{x}) + \alpha^{j-3}\log 2\Big] e^{x_1(\psi^{C_1'}(T\mathbf{x})+\psi^{C_2'}(T\mathbf{x}))}. \tag{11.20}$$

Now, differentiating the recurrence (11.15) with respect to x_m (using (11.6)) gives, for $i = 1, 2$,

$$e^{\psi^{C_i}(\mathbf{x})}\partial_m\psi^{C_i}(\mathbf{x}) = \sum_{C_i\to C_i'} x_1 e^{x_1\psi^{C_i'}(T\mathbf{x})}\partial_{m-1}\psi^{C_i'}(T\mathbf{x}). \tag{11.21}$$

Substituting (11.15) and (11.21) into (11.20), and using once again that $x_1 \leqslant \alpha$, gives

$$e^{\psi^C(\mathbf{x})}\partial_m\psi^C(\mathbf{x})e^{\psi^C(\mathbf{x})} \leqslant 2^{\sum_{i=1}^m \alpha^{j-i}}\Big(\partial_m\psi^{C_1}(\mathbf{x}) + \partial_m\psi^{C_2}(\mathbf{x}) + \alpha^{j-2}\log 2\Big)e^{\psi^{C_1}(\mathbf{x})+\psi^{C_2}(\mathbf{x})}.$$

Again, Proposition 11.5 implies that $e^{\psi^{C_1}(\mathbf{x})+\psi^{C_2}(\mathbf{x})} \leqslant e^{\psi^C(\mathbf{x})}$, and so by dividing both sides by $e^{\psi^C(\mathbf{x})}$, we obtain the stated result. □

Before proving Proposition 11.6, we isolate a lemma.

Lemma 11.8. *For $0 \leqslant x \leqslant 0.31$ we have $0 \leqslant 4\phi_2'(x) \leqslant 0.481$.*

Proof. From $e^{4\phi_2(x)} = 3^x + 4\cdot 2^x + 4$ we obtain

$$4\phi_2'(x) = \frac{\log 3\cdot 3^x + \log 2\cdot 4\cdot 2^x}{3^x + 4\cdot 2^x + 4}.$$

The lemma is therefore equivalent to $\frac{1}{4}(\log 3 - 0.481)3^x + (\log 2 - 0.481)2^x \leqslant 0.481$. The left-hand side here is increasing in x and, when $x = 0.31$, it is $0.480052\cdots$. □

Proof of Proposition 11.6. Henceforth, set $\alpha := 0.31$. Again, we may assume that $j \geqslant m+1$, as $\partial_m\phi_j(\mathbf{x}) = 0$ when $j \leqslant m$. If we apply (11.13) ℓ times we obtain

$$\begin{aligned} 0 \leqslant \partial_m\phi_j(\mathbf{x}) &\leqslant A_m^{\alpha^{j-m}+\cdots+\alpha^{j-m-(\ell-1)}}\partial_m\phi_{j-\ell}(\mathbf{x}) + \frac{\log 2}{\alpha^2}\sum_{k=0}^{\ell-1} A_m^{\alpha^{j-m}+\cdots+\alpha^{j-m-k}}\left(\frac{\alpha}{2}\right)^{j-k} \\ &\leqslant B_m^{\alpha^{j-m-(\ell-1)}}\partial_m\phi_{j-\ell}(\mathbf{x}) + \frac{\log 2}{\alpha^2}\sum_{k=0}^{\ell-1} B_m^{\alpha^{j-m-k}}\left(\frac{\alpha}{2}\right)^{j-k}, \end{aligned} \tag{11.22}$$

where

$$A_m := 2^{1+\alpha+\cdots+\alpha^{m-1}} \quad \text{and} \quad B_m := 2^{\frac{1+\alpha+\cdots+\alpha^{m-1}}{1-\alpha}}.$$

Applying this with $\ell = j - s$, where $1 \leqslant s \leqslant m+1$, gives

$$\Delta_m \leqslant B_m^{\alpha^{s+1-m}}\Big(\sup_{0\leqslant x_i\leqslant 0.31}|\partial_m\phi_s(\mathbf{x})| + \frac{\log 2}{\alpha^2}\left(\frac{\alpha}{2}\right)^{s+1}\frac{1}{1-\alpha/2}\Big). \tag{11.23}$$

Here, we observed that all the $B_m^{\alpha^t}$ terms in (11.22) have $t \geqslant s+1-m$; bounding them all above by $B_m^{\alpha^{s+1-m}}$ then allowed us to sum a geometric series.

For $m = 1$ we take $s = 2$. Then Lemma 11.8 and relation (11.23) give

$$\Delta_1 \leqslant 2^{\alpha^2/(1-\alpha)}\left(\frac{0.481}{4} + \frac{\alpha\log 2}{8(1-\alpha/2)}\right) < 0.17,$$

as required. For $m \geqslant 2$ we take $s = m$. Then $\partial_m \phi_s \equiv 0$ and so (11.23) degenerates to

$$\Delta_m \leqslant B_m^\alpha \frac{\log 2}{\alpha^2} \left(\frac{\alpha}{2}\right)^{m+1} \frac{1}{1-\alpha/2}. \tag{11.24}$$

This gives $\Delta_2 < 0.05$, and also confirms that $\Delta_m \ll 0.155^m$. To bound $\sum_{m\geqslant 3} \Delta_m$ we use (11.24) and the uniform bound $B_m \leqslant 2^{1/(1-\alpha)^2}$, obtaining

$$\sum_{m\geqslant 3} \Delta_m \leqslant \frac{\alpha^2 \log 2}{16(1-\alpha/2)^2} 2^{\alpha/(1-\alpha)^2} < 0.01.$$

This completes the proof of Proposition 11.6. □

12. Calculating the ρ_i and ρ

In this section we conclude our analysis of the parameters $\boldsymbol{\rho} = (\rho_1, \rho_2, \ldots)$ for the binary flags. The situation so far is that we have shown that these parameters exist, are unique and lie in $(0, 0.31)$. Moreover, their limit $\rho = \lim_{i\to\infty} \rho_i$ exists (Proposition 11.1).

None of this helps with actually computing the limit numerically or giving any kind of closed form for it, and the objective of this section is to provide tools for doing that. We prove the following two results.

Proposition 12.1. *Define a sequence $a_{i,j}$ by the relations $a_{i,1} = 2$, $a_{i,2} = 2 + 2^{\rho_{i-1}}$ and*

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

Then

$$a_{i,i+1} = a_{i-1,i}^{\rho_{i-1}} e^{2^{i-1}}. \tag{12.1}$$

In practice, these relations are enough to calculate the ρ_j to high precision. Indeed, a short computer program produced the data in Table 1. (We suppress any discussion of the numerical precision of our routines.)

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

Table 1. Table of ρ_j

Using Proposition 12.1 we may obtain the following reasonably satisfactory description of ρ, which we stated in Theorem 2 (b).

Proposition 12.2. *Define a sequence a_j (depending on an arbitrary parameter $\rho \in (0,1)$) by*

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

Then the limit $\rho = \lim_{i\to\infty} \rho_i$ of the solutions to the ρ-equations satisfies the relation

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

The aim of this section is to establish Propositions 12.1 and 12.2. The more substantial task, which we handle first, is the former; the latter then follows from it by a limiting argument, given in subsection 12.2.

12.1. Product formula for $f^C(\rho)$ and a double recursion for the ρ_i

Proposition 12.1 is a short deduction from a product formula for $F(g)$, or equivalently for $f^C(\boldsymbol{\rho})$, given in Proposition 12.4 below. Whilst is would be a stretch to say that this formula is of independent interest, it is certainly a natural result to prove in the context of our work.

Before we state the formula, the reader should recall the notion of genotype g (Definition 10.1) and of the function $F(g)$ (Proposition 10.4). We require the following further small definition.

Definition 12.3 (Defects)**.** Let g be an i-genotype. For positive integer m we define the mth consolidation

$$g^{(m)} := \{A' \subset [i-m] : A' \cup X \in g \text{ for all } X \subset \{i-m+1, \cdots, i\}\}.$$

If $m \geqslant i+1$ then by convention we define $g^{(m)}$ to be empty. We define

$$\Delta^m(g) := |g^{(m-1)}| - 2|g^{(m)}|.$$

Remark. Note that $g^{(0)} = g$, $g^{(1)} = g^*$ and $g^{(m)} = (g^{(m-1)})^*$. It is easy to see that $\Delta^m(g)$ is always a nonnegative integer. Observe that $\Delta^{i+1}(g) = 0$ unless $g = \mathcal{P}[i]$, in which case $\Delta^{i+1}(g) = 1$, and that $\Delta^m(g) = 0$ whenever $m > i+1$.

Proposition 12.4. *Suppose that g is an i-genotype. Then*

$$F(g) = \prod_m a_{i,m}^{\Delta^m(g)},$$

with the $a_{i,m}$ defined as in Proposition 12.1 above.

Proof of Proposition 12.1, given Proposition 12.4. From Proposition 12.4 and the observation that $\Delta^m(\mathcal{P}[i]) = 0$ unless $m = i+1$, we have $F(\mathcal{P}[i]) = a_{i,i+1}$. Thus $f^{\Gamma_i}(\boldsymbol{\rho}) = F(\mathcal{P}[i]) = a_{i,i+1}$. The equation (12.1) is then an immediate consequence of the ρ-equations (9.1). □

Before turning to the proof of Proposition 12.4, we isolate a couple of lemmas from the proof.

Lemma 12.5. *Let $\alpha \in \mathbb{R}$. Let g be an i-genotype, and suppose that k is an $(i-1)$-genotype with $k \leqslant g^*$. Then*

$$\sum_{\substack{g' \leqslant g \\ (g')^* = k}} \alpha^{|g'|} = (1+\alpha)^{\Delta^1(g)}(1+2\alpha)^{|g^*|-|k|}\alpha^{2|k|}.$$

Proof. For brevity, for any genotype g at level i and $A \subset [i]$ we write $g_A = \mathbf{1}_{A\in g}$, the indicator function of $A \in g$. For $A \subset [i-1]$, write $a = g'_A$ and $b = g'_{A\cup\{i\}}$. In this notation, the sum is

$$\prod_{A\subseteq[i-1]} T_A, \qquad T_A := \sum_{\substack{0\leqslant a\leqslant g_A\\ 0\leqslant b\leqslant g_{A\cup\{i\}}\\ ab=k_A}} \alpha^{a+b}.$$

Table 2 then contains all of the information needed to complete the calculation. □

$(g_A, g_{A\cup\{i\}})$	g^*_A	k_A	(a,b)	T_A	$\#A$
$(0,0)$	0	0	$(0,0)$	1	
$(0,1)$	0	0	$(0,0)$ or $(0,1)$		
$(1,0)$	0	0	$(0,0)$ or $(1,0)$	$1+\alpha$	$\lvert g\rvert - 2\lvert g^*\rvert = \Delta^1(g)$
	1	1	$(1,1)$	α^2	$\lvert k\rvert$
$(1,1)$	1	0	$(0,0)$, $(1,0)$ or $(0,1)$	$1+2\alpha$	$\lvert g^*\rvert - \lvert k\rvert$

TABLE 2. Combinatorics of genotypes

For $\mathbf{a} = (a_1, a_2, \cdots)$, and for some ($i$-)genotype g, write

$$P_{\mathbf{a}}(g) := \prod_m a_m^{\Delta^m(g)}. \tag{12.2}$$

If $\theta \in \mathbb{R}_{>0}$, define

$$\Phi_{\theta,\mathbf{a}}(g) := \sum_{g'\leqslant g} \theta^{|g|-|g'|} P_{\mathbf{a}}(g'). \tag{12.3}$$

Lemma 12.6. *We have the functional equation*

$$\Phi_{\theta,\mathbf{a}}(g) = (\theta + a_1)^{\Delta^1(g)} \Phi_{\theta^2+2a_1\theta,T\mathbf{a}}(g^*).$$

As before, $T\mathbf{a}$ denotes the shift operator $T\mathbf{a} = (a_2, a_3, \cdots)$.

Proof. Using the relation $P_{\mathbf{a}}(g') = a_1^{\Delta^1(g')} P_{T\mathbf{a}}((g')^*)$, we have

$$\begin{aligned}\Phi_{\theta,\mathbf{a}}(g) &= \theta^{|g|} \sum_{g'\leqslant g} \left(\frac{a_1}{\theta}\right)^{|g'|} \left(\frac{1}{a_1^2}\right)^{|(g')^*|} P_{T\mathbf{a}}((g')^*)\\ &= \theta^{|g|} \sum_{k\leqslant g^*} \left(\frac{1}{a_1^2}\right)^{|k|} P_{T\mathbf{a}}(k) \sum_{\substack{g'\leqslant g\\ (g')^*=k}} \left(\frac{a_1}{\theta}\right)^{|g'|}.\end{aligned}$$

The result now follows from Lemma 12.5 and a routine short calculation. □

We are now in a position to prove Proposition 12.4.

Proof of Proposition 12.4. Let $a_{i,m}$ be as in the statement of Proposition 12.4, and write $\mathbf{a}_i = (a_{i,1}, a_{i,2}, \cdots)$. In the notation introduced above (cf. (12.2)) the claim of Proposition 12.4 is then that

$$F(g) = P_{\mathbf{a}_i}(g). \tag{12.4}$$

We proceed by induction on i. Suppose that we have the result for $(i-1)$-genotypes, and let g be an i-genotype. By (10.3) it follows immediately that

$$F(g) = 2^{\Delta^1(g)}\Phi_{2,\mathbf{a}_{i-1}^{\rho_{i-1}}}(g^*). \tag{12.5}$$

Here, Φ is as defined in (12.3), and $\mathbf{a}_{i-1}^{\rho_{i-1}}$ is shorthand for $(a_{i-1,1}^{\rho_{i-1}}, a_{i-1,2}^{\rho_{i-1}}, \dots)$. The fact that the RHS of (12.5) is a product $P_*(g)$ is now clear by iterated application of Lemma 12.6. To get a handle on exactly which product, suppose that the result of applying Lemma 12.6 $j-1$ times is that

$$F(g) = \Big(\prod_{m=1}^{j} a_{i,m}^{\Delta^m(g)}\Big)\Phi_{b_{i,j},T^{j-1}(\mathbf{a}_{i-1}^{\rho_{i-1}})}(g^{(j)}).$$

Thus $a_{i,1} = b_{i,1} = 2$ and we have the relations

$$a_{i,j+1} = b_{i,j} + a_{i-1,j}^{\rho_{i-1}} \tag{12.6}$$

and

$$b_{i,j+1} = b_{i,j}^2 + 2a_{i-1,j}^{\rho_{i-1}} b_{i,j}. \tag{12.7}$$

Substituting (12.6) into (12.7) gives the claimed recurrence in terms of the a's only. □

12.2. **A single recurrence for ρ**

In this section we derive Proposition 12.2 from Proposition 12.1 by a limiting argument.

To carry this out, we will need the following fairly crude estimates for the $a_{i,j}$.

Lemma 12.7. *We have $3^{2^{j-2}} \leqslant a_{i,j} \leqslant 2^{2^{j-1}}$ for all i, j.*

Proof. First note that a simple induction using the recursion for the a's in Proposition 12.1 gives

$$a_{i,j+1} \leqslant a_{i,j}^2 \tag{12.8}$$

for all i, j. This immediately confirms the upper bound in the lemma, by another trivial induction.

For the lower bound, first note that all the a's are $\geqslant 1$ by a simple induction using (12.6). Therefore, from (12.7), we have the inequality

$$b_{i,j+1} + 1 \geqslant (b_{i,j}+1)^2. \tag{12.9}$$

By yet another trivial induction, this implies that

$$b_{i,j} \geqslant 3^{2^{j-1}} - 1.$$

Finally, the lower bound on the a's follows from this and (12.6). □

Now let us return to the relations (12.6) and (12.7) that involve the auxiliary parameters $b_{i,j}$. It is a simple matter to check that

$$\frac{b_{i,j+1}}{b_{i,j}^2} = \frac{a_{i,j+1} + a_{i-1,j}^{\rho_{i-1}}}{a_{i,j+1} - a_{i-1,j}^{\rho_{i-1}}}.$$

By a simple induction using (12.6) and (12.7) we see that $a_{u,v}, b_{u,v} > 0$, and so both the numerator and the denominator here are positive. Taking logs and summing, we obtain

$$\frac{\log b_{i,i}}{2^{i-1}} = \log 2 + \sum_{j=1}^{i-1} \frac{1}{2^j} \log\Big(\frac{a_{i,j+1} + a_{i-1,j}^{\rho_{i-1}}}{a_{i,j+1} - a_{i-1,j}^{\rho_{i-1}}}\Big). \tag{12.10}$$

By Lemma 12.7, we easily obtain

$$\frac{a_{i,j+1}+a_{i-1,j}^{\rho_{i-1}}}{a_{i,j+1}-a_{i-1,j}^{\rho_{i-1}}} = 1 + O\big((2/3)^{2^{j-1}}\big).$$

Thus the sum in (12.10) is extremely rapidly convergent and we may take limits as $i \to \infty$, noting that $a_j = \lim_{i\to\infty} a_{i,j}$, to obtain

$$\lim_{i\to\infty} \frac{\log b_{i,i}}{2^{i-1}} = \log 2 + \sum_{j=1}^{\infty} \frac{1}{2^j} \log\Big(\frac{a_{j+1}+a_j^{\rho}}{a_{j+1}-a_j^{\rho}}\Big).$$

Another easy application of (12.7) (and (12.6)) gives $a_{i,i+1} \sim b_{i,i}$, and so we deduce that

$$\lim_{i\to\infty} \frac{\log a_{i,i+1}}{2^{i-1}} = \log 2 + \sum_{j=1}^{\infty} \frac{1}{2^j} \log\Big(\frac{a_{j+1}+a_j^{\rho}}{a_{j+1}-a_j^{\rho}}\Big). \tag{12.11}$$

To conclude the argument from here, we use (12.1) (that is, the ρ-equations). Telescoping, we have

$$\begin{aligned} a_{i,i+1} = \exp(2^{i-1}) a_{i-1,i}^{\rho_{i-1}} &= \exp(2^{i-1}+\rho_{i-1}2^{i-2}) a_{i-2,i-1}^{\rho_{i-2}\rho_{i-1}} = \cdots \\ &= \exp\Big(2^{i-1} + \sum_{j=1}^{i-2} (\rho_{i-j}\cdots\rho_{i-1}) 2^{i-j-1}\Big) a_{1,2}^{\rho_1\cdots\rho_{i-1}}. \end{aligned}$$

Taking limits as $i \to \infty$ easily gives

$$\lim_{i\to\infty} \frac{\log a_{i,i+1}}{2^{i-1}} = 1 + \frac{\rho}{2} + \Big(\frac{\rho}{2}\Big)^2 + \ldots = \frac{1}{1-\rho/2}.$$

Comparing with (12.11) completes the proof of Proposition 12.2.

12.3. **Proof of Theorem 2 (b)**

To conclude the paper, we complete the proof of Theorem 2 (b). In fact, all of the ingredients have already been assembled and we must simply remark on how they fit together.

First, recall from Definition 9.6 that

$$\theta_r = (\log 3 - 1) \Big/ \Big(\log 3 + \sum_{i=1}^{r-1} \frac{2^i}{\rho_1 \cdots \rho_i} \Big).$$

Now, it is an easy exercise to see that if $x_1, x_2, \ldots$ is a sequence of positive real numbers for which $x = \lim_{i\to\infty} x_i$ exists and is positive, then

$$\lim_{r\to\infty} \Big(\sum_{i=1}^{r} x_1 \cdots x_i \Big)^{1/r} = \max(x, 1).$$

Applying this with $x_i = 2/\rho_i$ gives, by Proposition 11.1, that

$$\lim_{r\to\infty} \theta_r^{1/r} = \frac{\rho}{2}.$$

This, together with Proposition 12.2, completes the proof of Theorem 2.

APPENDIX

APPENDIX A. SOME PROBABILISTIC LEMMAS

Throughout this section, $\mathbf{A} \subset \mathbb{N}$ will be a random set, with $\mathbb{P}(i \in \mathbf{A}) = 1/i$ and these choices being independent for different values of i.

Lemma A.1. *For any finite subset $B \subset \mathbb{N}$ and any $k \in \mathbb{Z}_{\geqslant 0}$, we have*

$$\left(1 - O\left(\frac{k^2(\sum_{m\in B} 1/(m-1))^{-2}}{\min B}\right)\right) M \leqslant \mathbb{P}(\#(\mathbf{A}\cap B) = k) \leqslant M$$

where

$$M = \frac{1}{k!}\Big(\sum_{m\in B}\frac{1}{m-1}\Big)^k \prod_{m\in B}\Big(1-\frac{1}{m}\Big).$$

Proof. The result follows by a standard inclusion-exclusion argument. The upper bound is easier to establish: we have

$$\begin{aligned}\mathbb{P}(\#(\mathbf{A}\cap B) = k) &= \sum_{\substack{a_1,\dots,a_k\in B\\ a_1<\dots<a_k}} \frac{1}{a_1\cdots a_k} \prod_{\substack{m\in B\\ m\notin\{a_1,\dots,a_k\}}}\Big(1-\frac{1}{m}\Big)\\ &= \prod_{m\in B}\Big(1-\frac{1}{m}\Big)\sum_{\substack{a_1,\dots,a_k\in B\\ a_1<\dots<a_k}}\frac{1}{(a_1-1)\cdots(a_k-1)} \leqslant M.\end{aligned}$$

For the lower bound, we note that the difference

$$\frac{1}{k!}\Big(\sum_{m\in B}\frac{1}{m}\Big)^k - \sum_{\substack{a_1,\dots,a_k\in B\\ a_1<\dots<a_k}}\frac{1}{a_1\cdots a_k}$$

is bounded by the sum over those k-tuples with $a_i = a_j$ for some j, which gives the bound stated. □

Combining this with standard bounds on the tails of the Poisson distribution, we deduce the following.

Lemma A.2. *Uniformly for $B \subset \mathbb{N}$ with $\lambda := \sum_{m\in B} 1/m \geqslant 1$, we have*

$$\mathbb{P}\Big(\big|\#(\mathbf{A}\cap B) - \lambda\big| > \varepsilon\lambda\Big) \ll \exp(-\varepsilon^2\lambda/3).$$

Uniformly for $v \geqslant 2u \geqslant 4$ and $\alpha \geqslant 1$ we have

$$\mathbb{P}\Big(\#(\mathbf{A}\cap B) \geqslant (1+\alpha)\lambda\Big) \ll \exp\big(-\lambda(\alpha\log\alpha - \alpha + 1)\big).$$

Lemma A.3. *For any $x > 0$ and finite set $B \subset \mathbb{N}$,*

$$\mathbb{E}x^{\#(\mathbf{A}\cap B)} \leqslant \exp\Big((x-1)\sum_{j\in B}\frac{1}{j}\Big).$$

Proof. The random variable $\#(\mathbf{A}\cap B)$ is the sum of independent Bernouilli random variables and thus

$$\mathbb{E}x^{\#(\mathbf{A}\cap B)} = \prod_{j\in B}\left(1+\frac{x-1}{j}\right).$$

The lemma now follows from the inequality $1+y\leqslant e^y$, valid for all real y. □

Lemma A.4. *Given a finite sets $B\subset G$, with $\sum_{m\in G}1/m\geqslant 1/2$ and $|B|=k$,*

$$\mathbb{P}\big(\mathbf{A}\cap G=B\big|\#(\mathbf{A}\cap G)=k\big)=\frac{k!(1+O(\frac{k^2}{\min(G)}))}{(\sum_{m\in G}1/(m-1))^k}\prod_{b\in B}\frac{1}{b}\prod_{m\in G}\left(1-\frac{1}{m}\right).$$

Proof. Since $|B|=k$, we have

$$\mathbb{P}\big(\mathbf{A}\cap G=B\,\big|\,\#(\mathbf{A}\cap G)=k\big)=\frac{\mathbb{P}(\mathbf{A}\cap G=B)}{\mathbb{P}(\#(\mathbf{A}\cap G)=k)}.$$

The denominator is estimated using Lemma A.1, whereas for the numerator we simply note that

$$\mathbb{P}(\mathbf{A}\cap G=B)=\prod_{b\in B}\frac{1}{b}\prod_{m\in G\setminus B}\left(1-\frac{1}{m}\right)=\prod_{b\in B}\frac{1}{b-1}\prod_{m\in G}\left(1-\frac{1}{m}\right).$$

This completes the proof of the lemma. □

Lemma A.5. *Given $0<c<1$ and $D\geqslant e^{100/c}$, the probability that $\mathbf{A}\subset(D^c,D]$ satisfies*

$$\Big|\#\big(\mathbf{A}\cap(D^\alpha,D^\beta]\big)-(\beta-\alpha)\log D\Big|\leqslant(\log D)^{3/4}\quad(c\leqslant\alpha\leqslant\beta\leqslant 1)\tag{A.1}$$

is $\geqslant 1-O(e^{-(1/4)(\log D)^{1/2}})$.

Proof. It suffices to bound the probability that

$$\Big|\#\mathbf{A}\cap(D^\alpha,D^\beta]-(\beta-\alpha)\log D\Big|\geqslant(\log D)^{3/4}-2\tag{A.2}$$

whenever $\alpha\log D,\beta\log D\in\mathbb{N}$. The random variable $N=N(\alpha,\beta)$, which counts $\#(\mathbf{A}\cap(D^\alpha,D^\beta])$, is the sum of Bernouilli random variables and has expectation $\mathbb{E}N=M$, where

$$M=\sum_{D^\alpha<a\leqslant D^\beta}\frac{1}{a}=(\beta-\alpha)\log D+O(1).$$

By Lemma A.3, $\mathbb{E}\lambda^N\leqslant e^{(\lambda-1)M}$. Thus, for $y=(\log D)^{2/3}+O(1)$ and $\lambda_j=1+(-1)^j\frac{y}{\log D}$ we have

$$\mathbb{P}(N\geqslant M+y)\leqslant\mathbb{E}\lambda_2^{N-M-y}\ll\lambda_2^{-M-y}e^{(\lambda_2-1)M}\ll e^{-(1/3)(\log D)^{1/2}},$$
$$\mathbb{P}(N\leqslant M-y)\leqslant\mathbb{E}\lambda_1^{N-M+y}\ll\lambda_1^{-M-y}e^{(\lambda_1-1)M}\ll e^{-(1/3)(\log D)^{1/2}}.$$

Summing over all possible α,β completes the proof. □

Lemma A.6. *Uniformly for $X\geqslant 2$ we have*

$$\sum_{a\in\mathbf{A}\cap[2,X]}a\leqslant X/\delta$$

with probability $\geqslant 1-e^{2-1/\delta}$.

Proof. We use Markov's inequality, often called Rankin's trick in this context:

$$\begin{aligned}\mathbb{P}\Big(\sum_{a\in\mathbf{A}\cap[2,X]} a > X/\delta\Big) &\leqslant e^{-1/\delta}\sum_{A'\subset[2,X]}\mathbb{P}\big(\mathbf{A}\cap[2,X]=A'\big)e^{\frac{1}{X}\sum_{a\in A'}a}\\ &= e^{-1/\delta}\sum_{A'\subset[2,X]}\prod_{\substack{2\leqslant a\leqslant X\\ a\notin A'}}\Big(1-\frac{1}{a}\Big)\prod_{a\in A'}\frac{e^{a/X}}{a}\\ &= e^{-1/\delta}\prod_{2\leqslant a\leqslant X}\Big(1-\frac{1}{a}\Big)\Big(1+\frac{e^{a/X}}{a}\Big)\\ &\leqslant e^{-1/\delta}(1+2/X)^X \leqslant e^{2-1/\delta}.\end{aligned}$$

This concludes the proof. □

Lemma A.7. *Let $J_1,\dots,J_d\subset\mathbb{N}$ be mutually disjoint intervals. Suppose that $X\subset J_1\times\cdots\times J_d$ is a set of size $\eta\prod_i \max J_i$. If $\min_i|J_i|$ is sufficiently large in terms of η and d, then with probability $\geqslant(\eta/4)^d$, there are distinct elements $a_i\in\mathbf{A}$ with $(a_1,\dots,a_d)\in X$.*

Proof. Let $M_i=\max J_i$ for each i. We will prove the lemma by induction on d.

The case $d=1$ follows by direct calculation: Suppose that $X\subset J_1$ has size $\geqslant\eta M_1$. Then

$$\mathbb{P}(\mathbf{A}\cap X=\emptyset)=\prod_{n\in X}(1-1/n)\leqslant(1-1/M_1)^{\eta M_1}\leqslant e^{-\eta}\leqslant 1-\eta/2.$$

One may establish the case of general d by induction. By a simple averaging argument, there is a set $Y\subset J_1$, $|Y|\geqslant(\eta/2)M_1$, such that if $j_1\in Y$ then

$$|X_{j_1}|\geqslant(\eta/2)M_2\cdots M_d,$$

where

$$X_{j_1}:=\{(j_2,\dots,j_d)\in J_2\times\cdots\times J_d:(j_1,j_2,\dots,j_d)\in X\}.$$

By the case $d=1$ (just described), $\mathbf{A}\cap Y$ is nonempty with probability $\geqslant\eta/4$. Fix some $a_1\in\mathbf{A}\cap Y$. Then, by the inductive hypothesis and the fact that the J_i are disjoint, with probability $\geqslant(\eta/4)^{d-1}$, independent of the choice of a_1, there are elements $a_i\in\mathbf{A}\cap J_i$, $i=2,\dots,d$ with $(a_2,\dots,a_d)\in X_{a_1}$, and therefore $(a_1,\dots,a_d)\in X$. The disjointness of the J_i of course guarantees that the a_i are all distinct. This completes the proof. □

Appendix B. Basic properties of entropy

The notion of entropy plays a key role in our paper. In this appendix we record the key facts about it that we need. Proofs may be found in many places. One convenient resource is [1].

If X is a random variable taking values in a finite set then we define

$$\mathbb{H}(X):=-\sum_x\mathbb{P}(X=x)\log(\mathbb{P}(X=x)),$$

where the log is to base e.

If $\mathbf{p}=(p_1,\dots,p_n)$ is a vector of probabilities (that is, if $p_1,\dots,p_n\geqslant 0$ and $p_1+\cdots+p_n=1$), then we write

$$\mathbb{H}(\mathbf{p}):=-\sum_{i=1}^n p_i\log p_i.$$

There should be no danger of confusing the two slightly different usages.

Our first lemma gives a simple upper bound for multinomial coefficients in terms of entropies.

Lemma B.1. *Let $n, n_1, \dots, n_k$ be non-negative integers with $\sum n_i = n$. Then*

$$\frac{n!}{n_1! \cdots n_k!} \leqslant e^{\mathbb{H}(\mathbf{p})n},$$

where $\mathbf{p} = (p_1, \dots, p_k)$ with $p_i := n_i/n$.

Proof. The right-hand side is $(n/n_1)^{n_1} \cdots (n/n_k)^{n_k}$. Now simply observe that

$$\frac{n!}{(n_1)! \cdots (n_k)!}(n_1/n)^{n_1} \cdots (n_k/n)^{n_k} \leqslant \sum_{k_1+\cdots+k_m=n} \frac{n!}{k_1! \cdots k_m!}(n_1/n)^{k_1} \cdots (n_k/n)^{k_m} = 1.$$

□

Our next lemma is a simple and well-known upper bound for the entropy.

Lemma B.2. *Let X be a random variable taking values in a set of size N. Then $\mathbb{H}(X) \leqslant \log N$.*

Proof. Follows immediately from the convexity of the function $L(x) = -x \log x$ and Jensen's inequality. See [1, Lemma 14.6.1 (i)]. □

The next lemma is simple and has no doubt appeared elsewhere, but we do not know an explicit reference. In its statement, we use the notation $\langle \mathbf{a}, \mathbf{p} \rangle = \sum_{i=1}^n a_i p_i$.

Lemma B.3. *Let $\mathbf{p} = (p_1, \dots, p_n)$ be a vector of probabilities, and let $\mathbf{a} = (a_1, \dots, a_n)$ be a vector of real numbers. Then*

$$\mathbb{H}(\mathbf{p}) + \langle \mathbf{a}, \mathbf{p} \rangle \leqslant \log\Big(\sum_{j=1}^n e^{a_j}\Big),$$

and equality occurs when $p_j = e^{a_j} / \sum_{i=1}^n e^{a_i}$.

Proof. The expression to be maximised may be rewritten as

$$\sum_{j=1}^n p_j \log(e^{a_j}/p_j).$$

Since the weights p_j sum to 1, we may use the concavity of the log function to conclude that

$$\sum_{j=1}^n p_j \log(e^{a_j}/p_j) \leqslant \log\Big(\sum_{j=1}^n p_j \frac{e^{a_j}}{p_j}\Big) = \log\Big(\sum_{j=1}^n e^{a_j}\Big).$$

It is easy to check that equality occurs when stated. □

The next lemma, known as the chain rule for entropy, is nothing more than a short computation.

Lemma B.4. *Let X, Y be random variables taking values in finite sets. Then*

$$\mathbb{H}(X, Y) = \mathbb{H}(Y) + \sum_y \mathbb{P}(Y = y)\mathbb{H}(X|Y = y).$$

Remark. The sum over y is usually written $\mathbb{H}(X|Y)$ and called the conditional entropy.

We will apply the preceding result together with the following observation.

Lemma B.5. *Suppose that X, Y are random variables with finite ranges and that Y is a deterministic function of X. Then $\mathbb{H}(X,Y) = \mathbb{H}(X)$.*

Proof. This follows from Lemma B.4 with the role of X and Y reversed, since all the entropies $\mathbb{H}(Y|X=x)$ are zero. □

The next result, known as the submodularity property of entropy, is a crucial ingredient in our paper.

Lemma B.6. . *Let X, Y, Z be any random variables taking values in finite sets. Then*

$$\mathbb{H}(X,Y) + \mathbb{H}(X,Z) \geqslant \mathbb{H}(X,Y,Z) + \mathbb{H}(X).$$

Proof. This is [1, Lemma 14.6.1 (iv)]. □

APPENDIX C. MAIER-TENENBAUM FLAGS

The purpose of this appendix is to say a little more about the bound (3.11), which corresponds in the language of this paper to [22, Theorem 1.4]. Numerically, this bound is $\tilde{\gamma}_{2^r} \gg (0.12885796477\ldots)^r$, which is a little weaker than the bound leading to Theorem 2, which is $\tilde{\gamma}_{2^r} \gg (0.140605674848\ldots)^r$. What is interesting, however, is that the flags $\mathscr{V}$ which lead to (3.11) are completely different to the binary flags which have been the main focus of our paper. The fact that these very different flags – the "Maier–Tenenbaum flags" – lead to a result which appears to be within 10 % of optimal suggests that they will have a key role to play in any future upper bound arguments for these questions.

Definition C.1 (Maier–Tenenbaum flag of order r)**.** Let $k = 2^r$ be a power of two. Identify $\mathbb{Q}^k$ with $\mathbb{Q}^{\mathcal{P}[r]}$ and define a flag $\mathscr{V}$, $\langle \mathbf{1} \rangle = V_0 \leqslant V_1 \leqslant \cdots \leqslant V_r \leqslant \mathbb{Q}^{\mathcal{P}[r]}$, as follows: $V_i = \mathrm{Span}_{\mathbb{Q}}(\mathbf{1}, \omega^1, \ldots, \omega^r)$, where $\omega^i_S = 1_{i \in S}$ for $S \subset [r]$.

Remark. We have $\dim(V_i) = i+1$ and in particular V_r is much smaller than $\mathbb{Q}^k$, in contrast to the situation for binary systems. We leave it to the reader to check that $\mathscr{V}$ is nondegenerate.

Recall that $\mathscr{V}$ gives rise to a tree structure, with the cells at level i being the intersections of cosets $x + V_i$ with the cube $\{0,1\}^k$ (cf. subsection 7.2). It is easy to check that this tree structure has a very simple form, with the cell $\Gamma_i = V_i \cap \{0,1\}^k$ being $\{\mathbf{0}, \mathbf{1}, \omega^1, \mathbf{1} - \omega^1, \ldots, \omega^i, \mathbf{1} - \omega^i\}$, this dividing into three children at level $i-1$; the cell Γ_{i-1} together with two singletons $\{\omega^i\}$ and $\{\mathbf{1} - \omega^i\}$.

The recursive definition of the quantities $f^C(\boldsymbol{\rho})$ (see (7.4)) therefore becomes $f^{\Gamma_1}(\boldsymbol{\rho}) = 3$,

$$f^{\Gamma_{j+1}}(\boldsymbol{\rho}) = f^{\Gamma_j}(\boldsymbol{\rho})^{\rho_j} + 2.$$

The ρ-equations (7.5) then become

$$f^{\Gamma_{j+1}}(\boldsymbol{\rho}) = e(f^{\Gamma_j}(\boldsymbol{\rho}))^{\rho_j},$$

from which we obtain

$$\rho_1 = \frac{\log 2 - \log(e-1)}{\log 3}, \qquad \rho_2 = \rho_3 = \cdots = \frac{\log 2 - \log(e-1)}{\log 2 + 1 - \log(e-1)} =: \kappa.$$

Assuming that the conditions of Proposition 7.7 hold, we therefore have

$$\gamma_k^{\mathrm{res}}(\mathscr{V}) = (\log 3 - 1) \Big/ \Big(\log 3 + \frac{1}{\rho_1}\Big(1 + \frac{1}{\kappa} + \cdots + \frac{1}{\kappa^{r-2}}\Big)\Big) = \Big(1 - \frac{1}{\log 3}\Big)\kappa^{r-1}.$$

Now it can be shown by explicit calculation that the conditions of Proposition 7.7 do hold. We merely state the conclusions of this, leaving the somewhat lengthy verification to the reader. The optimal measures μ_i are all induced from the measure μ^* in which

$$\mu^*(\mathbf{0}) = \mu^*(\omega^1) = \mu^*(\mathbf{1} - \omega^1) = \frac{1}{3}e^{1-r},$$

$$\mu^*(\omega^j) = \mu^*(\mathbf{1} - \omega^j) = \frac{1}{2}e^{j-r}(1 - \frac{1}{e}), \quad j = 2, \dots, r,$$

and then the optimal parameters $\mathbf{c}^*$ are given by

$$c_1^* = 1, \quad c_j^* = \frac{1}{\kappa^2}\Big(\frac{e-\kappa}{e-1}\Big)\Big(1 - \frac{1}{\log 3}\Big)\kappa^j, \quad c_{r+1}^* = \Big(1 - \frac{1}{\log 3}\Big)\kappa^{r-1}.$$

It can also be shown that $\gamma_k^{\mathrm{res}}(\mathscr{V}) = \gamma_k(\mathscr{V})$, by showing that the full entropy condition (3.6) follows from the restricted conditions (7.9). This is a little involved, but a fairly direct inductive argument can be made to work and this is certainly less subtle than the arguments of Section 8. In this way one may establish the bound

$$\gamma_{2^r} \geqslant \left(1 - \frac{1}{\log 3}\right)\left(\frac{\log 2 - \log(e-1)}{\log 2 + 1 - \log(e-1)}\right)^{r-1} \gg (0.131810543\dots)^r. \tag{C.1}$$

Finally, a relatively routine perturbative argument yields the same bound for $\tilde{\gamma}_{2^r}$.

It will be noted that (C.1) is strictly stronger than (3.11), the bound obtained in [22]. This is because, in essence, Maier and Tenenbaum chose slightly suboptimal measures and parameters on the system $\mathscr{V}$, roughly corresponding to $\mu(\omega^j) \sim 3^{j-r}$, which then leads to $c_j \sim \big(\frac{1-1/\log 3}{1-1/\log 27}\big)^j$.

REFERENCES

[1] N. ALON AND J. H. SPENCER, *The probabilistic method*, Wiley Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., Hoboken, NJ, fourth ed., 2016.

[2] R. ARRATIA, A. D. BARBOUR, AND S. TAVARÉ, *On random polynomials over finite fields*, Math. Proc. Cambridge Philos. Soc., 114 (1993), pp. 347–368.

[3] R. ARRATIA AND S. TAVARÉ, *The cycle structure of random permutations*, Ann. Probab., 20 (1992), pp. 1567–1591.

[4] P. D. T. A. ELLIOTT, *Probabilistic number theory. I*, vol. 239 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], Springer-Verlag, New York-Berlin, 1979. Mean-value theorems.

[5] P. D. T. A. ELLIOTT, *Probabilistic number theory. II*, vol. 240 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin-New York, 1980. Central limit theorems.

[6] P. ERDŐS, *On some applications of probability to analysis and number theory*, J. London Math. Soc., 39 (1964), pp. 692–696.

[7] P. ERDŐS, *On abundant-like numbers*, Canad. Math. Bull., 17 (1974), pp. 599–602.

[8] P. ERDŐS AND R. R. HALL, *The propinquity of divisors*, Bull. London Math. Soc., 11 (1979), pp. 304–307.

[9] P. ERDŐS AND J.-L. NICOLAS, *Répartition des nombres superabondants*, Bull. Soc. Math. France, 103 (1975), pp. 65–90.

[10] ——, *Méthodes probabilistes et combinatoires en théorie des nombres*, Bull. Sci. Math. (2), 100 (1976), pp. 301–320.

[11] P. ERDÖS, *On the density of some sequences of integers*, Bull. Amer. Math. Soc., 54 (1948), pp. 685–692.

[12] J. FRIEDLANDER AND H. IWANIEC, *Opera de cribro*, vol. 57 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI, 2010.

[13] R. R. HALL AND G. TENENBAUM, *On the average and normal orders of Hooley's Δ-function*, J. London Math. Soc. (2), 25 (1982), pp. 392–406.

[14] ——, *The average orders of Hooley's Δ_r-functions*, Mathematika, 31 (1984), pp. 98–109.
[15] ——, *The average orders of Hooley's Δ_r-functions. II*, Compositio Math., 60 (1986), pp. 163–186.
[16] ——, *Divisors*, vol. 90 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 1988.
[17] C. HOOLEY, *On a new technique and its applications to the theory of numbers*, Proc. London Math. Soc. (3), 38 (1979), pp. 115–151.
[18] D. KOUKOULOPOULOS, *Localized factorizations of integers*, Proc. London Math. Soc., 101 (2010), pp. 392–426.
[19] D. KOUKOULOPOULOS, *On the number of integers in a generalized multiplication table*, J. Reine Angew. Math., 689 (2014), pp. 33–99.
[20] H. MAIER AND G. TENENBAUM, *On the set of divisors of an integer*, Invent. Math., 76 (1984), pp. 121–128.
[21] ——, *On the normal concentration of divisors*, J. London Math. Soc. (2), 31 (1985), pp. 393–400.
[22] H. MAIER AND G. TENENBAUM, *On the normal concentration of divisors. II*, Math. Proc. Cambridge Philos. Soc., 147 (2009), pp. 513–540.
[23] G. TENENBAUM, *Sur la concentration moyenne des diviseurs*, Comment. Math. Helv., 60 (1985), pp. 411–428.
[24] ——, *Fonctions Δ de Hooley et applications*, in Séminaire de théorie des nombres, Paris 1984–85, vol. 63 of Progr. Math., Birkhäuser Boston, Boston, MA, 1986, pp. 225–239.
[25] G. TENENBAUM, *Crible d'ératosthène et modèle de Kubilius*, in Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 1099–1129.
[26] G. TENENBAUM, *Some of Erdős' unconventional problems in number theory, thirty-four years later*, in Erdös centennial, vol. 25 of Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, 2013, pp. 651–681.
[27] G. TENENBAUM, *Introduction to analytic and probabilistic number theory*, vol. 163 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, third ed., 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA–CHAMPAIGN, URBANA, ILLINOIS 61801

E-mail address: ford126@illinois.edu

MATHEMATICAL INSTITUTE, ANDREW WILES BUILDING, RADCLIFFE OBSERVATORY QUARTER, WOODSTOCK ROAD, OXFORD OX2 6GG, UK

E-mail address: ben.green@maths.ox.ac.uk

DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUE, UNIVERSITÉ DE MONTRÉAL, CP 6128 SUCC. CENTRE-VILLE, MONTRÉAL, QC H3C 3J7, CANADA

E-mail address: koukoulo@dms.umontreal.ca