Tight Bounds on the Redundancy of Huffman Codes

Soheil Mohajer, Payam Pakzad, and Ali Kakhbod

Abstract—In this paper, we study the redundancy of Huffman codes. In particular, we consider sources for which the probability of one of the source symbols is known. We prove a conjecture of Ye and Yeung regarding the upper bound on the redundancy of such Huffman codes, which yields in a tight upper bound. We also derive a tight lower bound for the redundancy under the same assumption. We further apply the method introduced in this paper to other related problems. It is shown that several other previously known bounds with different constraints follow immediately from our results.

Index Terms—Huffman Code, redundancy, tight bounds.

I. INTRODUCTION

C onsider a discrete memoryless source \( S \) with finite alphabet \( S = \{s_1, s_2, \ldots, s_N\} \) of size \( N \), and the multiset\(^1\) of probabilities \( P = \{u_1, u_2, \ldots, u_N\} \), where \( u_i = \Pr(S = s_i) \). A variable-length \( D \)-ary lossless source code for the source \( S \) is defined by a one-to-one encoding function

\[
f_C : S \rightarrow \{0, 1, \ldots, D - 1\}^*\]

where \( A^* = \bigcup_{n \in \mathbb{N}} A^n \). Moreover, a code is called prefix-free if there is no valid codeword in the code that is a prefix of any other valid codeword. The length of the codeword assigned to the symbol \( s_i \) (with relative frequency \( u_i \)) by the code \( C \) is denoted by \( l_C(u_i) \). Therefore, the average codeword length of a code \( C \) is defined as

\[
L(C) := \sum_{i=1}^{N} u_i l_C(u_i).
\]

A basic goal in compression is to design codes with minimum average length. It is known that the average length of a prefix-free code cannot be less than the source entropy regardless of how efficient the code is, where the entropy of the source (in base \( D \)) is defined as

\[
\mathcal{H}(S) := -\sum_{i=1}^{N} u_i \log_D(u_i).
\]

An important performance measure of a source code, called the redundancy of the code, is the difference of its average length and the entropy of the source, i.e.,

\[
\mathcal{R}(C) := L(C) - \mathcal{H}(S).
\]

It is well known that the Huffman encoding algorithm \([1]\) provides an optimal prefix-free code for a discrete memoryless source, in the sense that no other code for distribution \( P \) can have a smaller expected length than that of the Huffman code. A \( D \)-ary Huffman code is usually represented using a \( D \)-ary tree \( T \), whose leaves correspond to the source symbols; the \( D \) edges emanating from each intermediate node of \( T \) are labeled with one of the \( D \) letters of the alphabet, and the codeword corresponding to a symbol is the string of labels on the path from the root to the corresponding leaf. Huffman’s algorithm is a recursive bottom-up construction of \( T \), where at each step, the \( D \) existing nodes with the smallest probabilities are merged\(^2\) into a new node, and henceforth represented by an intermediate node in the tree. Throughout this paper, unless \( D \) is explicitly specified, we talk about the binary Huffman codes (\( D = 2 \)).

We slightly modify the notation, and write the entropy, average length, and redundancy of a Huffman code in terms of its tree, \( \mathcal{H}(T) \), \( L(T) \), and \( \mathcal{R}(T) \), respectively. It is clear that the redundancy is always nonnegative, and easy to show that the redundancy of a Huffman code never exceeds 1 \([1]\). These bounds on \( \mathcal{R}(T) \) can be improved if partial knowledge about the source distribution is available. Gallager \([2]\), Johnsen \([3]\), Capocelli and Santis \([4]\), \([5]\), Manstetten \([6]\) and Capocelli et al. \([7]\) improved the upper bound on the redundancy (of binary Huffman codes) when \( p_1 := \max_i u_i \), the probability of the most likely source symbol is known. The problem of upper bounding the redundancy in terms of \( p_N := \min_i u_i \), the probability of the least likely source symbol, is addressed in \([4]\) and \([8]\). Capocelli et al. \([7]\) obtained upper bounds on \( \mathcal{R}(T) \) when both extreme probabilities \( p_1 \) and \( p_N \) are known. Furthermore, in \([8]\) and \([9]\), upper bound on the redundancy is derived as a function of probability of the two least likely source symbols \( p_{N-1} \) and \( p_N \).

Johnsen \([3]\) presented a tight lower bound on the redundancy of binary Huffman code in terms of \( p_1 \) when \( p_1 \geq 0.4 \). Subsequently, such lower bounds were generalized for all \( p_1 \) by Montgomery and Abrahams \([10]\). Later, Golić and Obradović

—

\(^1\)A multiset is a set that may contain repeated members, due to different source symbols with the same probabilities. We will define the notion of multiset and its properties in detail in Definition 1.

\(^2\)Before that, one has to add a number of dummy source symbols, all with probability zero, so that the number of source symbols \( N \) becomes of the form of \( k(D - 1) + 1 \), for some integer \( k \).
[11] extended Johnsen’s result to lower bound the redundancy of $D$-ary Huffman code in terms of the probability of the most likely symbol. The lower bound on $\mathcal{R}(T)$, when only $p_N$ is known, is considered in [4]. Furthermore, the problem of lower bounding $\mathcal{R}(T)$ for a binary code, when the two least likely probabilities $p_{N-1}$ and $p_N$ are known, is discussed in [4] and [9].

Ye and Yeung raised the problem of bounding the redundancy of Huffman code when the probability of one of the source symbols (regardless of its order) is known in [12], wherein they presented an upper bound on $\mathcal{R}(T)$. In this problem, the assumption is that we a priori know that the source contains a symbol with a given probability $p$, without knowing about its rank in the source distribution, as opposed to the case when the least or the most likely probability is given. A parametric upper bound for the redundancy is presented in [12], which is not tight in general. However, the authors conjectured another upper bound on $\mathcal{R}(T)$ in terms of the given probability $p$, which improves the other one.

In this work, we prove this conjecture with a simple approach and prove that this upper bound is tight. Moreover, we present a tight lower bound on $\mathcal{R}(T)$ for a source that contains a symbol with given probability $p$. We further characterize all possible sets of distribution which achieve this lower bound. We show that simple extensions of our results lead to the lower bound on the redundancy when either $p_1$ [10] or $p_N$ [4] are known. We also extend our proof to the $D$-ary Huffman codes and find the tight lower bound on $\mathcal{R}(T)$ when the probability of any symbol is known.

The rest of this paper is organized as follows. First, in Section II, we introduce the notation used in the paper and present a lemma which plays a key role in this study. Then, we state our main results in Section III. The proofs and discussions for the upper bound and lower bound are presented in Sections IV and V, respectively. The lower bound is extended to the $D$-ary Huffman codes in Section VI. Finally, we conclude the paper in Section VII.

II. NOTATIONS AND PRELIMINARIES

In this section, we present some definitions and review some known results that will be useful in the rest of this paper. We start with the definition of multiset [15].

**Definition 1:** Let $U$ be a universe set. A multiset over $U$ is defined as a pair $F = \langle U, f \rangle$, where the multiplicity function $f : U \rightarrow \mathbb{N} \cup \{0\}$ identifies the number of appearance of each element of the universe in the multiset.

Operations over sets can be generalized for multisets as follows.
1) Membership: An $x \in U$ is a member of $F$, if $f(x) > 0$.
2) Subset: A multiset $F = \langle U, f \rangle$ is a subset of $G = \langle U, g \rangle$, and denoted by $F \subseteq G$, if $f(x) < g(x)$ for any $x \in U$.
3) Union: The union of two multisets $F = \langle U, f \rangle$ and $G = \langle U, g \rangle$, denoted by $H = F \uplus G = \langle U, h \rangle$, is a multiset over $U$, with the multiplicity function $h(x) = f(x) + g(x)$.

4) Multiset removal: The removal of multiset $G = \langle U, g \rangle$ from $F = \langle U, f \rangle$, denoted $H = F \ominus G$, is the multiset $H = \langle U, h \rangle$, where
$$h(x) = \max\{f(x) - g(x), 0\}.$$  

In the rest of this study, whenever we talk about a probability distribution, it is referred to a multiset $P$ defined over the universe $U = \{0, 1\}$.

Consider a Huffman tree, with its end nodes (leaves) denoting the source symbols. In the following, we identify each node (including leaves and intermediate nodes) of the tree by its probability; this is defined as the probability of the corresponding symbol for the leaf nodes, and the sum of the probabilities of all the leaf nodes lying in the subtree under the node for the intermediate (nonleaf) nodes. In particular, the probability of the root is 1.

For each intermediate node $u$ in $T$, denote by $P_u \subseteq P$ the multiset of probabilities of the source symbols whose corresponding nodes lie under $u$. It is clear that $\sum_{p_i \in P_u} p_i = u$. Let $\Delta_u$ be the subtree of $T$ under $u$, and denote by $u^{-1} \ast \Delta_u$ its normalized version, where the probability of each node in $\Delta_u$ is scaled by a factor of $1/u$, so that the scaled leaf probabilities sum to one. Therefore, $u^{-1} \ast \Delta_u$ itself is a Huffman tree for a source with the probability distribution $u^{-1}P_u$.

Similarly, denote by $\Lambda_u$ the part of the Huffman tree above $u$ by collapsing the subtree $\Delta_u$ to a single node with probability $u$. It is easy to verify that $\Lambda_u$ is a valid Huffman tree for a source with probability distribution $P^\ast := (P \ominus P_u) \uplus \{u\}$. See Fig. 1 for a schematic diagram of the relationship between $\Delta_u$, $\Lambda_u$, and the original Huffman tree $T$.

The following lemma relates the redundancy of a Huffman tree to the redundancies of the subtrees $(u^{-1} \ast \Delta_u)$ and $\Lambda_u$.

**Lemma 1:** For any intermediate node $u$ in a Huffman tree $T$, we have
$$\mathcal{R}(T) = \mathcal{R}(\Lambda_u) + u \cdot \mathcal{R}(u^{-1} \ast \Delta_u).$$  

**Proof:** It is well known that the average length of any Huffman code equals the sum of the probabilities on the intermediate nodes (including the root) in the corresponding tree. Each intermediate node of $T$ is an intermediate node either in $\Lambda_u$ or in $(u^{-1} \ast \Delta_u)$, where the probabilities in the latter tree need to be scaled back by a factor of $u$. Note the node $u$ is not double counted in both trees, because it is a leaf in $\Lambda_u$, and so not counted in the first term. Therefore, we have
$$\mathcal{L}(T) = \mathcal{L}(\Lambda_u) + u \mathcal{L}(u^{-1} \ast \Delta_u).$$  

![Fig. 1. Decomposition of a Huffman tree with respect to the intermediate node $u$.](image-url)
On the other hand, we can rewrite the entropy of the original tree (source) in terms of the entropy of its associated subtrees by decomposing the leaf nodes of $T$ to those of $\Lambda_u$ and $(u^{-1} \cdot \Delta_u)$. We get

$$
\mathcal{H}(T) = - \sum_{p \in P} p \log p \\
= - \sum_{p \in \mathcal{P}_u} p \log p + \sum_{p \in \mathcal{P} \setminus \mathcal{P}_u} p \log p - u \log u + u \log u \\
= \sum_{p \in \mathcal{P}_u} p \log p + u \log u \\
- \sum_{p \in \mathcal{P}_u} p \log p - \sum_{p \in \mathcal{P}_u} p \log u \\
- \sum_{p \in \mathcal{P}_u} p \log p - u \sum_{p \in \mathcal{P}_u} q \log q \\
= \mathcal{H}(\Lambda_u) + u \mathcal{H}(u^{-1} \cdot \Delta_u) 
$$

where in (a) we used the fact that $\sum_{p \in P} p = u$. The desired result will be obtained immediately from (5) and (6).

III. MAIN RESULTS

In this section, we state the main results of this paper. The first theorem provides a tight upper bound on the redundancy of Huffman code for a source containing a symbol with a given probability $p$.

Theorem 1 (Tight Upper Bound on Huffman Redundancy): Consider the Huffman code for a source with finite alphabet, which includes a symbol with probability $p$, but is otherwise arbitrary. The redundancy of this code is upper bounded by

$$
R_{\text{max}}(p) := \begin{cases} 
2 - p - \mathcal{H}(p), & \text{if } 0.5 \leq p < 1 \\
1 + p - \mathcal{H}(p), & \text{if } 0 \leq p < 0.5 
\end{cases} 
$$

where $\mathcal{H}(p) := -p \log p - (1 - p) \log(1 - p)$ is the binary entropy function. Furthermore, this bound is tight, so there are sequences of source distributions whose Huffman redundancies converge to $R_{\text{max}}(p)$.

Our next theorem presents a lower bound for the redundancy of the Huffman code.

Theorem 2 (Tight Lower Bound on Huffman Redundancy): Consider the Huffman code for a source with finite alphabet, which includes a symbol with probability $p$, but is otherwise arbitrary. The redundancy of this code is lower bounded by

$$
R_{\text{min}}(p) := mp - \mathcal{H}(p) - (1 - p) \log(1 - 2^{-m}) 
$$

where $m > 0$ takes either of the values $|\log p|$ or $|\log p|$ which minimizes the expression. Furthermore, this bound is tight, i.e., there exist source distributions containing a symbol with probability $p$, whose Huffman redundancies equal $R_{\text{min}}(p)$.

We extend this result and introduce a lower bound for the redundancy of a $D$-ary Huffman code.

Theorem 3: The redundancy of a $D$-ary Huffman code containing a letter with probability $p$ is tightly lower bounded by

$$
R_{\text{min}}(p) = mp - \mathcal{H}(p) - \{1 - p\} \log(1 - D^{-m})
$$

where $m$ is either $\lfloor -\log_D p \rfloor$ or $\lceil -\log_D p \rceil$ which minimizes the aforementioned expression, and $\mathcal{H}(p) := \mathcal{H}(p)/\log(D)$ is the $D$-ary entropy function.

We prove the aforementioned theorems in the following sections. We also discuss derivation of some other known results using the techniques of our proofs.

IV. UPPER BOUND

In this section, we prove the upper bound introduced in Theorem 1, and then show that this bound is tight by providing sample probability distributions that can achieve this bound. Before proving this theorem, we shall review some known related results, which will be used in our proof.

Our result improves the following bound obtained in [12], and in fact proves a conjecture for the tightest upper bound given in the same paper.

Theorem 4 ([12, Th.1]): Let $p$ be the probability of any source symbol. Then, the redundancy of the corresponding Huffman code is upper bounded by

$$
R_{\text{ub}}(p) := \begin{cases} 
2 - p - \mathcal{H}(p), & \text{if } 0.5 \leq p < 1 \\
0.5, & \text{if } p \geq 0.5 \\
1 + p - \mathcal{H}(p), & \text{if } p \leq 0.5 
\end{cases} 
$$

where $\pi_0 := 0.18$ is the smallest root of equation $1 + p - \mathcal{H}(p) = 0.5$.

We will skip the proof of this theorem and refer the interested reader to the original paper [12]. This upper bound is tight when $p \geq 0.5$ or $p \leq \pi_0 \approx 0.18$, but as also suggested in [12], it is not tight for the central region $\pi_0 < p < 0.5$. Thus, we will only consider this central region in our proof for Theorem 1, and obtain a tight bound for the redundancy.

We will also use the following upper bound on the redundancy of a source whose most likely symbol probability is known.

Theorem 5 ([6, Table I]): Let $p_1$ be the probability of the most likely symbol of a source. Then, the Huffman redundancy of this source is upper bounded by the following function:

$$
f(p_1) = \begin{cases} 
2 - p_1 - \mathcal{H}(p_1), & \text{if } 0.5 \leq p_1 < 1 \\
3 - 5p_1 - \mathcal{H}(2p_1), & \text{if } p_1 \leq \pi_1 < 0.5 \\
\gamma, & \text{if } p_1 \leq \pi_1
\end{cases} 
$$

where $\gamma = R_{\text{max}}(\frac{1}{3}) = 1 + 1/3 - \mathcal{H}(1/3) \approx 0.415$, and $\pi_1 \approx 0.491$ is a root of $3 - 5\gamma - \mathcal{H}(2\gamma) = 0.5$.

All the three bounds introduced in Theorems 1, 4, and 5 are illustrated in Fig. 2.

Finally, we will need the following lemma from [3] in order to prove Theorem 1. The proof of this lemma is given in Appendix A for completeness.
Lemma 2 ([3, Th. 1]): Let $p_1$ be the probability of the most likely letter in a source. If $p_1 > 0.4$, then the length of the corresponding codeword in the Huffman code is one, i.e., $l(p_1) = 1$.

We are now ready to prove the upper bound.

Proof of Theorem 1: As stated earlier, when $p_1 > 0.4$, or $0.5 < p < 0.5$, our bound coincides with that of Theorem 4. It remains to show that for $\pi_0 < p < 0.5$, the redundancy of a Huffman code for a source which contains a symbol with probability $p$ does not exceed $R_{\text{max}}(p)$.

We prove this claim using an argument on $p_1$, the probability of the most likely symbol in $P$. First note that, if $p_1 = p$ is the most likely symbol, then from Theorem 5, we simply have $R(T) = f(p) \leq R_{\text{max}}(p)$.

On the other hand, if $p_1 < \pi_1$, then from Theorem 5, the Huffman redundancy of $P$ cannot exceed $\gamma - R_{\text{max}}(\frac{1}{2})$. Combining this with the fact that $R_{\text{max}}(\cdot)$ takes its minimum at $p = \frac{1}{2}$, we have $R(T) \leq f(p_1) = \gamma - R_{\text{max}}(\frac{1}{2}) \leq R_{\text{max}}(p)$.

So, we can focus our attention to the case where $\pi_0 < p_1 < p_1$. Note that for $p_1 > \pi_1 > 0.4$ from Lemma 2, we have $l(p_1) = 1$. Thus, $p$ should appear in the subtree under an intermediate node of probability $u := 1 - p_1$, i.e., $p \in P_u$, and hence $q = \frac{p}{1 - p_1}$. Using Lemma 1, we can expand the redundancy of the Huffman tree with respect to the intermediate node $u$ which results in

$$R(T) = R(\Lambda_u) + u \cdot R(u^{-1} \cdot \Delta_u)$$

where $1 - \mathcal{H}(p_1)$ is the redundancy of the Huffman tree $\Lambda_u$ which only contains two symbols of probabilities $\{p_1, 1 - p_1\}$. We then use Theorem 4 to upper bound the term $R(u^{-1} \cdot \Delta_u)$, which is the redundancy of the Huffman code corresponding to a source containing a symbol of probability $q = p/(1 - p_1)$. Note that $\pi_0 < q < 1$, since $p$ is assumed to be greater than $\pi_0$. We consider the following two cases for the possible values of $q = \frac{p}{1 - p_1}$.

Case I: $\pi_0 < q \leq 0.5$. From Theorem 4, we have $R(1 - p_1) \leq R_{\text{ub}}(q) \leq \frac{1}{2}$. Replacing this bound in (12), we get the bound

$$R(T) \leq 1 - \mathcal{H}(p_1) + \frac{1 - p_1}{2}$$

which can be further bounded by its maximum possible value for $p_1 \in (\pi_1, 1 - \pi_0)$: Note that the right hand side of the aforementioned inequality is a convex function of $p_1$ and it takes its maximum value at the boundary point $p_1 = 1 - \pi_0 \simeq 0.82$. Then, we have

$$R(T) \leq \max_{p_1 \in (\pi_1, 1 - \pi_0)} \left(1 - \mathcal{H}(p_1) + \frac{1 - p_1}{2}\right) \approx 0.410$$

Case II: $0.5 \leq q \leq 1$. Note that $u^{-1} \cdot \Delta_u$ is the Huffman tree of source containing a symbol of probability $q \geq 0.5$. Then, once again, we can upper bound its redundancy using Theorem 4 as

$$R(u^{-1} \cdot \Delta_u) \leq R_{\text{ub}}(q) = 2 - q - \mathcal{H}(q).$$

Replacing (15) in (12), we get

$$R(T) \leq 1 - \mathcal{H}(p_1) + (1 - p_1)(2 - q - \mathcal{H}(q))$$

$$\leq 1 - \mathcal{H}(p) + (1 - p_1)(2 - q - \mathcal{H}(q))$$

$$= 1 - \mathcal{H}(p) + p + (1 - p_1)(2(1 - q) - \mathcal{H}(1 - q))$$

$$\leq R_{\text{max}}(p)$$

where in (a) we used the fact $\mathcal{H}(p_1) \geq \mathcal{H}(p)$ which holds for $p \leq p_1 \leq 1 - p$, and the inequality in (b) follows from the fact that $\mathcal{H}(x) - 2x$ is a convex function of $x$.

Combining (14) and (15) gives us the desired inequality. It only remains to show the tightness of the bound. It is easy to check that the redundancy of a source with distribution $P(\epsilon) := \left((1 - \epsilon)(1 - p), p, 1(1 - p)\right)$ is

$$R(P(\epsilon)) = 1 - \epsilon - \mathcal{H}(p) - (1 - p)(\mathcal{H}(\epsilon) - \epsilon)$$

for $p \leq (1 - \epsilon)(1 - p)$, and

$$R(P(\epsilon)) = 2 - p - \mathcal{H}(p) - (1 - p)(\mathcal{H}(\epsilon) - \epsilon)$$

for $p \geq (1 - \epsilon)(1 - p)$, which tends to $R_{\text{max}}(p) = 1 + p - \mathcal{H}(p)$ as $\epsilon$ goes to zero. Note that the redundancy is a discontinuous function of the probability distribution at the boundary of this distribution space. More precisely, at the extreme case where $\epsilon = 0$, we have a source with only two symbols, for which the Huffman redundancy is $1 - \mathcal{H}(p)$. This completes the proof.

V. LOWER BOUND

In this section, we provide the proof of Theorem 2. We further show that the lower bound is tight, and we identify all distributions which achieve this redundancy.

Proof of Theorem 2: We first note that, for the purposes of minimizing the redundancy, it suffices to only consider a simple class of probability distributions for which the corresponding Huffman tree has a canonical structure, as depicted in Fig. 3. To see this, let $u$ be any intermediate node in a Huffman tree $T$, which does not contain $p$ in the subtree under it, i.e., $p \notin P_u$. Then, from Lemma 1

$$R(T) = R(\Lambda_u) + uR(u^{-1} \cdot \Delta_u) \geq R(\Lambda_u).$$

Therefore, the redundancy of $\Lambda_u$, the Huffman tree for the source with probability distribution $P_u$, which still contains a symbol of probability $p$, does not exceed that of $T$. A similar argument holds for any subtree which does not contain $p$ as a leaf. It is clear that this process converts $T$ into the canonical form of Fig. 3, in which each intermediate node has $p$ in its associated subtree, and the redundancy of the canonical form tree is at most the same as that of the original tree.

Suppose then, without loss of generality, that $T$ is a canonical form Huffman tree of depth $n_u$, which achieves the minimum re-
Fig. 2. Upper bounds of Theorems 1, 4, and 5, on the redundancy of a source containing a symbol with probability $p$.

Fig. 3. Canonical structure for minimum-redundancy Huffman trees that contain a symbol with probability $p$.

dundancy. Let $P = \{ x_1, x_2, \ldots, x_m, p \}$ be the corresponding probability distribution. Note that either $p$ or $x_m$ is the probability of the least likely symbol. Define $\alpha_i = x_i/(1-p)$, where $\sum_{i=1}^{m} \alpha_i = 1$. The expected length of this code can be written as

$$L(T) = \sum_{i=1}^{m} x_i \cdot i + p \cdot m$$

$$= 1 + (m-1)p + (1-p) \sum_{i=1}^{m} (i-1)\alpha_i$$

and the entropy of the source can be expressed in terms of $\alpha_i$'s as

$$H(T) = - \sum_{i=1}^{m} (1-p)\alpha_i \log[(1-p)\alpha_i] - p \log p$$

$$= \mathcal{R}(p) + (1-p)H(\alpha_1, \alpha_2, \ldots, \alpha_m)$$

where $H(\alpha_1, \alpha_2, \ldots, \alpha_m) = - \sum_{i=1}^{m} \alpha_i \log_2 \alpha_i$ is the entropy of the corresponding distribution. Thus

$$\mathcal{R}(T) = 1 + (m-1)p - \mathcal{H}(p)$$

$$+ (1-p) \left[ \sum_{i=1}^{m} (i-1)\alpha_i - H(\alpha_1, \alpha_2, \ldots, \alpha_m) \right]$$

$$= 1 + (m-1)p - \mathcal{H}(p) + (1-p)g(\alpha_1, \alpha_2, \ldots, \alpha_m)$$

(20)

where $g(\alpha_1, \alpha_2, \ldots, \alpha_m) := \sum_{i=1}^{m} (i-1)\alpha_i - H(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

The goal is to find the values of $\alpha_i$'s which minimize $g(\cdot)$ (and therefore $\mathcal{R}(T)$) for fixed value of $m$. Note first that the minimizing probability vector $(\alpha_1, \ldots, \alpha_m)$ must be an interior point in the probability simplex, since the redundancy function is discontinuous on the boundary of the simplex as mentioned earlier. More precisely, if $\alpha_m = 0$, one can remove $x_m = 0$ from the distribution,—replacing $m$ with $(m-1)$,—and reduce the redundancy. Next note that $g(\cdot)$ is a convex function. So, we can use the Karush–Kuhn–Tucker (KKT) theorem [13] to find its minimum, subject to the constraints $\sum_{i=1}^{m} \alpha_i = 1$ and $1 \geq \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_m \geq 0$. More precisely, we have to solve the following optimization problem:

$$\min_{(\alpha_1, \ldots, \alpha_m) \in [0,1]^m} \left\{ \sum_{i=1}^{m} \alpha_i (i-1 + \log \alpha_i) \right\}$$

subject to

$$\sum_{i=1}^{m} \alpha_i = 1$$

$$\sum_{i=1}^{m} \alpha_i - 1 = 0$$

$$\alpha_i - 1 \leq 0, \quad i = 0, \ldots, m$$

(21)
Fig. 4. Lower bound and upper bound on the redundancy of a source containing a symbol with probability $p$.

where we define $\alpha_0 := 1$ and $\alpha_{m+1} := 0$ for consistency. Finding the solution of this optimization problem is more involved and presented in Appendix B. Here, we just report the optimum solution which is

$$\alpha_i^* = \frac{2^{m-i}}{2^m-1}, \quad i = 1, \ldots, m.$$  \hfill (22)

Plugging the optimal values into (20) and after straightforward manipulations, we get

$$R(T) = mp - \mathcal{R}(p) - (1-p) \log \left(1 - 2^{-m}\right).$$

This is readily seen to be a convex function of $m$. To minimize, we differentiate with respect to $m$ and set the derivative equal to zero

$$\frac{\partial}{\partial m} R(T) = p - \frac{1-p}{2^m-1} = 0$$

yielding $m = -\log p$. Since $m$ needs to be an integer and by convexity, one of the two neighboring integers $\lfloor -\log p \rfloor$ or $\lceil -\log p \rceil$ will give the minimum. It remains to verify that the $\alpha_i$ values of (22) are consistent with a Huffman tree of the form in Fig. 3. A necessary and sufficient condition for this is that $p \leq x_{m-1} = (1-p)\alpha_{m-1}$. It is then easy to see that the chosen value of $m$ in $\lfloor -\log p \rfloor$, $\lceil -\log p \rceil$ which minimizes (8) results in an $\alpha_{m-1}$ coefficient which satisfies this condition.

Finally, note that in this proof, we have explicitly obtained probability distributions that achieve the minimum bound. This shows the tightness of the bound, and completes the proof. □

In the following, we point out a few remarks about Theorem 2.

Remark 1: The minimizing value of $m$ in Theorem 2 can be precisely expressed as follows. The optimal $m$ satisfies

$$\beta_m \leq p \leq \beta_{m-1}$$  \hfill (23)

where $\beta_0 := 1$ and $\beta_k$ is given by

$$\beta_k := 1 + 1/\log \left(1 + \frac{1}{2^{k+1} - 2}\right)^{-1}.$$ 

This equation is obtained by equating the values of $R(T)$ from (8) for two consecutive integers $\lfloor -\log p \rfloor$ and $\lceil -\log p \rceil$. It is easy to see that $\beta_k$ is a descending sequence, converging to 0 as $k$ tends to infinity, so that for any $p \in (0, 1)$ there exists a unique $m$ satisfying (23). The first few $\beta_k$’s are $\beta_1 = 0.369, \beta_2 = 0.182, \beta_3 = 0.091, \ldots$ and are displayed in Fig. 4.

Remark 2: From (8), the lower bound $R_{\text{min}}(p)$ can be zero if and only if $p = 2^{-m}$ is dyadic. In that case, from (22), $x_i = (1-p)\alpha_i = 2^{-i}$. Therefore, the entire distribution is dyadic.

Remark 3: The proof of Theorem 2 essentially describes all the source distributions that contain a symbol of probability $p$, and achieve the lower bound $R_{\text{min}}(p)$ on the redundancy. As argued previously, the Huffman trees for all such distributions have a “backbone” of canonical form shown in Fig. 3, with probabilities that are uniquely determined in the proof of the theorem. Any such tree which extends beyond this unique backbone must satisfy the inequality in (19) with equality, i.e., $R(x_i^{-1} \Delta_x)$ must be zero for all intermediate $x_i$’s. From the
aforementioned Remark 2, this can happen only if the corresponding distributions for the subtrees \( x_{i-1} \neq \Delta_x \) are dyadic. Thus, all the distributions containing a symbols of probability \( p \), which achieve the lower bound \( R_{\min}(p) \), can be obtained in the following way: start with the backbone distribution described in Theorem 2. At any time, choose a leaf node other than \( p \) and split its probability in half. It can be shown that each tree during this process is a valid Huffman tree with redundancy \( R_{\min}(p) \).

In the remainder of this section, we extend the results of Theorem 2 to the cases when the given probability \( p \) corresponds to the most, or the least likely symbol. This leads us to two known theorems lower bounding the redundancy for the corresponding cases.

A. Lower Bound When the Maximum Probability is Known

The following theorem extracted from [10] presents a tight lower bound on the redundancy of the Huffman code assigned to a source for which the probability of the most likely symbol is known. We will show in the proof of this theorem is a consequence of Theorem 2.

**Theorem 6:** ([10, Th. 2]) A tight lower bound for the Huffman redundancy of a source whose maximum symbol probability is \( p_1 \) is \( R_{\min}(p_1) \), as defined in Theorem 2.

**Proof:** It is clear from Theorem 2 that since the source contains a symbol with probability \( p_1 \), the redundancy of its Huffman code is lower bounded by \( R_{\min}(p_1) \). However, it is not clear whether this bound is achievable. In other words, we need to show that no other bound with larger values is a valid lower bound in general.

In the following, we argue that for any \( p_1 \in (0, 1) \), there exist sources whose most likely symbol has probability \( p_1 \), and its Huffman redundancy achieves \( R_{\min}(p_1) \). Let \( Q \) be a distribution containing \( p_1 \) (not necessarily as the maximum probability) which achieves the minimum redundancy \( R_{\min}(p_1) \). Then, by the argument of aforementioned Remark 3, each symbol probability of \( Q \) other than \( p_1 \) can be successively split into two halves, without changing the redundancy of the code. We can repeat this process until \( p_1 \) becomes the largest value in the distribution. Therefore, \( Q \) converts to a desired distribution which contains \( p_1 \) as the maximum probability, and its Huffman redundancy equals \( R_{\min}(p_1) \).

B. Lower Bound When the Minimum Probability is Known

Next suppose that \( p \leq 0.5 \) is constrained to be the probability of the least likely symbol of a source. The next theorem of Capocelli and Santis [4] characterizes the minimum achievable redundancy of the Huffman code in terms of the probability of the least likely symbol.

**Theorem 7:** ([4, Th. 2]) A tight lower bound for the Huffman redundancy of a source whose minimum symbol probability is \( p_N = p \) is given by

\[
\min \left\{ \frac{p}{p^*} \left( 1 - p \right) \ln \left( \frac{1 - 2^{-1} \left| \log \frac{p}{p} \right|}{p} \right), \right.
\]

\[
2p \left( 1 - 2^{-1} \left| \log \frac{p}{2p} \right| \right) \left( 1 - 2^{-1} \left| \log \frac{p}{2p} \right| \right) \right\},
\]

**(24)**

**Proof:** The argument used in the proof of Theorem 2 can be extended to this case. In fact, we have to solve a similar optimization problem, except an additional constraint \( x_m \geq p \).

Writing the KKT conditions [13], two cases may arise: (i) if the inequality \( x_m \geq p \) is strict, then the corresponding coefficient would be zero, and we have exactly the same solution as we had in Theorem 2. It is easy to see the optimal value for \( m \) for which satisfies \( x_m \geq p \) is \( m = \lfloor - \log p \rfloor + 2 \). If the constraint \( x_m \geq p \) becomes tight, then the optimal value for \( x_m \) is determined to be \( x_m = p \). In this case, the problem is equivalent to solving the optimization problem for \( (x_1, x_2, \ldots, x_{m-2}, 2p) \), where \( 2p = p + x_m \) is the intermediate note obtained by merging \( x_m \) and \( p \). For this problem, it turns out that the optimal value for \( m \) is \( m = \lfloor - \log 2p \rfloor \). The solution of the optimization problem in two cases gives us the bound claimed in the theorem.

The tightness of the bound can be shown by verifying that the two functions in the minimization expression are met by sources with probability distributions \( P_{\min}^{(1)} = \{2m-\lfloor (1-p)/2m - 1\} : m = \lfloor - \log p \rfloor, i = 1, 2, \ldots, m \} \cup \{p\} \) and \( P_{\min}^{(2)} = \{2m-\lfloor (1 - 2^i)/(2m - 1)\} : m = \lfloor - \log 2p \rfloor, i = 1, 2, \ldots, m \} \cup \{p\} \).

It is worth mentioning that the proof of Theorem 7 presented here is completely different and simpler than the proof given in the original paper [4]. The main simplification here is due to the restriction of the search space to the class of canonical Huffman trees, which is a consequence of Lemma 1.

**Remark 4:** As mentioned earlier, the bound in Theorem 7 coincides with \( R_{\min}(p) \) for some regimes of \( p \), where \( x_m \leq p \). The other function in the minimization expression (24) is precisely \( R_{\min}(2p) \), corresponding to the case in Theorem 2 when the optimal tree depth is \( m = \lfloor - \log 2p \rfloor \). This, of course, is not a coincidence, since one can easily verify that for a source whose two least probable symbols have probability \( p \), i.e., \( p_N = p_{N-1} = p \), merging the two corresponding leaves in the Huffman tree results in a tree with a single node of probability \( 2p \), and with the same redundancy as the original tree. This is because the subtree under the intermediate node \( 2p \) in the original tree has zero redundancy, since it represents a uniform distribution \( \{p, p\} \).

Fig. 5 plots the lower bounds in Theorems 2 and 7 as a function of the fixed probability \( p \).

VI. EXTENSION TO THE D-ARY HUFFMAN CODES

In this section, we present the proof of Theorem 3. Similar to the binary case, the basic idea in this proof is the restriction to (D-ary) canonical Huffman trees, and solving the optimization problem to find the optimal values for the symbol probabilities. We need the following lemma to simplify the proof. We refer to Appendix C for its proof.

**Lemma 3:** The minimum-redundancy D-ary Huffman tree for a source has a canonical structure as shown in Fig. 6. Moreover, all the leaves at the same depth (except possibly \( p \)) have the same probability, i.e., \( x_{i, j} = x_{i, j} \) for all \( i = 1, \ldots, m \) and \( j = 2, \ldots, D \), where \( x_{i, j} \) is the \( j \)th node in depth \( i \) of the tree.

**Proof of Theorem 3:** Using Lemma 3, it suffices to only consider Huffman trees of D-ary canonical form to find the min-
Fig. 5. Lower bounds for the Huffman redundancy of sources containing a symbol with probability $p$ with arbitrary rank, and least likely symbol with probability $p$.

Fig. 6. Canonical structure for minimum-redundancy $D$-ary Huffman trees that contain a symbol with probability $p$.

Fig. 7. Huffman tree with $l(p_1) = 2$.

VII. CONCLUSION

We introduced a lemma to expand the average length, entropy, and the redundancy of a Huffman tree with respect to any of its intermediate nodes. This method simplifies analyzing the redundancy behavior of the tree. In particular, we used this method to obtain tight upper and lower bounds for the Huffman tree associated to a source containing a symbol of probability $p$, without any further assumption on the rank of the symbol. The upper bound proves a conjecture of [12]. Our lower bound extends and completes several earlier partial results.

We have further discussed the explicit form of the distributions that achieve each of these bounds. Our arguments can be extended to the case of the $D$-ary Huffman codes, to obtain a lower bound for its redundancy in terms of any given source symbol probability.

APPENDIX A

PROOF OF LEMMA 2

We first note that as long as $p_1 > \frac{1}{2}$, the length $l(p_1)$ cannot be larger than 2; otherwise, there would be at least two independent intermediate nodes $x$ and $y$ on the Huffman tree (in the branch does not contain $p_1$) with lengths less than $l(p_1)$. Therefore, $x$ and $y$ both would have probabilities at least as large as $p_1$; but this is a contradiction since $p_1 + x + y \geq 3p_1$ cannot exceed 1.

Suppose next that $l(p_1) = 2$. Then, there can be no codeword of length 1 in the code, since $p_1$ is the largest probability. Therefore, the corresponding tree has a structure as in Fig. 7.

Replacing these values in the redundancy expression, we get

$$R_{\min, D} = mp - \mathcal{H}_D(p) - (1 - p) \log_D(1 - l^m)$$

which is minimized at $m^* = -\log_D p$. The convexity of the function with respect to $m$ implies that the optimal depth belongs to the set $\{-\log_D p, -\log_D p^2\}$. This completes the proof.
Next, note that \(v_1 + v_2 \geq p_1\) since \(l((v_1 + v_2)) = 1 < 2 = l(p_1)\). Moreover, \(u \geq \max(v_1, v_2) \geq \frac{1}{2}(u_1 + u_2)\) because it is merged after merging \(v_1\) and \(v_2\). This yields to

\[1 - p_1 + u + v_1 + v_2 \geq p_1 + \frac{1}{2}p_1 + p_1 - \frac{5}{2}p_1 > 1\]

which is a contradiction with \(p > 0.4\). \[\blacksquare\]

**APPENDIX B**

**OPTIMIZATION PROBLEM IN (21)**

We first define the Lagrangian

\[L(\varphi, \lambda, \mu) = g(\varphi) + \lambda \left( \sum_{i=1}^{m} \alpha_{k-1} + \sum_{j=0}^{m} \mu_j(\alpha_{j+1} - \alpha_j) \right)\]

in which \(\alpha = (\alpha_1, \ldots, \alpha_m)\). Moreover, \(\mu = (\mu_0, \ldots, \mu_m)\) and \(\lambda\) are the optimization parameters in the dual program. It is well known that for the optimal values \((\varphi^*, \lambda^*, \mu^*)\), we have

\[\frac{\partial}{\partial \varphi_k} L(\varphi, \lambda^*, \mu^*) \bigg|_{\varphi = \varphi^*} = (i - 1) + \log \alpha_i^* + \frac{1}{\ln 2} + \lambda^* + \mu_{i-1}^* - \mu_i^* = 0\]

for \(i = 1, 2, \ldots, m\). From the KKT conditions [13, Sec. 5.5.3], we have \(\mu_j^* \geq 0\) and \(\mu_j^*(\alpha_{j+1} - \alpha_j) = 0\). Let \(\mu_k^* = \max_j \mu_j^*\) be the maximum value among all optimization parameters. If \(\mu_k^* > 0\), from the KKT conditions, we get \(\alpha_k^* = \alpha_k^*\). Therefore, from (28), for \(i = k\) and \(i = k + 1\), we have

\[k - 1 + \log \alpha_k^* + \frac{1}{\ln 2} + \lambda^* + \mu_{k-1}^* - \mu_k^* = 2 + \log \alpha_k^* + \frac{1}{\ln 2} + \lambda^* + \mu_k^* - \mu_{k+1}^* = 0\]

which yields

\[\mu_k^* + \mu_{k+1}^* = 2\mu_k^* + 1\]

Therefore, we have either \(\mu_{k-1}^* > \mu_k^* \) or \(\mu_k^* > \mu_{k+1}^*\) which are both in contradiction with maximality of \(\mu_k^*\). This implies \(\mu_k^* = 0\) for \(i = 0, \ldots, m\). Hence

\[i - 1 + \log \alpha_i^* + \frac{1}{\ln 2} + \lambda^* = 0\]

which implies \(\alpha_i^* = K2^{-i}\) with \(K = 2^{1 - \frac{1}{\ln 2} - \lambda^*}\). Replacing this in \(\sum_{i=1}^{m} \alpha_i^* = 1\), we get

\[K \sum_{i=1}^{m} 2^{-i} = K \frac{2^m - 1}{2^m} = 1\]

which results in \(K = 2^m / (2^m - 1)\), and equivalently

\[\alpha_i^* = \frac{2^{m-i}}{2^m - 1}, \quad i = 1, \ldots, m\].

**REFERENCES**

[1] D. A. Huffman, “A method for the construction of minimum-redundancy codes,” Proc. IRE., vol. 40, no. 2, pp. 1098–1101, Sep. 1952.

[2] R. G. Gallager, “Variations on a theme by Huffman,” IEEE Trans. Inf. Theory, vol. 24, no. 6, pp. 668–674, Nov. 1978.

[3] O. Johnsen, “On the redundancy of binary Huffman codes,” IEEE Trans. Inf. Theory, vol. 26, no. 2, pp. 220–222, Mar. 1980.

[4] R. M. Capocelli and A. D. Santis, “New bounds on the redundancy of Huffman codes,” IEEE Trans. Inf. Theory, vol. 37, no. 4, pp. 1095–1104, Jul. 1991.

[5] R. M. Capocelli and A. D. Santis, “Tight upper bounds on the redundancy of Huffman codes,” IEEE Trans. Inf. Theory, vol. 33, no. 6, pp. 910–911, Nov. 1987.

[6] D. Manstetten, “Tight bounds on the redundancy of Huffman codes,” IEEE Trans. Inf. Theory, vol. 38, no. 1, pp. 144–151, Jan. 1992.

[7] R. M. Capocelli, R. Giancarlo, and I. J. Taneja, “Bounds on the redundancy of Huffman codes,” IEEE Trans. Inf. Theory, vol. 32, no. 6, pp. 854–857, Nov. 1986.

[8] R. D. Prisco and A. D. Santis, “On the redundancy achieved by Huffman codes,” Inf. Sci., vol. 88, pp. 131–148, Jan. 1996.

[9] R. W. Yeung, “Local redundancy and progressive bounds on the redundancy of a Huffman code,” IEEE Trans. Inf. Theory, vol. 37, no. 3, pp. 687–691, May 1991.

[10] B. Montgomery and J. Abrahams, “On the redundancy of optimal binary prefix-condition codes for finite and infinite sources,” IEEE Trans. Inf. Theory, vol. 33, no. 1, pp. 156–160, Jan. 1987.

[11] J. Golić and M. Obradović, “A lower bound on the redundancy of D-ary Huffman codes,” IEEE Trans. Inf. Theory, vol. 33, no. 6, pp. 910–911, Nov. 1987.
[12] C. Ye and R. W. Yeung, “A simple upper bound on the redundancy of Huffman codes,” *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 2132–2138, Jul. 2002.

[13] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[14] S. Mohajer, P. Pakzad, and A. Kakhbod, “Tight bounds on the redundancy of Huffman codes,” in *Proc. IEEE Inf. Theory Workshop*, Punta del Este, Uruguay, Mar. 2006, pp. 131–135.

[15] A. Syropoulos, “Mathematics of multisets,” in *Multiset Processing: Mathematical, Computer Science, and Molecular Computing Points of View*. New York: Springer-Verlag, 2001, pp. 347–358.

**Soheil Mohajer** received the B.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2004, and the M.Sc. and Ph.D. degrees in communication systems both from Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland, in 2005 and 2010, respectively. He was later a post-doctoral research associate in Princeton University.

Dr. Mohajer has been a post-doctoral researcher at the University of California at Berkeley, since October 2011. His research interests include multi-user information theory, statistical machine learning, and bioinformatics.

**Payam Pakzad** received the B.Sc. in Electrical Engineering and Applied Mathematics from Caltech, and M.Sc. and Ph.D. in the department of Electrical Engineering and Computer Science from UC Berkeley. He was later a post-doctoral researcher at EPFL.

Dr. Pakzad is currently a researcher with Qualcomm Research Lab in Silicon Valley. His research interests include coding theory, machine learning and statistical signal processing.

**Ali Kakhbod** received the B.Sc. degree in electrical engineering and the B.Sc. degree in mathematics from the Isfahan University Technology, Isfahan, Iran, in 2006 and 2007, respectively, and the M.Sc. degree in electrical engineering and the M.Sc. degree in mathematics from the University of Michigan, Ann Arbor, in 2009 and 2010, respectively, where he is currently pursuing the Ph.D. degree.

His research interests are in information economics, information theory, stochastic control, and decentralized systems.