Twenty (simple) questions

Yuval Dagan, Yuval Filmus, Ariel Gabizon, and Shay Moran

March 15, 2017

Abstract

A basic combinatorial interpretation of Shannon's entropy function is via the "20 questions" game. This cooperative game is played by two players, Alice and Bob: Alice picks a distribution π over the numbers $\{1, \ldots, n\}$, and announces it to Bob. She then chooses a number x according to π, and Bob attempts to identify x using as few Yes/No queries as possible, on average.

An optimal strategy for the "20 questions" game is given by a Huffman code for π: Bob's questions reveal the codeword for x bit by bit. This strategy finds x using fewer than $H(\pi) + 1$ questions on average. However, the questions asked by Bob could be arbitrary. In this paper, we investigate the following question: *Are there restricted sets of questions that match the performance of Huffman codes, either exactly or approximately?*

Our first main result shows that for every distribution π, Bob has a strategy that uses only questions of the form "$x < c$?" and "$x = c$?", and uncovers x using at most $H(\pi) + 1$ questions on average, matching the performance of Huffman codes in this sense. We also give a natural set of $O(rn^{1/r})$ questions that achieve a performance of at most $H(\pi) + r$, and show that $\Omega(rn^{1/r})$ questions are required to achieve such a guarantee.

Our second main result gives a set $\mathcal{Q}$ of $1.25^{n+o(n)}$ questions such that for every distribution π, Bob can implement an *optimal* strategy for π using only questions from $\mathcal{Q}$. We also show that $1.25^{n-o(n)}$ questions are needed, for infinitely many n. If we allow a small slack of r over the optimal strategy, then roughly $(rn)^{\Theta(1/r)}$ questions are necessary and sufficient.

Contents

1 Introduction

A basic combinatorial and operational interpretation of Shannon's entropy function, which is often taught in introductory courses on information theory, is via the "20 questions" game (see for example the well-known textbook [CT06]). This game is played between two players, Alice and Bob: Alice picks a distribution π over a (finite) set of objects X, and announces it to Bob. Alice then chooses an object x according to π, and Bob attempts to identify the object using as few Yes/No queries as possible, on average.[1]

The "20 questions" game is the simplest model of *combinatorial search theory* [AW87] and of *combinatorial group testing* [Dor43]. It also has a natural interpretation in the context of *interactive learning* [CAL94]: Bob wishes to learn the secret x, and may interact with the environment (Alice) by querying features of x.

What questions should Bob ask? An optimal strategy for Bob is to compute a Huffman code for π, and then follow the corresponding decision tree: his first query, for example, asks whether x lies in the left subtree of the root. While this strategy minimizes the expected number of queries, the queries themselves could be arbitrarily complex; already for the first question, Huffman's algorithm draws from an exponentially large reservoir of potential queries (see Theorem 7.3 for more details).

Therefore, it is natural to consider variants of this game in which the set of queries used is restricted; for example, it is plausible that Alice and Bob would prefer to use queries that (i) can be communicated efficiently (using as few bits as possible), and (ii) can be tested efficiently (i.e. there is an efficient encoding scheme for elements of X and a fast algorithm that given $x \in X$ and a query q as input, determines whether x satisfies the query q).

We summarize this with the following meta-question, which guides this work:

Main question

Are there "nice" sets of queries $\mathcal{Q}$ such that for any distribution, there is a "high quality" strategy that uses only queries from $\mathcal{Q}$?

Formalizing this question depends on how "nice" and "high quality" are quantified.

Variants of this question, which focus on specific sets of queries, are commonplace in computer science and related fields. Here are just a few examples:

- Binary decision trees, as used in statistics, machine learning, pattern recognition, data mining, and complexity theory, identify X as a subset of $\{0,1\}^n$, and allow only queries of the form "$x_i = 1$?".
- Feature selection and generation in machine learning can naturally be interpreted as the task of finding queries that reveal a lot of information about the learned concept.
- In the setting of binary search trees, X is a linearly ordered set, and the set of queries $\mathcal{Q}$ is the set of comparison queries, "$x < c$, $x = c$, or $x > c$?".[2]

[1] Another basic interpretation of Shannon's entropy function is via the transmission problem, in which Alice wishes to transmit to Bob a message x drawn from a distribution π over X, over a noiseless binary channel, using as few bits as possible on average. While the entropy captures the complexity of both problems, the two problems differ in the sense that in the "20 questions" game, Alice is "passive": she only answers the queries posed by Bob, but she does not help him by "actively" transmitting him the secret x, as she does in the transmission problem.

[2] A comparison query has three possible answers: "$<$", "$=$", and "$>$", and so in this setting it is more natural to consider the variant of the "20 questions" game in which three answers are allowed.

- In the setting of comparison-based sorting algorithms, X is the set of permutations or linear orders over an array $x_1, \ldots, x_n$, and $\mathcal{Q}$ contains queries of the form "$x_i < x_j$?".
- Algebraic decision trees, used in computational geometry and studied in complexity theory, identify $X = \mathbb{F}^n$ for some field $\mathbb{F}$, and allow queries of the form "$P(\vec{x}) = 0$?" (or "$P(\vec{x}) \geq 0$?" when $\mathbb{F}$ is an ordered field) for low-degree polynomials.
- Searching in posets generalizes binary search trees by allowing X to be an arbitrary poset (usually a rooted tree). The set of queries $\mathcal{Q}$ is the set of comparison queries of the form "$x \prec c$?".

We consider two different benchmarks for sets of queries:

1. **An information-theoretical benchmark**: A set of queries $\mathcal{Q}$ has *redundancy* r if for every distribution π there is a strategy using only queries from $\mathcal{Q}$ that finds x with at most $H(\pi)+r$ queries on average when x is drawn according to π.
2. **A combinatorial benchmark**: A set of queries $\mathcal{Q}$ is *r-optimal* (or has *prolixity* r) if for every distribution π there is a strategy using queries from $\mathcal{Q}$ that finds x with at most $\mathrm{Opt}(\pi) + r$ queries on average when x is drawn according to π, where $\mathrm{Opt}(\pi)$ is the expected number of queries asked by an optimal strategy for π (e.g. a Huffman tree).

Given a certain redundancy or prolixity, we will be interested in sets of questions achieving that performance that (i) are as small as possible, and (ii) allow efficient construction of high quality strategies which achieve the target performance. In some cases we will have to settle for only one of these properties.

Information-theoretical benchmark. Let π be a distribution over X. A basic result in information theory is that every algorithm that reveals an unknown element x drawn according to π (in short, $x \sim \pi$) using Yes/No questions must make at least $H(\pi)$ queries on average. Moreover, there are algorithms that make at most $H(\pi) + 1$ queries on average, such as Huffman coding and Shannon–Fano coding. However, these algorithms may potentially use arbitrary queries.

Are there restricted sets of queries that match the performance of $H(\pi) + 1$ queries on average, for every distribution π? Consider the setting in which X is linearly ordered (say $X = [n]$, with its natural ordering: $1 < \cdots < n$). Gilbert and Moore [GM59], in a result that paved the way to arithmetic coding, showed that two-way comparison queries ("$x < c$?") almost fit the bill: they achieve a performance of at most $H(\pi) + 2$ queries on average. Our first main result shows that the optimal performance of $H(\pi) + 1$ can be achieved by allowing also equality queries ("$x = c$?"):

Theorem (restatement of Theorem 5.1 and Theorem 5.2)**.** *For every distribution π there is a strategy that uses only comparison and equality queries which finds x drawn from π with at most $H(\pi) + 1$ queries on average. Moreover, this strategy can be computed in time $O(n \log n)$.*

In a sense, this result gives an affirmative answer to our main question above. The set of comparison and equality queries (first suggested by Spuler [Spu94a]) arguably qualifies as "nice": linearly ordered universes appear in many natural and practical settings (numbers, dates, names, IDs) in which comparison and equality queries can be implemented efficiently. Moreover, from a communication complexity perspective, Bob can communicate a comparison/equality query using just $\log_2 n + 1$ bits (since there are just $2n$ such queries). This is an exponential improvement over the $\Omega(n)$ bits he would need to communicate had he used Huffman coding.

We extend this result to the case where X is a set of vectors of length r, $\vec{x} = (x_1, \ldots, x_r)$, by showing that there is a strategy using entry-wise comparisons ("$x_i < c$?") and entry-wise equalities ("$x_i = c$?") that achieves redundancy r:

Theorem (restatement of Theorem 6.1)**.** *Let X be the set of vectors of length r over a linearly ordered universe. For every distribution π there is a strategy that uses only entry-wise comparison queries and entry-wise equality queries and finds $\vec{x} \sim \pi$ with at most $H(\pi) + r$ queries. Moreover, this strategy can be computed in time $O(|X| \log |X|)$.*

This shows that in settings that involve lists or vectors, entry-wise comparison and equality queries achieve redundancy that is equal to the length of the vectors. The theorem is proved by applying the algorithm of the preceding theorem to uncover the vector $\vec{x}$ entry by entry.

As a toy example, imagine that we wish to maintain a data structure that supports an operation *find*$(\vec{x})$, where each x is represented by a list $(x_1, \ldots, x_r)$ of r numbers (think of r as small, say $r = 9$ and the $\vec{x}$'s denote Social Security Numbers). Moreover, assume that we have a good prior estimate on $\pi(x)$ — the frequency of *find*(x) operations (derived from past experience, perhaps even in an online fashion). The above corollary shows how to achieve an amortized cost of $H(\pi)+r$ per *find*$(\vec{x})$ operation, accessing the input only via queries of the form "$x_i < c$?" and "$x_i = c$?".

As a corollary, we are able to determine almost exactly the minimum size of a set of queries that achieves redundancy $r \geq 1$. In more detail, let $u^H(n, r)$ denote the minimum size of a set of queries $\mathcal{Q}$ such that for every distribution π on $[n]$ there is a strategy using only queries from $\mathcal{Q}$ that finds x with at most $H(\pi) + r$ queries on average, when x is drawn according to π.

Corollary (Theorem 6.1)**.** *For every $n, r \in \mathbb{N}$,*

$$\frac{1}{e} r n^{1/r} \leq u^H(n, r) \leq 2 r n^{1/r}.$$

Obtaining this tight estimate of $u^H(n, r) = \Theta(r n^{1/r})$ hinges on adding equality queries; had we used only entry-wise comparison queries and the Gilbert–Moore algorithm instead, the resulting upper bound would have been $u^H(n, r) = O\big(r n^{2/r}\big)$, which is quadratically worse than the truth.

Combinatorial benchmark. The analytical properties of the entropy function make $H(\pi)$ a standard benchmark for the average number of bits needed to describe an element x drawn from a known distribution π, and so it is natural to use it as a benchmark for the average number of queries needed to find x when it is drawn according to π. However, there is a conceptually simpler, and arguably more natural, benchmark: $\mathrm{Opt}(\pi)$ — the average number of queries that are used by a best strategy for π (several might exist), such as one generated by Huffman's algorithm.

Can the optimal performance of Huffman codes be matched *exactly*? Can it be achieved without using all possible queries? Our second main result answers this in the affirmative:

Theorem (restatement of Theorem 7.2 and Theorem 7.3)**.** *For every n there is a set $\mathcal{Q}$ of $1.25^{n+o(n)}$ queries such that for every distribution over $[n]$, there is a strategy using only queries from $\mathcal{Q}$ which matches the performance of the optimal (unrestricted) strategy* exactly*. Furthermore, for infinitely many n, at least $1.25^{n-o(n)}$ queries are required to achieve this feat.*

Consider a setting (similar to the one analyzed in [AM01, WAF01]) in which Alice (the client) holds an element x coming from a domain of size n, and Bob (the server) tries to determine it. Bob (who has collected statistics on Alice) knows the distribution π of x, but Alice does not. Furthermore, the downlink channel from Bob to Alice is much cheaper than the uplink channel in

the opposite direction. If Bob's goal is to minimize the amount of information that Alice sends him, he can use a Huffman code to have her send the minimum amount of information on average, namely $\mathrm{Opt}(\pi)$. Naively representing a question as an arbitrary subset of $[n]$, Bob has to send $\mathrm{Opt}(\pi) \cdot n$ bits on average to Alice. Our theorem allows him to cut that amount by a factor of $\log 2 / \log 1.25 \approx 3.1$, since it only takes $\log_2 1.25^n$ bits to specify a question from $\mathcal{Q}$.

One drawback of our construction is that it is randomized. Thus, we do not consider it particularly "efficient" nor "natural". It is interesting to find an explicit set $\mathcal{Q}$ that achieves this bound (see Section 10.2 for more details). Our best explicit construction is:

Theorem (restatement of Theorem 7.5)**.** *For every n there is an explicit set $\mathcal{Q}$ of $O(2^{n/2})$ queries such that for every distribution over $[n]$, there is a strategy using only queries from $\mathcal{Q}$ which matches the performance of the optimal (unrestricted) strategy* exactly*. Moreover, we can compute this strategy in time $O(n^2)$.*

It is natural to ask in this setting how small can a set of queries be if it is *r-optimal*; that is, if it uses at most $\mathrm{Opt}(\pi) + r$ questions on average when the secret element is drawn according to π, for small $r > 0$. Let $u^{\mathrm{Opt}}(n, r)$ denote the minimum size of a set of queries $\mathcal{Q}$ such that for every distribution π on $[n]$ there is a strategy using only queries from $\mathcal{Q}$ that finds x with at most $\mathrm{Opt}(\pi)+r$ queries on average when x is drawn from π. We show that for any fixed $r > 0$, significant savings can be achieved:

Theorem (restatement of Theorem 8.1)**.** *For all $r \in (0, 1)$:*

$$(r \cdot n)^{\frac{1}{4r}} \lesssim u^{\mathrm{Opt}}(n, r) \lesssim (r \cdot n)^{\frac{16}{r}}.$$

Instead of the exponential number of questions needed to match Huffman's algorithm exactly, for fixed $r > 0$ an r-optimal set of questions has polynomial size. In this case the upper bound is achieved by an explicit set of queries $\mathcal{Q}_r$. We also present an efficient randomized algorithm for computing an r-optimal strategy that uses queries from $\mathcal{Q}_r$.

Spread-out distributions. Before closing this introduction, let us go back to the information-theoretical benchmark. We mentioned that the best performance that can be achieved is $H(\pi)+1$. This is due to distributions in which one element has probability $1 - \epsilon$: such distributions have very small entropy, but require at least one question to disambiguate the probable element form the rest.

When we rule out such distributions, by requiring all probabilities to be small, the best achievable performance improves to $H(\pi) + 0.086$, a classical result of Gallager [Gal78]. Comparison and equality queries also benefit from such a promise:

Theorem (informal restatement of Theorem 9.1)**.** *For every distribution π over $[n]$ in which all elements have low probability there is a strategy that uses only comparison and equality queries and finds x drawn from π with at most $H(\pi) + 0.586$ queries on average.*

There are distributions π, in which all elements have low probability, that require $H(\pi)+0.5011$ comparison and equality queries on average to find x drawn from π.

Comparison and equality queries thus no longer match the optimal performance in this setting, but they do take advantage of it. The algorithm used to construct the strategy mentioned in the theorem is very different from the one used to achieve $H(\pi)+1$, and therefore may be of independent interest.

Organization of the paper We provide a more complete summary of the paper in Section 2, followed by a brief literature review in Section 3. Several basic definitions are listed in Section 4, and the main body of the paper (Sections 5–9) follows (see Section 2 for more details). The paper concludes in Section 10 with an extensive list of open questions.

2 Paper outline

In this section we outline our results in more detail, and give some idea about their proofs. We also indicate the contents of the various technical sections (Sections 5–9).

We start with a few formal definitions:

Definition. Let $X_n = \{x_1, \ldots, x_n\}$. We think of X_n as linearly ordered: $x_1 \prec x_2 \prec \cdots \prec x_n$.

Consider the following game: Alice picks an element $x \in X_n$, which we call the *secret element* as it is unknown to Bob, and Bob asks Yes/No (binary) questions about x, one after the other, until x is revealed. Each question is of the form "$x \in A$?" for some subset $A \subseteq X_n$.

Bob's strategy can be modeled using a *decision tree*, which is a rooted binary tree in which each internal vertex (including the root) is labeled by a *question* (a subset of X_n), the two outgoing edges are labeled *Yes* and *No*, and each leaf is labeled by an element of X_n. A decision tree corresponds to a strategy for Bob: he starts by asking the question at the root, and continues recursively to one of its children according to the answer. When reaching a leaf, the secret element is revealed to be the leaf's label. Thus, in order for a tree to be valid, the label of each leaf must be the only element in X_n which is consistent with the answers to all questions on the way. If a decision tree uses only questions from $\mathcal{Q} \subseteq 2^{X_n}$, we call it a decision tree *using* $\mathcal{Q}$.

Alice picks the element x from a distribution $\pi = (\pi_1, \ldots, \pi_n)$, where $\pi_i = \Pr_{x \sim \pi}[x = x_i]$. Bob knows π, and he has to identify x among all elements in the support of π. Thus, a *decision tree for* π is defined as a decision tree for $\mathrm{supp}(\pi)$. The *cost* of such a tree is the average number of questions asked on a random element $x \sim \pi$. We denote the cost of the optimal unrestricted decision tree for π by $\mathrm{Opt}(\pi)$.

Given a distribution π, its binary entropy is defined by $H(\pi) = \sum_{i=1}^{n} \pi_i \log_2 \frac{1}{\pi_i}$. The binary entropy function is denoted $h(p) = p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p}$ for $0 \leq p \leq 1$. A classical inequality due to Shannon [Sha48] states that

$$H(\pi) \leq \mathrm{Opt}(\pi) < H(\pi) + 1.$$

We say that a set of questions $\mathcal{Q}$ has *redundancy* r if for every distribution π there exists a decision tree using $\mathcal{Q}$ whose cost is at most $H(\pi) + r$. We say that it has *prolixity* r if for every distribution π there exists a decision tree using $\mathcal{Q}$ whose cost is at most $\mathrm{Opt}(\pi) + r$.

We will be particularly interested in the following sets of questions:

- Equality queries: questions of the form "$x = x_i$?" for $i \in \{1, \ldots, n\}$.
- Comparison queries: questions of the form "$x \prec x_i$?" for $i \in \{2, \ldots, n\}$.
- Interval queries: questions of the form "$x_i \preceq x \preceq x_j$?" for $1 \leq i \leq j \leq n$.

Section organization. Our results on comparison and equality queries are described in Subsection 2.1, which covers Sections 5,6,9. Our results on sets of questions that match the performance of Huffman codes exactly are described in Subsection 2.2, which covers Section 7. Our results on sets of question that achieve small prolixity are described in Subsection 2.3, which covers Section 8.

2.1 Comparison and equality queries

2.1.1 Achieving redundancy 1

Huffman codes achieve redundancy 1. Are there small sets of questions which also achieve redundancy 1? A natural candidate is the set of comparison queries, which gives rise to a class of decision trees known as *alphabetic trees* (for the difference between these and binary search trees, see Section 3.1.2). However, for some distributions comparison queries cannot achieve redundancy smaller than 2: the distribution $(\epsilon, 1-2\epsilon, \epsilon)$ requires two comparison queries to identify the central element, but has entropy $O(\epsilon \log(1/\epsilon))$, which goes to 0 with ϵ.

The only way to achieve redundancy 1 on this kind of distribution is to also allow equality queries. The resulting class of decision trees, first suggested by Spuler [Spu94a, Spu94b], is known as *two-way comparison search trees* or *binary comparison search trees*. To the best of our knowledge, the redundancy of two-way comparison search trees has not been considered before. We show:

Theorem (restatement of Theorem 5.1)**.** *Comparison and equality queries achieve redundancy* 1*.*

Our proof is constructive: given a distribution π, we show how to construct efficiently a decision tree using comparison and equality queries whose cost is at most $H(\pi) + 1$. Our construction is based on the weight balancing algorithm of Rissanen [Ris73], which uses only comparison queries:

> **Weight balancing algorithm**
> Given a probability distribution π, ask a comparison query minimizing $|\Pr[\text{Yes}] - \Pr[\text{No}]|$, and recurse on the distribution of π conditioned on the answer. Stop when the secret element is revealed.

Horibe [Hor77] showed that this algorithm achieves redundancy 2. Given the additional power of asking equality queries, it is natural to ask such queries when some element has large probability. Indeed, this is exactly what our algorithm does:

> **Weight balancing algorithm with equality queries**
> If the most probable element has probability at least 0.3, compare it to the secret element, and recurse if the answer is negative.
> Otherwise, ask a comparison query minimizing $|\Pr[\text{Yes}] - \Pr[\text{No}]|$, and recurse on the answer.

The constant 0.3 here is just one of the possible values for which this algorithm achieves redundancy 1.

Our analysis of the redundancy in the proof of Theorem 5.1 depends on $\pi_{\max}$, the probability of the most probable element in the distribution π. It proceeds by first showing that if $\pi_{\max} \geq 0.3$ then the redundancy is at most 1, and then recursively reducing the case in which $\pi_{\max} < 0.3$ to the case $\pi_{\max} \geq 0.3$ via a careful analysis of how $\pi_{\max}$ (that now refers to the most probable element in the recursively defined conditional distribution) varies according to the answers that the algorithm receives.

2.1.2 Higher redundancy

The weight balancing algorithms assume that the domain of π is linearly ordered. Another natural setting is when the domain is Y^r, where Y is a linearly ordered set of size $n^{1/r}$. In other words, each element of X is a vector of length r, and the secret element is a vector $\vec{x} = (x^{(1)}, \ldots, x^{(r)})$.

A corollary to Theorem 5.1 is that in this setting, the set of all queries of the form "Is $x^{(i)}$ at most y?" and "Does $x^{(i)}$ equal y?", for $1 \le i \le r$ and $y \in Y$, achieves redundancy at most r.

Indeed, suppose that x is drawn according to a probability distribution π with components $\pi^{(1)}, \dots, \pi^{(r)}$. If we determine the components $x^{(1)}, \dots, x^{(r)}$ consecutively using the weight balancing algorithm with equality queries, we obtain a decision tree whose cost is at most

$$[H(\pi^{(1)}) + 1] + [H(\pi^{(2)}|\pi^{(1)}) + 1] + \cdots + [H(\pi^{(r)}|\pi^{(1)}, \dots, \pi^{(r-1)}) + 1] = H(\pi) + r.$$

Since the number of questions is roughly $rn^{1/r}$, this proves the first part of the following theorem:

Theorem (restatement of Theorem 6.1)**.** *There is a set of $O(rn^{1/r})$ questions that achieve redundancy r.*

Moreover, $\Omega(rn^{1/r})$ questions are required to achieve redundancy r.

The other direction is proved by considering distributions almost concentrated on a single element: a set of questions $\mathcal{Q}$ can have redundancy r only if it identifies any single element using at most r questions, and this shows that $2^r \binom{|\mathcal{Q}|}{\le r} \ge n$, implying the lower bound in the theorem.

Section 6.3 slightly improves this lower bound via a connection with *witness codes*, which are sets of vectors in $\{0,1\}^m$ in which each vector is identifiable using at most r coordinates.

2.1.3 Spread-out distributions

Theorem 5.1 shows that comparison and equality queries achieve redundancy 1. Although this is the best redundancy achievable, the only distributions which require this redundancy are those which are almost entirely concentrated on a single element. Can we obtain a better bound if this is not the case? More concretely, what redundancy is achievable when the distribution has high *min-entropy*, that is, when all elements have small probability?

To make this question precise, let r_p be the maximal redundancy of comparison and equality queries on distributions in which the maximal probability is at most p (on an arbitrarily large domain), and let $r_0 = \lim_{p \to 0} r_p$. We show:

Theorem (restatement of Theorem 9.1)**.** *The quantity r_0 is bounded by*

$$0.5011 < r_0 < 0.586.$$

The lower bound is attained by distributions of roughly the form $\epsilon, 1/n, \epsilon, 1/n, \dots, \epsilon, 1/n, \epsilon$ for $n \approx \frac{3}{\log_2 e} \cdot 2^k$, where k is a large integer. The upper bound is proved by modifying another algorithm achieving redundancy 2 using only comparison queries: the Gilbert–Moore algorithm [GM59], also known as Shannon–Fano–Elias encoding, which forms the basis of arithmetic encoding. Before describing our upper bound, we first explain this algorithm and why it achieves redundancy 2.

Given a distribution π on X_n in which x_i has probability π_i, the Gilbert–Moore algorithm proceeds as follows:

Gilbert–Moore algorithm

Partition $[0,1]$ into segments $T_1, \dots, T_n$ of lengths $\pi_1, \dots, \pi_n$, where T_{i+1} is placed to the right of T_i. Put a point p_i at the middle of T_i for all i. Intuitively speaking, we now perform binary search on $[0,1]$ to reveal the point p_i corresponding to the secret element.

Formally, we maintain an interval $I = [a,b]$, initialized at $[0,1]$. At every iteration we ask whether the secret element resides to the left or to the right of $\frac{a+b}{2}$, and update I accordingly, decreasing its length by a half (exactly). We stop once I contains only one point.

A simple argument shows that x_i is isolated after at most $\lceil \log_2 \frac{2}{\pi_i} \rceil < \log_2 \frac{1}{\pi_i} + 2$ steps, and so the Gilbert–Moore algorithm has redundancy 2. Indeed, after $\lceil \log_2 \frac{2}{\pi_i} \rceil$ steps, the binary search focuses on an interval containing p_i whose length is at most $\pi_i/2$ and is thus contained entirely inside T_i.

The choice of π_i as the length of T_i isn't optimal. A better choice is $2^{-\ell_i}$, where ℓ_i is the length of the codeword for x_i in a Huffman code for π. The same argument as before shows that x_i is isolated after at most $\ell_i + 1$ steps, and so the modified algorithm has cost at most $\mathrm{Opt}(\pi) + 1 < H(\pi) + 2$. This algorithm appears in Nakatsu [Nak91].

How can we use equality queries to improve on this algorithm? As in the modified weight balancing algorithm, the idea is to use equality queries to handle elements whose weight is large. However, the exact mechanism is rather different:

Random placement algorithm with interval queries

Partition $[0, 1]$ into segments $T_1, \ldots, T_n$ of length $2^{-\ell_1}, \ldots, 2^{-\ell_n}$, where $\ell_1, \ldots, \ell_n$ are defined as explained above, and put a point p_i at the middle of T_i. Then rotate the entire setup by a random amount.

Perform "modified binary search" on $[0, 1]$:

- If the current interval J contains a segment T_i of size $|J|/2$ in its entirety, ask whether $x = x_i$, and if the answer is negative, remove T_i from J.
- Otherwise, perform one step of binary search on J, as described in the Gilbert–Moore algorithm.

In both cases, the size of J exactly halves at each iteration of the modified binary search. The same argument as before shows that x_i is always isolated after at most $\ell_i + 1$ steps. After $\ell_i - 1$ steps, J is an interval of length $2 \cdot 2^{-\ell_i} = 2|T_i|$ containing p_i, and it contains all of T_i with probability $1/2$; in this case, x_i is isolated after only ℓ_i steps. The resulting algorithm has cost at most $\mathrm{Opt}(\pi) + 1/2$ (Theorem 9.3). However, since we rotated the entire setup, interval queries are needed to implement the binary search.

In order to obtain an algorithm which uses comparison queries rather than interval queries (in addition to equality queries), we need to constrain the rotation somehow. Reflecting on the argument above, we see that if all segments have length at most $2^{-\ell}$ then it suffices to randomly "slide" the setup across an interval of free space of length $2 \cdot 2^{-\ell}$. This leads to the following algorithm, in which $\ell = \min(\ell_1, \ldots, \ell_n)$:

Random placement algorithm with comparison queries

Partition $[0, 1]$ into segments $T_1, \ldots, T_n$ of length $2^{-\ell_1}, \ldots, 2^{-\ell_n}$. Choose a random set of intervals of total length $4 \cdot 2^{-\ell}$, and halve their lengths while keeping all intervals adjacent to each other, thus forming a slack of length $2 \cdot 2^{-\ell}$ at the right end of $[0, 1]$. Put a point p_i at the middle of I_i, and shift the entire setup to the right by a random amount chosen from $[0, 2 \cdot 2^{-\ell}]$.

Perform modified binary search as in the preceding algorithm.

Essentially the same analysis as before shows that this algorithm, which now uses only comparison and equality queries, has cost at most $\mathrm{Opt}(\pi) + 1/2 + 4 \cdot 2^{-\ell}$ (Lemma 9.3.1).

As the maximal probability $\pi_{\max}$ tends to zero, the length ℓ of the minimal codeword tends to infinity, and thus the cost is bounded by $\mathrm{Opt}(\pi) + 1/2$ in the limit. A classical result of Gallager [Gal78] states that $\mathrm{Opt}(\pi) \leq H(\pi) + 0.0861 + \pi_{\max}$, and so we obtain the bound $r_0 < 0.586$.

2.2 Optimal sets of questions of minimal size

We have shown above that comparison and equality queries suffice to obtain redundancy 1, matching the performance of Huffman's algorithm in this regard. What if we want to match the performance of Huffman's algorithm *exactly*?

Definition. A set of questions $\mathcal{Q}$ over X_n is *optimal* if for every distribution π there exists a decision tree using $\mathcal{Q}$ whose cost is $\mathrm{Opt}(\pi)$. Stated succinctly, a set of questions is optimal if it has zero prolixity.

It is not clear at the outset what condition can guarantee that a set of questions is optimal, since there are infinitely many distributions to handle. Fortunately, it turns out that there exists a "0-net" for this:

Definition. A distribution is *dyadic* if every non-zero element has probability $2^{-\ell}$ for some integer ℓ.

Observation 1 (restatement of Lemma 7.1.1)**.** A set of questions is optimal for all distributions over X_n if and only if it is optimal for all *dyadic* distributions over X_n.

Roughly speaking, this observation follows from the fact that binary decision trees correspond to dyadic distributions, a property that is exploited in Section 2.1.3 as well.

A further simplification is:

Observation 2 (restatement of Lemma 7.1.3)**.** A set of questions is optimal if and only if it is a *dyadic hitter*: for every non-constant dyadic distribution π it contains a question Q *splitting* π, that is, $\pi(Q) = \pi(\overline{Q}) = 1/2$.

This observation follows from the following characterization of optimal decision trees for dyadic distributions, whose proof is a straightforward application of the chain rule for entropy:

Lemma. *Let π be a dyadic distribution. A decision tree T for π has optimal cost* $\mathrm{Opt}(\pi)$ *if and only if the following holds for every internal node v with children v_1, v_2:*

$$\pi(v_1) = \pi(v_2) = \frac{\pi(v)}{2},$$

where $\pi(v)$ is the probability that the decision tree reaches the node v.

Our task is thus reduced to determining the size of a dyadic hitter. To understand what we are up against, consider distributions that have $2\beta n - 1$ "heavy" elements of probability $\frac{1}{2\beta n}$ each, and $(1-2\beta)n + 1$ "light" elements of total probability $\frac{1}{2\beta n}$, where β is a positive number such that βn is a power of 2.

A short argument shows that the only sets splitting such a distribution are those containing exactly βn heavy elements, and their complements. By considering all possible partitions of X_n into heavy and light elements, we see that every dyadic hitter must contain at least this many questions:

$$\begin{aligned}&\frac{\#\text{partitions to heavy and light elements}}{\#\text{partitions split by a question of size } \beta n}\\ =&\frac{\#\text{questions of size } \beta n}{\#\text{questions of size } \beta n \text{ splitting each partition}} = \frac{\binom{n}{\beta n}}{\binom{2\beta n - 1}{\beta n}} \approx 2^{(h(\beta)-2\beta)n}.\end{aligned}$$

(To see the first equality, cross-multiply to get two different expressions for the number of pairs consisting of a partition to heavy and light elements and a question of size βn splitting it.)

Choosing $\beta = 1/5$ (which maximizes $h(\beta) - 2\beta$), we find out that roughly 1.25^n questions are necessary just to handle distributions of this form. There is a fine print: the value $\beta = 1/5$ is only achievable when $n/5$ is a power of 2, and so the bound obtained for other values of n is lower.

Somewhat surprisingly, there is a matching upper bound: there is a set of roughly 1.25^n questions which forms a dyadic hitter! In order to show this, we first show that for every non-constant dyadic distribution π there is some question size $1 \leq c \leq n$ such that

$$\frac{\#\text{questions of size } c \text{ that split } \pi}{\#\text{questions of size } c} \geq 1.25^{-n-o(n)}.$$

Therefore, by choosing $1.25^{n+o(n)}$ random questions of size c, it is highly probable that one of them splits π.

This suggests considering a random set of questions $\mathcal{Q}$ formed by taking $1.25^{n+o(n)}$ questions at random of size c for each $1 \leq c \leq n$. Since there are only exponentially many dyadic distributions, a union bound shows that with high probability, $\mathcal{Q}$ splits *all* dyadic distributions.

How do we identify a value of c and a large set of questions of size c splitting an arbitrary dyadic distribution π? Roughly speaking, we bucket the elements of μ according to their probabilities. Suppose that there are m non-empty buckets, of sizes $c_1, \ldots, c_m$, respectively. Assume for simplicity that all c_i are even; in the actual proof, we essentially reduce to this case by bundling together elements of lower probability. A question containing exactly half the elements in each bucket thus splits μ. The number of such questions is

$$\prod_{i=1}^{m} \binom{c_i}{c_i/2} \approx \prod_{i=1}^{m} \frac{2^{c_i}}{\sqrt{c_i}} \approx \frac{2^{c_1+\cdots+c_m}}{n^{m/2}}.$$

By "throwing out" all elements of small probability (corresponding to the light elements considered above), we can guarantee that $m \leq \log n$, ensuring that the factor $n^{-m/2}$ is subexponential; however, this means that not all elements are going to belong to a bucket. If $c_1+\cdots+c_m = 2\beta n$ after throwing out all light elements then we have constructed roughly $2^{2\beta n}$ questions of size $c = \beta n$. Since

$$\frac{\binom{n}{c}}{2^{2\beta n}} \approx 2^{(h(\beta)-2\beta)n} \leq 1.25^n,$$

we have fulfilled our promise.

To summarize:

Theorem (restatement of Theorem 7.2 and Theorem 7.3)**.** *For every n there is an optimal set of questions of size $1.25^{n+o(n)}$.*

For infinitely many n, every optimal set of questions contains at least $1.25^{n-o(n)}$ questions.

While our upper bound works for every n, our lower bound only works for infinitely many n. For arbitrary n our best lower bound is only $1.232^{n-o(n)}$. We suspect that the true answer depends on the fractional part of $\log_2 n$; see Section 10.2 for an elaboration.

Our upper bound is non-constructive: it does not give an explicit optimal set of questions of size $1.25^{n+o(n)}$, but only proves that one exists. It is an interesting open question to obtain an explicit such set of this size. However, we are able to construct an explicit optimal set of questions of size $O(\sqrt{2}^n)$:

Theorem (restatement of Theorem 7.5)**.** *For every n there is an explicit optimal set of questions $\mathcal{Q}$ of size $O(2^{n/2})$.*

Furthermore, given a distribution on X_n, we can construct an optimal decision tree using $\mathcal{Q}$ in time $O(n^2)$.

The explicit set of questions is easy to describe: it consists of all subsets and all supersets of $S = \{x_1, \ldots, x_{\lfloor n/2 \rfloor}\}$. Why does this work? Given the observations above, it suffices to show that this collection contains a question splitting any non-constant dyadic distribution π on X_n. If $\pi(S) = 1/2$ then this is clear. If $\pi(S) > 1/2$, suppose for simplicity that $\pi_1 \geq \cdots \geq \pi_{\lfloor n/2 \rfloor}$. A simple parity argument shows that $\pi(\{x_1, \ldots, x_m\}) = 1/2$ for some $m < \lfloor n/2 \rfloor$. The case $\pi(S) < 1/2$ is similar.

This set of questions, known as a *cone*, appears in the work of Lonc and Rival [LR87] on *fibres*, which are hitting sets for maximal antichains. The lower bound $1.25^{n-o(n)}$ on optimal sets of questions appears, in the context of fibres, in Duffus, Sands and Winkler [DSW90]. The connection between these results and ours is that every fibre is an optimal set of questions. We explain this connection in Section 7.2.

2.3 Sets of questions with low prolixity

The hard distributions described in the preceding section show that any strictly optimal set of questions must have exponential size. The following theorem shows that this exponential barrier can be overcome by allowing a small prolixity:

Theorem (restatement of Theorem 8.1)**.** *For every n and $r \in (0, 1)$ there is a set $\mathcal{Q}_r$ of roughly $(r \cdot n)^{16/r}$ questions which has prolixity r.*

Furthermore, at least roughly $(r \cdot n)^{0.25/r}$ questions are required to achieve prolixity r.

As in the case of prolixity 0, the lower bound relies on a family of hard distributions: Assume that r is of the form 2^{-k} for some integer $k > 0$. A hard distribution consists of $2^k - 1$ "heavy elements" of total probability $1 - \delta$, and $n - (2^k - 1)$ "light elements" of total probability δ, where $\delta = r^2/2$ (or any smaller positive number). A case analysis shows that every 2^{-k}-optimal decision tree (one whose cost exceeds the optimal Huffman cost by at most 2^{-k}) for this distribution must partition the heavy elements evenly (into parts of size 2^{k-1} and $2^{k-1} - 1$), and put all light elements in the same part. Ignoring the difference between 2^{k-1} and $2^{k-1} - 1$, this shows that any 2^{-k}-optimal set of questions must contain at least this many questions:

$$\frac{\binom{n}{2^k - 1}}{\binom{n-(2^{k-1}-1)}{2^{k-1}}} \geq \left(\frac{n}{2^k}\right)^{2^{k-1}-1}.$$

In terms of $r = 2^{-k}$, this lower bound is $(r \cdot n)^{0.5/r-1}$, from which we obtain the form above (approximating an arbitrary r by a negative power of 2).

The upper bound is more involved. The set of questions consists of all interval queries with up to 2^k elements added or removed (in total, about $n^2 \binom{n}{\leq 2^k} 2^{2^k} = n^2 \cdot O(n/2^k)^{2^k}$ questions); we will aim at a redundancy of roughly $4 \cdot 2^{-k}$. The algorithm has some resemblance to the Gilbert–Moore line of algorithms described in Section 2.1.3. As in that section, given a distribution π, our starting point is the distribution $2^{-\ell_1}, \ldots, 2^{-\ell_n}$ formed from a Huffman code for π, where ℓ_i is the length of the codeword corresponding to x_i.

In contrast to Gilbert–Moore-style algorithms, though, instead of maintaining an interval we will maintain a *dyadic subestimate* for the probabilities of all elements "in play". That is, for every

element consistent with the answers so far we will assign a probability $q_i = 2^{-t_i}$, ensuring that $\sum_i q_i \leq 1$.

The algorithm is recursive, getting as input a dyadic subdistribution $q_1, \ldots, q_m$, which is initially $2^{-\ell_1}, \ldots, 2^{-\ell_n}$; the recursion stops when $m = 1$. The algorithm classifies its input elements according to the magnitude of q_i as either *heavy* (at least 2^{-k}), or *light* (otherwise), and proceeds as follows:

Random window algorithm

Case 1: the total mass of heavy elements is at least $1/2$**.** Find a set of heavy elements whose probability is exactly $1/2$, and ask whether the secret element lies in that set. Double the probability of all conforming elements, and recurse with the set of conforming elements.

Case 2: the total mass of heavy elements and the total mass of light elements are at most $1/2$**.** Ask whether the secret element is heavy or light. Double the probability of all conforming elements, and recurse with the set of conforming elements.

Case 3: The total mass σ **of light elements is at least** $1/2$**.** Identify a light element x_i with a segment T_i of length q_i, and place all such segments consecutively on a circle of circumference σ. Choose a random arc W of length $1/2$ (the *window*). Ask whether the secret element is a light element whose segment's midpoint lies in the window. Double the probability of all conforming elements not intersecting the boundaries of the window, and recurse with the set of conforming elements.

Achieving an optimal cost requires that at each step the probability of each conforming element is doubled. However, by Theorem 7.3 this would require exponentially many potential queries (rather than just our modified interval queries), and so we have to compromise by not doubling some of the probabilities of conforming elements in some steps (in Case 3, the probabilities of the two boundary elements are not doubled). Nevertheless, the above randomized algorithm ensures that the expected number of times each element is being "compromised" is $O(2^{-k})$.

How many questions does it take to find an element x_i whose starting probability is $2^{-\ell_i}$? At any iteration in which $q_i \geq 2^{-k}$, the probability q_i always doubles. When $q_i < 2^{-k}$, Case 3 could happen, but even then the probability that q_i doesn't double is only $2q_i/\sigma \leq 4q_i$. A straightforward calculation shows that q_i doubles after at most $\frac{1}{1-4q_i}$ questions in expectation when $q_i < 2^{-k}$, and so the expected number of questions needed to discover x_i is at most

$$k + \sum_{j=k+1}^{\ell_i} \frac{1}{1 - 4 \cdot 2^{-j}} < \ell_i + 4 \cdot 2^{-k} + \frac{2}{3}(4 \cdot 2^{-k})^2.$$

Roughly speaking, the resulting prolixity is $r \approx 4 \cdot 2^{-k}$, and the number of questions is about $n^2 \cdot O(n/2^k)^{2^k} \approx n^2 \cdot O(r \cdot n)^{4/r}$.

3 Related work

Our work can be seen as answering two different, but related, questions:

1. How good are certain particular sets of questions (particularly comparison and equality queries), compared to the information-theoretical benchmark and the combinatorial benchmark?

2. What is the smallest set of questions which matches the performance of Huffman codes, in terms of the information-theoretical benchmark or the combinatorial benchmark? What if we allow a small slack?

To the best of our knowledge, existing literature only deals with the first question. Apart from unrestricted questions, the only set of questions which has been extensively studied from the perspective of our two benchmarks is comparison queries.

We assume familiarity with the basic definitions appearing in Section 2 or in Section 4.

Section organization. We describe several sets of questions which have been studied in the literature in Section 3.1. Other relevant topics are discussed in Section 3.2.

3.1 Types of decision trees

We can identify sets of questions with decision trees using them (that is, using only questions from the set). For example, binary search trees (more accurately, alphabetic trees; see below) are decision trees using comparison queries.

The cost function that we study and attempt to minimize in this paper is *distributional* or *average case*: it is the average number of questions asked on an element chosen from a given distribution.

Another cost function studied in the literature, especially in problems whose motivation is algorithmic, is *worst case*: the maximum number of questions asked on any element. The most familiar examples are binary search and sorting.

We go on to list several types of decision trees appearing in the literature, briefly commenting on each of them.

3.1.1 Unrestricted decision trees

The simplest type of decision trees is unrestricted decision trees. Huffman [Huf52] showed how to construct optimal decision trees, and van Leeuwen [vL87] showed how to implement his algorithm in time $O(n \log n)$, or $O(n)$ if the probabilities are sorted. Huffman also considered non-binary decision trees, generalizing his algorithm accordingly.

Gallager [Gal78] showed that decision trees constructed by Huffman's algorithm are characterized by the *sibling property*: the nodes of the tree can be arranged in non-decreasing order of probability of being reached, in such a way that any two adjacent nodes are siblings. This shows, among else, that in some cases there are optimal decision trees which cannot be generated by Huffman's algorithm. In the parlance of codes, a distinction should be made between *Huffman codes* and the more general *minimum redundancy codes*.

Gallager also discussed the *redundancy* of Huffman codes in terms of the maximum probability of an element, showing that if π is a distribution with maximum probability $\pi_{\max}$ then $\mathrm{Opt}(\pi) \leq H(\pi) + \pi_{\max} + 1 - \log_2 e + \log_2 \log_2 e$, where $1 - \log_2 e + \log_2 \log_2 e \approx 0.086$. He also showed that the constant $1 - \log_2 e + \log_2 \log_2 e$ is optimal.

The question of the redundancy of Huffman codes in terms of $\pi_{\max}$ has attracted some attention: a line of work, including [Joh80, CGT86], culminated in the work of Montgomery and Abrahams [MA87], who found the optimal lower bound on $H(\pi) - \mathrm{Opt}(\pi)$ in terms of $\pi_{\max}$, and in the work of Manstetten [Man92], who found the optimal upper bound.

The redundancy of Huffman codes has also been considered in terms of other parameters, such as the minimum probability, both minimum and maximum probabilities, or some probability. See Mohajer et al. [MPK06] for a representative example with many references.

Gallager also gave an algorithm for dynamically updating Huffman trees, contemporaneously with Faller [Fal73] and Knuth [Knu85]. Their work was improved by Vitter [Vit87]. Vitter's data structure is given an online access to a stream of symbols $(\sigma_n)_{n\in\mathbb{N}}$, and it maintains a decision tree T_n which at time n is a Huffman tree for the empirical distribution μ_n of $\sigma_1, \ldots, \sigma_n$. The update time is $O(T_n(\sigma_n))$, where $T_n(\sigma_n)$ is the depth (or codeword length) of σ_n in T_n, and the output codewords satisfy

$$\frac{1}{n}\sum_{i=1}^{n} T_i(\sigma_i) \leq \mathrm{Opt}(\mu_n) + 1.$$

Many variants of Huffman coding have been considered: length-restricted codes [Gil71, EK04], other cost functionals [Bae07], unequal letter costs [Kar61], and many more. See the excellent survey of Abrahams [Abr97]. We expand on some of these topics in Section 10.5.

3.1.2 Binary search trees

A binary search tree (BST) stores an ordered list of elements $x_1 \prec \cdots \prec x_n$ over a linearly ordered domain, and supports a search operation, which given an element x can result in any of the following outcomes:

- $x = x_i$ for some i.
- $x \prec x_1$.
- $x_i \prec x \prec x_{i+1}$ for some $i < n$.
- $x \succ x_n$.

Each node of the tree contains an element x_i, and it tests whether $x \prec x_i$, $x = x_i$, or $x \succ x_i$. Given probabilities $p_1, \ldots, p_n$ for successful searches ($x = x_i$) and $q_0, \ldots, q_n$ for unsuccessful searches ($x_i \prec x \prec x_{i+1}$), an optimal BST is one that minimizes the number of questions it takes to identify the class of a secret element x.

Binary search trees do not fit the model considered in the paper as stated. However, if the probability of a successful search is zero (that is, $p_1 = \cdots = p_n = 0$), then the ternary queries become binary queries, and the resulting decision tree is a decision tree using comparison queries on the domain composed of the $n + 1$ *gaps* between and around the elements $x_1, \ldots, x_n$:

$$y_0 = (-\infty, x_1), y_1 = (x_1, x_2), \ldots, y_{n-1} = (x_{n-1}, x_n), y_n = (x_n, \infty).$$

The resulting model is also known as *alphabetical trees* or *lexicographical trees*, and has been suggested by Gilbert and Moore [GM59] in the context of variable-length binary encodings. Alphabetical trees (of words) are decision trees in which the leaves are ordered alphabetically. In our terminology, they are decision trees using comparison queries.

Kraft's inequality states that a decision tree whose leaves have depths $\ell_1, \ldots, \ell_n$ exists if and only if $\sum_{i=1}^{n} 2^{-\ell_i} \leq 1$. Nakatsu [Nak91] gave an analog of Kraft's inequality for alphabetical trees.

Knuth [Knu71] gave an $O(n^2)$ dynamic programming algorithm for finding the optimal BST. Hu and Tucker [HT71] and Garsia and Wachs [GW77] gave $O(n \log n)$ algorithms for finding optimal alphabetical trees. These algorithms are more complicated than Huffman's.

Several heuristics for constructing good alphabetical trees are described in the literature. Gilbert and Moore [GM59] gave one heuristic (described in Section 9) which produces a tree with cost at most $H(\pi) + 2$. Nakatsu [Nak91] gave the stronger bound $\mathrm{Opt}(\pi) + 1$ for a very similar heuristic.

Another heuristic, *weight balancing* (described in Section 5), was suggested by Rissanen [Ris73] (and even earlier by Walker and Gottlieb [WG72]), who showed that it produces a tree with cost at most $H(\pi) + 3$. Horibe [Hor77] improved the analysis, showing that the cost is at most $H(\pi) + 2$.

The question of the redundancy of alphabetical trees has been considered in the literature. While the bound $H(\pi)+2$ cannot be improved upon in general, a better bound can be obtained given some knowledge of the distribution π. Such improved bounds have been obtained by Nakatsu [Nak91], Sheinwald [She92], Yeung [Yeu91], De Prisco and De Santis [DPDS93] (who consider, among else, dyadic distributions), Bose and Douïeb [BD09] (for general BSTs), and others. The paper of De Prisco and De Santis contains a mistake, which we correct in Appendix A.

Kleitman and Saks [KS81] considered the following problem: given a probability distribution π, what order for π results in the largest redundancy of the optimal alphabetic tree? Assuming $\pi_1 \geq \cdots \geq \pi_n$, they showed that the worse order is $x_n, x_1, x_{n-1}, x_2, \ldots$, and gave a formula for the cost of the optimal alphabetical tree for that order.

Computing the optimal length-restricted alphabetical tree has been studied extensively [HT72, Gar74, Lar87, Sch98, Bae07]. Dynamic alphabetical trees have been considered by Grinberg, Rajagopalan, Venkatesan and Wei [GRVW95]. See Nagaraj [Nag97] for an extensive survey on these and other topics.

3.1.3 Binary search trees with comparison queries

As we have seen above, binary search trees involve a three-way comparison: "$x < c$, $x = c$, or $x > c$?". While modern programming languages usually support three-way comparisons, in the past a three-way comparison was implemented as two consecutive two-way comparisons: "$x = c$?" followed by "$x < c$?". This prompted Sheil [She78] to suggest replacing the first comparison above by "$x = d$?", where d is the current most probable element. The resulting data structure is known as a *binary split tree*.

Huang and Wong [HW84b] and Perl [Per84] (see also [HHHW86]) gave $O(n^5)$ dynamic programming algorithms that find the optimal binary split tree given a distribution on the elements, and this was improved to $O(n^4)$ by Chrobak et al. [CGMY15].

Huang and Wong [HW84a] suggested relaxing the requirement that d (the element participating in the query "$x = d$?") be the current most probable element. The resulting data structure is known as a *generalized binary split tree*. They suggested a dynamic programming algorithm for finding the optimal generalized binary split tree, but Chrobak et al. [CGMY15] showed that their algorithm is invalid; no other efficient algorithm is known.

Spuler [Spu94a, Spu94b] suggested uncoupling the two comparisons. His *two-way comparison tree* is a decision tree which uses comparison and equality queries. Anderson et al. [AKKL02] called this data structure a *binary comparison search tree* (BCST).

The notion of successful versus unsuccessful searches, which differentiates binary search trees and alphabetical trees (see above), also appears in the context of BCSTs. As an example, consider a domain with a single element c. If only successful searches are allowed, then the trivial BCST suffices. Otherwise, two nodes are needed to determine whether $x < c$, $x = c$, or $x > c$. The model considered in this paper only allows successful searches.

Spuler gave an $O(n^5)$ dynamic programming algorithm for finding the optimal BCST given a distribution on the successful searches, and Anderson et al. [AKKL02] improved this to $O(n^4)$. They also list several interesting properties of optimal BCSTs.

Chrobak et al. [CGMY15] generalized the algorithm of Anderson et al. to the case in which unsuccessful searches are allowed, and gave an $O(n \log n)$ algorithm based on weight-balancing which has redundnacy 3.

3.1.4 Searching in trees and posets

Ben-Asher, Farchi and Newman [BAFN99] consider the natural generalization of alphabetical trees to posets. Given a poset X, the the task is to find a secret element x using queries of the form "$x \prec c$?". When X is a linear order, this is just an alphabetical tree.

Ben-Asher et al. concentrate on the case in which the Hasse diagram of X is a rooted tree, the root being the maximum element. In this case the queries can also be considered as edge queries: given an edge $e = (s, t)$, "Is x closer to s or to t?". If t is the node closer to the root, then this query is equivalent to the comparison query "$x \prec t$?".

Ben-Asher et al. give several applications of this model, to data transfer, software testing, and information retrieval. They are interested in minimizing the depth of the decision tree. Their main result is an $\tilde{O}n^4)$ algorithm which finds a decision tree of minimum depth, improved to $O(n^3)$ by Onak and Parys [OP06]. Lam and Yue [LY01] and Mozes, Onak and Weimann [MOW08] give a linear time algorithm for the same problem.

Linial and Saks [LS85b, LS85a] consider a different model for searching in posets: searching with partial information. In their model (adapted to our setting[3]) we are given a linearly ordered set X whose order is unknown, but is consistent with a known partial order on X. Given an element x, the task is to identify x using comparison queries. They are interested in minimizing the maximum number of queries.

As an example, suppose that A is an $n \times n$ matrix in which the rows and columns are increasing. How many queries are needed, in the worst case, to locate an element? They show that the answer is $2n - 1$, and relate this to the complexity of the merging procedure in merge sort.

Let i be the number of ideals (downward-closed sets) in the given partial order. Linial and Saks mention that $\log_2 i$ questions are needed in the worst case, and show that $O(\log_2 i)$ is achievable.

3.1.5 Sorting

Suppose we are given an array of length n having distinct elements. Sorting the array is the same as finding the relative order of the elements, which is a permutation $\pi \in S_n$. We can thus construe comparison-based sorting as the problem of finding a permutation $\pi \in S_n$ using queries of the form "$\pi(i) < \pi(j)$?". We call such queries *relative order queries*. We are usually interested in the worst case complexity of sorting algorithms, that is, the maximum number of relative order queries made by the algorithm.

Every comparison-based sorting algorithm must make at least $n \log_2 n - O(n)$ comparisons in the worst case. Merge sort comes very close, making $n \log_2 n + O(n)$ comparisons. In our terminology, the minimum depth of a decision tree for S_n using relative order queries is $n \log_2 n \pm \Theta(n)$.

Fredman [Fre76] considered the problem of sorting with partial information. In this problem, we are given a set of permutation $\Gamma \subseteq S_n$, and the task is to identify a secret permutation $\pi \in \Gamma$ using relative order queries. Using the Gilbert–Moore algorithm, Fredman showed that this can be accomplished using at most $\log_2 |\Gamma| + 2n$ queries in the worst case.

Fredman applied his method to Berlekamp's $X + Y$ problem, which asks for sorting an array of the form $\{x_i + y_j : 1 \le i, j \le n\}$. Harper et al. [HPSS75] had improved on performance of merge sort (which uses $2n^2 \log_2 n + O(n^2)$ comparisons) by giving an algorithm which uses only $n^2 \log_2 n + O(n^2)$ comparisons. Fredman significantly improved on this by showing that $O(n^2)$ comparisons suffice, albeit the corresponding algorithm cannot be implemented efficiently. Lambert [Lam92] gave an explicit algorithm using $O(n^2)$ comparisons, which also cannot be implemented efficiently.

[3] In their setting $X \subseteq \mathbb{R}$, and the task is to decide, given $x \in \mathbb{R}$, whether $x \in X$.

When Γ consists of all completions of some partial order, Kahn and Saks [KS84] gave the upper bound $O(\log|\Gamma|)$ using the technique of poset balancing, but the corresponding algorithm cannot be implemented efficiently. Kahn and Kim [KK95] gave an algorithm with the same performance which can be implemented efficiently. Their algorithm relies on computing volumes of polytopes.

Moran and Yehudayoff [MY16] extended the results of Fredman to the distributional case. They showed that given a probability distribution μ on S_n, a secret permutation $\pi \sim \mu$ can be found using at most $H(\mu) + 2n$ relative order queries on average. In our terminology, they showed that the redundancy of relative order queries is at most $2n$. They actually proved a stronger bound: the number of queries required to identify π is at most $\log_2 \frac{1}{\mu(\pi)} + 2n$. This stronger bound implies Fredman's result.

Given a set of permutations $\Gamma \subseteq S_n$, endow S_n with the uniform permutation μ_Γ over Γ. A decision tree for Γ of depth $f(\log_2 \Gamma)$ is the same as a decision tree for μ_Γ of depth $f(H(\mu_\Gamma))$. In this way we can interpret all non-distributional results stated above as distributional results for uniform distributions.

3.1.6 Binary decision trees

Binary decision trees, or binary decision diagrams (BDDs), are used in statistics, machine learning, pattern recognition, data mining, and complexity theory. The setting is a set $X \subseteq \{0,1\}^n$ and a function $f\colon X \to Y$ (for an arbitrary set Y). The task is to construct a decision tree which on input $x \in X$ computes $f(x)$ using only queries of the form "$x_i = 1$?" (*binary queries*).

In many settings, $Y = \{0,1\}$, and such binary decision trees do not really fit our model. In other settings, $Y = X$ and f is the identity function. In this case these are decision trees in our sense which use binary queries.

We will not attempt to summarize the large literature on binary decision trees. We only mention the result of Hyafil and Rivest [HR76], who showed that it is NP-complete to compute the optimum cost of a decision tree using binary queries under the uniform distribution.

3.1.7 Algebraic decision trees

Algebraic decision trees are commonplace in computational geometry. Given a set of real numbers $x_1, \ldots, x_n \in \mathbb{R}$ and a function f on $\mathbb{R}^n$, a (two-way) *linear decision tree* (LDT) is a decision tree for computing f using queries of the form "$\sum_i a_i x_i + a < 0$?" (*linear queries*); three-way variants also exist. *Algebraic decision trees* (ADTs) of order d are more general: they allow queries of the form "$P(x_1, \ldots, x_n) < 0$?" (*d'th order queries*), where P is an arbitrary polynomial of degree at most d. Interest has mainly focused on the worst-case cost of algebraic decision trees.

While algebraic decision trees, as just described, do not fit our model, the following variant does: given a finite set $S \subseteq \mathbb{R}^n$, the task is to find a secret element $x \in S$ using linear or d'th order queries.

Out of the voluminous literature on algebraic decision trees, we only mention the important paper of Ben-Or [BO83], which gives a lower bound of $\Omega(n \log n)$ on the depth of algebraic decision trees of fixed order which solve the element distinctness problem, using the Milnor–Thom theorem in real algebraic geometry.

A restricted type of linear decision trees occurs in the context of the 3SUM problem. In this problem, which is related to the $X + Y$ problem discussed above in the context of sorting, we are given three arrays X, Y, Z of size n, and our goal is to decide whether there exist $x \in X$, $y \in Y$, $z \in Z$ such that $x + y + z = 0$ (there are many other equivalent formulations). In the more general

k-sum problem, we are given k arrays $X_1, \ldots, X_k$ of size n, and our goal is to decide whether there exist elements $x_i \in X_i$ such that $\sum_{i=1}^{k} x_i = 0$.

A classical algorithm solves 3SUM in time $O(n^2)$ by first sorting X and Y, and then, for each $z \in Z$, checking whether X and $-z - Y$ intersect using the merging procedure of merge sort. The classical algorithm can be construed as a three-way decision tree using queries of the form "$a_i < a_j$?" and "$a_i + a_j + a_k < 0$, $a_i + a_j + a_k = 0$, or $a_i + a_j + a_k > 0$?", where $a_1, \ldots, a_{3n}$ are the elements of X, Y, Z.

More generally, a (two-way) *s-linear decision tree* is a decision tree using questions of the form "$\sum_i c_i a_i < 0$?", where at most s of the c_i are non-zero; a three-way version is defined analogously. The classical algorithm uses a three-way 3-linear decision tree.

Erickson [Eri99] proved a lower bound of $\Omega(n^{(k+1)/2})$ on the depth of a k-linear decision tree solving k-SUM when k is odd, and a lower bound of $\Omega(n^{k/2})$ when k is even. Weaker lower bounds for s-linear decision trees when $s > k$ were proved by Ailon and Chazelle [AC05].

The 3SUM conjecture (in one formulation) states that 3SUM cannot be solved in time $\Omega(n^{2-\epsilon})$ for any $\epsilon > 0$ (in the RAM machine model). Indeed, the stronger lower bound of $\Omega(n^2)$ had been conjectured. Similar lower bounds (matching the exponents stated above) exist for k-SUM.

Recently, in a breakthrough result, Grønlund and Pettie [GP14] gave a $o(n^2)$ algorithm for 3SUM (see Freund [Fre15] for a simplification). Their algorithm is based on a 4-linear decision tree for 3SUM whose depth is $\tilde{O}(n^{3/2})$. More generally, for odd k they gave a $(2k-2)$-linear decision tree for k-SUM whose depth is $\tilde{O}(n^{k/2})$.

Meyer auf der Heide [MadH84] gave a linear decision tree for k-SUM whose depth is $\tilde{O}(n^4)$, for any constant k. Recently, Cardinal et al. [CIO16] improved this to $\tilde{O}(n^3)$ using a technique of Meiser [Mei93], and Ezra and Sharir [ES16] improved the bound to $\tilde{O}(n^2)$. These authors solve a variant of the k-SUM problem in which we are given only *one* list $x_1, \ldots, x_n$, and the task is to decide whether k of its elements sum to zero. Their methods also solve a generalization, *k-linear degeneracy testing* (k-LDT), which asks whether there exist k indices $i_1 < \cdots < i_k$ such that $a_0 + a_1 x_{i_1} + \cdots + a_k x_{i_k} = 0$, for some constants $a_0, \ldots, a_k$.

3.2 Other topics

We close the literature review by mentioning a few other related topics.

Combinatorial search theory The "20 questions" game is the starting point of combinatorial search theory. Well-known examples include counterfeit coin problems [Smi47] (also known as balance problems). See the survey by Katona [Kat73], the monograph of Ahlswede and Wegener [AW87], and the recent volume [ACD13] in memory of Ahlswede. Combinatorial search theory considers many different variants of the "20 questions" game, such as several unknown elements, non-adaptive queries, non-binary queries, and a non-truthful Alice; we expand below on the latter variant. Both average-case and worst-case complexity measures are of interest.

An important topic in combinatorial search theory is *combinatorial group testing*, in which we want to identify a set of at most d defective items out of n items using as few tests as possible. The original motivation was blood testing [Dor43]. See the monograph by Du and Hwang [DH99]. Combinatorial group testing is related to the area of *combinatorial designs*, see for example Colbourn et al. [CDS93].

Playing 20 questions with a liar We have described a distributional version of the "20 questions" game in the introduction. The more usual version has Alice pick an object x from a known finite set X of size n. Bob is then tasked with discovering the secret object x using as few Yes/No

questions as possible (in the worst case). If Bob is allowed to ask arbitrary questions, his optimal strategy reveals x using $\lceil \log_2 n \rceil$ questions at most.

In the usual version of the game, Alice is truthful. Rivest et al. [RMK+80] considered the case in which Alice is allowed to lie k times. They gave a strategy which asks at most $\log_2 n + k \log_2 \log_2 n + O(k \log k)$ questions in the worst case, all of them comparison queries. Moreover, they showed that $\log_2 n + k \log_2 \log_2 n + O(k \log k)$ questions are necessary, even if arbitrary questions are allowed.

Another line of work, which allows for a constant fraction r of lies, culminated in the work of Spencer and Winkler [SW92], who determined the threshold r for which Bob can win in the following three scenarios:

- Batch game: Alice knows Bob's strategy, and is allowed to lie in an r-fraction of answers.
- Adaptive game: Alice doesn't know Bob's strategy (which can depend on Alice's answers), and is allowed to lie in an r-fraction of answers.
- Prefix-bounded game: Alice doesn't know Bob's strategy, and is allowed to lie at most rm times in the first m questions, for every m.

Aslam and Dhagat [AD91] and Dhagat et al. [DGW92] analyze these scenarios under various restricted sets of questions, including:

- Bit queries: "Is the ith bit of the binary representation of x equal to 1?".
- Comparison queries, which they also call cut queries.
- Tree queries: "Is $i2^j \leq x < (i+1)2^j$?".

Asymmetric communication One practical motivation for the (distributional) "20 questions" game is a communication scenario in which two entities, a client (Alice) and a server (Bob), communicate, and the uplink for the client to the server is much more costly than the downlink from the server to the client.

Adler and Maggs [AM01] suggest a formalization of this setting. In their model, the client holds a string x, the server has black-box access to a distribution π on the set of possible strings, and the server's goal is to discover x, assuming it is drawn from π. The server is allowed to access π by determining, for any string t, the probability that a string drawn from π has t as a prefix. An algorithm is measured using four different parameters:

- The expected number of bits sent by the server.
- The expected number of bits sent by the client.
- The expected number of black box accesses.
- The expected number of rounds of communication.

Adler and Maggs give various algorithms exploring the various trade-offs. Watkinson et al. [WAF01], in follow-up work, give more algorithms, among them one based on comparison queries and the Gilbert–Moore algorithm.

Weight balancing The weight balancing algorithm of Walker and Gottlieb [WG72] and Rissanen [Ris73] (mentioned above in the section on binary search trees) is an instance of the more general *splitting* heuristic of Garey and Graham [GG74], also known as *generalized binary search* (GBS).

Given an arbitrary set of queries, at any given moment the splitting heuristic chooses the query which minimizes $|\Pr[Yes] - \Pr[No]|$. This is a special case of the well-known ID3 algorithm [Qui86], used in statistics, machine learning and data mining; the ID3 algorithm also handles k-way queries.

Kosaraju et al. [KPB99] analyzed the performance of the splitting heuristic on general sets of questions. They showed that a slight modification of the heuristic gives an $O(\log n)$ approximation for the optimal cost using the given set of questions, where $n = |X|$ is the size of the domain.

4 Preliminaries

Notation We use $\log n$ for the base 2 logarithm of n and $[n]$ to denote the set $\{1, \ldots, n\}$.

Throughout the document, we will consider probability distributions over the set $X_n = \{x_1, \ldots, x_n\}$ of size n. In some cases, we will think of this set as ordered: $x_1 \prec \cdots \prec x_n$.

If π is a probability distribution over X_n, we will denote the probability of x_i by π_i, and the probability of a set $S \subseteq X_n$ by $\pi(S)$.

Information theory The most basic definition in information theory is the *entropy* of a distribution:

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

While entropy is often measured in nats, our entropy is measured in bits. We will also use the *binary entropy* function,

$$h(p) = -p \log \frac{1}{p} - (1-p) \log \frac{1}{1-p}.$$

This is just the entropy of a Bernoulli p random variable.

The *conditional entropy* of a random variable X given a random variable Y is

$$H(X|Y) = \sum_{y} \Pr[Y = y] H(X|Y = y).$$

Here $H(X|Y = y)$ is the entropy of the distribution of X conditioned on $Y = y$.

The conditional entropy satisfies the chain rule

$$H(X, Y) = H(Y) + H(X|Y).$$

Here $H(Y)$ is the entropy of the distribution of Y, and $H(X, Y)$ is the entropy of the joint distribution of (X, Y).

When Y is a Bernoulli random variable, the chain rule takes the form

$$H(X|Y) = h(\Pr[Y = 1]) + \Pr[Y = 0] H(X|Y = 0) + \Pr[Y = 1] H(X|Y = 1).$$

We call this the *Bernoulli chain rule.*

We also use the *Kullback–Leibler divergence*:

$$D(\pi \| \sigma) = \sum_{i=1}^{n} \pi_i \log \frac{\pi_i}{\sigma_i}.$$

Decision trees In this paper we consider the task of revealing a secret element x from X_n by using Yes/No questions. Such a strategy will be called a *decision tree* or an *algorithm*.

A decision tree is a binary tree in which the internal nodes are labeled by subsets of X_n (which we call *questions* or *queries*), each internal node has two outgoing edges labeled *Yes* (belongs to the question set) and *No* (doesn't belong to the question set), and the leaves are labeled by elements of X_n.

Decision trees can be thought of as annotated prefix codes: the code of an element x_i is the concatenation of the labels of the edges leading to it. The mapping can also be used in the other direction: each binary prefix code of cardinality n corresponds to a unique decision tree over X_n.

Given a set $\mathcal{Q} \subseteq 2^{X_n}$ (a set of *allowed questions*), a *decision tree using* $\mathcal{Q}$ is one in which all questions belong to $\mathcal{Q}$.

Generally speaking, a decision tree is *valid* if given any element $x_i \in X_n$, if we follow the decision tree (in the natural way) then we reach a leaf labeled x_i. Since we are interested in decision trees in the context of distributions, we modify this definition slightly: a decision tree is valid for a distribution μ if given any element $x_i \in \mathrm{supp}(\mu)$, if we follow the decision tree then we reach a leaf labeled x_i.

We will only consider decision trees in which each element appears at most once. The depth of an element x_i in a decision tree T, denoted $T(x_i)$, is the number of edges in the unique path from the root to the unique leaf labeled x_i (if any).

Given a distribution μ and a decision tree T valid for μ, the *cost* (or *query complexity*) of T on μ, labeled $T(\mu)$, is the average number of questions asked on a random element:

$$T(\mu) = \sum_{i=1}^{n} \mu_i T(x_i).$$

Given a set $\mathcal{Q}$ of allowed questions and a distribution μ, the *optimal cost* of μ with respect to $\mathcal{Q}$, denoted $c(\mathcal{Q}, \mu)$, is the minimal cost of a valid decision tree for μ using $\mathcal{Q}$.

Dyadic distributions and Huffman's algorithm Huffman's algorithm [Huf52] finds the optimal cost of an unrestricted decision tree for a given distribution:

$$\mathrm{Opt}(\mu) = c(2^{X_n}, \mu).$$

We call a decision tree with this cost a *Huffman tree* or an *optimal decision tree* for μ. More generally, a decision tree is *r-optimal* for μ if its cost is at most $\mathrm{Opt}(\mu) + r$.

It will be useful to consider this definition from a different point of view. Say that a distribution is *dyadic* if the probability of each element in the support has the form 2^{-d} for some integer d. We can associate with each decision tree T a distribution τ on the leaves of T given by $\tau_i = 2^{-T(x_i)}$. This gives a bijection between decision trees and dyadic distributions.

In the language of dyadic distributions, Huffman's algorithm solves the following optimization problem:

$$\mathrm{Opt}(\mu) = \min_{\substack{\tau \text{ dyadic} \\ \mathrm{supp}(\tau)=\mathrm{supp}(\mu)}} \sum_{i=1}^{n} \mu_i \log \frac{1}{\tau_i} = \min_{\substack{\tau \text{ dyadic} \\ \mathrm{supp}(\tau)=\mathrm{supp}(\mu)}} \left[H(\mu) + D(\mu \| \tau) \right].$$

In other words, computing $\mathrm{Opt}(\mu)$ amounts to minimizing $D(\mu\|\tau)$, and thus to "rounding" μ to a dyadic distribution. We call τ a *Huffman distribution* for μ.

The following classical inequality shows that $\mathrm{Opt}(\mu)$ is very close to the entropy of μ:

$$H(\mu) \leq \mathrm{Opt}(\mu) < H(\mu) + 1.$$

The lower bound follows from the non-negativity of the Kullback–Leibler divergence; it is tight exactly when μ is dyadic. The upper bound from the Shannon–Fano code, which corresponds to the dyadic sub-distribution $\tau_i = 2^{-\lceil \log \mu_i \rceil}$.

Redundancy and prolixity We measure the quality of sets of questions by comparing the cost of decision trees using them to the entropy (the difference is known as *redundancy*) and to the cost of optimal decision trees (for the difference we coin the term *prolixity*). In more detail, the *redundancy* of a decision tree T for a distribution μ is $T(\mu) - H(\mu)$, and its *prolixity* is $T(\mu) - \mathrm{Opt}(\mu)$.

Given a set of questions $\mathcal{Q}$, the redundancy $r^H(\mathcal{Q}, \mu)$ and prolixity $r^{\mathrm{Opt}}(\mathcal{Q}, \mu)$ of a distribution μ are the best redundancy and prolixity achievable using questions from Q:

$$r^H(\mathcal{Q}, \mu) = c(\mathcal{Q}, \mu) - H(\mu),$$
$$r^{\mathrm{Opt}}(\mathcal{Q}, \mu) = c(\mathcal{Q}, \mu) - \mathrm{Opt}(\mu).$$

The redundancy of a set of questions $\mathcal{Q}$, denoted $r^H(\mathcal{Q})$, is the supremum of $r^H(\mathcal{Q}, \mu)$ over all distributions μ over X_n. The prolixity $r^{\mathrm{Opt}}(\mathcal{Q})$ of $\mathcal{Q}$ is defined similarly. These quantities are closely related, as the inequality $H(\mu) \leq \mathrm{Opt}(\mu) < H(\mu) + 1$ implies:

$$r^{\mathrm{Opt}}(\mathcal{Q}) \leq r^H(\mathcal{Q}) \leq r^{\mathrm{Opt}}(\mathcal{Q}) + 1.$$

A set of questions $\mathcal{Q}$ is *optimal* if $r^{\mathrm{Opt}}(\mathcal{Q}) = 0$, and r-optimal if $r^{\mathrm{Opt}}(\mathcal{Q}) \leq r$.

The parameters $u^H(n, r)$ and $u^{\mathrm{Opt}}(n, r)$ Our main object of study in this paper are the parameters $u^H(n, r)$ and $u^{\mathrm{Opt}}(n, r)$. The parameter $u^H(n, r)$ is the cardinality of the minimal set of questions $\mathcal{Q} \subseteq 2^{X_n}$ such that $r^H(\mathcal{Q}) \leq r$. Similarly, the parameter $u^{\mathrm{Opt}}(n, r)$ is the cardinality of the minimal set of questions $\mathcal{Q}$ such that $r^{\mathrm{Opt}}(\mathcal{Q}) \leq r$. These quantities are closely related:

$$u^{\mathrm{Opt}}(n, r) \leq u^H(n, r) \leq u^{\mathrm{Opt}}(n, r - 1).$$

Common sets of questions Some sets of questions will prove especially useful for us:

- Equality queries: $\mathcal{Q}_= = \{\{x_i\} : 1 \leq i \leq n\}$. In other words, $\mathcal{Q}_=$ consists of the questions "$x = x_i$?" for $i \in \{1, \ldots, n\}$. (Recall that x is the secret element.)
- Comparison queries: $\mathcal{Q}_\prec = \{\{x_1, \ldots, x_i\} : 1 \leq i \leq n - 1\}$. In other words, $\mathcal{Q}_\prec$ consists of the questions "$x \prec x_i$?" for $i \in \{2, \ldots, n\}$.
- Interval queries: $\mathcal{Q}_\square = \{\{x_i, \ldots, x_j\} : 1 \leq i \leq j \leq n\}$. In other words, $\mathcal{Q}_\square$ consists of the questions "$x_i \preceq x \preceq x_j$?" for $1 \leq i \leq j \leq n$.

When we wish to emphasize the domain of the set of questions, we will use an appropriate superscript: $\mathcal{Q}_=^{(n)}, \mathcal{Q}_\prec^{(n)}, \mathcal{Q}_\square^{(n)}$.

A useful lemma The following simple lemma will be used several times in the rest of the paper.

Lemma 4.1. *Let $p_1 \geq \ldots \geq p_n$ be a non-increasing list of numbers of the form $p_i = 2^{-a_i}$ (for integer a_i), and let $a \leq a_1$ be an integer. If $\sum_{i=1}^n p_i \geq 2^{-a}$ then for some m we have $\sum_{i=1}^m p_i = 2^{-a}$.*

If furthermore $\sum_{i=1}^n p_i$ is a multiple of 2^{-a} then for some ℓ we have $\sum_{i=\ell}^n p_i = 2^{-a}$.

Proof. Let m be the maximal index such that $\sum_{i=1}^{m} p_i \leq 2^{-a}$. 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 $S = 2^{-a}$.

The condition $p_1 \leq \cdots \leq p_n$ implies that $a_{m+1} \geq \cdots \geq a_1$, and so $k := 2^{a_{m+1}} S = \sum_{i=1}^{m} 2^{a_{m+1}-a_i}$ is an integer. By assumption $k \leq 2^{a_{m+1}-a}$ whereas $k+1 = 2^{a_{m+1}} \sum_{i=1}^{m+1} p_i > 2^{a_{m+1}-a}$. Since $2^{a_{m+1}-a}$ is itself an integer (since $a_{m+1} \geq a_1 \geq a$), we conclude that $k = 2^{a_{m+1}-a}$, and so $S = 2^{-a}$.

To prove the furthermore part, notice that by repeated applications of the first part of the lemma we can partition $[n]$ into intervals whose probabilities are 2^{-a}. The last such interval provides the required index ℓ. □

5 Comparisons and equality tests

Let π be a distribution over $X_n = \{x_1, \ldots, x_n\}$. A fundamental result in information theory is that the entropy of a distribution π captures the average number of queries needed to identify a random $x \sim \pi$. More specifically, every algorithm asks at least $H(\pi)$ questions in expectation, and there are algorithms that ask at most $H(\pi) + 1$ questions on average (such as Huffman coding and Shannon–Fano coding). However, these algorithms may potentially use arbitrary questions.

In this section we are interested in the setting where X_n is linearly ordered: $x_1 \prec x_2 \prec \cdots \prec x_n$. We wish to use questions that are compatible with the ordering. Perhaps the most natural question in this setting is a comparison query; namely a question of the form "$x \prec x_i$?". Gilbert and Moore [GM59] showed that there exists an algorithm that uses at most $H(\pi) + 2$ comparisons. Is this tight? Can comparison queries achieve the benchmark of $H(\pi) + 1$?

A simple argument shows that their result is tight: let $n = 3$, and let π be a distribution such that

$$\pi(x_1) = \epsilon/2, \quad \pi(x_2) = 1 - \epsilon, \quad \pi(x_3) = \epsilon/2,$$

for some small ϵ. Note that $H(\pi) = O(\epsilon \log(1/\epsilon))$, and therefore any algorithm with redundancy 1 must use the query "$x = x_2$?" as its first question. This is impossible if we only allow comparison queries (see Lemma 6.2.1 for a more detailed and general argument). In fact, this shows that any set of questions that achieves redundancy 1 must include all equality queries. So, we need to at least add all equality queries. Is it enough? Do comparison and equality queries achieve redundancy of at most 1?

Our main result in this section gives an affirmative answer to this question:

Theorem 5.1. *For all n, $r^H(\mathcal{Q}_{\prec}^{(n)} \cup \mathcal{Q}_{=}^{(n)}) = 1$. Moreover, if π has no element whose probability exceeds 0.9961 then $u^H(\mathcal{Q}_{\prec} \cup \mathcal{Q}_{=}, \pi) \leq 0.96711$.*

We prove the theorem by modifying the weight-balancing algorithm of Rissanen [Ris73], which uses only comparison queries and achieves redundancy 2 (as shown by Horibe [Hor77]).

The original weight-balancing algorithm is perhaps the first algorithm that comes to mind: it asks the most balanced comparison query (the one that splits the distribution into two parts whose probability is as equal as possible), and recurses according to the answer.

Our modified algorithm, Algorithm A_t, first checks whether the probability of the most probable element $x_{\max}$ exceeds the threshold t. If so, it asks the question "$x = x_{\max}$?". Otherwise, it proceeds as in the weight-balancing algorithm. The choice $t = 0.3$ results in an algorithm whose redundancy is at most 1.

While a naive implementation of Algorithm A_t takes time $O(n)$ to determine the next query, this can be significantly improved:

Theorem 5.2. *Algorithm A_t can be simulated on an element x requiring D questions in time $O(n + D \log n)$, using $O(n)$ extra space.*

Moreover, the decision tree corresponding to Algorithm A_t can be constructed in time $O(n \log n)$ using $O(n)$ extra space.

We comment that D can be as large as $n - 1$, for example if the probabilities in π decrease exponentially. On a more positive note, if the distribution is supported on m elements, then we can replace n by m in Theorem 5.2, assuming we are given a list of these elements.

Section organization. We present our proof of the first part of Theorem 5.1 in Section 5.1. In Section 5.2 we show how to slightly modify the argument of the preceding section in order to prove the second part of Theorem 5.1. We discuss an efficient implementation of Algorithm A_t in Section 5.3, thus sketching the proof of Theorem 5.2.

5.1 Algorithm A_t and its analysis

In this subsection we prove the first part of Theorem 5.1 by exhibiting Algorithm A_t, a natural and simple algorithm that achieves redundancy 1 using only comparison and equality queries.

Notation. Let π be a distribution over X_n. Let $x_{\max}$ denote the most probable element, and let $\pi_{\max}$ denote its probability. Let x_{mid} denote a point x_i that minimizes $|\pi(\{x : x \prec x_i\}) - 1/2|$ over $i \in [n]$. We call x_{mid} the middle[4] of π. Note that the query "$x \succeq x_{\text{mid}}$?" is the most balanced query among all queries of the form "$x \prec x_i$?", .

Let $A \subseteq \{x_1, \ldots, x_n\}$. We use π_A to denote $\pi(A)$; i.e. the probability of A. Specifically, we use $\pi_{\prec x_i}, \pi_{\succeq x_i}, \pi_{\neq x_i}$ to denote π_A when A is $\{x : x \prec x_i\}, \{x : x \succeq x_i\}, \{x : x \neq x_i\}$. We use $\pi|_A$ to denote the restriction of π to A; i.e., the distribution derived by conditioning π on A. Specifically, we use $\pi|_{\prec x_i}, \pi|_{\succeq x_i}, \pi|_{\neq x_i}$ to denote $\pi|_A$ when A is $\{x : x \prec x_i\}, \{x : x \succeq x_i\}, \{x : x \neq x_i\}$.

Algorithm A_t. Given a threshold $t \in (0, 1)$, Algorithm A_t takes as input a distribution π over X_n and a secret element x, and determines x using only comparison and equality queries, in the following recursive fashion:

1. If $\pi(x_i) = 1$ for some element x_i, then output x_i.
2. If $\pi_{\max} \geq t$ then ask whether $x = x_{\max}$, and either output $x_{\max}$, or continue with $\pi|_{\neq x_{\max}}$.
3. If $\pi_{\max} < t$, ask whether $x \prec x_{\text{mid}}$, and continue with either $\pi|_{\prec x_{\text{mid}}}$ or $\pi|_{\succeq x_{\text{mid}}}$.

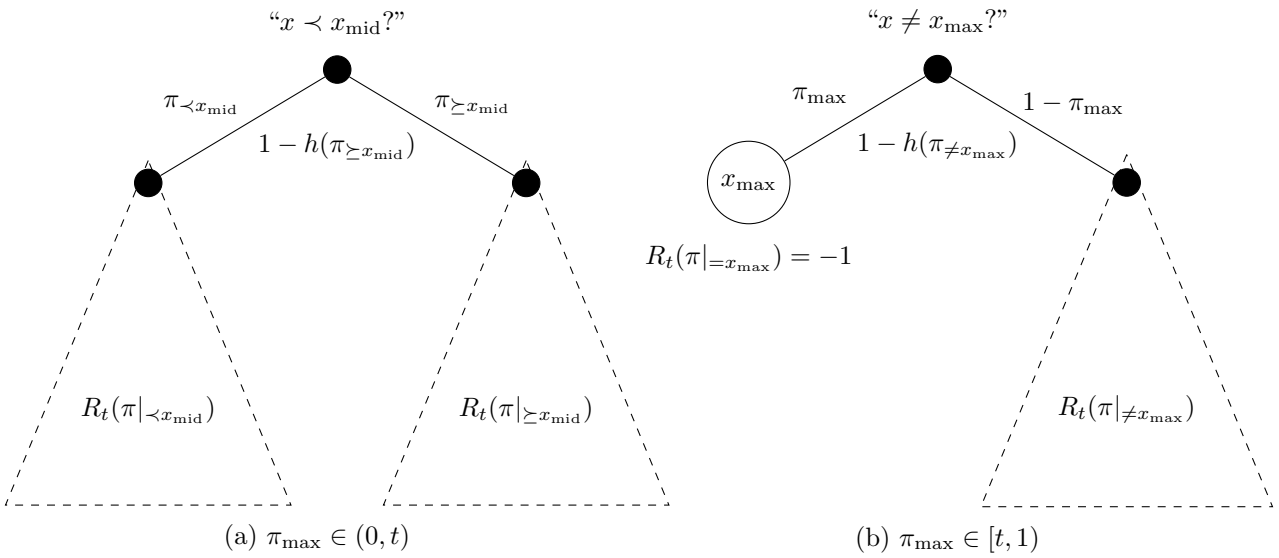
(When recursing on a domain D, we identify D with $X_{|D|}$.) ◁

The weight balancing algorithm of Rissanen [Ris73] is the special case $t = 1$; in this case no equality queries are needed, and the resulting redundancy is 2, as shown by Horibe [Hor77].

We will show that for a certain range of values of t (for example, $t = 0.3$), Algorithm A_t achieves redundancy at most 1, thus proving Theorem 5.1.

Recall that $A_t(\pi)$ is the cost of A_t on π, and let $R_t(\pi) := A_t(\pi) - H(\pi) - 1$. It is more convenient to present the proof in terms of $R_t(\pi)$ rather than in terms of the redundancy. Our goal, stated in these terms, is showing that there exists some t for which $R_t(\pi) \leq 0$ for all distributions π.

[4]Note that one of $\{x_{\text{mid}}, x_{\text{mid}-1}\}$ is a median.



(a) $\pi_{\max} \in (0, t)$ (b) $\pi_{\max} \in [t, 1)$

Figure 1: Recursive definition of R_t

We next observe two simple properties of the algorithm A_t. The proof of Theorem 5.1 relies only on these properties.

The first property is a recursive definition of R_t that is convenient to induct on. See Figure 1 for a pictorial illustration.

Lemma 5.1.1. *Let π be a distribution over X_n. Then*

$$R_t(\pi) = \begin{cases} -1 & \text{if } \pi_{\max} = 1, \\ 1 - h(\pi_{\max}) - \pi_{\max} + (1 - \pi_{\max}) R_t(\pi|_{\neq x_{\max}}) & \text{if } \pi_{\max} \in [t, 1), \\ 1 - h(\pi_{\prec x_{\text{mid}}}) + \pi_{\prec x_{\text{mid}}} R_t(\pi|_{\prec x_{\text{mid}}}) + \pi_{\succeq x_{\text{mid}}} R_t(\pi|_{\succeq x_{\text{mid}}}) & \text{if } \pi_{\max} \in (0, t). \end{cases}$$

Proof. If $\pi_{\max} = 1$ then $A_t(\pi) = 0$ and $H(\pi) = 0$, so $R_t(\pi) = -1$.

If $\pi_{\max} \in [t, 1)$ then

$$\begin{aligned} R_t(\pi) &= A_t(\pi) - H(\pi) - 1 \\ &= \Big[1 + (1 - \pi_{\max}) A_t(\pi|_{\neq x_{\max}})\Big] - \Big[h(\pi_{\max}) + (1 - \pi_{\max}) H(\pi|_{\neq x_{\max}})\Big] - \Big[\pi_{\max} + (1 - \pi_{\max})\Big] \\ &= 1 - h(\pi_{\max}) - \pi_{\max} + (1 - \pi_{\max})\Big[A_t(\pi|_{\neq x_{\max}}) - H(\pi|_{\neq x_{\max}}) - 1\Big] \\ &= 1 - h(\pi_{\max}) - \pi_{\max} + (1 - \pi_{\max}) R_t(\pi_{\neq x_{\max}}). \end{aligned}$$

If $\pi_{\max} \in (0, t)$ then

$$\begin{aligned} R_t(\pi) &= A_t(\pi) - H(\pi) - 1 \\ &= \Big[1 + \pi_{\prec x_{\text{mid}}} A_t(\pi|_{\prec x_{\text{mid}}}) + \pi_{\succeq x_{\text{mid}}} A_t(\pi|_{\succeq x_{\text{mid}}})\Big] \\ &\quad - \Big[h(\pi_{\prec x_{\text{mid}}}) + \pi_{\prec x_{\text{mid}}} H(\pi|_{\prec x_{\text{mid}}}) + \pi_{\succeq x_{\text{mid}}} H(\pi|_{\succeq x_{\text{mid}}})\Big] - \Big[\pi_{\prec x_{\text{mid}}} + \pi_{\succeq x_{\text{mid}}}\Big] \\ &= 1 - h(\pi_{\prec x_{\text{mid}}}) + \pi_{\prec x_{\text{mid}}}\Big[A_t(\pi|_{\prec x_{\text{mid}}}) - H(\pi|_{\prec x_{\text{mid}}}) - 1\Big] + \pi_{\succeq x_{\text{mid}}}\Big[A_t(\pi|_{\succeq x_{\text{mid}}}) - H(\pi|_{\succeq x_{\text{mid}}}) - 1\Big] \\ &= 1 - h(\pi_{\prec x_{\text{mid}}}) + \pi_{\prec x_{\text{mid}}} R_t(\pi|_{\prec x_{\text{mid}}}) + \pi_{\succeq x_{\text{mid}}} R_t(\pi|_{\succeq x_{\text{mid}}}). \end{aligned}$$

□

The second property is that whenever A_t uses a comparison query (i.e. when $\pi_{\max} < t$), then this question is balanced:

Lemma 5.1.2. *Let π be a distribution over X_n. Then $\pi_{\prec x_{\mathrm{mid}}}, \pi_{\succeq x_{\mathrm{mid}}} \in [\frac{1-\pi_{\max}}{2}, \frac{1+\pi_{\max}}{2}]$.*

Proof. By the definition of x_{mid}, it suffices to show that there exists some j with $\pi_{\prec j} \in [\frac{1-\pi_{\max}}{2}, \frac{1+\pi_{\max}}{2}]$. Indeed, for all j, $\pi_{\prec j+1} - \pi_{\prec j} = \pi_j \leq \pi_{\max}$, and therefore, if j is the maximum element with $\pi_{\prec j} < \frac{1}{2}$ (possibly $j = 0$), then either $\pi_{\prec j}$ or $\pi_{\prec j+1}$ are in $[\frac{1-\pi_{\max}}{2}, \frac{1+\pi_{\max}}{2}]$. □

We next use these properties to bound $R_t(\pi)$, and conclude the first part of Theorem 5.1. Since this involves quantifying over all distributions π, it is convenient to introduce a game that simulates A_t on a distribution π. The game involves one player, Alice, who we think of as an adversary that chooses the input distribution π (in fact, she only chooses $\pi_{\max}$), and wins a revenue of $R_t(\pi)$ (thus, her objective is to maximize the redundancy). This reduces our goal to showing that Alice's optimum revenue is nonpositive. The definition of the game is tailored to the properties stated in Lemma 5.1.1 and Lemma 5.1.2. We first introduce G_t, and then relate it to the redundancy of A_t (see Lemma 5.1.6 below).

Game G_t. Let $t \leq \frac{1}{3}$, and let $f, s\colon (0,1] \to \mathbb{R}$ be $f(x) := 1 - h(x) - x$ and $s(x) := 1 - h(x)$. The game G_t consists of one player called Alice, whose objective is to maximize her revenue. The game G_t begins at an initial state $p \in (0,1]$, and proceeds as follows.

1. If $p \in [t, 1]$, the game ends with revenue $f(p)$.
2. If $p \in (0, t)$, then Alice chooses a state[5] $p' \in \left[\frac{2p}{1+p}, \frac{2p}{1-p}\right]$ and recursively plays G_t with initial state p'. Let r' denote her revenue in the game that begins at p'. Alice's final revenue is

$$s\left(\frac{p}{p'}\right) + \frac{p}{p'} \cdot r'.$$

◁

Note that given any initial state p and a strategy for Alice, the game G_t always terminates: indeed, if $p = p_0, p_1, p_2, \ldots$ is the sequence of states chosen by Alice, then as long as $p_i < t$, it holds that $p_{i+1} \geq \frac{2p_i}{1+p_i} > \frac{2p_i}{1+1/3} = \frac{3}{2}p_i$ (the second inequality is since $p_i < t \leq \frac{1}{3}$). So the sequence of states grows at an exponential rate, which means that for $\ell = O(\log(1/p_0))$, the state p_ℓ exceeds the threshold t and the game terminates.

For $p \in (0,1]$, let $r_t(p)$ denote the supremum of Alice's revenue in G_t when the initial state is p, the supremum ranging over all possible strategies for Alice.

Our next step is using the game G_t to prove Theorem 5.1: We will show that $t = 0.3$ satisfies:

(i) $r_t(p) \leq 0$ for all $p \in (0,1]$, and

(ii) $R_t(\pi) \leq r_t(\pi_{\max})$ for all π.

Note that (i) and (ii) imply Theorem 5.1. Before establishing (i) and (ii), we state and prove three simple lemmas regarding G_t that are useful to this end.

The first lemma will be used in the proof of Lemma 5.1.6, which shows that if $r_t(p) \leq 0$ for all $p \in (0,1]$, then $R_t(\pi) \leq r_t(\pi_{\max})$. Its proof follows directly from the definition of r_t.

[5]Note that $p' \in (0,1]$, since $p < t \leq \frac{1}{3}$ implies that $\left[\frac{2p}{1+p}, \frac{2p}{1-p}\right] \subseteq (0,1]$.

Lemma 5.1.3. *For all $p < t$ and all $p' \in \left[\frac{2p}{1+p}, \frac{2p}{1-p}\right]$:*

$$r_t(p) \geq s\left(\frac{p}{p'}\right) + \frac{p}{p'} \cdot r_t(p').$$

The next two lemmas will be used in the proof of Lemma 5.1.7, which shows that $r_t(p) \leq 0$ for all $p \in (0, 1]$ when $t = 0.3$. The first one gives a tighter estimate on the growth of the sequence of states:

Lemma 5.1.4. *Let $p_0, p_1, \ldots, p_k$ be the sequence of states chosen by Alice. For every $i \leq k-1$:*

$$p_{k-1-i} < \frac{t}{2^i(1-t)+t}.$$

Proof. We prove the bound by induction on i. The case $i = 0$ follows from p_{k-1} being a non-final state, and therefore $p_{k-1} < t$ as required. Assume now that $i > 0$. By the definition of G_t it follows that $p_{k-1-(i-1)} \in \left[\frac{2p_{k-1-i}}{1+p_{k-1-i}}, \frac{2p_{k-1-i}}{1-p_{k-1-i}}\right]$, which implies that $p_{k-1-i} \in \left[\frac{p_{k-1-(i-1)}}{2+p_{k-1-(i-1)}}, \frac{p_{k-1-(i-1)}}{2-p_{k-1-(i-1)}}\right]$. Therefore,

$$\begin{aligned}
p_{k-1-i} &\leq \frac{p_{k-1-(i-1)}}{2 - p_{k-1-(i-1)}} \\
&< \frac{t/\big(2^{i-1}(1-t)+t\big)}{2 - t/\big(2^{i-1}(1-t)+t\big)} && \text{(by induction hypothesis on } i-1\text{)} \\
&= \frac{t}{2^i(1-t)+t}. && \square
\end{aligned}$$

The second lemma gives a somewhat more explicit form of the revenue of G_t:

Lemma 5.1.5. *Let $p_0, p_1, \ldots, p_k$ be the sequence of states chosen by Alice. Let $r(p_0, \ldots, p_k)$ denote the revenue obtained by choosing these states. Then*

$$r(p_0, \ldots, p_k) = \sum_{i=0}^{k-1} \frac{p_0}{p_i} s\left(\frac{p_i}{p_{i+1}}\right) + \frac{p_0}{p_k} f(p_k).$$

Proof. We prove the formula by induction on k. If $k = 0$ then $p_k \geq t$ and $r(p_k) = f(p_k) = \frac{p_0}{p_k} f(p_k)$. When $k \geq 1$:

$$\begin{aligned}
r(p_0, \ldots, p_k) &= s\left(\frac{p_0}{p_1}\right) + \frac{p_0}{p_1} \cdot r(p_1, \ldots, p_k) && \text{(by definition of } G_t\text{)} \\
&= \frac{p_0}{p_0} s\left(\frac{p_0}{p_1}\right) + \frac{p_0}{p_1} \cdot \left(\sum_{i=1}^{k-1} \frac{p_1}{p_i} s\left(\frac{p_i}{p_{i+1}}\right) + \frac{p_1}{p_k} f(p_k)\right) && \text{(by induction hypothesis)} \\
&= \sum_{i=0}^{k-1} \frac{p_0}{p_i} s\left(\frac{p_i}{p_{i+1}}\right) + \frac{p_0}{p_k} f(p_k). && \square
\end{aligned}$$

Relating A_t to G_t. Next, we relate the revenue in G_t to the redundancy of A_t by linking r_t and R_t. We first reduce the first part of Theorem 5.1 to showing that there exists some $t \in (0, 1]$ such that $r_t(p) \leq 0$ for all $p \in (0, 1]$ (Lemma 5.1.6), and then show that $t = 0.3$ satisfies this condition (Lemma 5.1.7).

Lemma 5.1.6. *Let t be such that $r_t(p) \leq 0$ for all $p \in (0,1]$. For every distribution π,*

$$R_t(\pi) \leq r_t(\pi_{\max}).$$

In particular, such t satisfies $R_t(\pi) \leq 0$ for all π.

Proof. We proceed by induction on the size of $\mathrm{supp}(\pi) = \{x_i : \pi(x_i) \neq 0\}$. If $\left|\mathrm{supp}(\pi)\right| = 1$ then $\pi_{\max} = 1$, and therefore $R_t(\pi) = -1$, $r_t(\pi_{\max}) = 0$, and indeed $R_t(\pi) \leq r_t(\pi_{\max})$. Assume now that $\left|\mathrm{supp}(\pi)\right| = k > 1$. Since $k > 1$, it follows that $\pi_{\max} < 1$. There are two cases, according to whether $\pi_{\max} \in (0,t)$ or $\pi_{\max} \in [t,1)$.

If $\pi_{\max} \in (0,t)$ then A_t asks whether $x \prec x_{\mathrm{mid}}$, and continues accordingly with $\pi|_{\prec x_{\mathrm{mid}}}$ or $\pi|_{\succeq x_{\mathrm{mid}}}$. Let $\sigma := \pi|_{\prec x_{\mathrm{mid}}}$ and $\tau := \pi|_{\succeq x_{\mathrm{mid}}}$. By Lemma 5.1.1:

$$\begin{aligned}
R_t(\pi) &= 1 - h(\pi_{\prec x_{\mathrm{mid}}}) + \pi_{\prec x_{\mathrm{mid}}} R_t(\sigma) + \pi_{\succeq x_{\mathrm{mid}}} R_t(\tau) && \text{(since } \pi_{\max} \in (0,t)\text{)} \\
&\leq 1 - h(\pi_{\prec x_{\mathrm{mid}}}) + \pi_{\prec x_{\mathrm{mid}}} r_t(\sigma_{\max}) + \pi_{\succeq x_{\mathrm{mid}}} r_t(\tau_{\max}) && \text{(by induction hypothesis)}
\end{aligned}$$

Without loss of generality, assume that $x_{\max} \prec x_{\mathrm{mid}}$. Therefore $\sigma_{\max} = \pi_{\max}/\pi_{\prec x_{\mathrm{mid}}}$, and by Lemma 5.1.2:

$$\sigma_{\max} \in \left[\frac{2\pi_{\max}}{1+\pi_{\max}}, \frac{2\pi_{\max}}{1-\pi_{\max}}\right]. \tag{1}$$

Thus,

$$\begin{aligned}
R_t(\pi) &\leq 1 - h(\pi_{\prec x_{\mathrm{mid}}}) + \pi_{\prec x_{\mathrm{mid}}} r_t(\sigma_{\max}) && \text{(since } r_t(\tau_{\max}) \leq 0\text{)} \\
&= 1 - h\left(\frac{\pi_{\max}}{\sigma_{\max}}\right) + \frac{\pi_{\max}}{\sigma_{\max}} r_t(\sigma_{\max}) && \text{(}\sigma_{\max} = \tfrac{\pi_{\max}}{\pi_{\prec x_{\mathrm{mid}}}}\text{)} \\
&= s\left(\frac{\pi_{\max}}{\sigma_{\max}}\right) + \frac{\pi_{\max}}{\sigma_{\max}} r_t(\sigma_{\max}) && \text{(by definition of } s\text{)} \\
&\leq r_t(\pi_{\max}). && \text{(by (1) and Lemma 5.1.3)}
\end{aligned}$$

The analysis when $\pi_{\max} \in [t,1)$ is very similar. In this case A_t asks whether $x = x_{\max}$, and continues with $\pi|_{\neq x_{\max}}$ if $x \neq x_{\max}$. Let $\sigma := \pi|_{\leq x_{\max}}$. By Lemma 5.1.1,

$$\begin{aligned}
R_t(\pi) &= 1 - h(\pi_{\max}) - \pi_{\max} + (1-\pi_{\max}) R_t(\sigma) && \text{(since } \pi_{\max} \in (t,1)\text{)} \\
&\leq 1 - h(\pi_{\max}) - \pi_{\max} + (1-\pi_{\max}) r_t(\sigma_{\max}) && \text{(by induction hypothesis)} \\
&\leq 1 - h(\pi_{\max}) - \pi_{\max} && \text{(since } r_t(\sigma_{\max}) \leq 0\text{)} \\
&= f(\pi_{\max}) && \text{(by definition of } f\text{)} \\
&= r_t(\pi_{\max}). && \text{(by definition of } r_t\text{, since } \pi_{\max} \geq t\text{)}
\end{aligned}$$

□

The following lemma shows that $t = 0.3$ satisfies $r_t(p) \leq 0$ for all $p \in (0,1]$, completing the proof of the first part of Theorem 5.1. It uses some technical results, proved below in Lemma 5.1.8.

Lemma 5.1.7. *Let $t = 0.3$. Then $r_t(p) \leq 0$ for all $p \in (0,1]$.*

Proof. Let $p \in (0,1]$. We consider two cases: (i) $p \geq t$, and (ii) $p < t$. In each case we derive a constraint on t that suffices for ensuring that $r_t(p) \leq 0$, and conclude the proof by showing that $t = 0.3$ satisfies both constraints.

Consider the case $t \le p$. Here $r_t(p) = f(p) = 1 - h(p) - p$, and calculation shows that $f(p)$ is non-positive on $[0.23, 1]$; therefore, $r_t(p) \le 0$ for all $p \ge t$, as long as $t \ge 0.23$.

Consider the case $p < t$. Here, we are not aware of an explicit formula for $r_t(p)$; instead, we derive the following upper bound, for all $p < t$:

$$\frac{r_t(p)}{p} \le \sum_{n=0}^{\infty} S\left(\frac{t}{2^n(1-t)+t}\right) + \max\left(F(t), F\Big(\frac{2t}{1-t}\Big)\right), \tag{2}$$

where

$$S(x) = \frac{s\Big(\frac{1+x}{2}\Big)}{x}, \qquad F(x) = \frac{f(x)}{x}.$$

With (2) in hand we are done: indeed, calculation shows that the right hand side of (2) is non-positive in some neighborhood of 0.3 (e.g. it is -0.0312 when $t = 0.3$, it is -0.0899 when $t = 0.294$); thus, as these values of t also satisfy the constraint from (i), this finishes the proof.

It remains to prove (2). Let $p = p_0, p_1, p_2, \ldots, p_k$ be a sequence of states chosen by Alice. It suffices to show that $\frac{r(p_0,\ldots,p_k)}{p_0} \le \sum_{n=0}^{\infty} S\left(\frac{t}{2^n(1-t)+t}\right) + \max\left(F(t), F\left(\frac{2t}{1-t}\right)\right)$. By Lemma 5.1.5:

$$\begin{aligned} r(p_0, \ldots, p_k) &= \sum_{i=0}^{k-1} \frac{p_0}{p_i} s\left(\frac{p_i}{p_{i+1}}\right) + \frac{p_0}{p_k} f(p_k) \\ &\le \sum_{i=0}^{k-1} \frac{p_0}{p_i} s\left(\frac{1+p_i}{2}\right) + \frac{p_0}{p_k} f(p_k) \\ &= p_0\Big(\sum_{i=0}^{k-1} S(p_i) + F(p_k)\Big), \end{aligned}$$

where in the second line we used that $\frac{p_i}{p_{i+1}} \in [\frac{1-p_i}{2}, \frac{1+p_i}{2}]$, and the fact that $s(x) = 1 - h(x)$ is symmetric around $x = 0.5$ and increases with $|x - 0.5|$. Therefore,

$$\begin{aligned} \frac{r(p_0, \ldots, p_k)}{p_0} &\le \sum_{i=0}^{k-1} S(p_i) + F(p_k) \\ &\le \sum_{i=0}^{k-1} S\left(\frac{t}{2^i(1-t)+t}\right) + F(p_k) \\ &\le \sum_{i=0}^{\infty} S\left(\frac{t}{2^i(1-t)+t}\right) + \max\left(F(t), F\Big(\frac{2t}{1-t}\Big)\right), \end{aligned}$$

where in the second last inequality we used that $p_{k-1-i} < \frac{t}{2^i(1-t)+t}$ (Lemma 5.1.4) and that $S(x)$ is monotone (Lemma 5.1.8 below), and in the last inequality we used that $p_k \in [t, \frac{2t}{1-t})$ and that $F(x)$ is convex (Lemma 5.1.8 below). □

The following technical lemma completes the proof of Lemma 5.1.7.

Lemma 5.1.8. *The function $S(x) = \frac{1-h(\frac{1+x}{2})}{x}$ is monotone, and the function $F(x) = \frac{1-h(x)-x}{x}$ is convex.*

Proof. The function $h(\frac{1-x}{2})$ is equal to its Maclaurin series for $x \in (-1,+1)$:

$$h\Big(\frac{1+x}{2}\Big) = 1 - \sum_{k=1}^{\infty} \frac{\log_2 e}{2k(2k-1)} \cdot x^{2k}.$$

Therefore,

$$S(x) = \sum_{k=1}^{\infty} \frac{\log_2 e}{2k(2k-1)} \cdot x^{2k-1},$$

and

$$F(x) = \Big(\sum_{k=1}^{\infty} \frac{\log_2 e}{2k(2k-1)} \cdot \frac{(1-2x)^{2k}}{x}\Big) - 1.$$

Now, each of the functions x^{2k-1} is monotone, and each of the functions $\frac{(1-2x)^{2k}}{x}$ is convex on $(0,\infty)$: its second derivative is

$$\frac{2(1-2x)^{2k-2}(1+4(k-1)x+4(k-1)(2k-1)x^2)}{x^3} > 0.$$

Therefore, $S(x)$ is monotone as a non-negative combination of monotone functions, and $F(x)$ is convex as a non-negative combination of convex functions. □

5.2 Improved analysis when $\pi_{\max} \ll 1$

The proof of the first part of Theorem 5.1 shows that for $t = 0.3$ the redundancy of Algorithm A_t is at most 1. Intuitively, the hardest distributions are those with $\pi_{\max}$ very close to 1 (these distributions have entropy close to 0, and so even an optimal algorithm has redundancy close to 1 on these distributions), and it is plausible that A_t has smaller redundancy on distributions with $\pi_{\max}$ that is not too close to 1. However, our proof of Lemma 5.1.7 only shows that the redundancy is $1 - \Omega(\pi_{\max})$.

In this subsection, we complete the proof of Theorem 5.1 by discussing how our analysis can be slightly tweaked in order to show that if $\pi_{\max} \le 0.99611$ then the limiting redundancy is $\alpha - \Omega(\pi_{\max})$, where $\alpha = 0.96711$. We only restate the lemmas with the required modifications, and do not provide complete proofs.

Let $R_t^{(\alpha)}(\pi) = A(\pi) - H(\pi) - \alpha$. The following lemma is the counterpart of Lemma 5.1.1.

Lemma (Counterpart of Lemma 5.1.1)**.** *Let π be a distribution over X_n. Then*

$$R_t^{(\alpha)}(\pi) = \begin{cases} -\alpha & \text{if } \pi_{\max} = 1, \\ 1 - h(\pi_{\max}) - \pi_{\max} \cdot \alpha + (1-\pi_{\max}) R_t^{(\alpha)}(\pi|_{\neq x_{\max}}) & \text{if } \pi_{\max} \in [t,1), \\ 1 - h(\pi_{\prec x_{\mathrm{mid}}}) + \pi_{\prec x_{\mathrm{mid}}} R_t^{(\alpha)}(\pi|_{\prec x_{\mathrm{mid}}}) + \pi_{\succeq x_{\mathrm{mid}}} R_t^{(\alpha)}(\pi|_{\succeq x_{\mathrm{mid}}}) & \text{if } \pi_{\max} \in (0,t). \end{cases}$$

The proof of this lemma is an almost verbatim adaptation of the original proof.

The next step is adapting the game G_t so that an analog of Lemma 5.1.6 holds. Here the change is that the function $f(x)$ is modified to

$$f^{(\alpha)}(x) = 2 - \alpha - h(x) - x.$$

Note that when $\alpha = 1$ it reduces to the original $f(x)$. Let $r_t^{(\alpha)}(p)$ be the counterpart of $r_t(p)$.

The following lemma is the counterpart of Lemma 5.1.6, which relates $R_t^{(\alpha)}$ and $r_t^{(\alpha)}$.

Lemma (Counterpart of Lemma 5.1.6)**.** *Let t be such that $r_t(p) \le 0$ for all $p \in (0,1]$, and $r_t^{(\alpha)}(p) \le 0$ for all $p \in (0,q]$, with $q \ge \frac{2t}{1-t}$. Then for every π with $\pi_{\max} \in (0,q]$:*

$$R_t^{(\alpha)}(\pi) \le r_t^{(\alpha)}(\pi_{\max}).$$

In particular, $R_t^{(\alpha)}(\pi) \le 0$ for all π with $\pi_{\max} \in (0,q]$.

Proof sketch. The proof is very similar to the proof of Lemma 5.1.6, and uses a similar induction. However, there is a subtlety here when applying the induction hypothesis: the induction hypothesis applies only to distributions π for which $\pi_{\max} \in (0,q]$. In the first case considered by the proof, $\pi_{\max} \in (0,t)$, and both $\tau_{\max}, \sigma_{\max} \le \frac{2t}{1-t} \le q$, and the induction hypothesis applies. In the second case, when $\pi_{\max} \ge t$, it could be that $\sigma_{\max} > q$, and the induction hypothesis does not apply. Instead, we use the assumption that $r_t(p) \le 0$ for $p \in (0,1]$, and bound $R_t^{(\alpha)}(\sigma)$ as follows:

$$\begin{aligned} R_t^{(\alpha)}(\sigma) &= R_t(\sigma) + 1 - \alpha \\ &\le r_t(\sigma_{\max}) + 1 - \alpha && \text{(By Lemma 5.1.6, since } r_t(p) \le 0 \text{ for } p \in (0,1]) \\ &\le 1 - \alpha. && \text{(since } r_t(\sigma_{\max}) \le 0) \end{aligned}$$

Thus

$$R_t^{(\alpha)}(\pi) \le 1 - h(\pi_{\max}) - \pi_{\max}\alpha + (1-\pi_{\max})(1-\alpha) = f^{(\alpha)}(\pi_{\max}). \qquad \square$$

Finally, the following lemma is the counterpart of Lemma 5.1.7, and its proof is very similar to the original proof.

Lemma (Counterpart of Lemma 5.1.7)**.** *Let $\alpha = 0.96711$, and let $t = 0.299395$. Then $r_t(p) \le 0$ for all $p \in (0,1]$, and $r_t^{(\alpha)}(p) \le 0$ for all $p \le 0.9961$.*

Proof sketch. For the proof, let $F^{(\alpha)}(x) = f^{(\alpha)}(x)/x$, and note that $F^{(\alpha)}(x) = F(x) + (1-\alpha)/x$ is convex, being the sum of two convex functions. When $p < t$, we can estimate as in Lemma 5.1.7:

$$\frac{r_t^{(\alpha)}(p)}{p} \le \sum_{n=0}^{\infty} S\left(\frac{t}{2^n(1-t)+t}\right) + \max\left(F^{(\alpha)}(t), F^{(\alpha)}\left(\frac{2t}{1-t}\right)\right) \approx -6.896 \times 10^{-6} < 0.$$

When $p \ge t$, $r_t^{(\alpha)}(p) = f^{(\alpha)}(p)$, and one checks that $f^{(\alpha)}(p) \le 0$ when $t \le p \le 0.9961$ directly, using the convexity of $f^{(\alpha)}(p)$ (which follows from the concavity of $h(p)$). $\square$

Since $0.9961 \ge \frac{2t}{1-t} \approx 0.85$, it follows that $A_t(\pi) \le H(\pi) + 0.96711$ whenever $\pi_{\max} \le 0.9961$, where $t = 0.299395$. This completes the proof of the second part of Theorem 5.1.

5.3 Implementing Algorithm A_t

A naive implementation of Algorithm A_t requires $O(n)$ work per question. However, using an appropriate data structure, we can construct the decision tree corresponding to the algorithm in time $O(n \log n)$.

The appropriate data structure, which we coin *Sum-Max-Tree*, is a dynamic array which supports the following operations:

init$(\pi_1, \ldots, \pi_n)$ Stores weight π_i under the key i for $1 \le i \le n$.

get-max(a, b) Returns the key i in the range $a \le i \le b$ maximizing π_i.

get-sum(a, b) Returns the total weight of elements whose keys are between a and b.

get-mid(a, b) Returns the key m which minimizes

$$\left| \sum_{i:\ a \le i \le m} \pi_i - \sum_{i:\ m < i \le b} \pi_i \right|.$$

remove(i) Removes the element with key i.

Lemma 5.3.1. *Sum-Max-Tree can be implemented so that* ***init*** *takes time $O(n)$, and all other operations take time $O(\log n)$. Furthermore, the space used is $O(n)$.*

Proof sketch. The operation **init** constructs a nearly complete binary tree (all leaves are at depth $\lfloor \log n \rfloor$ or $\lceil \log n \rceil$) in which the weights π_i are stored at the leaves, ordered by their key. Each internal node stores the following auxiliary information about its subtree: the maximum weight of an element, and the total weight of all elements.

The operations **get-max** and **get-sum** are implemented by finding a set of $O(\log n)$ internal nodes whose subtrees partition the leaves $a, \ldots, b$. Details left to the reader.

The operation **get-mid** is implemented along the following lines. First compute $\sigma := \sum_{i:\ a \le i \le b} \pi_i$; our task is to find the key m that minimizes $|\sum_{i:\ a \le i \le m} \pi_i - \sigma/2|$. We will do so by finding the maximal key M satisfying $\sum_{i:\ a \le i \le M} \pi_i \le \sigma/2$, and then choosing the best of $M, M+1$.

Let v be the least common ancestor of the leaves containing the keys a and b. We find M by descending from v toward the leaves, maintaining the invariant that the current node contains M. Details left to the reader.

Finally, the operation **remove** first removes the appropriate leaf, and then updates the auxiliary information by walking from the leaf to the root: the total weight at each internal node $v = (v_L, v_R)$ is simply decreased by π_i, and the maximum weight is updated recursively using the formula $\max(v) = \max(\max(v_L), \max(v_R))$. □

Using this data structure, it is a simple exercise to prove Theorem 5.2.

6 Information theoretical benchmark — Shannon's entropy

In this section we study the minimum number of questions that achieve redundancy of at most r, for a fixed $r \ge 1$. Note that $r = 1$ is the optimal redundancy: the distribution π on X_2 given by $\pi_1 = 1 - \epsilon, \pi_2 = \epsilon$ has redundancy $1 - \tilde{O}(\epsilon)$ (that is, $1 - O(\epsilon \log(1/\epsilon))$ even without restricting the set of allowed questions.

In the previous section we have shown that the optimal redundancy of $r = 1$ can be achieved with just $2n$ comparison and equality queries (in fact, as we show below, there are only $2n - 3$ of these queries). It is natural to ask how small the number of questions can be if we allow for a larger r. Note that at least $\log n$ questions are necessary to achieve any finite redundancy. Indeed, a smaller set of questions is not capable of specifying all elements even if all questions are being asked.

The main result of this section is that the minimum number of questions that are sufficient for achieving redundancy r is roughly $r \cdot n^{1/\lfloor r \rfloor}$:

Theorem 6.1. *For every $r \ge 1$ and $n \in \mathbb{N}$,*

$$\frac{1}{e} \lfloor r \rfloor n^{1/\lfloor r \rfloor} \le u^H(n, r) \le 2 \lfloor r \rfloor n^{1/\lfloor r \rfloor}.$$

In particular, $u^H(n,r) = \Theta\big(\lfloor r \rfloor n^{1/\lfloor r \rfloor}\big)$.

The algorithm underlying the upper bound can be implemented efficiently, along the lines of Theorem 5.2; we leave the details to the reader.

Section organization. The upper bound in Theorem 6.1 is proved in Section 6.1, and the lower bound in Section 6.2. The lower bound proof uses (implicitly) the concept of *witness codes*, a connection we discuss in Section 6.3.

6.1 Upper bound

The upper bound in Theorem 6.1 is based on the following corollary of Theorem 5.1:

Theorem 6.1.1. *Let Y be a linearly ordered set, and let $Z = Y^k$ (we don't think of Z as ordered).*

For any distribution π on Z there is an algorithm that uses only questions of the form (i) "$\vec{x}_i \prec y$?" and (ii) "$\vec{x}_i = y$?", where $i \in [k]$ and $y \in Y$, whose cost is at most $H(\pi) + k$.

Proof. Let $Z_1 Z_2 \dots Z_k \sim \pi$. Consider the algorithm which determines $Z_1, \dots, Z_k$ in order, where Z_i is determined by applying the algorithm from Theorem 5.1 on "$Z_i | Z_1 \dots Z_{i-1}$", which is the conditional distribution of Z_i given the known values of $Z_1, \dots, Z_{i-1}$. The expected number of queries is at most

$$\big(H(Z_1) + 1\big) + \big(H(Z_2|Z_1) + 1\big) + \dots + \big(H(Z_k|Z_1 \dots Z_{k-1}) + 1\big) = H(Z_1 \dots Z_k) + k,$$

using the chain rule. □

We use this theorem to construct a set of questions of size at most $2\lfloor r \rfloor n^{1/\lfloor r \rfloor}$ that achieves redundancy r for any distribution over X_n.

Note that $n \leq \left(\lceil n^{1/\lfloor r \rfloor} \rceil\right)^{\lfloor r \rfloor}$. Therefore every element $x \in X_n$ can be represented by a vector $\vec{x} \in \left\{1, \dots, \lceil n^{1/\lfloor r \rfloor} \rceil\right\}^{\lfloor r \rfloor}$. Let $\mathcal{Q}$ be the set containing all questions of the form (i) "$\vec{x}_i = y$?" and (ii) "$\vec{x}_i \prec y$?". By Theorem 6.1.1, $r(\mathcal{Q}) = \lfloor r \rfloor$.

The following questions from $\mathcal{Q}$ are redundant, and can be removed from $\mathcal{Q}$ without increasing its redundancy: (i) "$\vec{x}_i \prec 1$?" (corresponds to the empty set and therefore provides no information), (ii) "$\vec{x}_i \prec 2$?" (equivalent to the question "$\vec{x}_i = 1$?"), and (iii) "$\vec{x}_i \prec \lceil n^{1/\lfloor r \rfloor} \rceil$?" (equivalent to the question "$\vec{x}_i = \lceil n^{1/\lfloor r \rfloor} \rceil$?"). The number of remaining questions is

$$\lfloor r \rfloor \cdot \left(2\lceil n^{1/\lfloor r \rfloor} \rceil - 3\right) \leq 2\lfloor r \rfloor \cdot \left(n^{1/\lfloor r \rfloor}\right).$$

This proves the upper bound in Theorem 6.1.

6.2 Lower bound

The crux of the proof of the lower bound in Theorem 6.1 is that if $\mathcal{Q}$ is a set of questions whose redundancy is at most r then every $x \in X_n$ can be identified by at most $\lfloor r \rfloor$ questions from $\mathcal{Q}$.

We say that the questions $q_1, \dots, q_T$ *identify* x if for every $y \neq x$ there is some $i \leq T$ such that $q_i(x) \neq q_i(y)$. Define $t(n,r)$ to be the minimum cardinality of a set $\mathcal{Q}$ of questions such that every $x \in X$ has at most r questions in $\mathcal{Q}$ that identify it. The quantity $t(n,r)$ can be thought of as a non-deterministic version of $u(n,r)$: it is the minimal size of a set of questions so that every element can be "verified" using at most r questions.

The lower bound on $u(n,r)$ follows from Lemma 6.2.1 and Lemma 6.2.2 below.

Lemma 6.2.1. *For all n, r, $u(n,r) \geq t(n, \lfloor r \rfloor)$.*

Proof. It suffices to show that for every set of questions $\mathcal{Q}$ with redundancy at most r, every $x \in X$ has at most $\lfloor r \rfloor$ questions in $\mathcal{Q}$ that identify it.

Consider the distribution π given by $\pi(x) = 1 - \epsilon$ and $\pi(y) = \epsilon/(n-1)$ for $y \neq x$. Thus $H(\pi) = \tilde{O}(\epsilon)$. Consider an algorithm for π with redundancy r that uses only questions from $\mathcal{Q}$. Let T be the number of questions it uses to find x. The cost of the algorithm is at least $(1-\epsilon)T$, and so $(1-\epsilon)T \leq H(\pi) + r = \tilde{O}(\epsilon) + r$, implying $T \leq \tilde{O}(\epsilon) + (1 + \frac{\epsilon}{1-\epsilon})r$. For small enough $\epsilon > 0$, the right-hand side is smaller than $\lfloor r \rfloor + 1$, and so $T \leq \lfloor r \rfloor$. □

Lemma 6.2.1 says that in order to lower bound $u(n,r)$, it suffices to lower bound $t(n, \lfloor r \rfloor)$, which is easier to handle. For example, the following straightforward argument shows that $t(n,R) \geq \frac{1}{2e} R n^{1/R}$, for every $R, n \in \mathbb{N}$. Assume $\mathcal{Q}$ is a set of questions of size $u(n,R)$ so that every x is identified by at most R questions. This implies an encoding (i.e. a one-to-one mapping) of $x \in X_n$ by the R questions identifying it, and by the bits indicating whether x satisfies each of these questions. Therefore

$$n \leq \binom{|\mathcal{Q}|}{\leq R} 2^R \leq \left(\frac{2e|\mathcal{Q}|}{R}\right)^R,$$

where in the last inequality we used that $\binom{m}{\leq k} \leq \left(\frac{em}{k}\right)^k$ for all m, k. This implies that $t(n, \lfloor r \rfloor) \geq \frac{1}{2e} \lfloor r \rfloor n^{1/\lfloor r \rfloor}$. The constant $\frac{1}{2e}$ in front of $\lfloor r \rfloor n^{1/\lfloor r \rfloor}$ can be increased to $\frac{1}{e}$, using an algebraic argument:

Lemma 6.2.2. *For all $n, R \in \mathbb{N}$:*

$$t(n,R) \geq \frac{1}{e} R \cdot n^{1/R}.$$

Proof. We use the so-called polynomial method. Let $\mathcal{Q}$ be a set of questions such that each $x \in X$ can be identified by at most R queries. For each $x \in X$, let u_x be the $|\mathcal{Q}|$-dimensional vector $u_x = \big(q_1(x), \ldots, q_{|\mathcal{Q}|}(x)\big)$, and let $U = \{u_x : x \in X\} \subseteq \{0,1\}^{|\mathcal{Q}|}$. We will show that every function $F \colon U \to \mathbb{F}_2$ can be represented as a multilinear polynomial of degree at most R in $|\mathcal{Q}|$ variables. Since the dimension over $\mathbb{F}_2$ of all such functions is n, whereas the dimension of the space of all multilinear polynomials of degree at most R is $\binom{|\mathcal{Q}|}{\leq R}$, the bound follows:

$$n \leq \binom{|\mathcal{Q}|}{\leq R} \leq \left(\frac{e|\mathcal{Q}|}{R}\right)^R \Longrightarrow n \geq \frac{1}{e} R \cdot n^{1/R}.$$

It is enough to show that for any $u_x \in U$, the corresponding "delta function" $\delta_x \colon U \to \mathbb{F}_2$, defined as $\delta_x(u_x) = 1$ and $\delta_x(v) = 0$ for $u_x \neq v \in U$, can be represented as a polynomial of degree at most d. Suppose that $q_{i_1}, \ldots, q_{i_T}$ are $T \leq R$ questions that identify x. Consider the polynomial

$$P(y_1, \ldots, y_{|\mathcal{Q}|}) = (y_{i_1} - q_{i_1}(x) + 1) \cdots (y_{i_r} - q_{i_r}(x) + 1).$$

Clearly $P(u_x) = 1$. On the other hand, if $P(u_y) = 1$ then $q_{i_j}(y) = q_{i_j}(x)$ for all j, showing that $y = x$. So $P = \delta_x$, completing the proof. □

6.3 Witness codes and teaching dimension

Our proof of the lower bound in Theorem 6.1 is based on $t(n,R)$, which is the minimum cardinality of a set of queries such that each element can be identified by at most R questions. This quantity

is closely related to witness codes [Mes92, CRZ08]. In particular, as we will show, it is in some sense dual to the maximum size of a w-witness code.

A set $C \subseteq \{0,1\}^m$ is a *w-witness code* if for every $u \in C$ there exists $Y \subseteq [m]$ of size at most w such that every $v \in C$, if $v \neq u$ then $v|_Y \neq u|_Y$. The set Y is a *witness* of u. We define $f(m,w)$ as the maximum size of a set $C \subseteq \{0,1\}^m$ that is a w-witness code.

It is easy to see that for $w \leq m$, $f(m,w) \geq \binom{m}{w}$: indeed, consider the family of all vectors $u \in \{0,1\}^m$ of Hamming weight w. This family is of size $\binom{m}{w}$, and for every vector u it contains, the set $\{i : u(i) = 1\}$) is a witness of u. On the other hand, the proof of Lemma 6.2.2 shows that $f(m,w) \leq \binom{m}{\leq w}$.

Witness codes were first introduced by Aharoni and Holzman in unpublished work [AH91], in which they proved the bounds $\binom{m}{w} \leq f(m,w) \leq \binom{m}{\leq w}$ and conjectured that $f(m,w) = \binom{m}{w}$ whenever $m > 2w$. Meshulam [Mes92] proved their conjecture for $m \geq \gamma_0 w$, where $\gamma_0 \approx 9.0886$ satisfies $h(\gamma_0^{-1}) = 1/2$. Ellis [Ell11] simplified Meshulam's proof.

Witness codes were introduced again in the context of coding theory [CRZ08, Coh09, MM11, CM11], motivated by the concept of teaching dimension in learning theory [GK95, SM91, ABCS92, Kuh99, DSZ10, ZLHZ11, SSYZ14] and by Bondy's theorem and related results in combinatorics [Bon72, KLRS96, AH06] (see also Jukna [Juk01, §11]). Cohen et al. [CRZ08] also stated a version of the Aharoni–Holzman conjecture, unaware of Meshulam's work.

Duality. The quantities $f(m,w)$ and $t(n,w)$ are dual, in a sense that we now explain. We say that a binary matrix M is a w-witness matrix if for every row r in M there is a set Y of at most w columns such that $r|_Y \neq r'|_Y$ for every row $r' \neq r$. It is easy to verify that:

$f(m,w)$ is the maximum number of rows among all w-witness matrices with m columns,

$t(n,w)$ is the minimum number of columns among all w-witness matrices with n rows.

The duality between $f(m,w)$ and $t(n,w)$ is manifested in that swapping the pairs "maximum"/"minimum" and "columns"/"rows" transforms one definition to the other. In our context, we use the following lemma that translates between upper bounds on $f(m,w)$ and lower bounds on $t(n,w)$:

Lemma 6.2 (Duality)**.** *For all $n, m, w \in \mathbb{N}$:*

$$f(m,w) < n \iff t(n,w) > m\,.$$

Proof. The statement: "There exists no w-witness matrix with n rows and m columns" is equivalent to both statements. □

This lemma was implicitly used in the proof of Lemma 6.2.2, where it is in fact shown that $f(m,w) \leq \binom{m}{\leq w} < \left(\frac{em}{w}\right)^w$, and plugging $n = \left(\frac{em}{w}\right)^w$ (i.e. $m = \frac{1}{e} w \cdot n^{1/w}$) yields the bound. The bound $f(m,w) \leq \binom{m}{\leq w}$ was first proved by Aharoni and Holzman [AH91] in unpublished work, and reproduced by Ellis [Ell11]. It also follows from a stronger result concerning the recursive teaching dimension [SSYZ14]. All of these proofs are identical to the argument of Lemma 6.2.2.

7 Combinatorial benchmark — Huffman codes

Section 5 shows that the optimal redundancy, namely 1, can be achieved using only $O(n)$ questions. However, what if we want an *instance*-optimal algorithm? That is, we are looking for a set of questions which matches the performance of minimum redundancy codes such as Huffman codes.

Let us repeat the definition of an optimal set of questions that is central in this section.

Definition 7.1. A set $\mathcal{Q}$ of subsets of X_n is an *optimal set of questions over* X_n if for all distributions μ on X_n,

$$c(\mathcal{Q}, \mu) = \mathrm{Opt}(\mu).$$

Using the above definition, $u^{\mathrm{Opt}}(n, 0)$ is equal to the minimal size of an optimal set of questions over X_n. Perhaps surprisingly, the trivial upper bound of 2^{n-1} on $u^{\mathrm{Opt}}(n, 0)$ can be exponentially improved:

Theorem 7.2. *We have*

$$u^{\mathrm{Opt}}(n, 0) \leq 1.25^{n+o(n)}.$$

We prove a similar lower bound, which is almost tight for infinitely many n:

Theorem 7.3. *For n of the form $n = 5 \cdot 2^m$,*

$$u^{\mathrm{Opt}}(n, 0) \geq 1.25^n / O(\sqrt{n}).$$

For all n,

$$u^{\mathrm{Opt}}(n, 0) \geq 1.232^n / O(\sqrt{n}).$$

Corollary 7.4. *We have*

$$\limsup_{n \to \infty} \frac{\log u^{\mathrm{Opt}}(n, 0)}{n} = \log 1.25.$$

Unfortunately, the construction in Theorem 7.2 is not explicit. A different construction, which uses $O(\sqrt{2}^n)$ questions, is not only explicit, but can also be implemented efficiently:

Theorem 7.5. *There exists an explicit set of questions $\mathcal{Q}$ of size $2^{\lceil n/2 \rceil + 1}$ such that:*

1. *There is an indexing scheme $\mathcal{Q} = \{Q_q : q \in \{0,1\}^{\lceil n/2 \rceil + 1}\}$ such that given an index q and an element $x_i \in X_n$, we can decide whether $x_i \in Q_q$ in time $O(n)$.*
2. *Given a distribution π, we can construct an optimal decision tree for π using $\mathcal{Q}$ in time $O(n^2)$.*
3. *Given a distribution π, we can implement an optimal decision tree for π in an online fashion in time $O(n)$ per question, after $O(n \log n)$ preprocessing.*

Section organization. Section 7.1 shows that a set of questions is optimal if and only if it is a *dyadic hitter*, that is, contains a question splitting every non-constant dyadic distribution into two equal halves. Section 7.2 discusses a relation to hitting sets for maximal antichains, and proves Theorem 7.5. Section 7.3 shows that the optimal size of a dyadic hitter is controlled by the minimum value of another parameter, the *maximum relative density*. We upper bound the minimum value in Section 7.4, thus proving Theorem 7.3, and lower bound it in Section 7.5, thus proving Theorem 7.2.

7.1 Reduction to dyadic hitters

The purpose of this subsection is to give a convenient combinatorial characterization of optimal sets of questions. Before presenting this characterization, we show that in this context it suffices to look at dyadic distributions.

Lemma 7.1.1. *A set $\mathcal{Q}$ of questions over X_n is optimal if and only if $c(\mathcal{Q}, \mu) = \mathrm{Opt}(\mu)$ for all* dyadic *distributions μ.*

Proof. Suppose that $\mathcal{Q}$ is optimal for all dyadic distributions, and let π be an arbitrary distribution over X_n. Let μ be a dyadic distribution such that

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

By assumption, $\mathcal{Q}$ is optimal for μ. Let T be an optimal decision tree for μ using questions from $\mathcal{Q}$ only, and let τ be the corresponding dyadic distribution, given by $\tau_i = 2^{-T(x_i)}$ (recall that $T(x_i)$ is the depth of x_i). Since τ minimizes $T(\mu) = H(\mu) + D(\mu\|\tau)$ over dyadic distributions, necessarily $\tau = \mu$. Thus

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

showing that $\mathcal{Q}$ is optimal for μ. □

Given a dyadic distribution μ on X_n, we will be particularly interested in the collection of subsets of X_n that have probability exactly half under μ.

Definition 7.1.2 (Dyadic hitters)**.** Let μ be a non-constant dyadic distribution. A set $A \subseteq X_n$ *splits* μ if $\mu(A) = 1/2$. We denote the collection of all sets splitting μ by $\mathrm{Spl}(\mu)$. We call a set of the form $\mathrm{Spl}(\mu)$ a *dyadic set*.

We call a set of questions $\mathcal{Q}$ a *dyadic hitter* in X_n if it intersects $\mathrm{Spl}(\mu)$ for all non-constant dyadic distributions μ. (Lemma 4.1 implies that $\mathrm{Spl}(\mu)$ is always non-empty.)

A dyadic hitter is precisely the object we are interested in:

Lemma 7.1.3. *A set $\mathcal{Q}$ of subsets of X_n is an optimal set of questions if and only if it is a dyadic hitter in X_n.*

Proof. Let $\mathcal{Q}$ be a dyadic hitter in X_n. We prove by induction on $1 \le m \le n$ that for a dyadic distribution μ on X_n with support size m, $c(\mathcal{Q}, \mu) = H(\mu)$. Since $\mathrm{Opt}(\mu) = H(\mu)$, Lemma 7.1.1 implies that $\mathcal{Q}$ is an optimal set of questions.

The base case, $m = 1$, is trivial. Suppose therefore that μ is a dyadic distribution whose support has size $m > 1$. In particular, μ is not constant, and so $\mathcal{Q}$ contains some set $S \in \mathrm{Spl}(\mu)$. Let $\alpha = \mu|_S$ and $\beta = \mu|_{\overline{S}}$, and note that α, β are both dyadic. The induction hypothesis shows that $c(\mathcal{Q}, \alpha) = H(\alpha)$ and $c(\mathcal{Q}, \beta) = H(\beta)$. A decision tree which first queries S and then uses the implied algorithms for α and β has cost

$$1 + \frac{1}{2}H(\alpha) + \frac{1}{2}H(\beta) = h(\mu(S)) + \mu(S)H(\mu|_S) + \mu(\overline{S})H(\mu|_{\overline{S}}) = H(\mu),$$

using the Bernoulli chain rule; here $\mu|_S$ is the restriction of μ to the elements in S.

Conversely, suppose that $\mathcal{Q}$ is not a dyadic hitter, and let μ be a non-constant dyadic distribution such that $\mathrm{Spl}(\mu)$ is disjoint from $\mathcal{Q}$. Let T be any decision tree for μ using $\mathcal{Q}$, and let S be its first question. The cost of T is at least

$$1 + \mu(S)H(\mu|_S) + \mu(\overline{S})H(\mu|_{\overline{S}}) > h(\mu(S)) + \mu(S)H(\mu|_S) + \mu(\overline{S})H(\mu|_{\overline{S}}) = H(\mu),$$

since $\mu(S) \neq \frac{1}{2}$. Thus $c(\mathcal{Q}, \mu) > \mathrm{Opt}(\mu)$, and so $\mathcal{Q}$ is not an optimal set of questions. □

7.2 Dyadic sets as antichains

There is a surprising connection between dyadic hitters and hitting sets for maximal antichains. We start by defining the latter:

Definition 7.2.1. A *fibre* in X_n is a subset of 2^{X_n} which intersects every maximal antichain in X_n.

Fibres were defined by Lonc and Rival [LR87], who also gave a simple construction, via cones:

Definition 7.2.2. The *cone* $\mathfrak{C}(S)$ of a set S consists of all subsets and all supersets of S.

Any cone $\mathfrak{C}(S)$ intersects any maximal antichain A, since otherwise $A \cup \{S\}$ is also an antichain. By choosing S of size $\lfloor n/2 \rfloor$, we obtain a fibre of size $2^{\lfloor n/2 \rfloor} + 2^{\lceil n/2 \rceil} - 1 = \Theta(2^{n/2})$. Lonc and Rival conjectured that this fibre has minimal size, but gave no lower bound. The first lower bound was given by Duffus, Sands and Winkler [DSW90], who showed that any fibre contains at least $\Omega(1.25^n)$ sets, using an argument virtually the same as our lower bound, Theorem 7.3. This has been improved by Łuczak [Łu98, DS01] to $\Omega(\sqrt[3]{2}^n)$, but the conjecture of Lonc and Rival remains open.

Our goal now is to show that every fibre is a dyadic hitter:

Theorem 7.2.3. *every fibre is a dyadic hitter.*

This shows that every cone is a dyadic hitter, and allows us to give a simple algorithm for constructing an optimal decision tree using any cone.

We start with a simple technical lemma which will also be used in Section 7.4:

Definition 7.2.4. Let μ be a dyadic distribution over X_n. The *tail* of μ is the largest set of elements $T \subseteq X_n$ such that for some $a \geq 1$,

(i) The elements in T have probabilities $2^{-a-1}, 2^{-a-2}, \ldots, 2^{-a-(|T|-1)}, 2^{-a-(|T|-1)}$.

(ii) All elements not in T have probability at least 2^{-a}.

Lemma 7.2.5. *Suppose that μ is a non-constant dyadic distribution with non-empty tail T. Every set in $\mathrm{Spl}(\mu)$ either contains T or is disjoint from T.*

Proof. The proof is by induction on $|T|$. If $|T| = 2$ then there exist an integer $a \geq 1$ and two elements, without loss of generality x_1, x_2, of probability 2^{-a-1}, such that all other elements have probability at least 2^{-a}. Suppose that $S \in \mathrm{Spl}(\mu)$ contains exactly one of x_1, x_2. Then

$$2^{a-1} = \sum_{x_i \in S} 2^a \mu(x_i) = \sum_{x_i \in S \setminus \{x_1, x_2\}} 2^a \mu(x_i) + \frac{1}{2}.$$

However, the left-hand side is an integer while the right-hand side is not. We conclude that S must contain either both of x_1, x_2 or none of them.

For the induction step, let the elements in the tail T of μ have probabilities $2^{-a-1}, 2^{-a-2}, \ldots, 2^{-a-(|T|-1)}, 2^{-a-(|T|-1)}$. Without loss of generality, suppose that x_{n-1}, x_n are the elements whose probability is $2^{-a-(|T|-1)}$. The same argument as before shows that every dyadic set in $\mathrm{Spl}(\mu)$ must contain either both of x_{n-1}, x_n or neither. Form a new dyadic distribution ν on X_{n-1} by merging the elements x_{n-1}, x_n into x_{n-1}, and note that $\mathrm{Spl}(\mu)$ can be obtained from $\mathrm{Spl}(\nu)$ by replacing x_{n-1} with x_{n-1}, x_n. The distribution ν has tail $T' = T \setminus \{x_n\}$, and so by induction, every set in $\mathrm{Spl}(\nu)$ either contains T' or is disjoint from T'. This implies that every set in $\mathrm{Spl}(\mu)$ either contains T or is disjoint from T. □

The first step in proving Theorem 7.2.3 is a reduction to dyadic distributions having full support:

Lemma 7.2.6. *A set of questions is a dyadic hitter in X_n if and only if it intersects* $\mathrm{Spl}(\mu)$ *for all non-constant full-support dyadic distributions μ on X_n.*

Proof. A dyadic hitter clearly intersects $\mathrm{Spl}(\mu)$ for all non-constant full-support dyadic distributions on X_n. For the other direction, suppose that $\mathcal{Q}$ is a set of questions that intersects $\mathrm{Spl}(\mu)$ for every non-constant full-support dyadic distribution μ. Let ν be a non-constant dyadic distribution on X_n which doesn't have full support. Let $x_{\min}$ be an element in the support of ν with minimal probability, which we denote $\nu_{\min}$. Arrange the elements in $\overline{\mathrm{supp}(\nu)}$ in some arbitrary order $x_{i_1}, \ldots, x_{i_m}$. Consider the distribution μ given by:

- $\mu(x_i) = \nu(x_i)$ if $x_i \in \mathrm{supp}(\mu)$ and $x_i \neq x_{\min}$.
- $\mu(x_{\min}) = \nu_{\min}/2$.
- $\mu(x_{i_j}) = \nu_{\min}/2^{j+1}$ for $j < m$.
- $\mu(x_{i_m}) = \nu_{\min}/2^m$.

In short, we have replaced $\nu(x_{\min}) = \nu_{\min}$ with a tail $x_{\min}, x_{i_1}, \ldots, x_{i_m}$ of the same total probability. It is not hard to check that μ is a non-constant dyadic distribution having full support on X_n.

We complete the proof by showing that $\mathcal{Q}$ intersects $\mathrm{Spl}(\nu)$. By assumption, $\mathcal{Q}$ intersects $\mathrm{Spl}(\mu)$, say at a set S. Lemma 7.2.5 shows that S either contains all of $\{x_{\min}\} \cup \overline{\mathrm{supp}(\nu)}$, or none of these elements. In both cases, $\nu(S) = \mu(S) = 1/2$, and so $\mathcal{Q}$ intersects $\mathrm{Spl}(\nu)$. □

We complete the proof of Theorem 7.2.3 by showing that dyadic sets corresponding to full-support distributions are maximal antichains:

Lemma 7.2.7. *Let μ be a non-constant dyadic distribution over X_n with full support, and let $D = \mathrm{Spl}(\mu)$. Then D is a maximal antichain which is closed under complementation (i.e. $A \in D \implies X \setminus A \in D$).*

Proof. (i) That D is closed under complementation follows since if $A \in D$ then $\mu(X \setminus A) = 1 - \mu(A) = 1/2$.

(ii) That D is an antichain follows since if A strictly contains B then $\mu(A) > \mu(B)$ (because μ has full support).

(iii) It remains to show that D is maximal. By (i) it suffices to show that every B with $\mu(B) > 1/2$ contains some $A \in D$. This follows from applying Lemma 4.1 on the probabilities of the elements in B. □

Cones allow us to prove Theorem 7.5:

Proof of Theorem 7.5. Let $S = \{x_1, \ldots, x_{\lfloor n/2 \rfloor}\}$. The set of questions $\mathcal{Q}$ is the cone $\mathfrak{C}(S)$, whose size is $2^{\lfloor n/2 \rfloor} + 2^{\lceil n/2 \rceil} - 1 < 2^{\lceil n/2 \rceil + 1}$.

An efficient indexing scheme for $\mathcal{Q}$ divides the index into a bit b, signifying whether the set is a subset of S or a superset of S, and $\lfloor n/2 \rfloor$ bits (in the first case) or $\lceil n/2 \rceil$ bits (in the second case) for specifying the subset or superset.

To prove the other two parts, we first solve an easier question. Suppose that μ is a non-constant dyadic distribution whose sorted order is known. We show how to find a set in $\mathrm{Spl}(\mu) \cap \mathcal{Q}$ in time $O(n)$. If $\mu(S) = 1/2$ then $S \in \mathrm{Spl}(\mu)$. If $\mu(S) > 1/2$, go over the elements in S in non-decreasing

order. According to Lemma 4.1, some prefix will sum to 1/2 exactly. If $\mu(S) < 1/2$, we do the same with $\overline{S}$, and then complement the result.

Suppose now that π is a non-constant distribution. We can find a Huffman distribution μ for π and compute the sorted order of π in time $O(n \log n)$. The second and third part now follow as in the proof of Lemma 7.1.3. □

7.3 Reduction to maximum relative density

Section 7.1 shows that we are interested in the minimal size of a dyadic hitter. Section 7.4 gives a lower bound on the size of any dyadic hitter, along the following lines. For appropriate values of n, we describe a dyadic distribution μ, all of whose splitters have a certain size i or $n - i$. Moreover, only a ρ fraction of sets of size i split μ. We then consider all possible permutations of μ. Each set of size i splits a ρ fraction of these, and so any dyadic hitter must contain at least $1/\rho$ sets.

This lower bound argument prompts the definition of *maximum relative density* (MRD), which corresponds to the parameter ρ above; in the general case we will also need to optimize over i. We think of the MRD as a property of dyadic sets rather than dyadic distributions; indeed, the concept of MRD makes sense for any collection of subsets of 2^{X_n}. If a dyadic set has MRD ρ then any dyadic hitter must contain at least $1/\rho$ questions, due to the argument outlined above. Conversely, using the probabilistic method we will show that roughly $1/\rho_{\min}(n)$ questions suffice, where $\rho_{\min}(n)$ is the minimum MRD of a dyadic set on X_n.

Definition 7.3.1 (Maximum relative density)**.** Let D be a collection of subsets of X_n. For $i \in \{0, \ldots, n\}$ denote by $D_i \subseteq D$ the restriction of D to sets of size i. Define the *i'th relative density* of D, denoted $\rho_i(D)$, as

$$\rho_i(D) := \frac{|D_i|}{\binom{n}{i}}.$$

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

$$\rho(D) := \max_{i \in \{1,\ldots,n-1\}} \rho_i(D).$$

We define $\rho_{\min}(n)$ to be the minimum of $\rho(D)$ over all dyadic sets. That is, $\rho_{\min}(n)$ is the smallest possible maximum relative density of a set of the form $\mathrm{Spl}(\mu)$.

The following theorem shows that $u^{\mathrm{Opt}}(n, 0)$ is controlled by $\rho_{\min}(n)$, up to polynomial factors.

Theorem 7.3.1. *Fix an integer n, and denote $M := \frac{1}{\rho_{\min}(n)}$. Then*

$$M \leq u^{\mathrm{Opt}}(n, 0) \leq n^2 \log n \cdot M.$$

Proof. Note first that according to Lemma 7.1.3, $u^{\mathrm{Opt}}(n, 0)$ is equal to the minimal size of a dyadic hitter in X_n, and thus it suffices to lower- and upper-bound this size.

Let σ be a uniformly random permutation on X_n. If S is any set of size i then $\sigma^{-1}(S)$ is a uniformly random set of size i, and so

$$\rho_i(D) = \Pr_{\sigma \in \mathrm{Sym}(X_n)}[\sigma^{-1}(S) \in D] = \Pr_{\sigma \in \mathrm{Sym}(X_n)}[S \in \sigma(D)].$$

(Here $\mathrm{Sym}(X_n)$ is the group of permutations of X_n.)

Fix a dyadic set D on X_n with $\rho(D) = \rho_{\min}(n)$. The formula for $\rho_i(D)$ implies that for any subset S of X_n (of *any* size),

$$\Pr_{\sigma \in \mathrm{Sym}(X_n)}[S \in \sigma(D)] \leq \rho_{\min}(n).$$

Let $\mathcal{Q}$ be a collection of subsets of X_n with $|\mathcal{Q}| < M$. A union bound shows that

$$\Pr_{\sigma \in \mathrm{Sym}(X_n)}[\mathcal{Q} \cap \sigma(D) \neq \emptyset] \leq |\mathcal{Q}|\rho_{\min}(n) < 1.$$

Thus, there exists a permutation σ such that $\mathcal{Q} \cap \sigma(D) = \emptyset$. Since $\sigma(D)$ is also a dyadic set, this shows that $\mathcal{Q}$ is not a dyadic hitter. We deduce that any dyadic hitter must contain at least M questions.

For the upper bound on $u^{\mathrm{Opt}}(n, 0)$, construct a set of subsets $\mathcal{Q}$ containing, for each $i \in \{1, \ldots, n-1\}$, $Mn \log n$ uniformly chosen sets $S \subseteq X_n$ of size i. We show that with positive probability, $\mathcal{Q}$ is a dyadic hitter.

Fix any dyadic set D, and let $i \in \{1, \ldots, n-1\}$ be such that $\rho_i(D) = \rho(D) \geq \rho_{\min}(n)$. The probability that a random set of size i doesn't belong to D is at most $1 - \rho(D) \leq 1 - \rho_{\min}(n)$. Therefore the probability that $\mathcal{Q}$ is disjoint from D is at most

$$(1 - \rho_{\min}(n))^{Mn \log n} \leq e^{-\rho_{\min}(n) Mn \log n} = e^{-n \log n} < n^{-n}.$$

As we show below in Claim 7.3.2, there are at most n^n non-constant dyadic distributions, and so a union bound implies that with positive probability, $\mathcal{Q}$ is indeed a dyadic hitter. □

In order to complete the proof of Theorem 7.3.1, we bound the number of non-constant dyadic distributions:

Claim 7.3.2. *There are at most n^n non-constant dyadic distributions on X_n.*

Proof. Let μ be a dyadic distribution on a finite domain X. We will show that if the minimal probability in μ is $2^{-\ell}$ then $|X| > \ell$. It follows that if μ is a non-constant dyadic distribution over X_n then the possible values for μ_i are only $\{0, 2^{-1}, \ldots, 2^{-(n-1)}\}$, which means that there are at most n^n ways to assign the probabilities $\mu_1, \ldots, \mu_n$.

It remains to show that if μ is a dyadic distribution on a domain X and the minimal probability in μ is $2^{-\ell}$ then $|X| > \ell$. The proof is by induction on ℓ. The base case, $\ell = 0$, is trivial. For the induction step, assume that the claim holds for $\ell - 1$, and suppose that μ is a dyadic distribution on X having minimal probability $2^{-\ell}$. Since $\sum_i 2^\ell \mu_i = 2^\ell$ is even, the number of elements whose probability is $2^{-\ell}$ must be even. Merge these elements in pairs to obtain a dyadic distribution whose minimal probability is $2^{-(\ell-1)}$. The induction hypothesis shows that the merged domain must contain more than $\ell - 1$ elements. Since we merged at least one pair of elements, X must contain more than ℓ elements. □

Krenn and Wagner [KW16] showed that the number of full-support dyadic distributions on X_n is asymptotic to $\alpha\gamma^{n-1}n!$, where $\alpha \approx 0.296$ and $\gamma \approx 1.193$, implying that the number of dyadic distributions on X_n is asymptotic to $\alpha e^{1/\gamma}\gamma^{n-1}n!$. Boyd [Boy75] showed that the number of monotone full-support dyadic distributions on X_n is asymptotic to $\beta\lambda^n$, where $\beta \approx 0.142$ and $\lambda \approx 1.794$, implying that the number of monotone dyadic distributions on X_n is asymptotic to $\beta(1 + \lambda)^n$.

The proof of Theorem 7.3.1 made use of two properties of dyadic sets:

1. Any permutation of a dyadic set is a dyadic set.

2. There are $e^{n^{O(1)}}$ dyadic sets.

If $\mathcal{F}$ is any collection of subsets of 2^{X_n} satisfying the first property then the proof of Theorem 7.3.1 generalizes to show that the minimal size U of a hitting set for $\mathcal{F}$ satisfies

$$M \leq U \leq Mn \log |\mathcal{F}|, \qquad \text{where } M = \frac{1}{\min_{D \in \mathcal{F}} \rho(D)}.$$

7.4 Upper bounding $\rho_{\min}(n)$

Theorem 7.3 will ultimately follow from the following lemma, by way of Theorem 7.3.1:

Lemma 7.4.1. *Fix $0 < \beta \leq 1/2$. There exists an infinite sequence of positive integers n (namely, those of the form $\lfloor \frac{2^a}{2\beta} \rfloor$ for integer a) such that some dyadic set D in X_n satisfies $\rho(D) \leq O(\sqrt{n}) 2^{-(h(\beta)-2\beta)n}$.*

Proof. We prove the lemma under the simplifying assumption that $1/\beta$ is an integer (our most important application of the lemma has $\beta := 1/5$). Extending the argument for general β is straightforward and left to the reader.

Let n be an integer of the form $\frac{2^a}{2\beta}$, for a positive integer a. Note that for n of this form, $\beta n = 2^{a-1}$ is a power of two. Let $t = \beta n$, and construct a dyadic distribution μ on X_n as follows:

1. For $i \in [2t-1]$, $\mu(x_i) = 2^{-a} = \frac{1}{2t}$.

2. For $i \in [n-1] \setminus [2t-1]$, $\mu(x_i) = \mu(x_{i-1})/2 = 2^{-(a+i-2t+1)}$.

3. $\mu(x_n) = \mu(x_{n-1})$.

The corresponding decision tree is obtained by taking a complete binary tree of depth a and replacing one of the leaves by a "path" of length $n - 2^a$; see Figure 2. Alternatively, in the terminology of Definition 7.2.4 we form μ by taking the uniform distribution on X_{2t} and replacing x_{2t} with a tail on $x_{2t}, \ldots, x_n$.

We claim that $D := \mathrm{Spl}(\mu)$ contains only two types of sets:

1. Subsets of size t of X_{2t-1}.

2. Subsets of size $n-t$ containing $t-1$ elements of X_{2t-1} and all the elements $x_{2t}, \ldots, x_n$.

It is immediate that any such set S is in D. On the other hand, Lemma 7.2.5 shows that every set $S \in D$ either contains the tail $x_{2t}, \ldots, x_n$ or is disjoint from it. If S is disjoint from the tail then it must be of the first form, and if S contains the tail then it must be of the second form.

Using the estimate $\binom{n}{\beta n} \geq 2^{h(\beta)n}/O(\sqrt{n})$ (see for example [You12]), we see that

$$\rho_t(D) = \rho_{n-t}(D) = \frac{\binom{2t-1}{t}}{\binom{n}{t}} \leq \frac{2^{2t}}{\binom{n}{\beta n}} \leq O(\sqrt{n}) \frac{2^{2t}}{2^{h(\beta)n}} = O(\sqrt{n}) 2^{(2\beta - h(\beta))n}.$$

For $i \in \{1, \ldots, n-1\} \setminus \{t, n-t\}$ we have $\rho_i(D) = 0$. Thus indeed

$$\rho(D) \leq O(\sqrt{n}) 2^{(2\beta - h(\beta))n}. \qquad \square$$

Theorem 7.3 can now be easily derived. The first step is determining the optimal value of β:

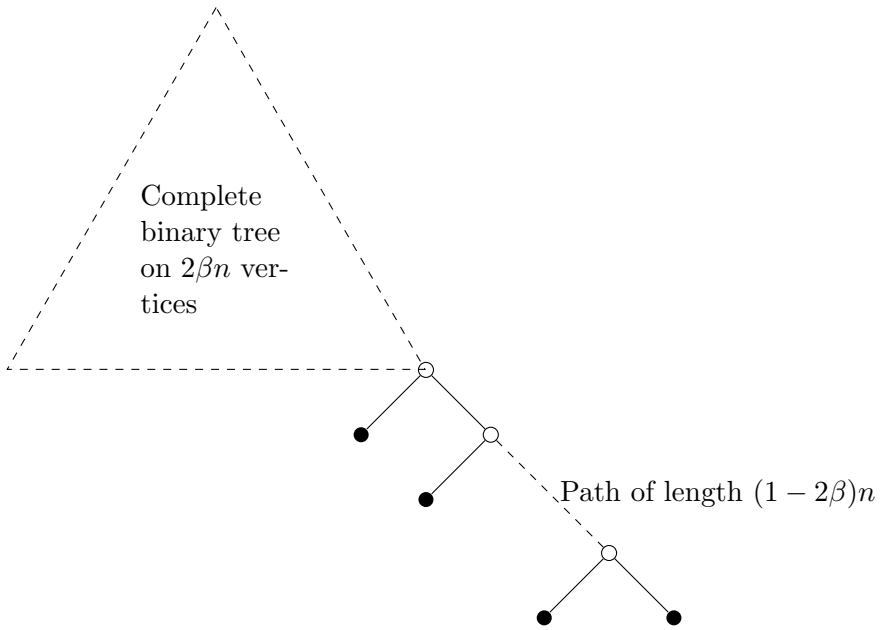


Figure 2: The hard distribution used to prove Lemma 7.4.1, in decision tree form

Claim 7.4.2. *We have*

$$\max_{\beta\in[0,1]} 2^{h(\beta)-2\beta} = 1.25,$$

and the maximum is attained (uniquely) at $\beta = 1/5$.

Proof. Let $f(\beta) = h(\beta) - 2\beta$. Calculation shows that the derivative $f'(\beta)$ is equal to

$$f'(\beta) = \log\left(\frac{1-\beta}{\beta}\right) - 2,$$

which is decreasing for $0 < \beta < 1$ and vanishes at $\beta = 1/5$. Thus $f(\beta)$ achieves a unique maximum over $\beta \in (0,1)$ at $\beta = 1/5$, where

$$2^{f(1/5)} = 2^{h(1/5)-2\cdot 1/5} = 1.25. \qquad \square$$

Proof of Theorem 7.3:

Proof. Let $\beta := 1/5$. Claim 7.4.2 shows that $2^{-(2\beta-h(\beta))} = 1.25$. Fix any n of the form $n = \frac{2^a}{2\beta}$ for a positive integer a. It follows from Lemma 7.4.1 together with the first inequality in Theorem 7.3.1 that $u^{\mathrm{Opt}}(n,0) \geq 1.25^n/O(\sqrt{n})$.

A general n can be written in the form $n = \frac{2^a}{2\beta}$ for a positive integer a and $1/4 \leq \beta \leq 1/2$. Lemma 7.4.1 and Theorem 7.3.1 show that for any integer $\ell \geq 0$,

$$u^{\mathrm{Opt}}(n,0) \geq 2^{[h(\beta/2^\ell)-2\beta/2^\ell]n}/O(\sqrt{n}).$$

Calculation shows that when $\beta \leq \beta_0 \approx 0.27052059413118146$, this is maximized at $\ell = 0$, and otherwise this is maximized at $\ell = 1$. Denote the resulting lower bound by $L(\beta)^n/O(\sqrt{n})$, the minimum of $L(\beta)$ is attained at β_0, at which point its value is $L(\beta_0) \approx 1.23214280723432$. $\square$

7.5 Lower bounding $\rho_{\min}(n)$

We will derive Theorem 7.2 from the following lemma:

Lemma 7.5.1. *For every non-constant dyadic distribution μ there exists $0 < \beta < 1$ such that*

$$\rho(\mathrm{Spl}(\mu)) \geq \frac{2^{(2\beta - h(\beta))n}}{O(\sqrt{n})^{O(\log n)}} = 2^{(2\beta - h(\beta))n - o(n)}.$$

Proof. Assume without loss of generality that the probabilities in μ are non-increasing:

$$\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n.$$

The idea is to find a partition of X_n of the form

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

which satisfies the following properties:

1. D_i consists of elements having the same probability p_i.
2. If D_i has an even number of elements then $E_i = \emptyset$.
3. If D_i has an odd number of elements then $\mu(E_i) = p_i$.
4. $\gamma = O(\log n)$. (In fact, $\gamma = o(n/\log n)$ would suffice.)

We will show later how to construct such a partition.

The conditions imply that $\mu(D_i \cup E_i)$ is an even integer multiple of p_i, say $\mu(D_i \cup E_i) = 2c_i p_i$. It is not hard to check that $c_i = \lceil |D_i|/2 \rceil$.

Given such a partition, we show how to lower bound the maximum relative density of $\mathrm{Spl}(\mu)$. If $S_i \subseteq D_i$ is a set of size c_i for each $i \in [\gamma]$ then the set $S = \bigcup_i S_i$ splits μ:

$$\mu(S) = \sum_{i=1}^{\gamma} c_i p_i = \frac{1}{2} \sum_{i=1}^{\gamma} \mu(D_i \cup E_i) = \frac{1}{2}.$$

Defining $c = \sum_{i=1}^{\gamma} c_i$, we see that each such set S contains c elements, and the number of such sets is

$$\prod_{i=1}^{\gamma} \binom{|D_i|}{c_i} \geq \prod_{i=1}^{\gamma} \frac{2^{2c_i}}{O(\sqrt{n})} = \frac{2^{2c}}{O(\sqrt{n})^{O(\log n)}},$$

using the estimate

$$\binom{m}{\lceil m/2 \rceil} = \Theta\left(\frac{2^{2\lceil m/2 \rceil}}{\sqrt{m}}\right),$$

which follows from Stirling's approximation.

In order to obtain an estimate on the maximum relative density of $\mathrm{Spl}(\mu)$, we use the following folklore upper bound[6] on $\binom{n}{c}$:

$$\binom{n}{c} \leq 2^{h(c/n)n}.$$

[6]Here is a quick proof: Let Y be a uniformly random subset of X_n of size c, and let Y_i indicate the event $x_i \in Y$. Then $\log \binom{n}{c} = H(Y) \leq nH(Y_1) = nh(c/n)$.

We conclude that the maximum relative density of $\mathrm{Spl}(\mu)$ is at least

$$\rho(\mu) \geq \rho_c(\mu) \geq \frac{\prod_{i=1}^{\gamma} \binom{|D_i|}{c_i}}{\binom{n}{c}} \geq \frac{2^{2c-h(c/n)n}}{O(\sqrt{n})^{O(\log n)}}.$$

To obtain the expression in the statement of the lemma, take $\beta := c/n$.

We now show how to construct the partition of X_n. We first explain the idea behind the construction, and then provide full details; the reader who is interested only in the construction itself can skip ahead.

Proof idea Let $q_1, \ldots, q_\gamma$ be the different probabilities of elements in μ. We would like to put all elements of probability q_i in the set D_i, but there are two difficulties:

1. There might be an odd number of elements whose probability is q_i.
2. There might be too many distinct probabilities, that is, γ could be too large. (We need $\gamma = o(n/\log n)$ for the argument to work.)

The second difficulty is easy to solve: we let $D_1 = \{x_1\}$, and use Lemma 4.1 to find an index ℓ such that $\mu(E_1) := \mu(\{x_\ell, \ldots, x_n\}) = \mu_1$. A simple argument shows that all remaining elements have probability at least μ_1/n, and so the number of remaining distinct probabilities is $O(\log n)$. (The reader should observe the resemblance between E_1 and the tail of the hard distribution constructed in Lemma 7.4.1.)

Lemma 4.1 also allows us to resolve the first difficulty. The idea is as follows. Suppose that the current set under construction, D_i, has an odd number of elements, each of probability q_i. We use Lemma 4.1 to find a set of elements whose total probability is q_i, and put them in E_i.

Detailed proof Let N be the maximal index such that $\mu_N > 0$. Since μ is non-constant, $\mu_1 \leq 1/2$, and so Lemma 4.1 proves the existence of an index M such that $\mu(\{x_{M+1}, \ldots, x_N\}) = \mu_1$ (we use the *furthermore* part of the lemma, and $M = \ell - 1$). We take

$$D_1 := \{x_1\}, \quad E_1 := \{x_{M+1}, \ldots, x_n\}.$$

Thus $\mu(D_1) = \mu(E_1) = \mu_1$, and so $\mu(\{x_2, \ldots, x_M\}) = 1 - 2\mu_1$ (possibly $M = 1$, in which case the construction is complete).

By construction $n\mu_M > \mu(E_1) = \mu_1$, and so $\mu_M < \mu_1/n$. In particular, the number of distinct probabilities among $\mu_2, \ldots, \mu_M$ is at most $\log n$. This will guarantee that $\gamma \leq \log n + 1$, as will be evident from the construction.

The construction now proceeds in steps. At step i, we construct the sets D_i and E_i, given the set of available elements $\{x_{\alpha_i}, \ldots, x_M\}$, where possibly $\alpha_i = M + 1$; in the latter case, we have completed the construction. We will maintain the invariant that $\mu(\{x_{\alpha_i}, \ldots, x_M\})$ is an even multiple of μ_{α_i}; initially $\alpha_2 := 2$, and $\mu(\{x_{\alpha_i}, \ldots, x_M\}) = (1/\mu_1 - 2)\mu_1$ is indeed an even multiple of μ_2.

Let β_i be the maximal index such that $\mu_{\beta_i} = \mu_{\alpha_i}$ (possibly $\beta_i = \alpha_i$). We define

$$D_i := \{x_{\alpha_i}, \ldots, x_{\beta_i}\}.$$

Suppose first that $|D_i|$ is even. In this case we define $E_i := \emptyset$, and $\alpha_{i+1} := \beta_i + 1$. Note that

$$\mu(\{x_{\alpha_{i+1}}, \ldots, x_M\}) = \mu(\{x_{\alpha_i}, \ldots, x_M\}) - |D_i|\mu_{\alpha_i},$$

and so the invariant is maintained.

Suppose next that $|D_i|$ is odd. In this case $\mu(\{x_{\beta_i+1}, \ldots, x_M\}) \geq x_{\alpha_i}$, since $\mu(\{x_{\beta_i+1}, \ldots, x_M\})$ is an odd multiple of μ_{α_i}. Therefore we can use Lemma 4.1 to find an index γ_i such that $\mu(\{x_{\beta_i+1}, \ldots, x_{\gamma_i}\}) = \mu_{\alpha_i}$. We take

$$E_i := \{x_{\beta_i+1}, \ldots, x_{\gamma_i}\}$$

and $\alpha_{i+1} := \gamma_i + 1$. Note that

$$\mu(\{x_{\alpha_{i+1}}, \ldots, x_M\}) = \mu(\{x_{\alpha_i}, \ldots, x_M\}) - (|D_i| + 1)\mu_{\alpha_i},$$

and so the invariant is maintained.

The construction eventually terminates, say after step γ. The construction ensures that $\mu_{\alpha_2} > \mu_{\alpha_3} > \cdots > \mu_{\alpha_\gamma}$. Since there are at most $\log n$ distinct probabilities among the elements $\{x_{\alpha_2}, \ldots, x_M\}$, $\gamma \leq \log n + 1$, completing the proof. □

Theorem 7.2 follows immediately from the second inequality in Theorem 7.3.1 together with the following lemma:

Lemma 7.5.2. *Fix an integer n and let D be a dyadic set in X_n. Then*

$$\rho(D) \geq 1.25^{-n-o(n)},$$

and thus

$$\rho_{\min}(n) \geq 1.25^{-n-o(n)}.$$

Proof. Fix a dyadic set D in X_n. Lemma 7.5.1 implies that there exists $0 < \beta < 1$ such that $\rho(D) \geq 2^{(2\beta - h(\beta))n - o(n)}$. Using Claim 7.4.2 we have $2^{2\beta - h(\beta)} \geq \frac{4}{5}$, and so

$$\rho(D) \geq (4/5)^n \cdot 2^{-o(n)} = 1.25^{-n-o(n)}.$$ □

8 Combinatorial benchmark with prolixity

In the previous section we studied the minimum size of a set $\mathcal{Q}$ of questions with the property that for every distribution, there is an optimal decision tree using only questions from $\mathcal{Q}$. In this section we relax this requirement by allowing the cost to be slightly worse than the optimal cost.

More formally, recall that $u^{\mathrm{Opt}}(n, r)$ is the minimum size of a set of questions $\mathcal{Q}$ such that for every distribution π there exists a decision tree that uses only questions from $\mathcal{Q}$ with cost at most $\mathrm{Opt}(\pi) + r$.

In a sense, $u^{\mathrm{Opt}}(n, r)$ is an extension of $u^H(n, r)$ for $r \in (0, 1)$: indeed, $u^H(n, r)$ is not defined for $r < 1$ since for some distributions π there is no decision tree with cost less than $H(\pi) + 1$ (see Section 5). Moreover, $\mathrm{Opt}(\pi)$, which is the benchmark used by $u^{\mathrm{Opt}}(n, r)$, is precisely the optimal cost, whereas $H(\pi)$, the benchmark used by $u^H(n, r)$ is a convex surrogate of $\mathrm{Opt}(\pi)$.

We focus here on the range $r \in (0, 1)$. We prove the following bounds on $u^{\mathrm{Opt}}(n, r)$, establishing that $u^{\mathrm{Opt}}(n, r) \approx (r \cdot n)^{\Theta(1/r)}$.

Theorem 8.1. *For all $r \in (0, 1)$, and for all $n > 1/r$:*

$$\frac{1}{n}(r \cdot n)^{\frac{1}{4r}} \leq u^{\mathrm{Opt}}(n, r) \leq n^2(3r \cdot n)^{\frac{16}{r}}.$$

As a corollary, we get that the threshold of exponentiality is $1/n$:

Corollary 8.2. *If $r = \omega(1/n)$ then $u^{\mathrm{Opt}}(n, r) = 2^{o(n)}$.*
Conversely, if $r = O(1/n)$ then $u^{\mathrm{Opt}}(n, r) = 2^{\Omega(n)}$.

For larger r, the following theorem is a simple corollary of Theorem 6.1 and the bound $u^{\mathrm{Opt}}(n, r) \leq u^{H}(n, r) \leq u^{\mathrm{Opt}}(n, r-1)$:

Theorem 8.3. *For every $r \geq 1$ and $n \in \mathbb{N}$,*

$$\frac{1}{e}\lfloor r+1 \rfloor n^{1/\lfloor r+1 \rfloor} \leq u^{\mathrm{Opt}}(n, r) \leq 2\lfloor r \rfloor n^{1/\lfloor r \rfloor}.$$

Theorem 8.1 is implied by the following lower and upper bounds, which provide better bounds when $r \in (0, 1)$ is a negative power of 2.

Theorem 8.4 (Lower bound)**.** *For every r of the form $1/2^k$, where $k \geq 1$ is an integer, and $n > 2^k$:*

$$u^{\mathrm{Opt}}(n, r) \geq (r \cdot n)^{\frac{1}{2r}-1}.$$

Theorem 8.5 (Upper bound)**.** *For every r of the form $4/2^k$, where $k \geq 3$ is an integer, and $n > 2^k$:*

$$u^{\mathrm{Opt}}(n, r + r^2) \leq n^2\big(\frac{3e}{4} r \cdot n\big)^{\frac{4}{r}}.$$

These results imply Theorem 8.1, due to the monotonicity of $u^{\mathrm{Opt}}(n, r)$, as follows.

Let $r \in (0, 1)$. For the *lower bound*, pick the smallest $t \geq r$ of the form $1/2^k$. Note that $t \leq 2r$, and thus:

$$u^{\mathrm{Opt}}(n, r) \geq u^{\mathrm{Opt}}(n, t) \geq (t \cdot n)^{\frac{1}{2t}-1} \geq (r \cdot n)^{\frac{1}{4r}-1} \geq \frac{1}{n}(r \cdot n)^{\frac{1}{4r}}.$$

For the *upper bound*, pick the largest t of the form $4/2^k$, $k \geq 3$ such that $t + t^2 \leq r$. Note that $t \geq r/4$ (since $s = r/2$ satisfies $s + s^2 \leq 2s \leq r$), and thus

$$u^{\mathrm{Opt}}(n, r) \leq u^{\mathrm{Opt}}(n, t + t^2) \leq n^2\big(\frac{3e}{4} t \cdot n\big)^{\frac{4}{t}} \leq n^2(3r \cdot n)^{\frac{16}{r}}.$$

Section organization. We prove the lower bound (Theorem 8.4) in Section 8.1, and the upper bound (Theorem 8.5) in Section 8.2.

8.1 Lower bound

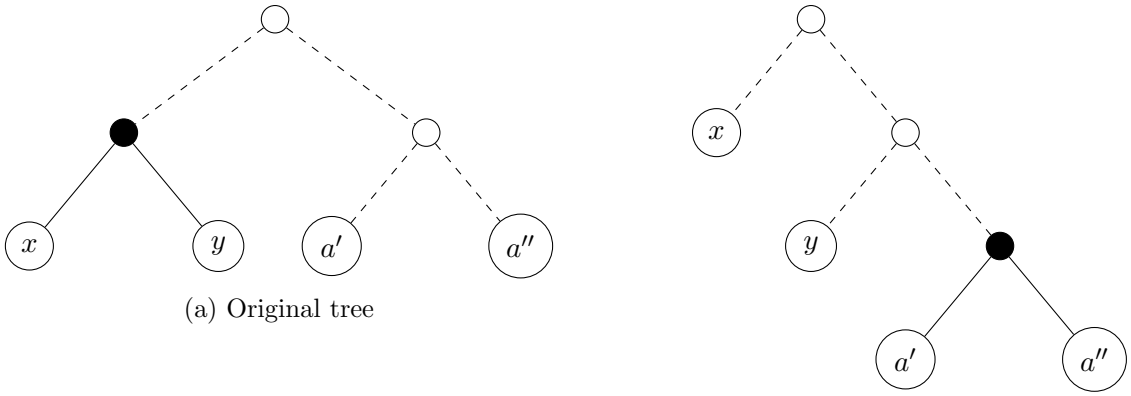
Pick a sufficiently small $\delta > 0$ (as we will soon see, $\delta < r^2$ suffices), and consider a distribution μ with $2^k - 1$ "heavy" elements (this many elements exist since $n > 1/r$), each of probability $\frac{1-\delta}{2^k-1}$, and $n - (2^k - 1)$ "light" elements with total probability of δ. Recall that a decision tree is *r-optimal* if its cost is at most $\mathrm{Opt}(\mu) + r$. The proof proceeds by showing that if T is an r-optimal tree, then the first question in T has the following properties:

(i) it separates the heavy elements to two sets of almost equal sizes (2^{k-1} and $2^{k-1} - 1$), and

(ii) it does not distinguish between the light elements.

The result then follows since there are $\binom{n}{2^k-1}$ such distributions σ (the number of ways to choose the light elements), and each question can serve as a first question to at most $\binom{n-(2^{k-1}-1)}{2^{k-1}}$ of them.

To establish these properties, we first prove a more general result (cf. Lemma 7.2.5):



(a) Original tree

(b) Transformed tree

Figure 3: The transformation in Lemma 8.1.1. The cost decreases by $\mu\big(\{x\}\big) - \mu\big(\{a', a''\}\big) > \epsilon$.

Lemma 8.1.1. *Let μ be a distribution over a finite set X, and let $A \subseteq X$ be such that for every $x \notin A$, $\mu\big(\{x\}\big) > \mu(A) + \epsilon$. Then every decision tree T which is ϵ-optimal with respect to μ has a subtree T' whose set of leaves is A.*

Proof. By induction on $|A|$. The case $|A| = 1$ follows since any leaf is a subtree. Assume $|A| > 1$. Let T be a decision tree which is ϵ-optimal with respect to μ. Let x, y be two siblings of maximal depth. Note that it suffices to show that $x, y \in A$, since then, merging x, y to a new element z with $\mu(\{z\}) = \mu(\{x\}) + \mu(\{y\})$ and applying the induction hypothesis yields that $A \cup \{z\} \setminus \{x, y\}$ is the set of leaves of a subtree of T with x, y removed. This finishes the proof since x, y are the children of z.

It remains to show that $x, y \in A$. Let d denote the depth of x and y. Assume toward contradiction that $x \notin A$. Pick $a', a'' \in A$, with depths d', d'' (this is possible since $|A| > 1$). If $d' < d$ or $d'' < d$ then replacing a' with x or a'' with x improves the cost of T by more than ϵ, contradicting its optimality. Therefore, it must be that $d' = d'' = d$, and we perform the following transformation (see Figure 3): the parent of x and y becomes a leaf with label x (decreasing the depth of x by 1), y takes the place of a' (the depth of y does not change), and a'' becomes an internal node with two children labeled by a', a'' (increasing the depths of a', a'' by 1). Since $\mu\big(\{x\}\big) - \mu\big(\{a', a''\}\big) > \epsilon$, this transformation improves the cost of T by more than ϵ, contradicting its ϵ-optimality. □

Corollary 8.1.2. *Let μ be a distribution over X, and let $A \subseteq X$ be such that for every $x \notin A$, $\mu\big(\{x\}\big) > \mu(A)$. Then every optimal tree T with respect to μ has a subtree T' whose set of leaves is A.*

Property (ii) follows from Lemma 8.1.1, which implies that if δ is sufficiently small then all light elements are clustered together as the leaves of some subtree. Indeed, by Lemma 8.1.1, this happens if the probability of a single heavy element (which is $\frac{1-\delta}{2^k-1}$) exceeds the total probability of all light elements (which is δ) by at least r. A simple calculation shows that setting δ smaller than r^2 suffices.

We summarize this in the following claim:

Claim 8.1.3 (light elements)**.** *Every r-optimal tree has a subtree whose set of leaves is the set of light elements.*

The next claim concerns the other property:

Claim 8.1.4 (heavy elements)**.** *In every r-optimal decision tree, the first question partitions the heavy elements into a set of size 2^{k-1} and a set of size $2^{k-1}-1$.*

Proof. When $k=2$, it suffices to prove that an r-optimal decision tree cannot have a first question which separates the heavy elements from the light elements. Indeed, the heavy elements in such a tree reside at depths $2,3,3$. Exchanging one of the heavy elements at depth 2 with the subtree consisting of all light elements (which is at depth 1) decreases the cost by $\frac{1-\delta}{2^k-1} - \delta > r$, showing that the tree wasn't r-optimal.

Suppose that some r-optimal decision tree T contradicts the statement of the claim, for some $k \geq 3$. The first question in T leads to two subtrees T_1, T_2, one of which (say T_1) contains at least $2^{k-1}+1$ heavy elements, and the other (say T_2) contain at most $2^{k-1}-2$. One of the subtrees also contains a subtree T' whose leaves are all the light elements. For the sake of the argument, we replace the subtree T' with a new element y.

We claim that T_1 contains an internal node v at depth $D(v) \geq k-1$ which has at least two heavy descendants. To see this, first remove y if it is present in T_1, by replacing its parent by its sibling. The possibly modified tree T_1' contains at least $2^{k-1}+1$ leaves, and in particular some leaf at depth at least k. Its parent v has depth at least $k-1$ and at least two heavy descendants, in both T_1' and T_1.

In contrast, T_2 contains at least two leaves (since $2^{k-1}-2 \geq 2$), and the two shallowest ones must have depth at most $k-2$. At least one of these is some heavy element x_ℓ.

Exchanging v and x_ℓ results in a tree T^* whose cost $c(T^*)$ is at most

$$c(T^*) \leq c(T) + (D(v) - D(x_\ell))(2-1)\frac{1-\delta}{2^k-1} \leq c(T^*) - \frac{1-\delta}{2^k-1} < c(T) - r,$$

contradicting the assumption that T is r-optimal. (That $\frac{1-\delta}{2^k-1} > r$ follows from the earlier assumption $\frac{1-\delta}{2^k-1} > \delta + r$.) □

By the above claims, there are two types of first questions for μ, depending on which of the two subtrees of the root contains the light elements:

- Type 1: questions that split the elements into a part with 2^{k-1} elements, and a part with $n - 2^{k-1}$ elements.
- Type 2: questions that split the elements into a part with $2^{k-1}-1$ elements, and a part with $n - (2^{k-1}-1)$ elements.

If we identify a question with its smaller part (i.e. the part of size 2^{k-1} or the part of size $2^{k-1}-1$), we deduce that any set of questions with redundancy r must contain a family $\mathcal{F}$ such that (i) every set in $\mathcal{F}$ has size 2^{k-1} or $2^{k-1}-1$, and (ii) for every set of size $n-(2^k-1)$, there exists some set in $\mathcal{F}$ that is disjoint from it. It remains to show that any such family $\mathcal{F}$ is large.

Indeed, there are $\binom{n}{2^k-1}$ sets of size $n-(2^k-1)$, and since every set in $\mathcal{F}$ has size at least $2^{k-1}-1$, it is disjoint from at most $\binom{n-(2^{k-1}-1)}{n-(2^k-1)} = \binom{n-(2^{k-1}-1)}{2^{k-1}}$ of them. Thus

$$|\mathcal{F}| \geq \frac{\binom{n}{2^k-1}}{\binom{n-(2^{k-1}-1)}{2^{k-1}}} = \frac{n(n-1)\cdots(n-(2^{k-1}-1)+1)}{(2^k-1)(2^k-2)\cdots(2^{k-1}+1)} \geq \left(\frac{n}{2^k}\right)^{2^{k-1}-1} = (r\cdot n)^{\frac{1}{2r}-1}.$$

8.2 Upper bound

The set of questions. In order to describe the set of queries it is convenient to assign a cyclic order on X_n: $x_1 \prec x_2 \prec \cdots \prec x_n \prec x_1 \prec \cdots$.The set of questions $\mathcal{Q}$ consists of all cyclic intervals, with up to 2^k elements added or removed. Since $r = 4 \cdot 2^{-k}$, the number of questions is plainly at most

$$n^2 \binom{n}{2^k} 3^{2^k} \leq n^2 \big(\frac{3e}{4} r \cdot n\big)^{\frac{4}{r}},$$

using the inequality $\binom{n}{d} \leq \big(\frac{en}{d}\big)^d$.

High level of the proof. Let π be an arbitrary distribution on X_n, and let $r \in (0,1)$ be of the form $4 \cdot 2^{-k}$, with $k \geq 3$. Let μ be a Huffman distribution for π; we remind the reader that μ is a dyadic distribution corresponding to some optimal decision tree for π. We construct a decision tree T that uses only queries from $\mathcal{Q}$, with cost

$$T(\pi) \leq \mathrm{Opt}(\pi) + r + r^2 = \sum_{x \in X_n} \pi(x) \log \frac{1}{\mu(x)} + r + r^2.$$

The construction is randomized: we describe a randomized decision tree T_R ('R' denotes the randomness that determines the tree) which uses queries from $\mathcal{Q}$ and has the property that for every $x \in X_n$, the expected number of queries T_R uses to find x satisfies the inequality

$$\mathop{\mathbb{E}}_{R}[T_R(x)] \leq \log \frac{1}{\mu(x)} + r + r^2, \tag{3}$$

where $T_R(x)$ is the depth of x. This implies the existence of a deterministic tree with cost $\mathrm{Opt}(\mu) + r + r^2$: indeed, when $x \sim \mu$, the expected cost of T_R is

$$\mathop{\mathbb{E}}_{x \sim \pi; R}[T_R(x)] \leq \sum_{x \in X_n} \pi(x) \Big(\frac{1}{\mu(x)} + r + r^2 \Big) = \mathrm{Opt}(\pi) + r + r^2.$$

Since the randomness of the tree is independent from the randomness of π, it follows that there is a choice of R such that the cost of the (deterministic) decision tree T_R is at most $\mathrm{Opt}(\pi) + r + r^2$.

It is routine to derandomize the algorithm using the method of conditional expectations.

The randomized decision tree. The randomized decision tree maintains a dyadic *sub-distribution* $\mu^{(i)}$ that is being updated after each query. A *dyadic sub-distribution* is a measure on X_n such that (i) $\mu^{(i)}(x)$ is either 0 or a power of 2, and (ii) $\mu^{(i)}(X_n) = \sum_{x \in X_n} \mu^{(i)}(x) \leq 1$. A natural interpretation of $\mu^{(i)}(x)$ is as a dyadic sub-estimate of the probability that x is the secret element, conditioned on the answers to the first i queries. The analysis hinges on the following properties:

1. $\mu^{(0)} = \mu$,
2. $\mu^{(i)}(x) \in \big\{2\mu^{(i-1)}(x), \mu^{(i-1)}(x), 0\big\}$ for all $x \in X_n$,
3. if x is the secret element then almost always $\mu^{(i)}(x)$ is doubled; that is, $\mu^{(i)}(x) > 0$ for all i, and the expected number of i's for which $\mu^{(i)}(x) = \mu^{(i-1)}(x)$ is at most $r + r^2$.

These properties imply (3), which implies Theorem 8.5.

Next, we describe the randomized decision tree and establish these properties.

The algorithm distinguishes between light and heavy elements. An element $x \in X_n$ is *light* if $\mu^{(i)}(x) < 2^{-k}$. Otherwise it is *heavy*. The algorithm is based on the following win-win-win situation:

(i) If the total mass of the heavy elements is at least $1/2$ then by Lemma 4.1, there is a set I of heavy elements whose mass is exactly $1/2$. Since the number of heavy elements is at most 2^k, the algorithm can ask whether $x \in I$ and recurse by doubling the sub-probabilities of the elements that are consistent with the answer (and setting the others to zero).

(ii) Otherwise, the mass of the heavy elements is less than $1/2$. If the mass of the light elements is also less than $1/2$ (this could happen since $\mu^{(i)}$ is a sub-distribution), then we ask whether x is a heavy element or a light element, and accordingly recurse with either the heavy or the light elements, with their sub-probabilities doubled (in this case the "true" probabilities conditioned on the answers become larger than the sub-probabilities).

(iii) The final case is when the mass of the light elements is larger than $1/2$. In this case we query a random cyclic interval of light elements of mass $\approx 1/2$, and recurse; there are two light elements in the recursion whose sub-probability is not doubled (the probabilities of the rest are doubled).

Elements whose probability is not doubled occur only in case (iii).

The randomized decision tree: formal description. The algorithm gets as input a subset $y_1, \ldots, y_m$ of X_n whose order is induced by that of X_n, and a dyadic sub-distribution $q_1, \ldots, q_m$. Initially, the input is $x_1, \ldots, x_n$, and $q_i = \mu_i$.

We say that an element is *heavy* is $q_i \geq 2^{-k}$; otherwise it is *light*. There are at most 2^k heavy elements. The questions asked by the algorithm are cyclic intervals in $y_1, \ldots, y_m$, with some heavy elements added or removed. Since each cyclic interval in $y_1, \ldots, y_m$ corresponds to a (not necessarily unique) cyclic interval in X_n (possibly including elements outside of $y_1, \ldots, y_m$), these questions belong to $\mathcal{Q}$.

Algorithm T_R.

1. If $m = 1$, return y_1. Otherwise, continue to Step 2.

2. If the total mass of heavy elements is at least $1/2$ then find (using Lemma 4.1) a subset I whose mass is exactly $1/2$, and ask whether $x \in I$. Recurse with either $\{2q_i : y_i \in I\}$ or $\{2q_i : y_i \notin I\}$, according to the answer. Otherwise, continue to Step 3.

3. Let S be the set of all light elements, and let σ be their total mass. If $\sigma \leq 1/2$ then ask whether $x \in S$, and recurse with either $\{2q_i : y_i \in S\}$ or $\{2q_i : y_i \notin S\}$, according to the answer. Otherwise, continue to Step 4.

4. Arrange all light elements according to their cyclic order on a circle of circumference σ, by assigning each light element x_i an arc A_i of length q_i of the circle. Pick an arc of length $1/2$ uniformly at random (e.g. by picking uniformly a point on the circle and taking an arc of length $1/2$ directed clockwise from it), which we call the *window*. Let $K \subseteq S$ consist of all light elements whose midpoints are contained in the window, and let B consist of the light elements whose arcs are cut by the boundary of the window (so $|B| \leq 2$); we call these elements *boundary elements*. Ask whether $x \in K$; note that K is a cyclic interval in $y_1, \ldots, y_m$ with some heavy elements removed.

If $x \in K$, recurse with $\{2q_i : y_i \in K \setminus B\} \cup \{q_i : y_i \in K \cap B\}$. The sum of these dyadic probabilities is at most 1 since the window contains at least $q_i/2$ of the arc A_i for each $y_i \in K \cap B$.

If $x \notin K$, recurse with $\{2q_i : y_i \in \overline{K} \setminus B\} \cup \{q_i : y_i \in \overline{K} \cap B\}$. As in the preceding case, the total mass of light elements in the recursion is at most $2(\sigma - 1/2)$ (since the complement of the window contains at least $q_i/2$ of the arc A_i for each $y_i \in \overline{K} \cap B$), and the total mass of heavy elements is $2(1-\sigma)$, for a total of at most $(2\sigma - 1) + (2 - 2\sigma) = 1$. ◁

Analysis. We now finish the proof by establishing the three properties of the randomized decision tree that are stated above. The first two properties follow immediately from the description of the algorithm, and it thus remains to establish the third property. Fix some $x \in X_n$, and let $d \in \mathbb{N}$ be such that $\mu(x) = 2^{-d}$. We need to show that the expected number of questions that are asked when the secret element is x is at most $d + r + r^2$.

Let $q = q^{(i)}$ denote the sub-probability of x after the i'th question; note that $q \in \{2^{-j} : j \leq d\}$.

Lemma 8.2.1. *If $q \geq 2^{-k}$ then q doubles (that is, $q^{(i+1)} = 2q^{(i)}$). Otherwise, the expected number of questions until q doubles is at most $\frac{1}{1-4q}$.*

Proof. From the description of the algorithm, it is clear that the only case in which the sub-probability of x is not doubled is when x is one of the two boundary elements in Step 4. This only happens when x is a light element (i.e. $q < 2^{-k}$). The probability that x is one of the boundary elements is at most $2q/\sigma \leq 4q$, where $\sigma \geq 1/2$ is the total mass of light elements: indeed, the probability that a given endpoint of the window lies inside the arc corresponding to q is q/σ, since each endpoint is distributed uniformly on the circle of circumference σ.

It follows that the distribution of the number of questions that pass until q doubles is dominated by the geometric distribution with failure probability $4q$, and so the expected number of questions until q doubles is at most $\frac{1}{1-4q}$. □

The desired bound on the expected number of questions needed to find x follows from Lemma 8.2.1: as long as q, the sub-probability associated with x, is smaller than 2^{-k}, it takes an expected number of $\frac{1}{1-4q}$ questions until it doubles. Once $q \geq 2^{-k}$, it doubles after every question. Thus, by linearity of expectation, the expected total number of questions is at most:

$$\begin{aligned}
k + \sum_{j=k+1}^{d} \frac{1}{1 - 4 \cdot 2^{-j}} &< k + \sum_{j=k+1}^{d} [1 + 4 \cdot 2^{-j} + 2(4 \cdot 2^{-j})^2] \\
&= d + \sum_{j=k+1}^{d} [4 \cdot 2^{-j} + 2(4 \cdot 2^{-j})^2] \\
&< d + 4 \cdot 2^{-k} + \frac{2}{3}(4 \cdot 2^{-k})^2 \\
&< \log \frac{1}{\mu(x)} + r + r^2.
\end{aligned}$$

9 High min-entropy

We have shown that using comparison and equality queries, we can achieve redundancy 1 on every distribution: $r^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=) = 1$. The worst case is distributions concentrated almost entirely on one element. One can ask what redundancy can be achieved when the maximal probability of the given distribution π, denoted as $\pi_{\max}$, is very low, and analyze its asymptotic behavior as $\pi_{\max}$ goes to zero. This regime can be described as *high min-entropy* (the min-entropy, a quantity important in pseudorandomness theory, is given by $H_\infty(\pi) = \log \frac{1}{\pi_{\max}}$).

This natural question has been studied extensively in the case of Huffman codes, in a body of work [Gal78, Joh80, CGT86, Man92] culminating in the work of Manstetten [Man92], who determined the worst-case redundancy in terms of $\pi_{\max}$. We extend this analysis for decision trees using $\mathcal{Q}_\prec$ and for decision trees using $\mathcal{Q}_\prec \cup \mathcal{Q}_=$. Using similar proof techniques, we show that $r^{\mathrm{Opt}}(\mathcal{Q}_\prec) = 1$ and bound $u^{\mathrm{Opt}}(n, 1/2)$ and $u^{\mathrm{Opt}}(n, 1)$.

Formally, assume that $\mathcal{Q} = (\mathcal{Q}^{(1)}, \mathcal{Q}^{(2)}, \dots)$ is a sequence of sets of questions, where $\mathcal{Q}^{(n)}$ contains questions for the set X_n. Given $0 < p \leq 1$, define

$$r_p^H(\mathcal{Q}) = \sup_{\substack{n \in \mathbb{N}; \\ \pi \text{ distribution over } X_n \\ \text{s.t. } \pi_{\max} \leq p}} r^H(\mathcal{Q}^{(n)}, \pi).$$

Let $r_0^H(\mathcal{Q}) = \lim_{p \to 0} r_p^H(\mathcal{Q})$; we call this quantity the *asymptotic redundancy* of $\mathcal{Q}$. We similarly define $r_p^{\mathrm{Opt}}(\mathcal{Q})$ and $r_0^{\mathrm{Opt}}(\mathcal{Q})$, the *asymptotic prolixity* of $\mathcal{Q}$.

The question of determining the asymptotic redundancy has been considered regarding Huffman codes by Gallager [Gal78], who showed that the value is

$$r_0^H(2^X) = 1 - \log e + \log\log e \approx 0.086,$$

where $2^X = (2^{X_1}, 2^{X_2}, \dots)$. In more detail, he showed that $r_p^H(2^X) \leq p + (1 - \log e + \log\log e)$, and mentioned that this bound is achievable. We provide a proof of the lower bound on $r_0^H(2^X)$ in Section 9.4.

Regarding comparison and equality queries, we prove the following theorem:

Theorem 9.1. *The asymptotic prolixity of $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ is*

$$r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=) = 1/2.$$

The asymptotic redundancy of $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ satisfies

$$0.5011 \approx 3 - \log 3 - \log e + \log\log e \leq r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=) \leq 3/2 - \log e + \log\log e \approx 0.586.$$

Regarding only comparison queries, we prove the following theorem:

Theorem 9.2. *The asymptotic redundancy of $\mathcal{Q}_\prec$ is*

$$r_0^H(\mathcal{Q}_\prec) = 2 - \log e + \log\log e \approx 1.086.$$

The asymptotic prolixity of $\mathcal{Q}_\prec$ is

$$r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec) = 1.$$

For comparison, it is known that $r^H(\mathcal{Q}_{\prec}^{(n)}) = 2$ for all $n \geq 3$: the upper bound follows from Gilbert and Moore [GM59], and the lower bound from distributions concentrated almost entirely on one element in the middle. Additionally, $r^{\mathrm{Opt}}(\mathcal{Q}_{\prec}^{(n)}) = 1$ for $n \geq 3$: the lower bound is due to the same distribution, and the upper bound is by Nakatsu [Nak91]. As a consequence, $u^{\mathrm{Opt}}(n, 1) \leq n-1$ for all $n \geq 1$. We reproduce the techniques of Gilbert–Moore and Nakatsu in Section 9.1.

Our proof method also allows us to analyze interval queries:

Theorem 9.3. *For all $n \geq 1$,*

$$r^{\mathrm{Opt}}(\mathcal{Q}_{\square}^{(n)}) \leq 1/2.$$

As a consequence, $u^{\mathrm{Opt}}(n, 1/2) \leq \binom{n+1}{2}$.

Our upper bounds are based on an extension of the Gilbert–Moore algorithm [GM59], also known as Shannon–Fano–Elias encoding, and a precursor of arithmetic coding. Our lower bounds follow by computing the cost of distributions of the form $\epsilon, \alpha, \epsilon, \alpha, \ldots, \epsilon, \alpha, \epsilon$, which we call *padded uniform distributions*.

Section organization. We describe the Gilbert–Moore method and discuss our extensions in Section 9.1. A simple application of this technique appears in Section 9.2, in which we prove Theorem 9.3. A more sophisticated application appears in Section 9.3, in which we prove the upper bound parts of Theorem 9.1. We prove all lower bounds and Theorem 9.2 in Section 9.4.

9.1 Gilbert–Moore and its extensions

The algorithms in this section are based on the Gilbert–Moore method [GM59] (also known as Shannon–Fano–Elias encoding). This encoding scheme, which corresponds to an algorithm using only comparison queries (i.e. the set $\mathcal{Q}_{\prec}$), proceeds as follows.

Let π be a distribution over X_n. We associate with each element $x_i \in X_n$ a point $p_i \in [0, 1]$. The algorithm performs a binary search over $[0, 1]$, maintaining an interval that contains the "live" elements (those consistent with the answers to the preceding questions). The initial interval is $[0, 1]$, and its length decreases by half in each iteration. At each step, the algorithm asks a comparison query which separates the elements in the left half of the interval from those in its right half. The algorithm stops whenever the interval contains only a single element. Setting $p_i = \pi_1 + \cdots + \pi_{i-1} + \pi_i/2$ guarantees that element x_i will be identified whenever the interval is of length at most $\pi_i/2$; this takes at most $\lceil \log(2/\pi_i) \rceil$ questions, for a total average of

$$\sum_{i=1}^{n} \pi_i \left\lceil \log \frac{2}{\pi_i} \right\rceil < \sum_{i=1}^{n} \pi_i \left(\log \frac{2}{\pi_i} + 1 \right) = H(\pi) + 2.$$

The bound can be improved to $\mathrm{Opt}(\pi) + 1$ (this implies the preceding bound since $\mathrm{Opt}(\pi) < H(\pi) + 1$), as was noticed by Nakatsu [Nak91]. Let τ be a Huffman distribution for π (recall that this is a dyadic distribution which corresponds to some optimal unrestricted decision tree for π). Setting $p_i = \tau_1 + \cdots + \tau_{i-1} + \tau_i/2$ guarantees that it takes $\lceil \log(2/\tau_i) \rceil = \log(2/\tau_i)$ questions to identify x_i, for a total average of

$$\sum_{i=1}^{n} \pi_i \left(\log \frac{2}{\tau_i} \right) = \mathrm{Opt}(\pi) + 1.$$

This proves that $r^{\mathrm{Opt}}(\mathcal{Q}_{\prec}) \leq 1$.

Enabling also equality queries (i.e. the set $\mathcal{Q}_=$), and introducing randomness, we can reduce the cost further. Each element x_i is assigned an interval $T_i \subseteq [0,1]$ which is disjoint from the other intervals and placed between T_{i-1} and T_{i+1}, and a point p_i which is the midpoint of T_i. While Gilbert–Moore maintains an interval in its binary search, the new algorithm maintains an interval-with-holes I. The algorithm behaves similarly to Gilbert–Moore, with the following change: whenever I contains an interval T_i of size $|I|/2$ in its entirety, the algorithm asks whether $x = x_i$ (recall that x is the secret element). If the question is answered positively then the algorithm stops, and otherwise T_i is removed from I, creating a hole.

Placing the intervals $T_1, \ldots, T_n$ along $[0,1]$ randomly allows getting non-trivial bounds on the expected number of questions required to identify each element. Such random placements enables us to prove Theorem 9.3 as well as the following Lemma 9.4:

Lemma 9.4. *Suppose that π is a distribution in which the maximum element has probability less than $1/(2^\ell - 1)$. Then there is an algorithm using $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ with cost at most* $\mathrm{Opt}(\pi) + 1/2 + 2^{2-\ell}$.

Lemma 9.4 almost immediately implies the upper bound parts of Theorem 9.1.

9.2 Upper bound for interval queries

In this subsection we flesh out the ideas in the preceding subsection, proving Theorem 9.3: given a distribution π, we construct a randomized algorithm using $\mathcal{Q}_\square$ whose expected cost is at most $\mathrm{Opt}(\pi) + 1/2$.

Let π be a distribution over X_n, and let τ be a Huffman distribution for π.

Algorithm CP. Associate with each element x_i an interval of length τ_i on the unit circumference circle, whose points we identify with $[0,1)$: choose a uniformly random starting point, and place the intervals $T_1, \ldots, T_n$ consecutively. Denote the midpoint of T_i by p_i.

The algorithm maintains an interval-with-holes—an interval in $[0,1)$ from which some of the intervals T_i have potentially been removed—which contains the midpoints p_i corresponding to the *live elements*, which are those consistent with the answers to previous questions. We denote the interval-with-holes after the ℓ'th question by I_ℓ, and maintain the invariant that the length of I_ℓ (excluding the holes) is exactly $2^{-\ell}$.

Initialize $I_0 = [0,1)$, and execute the following steps for $\ell = 1, 2, \ldots$ until I_ℓ contains a single element:

1. If $I_{\ell-1}$ completely contains some interval T_i of size $2^{-\ell}$ then ask whether $x = x_i$ (if there exist two such elements, choose one arbitrarily; both questions are equivalent). If so, terminate. Otherwise, remove T_i from $I_{\ell-1}$ to obtain I_ℓ, and continue to the next iteration.

2. If $I_{\ell-1}$ contains no interval of size $2^{-\ell}$ in its entirety, partition $I_{\ell-1}$ into two intervals-with-holes of length $2^{-\ell}$ (this could cut one of the intervals T_i into two halves), and ask which one contains the midpoint corresponding to x. Set I_ℓ accordingly, and continue to the next iteration. ◁

Each question in the algorithm can be implemented using an interval query, since in Step 1 it is an equality query (which is also an interval query), and in Step 2 it is patently an interval query.

The analysis of the algorithm relies on crucial properties of I_ℓ:

Lemma 9.2.1. *For all $\ell \geq 0$, the interval I_ℓ satisfies the following two properties:*

1. *The two endpoints of I_ℓ are of the form $a/2^\ell$ for some integer a.*

2. *The length of each hole is 2^{-r} for $r \leq \ell$.*

Proof. The proof is by induction. Both properties clearly hold for I_0. Supposing that they hold for $I_{\ell-1}$, we will prove that they also hold for I_ℓ, depending on which of the two steps in the algorithm was executed.

In Step 1, we form I_ℓ by removing an interval of length $2^{-\ell}$ from $I_{\ell-1}$. This shows that the second property is maintained. If the hole doesn't touch the endpoints, the first property is clearly maintained. If the hole touches the left endpoint $a/2^{\ell-1}$ (the other case is similar) then the new left endpoint is

$$\frac{a}{2^{\ell-1}} + 2^{-\ell} + \sum_j 2^{-r_j},$$

where the 2^{-r_j} are the lengths of all holes which are skipped (if any). Since $r_j \leq \ell - 1$ for all j by the induction hypothesis, the new left endpoint is of the form $a'/2^\ell$.

In Step 2, we form I_ℓ by splitting $I_{\ell-1}$ at a midpoint (there could be two midpoints, on two sides of a hole). This is the same as cutting out intervals of total length $2^{-\ell}$ (possibly splitting one of them into two parts), and an analysis as in Step 1 shows that both properties are maintained. □

The performance of the algorithm is captured by the following lemma:

Lemma 9.2.2. *For all $x_i \in X_n$, Algorithm CP uses at most $\log \frac{1}{\tau_i} + 1/2$ questions, in expectation, to identify x_i as the secret element.*

Proving the lemma completes the proof of Theorem 9.3, since the expected number of queries of Algorithm CP is at most

$$\sum_{i=1}^{n} \pi_i \left(\log \frac{1}{\tau_i} + \frac{1}{2} \right) = \mathrm{Opt}(\pi) + \frac{1}{2}.$$

It is routine to derandomize the algorithm using the method of conditional expectations.

Proof of Lemma 9.2.2. Consider an element $x_i \in X_n$ as the secret element, and let $\tau_i = 2^{-m}$. Since T_i is placed at a random position in the unit circle, its midpoint p_i is a random point on the unit circle. We let $p_i = (b + \theta)/2^{1-m}$, where b is an integer and $\theta \in [0, 1)$ is distributed uniformly on $[0, 1)$. Denote by E the event that $1/4 \leq \theta \leq 3/4$, which happens with probability $1/2$. Since $(1/4)/2^{1-m} = |T_i|/2$, in that case $T_i \subseteq [b/2^{1-m}, (b + 1)/2^{1-m}]$.

If the algorithm reaches iteration $\ell = m + 1$, then the interval I_{m+1} is an interval of length 2^{-m-1} containing the midpoint of T_i. Since half of T_i already has length 2^{-m-1}, we see that I_{m+1} must contain only T_i. In other words, the algorithm always terminates after asking at most $m + 1$ questions.

We now show that if the event E happens then the algorithm finds x_i after asking at most m questions. Indeed, suppose that x_i has not been found after $m - 1$ questions. Since I_{m-1} contains the midpoints of all live elements, it contains $p_i = (b + \theta)/2^{1-m}$. On the other hand, the endpoints of I_{m-1} are of the form $a/2^{1-m}$, and so I_{m-1} contains all of $[b/2^{1-m}, (b + 1)/2^{1-m}] \supseteq T_i$. Thus Step 1 is executed at iteration $\ell = m$, revealing x_i.

We conclude that x_i is found after at most $(1/2)m + (1/2)(m + 1) = m + 1/2 = \log \frac{1}{\tau_i} + 1/2$ questions, in expectation. □

We can slightly modify the algorithm in order to handle non-dyadic distributions τ. We change the condition of Case 1 from containing all of an interval T_i of length $2^{-\ell}$ to containing a part of length at least $2^{-\ell}$ of an interval T_i, including its midpoint p_i. Also, instead of removing T_i from $I_{\ell-1}$ we remove a sub-interval of T_i of length $2^{-\ell}$ that contains the midpoint p_i.

A very similar analysis then shows that element x_i is found after $\log \frac{1}{\tau_i} + 1 - \alpha$ questions in expectation, where $\alpha \in [1/2, 1)$ is the unique number in $[1/2, 1)$ satisfying $\tau_i = \alpha/2^{1-m}$.

9.3 Upper bound for comparison and equality queries

The main idea in the previous subsection was to place the intervals at a uniformly random position, and this implied that the expected number of queries required to find x_i is $\log \frac{1}{\tau_i} + 1/2$. As can be verified by examining the proof of Lemma 9.2.2, it is sufficient that $p_i \bmod 2\tau_i$ be distributed uniformly in $[0, 2\tau_i)$. The following algorithm exploits this idea to reduce the set of questions from $\mathcal{Q}_\square$ to $\mathcal{Q}_\prec \cup \mathcal{Q}_=$.

Let π be a distribution over X_n, and let τ be a Huffman distribution for π with maximal probability $\tau_{\max} = 2^{-\ell}$.

Algorithm IP. Partition X_n into $2^{\ell-2}$ sets of measure $2^{-(\ell-2)}$ (Lemma 4.1 shows that this is always possible). Choose a random such set, and halve all of its probabilities. Let $q_1, \ldots, q_n$ be the resulting sub-distribution; note that these probabilities sum to $1 - 2^{-(\ell-1)}$.

Associate with each element x_i an interval of length q_i on the unit interval $[0, 1]$ by choosing a random starting point in $[0, 2^{-(\ell-1)})$ and placing the intervals $T_1, \ldots, T_n$ consecutively.

Continue as in Algorithm CP, replacing the placement of the intervals $T_1, \ldots, T_n$ with the one described here. ◁

The analog of Lemma 9.2.2 is:

Lemma 9.3.1. *For all $x_i \in X_n$, Algorithm IP uses at most $\log \frac{1}{\tau_i} + 1/2 + 4\tau_{\max}$ questions, in expectation, to identify x_i as the secret element.*

Proof. Let $p_i = (b + \theta)/2^{1-m}$, as in the proof of Lemma 9.2.2. That proof only relied on the fact that θ is distributed uniformly on $[0, 1)$. Since $m \geq \ell$ and the starting point of T_1 was uniform in $[0, 2^{-(\ell-1)})$, this still holds, and so the proof of Lemma 9.2.2 implies that given $q_1, \ldots, q_n$, the expected number of questions to identify x_i is at most

$$\log \frac{1}{q_i} + \frac{1}{2}.$$

On the other hand, $q_i = \tau_i$ with probability $1 - 2^{-(\ell-2)} = 1 - 4\tau_{\max}$, and $q_i = \tau_i/2$ with probability $4\tau_{\max}$. The lemma immediately follows. □

In order to deduce Lemma 9.4, we need to relate the maximal probability in an arbitrary distribution π to the maximal probability in a Huffman distribution τ for π:

Claim 9.3.2 ([CS92, Lemma 1])**.** *Let π be any distribution, and let τ be a corresponding Huffman distribution. If the maximal probability in τ is $2^{-\ell}$ then the maximal probability in π is at least $1/(2^{\ell+1} - 1)$.*

In order to make the paper self-contained, we prove this simple claim.

Proof. Consider the decision tree corresponding to τ, and let x_i be a leaf at depth ℓ of maximum measure under π; such a leaf exists by assumption.

If y is an internal node at depth ℓ then we claim that $\pi(y) \le 2\pi(x_i)$ (here $\pi(y)$ is the weight of leaves in the subtree rooted at y). Indeed, otherwise y has a child z satisfying $\pi(z) > \pi(x_i)$; since z is at depth $\ell + 1$ while x_i is at depth ℓ, exchanging x_i and z would decrease the cost of the tree, leading to a contradiction.

Since x_i is a leaf at minimum depth, there are exactly $2^\ell - 1$ other nodes at level ℓ. Each such node y satisfies $\pi(y) \le 2\pi(x_i)$ (we have shown this for internal nodes, and it holds for leaves by the choice of x_i). In total, we find that the sum of $\pi(y)$ over all nodes at level ℓ is at most $\pi(x_i) + (2^\ell - 1) \cdot 2\pi(x_i) = (2^{\ell+1} - 1)\pi(x_i)$. Since this sum equals 1, we deduce that $\pi(x_i) \ge 1/(2^{\ell+1} - 1)$. □

Lemma 9.4 immediately follows:

Proof of Lemma 9.4. Let τ be a Huffman distribution corresponding to π. Claim 9.3.2 shows that all probabilities in τ are at most $2^{-\ell}$. Lemma 9.3.1 shows that Algorithm IP uses this many questions in expectation:

$$\sum_{i=1}^{n} \pi_i \left(\log \frac{1}{\tau_i} + \frac{1}{2} + 2^{2-\ell} \right) = \mathrm{Opt}(\pi) + \frac{1}{2} + 2^{2-\ell}. \qquad \square$$

The upper bound $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=) \le 1/2$ in Theorem 9.1 immediately follows. The upper bound on $r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=)$ follows from a classical result of Gallager:

Theorem 9.3.3 ([Gal78, Theorem 2])**.** *If the distribution π on X_n has maximum probability $\pi_{\max}$ then $r^{\mathrm{Opt}}(2^{X_n}, \pi) \le \pi_{\max} + 1 - \log e + \log\log e$.*

We prove the corresponding lower bound $r_0^{\mathrm{Opt}}(2^X) \ge 1 - \log e + \log\log e$ in Section 9.4.

9.4 Lower bounds

In this subsection we lower bound the values of r_0^H and r_0^{Opt} on the sets $\mathcal{Q}_\prec$ and $\mathcal{Q}_\prec \cup \mathcal{Q}_=$:

Lemma 9.5. *The asymptotic redundancy and prolixity of $\mathcal{Q}_\prec$ and $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ are lower bounded by*

$$\begin{aligned}
&r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=) \ge 3 - \log 3 - \log e + \log\log e \approx 0.5011,\\
&r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=) \ge 1/2,\\
&r_0^H(\mathcal{Q}_\prec) \ge 2 - \log e + \log\log e \approx 1.08607,\\
&r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec) \ge 1.
\end{aligned}$$

This allows us to complete the proofs of all theorems stated in the introduction: the first two inequalities complete the proof of Theorem 9.1 (the upper bound on $r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=)$ was proved in Section 9.3, and the one on $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=)$ follows from Lemma 9.4), and the latter two inequalities complete the proof of Theorem 9.2 (the upper bound on $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec)$ is the same as the upper bound on $r^{\mathrm{Opt}}(\mathcal{Q}_\prec)$ presented in Section 9.1 and due to Nakatsu [Nak91], and the one on $r_0^H(\mathcal{Q}_\prec)$ follows via Theorem 9.3.3).

To simplify notation, in this subsection we consider distributions in which some elements have zero probability. In contrast to the definition in Section 4, we ask that any decision tree for such distributions be correct on *all* elements. The same lower bounds can be achieved on full support

distributions by replacing all zero probability elements with small probability elements; details left to the reader.

The distributions we are interested in are *padded uniform distributions*:

- $\mathrm{U}_n = (1/n, \ldots, 1/n)$; for example, $\mathrm{U}_2 = (1/2, 1/2)$.
- $\mathrm{U}_n^0 = (0, 1/n, \ldots, 1/n)$; for example, $\mathrm{U}_2^0 = (0, 1/2, 1/2)$.
- $\mathrm{P}_n = (1/n, 0, 1/n, \ldots, 0, 1/n)$; for example, $\mathrm{P}_2 = (1/2, 0, 1/2)$.
- $\mathrm{P}_n^0 = (0, 1/n, 0, 1/n, \ldots, 0, 1/n)$; for example, $\mathrm{P}_2^0 = (0, 1/2, 0, 1/2)$.
- $\mathrm{P}_n^{00} = (0, 1/n, 0, 1/n, \ldots, 0, 1/n, 0)$; for example, $\mathrm{P}_2^{00} = (0, 1/2, 0, 1/2, 0)$.

We calculate the cost of these distributions under $\mathcal{Q}_{\prec}$ and under $\mathcal{Q}_{\prec} \cup \mathcal{Q}_{=}$, and compare these to the optimal costs. In all cases, we will show that the best strategy is to split the distributions as equally as possible, at least for large enough n.

It will be useful to work with a scaled cost,

$$C(Q, \mathrm{U}_n) = n \cdot c(Q, \mathrm{U}_n),$$

defined analogously for the other distributions.

The following observation will be crucial:

Lemma 9.4.1. *Suppose $n = \alpha 2^k$, where $\alpha \in [1/2, 1]$. Then $\ell n - 2^\ell$ is maximized over the integers at $\ell = k$.*

Proof. Let $\Delta_\ell = \ell n - 2^\ell$. Note that

$$\Delta_{\ell+1} - \Delta_\ell = (\ell + 1)n - \ell n - 2^{\ell+1} + 2^\ell = n - 2^\ell.$$

Thus $\Delta_{\ell+1} \geq \Delta_\ell$ iff $n \geq 2^\ell$. In particular, since $n \geq 2^{k-1}$ we conclude that $\Delta_k \geq \Delta_{k-1} \geq \cdots$, and since $n \leq 2^k$ we conclude that $\Delta_k \geq \Delta_{k+1} \geq \cdots$. □

Corollary 9.4.2. *Let $B > 0$, and suppose that $n = B\alpha 2^k$, where $\alpha \in [1/2, 1]$. Then $\ell n - B2^\ell$ is maximized over the integers at $\ell = k$.*

Proof. Apply the lemma to $m = n/B$, noticing that $\ell n - B2^\ell = B(\ell m - 2^\ell)$. □

We start by analyzing the cost of these distributions under unrestricted decision trees:

Lemma 9.4.3. *Suppose $n = \alpha 2^k$, where $\alpha \in [1/2, 1]$. Then*

$$c(2^{X_n}, \mathrm{U}_n) = k + 1 - \frac{1}{\alpha},$$
$$c(2^{X_n}, \mathrm{U}_n^0) = k + 1 - \frac{1 - 2^{-k}}{\alpha}.$$

Moreover, the bound on U_n^0 holds for any distribution obtained from U_n by adding any (positive) number of zeroes, and in particular for $\mathrm{P}_n, \mathrm{P}_n^0, \mathrm{P}_n^{00}$.

Proof. In terms of the scaled cost, our goal is to prove

$$C(2^X, \mathrm{U}_n) = (k+1)n - 2^k,$$
$$C(2^X, \mathrm{U}^0_n) = (k+1)n - 2^k + 1.$$

The proof is by induction on n. For the base case, $n = 1$, we are claiming that $C(2^X, (1)) = 0$ and $C(2^X, (0,1)) = 1$; both claims are easy to verify.

Suppose now that $n > 1$. Any non-trivial algorithm for U_n splits U_n into $\mathrm{U}_{n_1}, \mathrm{U}_{n_2}$ for some $n_1 + n_2 = n$, where $n_1, n_2 \geq 1$. Lemma 9.4.1 (choosing $\ell = k - 1$) shows that the scaled cost of such an algorithm is

$$n + C(2^X, \mathrm{U}_{n_1}) + C(2^X, \mathrm{U}_{n_2}) \geq n + [kn_1 - 2^{k-1}] + [kn_2 - 2^{k-1}] = (k+1)n - 2^k.$$

To show that $(k+1)n - 2^k$ can be achieved, we consider two cases. If $n = 2m$ then $2^{k-2} \leq m \leq 2^{k-1}$, and so splitting U_n into $\mathrm{U}_m, \mathrm{U}_m$ results in a scaled cost of

$$n + 2(km - 2^{k-1}) = (k+1)n - 2^k.$$

If $n = 2m + 1$ then $2^{k-2} \leq m + 1/2 \leq 2^{k-1}$, and so $2^{k-2} \leq m \leq m + 1 \leq 2^{k-1}$. Splitting U_n into $\mathrm{U}_m, \mathrm{U}_{m+1}$ thus results in a scaled cost of

$$n + [km - 2^{k-1}] + [k(m+1) - 2^{k-1}] = (k+1)n - 2^k.$$

This completes the proof in the case of U_n.

The proof of the inductive step for U^0_n is very similar, and left to the reader; the crucial observation is that any non-trivial algorithm splits U^0_n into $\mathrm{U}_{n_1}, \mathrm{U}^0_{n_2}$ for some positive n_1, n_2 satisfying $n_1 + n_2 = n$.

Finally, the claim about distributions obtained from U^0_n by adding zeroes follows from Huffman's algorithm. □

We continue by analyzing the cost under decision trees using $\mathcal{Q}_\prec$:

Lemma 9.4.4. *Suppose $n = \alpha 2^k$, where $\alpha \in [1/2, 1]$. Then*

$$c(\mathcal{Q}_\prec, \mathrm{P}_n) = k + 2 - \frac{1 + 2^{-k}}{\alpha},$$
$$c(\mathcal{Q}_\prec, \mathrm{P}^0_n) = k + 2 - \frac{1}{\alpha},$$
$$c(\mathcal{Q}_\prec, \mathrm{P}^{00}_n) = k + 2 - \frac{1 - 2^{-k}}{\alpha}.$$

Proof. The proof of this lemma is very similar to the proof of Lemma 9.4.3. In terms of the scaled cost, we are aiming at proving the following:

$$C(\mathcal{Q}_\prec, \mathrm{P}_n) = (k+2)n - 2^k - 1,$$
$$C(\mathcal{Q}_\prec, \mathrm{P}^0_n) = (k+2)n - 2^k,$$
$$C(\mathcal{Q}_\prec, \mathrm{P}^{00}_n) = (k+2)n - 2^k + 1.$$

When $n = 1$, we verify that $c(\mathcal{Q}_\prec, (1)) = 0$, $c(\mathcal{Q}_\prec, (0,1)) = 1$, and $c(\mathcal{Q}_\prec, (0,1,0)) = 2$.

For the induction step, note that the distributions split as follows:

$$\begin{aligned}
\mathrm{P}_n &\longrightarrow \mathrm{P}_{n_1}, \mathrm{P}^0_{n_2}, \\
\mathrm{P}^0_n &\longrightarrow \mathrm{P}_{n_1}, \mathrm{P}^{00}_{n_2} \mid \mathrm{P}^0_{n_1}, \mathrm{P}^0_{n_2}, \\
\mathrm{P}^{00}_n &\longrightarrow \mathrm{P}^0_{n_1}, \mathrm{P}^{00}_{n_2},
\end{aligned}$$

where in all cases, $n_1 + n_2 = n$. The rest of the proof is very similar to that of Lemma 9.4.3, and we leave it to the reader. □

Finally, we analyze the cost under decision trees using $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ (a similar calculation appears in Spuler [Spu94b]):

Lemma 9.4.5. *Suppose $n = 3\alpha 2^k$, where $\alpha \in [1/2, 1]$ and $k \geq 0$. Then*

$$c(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}_n) = k + 3 - \frac{1}{\alpha},$$

and the same formula holds for P^0_n and P^{00}_n.

When $n = 1$:

$$\begin{aligned}
c(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}_1) &= 0, \\
c(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}^0_1) &= c(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}^{00}_1) = 1.
\end{aligned}$$

Proof. In terms of the scaled cost, our goal is to prove that for $n > 1$,

$$C(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}_n) = (k+3)n - 3 \cdot 2^k,$$

and the same holds for P^0_n and P^{00}_n.

The base case requires us to verify that $C(\mathcal{Q}_\prec \cup \mathcal{Q}_=, (1)) = 0$ while $C(\mathcal{Q}_\prec \cup \mathcal{Q}_=, (0;1)) = C(\mathcal{Q}_\prec \cup \mathcal{Q}_=, (0;1;0)) = 1$.

We also need to verify the cases $n = 2$ and $n = 3$ manually. We verify that the scaled cost of the distributions $\mathrm{P}_2, \mathrm{P}^0_2, \mathrm{P}^{00}_2$ is 3, and that of $\mathrm{P}_3, \mathrm{P}^0_3, \mathrm{P}^{00}_3$ is 6.

The induction step is very similar to the analysis in Lemma 9.4.4, replacing Lemma 9.4.1 by Corollary 9.4.2 (with $B = 3$); note that equality queries correspond to the choice $n_1 = 1$, since the surrounding zero probability elements (if there is more than one) can be merged without affecting the cost.

There is one slight difficulty: the analysis uses the formulas for the scaled costs of $\mathrm{P}_m, \mathrm{P}^0_m, \mathrm{P}^{00}_m$, but these are invalid when $m = 1$. These formulas are used for both the lower bound and the upper bound. The case $m = 1$ only appears in the upper bound when $n \leq 3$. In the lower bound, the formulas are used only via Corollary 9.4.2 applied to $\ell = k - 1$. In view of this, it suffices to verify that when $n \geq 4$ (and so $k \geq 1$), the inequality $C(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}_1) = 0 \geq (k+2) - 3 \cdot 2^{k-1}$ holds. □

We conclude with the proof of Lemma 9.5:

Proof of Lemma 9.5. We start by proving the results on $\mathcal{Q}_\prec$. Let $n = \alpha 2^k$, where $\alpha \in [1/2, 1]$. Lemma 9.4.4 shows that

$$c(\mathcal{Q}_\prec, \mathrm{P}^0_n) - H(\mathrm{P}^0_n) = \big[k + 2 - \frac{1}{\alpha}\big] - \big[k + \log \alpha\big] = 2 - \frac{1}{\alpha} - \log \alpha.$$

The choice of $\alpha \in [1/2, 1]$ that maximizes this quantity is $\alpha = 1/\log e$, and this shows that $r^H_0(\mathcal{Q}_\prec) \geq 2 - \log e + \log\log e$; note that while $2^k/\log e$ is never an integer, for large k the quantity

α_k defined by $\alpha_k 2^k = \lfloor \alpha 2^k \rfloor$ is very close to α, and so in the limit $k \to \infty$ we obtain the stated bound.

Lemma 9.4.4 and Lemma 9.4.3 together show that

$$c(\mathcal{Q}_\prec, \mathrm{P}_n^{00}) - c(2^X, \mathrm{P}_n^{00}) = \big[k + 2 - \frac{1-2^{-k}}{\alpha}\big] - \big[k + 1 - \frac{1-2^{-k}}{\alpha}\big] = 1.$$

This shows that $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec) \geq 1$.

We continue with the lower bound on $r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=)$. Let $n = 3\alpha 2^k$, where $\alpha \in [1/2, 1]$ and $k \geq 0$. Lemma 9.4.5 shows that

$$c(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}_n) - H(\mathrm{P}_n) = \big[k + 3 - \frac{1}{\alpha}\big] - \big[k + \log 3 + \log \alpha\big] = 3 - \log 3 - \frac{1}{\alpha} - \log \alpha.$$

The choice of $\alpha \in [1/2, 1]$ that maximizes this quantity is $\alpha = 1/\log e$, and this shows that $r_0^H(\mathcal{Q}_\prec) \geq 3 - \log 3 - \log e + \log \log e$.

Finally, we prove the lower bound on $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=)$. Let $n = 2^k = 3\alpha 2^{k-1}$, where $\alpha := 2/3$. Lemma 9.4.5 and Lemma 9.4.3 together show that

$$c(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \mathrm{P}_n) - c(2^X, \mathrm{P}_n) = \big[k + \frac{1}{2}\big] - \big[k + 2^{-k}\big] = \frac{1}{2} - 2^{-k}.$$

This shows that $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=) \geq 1/2$. □

10 Open questions

Our work naturally leads to many open questions. We list quite a few of them.

10.1 Questions on $\mathcal{Q}_\prec \cup \mathcal{Q}_=$

Let us start by listing our main results on this set of questions:

- Theorem 5.1 shows that $r^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=) \leq 1$.
- Theorem 9.1 shows that $r_0^{\mathrm{Opt}}(\mathcal{Q}_\prec \cup \mathcal{Q}_=) = 1/2$ (see Section 9 for the relevant definitions).
- Theorem 9.1 also gives the bounds $0.5011 < r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=) < 0.5861$.

This prompts the following questions:

Open Question 1. *What is $u^H(n, 1)$?*

Notes Theorem 5.1 implies that $u^H(n, 1) \leq 2n - 3$, and on the other hand it is easy to see that $u^H(n, 1) \geq n$, since all equality queries are necessary. Can we replace $\mathcal{Q}_\prec$ with a smaller set of questions? Concretely, what happens if we only use comparison queries of the form $x \prec x_{2i}$?

Open Question 2. *How fast can we compute $r^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \pi)$?*

Notes The optimal Huffman tree (that is, $r^H(2^{X_n}, \pi)$) can be computed in time $O(n \log n)$, as shown by van Leeuwen [vL87]. The optimal alphabetic tree (that is, $r^H(\mathcal{Q}_\prec, \pi)$) can also be computed in time $O(n \log n)$, as shown by Hu and Tucker [HT71] and by Garsia and Wachs [GW77].

In contrast, the fastest known algorithm to compute the best binary comparison search tree (that is, $r^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \pi)$), due to Anderson et al. [AKKL02] (who improved the algorithm of Spuler [Spu94a]), runs in time $O(n^4)$. In contrast to the algorithms in the preceding cases, this algorithm uses a simple dynamic programming approach. Can one compute $r^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=, \pi)$ in time $O(n \log n)$?

Open Question 3. *What is $r_0^H(A_t)$?*

Notes As in Section 9, we can define $r_p^H(A_t)$ is the supremum of the redundancy of A_t on distributions π with $\pi_{\max} \le p$ (where $\pi_{\max}$ is the maximal probability of an element in π), and $r_0^H(A_t)$ as the limit at $p = 0$.

In this language, Theorem 5.1 shows that $r_{0.9961}^H(A_t) \le 0.96711$. On the other hand, Theorem 9.1 implies that $r_0^H(A_t) > 0.5011$.

Open Question 4. *What is the redundancy of $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ if we limit the number of questions that the algorithm can ask in the worst case?*

Notes While Algorithm A_t asks a small expected number of questions (at most 1 more than the optimum), there could be elements on which the algorithm asks $n-1$ questions; this is the case for the distribution $1/2, 1/4, \ldots, 1/2^{n-1}, 1/2^{n-1}$, for example.

For unrestricted decision trees, it is known that restricting the maximal number of questions per element to roughly $\log n$ suffices to obtain small redundancy: Gilbert [Gil71] showed that bounding the number of questions per element by $\log n + \log\log n + K + 1$ achieves redundancy $1 + 2^{-K}$, and Evans and Kirkpatrick [EK04] showed that bounding it by $\lceil \log n \rceil + 1$ achieves redundancy 2. Computing the optimal length-restricted binary search tree has also been studied extensively [HT72, Gar74, Lar87, Sch98, Bae07].

Can we achieve constant redundancy using $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ under the restriction that at most $O(\log n)$ questions are asked on every element?

Open Question 5. *What is $r_0^H(\mathcal{Q}_\prec \cup \mathcal{Q}_=)$?*

Notes As stated above, Theorem 9.1 gives non-matching lower and upper bounds.

Open Question 6. *Is there a dynamic version of Algorithm A_t?*

Notes Vitter [Vit87], improving on earlier work of Faller [Fal73], Gallager [Gal78], and Knuth [Knu85], gave an algorithm for maintaining a dynamic Huffman tree. His algorithm runs in real time (updating the tree takes $O(1)$ operations per output bit), and its average cost is at most $\mathrm{Opt}(\mu) + 1$, where μ is the empirical distribution.

Grinberg, Rajagopalan, Venkatesan and Wei [GRVW95] considered the same question for alphabetic trees (binary search trees without keys in internal nodes). Their algorithm, based on splay trees (but using the improved technique of "semisplaying"), achieves an average cost of at most roughly $2c(\mathcal{Q}_\prec, \mu) + 2$.

Can we match Vitter's result in the context of Algorithm A_t? A dynamic version of Algorithm A_t would maintain a decision tree using $\mathcal{Q}_\prec \cup \mathcal{Q}_=$ with redundancy 1 with respect to the current empirical distribution, and will have average cost of at most $H(\mu) + O(1)$, or at the very least, at most $O(H(\mu))$.

10.2 Questions on $u^{\mathrm{Opt}}(n, 0)$

Our main results on $u^{\mathrm{Opt}}(n, 0)$ include:

1. For all n, $u^{\mathrm{Opt}}(n, 0) \leq 1.25^{n+o(n)}$ (Theorem 7.2).
2. For all n, $u^{\mathrm{Opt}}(n, 0) \geq 1.232^{n-o(n)}$ (Theorem 7.3).
3. For all n of the form $n = 1.25 \cdot 2^m$, $u^{\mathrm{Opt}}(n, 0) \geq 1.25^{n-o(n)}$ (Theorem 7.3).
4. For all n there is an explicit set of $O(2^{n/2})$ questions which supports efficient construction of optimal decision trees (Theorem 7.5).

Our work leaves several questions unanswered:

Open Question 7. *What is the value of $u^{\mathrm{Opt}}(n, 0)$ for n not of the form $n = 1.25 \cdot 2^m$?*

Notes While our work determines $u^{\mathrm{Opt}}(n, 0)$ for $n = 1.25 \cdot 2^m$ up to subexponential factors, for general n our bounds only imply

$$1.232^{n-o(n)} \leq u^{\mathrm{Opt}}(n, 0) \leq 1.25^{n+o(n)}.$$

Theorem 7.3.1 reduces the problem to that of computing the quantity $\rho_{\min}(n)$, which determines $u^{\mathrm{Opt}}(n, 0)$ up to polynomial factors.

The hard distribution used to derive the lower bound for $n = 1.25 \cdot 2^m$ consists of $0.4n - 1$ leaves at depth $m - 1$, and $0.6n + 1$ "small" elements. We can obtain a similar lower bound for values of n close to $1.25 \cdot 2^m$, but for other values of n it seems that a different construction is needed.

We conjecture that rate of growth of $u^{\mathrm{Opt}}(n, 0)$ depends only on the fractional value of $\log n$. In more detail, we conjecture that there exists a function $G\colon [1, 2] \to \mathbb{R}$ such that for $\alpha \in [1, 2]$ and $n = \alpha 2^m$,

$$u^{\mathrm{Opt}}(n, 0) = G(\alpha)^{n \pm o(n)}.$$

The proof of Theorem 7.3 shows that

$$G(\alpha) \geq \max(2^{h(\frac{1}{2\alpha}) - \frac{1}{\alpha}}, 2^{h(\frac{1}{4\alpha}) - \frac{1}{2\alpha}}),$$

and in particular $G(1.25) = 1.25$. Theorem 7.2 shows that $G(\alpha) \leq 1.25$. Also, $G(1) = G(2)$, and presumably, G is continuous.

Moreover, we conjecture that for every α there is a sequence of hard distributions which specify how many elements are at level $m - 1, m, \ldots$ (as a fraction of n), and how many are "small". This conjecture reduces the problem of computing G to an optimization problem which we do not know how to solve, even numerically.

Open Question 8. *Is there an explicit optimal set of questions of size $1.25^{n+o(n)}$?*

Notes Theorem 7.2 shows that for every n there exists an optimal set of questions (one matching $\mathrm{Opt}(\mu)$ for every distribution μ) of size $1.25^{n+o(n)}$. However, the construction is probabilistic.

Theorem 7.5 gives an explicit set of questions of size $O(\sqrt{2}^n)$ which allows the efficient construction of optimal decision trees. This explicit set of questions is a hitting set not only for all dyadic sets (defined in Section 7.1), but even for all maximal antichains.

It would be very interesting to find an explicit optimal set of questions of size $1.25^{n+o(n)}$, or even of any size $(\sqrt{2}-\epsilon)^n$. It would be even better if one can efficiently construct optimal decision trees using this set of questions.

The proof of Theorem 7.2 shows that it suffices to construct a hitting set for combinatorial cubes of the form

$$\prod_{i=1}^{\gamma} \binom{D_i}{\lceil |D_i|/2 \rceil},$$

where $\gamma \leq \log n + 1$, the sets $D_1, \ldots, D_\gamma \subseteq X_n$ are disjoint (but don't necessarily partition X_n), and $\binom{D}{c}$ consists of all subsets of D of size c.

Open Question 9. *Can Huffman's algorithm achieve the bound $1.25^{n+o(n)}$ for dyadic distributions?*

Proof. Huffman's algorithm is *non-deterministic*, in the sense that at any given step there might be more than one possible move. This is because at each step we merge two elements of minimum probability, and there might be many elements having the minimum probability.

Gallager [Gal78] showed that each Huffman tree satisfies the *sibling property*: the nodes in the tree can be arranged in non-decreasing order of probability (the probability of an internal node being the sum of the probabilities of all leaves in its subtree) such that two adjacent nodes are siblings. Conversely, any such tree can be produced by Huffman's algorithm.

It is easy to see that even considering this non-determinism, Huffman's algorithm potentially uses $2^{n-o(n)}$ questions; just pick a generic distribution with a balanced first question, and consider all of its permutations. However, it could be the case that if we only consider dyadic distributions, then we can make intelligent non-deterministic choices that restrict the number of questions needed to implement the resulting decision tree. □

Open Question 10. *How many questions are needed if the support has size $m \ll n$?*

Notes Some of our results are sensitive to the size m of the support. For example, Algorithm A_t of Section 5.1 can be implemented in time $O(m \log m)$ rather than just $O(n \log n)$.

How large should a set of questions be if we only require it to be optimal for distributions with bounded support, as a function of both the domain size n and the support size m?

10.3 Questions on $u^H(n,r)$ and $u^{\mathrm{Opt}}(n,r)$

Here is a summary of our results on $u^H(n,r)$ and $u^{\mathrm{Opt}}(n,r)$ (for $r > 0$):

- Distributions almost concentrated on a single element show that $u^H(n,1) \geq n$.
- Theorem 5.1 shows that $u^H(n,1) \leq 2n - 3$.
- Theorem 6.1 states that for every $r \geq 1$ and $n \in \mathbb{N}$,

$$\frac{1}{e}\lfloor r \rfloor n^{1/\lfloor r \rfloor} \leq u^H(n,r) \leq 2\lfloor r \rfloor n^{1/\lfloor r \rfloor}.$$

- Theorem 8.1 states that for all $r \in (0,1)$ and $n > 1/r$:

$$\frac{1}{n}(r \cdot n)^{\frac{1}{4r}} \leq u^{\mathrm{Opt}}(n,r) \leq n^2(3r \cdot n)^{\frac{16}{r}}.$$

- Theorem 8.3 states that for every $r \geq 1$ and $n \in \mathbb{N}$,

$$\frac{1}{e}\lfloor r+1 \rfloor n^{1/\lfloor r+1 \rfloor} \leq u^{\mathrm{Opt}}(n,r) \leq 2\lfloor r \rfloor n^{1/\lfloor r \rfloor}.$$

- Theorem 9.2 states that $u^{\mathrm{Opt}}(n,1) \leq n-1$.
- Theorem 9.3 states that $u^{\mathrm{Opt}}(n,1/2) \leq \binom{n+1}{2}$.

Open Question 11. *What are the exact asymptotics of $u^H(n,r)$?*

Notes Theorem 6.1 shows that for integer r,

$$\frac{1}{e}rn^{1/r} \leq u^H(n,r) \leq 2rn^{1/r}.$$

When $r=1$ we have the improved lower bound $u^H(n,1) \geq n$, showing that the constant $1/e$ can be improved in this case.

Does the following limit exist? What is its value?

$$L = \lim_{\text{integer } r \to \infty} \frac{u^H(n,r)}{rn^{1/r}}.$$

Open Question 12. *Does $u^H(n,r)$ depend only on $\lfloor r \rfloor$?*

Notes Our only general bound, Theorem 6.1, has this property.

Open Question 13. *What are the asymptotics of $u^{\mathrm{Opt}}(n,r)$?*

Notes We consider the cases $r \in (0,1)$ and $r \geq 1$ separately.

Small r. When $r \in (0,1)$, Theorem 8.1 shows that for $n > 1/r$,

$$(rn)^{1/4r-O(1)} \leq u^{\mathrm{Opt}}(n,r) \leq C_r(rn)^{16/r+O(1)},$$

where C_r depends only on r.

Does there exist a constant K such that for $r \in (0,1)$,

$$u^{\mathrm{Opt}}(n,r) \approx (rn)^{K/r},$$

the approximation possibly hiding factors of the form $C_r n^{O(1)}$?

Large r. When $r \geq 1$ is an integer, Theorem 8.3 shows that

$$\frac{1}{e}(r+1)n^{1/(r+1)} \leq u^{\mathrm{Opt}}(n,r) \leq 2rn^{1/r}.$$

What is the correct exponent of n? Is it $1/(r+1)$, $1/r$, or something in between? For non-integer r, does it depend only on $\lfloor r \rfloor$?

Open Question 14. *What are $u^{\mathrm{Opt}}(n,1)$ and $u^{\mathrm{Opt}}(n,1/2)$?*

Notes The Gilbert–Moore algorithm shows that $u^{\mathrm{Opt}}(n,1) \leq n-1$, using $\mathcal{Q}_{\prec}$ as the set of questions. Theorem 9.3 shows that $u^{\mathrm{Opt}}(n,1/2) \leq \binom{n+1}{2}$, using $\mathcal{Q}_{\square}$ as the set of questions.

Are these bounds optimal? If not, are there exponents α, β such that $u^{\mathrm{Opt}}(n,1) = \Theta(n^{\alpha})$ and $u^{\mathrm{Opt}}(n,1/2) = \Theta(n^{\beta})$?

10.4 Other questions

The following question is prompted by the results of Section 9 on distributions with high min-entropy:

Open Question 15. *What is the smallest set of questions satisfying* $r_0^H(\mathcal{Q}) = 1 - \log e + \log\log e \approx 0.086$*?*

Notes Gallager [Gal78] showed that if μ has maximal probability $\mu_{\max}$ then the redundancy of a Huffman code for μ is at most $\mu_{\max} + 1 - \log e + \log\log e$, and furthermore, there are distributions with arbitrarily small $\mu_{\max}$ which require redundancy $1 - \log e + \log\log e$. In other words, $r_0^H(2^X) = 1 - \log e + \log\log e$.

Comparison and equality queries match Huffman codes in terms of redundancy on unrestricted distributions. When the maximal probability is taken into account, this is no longer the case: Theorem 9.1 shows that the asymptotic redundancy, as the maximal probability tends to zero, is at least $3 - \log 3 - \log e + \log\log e \approx 0.5011$.

How many questions are needed to achieve the optimal asymptotic redundancy 0.086? How many are needed to get below 0.5?

The next question is prompted by Lemma 7.2.7:

Open Question 16. *What is the smallest hitting set for maximal antichains which are closed under complementation?*

Notes Section 7 shows that $u^{\mathrm{Opt}}(n,0)$ is the size of the smallest hitting set for dyadic sets (defined in Section 7.1). One of our main results there is a lower bound of roughly 1.25^n on the size of a hitting set for dyadic sets, which holds for infinitely many n.

Lemma 7.2.7 shows that every dyadic set is a maximal antichain which is closed under complementation. Hitting sets for maximal antichains have been considered by Lonc and Rival [LR87], who called them *fibres*. They conjectured that the smallest hitting set has size $O(2^{n/2})$, but the best lower bound is only $\Omega(2^{n/3})$, due to Łuczak [Łu98, DS01]; Łuczak improved on Duffus, Sands and Winkler [DSW90], who gave a lower bound of $\Omega(1.25^n)$ using the techniques of Section 7.

It is natural to ask what is the size of a hitting set for all maximal antichains closed under complementation. Is there a hitting set of size $(2-\epsilon)^{n/2}$? Can we prove a lower bound of $(1.25+\epsilon)^n$?

Maximal antichains which are closed under complementation are closely related to maximal qualitatively independent families of sets. A family $\mathcal{F} \subseteq 2^{X_n}$ is *qualitively independent* if for every two sets $A, B \in \mathcal{F}$, all of $A \cap B, \overline{A} \cap B, A \cap \overline{B}, \overline{A} \cap \overline{B}$ are non-empty. It is not hard to check that if $\mathcal{F}$ is a maximal qualitatively independent family then $\{A, \overline{A} : A \in \mathcal{F}\}$ is a maximal antichain which is closed under complementation. Conversely, given a maximal antichain $\mathcal{F}$ which is closed under complementation, if we take one set out of each pair $A, \overline{A}$ then we get a maximal qualitatively independent family.

As a consequence of the foregoing, if $\mathcal{Q}$ is a hitting set for maximal qualitatively independent families then $\mathcal{Q}$ is a hitting set for maximal antichains closed under complementation. Conversely, if $\mathcal{Q}$ is a hitting set for maximal antichains closed under complementation, then $\{A, \overline{A} : A \in \mathcal{Q}\}$

is a hitting set for maximal qualitatively independent families. Denoting the minimal size of a hitting set for all maximal antichains closed under complementation by N_1, and the minimal size of a hitting set for all qualitatively independent families by N_2, we conclude that $N_1 \leq N_2 \leq 2N_1$.

10.5 Suggestions for future research

Many variants of Huffman codes appear in the literature; see for example the survey by Abrahams [Abr97]. This prompts several venues for future exploration, only some of which we mention here.

Open Question 17. *Generalize the results in the paper to D-way questions.*

Notes What happens if we allow questions to have D answers rather than just two answers? This is a classical topic in information theory, and most results generalize to this case; it is even mentioned in Huffman's original paper.

The set of questions $\mathcal{Q}_{\prec}$ naturally generalize to this case: instead of comparing against a single element, partition X_n into D intervals; this includes $\mathcal{Q}_{=}$ as a special case. What redundancy can be achieved by this set of questions?

Open Question 18. *Generalize the results in the paper to the length-restricted case.*

Notes What happens if we demand that every element be found after at most B questions, for some bound B? We have already mentioned this case above, in relation to $u^H(n, 1)$, but it makes sense for all other questions studied in this paper as well.

Open Question 19. *Generalize the results in the paper to other cost functionals.*

Notes The quantity of study in this paper is the *average* number of questions per element. However, there is a lot of literature on other cost functions, see Baer [Bae07] for example; the length-restricted case also fits to this framework.

Open Question 20. *Generalize the results in the paper to the case of unequal costs.*

Notes Suppose that instead of measuring the number of *questions* we measure the total cost of *answers*, where a Yes answer has a different cost from a No answer; this is the case for Morse code, for example, in which the two symbols have different duration. This is known as Karp's problem [Kar61].

References

[ABCS92] Martin Anthony, Graham Brightwell, Dave A. Cohen, and John Shawe-Taylor. On exact specification by examples. In *Proceedings of the Fifth Annual ACM Conference on Computational Learning Theory (COLT 1992)*, pages 311–318, 1992.

[Abr97] Julia Abrahams. Code and parse trees for lossless source encoding. In *Compression and Complexity of Sequences*, pages 145–171, 1997.

[AC05] Nir Ailon and Bernard Chazelle. Lower bounds for linear degeneracy testing. *Journal of the ACM*, 52(2):151–171, 2005.

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

[AD91] Javad A. Aslam and Aditi Dhagat. Searching in the presence of linearly bounded errors. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing (STOC '91)*, pages 486–493, 1991.

[AH91] Ron Aharoni and Ron Holzman. Private communication, 1991. Oberwolfach.

[AH06] Martin Anthony and Peter L. Hammer. A boolean measure of similarity. *Discrete Applied Mathematics*, 154(16):2242–2246, 2006.

[AKKL02] Richard Anderson, Sampath Kannan, Howard Karloff, and Richard E. Ladner. Thresholds and optimal binary comparison search trees. *Journal of Algorithms*, 44:338–358, 2002.

[AM01] Micah Adler and Bruce M. Maggs. Protocols for asymmetric communication channels. *Journal of Computer and System Sciences*, 63(4):573–596, 2001.

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

[Bae07] Michael B. Baer. Twenty (or so) questions: D-ary length-bounded prefix coding. In *IEEE International Symposium on Information Theory (ISIT 2007)*, pages 896–900, 2007.

[BAFN99] Yosi Ben-Asher, Eitan Farchi, and Ilan Newman. Optimal search in trees. *SIAM Journal on Computing*, 28(6):2090–2102, 1999.

[BD09] Prosenjit Bose and Karim Douïeb. Efficient construction of near-optimal binary and multiway search trees. In *Algorithms and Data Structures (WADS 2009)*, pages 230–241, 2009.

[BO83] Michael Ben-Or. Lower bounds for algebraic computation trees. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 80–86, 1983.

[Bon72] John A. Bondy. Induced subsets. *Journal of Combinatorial Theory, Series B*, 12(2):201 – 202, 1972.

[Boy75] David W. Boyd. The asymptotic number of solutions of a diophantine equation from coding theory. *Journal of Combinatorial Theory, Series A*, 18:210–215, 1975.

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

[CDS93] C. J. Colbourn, J. H. Dinitz, and D. R. Stinson. Applications of combinatorial designs to communications, cryptography, and networking. In K. Walker, editor, *Surveys in Combinatorics, 1993*, volume 187 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1993.

[CGMY15] Marek Chrobak, Mordecai Golin, J. Ian Munro, and Neal E. Young. Optimal search trees with 2-way comparisons. In *Algorithms and Computation (ISAAC 2015)*, pages 71–82, 2015.

[CGT86] Renato M. Capocelli, Raffaele Giancarlo, and Indeer Jeet Taneja. Bounds on the redundancy of Huffman codes. *IEEE Transactions on Information Theory*, IT-32(6):854–857, 1986.

[CIO16] Jean Cardinal, John Iacono, and Aurélien Ooms. Solving k-SUM using few linear queries. In *24th Annual European Symposium on Algorithms (ESA 2016)*, pages 25:1–25:17. LIPIcs, 2016.

[CM11] Gérard Cohen and Sihem Mesnager. Generalized witness sets. In *Proceedings of the 2011 First International Conference on Data Compression, Communications and Processing (CCP'11)*, pages 255–256, 2011.

[Coh09] Gérard Cohen. Separation and witnesses. In *Conding and Cryptology*, volume 5557 of *LNCS*, pages 12–21. Springer, 2009.

[CRZ08] Gérard Cohen, Hugues Randriam, and Gilles Zémor. Witness sets. In *Coding Theory and Applications (ICMCTA 2008)*, volume 5228 of *LNCS*. Springer, 2008.

[CS92] Renato M. Capocelli and Alfredo De Santis. Variations on a theme by Gallager. In *Image and Text Compression*, volume 176 of *The Kluwer International Series in Engineering and Computer Science*, pages 181–213, 1992.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of information theory (2. ed.)*. Wiley, 2006.

[DGW92] Aditi Dhagat, Peter Gács, and Peter Winkler. On playing "twenty questions" with a liar. In *Proceedings of 3rd Symposium on Discrete Algorithms (SODA'92)*, pages 16–22, 1992.

[DH99] Ding-Zhu Du and Frank K. Hwang. *Combinatorial Group Testing and Its Applications*, volume 12 of *Series on Applied Mathematics*. World Scientific, 2nd edition, 1999.

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

[DPDS93] Roberto De Prisco and Alfredo De Santis. On binary search trees. *Information Processing Letters*, 45(5):249–253, 1993.

[DS01] Dwight Duffus and Bill Sands. Minimum sized fibers in distributive lattices. *Journal of the Australian Mathematical Society*, 70:337–350, 2001.

[DSW90] Dwight Duffus, Bill Sands, and Peter Winkler. Maximal chains and antichains in Boolean lattices. *SIAM Journal on Discrete Mathematics*, 3(2):197–205, 1990.

[DSZ10] Thorsten Doliwa, Hans Ulrich Simon, and Sandra Zilles. Recursive teaching dimension, learning complexity, and maximum classes. In *Proceedings of the 21st International Conference on Algorithmic Learning Theory (ALT 2010)*, pages 209–223, 2010.

[EK04] William Evans and David Kirkpatrick. Restructuring ordered binary trees. *Journal of Algorithms*, 50(2):168–193, 2004.

[Ell11] David Ellis. Irredundant families of subcubes. *Mathematical Proceedings of the Cambridge Philosophical Society*, 150(2):257–272, March 2011.

[Eri99] Jeff Erickson. Lower bounds for linear satisfiability problems. *Chicago Journal of Theoretical Computer Science*, 8, 1999.

[ES16] Ester Ezra and Micha Sharir. The decision tree complexity for k-SUM is at most nearly quadratic. Manuscript, 2016.

[Fal73] Newton Faller. An adaptive system for data compression. In *Record of the 7th Asilomar Conference on Circuits, Systems, and Computers*, pages 593–597, 1973.

[Fre76] Michael L. Fredman. How good is the information theory bound in sorting? *Theoretical Computer Science*, 1(4):355–361, 1976.

[Fre15] Ari Freund. Improved subquadratic 3SUM. *Algorithmica*, pages 1–19, 2015.

[Gal78] Robert G. Gallager. Variations on a theme by Huffman. *IEEE Transactions on Information Theory*, IT-24(6):668–674, 1978.

[Gar74] Michael R. Garey. Optimal binary search trees with restricted maximal depth. *SIAM Journal on Computing*, 3(2):101–110, 1974.

[GG74] Michael R. Garey and Ronald L. Graham. Performance bounds on the splitting algorithm for binary testing. *Acta Informatica*, 3:347–355, 1974.

[Gil71] Edgar N. Gilbert. Codes based on inaccurate source probabilities. *IEEE Transactions on Information Theory*, 17(3):304–314, 1971.

[GK95] Sally A. Goldman and Michael J. Kearns. On the complexity of teaching. *Journal of Computer and System Sciences*, 50(1):20–31, 1995.

[GM59] E. N. Gilbert and E. F. Moore. Variable-length binary encodings. *Bell System Technical Journal*, 38:933–967, 1959.

[GP14] Allan Grønlund and Seth Pettie. Threesomes, degenerates, and love triangles. In *55th Annual Symposium on Foundations of Computer Science (FOCS'14)*, pages 621–630, 2014.

[GRVW95] Dennis Grinberg, Sivaramakrishnan Rajagopalan, Ramarathnam Venkatesan, and Vicor K. Wei. Splay trees for data compression. In *Proceedings of the sixth annual ACM–SIAM symposium on Discrete algorithms (SODA'95)*, pages 522–530, 1995.

[GW77] Adriano M. Garsia and Michelle L. Wachs. A new algorithm for minimum cost binary trees. *SIAM Journal on Computing*, 6(4):622–642, 1977.

[HHHW86] James H. Hester, Daniel S. Hirschberg, Shou-Hsuan Stephen Huang, and C. K. Wong. Faster construction of optimal binary split trees. *Journal of Algorithms*, 7(3):412–424, 1986.

[Hor77] Yasuichi Horibe. An improved bound for weight-balanced tree. *Information and Control*, 34(2):148–151, 1977.

[HPSS75] L. H. Harper, T. H. Payne, J. E. Savage, and E. Straus. Sorting X+Y. *Communications of the ACM*, 18(6):347–349, 1975.

[HR76] Laurent Hyafil and Ronald L. Rivest. Constructing optimal binary decision trees is NP-complete. *Information Processing Letters*, 5(1):15–17, 1976.

[HT71] T. C. Hu and Alan Curtiss Tucker. Optimal computer search trees and variable length alphabetic codes. *Journal of Applied Mathematics*, 21:514–532, 1971.

[HT72] T. C. Hu and K. C. Tan. Path length of binary search trees. *SIAM Journal on Applied Mathematics*, 22(2):225–234, 1972.

[Huf52] David A. Huffman. A method for the construction of minimum-redundancy codes. In *Proceedings of the I.R.E.*, pages 1098–1103, 1952.

[HW84a] Shou-Hsuan Stephen Huang and C. K. Wong. Generalized binary split trees. *Acta Informatica*, 21(1):113–123, 1984.

[HW84b] Shou-Hsuan Stephen Huang and C. K. Wong. Optimal binary split trees. *Journal of Algorithms*, 5(1):69–79, 1984.

[Joh80] Ottar Johnsen. On the redundancy of binary Huffman codes. *IEEE Transactions on Information Theory*, IT-26(2):220–222, 1980.

[Juk01] Stasys Jukna. *Extremal Combinatorics — With Applications in Computer Science*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2001.

[Kar61] Richard M. Karp. Minimum-redundancy coding for the discrete noiseless channel. *I.R.E. Transactions on Information Theory*, pages 27–38, 1961.

[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.

[KK95] Jeff Kahn and Jeong Han Kim. Entropy and sorting. *Journal of Computer and System Sciences*, 51(3):390–399, 1995.

[KLRS96] Eyal Kushilevitz, Nati Linial, Yuri Rabinovitch, and Michael Saks. Witness sets for families of binary vectors. *J. Combin. Theory (A)*, 73:376–380, 1996.

[Knu71] Donald E. Knuth. Optimum binary search trees. *Acta Informatica*, 1(1):14–25, 1971.

[Knu85] Donald E. Knuth. Dynamic Huffman coding. *Journal of Algorithms*, 6:163–180, 1985.

[KPB99] S. Rao Kosaraju, Teresa M. Przytycka, and Ryan Borgstrom. On an optimal split tree problem. In Frank Dehne, Jörg-Rüdiger Sack, Arvind Gupta, and Roberto Tamassia, editors, *Algorithms and Data Structures: 6th International Workshop, WADS'99 Vancouver, Canada, August 11–14, 1999 Proceedings*, pages 157–168, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[KS81] Daniel J. Kleitman and Michael E. Saks. Set orderings requiring costliest alphabetic binary trees. *SIAM Journal on Algebraic Discrete Mathematics*, 2(2):142–146, 1981.

[KS84] Jeff Kahn and Michael Saks. Balancing poset extensions. *Order*, 1(2):113–126, 1984.

[Kuh99] Christian Kuhlmann. On teaching and learning intersection-closed concept classes. In *Proceedings of the 4th European Conference on Computational Learning Theory (EuroCOLT '99)*, pages 168–182, 1999.

[KW16] Daniel Krenn and Stephan Wagner. Compositions into powers of b: asymptotic enumeration and parameters. *Algorithmica*, 75(4):606–631, August 2016.

[Lam92] Jean-Luc Lambert. Sorting the sums $(x_i + y_j)$ in $O(n^2)$ comparisons. *Theoretical Computer Science*, 103(1):137–141, 1992.

[Lar87] Lawrence L. Larmore. Height-restricted optimal binary trees. *SIAM Journal on Computing*, 16:1115–1123, 1987.

[LR87] Zbigniew Lonc and Ivan Rival. Chains, antichains, and fibres. *Journal of Combinatorial Theory, Series A*, 44:207–228, 1987.

[LS85a] Nati Linial and Michael Saks. Every poset has a central element. *Journal of Combinatorial Theory*, 40:195–210, 1985.

[LS85b] Nati Linial and Michael Saks. Searching order structures. *Journal of Algorithms*, 6:86–103, 1985.

[Łu98] Tomasz Łuczak. Private communication to Dwight Duffus and Bill Sands, 1998.

[LY01] T. W. Lam and F. L. Yue. Optimal edge ranking of trees in linear time. *Algorithmica*, 30(1):12–33, 2001.

[MA87] Bruce L. Montgomery and Julia Abrahams. On the redundancy of optimal binary prefix-condition codes for finite and infinite sources. *IEEE Transactions on Information Theory*, IT-33(1):156–160, 1987.

[MadH84] Friedhelm Meyer auf der Heide. A polynomial linear search algorithm for the n-dimensional knapsack problem. *Journal of the ACM*, 31:668–676, 1984.

[Man92] Dietrich Manstetten. Tight bounds on the redundancy of Huffman codes. *IEEE Transactions on Information Theory*, IT-38(1):144–151, 1992.

[Mei93] S. Meiser. Point location in arrangements of hyperplanes. *Information and Computation*, 106(2):286–303, 1993.

[Mes92] Roy Meshulam. On families of faces in discrete cubes. *Graphs and Combinatorics*, 8:287–289, 1992.

[MM11] Nikolaos Makriyannis and Bertrand Meyer. Some constructions of maximal witness codes. In *IEEE International Symposium on Information Theory (ISIT 2011)*, pages 2105–2109, 2011.

[MOW08] Shay Mozes, Krzysztof Onak, and Oren Weimann. Finding an optimal tree searching strategy in linear time. In *Proceedings of 19th Symposium on Discrete Algorithms (SODA'08)*, pages 1096–1105, 2008.

[MPK06] Soheil Mohajer, Payam Pakzad, and Ali Kakhbod. Tight bounds on the redundancy of Huffman codes. In *Information Theory Workshop (ITW '06)*, pages 131–135, 2006.

[MY16] Shay Moran and Amir Yehudayoff. A note on average-case sorting. *Order*, 33(1):23–28, 2016.

[Nag97] S. V. Nagaraj. Optimal binary search trees. *Theoretical Computer Science*, 188(1–2):1–44, 1997.

[Nak91] Narao Nakatsu. Bounds on the redundancy of binary alphabetical codes. *IEEE Transactions on Information Theory*, IT-37(4):1225–1229, 1991.

[OP06] Krzysztof Onak and Paweł Parys. Generalization of binary search: Searching in trees and forest-like partial orders. In *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006), 21-24 October 2006, Berkeley, California, USA, Proceedings*, pages 379–388, 2006.

[Per84] Yehoshua Perl. Optimum split trees. *Journal of Algorithms*, 5(3):367–374, 1984.

[Qui86] J. Ross Quinlan. Induction of decision trees. *Machine Learning*, 1:81–106, 1986.

[Ris73] Jorma Rissanen. Bounds for weight balanced trees. *IBM Journal of Research and Development*, 17:101–105, 1973.

[RMK+80] Ronald L. Rivest, Albert R. Meyer, Daniel J. Kleitman, Karl Winklmann, and Joel Spencer. Coping with errors in binary search procedures. *Journal of Computer and System Sciences*, 20:396–404, 1980.

[Sch98] Baruch Schieber. Computing a minimum weight k-link path in graphs with the concave Monge property. *Journal of Algorithms*, 29:204–222, 1998.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[She78] B. A. Sheil. Median split trees: a fast lookup technique for frequently occuring keys. *Communications of the ACM*, 21(11):947–958, 1978.

[She92] Dafna Sheinwald. On binary alphabetical codes. In *Data Compression Conference (DCC'92)*, pages 112–121, 1992.

[SM91] Ayumi Shinohara and Satoru Miyano. Teachability in computational learning. *New Generation Computing*, 8(4):337–347, 1991.

[Smi47] Cedric A. B. Smith. The counterfeit coin problem. *The Mathematical Gazette*, 31(293):31–39, 1947.

[Spu94a] David Spuler. Optimal search trees using two-way key comparisons. *Acta Informatica*, 31:729–740, 1994.

[Spu94b] David A. Spuler. *Optimal Binary Trees With Two-Way Key Comparisons*. PhD thesis, James Cook University, 1994.

[SSYZ14] Rahim Samei, Pavel Semukhin, Boting Yang, and Sandra Zilles. Algebraic methods proving Sauer's bound for teaching complexity. *Theoretical Computer Science*, 558:35–50, 2014.

[SW92] Joel Spencer and Peter Winkler. Three thresholds for a liar. *Combinatorics, Probability and Computing*, 1(1):81–93, 1992.

[Vit87] Jeffrey Scott Vitter. Design and analysis of dynamic Huffman codes. *Journal of the ACM*, 34(4):825–845, 1987.

[vL87] Jan van Leeuwen. On the construction of Huffman trees. In *Third International Colloquium on Automata, Languages and Programming (ICALP '87)*, pages 382–410, 1987.

[WAF01] John Watkinson, Micah Adler, and Faith E. Fich. New protocols for asymmetric communication channels. In *8th International Colloquium on Structural Information and Communication Complexity (SIROCCO)*, pages 337–350, 2001.

[WG72] W. A. Walker and C. C. Gottlieb. *A top-down algorithm for constructing nearly optimal lexicographical trees*, pages 303–323. Academic Press, 1972.

[Yeu91] Raymond W. Yeung. Alphabetic codes revisited. *IEEE Transactions on Information Theory*, IT-37(3):564–572, 1991.

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

[ZLHZ11] Sandra Zilles, Steffen Lange, Robert Holte, and Martin Zinkevich. Models of cooperative teaching and learning. *Journal of Machine Learning Research*, 12:349–384, 2011.

A Correct version of *On binary search trees*

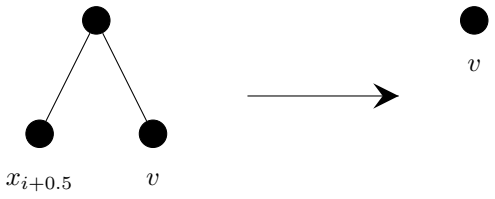
De Prisco and De Santis, in their paper *On binary search trees* [DPDS93], claim that $r^H(\mathcal{Q}_\prec, \pi) \leq 1 + p_{\max}$, where $p_{\max}$ is the maximum probability of an element in π. However, this is wrong even for the simple distribution $0, 1/3, 0, 1/3, 0, 1/3, 0$ (using the convention of Section 9.4 regarding zero probability elements), as a simple calculation reveals. Nevertheless, their ideas can be used to prove the following result:

Lemma A.1. *For any distribution π over X_n,*

$$r^H(\mathcal{Q}_\prec, \pi) < 1 - \frac{\pi_1 + \pi_n}{2} + \frac{1}{2}\sum_{i=1}^{n-1} |\pi_{i+1} - \pi_i|.$$

Proof. Let $Y = x_{0.5} \prec x_1 \prec x_{1.5} \prec x_2 \prec \cdots \prec x_{n-0.5} \prec x_n \prec x_{n+0.5}$, and extend π to a distribution σ by giving all new elements zero probability. The Gilbert–Moore algorithm [GM59] (described in Section 9.1) produces a decision tree using $\mathcal{Q}_\prec$ whose cost is less than $H(\sigma) + 2 = H(\pi) + 2$.

The decision tree contains $n + 1$ redundant leaves, corresponding to the newly added elements. We get rid of them one by one:



Getting rid of $x_{i+0.5}$ in this way bumps up at least one of x_i, x_{i+1} by one level; when $i = 0$ or $i = n$, only one of these options is available. In total, we bump up leaves whose total probability

is at least

$$\pi_1+\pi_n+\sum_{i=1}^{n-1}\min(\pi_i,\pi_{i+1})=\pi_1+\pi_n+\sum_{i=1}^{n-1}\frac{\pi_i+\pi_{i+1}-|\pi_i-\pi_{i+1}|}{2}=1+\frac{\pi_1+\pi_n}{2}-\frac{1}{2}\sum_{i=1}^{n-1}|\pi_i-\pi_{i+1}|.$$

The cost of the pruned tree is thus as stated. Replacing each question $\prec x_{i+0.5}$ by the equivalent question $\prec x_{i+1}$, we get a legal decision tree for the original distribution π using $\mathcal{Q}_{\prec}$. □