Optimal sets of questions for Twenty Questions

Yuval Filmus[1] and Idan Mehalel[1]

[1]The Henry and Marilyn Taub Faculty of Computer Science, Technion, Israel. The research was funded by ISF grant 1337/16.

June 1, 2021

Abstract

In the distributional Twenty Questions game, Bob chooses a number x from 1 to n according to a distribution μ, and Alice (who knows μ) attempts to identify x using Yes/No questions, which Bob answers truthfully. Her goal is to minimize the expected number of questions.

The optimal strategy for the Twenty Questions game corresponds to a Huffman code for μ, yet this strategy could potentially uses all 2^n possible questions. Dagan et al. constructed a set of $1.25^{n+o(n)}$ questions which suffice to construct an optimal strategy for *all* μ, and showed that this number is optimal (up to sub-exponential factors) for infinitely many n.

We determine the optimal size of such a set of questions for *all* n (up to sub-exponential factors), answering an open question of Dagan et al. In addition, we generalize the results of Dagan et al. to the d-ary setting, obtaining similar results with 1.25 replaced by $1 + (d-1)/d^{d/(d-1)}$.

1 Introduction

The distributional Twenty Questions game is a cooperative game between two players, Alice and Bob. Bob picks an object in $X_n = \{x_1, \ldots, x_n\}$ according to a distribution μ known to both players, and Alice determines the object by asking Yes/No questions, to which Bob answers truthfully. Alice's goal is to minimize the expected number of questions she asks.

This game is often related to information theory (see [CT06], for example) as an interpretation of Shannon's entropy [Sha48]. Moreover, it is the prototypical example of a combinatorial search game [Kat73, AW87, ACD13]. It is also a model of *combinatorial group testing* [Dor43], and can be interpreted as a learning task in the *interactive learning* model [CAL94].

In this game, Alice's strategy corresponds to a prefix code: the code of $x \in X_n$ is the list of Bob's answers to all questions asked by Alice. Alice's optimal strategy therefore corresponds to a *minimum redundancy code* for μ. Huffman [Huf52] (and, independently, Zimmerman [Zim59]) showed how to construct such a strategy efficiently. However, the strategy produced by Huffman's algorithm could use arbitrary questions. We ask:

> What is the smallest set of questions that allows Alice to construct an optimal strategy for every distribution μ?

We call such a set of questions an *optimal* set of questions, and denote the minimum cardinality of an optimal set of questions for X_n by $q(n)$. We stress that the same set of questions must be used for *all* μ.

Surprisingly, it is possible to improve on the trivial set of all 2^n questions *exponentially*: Dagan et al. [DFGM17, DFGM19] showed that $q(n) \le 1.25^{n+o(n)}$, and furthermore, $q(n) \ge 1.25^{n-o(n)}$ for infinitely many n (specifically, n of the form $1.25 \cdot 2^k$). Thus 1.25 is the smallest constant C such that $q(n) \le C^{n+o(n)}$ for all n.

The fact that the lower bound $q(n) \ge 1.25^{n-o(n)}$ holds only for some n suggests that the upper bound $1.25^{n+o(n)}$ can be improved for other n. This is what our first main result shows:

Theorem 1.1. *There exists a function $G\colon [1,2) \to \mathbb{R}$ such that for $\beta \in [1,2)$,*

$$q(n) = 2^{-G(\beta)n \pm o(n)} \text{ for all } n \text{ of the form } n = \beta \cdot 2^k.$$

Furthermore, if $\beta \neq 1.25$ then

$$2^{-G(\beta)} < 1.25.$$

This confirms a conjecture of Dagan et al. The exact formula for $G(\beta)$ appears in Theorem 4.1.

Optimal sets of questions and fibers The proof of Theorem 1.1 relies on a result of Dagan et al.

Lemma 1.2. *A set of questions $\mathcal{Q}$ is optimal if for every dyadic distribution μ on X_n (that is, a distribution in which the probability of each elements is 2^{-k} for some $k \in \mathbb{N}_+$), there is a set $Q \in \mathcal{Q}$ of probability exactly $1/2$.*

Equivalently, $\mathcal{Q}$ is optimal if it hits $\mathrm{Spl}(\mu)$ for all dyadic μ, where

$$\mathrm{Spl}(\mu) = \{A : \mu(A) = 1/2\}.$$

To prove this result, Dagan et al. first show that a set of questions is optimal iff there is an optimal strategy for every dyadic distribution. Roughly speaking, given an arbitrary distribution ν, we construct a Huffman code C for ν and convert it to a distribution $\mu(x_i) = 2^{-|C(x_i)|}$. An optimal strategy for μ turns out to be an optimal strategy for ν.

Dagan et al. then show that an optimal strategy for a dyadic distribution must split the probability evenly at every step. Distributions encountered in this way could have elements whose probability is zero, but by choosing an element of minimal positive probability 2^{-k} and "splitting" it into elements of probability $2^{-k+1}, 2^{-k+2}, \ldots, 2^{-k+t}, 2^{-k+t}$ (where t is the number of zero probability elements), we can reduce to the case of distributions of full support.

It is easy to see that $\mathrm{Spl}(\mu)$ is an antichain: if $A \subsetneq B$ then $\mu(A) < \mu(B)$. It is less obvious that $\mathrm{Spl}(\mu)$ is a maximal antichain, as observed by Dagan et al. Indeed, given any set A, if $\mu(A) > 1/2$ and we arrange the elements of A in nonincreasing order of probability, then some prefix has probability exactly $1/2$, and so some subset of A belongs to $\mathrm{Spl}(\mu)$; and if $\mu(A) < 1/2$, then we can apply the same argument on $\overline{A}$ to find a superset of A in $\mathrm{Spl}(\mu)$.

These observations connect optimal sets of questions with another combinatorial object: *fibers*, defined by Lonc and Rival [LR87]. Given any poset, a *fiber* is a hitting set for the family of all maximal antichains. Any fiber of the lattice 2^{X_n} is thus an optimal set of questions.

Duffus, Sands and Winkler [DSW90] showed that every fiber of 2^{X_n} contains $\Omega(1.25^n)$ elements. To show this, they considered maximal antichains of the following form, for a parameter a:

$$S(B) = \{A, \overline{A} : A \subset B, |A| = a\}, \text{ where } |B| = 2a - 1.$$

It is easy to check that these are maximal antichains. There are $\binom{n}{2a-1}$ such maximal antichains, and each set in a fiber can handle at most $\binom{n-a}{a-1}$ of them, giving a lower bound of

$$\frac{\binom{n}{2a-1}}{\binom{n-a}{a-1}} \approx 2^{n(h(2\theta)-(1-\theta)h(\theta/(1-\theta))}, \quad \theta = \frac{a}{n}.$$

Here $h(p) = p\log_2(1/p) + (1-p)\log_2(1/(1-p))$ is the binary entropy. This expression is maximized at $\theta = 1/5$, giving a lower bound of roughly 1.25^n.

Dagan et al. used the exact same argument to prove their lower bound of $1.25^{n-o(n)}$ for optimal sets of questions. To this end, they needed to realize $S(B)$ as a set of the form $\mathrm{Spl}(\mu)$. The idea is to give all elements of B a probability of $1/2a$, and the remaining elements (the "tail") probabilities $1/4a, 1/8a, \ldots, 1/2^{n-2a+1}a, 1/2^{n-2a+1}a$; any set of measure $1/2$ must either contain the tail and $a-1$ elements of B, or must consist of a elements of B.

For this construction to work, we need $1/2a$ to be a negative power of 2, that is, we need a to be a power of 2. Since $a = n/5$, this works as long as n is of the form $1.25 \cdot 2^k$, or at least close to such a number. When n is close to $\beta \cdot 2^k$ for $\beta \in [1,2)$ other than 1.25, the sets $S(B)$ are not realizable in the form $\mathrm{Spl}(\mu)$.

In order to prove the lower bound part of Theorem 1.1, we identify, for each value of β, a more general collection of hard-to-hit maximal antichains which are realizable as $\mathrm{Spl}(\mu)$ for $n = \beta \cdot 2^k$. Instead of having a single set B of elements of equal probability together with a "tail", we allow several such sets $B_1, B_2, B_3, \ldots$, where the probability of elements in B_t is $1/2^t a$. This results in an expression for $G(\beta)$ which describes a game between Asker and Builder, in which Builder picks the proportions of the sets B_t, and Asker picks the type of questions which are best suited to handle the sets $S(B_1, B_2, B_3, \ldots)$; we leave the details to Section 3.

Dagan et al. showed that the bound 1.25^n is tight, by constructing an optimal set of questions of this size for every n. The bound is not tight for fibers of 2^{X_n}: Łuczak improved the lower bound $\Omega(1.25^n)$ to $\Omega(2^{n/3}) = \Omega(1.2599^n)$, as described in Duffus and Sands [DS01]. Lonc and Rival conjectured that the optimal size of a fiber of 2^{X_n} is $\Theta(2^{n/2})$, realized by the collection of all sets comparable with $\{x_1, \ldots, x_{\lfloor n/2 \rfloor}\}$. This is also the best known explicit construction of an optimal set of questions.

Instead of designing an optimal set of questions explicitly, Dagan et al. show that if we pick roughly 1.25^n random questions of each size, then with high probability we get an optimal set of questions. A similar approach works for proving the upper bound in Theorem 1.1, though the calculations are more intricate.

Much of the difficulty in proving Theorem 1.1 comes from the fact that $G(\beta)$ describes an idealized game between Asker and Builder which only makes sense in the limit $k \to \infty$, which we need to connect with the corresponding game for a fixed value of k. This difficulty doesn't come up in Dagan et al. since in their case, the optimal construction only has a single set B_1.

Computing $G(\beta)$ Unfortunately, the formula for $G(\beta)$ involves non-convex optimization over infinitely many variables, and for this reason we are unable to compute $G(\beta)$ beyond the already known value $G(1.25) = -\log_2 1.25$.

Nevertheless, our techniques allow us to improve the bound on $\max_\beta G(\beta)$ given by Dagan et al. Stated in terms of $q(n)$, Dagan et al. showed that $q(n) \geq 1.232^{n-o(n)}$ for every n, and we improve this to $q(n) \geq 1.236^{n-o(n)}$ for every n.

d-ary questions Our second main result concerns *d-ary questions*. What happens if Alice asks Bob d-ary questions, that is, questions with d possible answers? The optimal strategy in this case corresponds to a d-ary Huffman code, a setting already considered in Huffman's original paper.

We are able to generalize the main result of Dagan et al. to this setting:

Theorem 1.3. *Let $q^{(d)}(n)$ be the minimum cardinality of an optimal set of d-ary questions. For all n,*

$$q^{(d)}(n) \leq \left(1 + \frac{d-1}{d^{\frac{d}{d-1}}}\right)^{n+o(n)}.$$

Furthermore, this inequality is tight (up to sub-exponential factors) for infinitely many values of n.

This result holds not only for constant d, but also uniformly for all $d = o(n/\log^2 n)$. The techniques closely follow the ideas of Dagan et al., as outlined above in the case $d = 2$.

Theorem 1.3 shows that the magic constant 1.25 appearing in [DFGM19] generalizes to

$$1 + \frac{d-1}{d^{\frac{d}{d-1}}} = 2 - \Theta\left(\frac{\log d}{d}\right).$$

for arbitrary d.

We leave a combination of Theorem 1.1 and Theorem 1.3 to future work.

Paper organization After brief preliminaries (Section 2), we prove the first half of Theorem 1.1 in Sections 3–4. We prove the "furthermore" part of Theorem 1.1 and reprove some results of [DFGM19] using our framework in Section 5, in which we also derive the improved lower bound $1.236^{n-o(n)}$ (Theorem 5.3). Our results on d-ary questions appear in Section 6. Section 7 closes the paper with some open questions.

2 Preliminaries

Given a distribution π over $X_n = \{x_1, \ldots, x_n\}$, denote $\pi_i := \pi(x_i)$. For any set $S \subseteq X_n$ we denote the sum $\sum_{i \in S} \pi_i$ with $\pi(S)$.

2.1 Decision trees

We represent a strategy to reveal a secret element $x \in X_n$ as a *decision tree*. A decision tree is a binary tree $T = (V, E)$ such that every internal node $v \in V$ is labeled with a query $Q \subseteq X_n$, every leaf $l \in V$ is labeled with an object $x_i \in X_n$, and every edge $e \in E$ is labeled with "Yes" or "No". Moreover, if v is an internal node that is labeled with the query Q, and x is the secret element, then v has two outgoing edges: one is labeled with "Yes" (representing the decision "$x \in Q$") and the other with "No" (representing the decision "$x \notin Q$").

Given a set of queries $\mathcal{Q} \subseteq 2^{X_n}$ (which is called the set of *allowed questions*), we say that T is a *decision tree using* $\mathcal{Q}$ if for any internal node $v \in V$, the query Q that v is labeled with satisfies $Q \in \mathcal{Q}$.

Given a distribution π over X_n, we say that a decision tree T is *valid* for π if for any object $x \in \operatorname{supp}(\pi)$ there is a path in T that begins in the root and ends in a leaf that is labeled with x. The decision trees we will consider are only those in which each object $x \in X_n$ labels at most one leaf.

If there is a path from the root to $x \in X_n$, we say that the number of its edges is the depth of x, and denote this number with $T(x)$. If T is valid for π, the *cost* of T on π is $\sum_{i=1}^{n} \pi_i T(x_i)$.

2.2 Optimal sets of questions

For a distribution π, let $\operatorname{Opt}(\pi)$ be the minimum cost of a decision tree for π.

A set $\mathcal{Q} \subseteq 2^{X_n}$ of queries is *optimal* if for every distribution π, there is a decision tree using $\mathcal{Q}$ whose cost is $\operatorname{Opt}(\pi)$.

We denote the minimum cardinality of an optimal set of queries over X_n by $q(n)$. A major goal of this paper is to estimate $q(n)$ for all values of n. We do this using the concept of *maximum relative density*, borrowed from [DFGM19].

Definition 2.1. A distribution μ is *dyadic* if for all i, $\mu_i = 2^{-d}$ for some $d \in \mathbb{N}$ or $\mu_i = 0$.

If μ is a non-constant dyadic distribution, then a set $A \subseteq X_n$ *splits* μ if $\mu(A) = 1/2$. We denote the collection of all sets splitting μ by $\mathrm{Spl}(\mu)$, and the collection of all sets of size i splitting μ by $\mathrm{Spl}(\mu)_i$.

The *i'th relative density* of $\mathrm{Spl}(\mu)$ is

$$\rho_i(\mathrm{Spl}(\mu)) = \frac{|\mathrm{Spl}(\mu)_i|}{\binom{n}{i}}.$$

The *maximum relative density* of $\mathrm{Spl}(\mu)$ is

$$\rho(\mathrm{Spl}(\mu)) = \max_{i \in \{1,\ldots,n-1\}} \rho_i(\mathrm{Spl}(\mu)).$$

The following result reduces the calculation of $q(n)$, up to polynomial factors, to the calculation of the quantity

$$\rho_{\min}(n) = \min_{\mu} \rho(\mathrm{Spl}(\mu)),$$

where the minimum is taken over all non-constant and full-support dyadic distributions.

Theorem 2.2 ([DFGM19, Theorem 3.3.1 and Lemma 3.2.6])**.** *It holds that*

$$\frac{1}{\rho_{\min}(n)} \leq q(n) \leq n^2 \log n \frac{1}{\rho_{\min}(n)}.$$

Hence, from now on, we will consider the problem of finding a formula for $\rho_{\min}(n)$ (up to sub-exponential factors) instead of a formula for $q(n)$.

2.3 Tails

The *tail* of a dyadic distribution μ over X_n is the largest set $T \subseteq X_n$ which satisfies, for some $a \in \mathbb{N}$:

- The probabilities of the elements in T are $2^{-a-1}, 2^{-a-2}, \ldots, 2^{-a-(|T|-1)}, 2^{-a-(|T|-1)}$.
- Any element $x_i \in X_n \backslash T$ has probability at least 2^{-a}.

If μ is a dyadic distribution, then [DFGM19, Lemma 3.2.5] shows that each set in $\mathrm{Spl}(\mu)$ either contains T or is disjoint from T.

2.4 Entropy

The *entropy* of a distribution π is

$$H(\pi) := \sum_{i=1}^{n} \pi_i \log \frac{1}{\pi_i}.$$

For $n = 2$, define the *binary entropy function*:

$$h(\pi_1) := \pi_1 \log \frac{1}{\pi_1} + (1 - \pi_1) \log \frac{1}{1 - \pi_1}.$$

We prove some simple bounds on the binary entropy function, which will be useful in some of the proofs in this work. If $y - \epsilon \leq x \leq y + \epsilon$ for some x, y, ϵ, denote $x = y \pm \epsilon$.

Lemma 2.3. *For any $0 \leq x, \epsilon_1, \epsilon_2 \leq 1$ such that $\epsilon_2 \leq x \leq 1 - \epsilon_1$ it holds that*

$$h(x + \epsilon_1) = h(x) \pm h(\epsilon_1),$$
$$h(x - \epsilon_2) = h(x) \pm h(\epsilon_2).$$

Proof. Let $0 \leq x, \epsilon_1 \leq 1$ such that $x + \epsilon_1 \leq 1$. Since h is concave and $h(0) = 0$ it is known that h is sub-additive, that is $h(x + \epsilon_1) \leq h(x) + h(\epsilon_1)$. Using that inequality together with the fact that h is symmetric, we have:

$$h(x) = h(1 - (x + \epsilon_1) + \epsilon_1) \leq h(1 - (x + \epsilon_1)) + h(\epsilon_1) = h(x + \epsilon_1) + h(\epsilon_1).$$

The second inequality is proved similarly. □

Throughout this paper, we also use the fact that $h(x)$ is increasing for $x < 1/2$.

3 An exact (and almost exact) formula for $\rho_{\min}(n)$

Our goal in this section and the next is to find a formula for $\rho_{\min}(n)$ up to sub-exponential factors. We use the expression

$$\rho_{\min}(n) = \min_{\mu} \max_{d \in [n]} \rho_d(\mathrm{Spl}(\mu))$$

as our starting point. We want to present $\rho_{\min}(n)$ in a more "direct" or "numeric" fashion, rather than through a choice of a non-constant dyadic distribution μ. Denote $n = \beta \cdot 2^k$ where $\beta \in [1, 2)$ and $k \in \mathbb{N}$. From now on and throughout this paper, when we refer to β and k that is always their meaning unless specified otherwise. Let $[0,1]^{\mathbb{N}}$ be the set of all sequences $\{c_i\}_{i=0}^{\infty}$ where $0 \leq c_i \leq 1$ for any i and denote a sequence $\{c_i\}_{i=0}^{\infty} \in [0,1]^{\mathbb{N}}$ with $\boldsymbol{c}$ (the notation is the elements' letter in bold). In order to describe a non-constant and full support dyadic distribution μ in this language, we can determine the following sufficient and necessary values:

- $b \in \mathbb{N}$, where the highest probability in μ is determined to be $\mu_1 = 2^{b-k}$.
- An "amount sequence" $\boldsymbol{c}$ which describes how many elements μ will have of each probability. In order to obtain a valid dyadic distribution the following must hold:

$$\sum_{i=0}^{\infty} c_i / 2^i = \frac{1}{\beta \cdot 2^b},$$
$$\sum_{i=0}^{\infty} c_i \leq 1,$$
$$\forall i \colon c_i n \in \mathbb{N}.$$

Those values indeed determine μ uniquely: for any i, $c_i n$ elements have probability $\mu_1/2^i$ (assume that $c_0 > 0$). Actually, in order to describe μ precisely, we also have to say exactly **which elements** are the $c_i n$ elements having probability $\mu_1/2^i$. However, since we are only interested in the identity of a distribution μ which minimizes $\rho(\mathrm{Spl}(\mu))$, the identity of the $c_i n$ elements having probability $\mu_1/2^i$ does not matter — what matters is only their quantity. If t is the highest index such that $c_t > 0$, then one element with probability $\mu_1/2^t$ is "turned" into a tail with total probability 2^{-a-t}, such that we get n elements in total. The first constraint assures that the probabilities in μ sum up to 1. The second constraint assures that there are no more

than n non-tail elements, that is, exactly n elements in total. The third constraint assures that there is an integral number of elements of each type.

For the proof of our formula for $\rho_{\min}(n)$ which we will present soon, we want to distinguish between pairs $(\boldsymbol{c}, b) \in [0,1]^{\mathbb{N}} \times \mathbb{N}$ which satisfy all of those three constraints, and those which do not necessarily satisfy the third "integrality" constraint. Hence, denote the set of all pairs $(\boldsymbol{c}, b) \in [0,1]^{\mathbb{N}} \times \mathbb{N}$ satisfying the first two constraints, that is, $\sum_{i=0}^{\infty} 2^{b-i} c_i \beta = 1$ and $\sum_{i=0}^{\infty} c_i \leq 1$ with $\mathcal{C} = \mathcal{C}(\beta)$. If a pair $(\boldsymbol{c}, b) \in \mathcal{C}$ satisfies the third constraint as well, we say that $(\boldsymbol{c}, b)$ (or, simply $\boldsymbol{c}$, when the identity of b is clear) is *k-feasible.*[1]

Now we want to describe the choice of an integer d for the maximization part in $\rho_{\min}(n)$. Due to [DFGM19], we know that each splitting set either contains all tail elements, or none of them. For a sequence $\boldsymbol{c} \in [0,1]^{\mathbb{N}}$, denote by t the last index such that $c_t > 0$. If there is no such index, $t = \infty$. Fix $(\boldsymbol{c}, b) \in \mathcal{C}$ which is k-feasible, that describes a dyadic distribution μ (in that case, $t < \infty$). In order to describe the set $\mathrm{Spl}(\mu)_d$ for some $d \in [n]$ (recall that those are all splitting sets of μ of size d) we can consider the following sets of sequences in $[0,1]^{\mathbb{N}}$:

- A set S_d of all sequences $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ describing sets in $\mathrm{Spl}(\mu)_d$ which do not contain the tail elements. Those sequences satisfy:

$$\begin{gathered}\sum_{i=0}^{t} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}, \\ \sum_{i=0}^{t} \alpha_i c_i n = d, \\ \forall i \colon \alpha_i c_i n \in \mathbb{N}, \\ \alpha_t < 1.\end{gathered}$$

- A set T_d of all sequences $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ describing sets in $\mathrm{Spl}(\mu)_d$ which contain the tail elements. Those sequences satisfy:

$$\begin{gathered}\sum_{i=0}^{t} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}, \\ \sum_{i=0}^{t} \alpha_i c_i n + \left(1 - \sum_{i=0}^{t} c_i\right) n - 1 = d, \\ \forall i \colon \alpha_i c_i n \in \mathbb{N}, \\ \alpha_t > 0.\end{gathered}$$

The constraints of S_d, T_d indeed describe splitting sets of size d: The first constraint assures that the set described by a sequence $\boldsymbol{\alpha}$ is a splitting set. The second constraint assures that its size is d. The third constraint assures that each probability type appears in the set an integral number of times. The last constraint on S_d or T_d assures that the tail elements may not be or may be a part of the splitting set, respectively. Note that a sequence $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ satisfying those constraints does not determine **which elements** are exactly the elements chosen to the splitting set. We soon handle that, since here, in contrast to the choice of μ, the identity of the elements chosen having given probability matters, since any choice of different elements defines

[1] Even though this constraint relates to n, we choose to relate k instead of n to conform with future notations which relate to k as well. Our discussion will fix $\beta \in [1,2)$, and thus n will be determined uniquely by k, so this is not a problem.

a different splitting set. This discussion implies that we can write $\rho_{\min}(n)$ in the following way, which will be convenient for our purposes:

$$\rho_{\min}(n) = \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{\substack{d\in[n]:\\ S_d\cup T_d\neq\emptyset}} \sum_{\boldsymbol{\alpha}\in S_d} \frac{\binom{c_t n-1}{\alpha_t c_t n}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} + \sum_{\boldsymbol{\alpha}\in T_d} \frac{\binom{c_t n-1}{\alpha_t c_t n-1}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}}.$$

For $0 \le i < t$, each binomial coefficient $\binom{c_i n}{\alpha_i c_i n}$ is the number of possibilities to choose $\alpha_i c_i n$ elements of probability 2^{-k+b-i} to the splitting set. For the index t, we use the expressions $\binom{c_t n-1}{\alpha_t c_t n}$ and $\binom{c_t n-1}{\alpha_t c_t n-1}$ because we must use or not use the tail elements, depends on whether α is in S_d or T_d.

Since our goal is to find a formula for $\rho_{\min}(n)$ up to sub-exponential factors, we can simplify the expression a bit, and ignore the sequences in T_d. Define

$$\rho^*_{\min}(n) = \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{\substack{d\in[n]:\\ S_d\neq\emptyset}} \sum_{\boldsymbol{\alpha}\in S_d} \frac{\prod_{i=0}^{t}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}}.$$

The idea is that any splitting set S described by a sequence $\alpha \in T_d$, has a matching splitting set $\overline{S}$ (the complement set of S) described by a sequence $\alpha' \in S_{n-d}$ such that

$$\frac{\binom{c_t n-1}{\alpha_t c_t n}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} = \frac{\binom{c_t n-1}{\alpha'_t c_t n-1}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha'_i c_i n}}{\binom{n}{n-d}}.$$

Thus by considering only sequences in S_d, we get an approximation for $\rho_{\min}(n)$. Here is a detailed proof for that, for the interested reader:

Lemma 3.1. *It holds that*

$$\rho_{\min}(n)/2 \le \rho^*_{\min}(n) \le n \cdot \rho_{\min}(n).$$

Proof. Let $n = \beta \cdot 2^k$. Fix $(\boldsymbol{c}, b) \in \mathcal{C}$ which is k-feasible and $d \in [n]$. To handle the case $S_d = \emptyset$ or $T_d = \emptyset$, define

$$f_S(d) = \begin{cases} \sum_{\boldsymbol{\alpha}\in S_d} \frac{\binom{c_t n-1}{\alpha_t c_t n}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} & S_d \neq \emptyset, \\ 0 & S_d = \emptyset, \end{cases}$$

and

$$f_T(d) = \begin{cases} \sum_{\boldsymbol{\alpha}\in T_d} \frac{\binom{c_t n-1}{\alpha_t c_t n-1}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} & T_d \neq \emptyset, \\ 0 & T_d = \emptyset. \end{cases}$$

In this language, we can write:

$$\rho_{\min}(n) = \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{d\in[n]} f_S(d) + f_T(d).$$

Define:

$$\rho^{**}_{\min}(n) = \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{d\in[n]} f_S(d).$$

If $f_S(d) \ge f_T(d)$, then

$$f_S(d) + f_T(d) \le 2 \cdot f_S(d).$$

Else, assume $f_S(d) < f_T(d)$. Since for any $\boldsymbol{\alpha} \in T_d$ we have $\boldsymbol{\alpha'} \in S_{n-d}$ such that

$$\frac{\binom{c_t n-1}{\alpha_t c_t n}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} = \frac{\binom{c_t n-1}{\alpha'_t c_t n-1}\prod_{i=0}^{t-1}\binom{c_i n}{\alpha'_i c_i n}}{\binom{n}{n-d}}$$

($\alpha'_i = 1-\alpha_i$ for any i), and the opposite holds as well in a similar fashion, we have

$$f_S(n-d) = f_T(d) > f_S(d) = f_T(n-d)$$

and thus

$$f_S(d) + f_T(d) = f_S(n-d) + f_T(n-d) \leq 2 \cdot f_S(n-d).$$

Hence, we can always choose $d' \in [n]$ such that

$$\rho_{\min}(n) = \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} f_S(d') + f_T(d')$$

and $f_S(d') \geq f_T(d')$. Hence:

$$\begin{aligned}\rho_{\min}(n) &\leq 2 \cdot \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} f_S(d') \\ &\leq 2 \cdot \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{d\in[n]} f_S(d) = 2 \cdot \rho^{**}_{\min}(n).\end{aligned}$$

Now, note that:

$$\binom{x}{y}/x \leq \binom{x-1}{y} \leq \binom{x}{y}$$

(the left inequality holds as long as $x > y$), and hence $\rho_{\min}(n)/2 \leq \rho^{**}_{\min}(n) \leq \rho^{*}_{\min}(n)$ and moreover $\rho^{*}_{\min}(n) \leq n \cdot \rho^{**}_{\min}(n) \leq n \cdot \rho_{\min}(n)$, since $\alpha_t < 1$. Hence the lemma follows. □

Due to that approximation, it is enough to find a formula that estimates $\rho^{*}_{\min}(n)$ instead of $\rho_{\min}(n)$, up to sub-exponential factors.

4 Approximating $\rho_{\min}(n)$

In this section we prove our first main result, which is the following theorem:

Theorem 4.1. *There is a function $G\colon [1,2) \to \mathbb{R}$ such that $\rho_{\min}(n) = 2^{G(\beta)n \pm o(n)}$, where $n = \beta \cdot 2^k$, $k \in \mathbb{N}$ and $\beta \in [1,2)$. The function G is given by the following formula:*

$$G(\beta) = \inf_{\substack{b\in\mathbb{N},\boldsymbol{c}\in[0,1]^{\mathbb{N}}:\\ \sum_{i=0}^{\infty} c_i/2^i = \frac{1}{\beta\cdot 2^b}\\ \sum_{i=0}^{\infty} c_i \leq 1}} \max_{\substack{\boldsymbol{\alpha}\in[0,1]^{\mathbb{N}}:\\ \sum_{i=0}^{\infty} \alpha_i c_i/2^i = \frac{1}{\beta\cdot 2^{b+1}}}} \sum_{i=0}^{\infty} h(\alpha_i)c_i - h\left(\sum_{i=0}^{\infty}\alpha_i c_i\right).$$

Corollary 4.2. *Putting together Theorems 2.2 and 4.1, it holds that $q(n) = 2^{-G(\beta)n \pm o(n)}$, where $n = \beta \cdot 2^k$, $k \in \mathbb{N}$ and $\beta \in [1,2)$.*

An immediate corollary is that the exponent base of $\rho_{\min}(n)$ (and $q(n)$) does not depend on n, but only on β. We assume that $c_0 > 0$, since if $c_0 = 0$ then we can choose another b and construct an equivalent sequence with $c_0 > 0$. For the rest of the section, fix $\beta \in [1, 2)$ and denote $P(\boldsymbol{c}, \boldsymbol{\alpha}) = \sum_{i=0}^{\infty} h(\alpha_i) c_i - h(\sum_{i=0}^{\infty} \alpha_i c_i)$. For a fixed $(\boldsymbol{c}, b) \in \mathcal{C}$ (that is, $(\boldsymbol{c}, b) \in [0,1]^{\mathbb{N}} \times \mathbb{N}$ which satisfies also $\sum_{i=0}^{\infty} c_i / 2^i = \frac{1}{\beta \cdot 2^b}$ and $\sum_{i=0}^{\infty} c_i \leq 1$), we denote by $\mathcal{A}(\boldsymbol{c}, b)$ (or simply $\mathcal{A}$, from now on, assuming $(\boldsymbol{c}, b)$ is fixed) the set of all sequences $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ which satisfy $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$ (the maximization constraint in $G(\beta)$). In this language, we can write

$$G(\beta) = \inf_{(\boldsymbol{c}, b) \in \mathcal{C}} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}).$$

4.1 G is well-defined

Before we prove our formula, we first show that G is indeed well-defined and finite: if we change the inner max to sup, then it is clear that $G(\beta)$ is well-defined and finite: it always holds that $\sum_{i=0}^{\infty} c_i \leq 1$, and thus $-1 \leq P(\boldsymbol{c}, \boldsymbol{\alpha}) \leq 1$ for any $(\boldsymbol{c}, b) \in \mathcal{C}$, $\boldsymbol{\alpha} \in \mathcal{A}$. Moreover, for any $(\boldsymbol{c}, b) \in \mathcal{C}$, $\mathcal{A}$ is non-empty: choosing the sequence $\boldsymbol{\alpha}$ to be $\alpha_i = 1/2$ for any i satisfies $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$ for any $(\boldsymbol{c}, b) \in \mathcal{C}$, thus it always belongs to $\mathcal{A}$. It is known that supremum/infimum values are defined and finite for non-empty bounded sets, thus it remains to show that the inner supremum is attained, and hence can be written as maximum. Fix $(\boldsymbol{c}, b) \in \mathcal{C}$. First we show:

Lemma 4.3. *Let $\left(\boldsymbol{\alpha}^j\right)_{j \in \mathbb{N}}$ be a sequence of sequences $\boldsymbol{\alpha}^j \in \mathcal{A}$ such that $\lim_{j \to \infty} P\left(\boldsymbol{c}, \boldsymbol{\alpha}^j\right) = \sup_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha})$. Then there is a sequence $\boldsymbol{\alpha}$, and a subsequence of $\left(\boldsymbol{\alpha}^j\right)_{j \in \mathbb{N}}$ which we denote by $\left(\boldsymbol{\alpha}'^j\right)_{j \in \mathbb{N}}$, such that $\boldsymbol{\alpha}'^j \to \boldsymbol{\alpha}$ pointwise, that is, for any i: $\lim_{j \to \infty} \alpha_i'^j = \alpha_i$.*

Proof. Consider the sequence $\left(\alpha_0^j\right)_{j \in \mathbb{N}}$. Since $\alpha_0^j \in [0,1]$ for any j, $\left(\alpha_0^j\right)_{j \in \mathbb{N}}$ must have a convergent subsequence due to Bolzano-Weiersrtrass. Denote that subsequence by $\left(\alpha_0'^j\right)_{j \in \mathbb{N}}$, and let $\alpha_0 = \lim_{j \to \infty} \alpha_0'^j$. Deonte by $\boldsymbol{\alpha}^{(0)} = \left(\boldsymbol{\alpha}^{(0),j}\right)_{j \in \mathbb{N}}$ the subsequence of $\left(\boldsymbol{\alpha}^j\right)_{j \in \mathbb{N}}$ that is constructed from the same indices as $\left(\alpha_0'^j\right)_{j \in \mathbb{N}}$. Now, consider the sequence $\left(\alpha_1^{(0),j}\right)_{j \in \mathbb{N}}$. This sequence as well has a subsequence which converges, say to α_1. Let $\boldsymbol{\alpha}^{(1)}$ be the subsequence of $\left(\boldsymbol{\alpha}^j\right)_{j \in \mathbb{N}}$ that is constructed from the same indices of the subsequence of $\left(\alpha_1^{(0),j}\right)_{j \in \mathbb{N}}$ which converges to α_1. Note that in addition to $\alpha_1^{(1),j} \to \alpha_1$, we also have $\alpha_0^{(1),j} \to \alpha_0$ since the limit of a convergent sequence equals the limit of any of its subsequences. We can proceed in the same fashion, constructing a sequence $\boldsymbol{\alpha}$, and for any r a subsequence $\boldsymbol{\alpha}^{(r)}$ of $\left(\boldsymbol{\alpha}^j\right)_{j \in \mathbb{N}}$ such that $\alpha_s^{(r),j} \to \alpha_s$ for any $s \leq r$. We take as $\left(\boldsymbol{\alpha}'^j\right)_{j \in \mathbb{N}}$ the diagonal sequence $\left(\boldsymbol{\alpha}^{(j),j}\right)_{j \in \mathbb{N}}$ which converges pointwise to $\boldsymbol{\alpha}$. □

Let $\boldsymbol{\alpha}$ be the sequence guaranteed by this lemma. We will show that the supremum is attained at $\boldsymbol{\alpha}$, that is, $P(\boldsymbol{c}, \boldsymbol{\alpha}) = \sup_{\boldsymbol{\alpha}' \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}')$. It remains to show:

Lemma 4.4. *The sequence $\boldsymbol{\alpha}$ found by Lemma 4.3 is in $\mathcal{A}$ (that is, $\boldsymbol{\alpha}$ is feasible for $(\boldsymbol{c}, b)$) and $\lim_{j \to \infty} P\left(\boldsymbol{c}, \boldsymbol{\alpha}^j\right) = P(\boldsymbol{c}, \boldsymbol{\alpha})$.*

Proof. Let us begin by showing $\boldsymbol{\alpha} \in \mathcal{A}$: pointwise convergence of $\left(\boldsymbol{\alpha}^j\right)_{j \in \mathbb{N}}$ to $\boldsymbol{\alpha}$ ensures that $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$, since $\boldsymbol{\alpha}^j \in [0,1]^{\mathbb{N}}$ for any j. It remains to show that $\frac{1}{\beta \cdot 2^{b+1}} = \sum_{i=0}^{\infty} \alpha_i c_i / 2^i$: Take an arbitrary $\epsilon > 0$ and find I such that $\sum_{i>I} c_i < \epsilon/3$. Then, find J such that $\left|\alpha_i^J - \alpha_i\right| < \epsilon/3$ for

all $i \leq I$. Thus:

$$\begin{aligned}\frac{1}{\beta \cdot 2^{b+1}} &= \sum_{i=0}^{\infty} \alpha_i^J c_i / 2^i \\ &= \sum_{i=0}^{I} \alpha_i^J c_i / 2^i \pm \epsilon/3 \\ &= \sum_{i=0}^{I} (\alpha_i \pm \epsilon/3) c_i / 2^i \pm \epsilon/3 \\ &= \sum_{i=0}^{I} \alpha_i c_i / 2^i \pm 2\epsilon/3 = \sum_{i=0}^{\infty} \alpha_i c_i / 2^i \pm \epsilon,\end{aligned}$$

and so indeed $\boldsymbol{\alpha} \in \mathcal{A}$. Let us show that $\lim_{j\to\infty} P\big(\boldsymbol{c}, \boldsymbol{\alpha}^j\big) = P(\boldsymbol{c}, \boldsymbol{\alpha})$. For some $I \in \mathbb{N}$, denote $P^I(\boldsymbol{c},\boldsymbol{\alpha}) = \sum_{i=0}^{I} h(\alpha_i) c_i - h\Big(\sum_{i=0}^{I} \alpha_i c_i\Big)$. Take an arbitrary $\epsilon > 0$ and let I such that $\sum_{i>I} c_i < \epsilon$. So:

$$P(\boldsymbol{c}, \boldsymbol{\alpha}) = \sum_{i=0}^{I} h(\alpha_i) c_i + \sum_{i=I+1}^{\infty} h(\alpha_i) c_i - h\left(\sum_{i=0}^{I} \alpha_i c_i + \sum_{i=I+1}^{\infty} \alpha_i c_i\right) = P^I(\boldsymbol{c},\boldsymbol{\alpha}) \pm (\epsilon + h(\epsilon)) \quad (1)$$

due to Lemma 2.3. Now we can use an argument similar to the one used to show feasibility of $\boldsymbol{\alpha}$: find J such that $\left|\alpha_i^J - \alpha_i\right| < \epsilon$ for all $i \leq I$. So:

$$\begin{aligned}P^I(\boldsymbol{c},\boldsymbol{\alpha}) &= \sum_{i=0}^{I} h\big(\alpha_i^J \pm \epsilon\big) c_i - h\left(\sum_{i=0}^{I} \big(\alpha_i^J \pm \epsilon\big) c_i\right) \\ &= \sum_{i=0}^{I} h\big(\alpha_i^J\big) c_i \pm h(\epsilon) \sum_{i=0}^{I} c_i - h\left(\sum_{i=0}^{I} \alpha_i^J c_i \pm \epsilon \sum_{i=0}^{I} c_i\right) = P^I\big(\boldsymbol{c},\boldsymbol{\alpha^J}\big) \pm 2h(\epsilon). \quad (2)\end{aligned}$$

And so:

$$P\big(\boldsymbol{c}, \boldsymbol{\alpha^J}\big) \underset{(*)}{=} P^I\big(\boldsymbol{c}, \boldsymbol{\alpha^J}\big) \pm (\epsilon + h(\epsilon)) \underset{(2)}{=} P^I(\boldsymbol{c},\boldsymbol{\alpha}) \pm (\epsilon + 3h(\epsilon)) \underset{(1)}{=} P(\boldsymbol{c}, \boldsymbol{\alpha}) \pm (2\epsilon + 4h(\epsilon)),$$

where $(*)$ is since $\sum_{i>I} c_i < \epsilon$, similarly to eq. (1). So indeed, $\lim_{j\to\infty} P\big(\boldsymbol{c}, \boldsymbol{\alpha}^j\big) = P(\boldsymbol{c}, \boldsymbol{\alpha})$. □

The following desired result is an immediate corollary:

Lemma 4.5. *For any $(\boldsymbol{c}, b) \in \mathcal{C}$ there is $\boldsymbol{\alpha} \in \mathcal{A}$ such that $\sup_{\boldsymbol{\alpha'}\in\mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha'}) = P(\boldsymbol{c}, \boldsymbol{\alpha})$.*

4.2 Proving our formula for $\rho_{\min}(n)$

The following bounds on $\rho^*_{\min}(n)$ immediately imply theorem 4.1, due to Lemma 3.1:

Lemma 4.6. *It holds that $\rho^*_{\min}(n) \geq 2^{G(\beta)n - o(n)}$.*

Lemma 4.7. *It holds that $\rho^*_{\min}(n) \leq 2^{G(\beta)n + o(n)}$.*

In the following subsections we prove those bounds.

4.2.1 Lower bounding $\rho^*_{\min}(n)$

Recall that if a pair $(\boldsymbol{c}, b) \in \mathcal{C}$ satisfies $c_i n \in \mathbb{N}$ for all i, we say that $\boldsymbol{c}$ is k-feasible. Similarly, if a sequence $\boldsymbol{\alpha} \in \mathcal{A}$ satisfies $\alpha_i c_i n \in \mathbb{N}$ for all i, and $\alpha_t < 1$, we say that $\boldsymbol{\alpha}$ is k-feasible. Note that for a fixed $(\boldsymbol{c}, b) \in \mathcal{C}$ which is k-feasible, by our definitions:

$$\{\boldsymbol{\alpha} \in \mathcal{A} \colon \boldsymbol{\alpha} \text{ is } k\text{-feasible}\} = \bigcup_{d \in [n]} S_d.$$

We will use that connection throughout the proof, when linking between $\rho^*_{\min}(n)$, which uses the set S_d for some optimal d, and $G(\beta)$ which uses the set $\mathcal{A}$. For a set of sequences $\mathcal{S} \subseteq [0,1]^{\mathbb{N}}$, let

$$\mathcal{S}^{\leq l} = \{\boldsymbol{s} \in \mathcal{S} \colon i > l \implies s_i = 0\}.$$

Lemma 4.6 can be inferred from the following two lemmas:

Lemma 4.8. *If $(\boldsymbol{c}, b) \in \mathcal{C}$ and $\boldsymbol{c}$ is k-feasible, then there is $\boldsymbol{\alpha} \in \mathcal{A}^{\leq k}$ which is k-feasible.*

The purpose of this lemma is to allow us to use the estimate

$$2^{h(\lambda)n}/O\left(\sqrt{n}\right) \leq \binom{n}{\lambda n} \leq 2^{h(\lambda)n} \tag{3}$$

(the lower bound is due to [You12], for example) while proving Lemma 4.6, in a sufficiently efficient fashion.

Lemma 4.9. *Fix $(\boldsymbol{c}, b) \in \mathcal{C}$. Then:*

$$\lim_{k \to \infty} \max_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^{\leq k} \colon \\ \boldsymbol{\alpha} \text{ is } k\text{-feasible}}} P(\boldsymbol{c}, \boldsymbol{\alpha}) = \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}).$$

For large values of k, Lemma 4.9 allows us to remove the k-feasibility and $i > k \implies \alpha_i = 0$ constraints on $\boldsymbol{\alpha}$ without changing much the value of $P(\boldsymbol{c}, \boldsymbol{\alpha})$. Having Lemmas 4.8–4.9 in hand and using the estimate (3), Lemma 4.6 can be proved:

Proof of Lemma 4.6. Let $n = \beta \cdot 2^k$ and $(\boldsymbol{c}, b) \in \mathcal{C}$ which is k-feasible. So:

$$\begin{aligned}
\max_{\substack{d \in [n] \colon \\ S_d \neq \emptyset}} \sum_{\boldsymbol{\alpha} \in S_d} \frac{\prod_{i=0}^{\infty} \binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} &\underset{\text{Lem 4.8}}{\geq} \max_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^{\leq k} \colon \\ \boldsymbol{\alpha} \text{ is } k\text{-feasible}}} \frac{\prod_{i=0}^{\infty} \binom{c_i n}{\alpha_i c_i n}}{\binom{n}{\sum_{i=0}^{\infty} \alpha_i c_i n}} \\
&\underset{(3)}{\geq} \max_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^{\leq k} \colon \\ \boldsymbol{\alpha} \text{ is } k\text{-feasible}}} \frac{\exp_2(\sum_{i=0}^{\infty} h(\alpha_i) c_i n)/O\left(\sqrt{n^k}\right)}{\exp_2(h(\sum_{i=0}^{\infty} \alpha_i c_i) n)} \\
&= \exp_2 \max_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^{\leq k} \colon \\ \boldsymbol{\alpha} \text{ is } k\text{-feasible}}} P(\boldsymbol{c}, \boldsymbol{\alpha}) n - o(n) \\
&\underset{\text{Lem 4.9}}{\geq} \exp_2\left(\max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) n - o(n)\right).
\end{aligned}$$

Let $(\boldsymbol{c}, b) \in \mathcal{C}$ which is k-feasible and

$$\min_{\substack{(\boldsymbol{c'}, b) \in \mathcal{C} \colon \\ \boldsymbol{c'} \text{ is } k\text{-feasible}}} \max_{\substack{d \in [n] \colon \\ S_d \neq \emptyset}} \sum_{\boldsymbol{\alpha} \in S_d} \frac{\prod_{i=0}^{\infty} \binom{c'_i n}{\alpha_i c'_i n}}{\binom{n}{d}} = \max_{\substack{d \in [n] \colon \\ S_d \neq \emptyset}} \sum_{\boldsymbol{\alpha} \in S_d} \frac{\prod_{i=0}^{\infty} \binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}},$$

and deduce:

$$\begin{aligned}
\rho^*_{\min}(n) &= \min_{\substack{(\boldsymbol{c'},b)\in\mathcal{C}:\\ \boldsymbol{c'}\text{ is }k\text{-feasible}}} \max_{\substack{d\in[n]:\\ S_d\neq\emptyset}} \sum_{\boldsymbol{\alpha}\in S_d} \frac{\prod_{i=0}^{\infty}\binom{c'_i n}{\alpha_i c'_i n}}{\binom{n}{d}} \\
&= \max_{\substack{d\in[n]:\\ S_d\neq\emptyset}} \sum_{\boldsymbol{\alpha}\in S_d} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} \\
&\geq \exp_2\left(\max_{\boldsymbol{\alpha}\in\mathcal{A}} P(\boldsymbol{c},\boldsymbol{\alpha})n - o(n)\right) \\
&\geq \inf_{(\boldsymbol{c'},b)\in\mathcal{C}} \exp_2\left(\max_{\boldsymbol{\alpha}\in\mathcal{A}} P\big(\boldsymbol{c'},\boldsymbol{\alpha}\big)n - o(n)\right) = 2^{G(\beta)n-o(n)}. \qquad \square
\end{aligned}$$

Now we shall prove Lemmas 4.8–4.9:

Proof of Lemma 4.8. Let $(\boldsymbol{c},b)\in\mathcal{C}$ and assume $\boldsymbol{c}$ is k-feasible, then we have:

$$\sum_{i=k+1}^{\infty} c_i\cdot 2^{b-i}\cdot\beta \underset{(*)}{<} \sum_{i=k+1}^{\infty} c_i\cdot 2^{k-1-(k+1)}\cdot 2 = 2^{-1}\cdot\sum_{i=k+1}^{\infty} c_i \leq 1/2$$

where $(*)$ is since $b\leq k-1$ (otherwise $(\boldsymbol{c},b)$ represents a constant dyadic distribution), $i\geq k+1$, and $\beta<2$. Since $\sum_{i=0}^{\infty} c_i\cdot 2^{b-i}\cdot\beta = 1$, we deduce that $\sum_{i=0}^{k} c_i\cdot 2^{b-i}\cdot\beta > 1/2$. Thus, by Lemma 4.1 in [DFGM19] (called there "A useful lemma"), we know that there is a splitting set of the dyadic distribution represented by $(\boldsymbol{c},b)$ containing only elements with probabilities $\mu_1,\mu_1/2,\ldots,\mu_1/2^k$. The same lemma also implies that $\alpha_t<1$. That is, there is $\boldsymbol{\alpha}\in\mathcal{A}^{\leq k}$ which is k-feasible. $\square$

The proof of Lemma 4.9 will require the following:

Lemma 4.10. *Fix $(\boldsymbol{c},b)\in\mathcal{C}$, $\epsilon>0$ and $\boldsymbol{\alpha}\in\mathcal{A}$. There are $K\in\mathbb{N}$ and $\tilde{\boldsymbol{\alpha}}\in\mathcal{A}^{\leq K}$, where $\tilde{\boldsymbol{\alpha}}$ is K-feasible and satisfies $P(\boldsymbol{c},\boldsymbol{\alpha}) = P(\boldsymbol{c},\tilde{\boldsymbol{\alpha}})\pm\epsilon$.*

Having Lemma 4.10, Lemma 4.9 is almost immediate:

Proof of Lemma 4.9. Fix $(\boldsymbol{c},b)\in\mathcal{C}$ and let $\epsilon>0$. Let $\boldsymbol{\alpha}\in\mathcal{A}$ such that $P(\boldsymbol{c},\boldsymbol{\alpha}) = \max_{\boldsymbol{\alpha'}\in\mathcal{A}} P(\boldsymbol{c},\boldsymbol{\alpha'})$. Let $K\in\mathbb{N}$ large enough such that Lemma 4.10 holds for $(\boldsymbol{c},b)$, $\boldsymbol{\alpha}$ and ϵ. Then for any $k\geq K$:

$$\max_{\boldsymbol{\alpha'}\in\mathcal{A}} P\big(\boldsymbol{c},\boldsymbol{\alpha'}\big) = P(\boldsymbol{c},\boldsymbol{\alpha}) \underset{\text{Lem 4.10}}{\leq} P(\boldsymbol{c},\tilde{\boldsymbol{\alpha}})+\epsilon \leq \max_{\substack{\boldsymbol{\alpha'}\in\mathcal{A}\\ \boldsymbol{\alpha'}\text{ is }k\text{-feasible}}} P\big(\boldsymbol{c},\boldsymbol{\alpha'}\big)+\epsilon.$$

Obviously,

$$\max_{\substack{\boldsymbol{\alpha'}\in\mathcal{A}^{\leq k}\\ \boldsymbol{\alpha'}\text{ is }k\text{-feasible}}} P\big(\boldsymbol{c},\boldsymbol{\alpha'}\big) \leq \max_{\boldsymbol{\alpha'}\in\mathcal{A}} P\big(\boldsymbol{c},\boldsymbol{\alpha'}\big)$$

for any large enough k, thus the lemma follows. It is necessary that k is large enough: Note that for the K determined by Lemma 4.10, for example, we can be sure that there is $\boldsymbol{\alpha}\in\mathcal{A}^{\leq K}$ which is K-feasible, while for small k values there might not be such $\boldsymbol{\alpha}$, and then the left-hand side is not well defined. $\square$

It remains to prove Lemma 4.10, which is the main part of the proof for the lower bound. We first explain the proof idea, and then give the detailed proof.

Proof sketch of Lemma 4.10. Let $(\boldsymbol{c}, b) \in \mathcal{C}$ and $\boldsymbol{\alpha} \in \mathcal{A}$. Since the binary entropy function is sub-additive and symmetric, it holds that $\mathrm{h}(x \pm \epsilon) = h(x) \pm h(\epsilon)$ for $0 \leq x \pm \epsilon \leq 1$ (as we have shown in Lemma 2.3). Based on that, the proof idea is that if we make very small changes in $\boldsymbol{\alpha}$, to get some other sequence which we denote $\tilde{\boldsymbol{\alpha}}$, we can get $P(\boldsymbol{c}, \boldsymbol{\alpha}) = P(\boldsymbol{c}, \tilde{\boldsymbol{\alpha}}) \pm \epsilon$. The main difficulty is to make small changes to $\boldsymbol{\alpha}$ while ensuring that for some $K \in \mathbb{N}$, $\tilde{\boldsymbol{\alpha}} \in \mathcal{A}^{\leq K}$ and $\tilde{\boldsymbol{\alpha}}$ is K-feasible. We can solve that difficulty by defining a sequence $\boldsymbol{\epsilon}$ of very small values carefully selected, and then defining $\tilde{\boldsymbol{\alpha}}$ in the following way:

$$\tilde{\alpha}_i = \begin{cases} \alpha_s + \epsilon_s & i = s, \\ \alpha_i - \epsilon_i & i \neq s, \end{cases}$$

where s is some index chosen to make sure that $\tilde{\boldsymbol{\alpha}} \in [0,1]^{\mathbb{N}}$. The value $\tilde{\alpha}_s$ adds ϵ_s in order to "balance", in a way, the subtraction of ϵ_i in other indices, such that we have $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \sum_{i=0}^{\infty} \tilde{\alpha}_i c_i / 2^i$ and hence the constraint $\sum_{i=0}^{\infty} \tilde{\alpha}_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$ is satisfied (since the constraint $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$ is satisfied). The purpose of the addition or subtraction of the $\boldsymbol{\epsilon}$ sequence values is to "round" the values of $\boldsymbol{\alpha}$ to get $\tilde{\boldsymbol{\alpha}}$ which is K-feasible and belongs to $\mathcal{A}^{\leq K}$. The exact choice of the sequence $\boldsymbol{\epsilon}$ that guarantees that is described in the detailed proof. □

Before we give a detailed proof of Lemma 4.10, we prove a lemma which will be useful in the detailed proof, and also later when upper bounding $\rho^*_{\min}(n)$. Its purpose is to ensure that when we change a sequence $\boldsymbol{\alpha} \in \mathcal{A}$ to a sequence $\tilde{\boldsymbol{\alpha}}$, we use $\tilde{\boldsymbol{\alpha}} \in [0,1]^{\mathbb{N}}$.

Lemma 4.11. *Fix $b \in \mathbb{N}$. For any $\boldsymbol{c} \in [0,1]^{\mathbb{N}}$ such that $\sum_{i=0}^{\infty} c_i / 2^i = \frac{1}{\beta \cdot 2^b}$ for some $1 \leq \beta < 2$, and for any $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ which satisfies $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{2^{b+1}\beta}$, there are indices $s_1, s_2 \leq 2^{b+4}$ (possibly $s_1 = s_2$) such that $c_{s_1}, c_{s_2} > 1/2^{2(b+5)}$ and $\alpha_{s_1} > 1/2^{2(b+5)}$, $\alpha_{s_2} < 3/4$.*

Proof. Fix $b \in \mathbb{N}$ and take arbitrary $\boldsymbol{c}, \beta$ such that $\sum_i c_i / 2^i = \frac{1}{\beta \cdot 2^b}$. Let us find s_1: take an arbitrary sequence $\boldsymbol{\alpha}$ such that $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{2^{b+1}\beta}$. Denote $I = \left\{ i : i \leq 2^{b+4} \right\}$ and let $S \subseteq I$ be the set of indices in I which satisfy $c_i \geq 1/2^{2(b+5)}$. Assume towards contradiction that for any $i \in S$, $\alpha_i \leq \frac{1}{2^{2(b+5)}}$. Note that since $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{2^{b+1}\beta} > 1/2^{b+2}$ and $\sum_{i > 2^{b+4}} c_i / 2^i \leq \sum_{i > 2^{b+4}} 1/2^i = \frac{1}{2^{b+4}}$, it must hold that $\sum_{i=0}^{2^{b+4}} \alpha_i c_i / 2^i \geq \frac{3}{2^{b+4}}$. However, we have:

$$\begin{aligned} \sum_{i=0}^{2^{b+4}} \alpha_i c_i / 2^i &= \sum_{i \in S} \alpha_i c_i / 2^i + \sum_{i \in I \setminus S} \alpha_i c_i / 2^i \\ &\leq \frac{1}{2^{2(b+5)}} \cdot \sum_{i \in S} c_i + \sum_{i \in I \setminus S} c_i \\ &< \frac{2^{b+5}}{2^{2(b+5)}} + \frac{2^{b+5}}{2^{2(b+5)}} \\ &= 2 \cdot \frac{1}{2^{b+5}} = \frac{1}{2^{b+4}}, \end{aligned}$$

and that is a contradiction, thus there is $i \in S$ with $\alpha_i \geq 1/2^{2(b+5)}$. That is, there is an index $i \leq 2^{b+4}$ with $c_i, \alpha_i \geq 1/2^{2(b+5)}$, and this is s_1. Let us now find s_2: assume towards contradiction that for any $i \in S$, $\alpha_i \geq 3/4$. We show that if that assumption is true, then $\sum_{i \in S} \alpha_i c_i / 2^i$ is too large. First, we have:

$$\frac{1}{2^b \beta} = \sum_{i=0}^{\infty} c_i / 2^i = \sum_{i=0}^{2^{b+4}} c_i / 2^i + \sum_{i > 2^{b+4}} c_i / 2^i \leq \sum_{i=0}^{2^{b+4}} c_i / 2^i + 1/2^{b+4},$$

that is:

$$\sum_{i=0}^{2^{b+4}} c_i/2^i \geq \frac{1}{2^b\beta} - 1/2^{b+4}.$$

Moreover, it holds that:

$$\sum_{i\in I\setminus S} c_i/2^i \leq \frac{2^{b+5}}{2^{2(b+5)}} = 1/2^{b+5}.$$

Hence, we get that:

$$\sum_{i\in S} c_i/2^i \geq \frac{1}{2^b\beta} - 1/2^{b+4} - 1/2^{b+5} = \frac{1}{2^b\beta} - 3/2^{b+5}.$$

And thus, assuming $\alpha_i \geq 3/4$ for any $i \in S$:

$$\sum_{i\in S} \alpha_i c_i/2^i \geq \frac{3}{4}\sum_{i\in S} c_i/2^i \geq \frac{3}{4}\cdot\left(\frac{1}{2^b\beta} - 3/2^{b+5}\right).$$

But then we get:

$$\begin{aligned}
\frac{3}{4}\left(\frac{1}{2^b\beta} - 3/2^{b+5}\right) &= \frac{3}{4}\left(\frac{2^5 - 3\beta}{2^{b+5}\beta}\right) \\
&> \frac{3}{4}\cdot\frac{2^5 - 2^3}{2^{b+5}\beta} \\
&= \frac{3}{4}\cdot\frac{2^3\left(2^2-1\right)}{2^{b+5}\beta} \\
&= \frac{3\cdot 3}{2^2\cdot 2^{b+2}\beta} \\
&> \frac{2^3}{2^{b+4}\beta} = \frac{1}{2^{b+1}\beta},
\end{aligned}$$

and this contradicts the fact $\sum_{i=0}^{\infty}\alpha_i c_i/2^i = \frac{1}{2^{b+1}\beta}$. Thus there is $i \leq 2^{b+4}$ with $c_i \geq 1/2^{2(b+5)}$ and $\alpha_i < 3/4$, and this is s_2. □

Now we can go on with the detailed proof of Lemma 4.10.

Proof of Lemma 4.10. We divide the proof into three parts: First we define the sequence $\tilde{\boldsymbol{\alpha}}$ and show it exists. Then we show $\tilde{\boldsymbol{\alpha}} \in \mathcal{A}^{\leq K'}$ and $\tilde{\boldsymbol{\alpha}}$ is K'-feasible for some $K' \in \mathbb{N}$. Finally, we show $P(\boldsymbol{c}, \boldsymbol{\alpha}) = P(\boldsymbol{c}, \tilde{\boldsymbol{\alpha}}) \pm \epsilon$.

Defining $\tilde{\boldsymbol{\alpha}}$. Fix $(\boldsymbol{c}, b) \in [0,1]^{\mathbb{N}}$ satisfying $\sum_{i=0}^{\infty} c_i/2^i = \frac{1}{\beta\cdot 2^b}$ and $\sum_{i=0}^{\infty} c_i \leq 1$ (that is, $(\boldsymbol{c}, b) \in \mathcal{C}$). Fix $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ satisfying $\sum_{i=0}^{\infty}\alpha_i c_i/2^i = \frac{1}{\beta\cdot 2^{b+1}}$ (that is, $\boldsymbol{\alpha} \in \mathcal{A}$). Let $\epsilon > 0$ small enough (the proof holds for any $\epsilon > 0$ smaller than some constant). Let s be the lowest index satisfying $c_s > 1/2^{2(b+5)}$ and $\alpha_s < 3/4$ (s exists due to Lemma 4.11). Since $\sum_{i=0}^{\infty} c_i \leq 1$, there is $K \in \mathbb{N}$ such that $\sum_{i>K} c_i < \epsilon$ and $K \geq s$. Define the sequence $\tilde{\boldsymbol{\alpha}}$ as follows:

$$\tilde{\alpha}_i = \begin{cases} \alpha_s + \epsilon_s & i = s, \\ \alpha_i - \epsilon_i & i \neq s, \end{cases}$$

where $\boldsymbol{\epsilon}$ is an arbitrary sequence of small values satisfying the following constraints:

1. If $i > K$, or $c_i = 0$, or $\alpha_i = 0$: $\epsilon_i = \alpha_i$.
2. Otherwise, if $0 \leq i \leq K$ and $i \neq s$: $\epsilon_i = \alpha_i - \frac{l_i}{c_i \cdot \beta \cdot 2^{t_i}}$, where $l_i, t_i \in \mathbb{N}$, $\epsilon_i > 0$ and $h(\epsilon_i) \leq \epsilon/K$.
3. $\epsilon_s = \sum_{i \neq s} \epsilon_i c_i \cdot 2^{s-i}/c_s = \frac{l_s}{c_s \cdot \beta \cdot 2^{t_s}} - \alpha_s$, where $l_s, t_s \in \mathbb{N}$.

In order to continue with the proof, we first have to show that such a sequence $\boldsymbol{\epsilon}$ exists. Denote by I the set of all indices "that matter" in $\tilde{\boldsymbol{\alpha}}$, that is, $I = \{i \leq K \colon c_i, \alpha_i > 0\}$. It is not hard to construct a sequence $\boldsymbol{\epsilon}$ that satisfies constraints (1), (2). We should satisfy constraint (3) as well, that is

$$\begin{aligned}
\frac{l_s}{c_s \cdot \beta \cdot 2^{t_s}} - \alpha_s &= \sum_{i \neq s} \epsilon_i c_i \cdot 2^{s-i}/c_s \\
&= \frac{2^s}{c_s} \left[\sum_{i \in I \setminus \{s\}} \left(\alpha_i - \frac{l_i}{c_i \cdot \beta \cdot 2^{t_i}} \right) \cdot c_i/2^i + \sum_{i > K} \alpha_i c_i/2^i \right] \\
&= \frac{2^s}{c_s} \left[\sum_{i \neq s} \alpha_i c_i/2^i - \sum_{i \in I \setminus \{s\}} \frac{l_i}{\beta \cdot 2^{t_i+i}} \right].
\end{aligned}$$

This can be written as:

$$\begin{gathered}
2^s \left[\sum_{i \neq s} \alpha_i c_i/2^i - \sum_{i \in I \setminus \{s\}} \frac{l_i}{\beta \cdot 2^{t_i+i}} \right] = \frac{l_s}{\beta \cdot 2^{t_s}} - \alpha_s c_s \\
\iff \\
\sum_{i \neq s} \alpha_i c_i/2^i - \sum_{i \in I \setminus \{s\}} \frac{l_i}{\beta \cdot 2^{t_i+i}} = \frac{l_s}{\beta \cdot 2^{t_s+s}} - \alpha_s c_s/2^s \\
\iff \\
\sum_{i=0}^{\infty} \alpha_i c_i/2^i - \sum_{i \in I \setminus \{s\}} \frac{l_i}{\beta \cdot 2^{t_i+i}} = \frac{l_s}{\beta \cdot 2^{t_s+s}}.
\end{gathered}$$

Recall that $\sum_{i=0}^{\infty} \alpha_i c_i/2^i = \frac{1}{\beta \cdot 2^{b+1}}$, thus we have:

$$\begin{gathered}
\frac{1}{\beta \cdot 2^{b+1}} - \sum_{i \in I \setminus \{s\}} \frac{l_i}{\beta \cdot 2^{t_i+i}} = \frac{l_s}{\beta \cdot 2^{t_s+s}} \\
\iff \\
1/2^{b+1} - \sum_{i \in I \setminus \{s\}} l_i/2^{t_i+i} = l_s/2^{t_s+s},
\end{gathered}$$

and there are $l_s, t_s \in \mathbb{N}$ satisfying this equation: Let $t_s = b + 1 + \sum_{i \in I \setminus \{s\}} t_i + i$, then l_s is determined accordingly such that the equation holds. Clearly, $t_s \in \mathbb{N}$. As for l_s, note that by the constraints:

$$0 \leq \left(\alpha_s + \sum_{i \neq s} \epsilon_i c_i \cdot 2^{s-i}/c_s \right) \cdot c_s \cdot \beta \cdot 2^{t_s} = l_s.$$

Since clearly $l_s \in \mathbb{Z}$ as a sum of numbers in $\mathbb{Z}$, we get $l_s \in \mathbb{N}$, and thus there is such a sequence $\boldsymbol{\epsilon}$. We now show a few bounds on values involving the sequence $\boldsymbol{\epsilon}$, which will help us during the rest

of the proof. By the definition of the sequence $\boldsymbol{\epsilon}$ and since for $x \leq 1/2$ we have $h(x) \geq x \log \frac{1}{x} \geq x$, it holds that:

$$\sum_{i \leq K, i \neq s} \epsilon_i \leq \sum_{i \leq K, i \neq s} h(\epsilon_i) \leq \sum_{i \leq K, i \neq s} \epsilon / K = \epsilon. \tag{4}$$

Moreover:

$$\sum_{i \neq s} \epsilon_i c_i / 2^i = \sum_{i \leq K, i \neq s} \epsilon_i c_i / 2^i + \sum_{i > K} \epsilon_i c_i / 2^i \leq \sum_{i \leq K, i \neq s} \epsilon_i + \sum_{i > K} c_i = 2\epsilon,$$

and thus:

$$\epsilon_s = \sum_{i \neq s} \epsilon_i c_i \cdot 2^{s-i} / c_s \leq 2^s 2\epsilon / c_s. \tag{5}$$

$\tilde{\boldsymbol{\alpha}}$ is feasible. Now we show that $\tilde{\boldsymbol{\alpha}} \in \mathcal{A}^{\leq K}$ and K'-feasible for some $K' \in \mathbb{N}$. Based on the fact $\boldsymbol{\alpha} \in \mathcal{A}$, we first show $\tilde{\boldsymbol{\alpha}} \in \mathcal{A}^{\leq K}$, that is:

1. $\tilde{\boldsymbol{\alpha}} \in [0,1]^{\mathbb{N}}$.
2. $\sum_{i=0}^{\infty} \tilde{\alpha}_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$.
3. $i > K \implies \tilde{\alpha}_i = 0$ (this is obvious by the definition of $\tilde{\boldsymbol{\alpha}}$).

We show (1): For $i \neq s$, it is not hard to check that $0 \leq \tilde{\alpha}_i \leq 1$ by the definition of the sequence $\boldsymbol{\epsilon}$. For $i = s$, recall that $0 \leq \alpha_s < 3/4$ and thus $0 \leq \tilde{\alpha}_s = \alpha_s + \epsilon_s \leq 1$ for small enough ϵ (due to (5)). Let us show (2), depending on the fact $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$:

$$\begin{aligned}
\sum_{i=0}^{\infty} \tilde{\alpha}_i c_i / 2^i &= (\alpha_s + \epsilon_s) c_s / 2^s + \sum_{i \neq s} (\alpha_i - \epsilon_i) c_i / 2^i \\
&= \sum_{i=0}^{\infty} \alpha_i c_i / 2^i + \epsilon_s c_s / 2^s - \sum_{i \neq s} \epsilon_i c_i / 2^i \\
&= \frac{1}{\beta \cdot 2^{b+1}} + \frac{\sum_{i \neq s} \epsilon_i c_i \cdot 2^{s-i}}{c_s} c_s / 2^s - \sum_{i \neq s} \epsilon_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}.
\end{aligned}$$

Thus, indeed $\tilde{\boldsymbol{\alpha}} \in A^{\leq K}$. Now we show that $\tilde{\boldsymbol{\alpha}}$ is K'-feasible where

$$K' = \max(\{K\} \cup \{t_i : i \in I\}).$$

That is:

1. For any $i \in \mathbb{N}$: $\tilde{\alpha}_i c_i n \in \mathbb{N}$ where $n = \beta \cdot 2^{K'}$.
2. If there is t such that $c_t > 0$ and $c_i = 0$ for any $i > t$, then $\alpha_t < 1$.

We show (1): If $i > K$, or $c_i = 0$, or $\alpha_i = 0$ then by definition of $\tilde{\boldsymbol{\alpha}}$, $\tilde{\alpha}_i c_i n = 0 \in \mathbb{N}$. Otherwise:

$$\tilde{\alpha}_i c_i n = \frac{l_i}{c_i \cdot \beta \cdot 2^{t_i}} c_i \cdot \beta \cdot 2^{K'} = l_i \cdot 2^{K' - t_i} \in \mathbb{N}$$

since $K' \geq t_i$. Let us show (2): If $t > K$ or $\alpha_t = 0$ then $\tilde{\alpha}_t = 0 < 1$. Otherwise, if $t \leq K$ and $t \neq s$ then $\epsilon_t > 0$ and thus

$$\tilde{\alpha}_t = \alpha_t - \epsilon_t \leq 1 - \epsilon_t < 1.$$

If $t = s$, then since $\alpha_s < 3/4$, we have $\tilde{\alpha}_t = \alpha_s + \epsilon_s < 1$ for small enough ϵ. So $\tilde{\boldsymbol{\alpha}} \in \mathcal{A}^{\leq K} \subseteq \mathcal{A}^{\leq K'}$ and is K'-feasible, as required.

$P(\boldsymbol{c}, \tilde{\boldsymbol{\alpha}})$ **approximates** $P(\boldsymbol{c}, \boldsymbol{\alpha})$**.** It only remains to show $P(\boldsymbol{c}, \boldsymbol{\alpha}) = P(\boldsymbol{c}, \tilde{\boldsymbol{\alpha}}) \pm \epsilon$. Due to Lemma 2.3, We have:

$$\begin{aligned}
P(\boldsymbol{c}, \boldsymbol{\alpha}) &= \sum_{i=0}^{\infty} h(\alpha_i) c_i - h\left(\sum_{i=0}^{\infty} \alpha_i c_i\right) \\
&= h(\tilde{\alpha}_s - \epsilon_s) c_s + \sum_{i \neq s} h(\tilde{\alpha}_i + \epsilon_i) c_i - h\left((\tilde{\alpha}_s - \epsilon_s) c_s + \sum_{i \neq s} (\tilde{\alpha}_i + \epsilon_i) c_i\right) \\
&= \sum_{i=0}^{\infty} h(\tilde{\alpha}_i) c_i - h\left(\sum_{i=0}^{\infty} \tilde{\alpha}_i c_i\right) \pm h\left(\sum_{i=0}^{\infty} \epsilon_i c_i\right) \pm \sum_{i=0}^{\infty} h(\epsilon_i) c_i \\
&= P(\boldsymbol{c}, \tilde{\boldsymbol{\alpha}}) \pm h\left(\sum_{i=0}^{\infty} \epsilon_i c_i\right) \pm \sum_{i=0}^{\infty} h(\epsilon_i) c_i.
\end{aligned}$$

We show that the expressions $h(\sum_{i=0}^{\infty} \epsilon_i c_i)$ and $\sum_{i=0}^{\infty} h(\epsilon_i) c_i$ are small. It holds that:

$$\begin{aligned}
h\left(\sum_{i=0}^{\infty} \epsilon_i c_i\right) &\underset{\text{Lem 2.3}}{\leq} h\left(\sum_{i=0}^{K} \epsilon_i c_i\right) + h\left(\sum_{i=K+1}^{\infty} \epsilon_i c_i\right) \\
&\leq h\left(\sum_{i=0}^{K} \epsilon_i\right) + h\left(\sum_{i=K+1}^{\infty} c_i\right) \underset{(4),(5)}{\leq} h(\epsilon + 2^s 2\epsilon / c_s) + h(\epsilon),
\end{aligned}$$

and:

$$\begin{aligned}
\sum_{i=0}^{\infty} h(\epsilon_i) c_i &= \sum_{i=0}^{K} h(\epsilon_i) c_i + \sum_{i=K+1}^{\infty} h(\epsilon_i) c_i \\
&\leq h(\epsilon_s) + \sum_{i \leq K, i \neq s} h(\epsilon_i) + \sum_{i=K+1}^{\infty} c_i \underset{(4),(5)}{\leq} h(2^s 2\epsilon / c_s) + 2\epsilon.
\end{aligned}$$

Thus, we can choose $\epsilon' > 0$ small enough and apply the proof for ϵ', such that $P(\boldsymbol{c}, \boldsymbol{\alpha}) = P(\boldsymbol{c}, \tilde{\boldsymbol{\alpha}}) \pm \epsilon$. □

4.2.2 Upper bounding $\rho^*_{\min}(n)$

The idea here is similar to the idea of the lower bound proof. Here $\mathcal{C}^{\leq l}$ is the set of all pairs $(\boldsymbol{c}, b) \in \mathcal{C}$ such that if $i > l$ then $c_i = 0$. In order to prove Lemma 4.7, we will prove two claims. The first allows us to remove or add constraints on the choice of a pair $(\boldsymbol{c}, b) \in \mathcal{C}$ without changing much the value of $P(\boldsymbol{c}, \boldsymbol{\alpha})$:

Lemma 4.12. *It holds that:*

$$\lim_{k \to \infty} \min_{\substack{(\boldsymbol{c}, b) \in \mathcal{C}^{\leq k}: \\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) = G(\beta).$$

The second claim shows, essentially, that the summation appearing in $\rho^*_{\min}(n)$ is redundant for approximation up to sub-exponential factors, if the pair $(\boldsymbol{c}, b)$ chosen by the minimization belongs to $\mathcal{C}^{\leq k}$:

Lemma 4.13. *Let $n = \beta \cdot 2^k$ and $(\boldsymbol{c}, b) \in \mathcal{C}^{\leq k}$ such that $\boldsymbol{c}$ is k-feasible. Then:*

$$\max_{d\in[n]} \sum_{\boldsymbol{\alpha}\in S_d^{\leq k}} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} \leq \exp_2\Big(\max_{\alpha\in\mathcal{A}} P(\boldsymbol{c},\boldsymbol{\alpha})n + o(n)\Big).$$

Having Lemmas 4.12 and 4.13, we can prove Lemma 4.7:

Proof of Lemma 4.7. We have:

$$\begin{aligned}
\rho^*_{\min}(n) &= \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}:\\ \boldsymbol{c}\text{ is }k\text{-feasible}}} \max_{\substack{d\in[n]:\\ S_d\neq\emptyset}} \sum_{\boldsymbol{\alpha}\in S_d} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} \\
&\leq \min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}^{\leq k}:\\ \boldsymbol{c}\text{ is }k\text{-feasible}}} \max_{\substack{d\in[n]:\\ S_d\neq\emptyset}} \sum_{\boldsymbol{\alpha}\in S_d^{\leq k}} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{d}} \\
&\underset{\text{Lem 4.13}}{\leq} \exp_2\left(\min_{\substack{(\boldsymbol{c},b)\in\mathcal{C}^{\leq k}:\\ \boldsymbol{c}\text{ is }k\text{-feasible}}} \max_{\alpha\in\mathcal{A}} P(\boldsymbol{c},\boldsymbol{\alpha})n + o(n)\right) \\
&\underset{\text{Lem 4.12}}{\leq} \exp_2\Big(\inf_{(\boldsymbol{c},b)\in\mathcal{C}} \max_{\alpha\in\mathcal{A}} P(\boldsymbol{c},\boldsymbol{\alpha})n + o(n)\Big) = 2^{G(\beta)n+o(n)}.
\end{aligned}$$

□

Now we shall prove Lemmas 4.12–4.13. We prove Lemma 4.13 first since it is simpler.

Proof of Lemma 4.13. Let $n = \beta \cdot 2^k$ and $(\boldsymbol{c}, b) \in \mathcal{C}^{\leq k}$ such that $\boldsymbol{c}$ is k-feasible. Let $\boldsymbol{\alpha} \in \bigcup_{d\in[n]} S_d^{\leq k}$ such that

$$\max_{\boldsymbol{\alpha'}\in\bigcup_{d\in[n]} S_d^{\leq k}} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha'_i c_i n}}{\binom{n}{\sum_{i=0}^{\infty}\alpha'_i c_i n}} = \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{\sum_{i=0}^{\infty}\alpha_i c_i n}}. \tag{6}$$

Combinatorial considerations imply that

$$\left|\bigcup_{d\in[n]} S_d^{\leq k}\right| \leq (n+1)^{k+1} = O\Big(n^{\log n+1}\Big) \tag{7}$$

since for a sequence $\boldsymbol{\alpha'} \in \bigcup_{d\in[n]} S_d^{\leq k}$, if $0 \leq i \leq k$ then $\alpha'_i n$ can potentially be any number between 0 and n, and else $\alpha'_i n = 0$. Hence:

$$\begin{aligned}
\max_{d\in[n]} \sum_{\boldsymbol{\alpha'}\in S_d^{\leq k}} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha'_i c_i n}}{\binom{n}{d}} &\leq \sum_{\boldsymbol{\alpha'}\in\bigcup_{d\in[n]} S_d^{\leq k}} \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha'_i c_i n}}{\binom{n}{\sum_{i=0}^{\infty}\alpha'_i c_i n}} \\
&\underset{(6),(7)}{\leq} O\Big(n^{\log n+1}\Big) \cdot \frac{\prod_{i=0}^{\infty}\binom{c_i n}{\alpha_i c_i n}}{\binom{n}{\sum_{i=0}^{\infty}\alpha_i c_i n}} \\
&\underset{(3)}{\leq} O\Big(n^{\log n+1}\Big) \cdot \frac{\exp_2(h(\alpha_i)c_i n)}{\exp_2(h(\sum_{i=0}^{\infty}\alpha_i c_i)n)/O(\sqrt{n})} \\
&= \exp_2(P(\boldsymbol{c},\boldsymbol{\alpha})n + o(n)) \underset{(*)}{\leq} \exp_2\Big(\max_{\boldsymbol{\alpha'}\in\mathcal{A}} P\big(\boldsymbol{c},\boldsymbol{\alpha'}\big)n + o(n)\Big)
\end{aligned}$$

where $(*)$ is since $\bigcup_{d\in[n]} S_d^{\leq k} \subseteq \mathcal{A}$ by definition, and hence $\boldsymbol{\alpha} \in \mathcal{A}$. □

The proof of Lemma 4.12 is implied by the following:

Lemma 4.14. *Fix $(\boldsymbol{c}, b) \in \mathcal{C}$ and let $\epsilon > 0$. There is $K \in \mathbb{N}$ and $(\tilde{\boldsymbol{c}}, b) \in \mathcal{C}^{\leq K}$, where $\tilde{\boldsymbol{c}}$ is K-feasible, such that for any $\tilde{\boldsymbol{\alpha}} \in [0,1]^{\mathbb{N}}$ satisfying $\sum_{i=0}^{\infty} \tilde{\alpha}_i \tilde{c}_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$ there is $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ satisfying $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$, and $P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) = P(\boldsymbol{c}, \boldsymbol{\alpha}) \pm \epsilon$.*

Having Lemma 4.14 in hand, we can prove Lemma 4.12:

Proof of Lemma 4.12. Let $\epsilon > 0$ and $\epsilon' = \epsilon/3$. Let $(\boldsymbol{c}, b) \in \mathcal{C}$ which satisfies:

$$\max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) \leq G(\beta) + \epsilon'. \tag{8}$$

Let $K \in \mathbb{N}$ large enough such that Lemma 4.14 holds for $(\boldsymbol{c}, b)$ and ϵ'. Let $\tilde{\boldsymbol{\alpha}} \in [0,1]^{\mathbb{N}}$ which satisfies $\sum_{i=0}^{\infty} \tilde{\alpha}_i \tilde{c} / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$ and:

$$\max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\tilde{\boldsymbol{c}}, \boldsymbol{\alpha}) \leq P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) + \epsilon'. \tag{9}$$

Hence for any $k \geq K$:

$$\begin{aligned}
\min_{\substack{(\boldsymbol{c}, b) \in \mathcal{C}^{\leq k} \\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) &\underset{(*)}{\leq} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\tilde{\boldsymbol{c}}, \boldsymbol{\alpha}) \\
&\underset{(9)}{\leq} P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) + \epsilon' \\
&\underset{\text{Lem 4.14}}{\leq} P(\boldsymbol{c}, \boldsymbol{\alpha}) + 2\epsilon' \\
&\underset{(**)}{\leq} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) + 2\epsilon' \underset{(8)}{\leq} G(\beta) + 3\epsilon'
\end{aligned}$$

where $(*)$ is since $(\tilde{\boldsymbol{c}}, b) \in \mathcal{C}^{\leq k}$ and $\tilde{\boldsymbol{c}}$ is k-feasible, and $(**)$ is since $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ and satisfies $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$. Since $3\epsilon' = \epsilon$, and since obviously

$$\inf_{(\boldsymbol{c}, b) \in \mathcal{C}} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) \leq \min_{\substack{(\boldsymbol{c}, b) \in \mathcal{C}^{\leq k} \\ \boldsymbol{c} \text{ is } k\text{-feasible}}} \max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}),$$

the lemma follows. □

It remains to prove Lemma 4.14. The proof idea is similar to the idea appearing in the proof of Lemma 4.10 presented in the previous subsection. Hence, we only present a detailed proof for this Lemma (without a proof sketch):

Proof of Lemma 4.14. Fix $(\boldsymbol{c}, b) \in [0,1]^{\mathbb{N}}$ satisfying $\sum_{i=0}^{\infty} c_i / 2^i = \frac{1}{\beta \cdot 2^b}$ and $\sum_{i=0}^{\infty} c_i \leq 1$ (that is, $(\boldsymbol{c}, b) \in \mathcal{C}$). Consider two different cases. First, assume that $\boldsymbol{c}$ is the following sequence:

$$c_i = \begin{cases} 1 & i = 0, \\ 0 & i \neq 0. \end{cases}$$

It is possible since the equation $\sum_{i=0}^{\infty} c_i / 2^i = 1 = \frac{1}{\beta \cdot 2^b}$ holds whenever $\beta = 1, b = 0$. In that case, $\boldsymbol{c} \in \mathcal{C}^{\leq 0}$ and $\boldsymbol{c}$ is 0-feasible, thus the lemma follows with $K = 0$, $\tilde{\boldsymbol{c}} = \boldsymbol{c}$. So, assume now that $c_0 < 1$. We divide the proof under that assumption into four parts: First we define $\tilde{\boldsymbol{c}}$. Then we show that $\tilde{\boldsymbol{c}} \in \mathcal{C}^{\leq K'}$ and $\tilde{\boldsymbol{c}}$ is K'-feasible for some $K' \in \mathbb{N}$. After that, given $\tilde{\boldsymbol{\alpha}}$ we define $\boldsymbol{\alpha}$ and show $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$. Finally, we show $P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) = P(\boldsymbol{c}, \boldsymbol{\alpha}) \pm \epsilon$.

Defining $\tilde{c}$. Recall that $\sum_{i=0}^{\infty} c_i \leq 1$ and thus there is $K \in \mathbb{N}$ such that $\sum_{i>K} c_i < \epsilon$. Let $\tilde{\boldsymbol{c}}$ be the following sequence:

$$\tilde{c}_i = \begin{cases} c_0 + \epsilon_0 & i = 0, \\ c_i - \epsilon_i & i \neq 0, \end{cases}$$

where $\boldsymbol{\epsilon}$ is an arbitrary sequence satisfying the following constraints:

1. If $i > K$: $\epsilon_i = c_i$.
2. Otherwise, if $1 \leq i \leq K$: $\epsilon_i = c_i - \frac{l_i}{\beta \cdot 2^{t_i}}$, where $l_i, t_i \in \mathbb{N}$ and $0 \leq \epsilon_i \leq \epsilon/K$.
3. $\epsilon_0 = \sum_{i=1}^{\infty} \epsilon_i / 2^i = \frac{l_0}{\beta \cdot 2^{t_0}} - c_0$, where $l_0, t_0 \in \mathbb{N}$.

In order to continue with the proof, we first have to show that such a sequence $\boldsymbol{\epsilon}$ exists. It is not hard to construct a sequence that satisfies constraints $(1), (2)$. We should satisfy constraint (3) as well, that is:

$$\begin{aligned} \frac{l_0}{\beta \cdot 2^{t_0}} - c_0 &= \sum_{i=1}^{\infty} \epsilon_i / 2^i \\ &= \sum_{i=1}^{K} \left(c_i - \frac{l_i}{\beta \cdot 2^{t_i}} \right) / 2^i + \sum_{i>K} c_i / 2^i = \sum_{i=1}^{\infty} c_i / 2^i - \sum_{i=1}^{K} \frac{l_i}{\beta \cdot 2^{t_i + i}}. \end{aligned}$$

That can be written as:

$$\sum_{i=0}^{\infty} c_i / 2^i - \sum_{i=1}^{K} \frac{l_i}{\beta \cdot 2^{t_i + i}} = \frac{l_0}{\beta \cdot 2^{t_0}}.$$

Recall that since $(\boldsymbol{c}, b) \in \mathcal{C}$, we have $\sum_{i=0}^{\infty} c_i / 2^i = \frac{1}{\beta \cdot 2^b}$, and thus we get:

$$\begin{gathered} \frac{1}{\beta \cdot 2^b} - \sum_{i=1}^{K} \frac{l_i}{\beta \cdot 2^{t_i + i}} = \frac{l_0}{\beta \cdot 2^{t_0}} \\ \iff \\ \frac{1}{2^b} - \sum_{i=1}^{K} \frac{l_i}{2^{t_i + i}} = \frac{l_0}{2^{t_0}}. \end{gathered}$$

We can find $l_0, t_0 \in \mathbb{N}$ satisfying this equation: $t_0 = b + \sum_{i=1}^{K} t_i + i$, and l_0 is determined accordingly. Obviously, $t_0 \in \mathbb{N}$. As for l_0, it is obviously in $\mathbb{Z}$ as a sum of numbers in $\mathbb{Z}$. Moreover, by the constraints:

$$l_0 = \left(c_0 + \sum_{i=1}^{\infty} \epsilon_i / 2^i \right) \beta \cdot 2^{t_0} \geq 0,$$

and thus $l_0 \in \mathbb{N}$. We have satisfied all constraints, thus we can find such a sequence $\boldsymbol{\epsilon}$. Let us now show that the values of $\boldsymbol{\epsilon}$ are small, even if we sum all of them together. That fact will help us show that the change of $\boldsymbol{c}$ to $\tilde{\boldsymbol{c}}$ has only little affect.

$$\sum_{i=0}^{\infty} \epsilon_i = \sum_{i=1}^{\infty} \epsilon_i / 2^i + \sum_{i=1}^{K} \epsilon_i + \sum_{i=K+1}^{\infty} \epsilon_i \leq 2 \sum_{i=1}^{K} \epsilon_i + 2 \sum_{i=K+1}^{\infty} \epsilon_i \leq 2 \sum_{i=1}^{K} \epsilon / K + 2\epsilon = 4\epsilon. \tag{10}$$

$\tilde{\boldsymbol{c}}$ is feasible. Now we will show that $(\tilde{\boldsymbol{c}}, b) \in \mathcal{C}^{\leq K}$ and $\tilde{\boldsymbol{c}}$ is K'-feasible for some $K' \geq K$. Based on the fact that $(\boldsymbol{c}, b) \in \mathcal{C}$, we first show $(\tilde{\boldsymbol{c}}, b) \in \mathcal{C}^{\leq K}$, that is:

1. $\tilde{\boldsymbol{c}} \in [0,1]^{\mathbb{N}}$.
2. $\sum_{i=0}^{\infty} \tilde{c}_i \leq 1$.
3. $\sum_{i=0}^{\infty} \tilde{c}_i / 2^i = \frac{1}{\beta \cdot 2^b}$.
4. $i > K \implies \tilde{c}_i = 0$ (this is obvious by the definition of $\tilde{\boldsymbol{c}}$).

We show (1): For any $i \neq 0$ it is obvious that $0 \leq \tilde{c}_i \leq 1$ from the definition of $\tilde{\boldsymbol{c}}$. For $i = 0$, $0 \leq c_0 < 1$ and hence $0 \leq \tilde{c_0} = c_0 + \epsilon_0 \leq 1$ for small enough ϵ. Thus $\tilde{\boldsymbol{c}} \in [0,1]^{\mathbb{N}}$. Now we show (2):

$$\begin{aligned}
\sum_{i=0}^{\infty} \tilde{c}_i &= c_0 + \sum_{i=1}^{\infty} \epsilon_i / 2^i + \sum_{i=1}^{K} (c_i - \epsilon_i) \\
&= \sum_{i=1}^{\infty} \epsilon_i / 2^i + \sum_{i=0}^{K} c_i - \sum_{i=1}^{K} \epsilon_i \\
&\leq \sum_{i=0}^{K} c_i + \sum_{i=K+1}^{\infty} \epsilon_i \\
&= \sum_{i=0}^{\infty} c_i \leq 1.
\end{aligned}$$

And finally (3):

$$\sum_{i=0}^{\infty} \tilde{c}_i / 2^i = c_0 + \epsilon_0 + \sum_{i=1}^{\infty} (c_i - \epsilon_i)/2^i = \sum_{i=0}^{\infty} c_i / 2^i + \epsilon_0 - \sum_{i=1}^{\infty} \epsilon_i / 2^i = \sum_{i=0}^{\infty} c_i / 2^i = \frac{1}{\beta \cdot 2^b}.$$

So indeed $(\tilde{\boldsymbol{c}}, b) \in \mathcal{C}^{\leq K}$. We show that $(\tilde{\boldsymbol{c}}, b)$ is K'-feasible where

$$K' = \max\{K, t_0, \ldots, t_K\}.$$

Let $i \in \mathbb{N}$. If $i > K$ then $\tilde{c}_i n = 0 \in \mathbb{N}$. Else:

$$\tilde{c}_i n = \frac{l_i}{\beta \cdot 2^{t_i}} \beta \cdot 2^{K'} = l_i \cdot 2^{K' - t_i} \in \mathbb{N},$$

since $K' \geq t_i$.

Defining $\boldsymbol{\alpha}$. Given $\tilde{\boldsymbol{\alpha}} \in [0,1]^{\mathbb{N}}$ such that $\sum_{i=0}^{\infty} \tilde{\alpha}_i \tilde{c}_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$, we construct $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ that "imitates" $\tilde{\boldsymbol{\alpha}}$ and satisfies $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$. For such a sequence $\tilde{\boldsymbol{\alpha}}$, consider the following expression:

$$r(\tilde{\boldsymbol{\alpha}}) = \sum_{i=1}^{\infty} \tilde{\alpha}_i \epsilon_i / 2^i - \tilde{\alpha}_0 \epsilon_0.$$

If $r(\tilde{\boldsymbol{\alpha}}) \geq 0$, let s be the first index such that $\tilde{c}_s, \tilde{\alpha}_s > 1/2^{2(b+5)}$. Else, let s be the first index such that $\tilde{c}_s > 1/2^{2(b+5)}$ and $\tilde{\alpha}_s < 3/4$. In any case, s exists and is bounded by 2^{b+4}, by Lemma 4.11. Define the sequence $\boldsymbol{\alpha}$ as follows:

$$\alpha_i = \begin{cases} \tilde{\alpha}_s - \delta_s & i = s, \\ \tilde{\alpha}_i & i \neq s, \end{cases}$$

where $\delta_s = \frac{2^s}{c_s} r(\tilde{\boldsymbol{\alpha}})$. Note that $|\delta_s|$ is small since $|r(\tilde{\boldsymbol{\alpha}})|$ is small:

$$|r(\tilde{\boldsymbol{\alpha}})| \leq \sum_{i=1}^{\infty} \tilde{\alpha}_i \epsilon_i / 2^i + \tilde{\alpha}_0 \epsilon_0 \leq \sum_{i=0}^{\infty} \epsilon_i \underset{(10)}{\leq} 4\epsilon,$$

and s is bounded by a constant. We show that $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$: If $i \neq s$ then $0 \leq \tilde{\alpha}_i = \alpha_i \leq 1$. For $i = s$, if $r(\tilde{\boldsymbol{\alpha}}) \geq 0$ then:

$$\alpha_s = \tilde{\alpha}_s - \delta_s > 1/2^{2(b+5)} - \delta_s > 0$$

for small enough ϵ and obviously $\alpha_s = \tilde{\alpha}_s - \delta_s \leq \tilde{\alpha}_s \leq 1$. Otherwise, assume $r(\tilde{\boldsymbol{\alpha}}) < 0$, then:

$$\alpha_s = \tilde{\alpha}_s - \delta_s < 3/4 - \delta_s \leq 1$$

for small enough ϵ and obviously $\alpha_s = \tilde{\alpha}_s - \delta_s \geq \tilde{\alpha}_s \geq 0$. Thus $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$. We show that $\sum_{i=1}^{\infty} \alpha_i c_i / 2^i = \frac{1}{\beta \cdot 2^{b+1}}$, that is, $\sum_{i=1}^{\infty} \alpha_i c_i / 2^i = \sum_{i=1}^{\infty} \tilde{\alpha}_i \tilde{c}_i / 2^i$:

$$\begin{aligned}
\sum_{i=1}^{\infty} \tilde{\alpha}_i \tilde{c}_i / 2^i &= \tilde{\alpha}_0 (c_0 + \epsilon_0) + \sum_{i=1}^{\infty} \tilde{\alpha}_i (c_i - \epsilon_i) / 2^i \\
&= \sum_{i=0}^{\infty} \tilde{\alpha}_i c_i / 2^i + \tilde{\alpha}_0 \epsilon_0 - \sum_{i=1}^{\infty} \tilde{\alpha}_i \epsilon_i / 2^i \\
&= \sum_{i=0}^{\infty} \alpha_i c_i / 2^i + \delta_s c_s / 2^s - r(\tilde{\boldsymbol{\alpha}}) \\
&= \sum_{i=0}^{\infty} \alpha_i c_i / 2^i + \frac{2^s}{c_s} r(\tilde{\boldsymbol{\alpha}}) \cdot \frac{c_s}{2^s} - r(\tilde{\boldsymbol{\alpha}}) = \sum_{i=0}^{\infty} \alpha_i c_i / 2^i.
\end{aligned}$$

$P(\boldsymbol{c}, \boldsymbol{\alpha})$ approximates $P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}})$. It remains to show $P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) = P(\boldsymbol{c}, \boldsymbol{\alpha}) \pm \epsilon$. Due to Lemma 2.3, indeed:

$$\begin{aligned}
P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) &= \sum_{i=0}^{\infty} h(\tilde{\alpha}_i) \tilde{c}_i - h\left(\sum_{i=0}^{\infty} \tilde{\alpha}_i \tilde{c}_i \right) \\
&= h(\alpha_s + \delta_s) \tilde{c}_s + \sum_{i \neq s} h(\alpha_i) \tilde{c}_i - h\left(\sum_{i=0}^{\infty} \alpha_i \tilde{c}_i + \delta_s \tilde{c}_s \right) \\
&= \sum_{i=0}^{\infty} h(\alpha_i) \tilde{c}_i - h\left(\sum_{i=0}^{\infty} \alpha_i \tilde{c}_i \right) \pm h(|\delta_s|) \tilde{c}_s \pm h(|\delta_s| \tilde{c}_s) \\
&= P(\tilde{\boldsymbol{c}}, \boldsymbol{\alpha}) \pm h(|\delta_s|) \tilde{c}_s \pm h(|\delta_s| \tilde{c}_s).
\end{aligned}$$

Recall that $|\delta_s|$ is small. Now:

$$\begin{aligned}
P(\tilde{\boldsymbol{c}}, \boldsymbol{\alpha}) &= \sum_{i=0}^{\infty} h(\alpha_i) \tilde{c}_i - h\left(\sum_{i=0}^{\infty} \alpha_i \tilde{c}_i \right) \\
&= \sum_{i=0}^{\infty} h(\alpha_i) c_i + h(\alpha_0) \epsilon_0 - \sum_{i=1}^{\infty} h(\alpha_i) \epsilon_i - h\left(\sum_{i=0}^{\infty} \alpha_i c_i + \alpha_0 \epsilon_0 - \sum_{i=1}^{\infty} \alpha_i \epsilon_i \right) \\
&= \sum_{i=0}^{\infty} h(\alpha_i) c_i - h\left(\sum_{i=0}^{\infty} \alpha_i c_i \right) + h(\alpha_0) \epsilon_0 - \sum_{i=1}^{\infty} h(\alpha_i) \epsilon_i \pm h(\alpha_0 \epsilon_0) \pm h\left(\sum_{i=1}^{\infty} \alpha_i \epsilon_i \right) \\
&= P(\boldsymbol{c}, \boldsymbol{\alpha}) + h(\alpha_0) \epsilon_0 - \sum_{i=1}^{\infty} h(\alpha_i) \epsilon_i \pm h(\alpha_0 \epsilon_0) \pm h\left(\sum_{i=1}^{\infty} \alpha_i \epsilon_i \right).
\end{aligned}$$

Recall that $\sum_{i=0}^{\infty} \epsilon_i \leq 4\epsilon$ due to (10). Thus, we can choose ϵ' small enough and apply the proof for ϵ', such that

$$P(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{\alpha}}) = P(\tilde{\boldsymbol{c}}, \boldsymbol{\alpha}) \pm \epsilon' = P(\boldsymbol{c}, \boldsymbol{\alpha}) \pm 2\epsilon' = P(\boldsymbol{c}, \boldsymbol{\alpha}) \pm \epsilon. \qquad \square$$

5 Applications of Theorem 4.1

5.1 Alternative proofs for known bounds on $q(n)$

In the previous sections we have shown the estimate $q(n) = 2^{-G(\beta)n \pm o(n)}$. Unfortunately, we do not know how to calculate $G(\beta)$ in general. However, we can use this estimate to give alternative proofs for known bounds on $q(n)$, and in the next subsection, also to give a better lower bound. The following theorems are stated and proved in [DFGM19]:

Theorem 5.1 ([DFGM19])**.** *For any n, it holds that $q(n) \leq 1.25^{n+o(n)}$.*

Theorem 5.2 ([DFGM19])**.** *For $n = \beta \cdot 2^k$ it holds that $q(n) \geq 2^{\left(h\left(\frac{1}{2^{b+1}\beta}\right) - \frac{1}{2^b \beta}\right)n - o(n)}$ for any $b \in \mathbb{N}$.*

For any β, we can find a "good" lower bound on $q(n)$ by choosing $b = 0$ or $b = 1$ and applying Theorem 5.2. Specifically, when $\beta = 1.25$ we get $q(n) = 1.25^{n \pm o(n)}$ by choosing $b = 1$, and for other values of β we can always ensure that $q(n) \geq 1.232^{n - o(n)}$ by choosing $b = 0$ or $b = 1$, depending on β. We give alternative, simple proofs for these bounds:

Proof of Theorem 5.1. Fix $\beta \in [1, 2)$. Let $\boldsymbol{\alpha}$ such that: $\alpha_i = 1/2$ for any i. Note that $\boldsymbol{\alpha} \in \mathcal{A}$ for any fixed $(\boldsymbol{c}, b) \in \mathcal{C}$. Thus:

$$\begin{aligned} G(\beta) &= \inf_{(\boldsymbol{c},b)\in\mathcal{C}} \max_{\boldsymbol{\alpha}\in\mathcal{A}} \sum_{i=0}^{\infty} h(\alpha_i)c_i - h\left(\sum_{i=0}^{\infty} \alpha_i c_i\right) \\ &\geq \inf_{(\boldsymbol{c},b)\in\mathcal{C}} \sum_{i=0}^{\infty} h(1/2)c_i - h\left(\sum_{i=0}^{\infty} \frac{1}{2} c_i\right) \\ &= \inf_{(\boldsymbol{c},b)\in\mathcal{C}} \sum_{i=0}^{\infty} c_i - h\left(\frac{1}{2}\sum_{i=0}^{\infty} c_i\right). \end{aligned}$$

Denote $x = \sum_{i=0}^{\infty} c_i$, so $0 \leq x \leq 1$, since $(\boldsymbol{c}, b) \in \mathcal{C}$. Hence :

$$\inf_{(\boldsymbol{c},b)\in\mathcal{C}} \sum_{i=0}^{\infty} c_i - h\left(\frac{1}{2}\sum_{i=0}^{\infty} c_i\right) \geq \inf_{0\leq x\leq 1} x - h(x/2).$$

Calculation shows that:

$$\inf_{0\leq x\leq 1} x - h(x/2) = 0.4 - h(0.4/2) = -\log 1.25.$$

That is, $G(\beta) \geq -\log 1.25$, and hence indeed:

$$q(n) = 2^{-G(\beta)n \pm o(n)} \leq 2^{\log 1.25 n + o(n)} = 1.25^{n+o(n)}. \qquad \square$$

Proof of Theorem 5.2. Fix $\beta \in [1, 2)$. Let $(\boldsymbol{c(b)}, b) \in \mathcal{C}$ such that $b \in \mathbb{N}$ and $\boldsymbol{c(b)}$ is the following sequence:

$$c(b)_i = \begin{cases} \frac{1}{2^b \beta} & i = 0, \\ 0 & i \neq 0. \end{cases}$$

Indeed $(\boldsymbol{c(b)}, b) \in \mathcal{C}$ for any b, since all constraints are satisfied:

- $b \in \mathbb{N}$.
- We have $0 \leq \frac{1}{2^b \cdot 2} \leq \frac{1}{2^b \beta} \leq \frac{1}{2^0 \cdot 1} = 1$ and hence $0 \leq c(b)_i \leq 1$ for any i.
- $\sum_{i=0}^{\infty} c(b)_i = \frac{1}{2^b \beta} \leq 1$.
- $\sum_{i=0}^{\infty} c(b)_i 2^{b-i} \cdot \beta = \frac{1}{2^b \beta} \cdot 2^b \beta = 1$.

Moreover, a sequence $\boldsymbol{\alpha} \in \mathcal{A}$ must satisfy $\alpha_0 = 1/2$, and for any other i the value of α_i does not have any effect. Thus:

$$\begin{aligned} G(\beta) &= \inf_{(\boldsymbol{c},b) \in \mathcal{C}} \max_{\boldsymbol{\alpha} \in \mathcal{A}} \sum_{i=0}^{\infty} h(\alpha_i) c_i - h\left(\sum_{i=0}^{\infty} \alpha_i c_i \right) \\ &\leq \max_{\boldsymbol{\alpha} \in \mathcal{A}} \sum_{i=0}^{\infty} h(\alpha_i) c(b)_i - h\left(\sum_{i=0}^{\infty} \alpha_i c(b)_i \right) \\ &= h(1/2) \cdot \frac{1}{2^b \beta} - h\left(\frac{1}{2} \cdot \frac{1}{2^b \beta} \right) = \frac{1}{2^b \beta} - h\left(\frac{1}{2^{b+1} \beta} \right). \end{aligned}$$

Hence:

$$q(n) = 2^{-G(\beta)n \pm o(n)} \geq 2^{\left(h\left(\frac{1}{2^{b+1}\beta} \right) - \frac{1}{2^b \beta} \right) n - o(n)}. \qquad \square$$

5.2 A new lower bound on $q(n)$

Using our estimate $q(n) = 2^{-G(\beta)n \pm o(n)}$ we can find a tighter lower bound on $q(n)$ than the one appearing in [DFGM19], that is, $1.232^{n-o(n)}$. We do that by finding a matching upper bound on $G(\beta)$. We already know that $G(\beta) \leq \frac{1}{2^b \beta} - h\left(\frac{1}{2^{b+1}\beta} \right)$ for any $b \in \mathbb{N}$, as described in our alternative proof for the known lower bound on $q(n)$. For $\beta \leq 1.7$ and $b = 1$ we have $G(\beta) \leq \frac{1}{2 \cdot 1.7} - h\left(\frac{1}{4 \cdot 1.7} \right) \approx -0.3083$ and for $\beta \geq 1.95$ we have $G(\beta) \leq \frac{1}{1.95} - h\left(\frac{1}{2 \cdot 1.95} \right) \approx -0.30846$. So, if we find $M > -0.3083$ such that for $1.7 < \beta < 1.95$: $G(\beta) \leq M$, then M is an upper bound for $G(\beta)$. As we will now show, it is possible for $M \approx -0.305758$. The idea is to fix $b = 1$ and consider sequences $\boldsymbol{c}$ in which $s = c_0 + c_1$ is fixed and $c_i = 0$ for all $i \geq 2$. Then, due to the constraint $\sum_{i=0}^{\infty} c_i / 2^i = 1/2\beta$ we can express c_0 and c_1 in terms of β. Finally, we use Lagrange multipliers to find the maximizing $\boldsymbol{\alpha}$ for $\boldsymbol{c}$.

Theorem 5.3. *For any $n \in \mathbb{N}$, it holds that $q(n) \geq 1.236^{n-o(n)}$.*

Proof. Consider the sequence $\boldsymbol{c}$ defined by $c_0 = 1/\beta - s$, $c_1 = 2s - 1/\beta$ and $c_i = 0$ for all $i \geq 2$, for some fixed s. It is feasible:

$$\sum_{i=0}^{\infty} c_i / 2^i = 1/\beta - s + (2s - 1/\beta)/2 = 1/2\beta,$$

as required. We calculate $\max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha})$ using Lagrange multipliers. Our only constraint is $\sum_{i=0}^{\infty} \alpha_i c_i / 2^i - 1/4\beta = 0$, so we get the Lagrangian function

$$\mathcal{L}(\alpha_0, \alpha_1, \lambda) = h(\alpha_0) c_0 + h(\alpha_1) c_1 - h(\alpha_0 c_0 + \alpha_1 c_1) + \lambda(\alpha_0 c_0 + \alpha_1 c_1 / 2 - 1/4\beta).$$

Recall that $h'(x) = \log \frac{1-x}{x}$ and compute the derivatives:

$$\begin{aligned} \frac{d\mathcal{L}(\alpha_0, \alpha_1, \lambda)}{d\alpha_0} &= c_0 \log \frac{1 - \alpha_0}{\alpha_0} - c_0 \log \frac{1 - \alpha_0 c_0 - \alpha_1 c_1}{\alpha_0 c_0 + \alpha_1 c_1} + \lambda c_0 \\ &= c_0 \log \frac{(1 - \alpha_0)(\alpha_0 c_0 + \alpha_1 c_1)}{\alpha_0 (1 - \alpha_0 c_0 - \alpha_1 c_1)} + \lambda c_0 = 0, \end{aligned} \tag{11}$$

$$\frac{d\mathcal{L}(\alpha_0,\alpha_1,\lambda)}{d\alpha_1} = c_1\log\frac{1-\alpha_1}{\alpha_1} - c_1\log\frac{1-\alpha_0c_0-\alpha_1c_1}{\alpha_0c_0+\alpha_1c_1} + \lambda c_1/2$$
$$= c_1\log\frac{(1-\alpha_1)(\alpha_0c_0+\alpha_1c_1)}{\alpha_1(1-\alpha_0c_0-\alpha_1c_1)} + \lambda c_1/2 = 0, \tag{12}$$

$$\frac{d\mathcal{L}(\alpha_0,\alpha_1,\lambda)}{d\lambda} = \alpha_0c_0+\alpha_1c_1/2 - 1/4\beta = 0. \tag{13}$$

We assume $c_0, c_1 > 0$, so equations (11),(12) can be written as

$$\log\frac{(1-\alpha_0)(\alpha_0c_0+\alpha_1c_1)}{\alpha_0(1-\alpha_0c_0-\alpha_1c_1)} = -\lambda,$$
$$\log\left(\frac{(1-\alpha_1)(\alpha_0c_0+\alpha_1c_1)}{\alpha_1(1-\alpha_0c_0-\alpha_1c_1)}\right)^2 = -\lambda,$$

so we get:

$$\frac{1-\alpha_0}{\alpha_0}\cdot\frac{\alpha_0c_0+\alpha_1c_1}{1-\alpha_0c_0-\alpha_1c_1} = \frac{(1-\alpha_1)^2}{\alpha_1^2}\cdot\left(\frac{\alpha_0c_0+\alpha_1c_1}{1-\alpha_0c_0-\alpha_1c_1}\right)^2$$
$$\iff$$
$$\frac{1-\alpha_0}{\alpha_0} = \frac{(1-\alpha_1)^2}{\alpha_1^2}\cdot\frac{\alpha_0c_0+\alpha_1c_1}{1-\alpha_0c_0-\alpha_1c_1}$$

since $\alpha_0c_0+\alpha_1c_1 > 0$. Together with equation (13), we can solve two equations with two unknowns and find α_0, α_1. Calculation shows that there is only one real solution, which is a critical point, and we will deduce that it is also a maximum point. First, we have to fix s. We used a software program to try and find a good value for s. It must hold that $c_1 = 2s - 1/\beta > 0$, that is, $s > \frac{1}{2\beta}$, implying $s > 5/17$ (since $\beta > 1.7$). Iteratively checking all feasible values of s with gaps of $1/1000$, it seems that $s = 829/2000$ is a good choice. For that value of s, the maximal value of $P(\boldsymbol{c},\boldsymbol{\alpha})$ (where $\boldsymbol{\alpha}$ is defined by the critical point solution found for α_0, α_1) is ~ -0.305758, attained at $\beta \approx 1.80941$. It remains to check that the critical point solution found for α_0, α_1 is indeed a maximum point. Since in our critical point $\alpha_0, \alpha_1 \notin \{0,1\}$ for any β, we can do that by checking the values attained when $\alpha_0 \in \{0,1\}$ or $\alpha_1 \in \{0,1\}$ and verify they are lower than the value attained at our critical point. Calculation shows that when choosing such points we get a lower value for $P(\boldsymbol{c},\boldsymbol{\alpha})$ for any β, compared to the value attained at the critical point. Thus the critical point we have found is indeed a maximum point and $G(\beta) \leq -0.305758$ for any $1 \leq \beta < 2$. That is, $q(n) \geq 2^{0.305758n-o(n)} > 1.236^{n-o(n)}$. □

Figure 1 demonstrates our new bound for different values of β.

5.3 Improving the bound $q(n) \leq 1.25^{n+o(n)}$ for n far from $1.25 \cdot 2^k$

Using our formula for $G(\beta)$, it can be shown that when $\beta \neq 1.25$, the upper bound of $q(n) \leq 1.25^{n+o(n)}$ can be exponentially improved. This result is formally stated as follows:

Theorem 5.4. *If $\beta = 5/4 + \delta_\beta$ such that $|\delta_\beta| > 0$, then there exists $\gamma > 1$ such that $q(n) \leq (1.25/\gamma)^{n+o(n)}$. Furthermore, $\gamma = 2^{\Omega\left(|\delta_\beta|^{2+\epsilon}\right)}$, where $\epsilon > 0$ is any fixed constant of our choice.*

We prove the theorem using a sequence of steps. First, we show that sequences $\boldsymbol{c} \in \mathcal{C}$ with $\sum_{i=0}^{\infty} c_i$ which is far from $2/5$ can be ruled out as witnesses for $q(n) = 1.25^{n\pm o(n)}$:

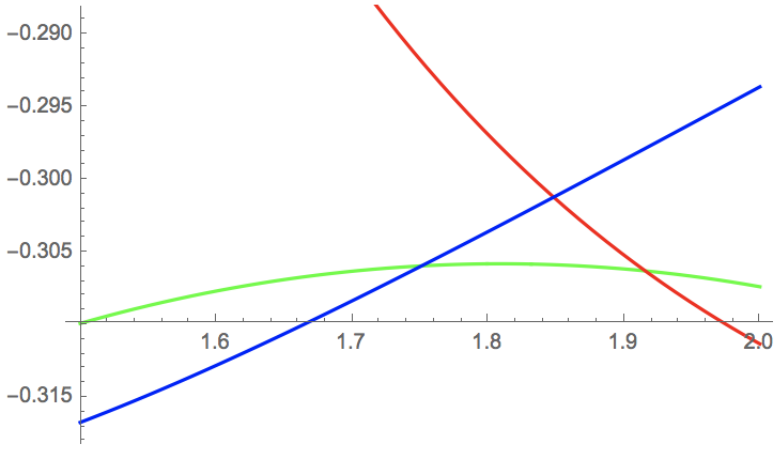

Figure 1: The blue and red curves are the known upper bounds $\frac{1}{2\beta} - h\left(\frac{1}{4\beta}\right)$ and $\frac{1}{\beta} - h\left(\frac{1}{\beta}\right)$, respectively. Our new upper bound is the green curve, which is better in a range of β values.

Lemma 5.5. *Let $\boldsymbol{c} \in \mathcal{C}$ and $x = \sum_{i=0}^{\infty} c_i$. If $x = 2/5 \pm \delta$, then $\max_{\boldsymbol{\alpha} \in \mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha}) \geq -\log(5/4) + \Omega(\delta^2)$.*

Proof. Define $\boldsymbol{\alpha} \in \mathcal{A}$ that assigns $\alpha_i = 1/2$ for all $i \in \mathbb{N}$, which is always a feasible choice. Then:

$$P(\boldsymbol{c}, \boldsymbol{\alpha}) = x - h(x/2).$$

The function $x - h(x/2)$ attains its unique minimum at $x = 2/5$, at which point its value is $-\log(5/4)$. By a linear approximation around $2/5$,

$$x - h(x/2) = -\log 1.25 + \Omega(\delta^2). \qquad \square$$

The next technical lemma is required for the argument used in the proof of the theorem.

Lemma 5.6. *For every $\delta_\beta \neq 0$ the following holds for $\delta_0 = |\delta_\beta|/100$.*

Let $\beta = 5/4 + \delta_\beta$ and let $\boldsymbol{c} \in \mathcal{C}$ with $x := \sum_{i=0}^{\infty} c_i = 2/5 \pm \delta \geq \frac{1}{\beta 2^b}$, where $0 \leq \delta \leq \delta_0$. Then there exists $I \in \mathbb{N}$ such that:

$$x - \frac{2^{I-b}}{\beta} = \Omega(|\delta_\beta|),$$
$$x - \frac{2^{I+1-b}}{\beta} = -\Omega(|\delta_\beta|).$$

Proof. Let $I \in \mathbb{N}$ be the largest value for which $x - \frac{2^{I-b}}{\beta} \geq 0$. There must be such I: clearly, there exists I' for which $x - \frac{2^{i-b}}{\beta} < 0$ for any $i \geq I'$. Moreover, by assumption, when choosing $I = 0$ we have $x - \frac{2^{I-b}}{\beta} = x - \frac{1}{\beta 2^b} \geq 0$.

Having that, the correctness of the lemma boils down to whether the expression $\left|x - \frac{2^l}{\beta}\right|$ might be very small when x is close enough to $2/5$ and β is far enough from 1.25. The answer is negative: if $l \leq -2$ then $2^l/\beta \leq \frac{1}{4\beta} \leq 1/4$ and hence $\left|x - \frac{2^l}{\beta}\right| = \Omega(1)$ even for a constant δ. On

the other hand, if $l \geq 0$ then $2^l/\beta \geq 1/\beta \geq 1/2$, so in this case too $\left|x - \frac{2^l}{\beta}\right| = \Omega(1)$ even for a constant δ. So, the only difficult value of l is $l = -1$. In this case:

$$x - \frac{2^l}{\beta} = 2/5 \pm \delta - \frac{1}{2(1.25 + \delta_\beta)} = \frac{\delta_\beta(8 \pm 20\delta) \pm 25\delta}{25 + 25\delta_\beta} = \pm\Omega(|\delta_\beta|). \qquad \square$$

Now we are ready to prove the theorem.

Proof of Theorem 5.4. Let $\epsilon > 0$ be a fixed constant. We will show that $G(\beta) \geq -\log(5/4) + \Omega\Big(|\delta_\beta|^{2+\epsilon}\Big)$, thus implying the result stated in the theorem. We show that for all $b \in \mathbb{N}$ and $\boldsymbol{c} \in [0,1]^{\mathbb{N}}$ satisfying $\sum_{i=0}^{\infty} c_i/2^i = \frac{1}{\beta \cdot 2^b}$ and $\sum_{i=0}^{\infty} c_i \leq 1$, we can find $\boldsymbol{\alpha} \in [0,1]^{\mathbb{N}}$ such that $\sum_{i=0}^{\infty} \alpha_i c_i/2^i = \frac{1}{\beta \cdot 2^{b+1}}$ and $P(\boldsymbol{c}, \boldsymbol{\alpha}) \geq -\log(5/4) + \Omega\Big(|\delta_\beta|^{2+\epsilon}\Big)$.

Let $\delta_0 = |\delta_\beta|/100$ and denote $x = \sum_{i=0}^{\infty} c_i = 2/5 \pm \delta$. By Lemma 5.5, if $|x - 2/5| \geq \delta_0$, then the theorem follows even with $\epsilon = 0$. Hence we can assume, from now on, that $|x - 2/5| < \delta_0$.

Let $S \subseteq \mathbb{N}$, let $T = \mathbb{N} \setminus S$, and let $\eta_S, \eta_T \in [-1, 1]$ be two parameters small in magnitude. Define

$$p_S = \sum_{i \in S} c_i/2^i, \qquad q_S = \sum_{i \in S} c_i,$$
$$p_T = \sum_{i \in T} c_i/2^i, \qquad q_T = \sum_{i \in T} c_i.$$

Consider the assignment

$$\alpha_i = \begin{cases} \frac{1}{2} + \eta_S & \text{if } i \in S, \\ \frac{1}{2} + \eta_T & \text{if } i \in T. \end{cases}$$

Since $\sum_{i=0}^{\infty} \frac{1}{2} \cdot c_i/2^i = \frac{1}{\beta \cdot 2^{b+1}}$, this assignment is feasible if

$$\eta_S p_S + \eta_T p_T = 0.$$

We assume henceforth that $\eta = \max(|\eta_S|, |\eta_T|) \leq \eta_0$, where $\eta_0 = O\Big(|\delta_\beta|^{1+\epsilon}\Big)$. By construction, we have $h(\alpha_i) = 1 - O(\eta^2)$ using a linear approximation. In contrast,

$$\sum_{i=0}^{\infty} \alpha_i c_i = \frac{x}{2} + \eta_S q_S + \eta_T q_T.$$

Since $|x - 2/5| < \delta_0$, this shows that

$$h\left(\sum_{i=0}^{\infty} \alpha_i c_i\right) = h(x/2) + (\eta_S q_S + \eta_T q_T) h'(x/2) \pm O(\eta^2)$$

using a linear approximation. Overall, this shows that

$$P(\boldsymbol{c}, \boldsymbol{\alpha}) = x - h(x/2) + (\eta_S q_S + \eta_T q_T) h'(x/2) \pm O\Big(|\delta_\beta|^{2+2\epsilon}\Big).$$

Moreover, we have $h'(x/2) = \Omega(1)$ since $x < 2/5 + \delta < 1/2$. Since $x - h(x/2) \geq -\log(5/4)$, it suffices to show that there exist η_S, η_T which are bounded in magnitude by η_0 such that $|\eta_S q_S + \eta_T q_T| = \Omega(|\delta_\beta|^{2+\epsilon})$ (if $\eta_S q_S + \eta_T q_T < 0$, we simply negate η_S, η_T).

Suppose $p_S \geq p_T$, or equivalently $p_S \geq (p_S + p_T)/2 = \frac{1}{\beta \cdot 2^{b+1}}$. Then the condition $\eta_S p_S + \eta_T p_T = 0$ shows that $\eta_S = -\frac{p_T}{p_S}\eta_T$, and so

$$\eta_S q_S + \eta_T q_T = \left(q_T - \frac{p_T}{p_S} q_S\right) \eta_T.$$

Since $|\eta_S| \leq |\eta_T|$, if $|q_T - \frac{p_T}{p_S} q_S| = \Omega(|\delta_\beta|)$ then by choosing $\eta_T = \Omega\left(|\delta_\beta|^{1+\epsilon}\right)$ we would be done.

Recall that $p_S + p_T = \frac{1}{\beta \cdot 2^b}$ and $q_S + q_T = x$. Therefore

$$q_T - \frac{p_T}{p_S} q_S = x - q_S - \frac{p_T}{p_S} q_S = x - \frac{1}{\beta \cdot 2^b} \frac{q_S}{p_S}.$$

Our goal therefore is to find a set S such that the following two conditions hold:

$$p_S \geq \frac{1}{\beta \cdot 2^{b+1}},$$
$$\left| x - \frac{1}{\beta \cdot 2^b} \frac{q_S}{p_S} \right| = \Omega(|\delta_\beta|).$$

Let $S_{\leq I} = \{0, \ldots, I\}$ and $S_{>I} = \{I+1, \ldots\}$. Let us first assume that the choice of S to be $S_{\leq 0}$ yields

$$x - \frac{1}{\beta \cdot 2^b} \frac{q_{S_{\leq 0}}}{p_{S_{\leq 0}}} = x - \frac{1}{\beta \cdot 2^b} < 0.$$

So, it must hold that $b = 1$: notice that

$$\frac{1}{2^{b+1}} \leq \frac{1}{\beta 2^b} = \sum_{i=0}^{\infty} c_i / 2^i \leq x = 2/5 \pm \delta,$$

so if $b = 0$ it is a contradiction. On the other hand, if $b \geq 2$ then

$$0 > x - \frac{1}{\beta \cdot 2^b} \geq 2/5 \pm \delta - \frac{1}{4\beta} \geq 2/5 \pm \delta - \frac{1}{4}$$

is a contradiction. So, we get that

$$0 > x - \frac{1}{\beta \cdot 2^b} \frac{q_{S_{\leq 0}}}{p_{S_{\leq 0}}} = x - \frac{1}{2\beta} = 2/5 \pm \delta - \frac{2}{5 + 4\delta_\beta},$$

implying that $\delta_\beta < 0$, and hence indeed $2/5 + \delta - \frac{2}{5+4\delta_\beta} = -\Omega(|\delta_\beta|)$. Notice that

$$\frac{q_{S_{\leq i}}}{p_{S_{\leq i}}} \geq \frac{q_{S_{\leq 0}}}{p_{S_{\leq 0}}} = 1$$

for any i, so we choose S to be $S_{\leq I}$ such that $p_{S_{\leq I}} \geq \frac{1}{\beta \cdot 2^{b+1}}$ and then both conditions hold.

Suppose now that the choice of S to be $S_{\leq 0}$ yields

$$x - \frac{1}{\beta \cdot 2^b} \frac{q_{S_0}}{p_{S_0}} = x - \frac{1}{\beta \cdot 2^b} \geq 0$$

and let $I \in \mathbb{N}$ be the one picked by Lemma 5.6. By construction, one of $S_{\leq I}, S_{>I}$ satisfies the first condition. As for the second condition,

$$x - \frac{1}{\beta \cdot 2^b} \frac{q_{S_{\leq I}}}{p_{S_{\leq I}}} \geq x - \frac{1}{\beta \cdot 2^b} 2^I = x - \frac{2^{I-b}}{\beta} = \Omega(|\delta_\beta|),$$
$$x - \frac{1}{\beta \cdot 2^b} \frac{q_{S_{>I}}}{p_{S_{>I}}} \leq x - \frac{1}{\beta \cdot 2^b} 2^{I+1} = x - \frac{2^{I+1-b}}{\beta} = -\Omega(|\delta_\beta|),$$

by Lemma 5.6, and so it is satisfied for both $S_{\leq I}, S_{>I}$. □

6 d-ary questions

In this section we generalize some results on $q(n)$ appearing in [DFGM19] to the d-ary setting, in which each question has d possible answers (instead of only "Yes" or "No"). In this setting, a set of allowed questions $\mathcal{Q}$ contains a collection of partitions of X_n to d distinguished subsets $(S_i)_{i\in[d]}$. We denote the natural generalization of $q(n)$ to the d-ary setting with $q^{(d)}(n)$. That is, $q^{(d)}(n)$ is the minimal size of a set of allowed questions $\mathcal{Q}$ that allows Alice to construct an optimal strategy for any distribution on X_n picked by Bob.

We present two results in this section. The first states that for any $d = o\big(n/\log^2 n\big)$, it holds that $q^{(d)}(n) < 2^{n+o(n)}$; this improves exponentially on the trivial upper bound $q^{(d)}(n) \le d^n/d!$. The second result is that for any fixed d, the upper bound we have just mentioned is tight up to sub-exponential factors for infinitely many n values.

In the binary setting, our results on $q(n)$ rely on the reduction of [DFGM19] from calculating $q(n)$ to calculating $\rho_{\min}(n)$, that is, on the fact that $q(n) \approx 1/\rho_{\min}(n)$ (Theorem 2.2). We take here the same approach: define $\rho^{(d)}_{\min}(n)$ to be the natural generalization of $\rho_{\min}(n)$ to the d-ary setting (a formal definition appears later). We will show that $q^{(d)}(n) \approx 1/\rho^{(d)}_{\min}(n)$, and then we find bounds on $\rho^{(d)}_{\min}(n)$ to derive bounds on $q^{(d)}(n)$. Most of the lemmas in this section are simple generalizations of those appearing in [DFGM19].

Let us first generalize some basic notions from the standard binary setting. All logarithms have base d, unless written otherwise.

Definition 6.1. A distribution μ is d-adic if every element with non-zero probability in μ has probability $d^{-\ell}$ for some positive integer ℓ.

d-ary search trees. In the d-ary setting, similarly to the standard binary setting, a strategy to reveal the secret element x is represented by a search tree. The difference is that in the d-ary setting, we use d-ary search trees (instead of binary search trees, namely, decision trees): each internal node, representing a question, has d outgoing edges, representing the possible answers.

However, if $n = |X_n|$ is not equivalent to 1 modulo $d-1$, then such a tree can not be constructed. So, if that is the case, we add a minimal set X_l of zero probability elements, such that $n+l$ is equivalent to 1 modulo $d-1$. A d-ary search tree can now be successfully constructed for $X_n \cup X_l$. For our convenience, we still relate to X_n as the set of elements (and not to $X_n \cup X_l$): note that $l < d$, and thus if we assume that d is an asymptotically small enough function of n, this has no affect on the results in this section (in particular, we do not care about sub-exponential factors in our estimates). Indeed, we have to limit the discussion only for $d = o(n/(\log n \log\log n))$, from other reasons, even when n is equivalent to 1 modulo $d-1$, so this issue has no meaning in our work.

Decision trees definitions and notation from Section 2 naturally generalize to d-ary search trees.

d-ary Huffman algorithm. Similarly to the binary case, if μ is a distribution over X_n, then the d-ary version of Huffman's algorithm finds a d-adic distribution τ that defines a search tree T with $T(x_i) = \log\frac{1}{\tau_i}$ for any non-zero element, such that the cost of T on μ, which is

$$T(\mu) = \sum_{i=1}^{n} \mu_i \log\frac{1}{\tau_i} = \sum_{i=1}^{n} \mu_i \log\frac{1}{\mu_i} + \sum_{i=1}^{n} \mu_i \log\frac{\mu_i}{\tau_i} = H(\mu) + D(\mu\|\tau)$$

(where $D(\mu\|\tau) = \sum_{i=1}^{n} \mu_i \log(\mu_i/\tau_i)$ is the *Kullback–Leibler divergence*), is optimal. This implies the inequality $T(\mu) \ge H(\mu)$ due to non-negativity of $D(\mu\|\tau)$. It holds as equality when μ is d-adic.

The chain rule of conditional entropy. Let $S = (S_j)_{j\in[d]}$ be a partition of X_n into d sets, and let μ be a distribution over X_n. Let M be a random variable drawn from μ, and let P be a random variable indicating the set in S that M belongs to. The probability distribution of P is the distribution π, defined by $\pi_j = \sum_{i\in D_j} \mu_i$ for any $j \in [d]$. The chain rule of conditional entropy states that:

$$H(M) = H(P) + H(M|P),$$

where

$$H(M|P) = \sum_p \Pr[P = p] \cdot H[M|P = p].$$

We will use it in the following equivalent form:

$$H(\mu) = H(\pi) + \sum_{j=1}^{d} \pi_j H\big(\mu|_{S_j}\big).$$

The multinomial coefficient. Let $n \in \mathbb{N}$ and $k_1, \ldots, k_d \in \mathbb{N}$ such that $\sum_{i=1}^{d} k_d = n$. Let π be the induced distribution defined by $\pi_i = k_i/n$ for any $1 \le i \le d$. We will use the following known bounds on the multinomial coefficient (see [CS04], for example):

$$\frac{1}{O(n^d)} 2^{nH(\pi)} \le \binom{n}{k_1, k_2, \ldots, k_d} \le 2^{nH(\pi)}. \tag{14}$$

In the following subsections we show the reduction $q^{(d)}(n) \approx 1/\rho^{(d)}_{\min}(n)$, then we upper and lower bound $\rho^{(d)}_{\min}(n)$, and finally prove the two main results of this section.

6.1 Reduction to d-adic hitters

First we state the following reduction.

Lemma 6.2. *A set $\mathcal{Q}$ of questions is optimal if and only if $c(\mathcal{Q}, \mu) = \mathrm{Opt}(\mu)$ for all d-adic distributions μ.*

Proof. Assume that $\mathcal{Q}$ is optimal for all d-adic distributions and let π be some arbitrary distribution. Let μ be a d-adic distribution such that:

$$\mathrm{Opt}(\pi) = \sum_{i=1}^{n} \pi_i \log \frac{1}{\mu_i}.$$

Let T be an optimal decision tree for μ using $\mathcal{Q}$ only, and let τ be the corresponding d-adic distribution, that is $\tau_i = d^{-T(x_i)}$. Since τ minimizes $H(\mu) + D(\mu\|\tau)$, $\tau = \mu$ must hold. Hence:

$$T(\pi) = \sum_{i=1}^{n} \pi_i \log \frac{1}{\tau_i} = \sum_{i=1}^{n} \pi_i \log \frac{1}{\mu_i} = \mathrm{Opt}(\pi). \qquad \square$$

Now we define the notion of *d-adic hitters*.

Definition 6.3. If μ is a non-constant d-adic distribution, we say that a partition $(S_i)_{i\in[d]}$ of X_n *divides* μ if $\mu(S_i) = 1/d$ for any $i \in [d]$. The collection of all such partitions of X_n is denoted $\mathrm{Div}(\mu)$. A set $\mathrm{Div}(\mu)$, for some distribution μ, is called a *d-adic set*. A set of questions $\mathcal{Q}$ is called a *d-adic hitter* if it intersects $\mathrm{Div}(\mu)$ for all non-constant d-adic distributions μ.

Let us generalize the "useful lemma" appearing in [DFGM19] for our usage:

Lemma 6.4. *Let $d \in \mathbb{N}$ and let $p_1 \geq \cdots \geq p_n$ be a non-increasing list of numbers of the form $p_i = d^{-a_i}$, where $a_i \in \mathbb{N}$, and let $a \in \mathbb{N}$ be such that $a \leq a_1$. If $\sum_{i=1}^{n} p_i \geq d^{-a}$ then for some m we have $\sum_{i=1}^{m} p_i = d^{-a}$. If furthermore $\sum_{i=1}^{n} p_i = l \cdot d^{-a}$ for some $l \in \mathbb{N}$ then we can divide $[n]$ to l intervals $(I_j)_{j\in[l]}$ such that for any interval $I_j \subset [n]$ we have $\sum_{i\in I_j} p_i = d^{-a}$.*

Proof. Let m be the maximal index such that $\sum_{i=1}^{m} p_i \leq d^{-a}$. If $m = n$ then we are done, so suppose that $m < n$. Let $S = \sum_{i=1}^{m} p_i$. We would like to show that $S = d^{-a}$. The condition $p_1 \geq \cdots \geq p_n$ implies that $a_{m+1} \geq \cdots \geq a_1$, and so $k = d^{a_{m+1}} S = \sum_{i=1}^{m} d^{a_{m+1}-a_i}$ is an integer. By assumption, $k \leq d^{a_{m+1}-a}$, whereas $k + 1 = d^{a_{m+1}} \sum_{i=1}^{m+1} d^{-a_i} > d^{a_{m+1}-a}$. Since $d^{a_{m+1}-a} \in \mathbb{N}$ (since $a_{m+1} \geq a_1 \geq a$), we conclude that $k = d^{a_{m+1}-a}$, and so $S = d^{-a}$.

To prove the furthermore part, notice that by repeated applications of the first part of the lemma we can partition $[n]$ into intervals with probabilities d^{-a}. □

Among else, this lemma shows (by choosing $a = 1$) that $\mathrm{Div}(\mu)$ is non-empty for any non-constant d-adic μ.

Lemma 6.5. *A set $\mathcal{Q}$ of partitions of X_n to d subsets is an optimal set of questions if and only if it is a d-adic hitter in X_n.*

Proof. Let $\mathcal{Q}$ be a d-adic hitter in X_n, and let μ be a d-adic distribution. We show by induction on the support size $m \leq n$ that $c(\mathcal{Q}, \mu) = H(\mu)$. Recall that $\mathrm{Opt}(\mu) = H(\mu)$, and thus due to Lemma 6.2 optimality of $\mathcal{Q}$ will follow. The base case $m = 1$ is trivial. So, suppose that $m > 1$ and hence μ is non-constant, and therefore $\mathcal{Q}$ contains a partition $D = (D_i)_{i\in[d]} \in \mathrm{Div}(\mu)$. Since $D \in \mathrm{Div}(\mu)$, it holds that $\mu|_{D_i}$ is d-adic for all $i \in [d]$. The induction hypothesis implies $c(\mathcal{Q}, \mu|_{D_i}) = H(\mu|_{D_i})$ for all $i \in [d]$. Having that, let us calculate $H(\mu)$. Let π be the distribution defined by $\pi_i = \mu(D_i) = 1/d$ for any $i \in [d]$, so due to the chain rule of conditional entropy and the induction hypothesis:

$$H(\mu) = H(\pi) + \sum_{i=1}^{d} \pi_i H(\mu|_{D_i}) = 1 + \sum_{i=1}^{d} \frac{1}{d} c(\mathcal{Q}, \mu|_{D_i}).$$

Now, consider the cost of a decision tree T asking D, and then uses the implied algorithms for $\mu|_{D_1}, \ldots, \mu|_{D_d}$, depending on the answer for D:

$$T(\mu) = 1 + \sum_{i=1}^{d} \mu(D_i) \cdot c(\mathcal{Q}, \mu|_{D_i}) = 1 + \sum_{i=1}^{d} \frac{1}{d} c(\mathcal{Q}, \mu|_{D_i}) = H(\mu),$$

and so $c(\mathcal{Q}, \mu) \leq H(\mu)$, thus $\mathcal{Q}$ is optimal.

Conversely, suppose that $\mathcal{Q}$ is not a d-adic hitter, so let μ be a non-constant d-adic distribution such that $\mathrm{Div}(\mu)$ is disjoint from $\mathcal{Q}$. Consider an arbitrary decision tree T for μ using $\mathcal{Q}$, and let $P = (P_i)_{i\in[d]}$ be its first question. Let also π be the distribution defined by $\pi_i = \mu(P_i)$ for any $i \in [d]$. Then

$$T(\mu) \geq 1 + \sum_{i=1}^{d} \pi_i \cdot c(\mathcal{Q}, \mu|_{P_i}) > H(\pi) + \sum_{i=1}^{d} \pi_i \cdot H(\mu|_{P_i}) = H(\mu),$$

since there is i such that $\pi_i \neq 1/d$, otherwise it contradicts $\mathcal{Q}$ and $\mathrm{Div}(\mu)$ being disjoint, thus $H(\pi) < 1$, and moreover $c(\mathcal{Q}, \mu|_{P_i}) \geq H(\mu|_{P_i})$. So the cost of any such arbitrary tree is more than $H(\mu)$, thus $\mathcal{Q}$ is not optimal. □

6.2 Reduction to maximum relative density

Let us generalize the concept of maximum relative density defined in Section 2.

Definition 6.6. Let $\mathcal{D}$ be a collection of partitions $D = (D_i)_{i\in[d]}$ of X_n. Let K be the set of all vectors $\overline{k} = (k_1, k_2, \ldots, k_d) \in \{0, \ldots, n\}^d$ such that $\sum_{i=1}^{d} k_i = n$. For $\overline{k} \in K$, denote by $\mathcal{D}_{\overline{k}} \subset \mathcal{D}$ the restriction of $\mathcal{D}$ to partitions with $|D_i| = k_i$ for all $i \in [d]$. We say that each such vector $\overline{k} \in K$ is a *type* of partitions, as this usage is similar to the concept of types in the theory of types. Define $\overline{k}$*'s relative density* of $\mathcal{D}$, denoted $\rho_{\overline{k}}(\mathcal{D})$, as

$$\rho_{\overline{k}}(\mathcal{D}) := \frac{\left|\mathcal{D}_{\overline{k}}\right|}{\binom{n}{k_1,k_2,\ldots,k_d}}.$$

We define the *maximum relative density* of $\mathcal{D}$, denoted $\rho(\mathcal{D})$, as

$$\rho(\mathcal{D}) := \max_{\overline{k}\in K} \rho_{\overline{k}}(\mathcal{D}).$$

Define $\rho^{(d)}_{\min}(n)$ to be the minimal $\rho(\mathcal{D})$ over all d-adic sets $\mathcal{D}$. We will show that calculating $q^{(d)}(n)$ up to sub-exponential factors can be reduced to calculating $\rho^{(d)}_{\min}(n)$. First, we prove an argument used in the reduction:

Lemma 6.7. *There are at most n^n non-constant d-adic distributions over X_n.*

Proof. Let μ be a non-constant d-adic distribution over X_n. We assume that the minimal non-zero probability in μ is d^{-l} and show that $n > l$ by induction on l. This argument implies that for a fixed n, the possible probabilities are only $0, d^{-1}, d^{-2}, \ldots, d^{-(n-1)}$ and hence there are at most n^n ways to construct a d-adic distribution on X_n. For the base case $l = 0$ it holds that $n > 0$. For the induction step, assume that the claim holds for $l - 1$. Let us first show that the number of elements with probability d^{-l} is a multiple of d. Denote the set of these elements with L. Since the minimal non-zero probability in $X_n \backslash L$ is at least d^{-l+1}, the total weight of the elements in $X_n \backslash L$ can be written as $x \cdot d^{-l+1}$ where $x \in \mathbb{N}$, because each element with probability d^{-l+y} for some $y \geq 1$ simply contributes d^{y-1} to x, and d^{y-1} is an integer. So, the following must hold:

$$1 = \sum_{i=1}^{n} \mu_i = \sum_{\mu_i : x_i \in L} \mu_i + \sum_{\mu_i : x_i \in X_n \backslash L} \mu_i = |L| \cdot d^{-l} + x \cdot d^{-l+1}$$

$$\iff$$

$$|L| \cdot d^{-l} = 1 - x \cdot d^{-l+1}$$

$$\iff$$

$$|L| = d^l - x \cdot d = d\Big(d^{l-1} - x\Big).$$

That is, $|L|$ is a multiple of d, since $\left(d^{l-1} - x\right)$ is an integer. Following that, we define a new distribution μ' on $X_{n'}$ by merging the elements in L into $\left(d^{l-1} - x\right)$ elements with probability d^{-l+1}. Now the minimal non-zero probability in μ' is d^{-l+1} and since we have merged at least $d > 1$ elements, it holds that $n' \leq n-1$. So, by the induction hypothesis we have $n-1 \geq n' > l-1$, that is, $n > l$. □

Now we can prove the reduction.

Theorem 6.8. *Fix $n \in \mathbb{N}$. Then:*

$$1/\rho^{(d)}_{\min}(n) \leq q^{(d)}(n) \leq 2n^{2d} \ln n / \rho^{(d)}_{\min}(n).$$

Proof. Recall that $q^{(d)}(n)$ is actually the size of a minimal d-adic hitter for X_n, due to Lemma 6.5. Hence we bound the size of such a set, instead of $q^{(d)}(n)$ directly. Fix a d-adic set $\mathcal{D}$ over X_n with $\rho(\mathcal{D}) = \rho^{(d)}_{\min}(n)$. Fix $\overline{k} \in K$ and consider an arbitrary partition $S = (S_i)_{i\in[d]}$ of X_n with $|S_i| = k_i$ for any $i \in [d]$. Let σ be a uniformly random permutation on X_n, then:

$$\rho_{\overline{k}}(\mathcal{D}) = \Pr[S \in \sigma(\mathcal{D})].$$

Having that and the definition of $\rho^{(d)}_{\min}(n)$, it follows that for any partition S on X_n:

$$\Pr[S \in \sigma(\mathcal{D})] \leq \rho^{(d)}_{\min}(n).$$

Let $\mathcal{Q}$ be a collection of partitions of X_n with $|\mathcal{Q}| < 1/\rho^{(d)}_{\min}(n)$. Then by the union bound:

$$\Pr[\mathcal{Q} \cap \sigma(\mathcal{D}) \neq \emptyset] \leq \sum_{Q\in\mathcal{Q}} \Pr[Q \in \sigma(\mathcal{D})] < \frac{1}{\rho^{(d)}_{\min}(n)} \cdot \rho^{(d)}_{\min}(n) = 1.$$

Thus, there is a permutation σ such that $\mathcal{Q} \cap \sigma(\mathcal{D}) = \emptyset$. Since $\sigma(\mathcal{D})$ is a d-adic set, it follows that $\mathcal{Q}$ is not a d-adic hitter. So, indeed any d-adic hitter must contain at least $1/\rho^{(d)}_{\min}(n)$ questions.

Now we shall upper bound $q^{(d)}(n)$. Construct a set $\mathcal{Q}$ of questions containing, for any $\overline{k} \in K$, $\frac{1}{\rho^{(d)}_{\min}(n)} 2n \ln n$ uniformly chosen partitions $(S_i)_{i\in[d]}$ of X_n with $|S_i| = k_i$ for any $i \in [d]$. Note that $|K| \leq (n+1)^d$ and thus $|\mathcal{Q}| \leq \frac{1}{\rho^{(d)}_{\min}(n)} 2n^{2d} \ln n$. We will show that with positive probability, $\mathcal{Q}$ is a d-adic hitter. Fix an arbitrary d-adic set $\mathcal{D}$. Let $\overline{k} \in K$ such that $\rho_{\overline{k}}(\mathcal{D}) = \rho(\mathcal{D})$. The probability that a random partition $(S_i)_{i\in[d]}$ of X_n with $|S_i| = k_i$ for all $i \in [d]$ does not belong to $\mathcal{D}$ is at most

$$1 - \rho_{\overline{k}}(\mathcal{D}) = 1 - \rho(\mathcal{D}) \leq 1 - \rho^{(d)}_{\min}(n)$$

(since $\rho(\mathcal{D}) \geq \rho^{(d)}_{\min}(n)$). Therefore the probability that $\mathcal{Q}$ is disjoint from $\mathcal{D}$ is at most

$$\left(1 - \rho^{(d)}_{\min}(n)\right)^{\frac{1}{\rho^{(d)}_{\min}(n)} 2n \ln n} \leq e^{-\rho^{(d)}_{\min}(n) \frac{1}{\rho^{(d)}_{\min}(n)} 2n \ln n} = n^{-2n}.$$

By Lemma 6.7, there are fewer than n^{2n} d-adic distributions over X_n. Having that, a union bound shows that the probability that a d-adic set $\mathcal{D}$ (corresponding to some d-adic distribution μ) which is disjoint from $\mathcal{Q}$ exists is less than 1. That is, the probability that $\mathcal{Q}$ is a d-adic hitter is positive. □

Due to this theorem, if $d = o(n/(\log n \log\log n))$, we have:

$$q^{(d)}(n) = 2^{\pm o(n)} \cdot \frac{1}{\rho^{(d)}_{\min}(n)}.$$

Hence, from now on we discuss $\rho^{(d)}_{\min}(n)$ instead of $q^{(d)}(n)$, and restrict the discussion to $d = o(n/(\log n \log\log n))$.

Before we discuss some bounds on $\rho^{(d)}_{\min}(n)$, let us define the *generalized tail* of a d-adic distribution:

Definition 6.9. Let μ be a d-adic distribution over X_n. The *generalized tail* of μ is the largest set $T \subset X_n$ such that for some $a \geq 1$:

1. $\mu(T) = d^{-a}$.
2. T does not contain zero-probability elements.
3. All elements in $X_n \backslash T$ have probability at least d^{-a} or zero.

If there are a few sets satisfying those requirements, the generalized tail is one of them, arbitrarily.

Lemma 6.10. *Suppose that μ is a non-constant d-adic distribution. Let $D = (D_j)_{j\in[d]} \in \mathrm{Div}(\mu)$ be a partition of X_n. For all $j \in [d]$, D_j either contains T or disjoint from T.*

Proof. Let $j \in [d]$. If D_j is disjoint from μ then we are done. So, Assume that $D_j \cap T \neq \emptyset$. Since all non-zero elements in $X_n \backslash T$ have probability at least d^{-a}, we can denote $\mu(D_j \cap (X_n \backslash T)) = s \cdot d^{-a}$ where $s \in \mathbb{N}$. Recall that $\mu(D_j) = 1/d$, so if we denote $\mu(D_j \cap T) = y$ we can write:

$$1/d = s \cdot d^{-a} + y.$$

Now, note that $s \leq d^{a-1} - 1$: recall that $D_j \cap T \neq \emptyset$ and thus $y > 0$. Assume towards contradiction that $s > d^{a-1} - 1$, that is, $s \geq d^{a-1}$. Then:

$$1/d = s/d^a + y \geq d^{a-1}/d^a + y = 1/d + y > 1/d$$

which is a contradiction. Having that, we lower bound y:

$$y = 1/d - s/d^a \geq 1/d - \frac{d^{a-1} - 1}{d^a} = 1/d - 1/d + 1/d^a = \mu(T),$$

and hence $\mu(D_j \cap T) = \mu(T)$, that is, $D_j \cap T = T$, and so D_j contains T completely. □

In the following sections we prove upper and lower bounds on $\rho^{(d)}_{\min}(n)$. The following function $f_d : (0, 1) \to \mathbb{R}$, defined for any $d \in \mathbb{N}$, will appear in both of our bounds:

$$f_d(\beta) = d \cdot \beta \cdot \log_2 d - \left((1 - (d-1)\beta) \log_2 \frac{1}{1 - (d-1)\beta} + (d-1)\beta \log_2 \frac{1}{\beta} \right).$$

6.3 Upper bounding $\rho^{(d)}_{\min}(n)$

The following lemma implies different upper bounds on $\rho^{(d)}_{\min}(n)$ for different sequences of n values.

Lemma 6.11. *Fix $d \in \mathbb{N}$ and $\frac{1}{d^2+1} \leq \beta \leq 1/d$. For any n of the form $n = \left\lfloor \frac{d^a}{d \cdot \beta} \right\rfloor$, where $a \in \mathbb{N}$, there exists a d-adic distribution μ over X_n which satisfies*

$$\rho(\mathrm{Div}(\mu)) \leq 2^{f_d(\beta)n + o(n)}.$$

Proof. We first assume that $\left\lfloor \frac{d^a}{d \cdot \beta} \right\rfloor = \frac{d^a}{d \cdot \beta}$. Let $n = \frac{d^a}{d \cdot \beta}$ where $a \in \mathbb{N}$. Note that $\beta n = d^{a-1}$, and construct the following d-adic distribution μ on X_n:

1. For $i \in [d \cdot \beta n - 1]$: $\mu_i = d^{-a} = \frac{1}{d \cdot d^{a-1}} = \frac{1}{d \cdot \beta n}$.
2. All other $(1 - d\beta)n + 1$ elements are a (generalized) tail of probability d^{-a}.

As we have shown, the generalized tail elements must be chosen to the same set in a partition, in order to get a partition which divides μ, thus we can think of them as a single element when constructing a partition in $\mathrm{Div}(\mu)$, such that we have $d \cdot \beta n$ elements in total, with equal probabilities. Thus, there is only one feasible type $\overline{k}$ of partition: choosing $\beta n = d^{a-1}$ elements to each set in the partition (that is, $k_i = \beta n$ for any $i \in [d]$, assuming that the tail is treated as a single element). The total probability of each set in the partition is thus $d^{a-1} \cdot d^{-a} = 1/d$. This discussion leads us to the following bound:

$$\begin{aligned}
\rho(\mathrm{Div}(\mu)) &= \rho_{\overline{k}}(\mathrm{Div}(\mu)) \\
&= \frac{\frac{(d\beta n)!}{(\beta n)!^d}}{\frac{n!}{(\beta n)!^{d-1}((1-(d-1)\beta)n)!}} \\
&\underset{(14)}{\leq} \frac{2^{d\cdot\beta n\cdot\log_2 d}}{2^{n\left((1-(d-1)\beta)\log_2\frac{1}{1-(d-1)\beta}+\sum_{i=1}^{d-1}\beta\log_2\frac{1}{\beta}\right)}/O(n^d)} \\
&= O\left(n^d\right)\cdot 2^{\left[d\cdot\beta\cdot\log_2 d-\left((1-(d-1)\beta)\log_2\frac{1}{1-(d-1)\beta}+(d-1)\beta\log_2\frac{1}{\beta}\right)\right]n} = 2^{f_d(\beta)n+o(n)}.
\end{aligned}$$

Now, assume that $\left\lfloor \frac{d^a}{d\cdot\beta} \right\rfloor < \frac{d^a}{d\cdot\beta}$. In that case, let β' such that

$$\left\lfloor \frac{d^a}{d\cdot\beta} \right\rfloor = \frac{d^a}{d\cdot\beta'}.$$

Now, construct the aforementioned d-adic distribution μ for β' instead of β. From previous arguments, we have:

$$\rho(\mathrm{Div}(\mu)) \leq 2^{f_d(\beta')n+o(n).}$$

Fortunately, this is enough: by the definition of β' and the constraint $\beta \leq 1/d$, it holds that

$$\beta \leq \beta' \leq \beta + \frac{1}{d(d^a-1)}.$$

Recall that $\beta \geq \frac{1}{d^2+1}$. This implies $d(d^a-1) = \Theta(n)$, that is

$$\beta \leq \beta' \leq \beta + \Theta(1/n).$$

Therefore, it holds that $f_d(\beta')n \leq f_d(\beta)n + O(1)$, and hence the lemma holds also for the case $\left\lfloor \frac{d^a}{d\cdot\beta} \right\rfloor < \frac{d^a}{d\cdot\beta}$. □

For n of the form $n = \left\lfloor \frac{d^a}{d\cdot\beta} \right\rfloor$, obviously $\rho^{(d)}_{\min}(n) \leq \rho(\mathrm{Div}(\mu))$, where μ is the distribution defined in the proof of Lemma 4.7. Hence for such n values we have

$$\rho^{(d)}_{\min}(n) \leq 2^{f_d(\beta)n+o(n)}.$$

6.4 Lower bounding $\rho^{(d)}_{\min}(n)$

We will use the following partition of X_n in order to lower bound $\rho(\mathrm{Div}(\mu))$ for some non-constant d-adic distribution μ:

Lemma 6.12. *Let μ be a non-constant d-adic distribution over X_n. There exists a partition of X_n of the form*

$$X_n = \bigcup_{i=1}^{\gamma}(D_i \cup E_i)$$

such that:

1. *D_i consists of elements with equal probabilities p_i.*

2. *$|D_i| = dc_i - r_i$ for some natural c_i and $0 \leq r_i < d$, and $\mu(E_i) = r_i p_i$.*

3. *$\gamma = O(\log n)$.*

Proof. We assume w.l.o.g that the elements are sorted $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$. We construct the sets D_i, E_i in iterations on i from 1 to γ. In each iteration i, assume we have ordered probabilities $\mu_{\alpha_i} \geq \mu_2 \geq \cdots \geq \mu_{N_i}$ of the available elements which were not chosen in previous iterations to D_i, E_i (initially, $\alpha_1 = 1, N_1 = n$). The elements chosen for D_i are always an interval which begins in the leftmost index α_i and up to some index β_i. The elements in E_i (if it is not empty) are always an interval which begins in some index $M_i > \beta_i$ and ends at N_i. The rest of the elements are available for the next iteration, until no elements are available and the partition is complete. The partition must be completed since $D_i \neq \emptyset$ for any i. Now let us describe an iteration i in detail. Let β_i be the last index with $\mu_{\beta_i} = \mu_{\alpha_i}$ (that is, $\mu_{\beta_i+1} < \mu_{\alpha_i}$ or $\beta_i = N_i$). Let $D_i = \{x_{\alpha_i}, \ldots, x_{\beta_i}\}$. Denote $|D_i| = dc_i - r_i$ where $c_i, r_i \in \mathbb{N}$ and $0 \leq r_i < d$. Let $M_i > \beta_i$ be an index such that $\sum_{j=M_i}^{N_i} \mu_j = r_i p_i$ if $r_i > 0$, and $M_i = \infty$ otherwise. Define $E_i = \{x_{M_i}, \ldots, x_{N_i}\}$ (if $M_i = \infty$, then $E_i = \emptyset$). We show inductively that for any i, $\sum_{j=\alpha_i}^{N_i} \mu_j$ is a multiple of $d \cdot \mu_{\alpha_i}$, and M_i exists. For the base case $\alpha_1 = 1$ and $N_1 = n$, note that $\sum_{j=1}^{n} \mu_i = 1$ which is a multiple of $d \cdot \mu_1$ since μ is non-constant. The existence of the index M_1 now follows from Lemma 6.4: Suppose that $\sum_{j=\alpha_1}^{N_1} \mu_j = k \cdot dp_1$, so by Lemma 6.4 we can partition $\{x_{\alpha_1}, \ldots, x_{N_1}\}$ to k intervals, each of probability p_1. So, M_1 is simply the first index of the interval composed from the concatenation of the last r_1 intervals, if $r_1 > 0$. For the induction step, assume that for iteration $i-1$, $\sum_{j=\alpha_{i-1}}^{N_{i-1}} \mu_j$ is a multiple of $d \cdot \mu_{\alpha_{i-1}}$ and that M_{i-1} exists. By assumption, $\sum_{j=\alpha_{i-1}}^{\beta_{i-1}} \mu_j + \sum_{j=M_{i-1}}^{N_{i-1}} \mu_j = d \cdot \mu_{\alpha_{i-1}} \cdot c_{i-1}$ for some integer c_{i-1}. When continuing to iteration i, we are removing $D_{i-1} \cup E_{i-1}$ from the available elements, and recall that $\sum_{j=\alpha_{i-1}}^{N_{i-1}} \mu_j$ is also a multiple of $d \cdot \mu_{\alpha_{i-1}}$ by assumption, and thus we still have a multiple of $d \cdot \mu_{\alpha_{i-1}}$ in the available elements of iteration i (that is, after removing $D_{i-1} \cup E_{i-1}$). Since $\mu_{\alpha_{i-1}}$ is a multiple of μ_{α_i}, we also have a multiple of $d \cdot \mu_{\alpha_i}$. The existence of the index M_i now follows from Lemma 6.4 similarly as in the base case.

It remains to show that $\gamma = O(\log n)$. Let us consider the first iteration. If the case is that $|D_1|$ is a multiple of $d \cdot \mu_1$, we change the partition a bit, and leave the last element of D_1 out, and therefore use a non-empty E_1. Now, it must hold that $\mu(E_1) \geq \mu_1$. Since the probabilities are ordered $\mu_1 \geq \cdots \geq \mu_n$ we have

$$n \cdot \mu_{M_1 - 1} \geq n \cdot \mu_{M_1} \geq \mu(E_1) \geq \mu_1,$$

that is, $\mu_{M_1-1} \geq \mu_1/n$. Since the probabilities are d-adic, there are at most $\log n + 1$ different probabilities in $\mu_2, \ldots, \mu_{M_1-1}$:

$$\mu_1/d^0, \mu_1/d^1, \mu_1/d^2, \ldots, \mu_1/d^{\log n}$$

and therefore $\gamma = O(\log n)$. □

Now we can prove the main lemma:

Lemma 6.13. *If $d = o\big(n/\log^2 n\big)$, then for every non-constant d-adic distribution μ there is $0 < \beta < 1$ such that*

$$\rho(\mathrm{Div}(\mu)) \geq 2^{f_d(\beta)n - o(n)}.$$

Proof. We will use a partition of X_n of the form

$$X_n = \bigcup_{i=1}^{\gamma}(D_i \cup E_i)$$

as constructed in Lemma 6.12. It is implied from Lemma 6.12 that $\mu(D_i \cup E_i) = d \cdot c_i \cdot p_i$ for some $c_i \in \mathbb{N}$. If $E_i \neq \emptyset$, we consider a partition of E_i into r_i subsets, each with total probability p_i. Indeed, such a partition exists by Lemma 6.4. Denote by E_i' the set of those subsets, where each subset is contracted into a single element. So, E_i' is a set of r_i elements with probability p_i each, and thus in $D_i \cup E_i'$ we have $d \cdot c_i$ elements, each with probability p_i. Denote $X_n' = \bigcup_{i=1}^{\gamma}(D_i \cup E_i')$.

Let us define a form of partition of X_n' into d subsets with equal total probabilities: for any $i \in [\gamma]$, let the sets $S_i(1), S_i(2), \ldots, S_i(d)$ be d distinct subsets of $D_i \cup E_i'$ of size c_i each. For any $j \in [d]$, define S_j by

$$S_j := \bigcup_{i=1}^{\gamma} S_i(j).$$

Indeed $S = (S_j)_{j\in[d]}$ exists in $\mathrm{Div}(\mu)$ after "unpacking" all elements in $\bigcup_{i\in[\gamma]} E_i'$ back to their original state: for any $j \in [d]$ we have

$$\mu(S_j) = \sum_{i=1}^{\gamma}\mu(S_i(j)) = \sum_{i=1}^{\gamma} c_i p_i = \frac{1}{d}\sum_{i=1}^{\gamma}\mu(D_i \cup E_i) = 1/d.$$

So, any partition $S = (S_j)_{j\in[d]}$ defined in this fashion exists in $\mathrm{Div}(\mu)$. Having that, consider the following type $\overline{k}$ of partitions which includes at least some of those partitions: let $k_j = \sum_{i=1}^{\gamma} c_i$ for any $1 \leq j \leq d-1$ and $k_d = n - (d-1)k_1$ (k_d can be thought as the size of the set that "contains the tail", as discussed in the upper bound). $\mathrm{Div}(\mu)_{\overline{k}}$ contains at least the partitions in which $S_1, \ldots, S_{d-1}$ contain only elements from $\bigcup_{i=1}^{\gamma} D_i$. So, for any $i \in [\gamma]$ we choose c_i elements from D_i to S_j, for $1 \leq j \leq d-1$. Moreover, we put all the elements of $\bigcup_{i=1}^{\gamma} E_i$ in S_d. Thus:

$$\left|\mathrm{Div}(\mu)_{\overline{k}}\right| \geq \prod_{i=1}^{\gamma} \frac{(d\cdot c_i - r_i)!}{(c_i!)^{d-1}(c_i - r_i)!}.$$

Hence:

$$\begin{aligned}
\left|\mathrm{Div}(\mu)_{\overline{k}}\right| &\geq \prod_{i=1}^{\gamma} \frac{(d\cdot c_i - d)!}{(c_i!)^{d}} \\
&\geq \prod_{i=1}^{\gamma} \frac{1}{(dc_i)^d}\frac{(d\cdot c_i)!}{(c_i!)^{d}} \\
&\geq \frac{1}{n^{d\gamma}}\prod_{i=1}^{\gamma} \frac{(d\cdot c_i)!}{(c_i!)^{d}} \\
&\underset{(14)}{\geq} \frac{1}{O(n^{2d\gamma})}\prod_{i=1}^{\gamma} 2^{c_i \cdot d\log d} \\
&\geq \frac{1}{2^{2\log_2 n \cdot o\left(\frac{n}{\log^2 n}\right)\cdot O(\log n)}}\prod_{i=1}^{\gamma} 2^{c_i\cdot d\log d} \geq 2^{d\log_2 d\sum_{i=1}^{\gamma} c_i - o(n)}.
\end{aligned}$$

Now, denote $\beta = \frac{1}{n}\sum_{i=1}^{\gamma} c_i$ and note that

$$\binom{n}{k_1, k_2, \ldots, k_d} \leq 2^{\left[(d-1)\beta \log_2 \frac{1}{\beta} + (1-(d-1)\beta)\log_2 \frac{1}{(1-(d-1)\beta)}\right] n}$$

(similarly to the discussion in the upper bound section). Therefore overall

$$\rho_{\overline{k}}(\mathrm{Div}(\mu)) \geq 2^{\left[\beta d \log_2 d - \left((d-1)\beta \log_2 \frac{1}{\beta} + (1-(d-1)\beta)\log_2 \frac{1}{(1-(d-1)\beta)}\right)\right] n - o(n)} = 2^{f_d(\beta) n - o(n)},$$

and since obviously $\rho(\mathrm{Div}(\mu)) \geq \rho_{\overline{k}}(\mathrm{Div}(\mu))$, we get the desired result. □

6.5 Estimating $q^{(d)}(n)$

Now we can deduce some explicit bounds on $q^{(d)}(n)$. Those bounds allow us to calculate $q^{(d)}(n)$ up to sub-exponential factors, for infinitely many n values. The upper bound on $q^{(d)}(n)$ will imply that even though the trivial upper bound on the cardinality of $\mathcal{Q}$ which allows constructing optimal strategies for all distributions is $d^n/d!$, the true minimal cardinality is much smaller, and in particular it is less than $2^{n+o(n)}$.

Theorem 6.14. *For any n and any $d = o\big(n/\log^2 n\big)$:*

$$q^{(d)}(n) \leq \left(1 + \frac{d-1}{d^{\frac{d}{d-1}}}\right)^{n+o(n)} = \left(2 - \Theta\left(\frac{\log d}{d}\right)\right)^{n+o(n)}.$$

Moreover, for any fixed d, the following holds for infinitely many n values:

$$q^{(d)}(n) = \left(1 + \frac{d-1}{d^{\frac{d}{d-1}}}\right)^{n\pm o(n)} = \left(2 - \Theta\left(\frac{\log d}{d}\right)\right)^{n\pm o(n)}.$$

Proof. Since Lemma 6.13 holds for any d-adic distribution μ where $d = o\big(n/\log^2 n\big)$, we can deduce the lower bound

$$\rho_{\min}^{(d)}(n) \geq \exp_2\left(\left(\min_{0<\beta<1} f_d(\beta)\right) n - o(n)\right).$$

Calculation shows that

$$f_d'(\beta) = (d-1)\log_2 \frac{\beta}{(1-(d-1)\beta)} + d\log_2 d$$

and the minimum is attained at

$$\beta = \frac{1}{d^{\frac{d}{d-1}} - 1 + d}.$$

We are interested in what happens when β minimizes f_d. So, we want to estimate the following function of d:

$$f(d) = f_d\left(\frac{1}{d^{\frac{d}{d-1}} - 1 + d}\right).$$

After some algebraic simplifications, we get:

$$f(d) = \log_2\left(\frac{d^{\frac{d}{d-1}}}{d^{\frac{d}{d-1}} + d - 1}\right).$$

Since $d = o(n/\log n \log\log n)$, the reduction in Theorem 6.8 allows us to calculate $\exp_2(-f(d))$ in order to get an estimate of $q^{(d)}(n)$: we have

$$\exp_2(-f(d)) = \frac{d^{\frac{d}{d-1}} + d - 1}{d^{\frac{d}{d-1}}} = 1 + \frac{d-1}{d^{\frac{d}{d-1}}},$$

which implies

$$q^{(d)}(n) \leq \left(1 + \frac{d-1}{d^{\frac{d}{d-1}}}\right)^{n+o(n)}.$$

Moreover, it holds that:

$$\frac{d-1}{d^{\frac{d}{d-1}}} = \Theta\Big(d^{1-\frac{d}{d-1}}\Big) = \Theta\Big(d^{-\frac{1}{d-1}}\Big).$$

Calculating the Puiseux expansion of $d^{-\frac{1}{d-1}}$ shows that $d^{-\frac{1}{d-1}} = 1 - \Theta\Big(\frac{\log d}{d}\Big)$ and hence:

$$q^{(d)}(n) \leq \exp_2(-f(d)n + o(n)) = \left(2 - \Theta\left(\frac{\log d}{d}\right)\right)^{n+o(n)}.$$

For the second part of the theorem, assume that d is fixed, let $\beta = \frac{1}{d^{\frac{d}{d-1}} - 1 + d}$ and suppose that $n = \left\lfloor \frac{d^a}{d \cdot \beta} \right\rfloor$ where $a \in \mathbb{N}$. Note that $\frac{1}{d^2+1} \leq \frac{1}{d^{\frac{d}{d-1}} - 1 + d} \leq 1/d$, so we can use Lemma 6.11 and deduce

$$\rho^{(d)}_{\min}(n) \leq \exp_2(f_d(\beta)n + o(n)) = \exp_2(f(d)n + o(n)) = \left(\frac{d^{\frac{d}{d-1}}}{d^{\frac{d}{d-1}} + d - 1}\right)^{n+o(n)},$$

and hence

$$q^{(d)}(n) \geq \left(1 + \frac{d-1}{d^{\frac{d}{d-1}}}\right)^{n-o(n)} = \left(2 - \Theta\left(\frac{\log d}{d}\right)\right)^{n-o(n)}. \qquad \square$$

7 Open questions

Our work suggests a few open questions which we think are interesting enough for future research.

Open Question 1. *Is G continuous?*

Notes It seems that techniques similar to those used in Section 4 can show continuity-related results, but additional work seems necessary in order to determine whether G is continuous. First, it seems not hard to show that G is upper semi-continuous. Moreover, denote by G_b the function G restricted to some fixed b, such that $G(\beta) = \inf_{b \in \mathbb{N}} G_b(\beta)$. It also seems not hard to show that G_b is continuous. We should use a fixed b since otherwise Lemma 4.11 is not helpful. It is not clear, however, whether G is continuous as well. If we could show that G is lower semi-continuous, or that b can be chosen over some compact subset of $\mathbb{N}$ instead of the entirety of $\mathbb{N}$, then continuity of G would follow.

Open Question 2. *Is the outer infimum in G attained?*

Notes We have shown that the inner supremum in the definition of G is attained and thus can be written as maximum. It is not clear, however, whether the outer infimum is attained as well. Unfortunately, even if we assume that b is fixed, we still can not apply a similar

argument to the one used in the supremum case: Say we have a fixed $b \in \mathbb{N}$ and a sequence of sequences $\left(\boldsymbol{c}^j\right)_{j\in\mathbb{N}} \in \mathcal{C}$ converging to the infimum, and converging pointwise to a sequence $\boldsymbol{c}$. It does not guarantee (not immediately, at least) that $\left(\boldsymbol{c}^j\right)_{j\in\mathbb{N}}$ converges to $\boldsymbol{c}$ in ℓ_1-norm, and that property is crucial for $\boldsymbol{c}$ being a minimizing sequence for $\max_{\boldsymbol{\alpha}\in\mathcal{A}} P(\boldsymbol{c}, \boldsymbol{\alpha})$ across all sequences in $\mathcal{C}$.

Open Question 3. *Can we calculate $G(\beta)$?*

Notes While our formula for G implies $G(\beta) \leq -0.305758$ for any $1 \leq \beta < 2$, it would be interesting to calculate $G(\beta)$ in terms of β, similarly to the calculation suggested in [DFGM19] for $\beta = 1.25$, that is $G(1.25) = -\log 1.25$. This will allow us to calculate $q(n)$ for n of the form $n = \beta 2^k$, up to sub-exponential factors.

Open Question 4. *Can we generalize the function $G\colon [1,2) \to \mathbb{R}$ to a function $G^{(d)}\colon [1,d) \to \mathbb{R}$ such that $\rho^{(d)}_{\min}(n) = 2^{G^{(d)}(\beta)n \pm o(n)}$?*

References

[ACD13] Harout Aydinian, Ferdinando Cicalese, and Christian Deppe, editors. *Information Theory, Combinatorics, and Search Theory*. Springer-Verlag Berlin Heidelberg, 2013.

[AW87] Rudolf Ahlswede and Ingo Wegener. *Search problems*. John Wiley & Sons, Inc., New York, 1987.

[CAL94] David Cohn, Les Atlas, and Richard Ladner. Improving generalization with active learning. *Machine learning*, 15(2):201–221, 1994.

[CS04] Imre Csiszár and Paul C Shields. *Information theory and statistics: A tutorial*. Now Publishers Inc, 2004.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, USA, 2006.

[DFGM17] Yuval Dagan, Yuval Filmus, Ariel Gabizon, and Shay Moran. Twenty (simple) questions. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 9–21, 2017.

[DFGM19] Yuval Dagan, Yuval Filmus, Ariel Gabizon, and Shay Moran. Twenty (short) questions. *Combinatorica*, 39(3):597–626, 2019.

[Dor43] Robert Dorfman. The detection of defective members of large populations. *The Annals of Mathematical Statistics*, 14(4):436–440, 1943.

[DS01] Dwight Duffus and Bill Sands. Minimum sized fibres in distributive lattices. *J. Aust. Math. Soc.*, 70(3):337–350, 2001.

[DSW90] D. Duffus, B. Sands, and P. Winkler. Maximal chains and antichains in Boolean lattices. *SIAM J. Discrete Math.*, 3(2):197–205, 1990.

[Huf52] David A. Huffman. A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, 40(9):1098–1101, 1952.

[Kat73] Gyula O. H. Katona. Combinatorial search problems. In J. N. Srivastava et al., editor, *A Survery of Combinatorial Theory*. North-Holland Publishing Company, 1973.

[LR87] Zbigniew Lonc and Ivan Rival. Chains, antichains, and fibres. *J. Combin. Theory Ser. A*, 44(2):207–228, 1987.

[Sha48] Claude E Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[You12] Neal Young. Reverse Chernoff bound. Theoretical Computer Science Stack Exchange, 2012. URL:https://cstheory.stackexchange.com/q/14476 (version: 2012-11-26).

[Zim59] Seth Zimmerman. An optimal search procedure. *Amer. Math. Monthly*, 66:690–693, 1959.