

Received February 8, 2020, accepted May 2, 2020, date of publication May 14, 2020, date of current version May 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2994319

Network Traffic Compression With Side Information

AHMAD BEIRAMI¹ AND FARAMARZ FEKRI¹, (Fellow, IEEE)

Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA

Corresponding author: Ahmad Beirami (beirami@ece.gatech.edu)

ABSTRACT There is a high degree of correlation among packets traversing the Internet. As these packets are often routed through different paths, eliminating such correlation requires to process them individually. Traditional universal compression solutions would not perform well over a single short packet because of the insufficient data available for learning the unknown source parameters. In this paper, we define a notion of correlation between information sources and characterize the average redundancy in universal compression when side information from a correlated source is available. We show that the presence of side information provides at least 50% traffic reduction over traditional universal compression when applied to network packet data providing theoretical evidence for previous empirical studies.

INDEX TERMS Redundancy elimination, network compression, side information, correlated information sources.

I. INTRODUCTION

Several studies have confirmed the presence of considerable amount of correlation in network traffic data [1]–[5]. Specifically, we may broadly define two types of correlation in network traffic:

- 1) Temporal correlation within content from an information source being delivered to a client.
- 2) Spatial correlation across content from different information sources delivered to the same/different clients.

Network traffic abounds with the first dimension of temporal correlation, which is well understood. For example, if traffic contains mostly English text, there is significant correlation within the content. The existence of the second dimension of correlation is also confirmed in several real data experiments [1]–[5].

This has motivated the employment of correlation elimination techniques for network traffic data.¹ The present correlation elimination techniques are mostly based on content caching mechanisms used by solutions such as web-caching [6], CDNs [7], and P2P networks [8]. However, caching approaches that take place at the application layer, do not effectively leverage the spatial correlation, which

The associate editor coordinating the review of this manuscript and approving it for publication was Honglong Chen¹.

¹Within the networking community, these techniques are known as redundancy elimination (RE) but since redundancy has a specific meaning within the universal compression community, we chose to refer to these techniques as correlation elimination for the clarity of discussion.

exists mostly at the packet level [1]–[4]. To address these issues, a few studies have considered ad-hoc methods such as packet-level correlation elimination (deduplication) in which redundant transmissions of segments of a packet that are seen in previously sent packets are avoided [3], [4]. However, these techniques are limited in scope and can only eliminate exact duplicates from the segments of the packets leaving statistical correlations intact.

It is natural to consider universal compression algorithms for correlation elimination from network traffic data. While universal compression algorithms, e.g., the Lempel-Ziv algorithm [9], [10] and context tree weighting (CTW) [11], have been very successful in many domains, they do not perform very well on limited amount of data as learning the unknown source statistics incurs an inevitable redundancy (compression overhead). This redundancy depends on the richness of the class of the sources with respect to which the code is universal [12]–[16]. Further, traditional universal compression would only attempt to deal with temporal correlation from a stationary source and lacks the structure to leverage the spatial correlation dimension.

In this paper, as an abstraction of correlation elimination from network traffic, we study universal compression with side information from a correlated source. The organization of the paper and our contributions are summarized below.

- In Section II, we demonstrate that universal compression of finite-length sequences (up to hundreds of kilobytes) fundamentally suffers from a significant compression

overhead. This motivates using side information for removing this redundancy.

- In Section III, we present the formal problem setup. We define a notion of correlation between two parametric information sources, and study strictly lossless and almost lossless compression when side information from a correlated source is available to the encoder and/or the decoder.
- In Section IV, we establish several nice properties of correlated information sources. We show that the degree of correlation is tuned with a single hyperparameter, which results in independent information sources in one end and duplicate sources in the other end.
- In Section V, we characterize the average maximin redundancy with side information from a correlated source. We also show that if permissible error is sufficiently small the redundancy of almost lossless compression dominates the reduction in codeword length due to the permissible error.
- In Section VI, we define and characterize a notion of side information gain and establish a sufficient condition on the length of a side information string that would guarantee almost all of the benefits. We show that the side information gain can be considerable in many scenarios and derive a cutoff threshold on the size of memory needed to obtain all of the side information gain.
- In Section VII, we show that the side information gain is largely preserved even if the prefix constraint on the code is dropped.
- In Section VIII, we provide a case study that shows how these benefits would be extended in a network setting.
- Finally, the conclusions are summarized in Section IX.

II. MOTIVATION

We describe universal compression with side information from a correlated source in the most basic scenario. We use the notation $x^n = (x_1, \dots, x_n)$ to denote a string of length n on the finite alphabet \mathcal{X} . For example, for an 8-bit alphabet that has 256 characters, each x_i is a byte and x^n denotes a packet at the network layer. We assume that, as shown in Fig. 1, the network consists of content server nodes S_1 and S_2 , an intermediate memory-enabled (relay or router) node M , and client nodes C_1 and C_2 .

Let's assume that the content at S_1 is stationary and correlated with the content at S_2 . Assume that y^m has already

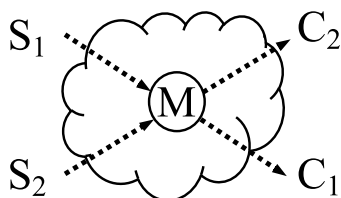


FIGURE 1. The basic abstraction of universal compression with side information.

been routed through $S_2 \rightarrow M \rightarrow C_2$ path. Also, assume that all nodes in the route, i.e., S_2 , M and C_2 , have memorized the content y^m . Now, assume that x^n is to be routed through $S_1 \rightarrow M \rightarrow C_1$ path. In this case, at the $S_1 \rightarrow M$ link the side information string is only available to the decoder, while at the $M \rightarrow C_1$ link, the side information is only available to the encoder. If x^n was to be routed through $S_1 \rightarrow M \rightarrow C_2$ path, in this case, the side information would be available to both the encoder and the decoder at $M \rightarrow C_2$ link. As such, we wish to study universal compression with side information that is available to the encoder and/or the decoder in this paper.

Given the side information gain, in [17], we analyzed the network-wide benefits of introducing memory-enabled nodes to the network and provided results on memory placement and routing for extending the gain to the entire network. However, [17] did not explain how to characterize the side information gain.

Let redundancy be the overhead in the number of bits used for describing a random string drawn from an unknown information source compared to the optimal codeword length given by the Shannon code. In the universal compression of a family of information sources that could be parametrized with d unknown parameters, Rissanen showed that the expected redundancy asymptotically scales as $\frac{d}{2} \log n + o(\log n)$ for almost all sources in the family [13].² Clarke and Barron [18] derived the asymptotic average minimax redundancy for memoryless sources to be $\frac{d}{2} \log n + O_n(1)$.³ This was later generalized by Atteson to Markov information sources [19]. The average minimax redundancy is concerned with the redundancy of the worst parameter vector for the best code, and hence, does not provide much information about the rest of the source parameter values. However, in light of Rissanen's result one would expect that asymptotically almost all information sources in the family behave similarly. The question remains as how these would behave in the finite-length regime.

In [16, Theorem 1], using a probabilistic treatment, we derived sharp lower bounds on the probability of the event that the redundancy in the compression of a random string of length n from a parametric source would be larger than a certain fraction of $\frac{d}{2} \log n$. [16, Theorem 1] provides, for any n , a lower bound on the probability measure of the information sources for which the average redundancy of the best universal compression scheme would be larger than $\frac{d}{2} \log n$. To demonstrate the implications of this result in the finite-length regime of interest in this paper, we consider an example using a first-order Markov information source with alphabet size $k = 256$. This information source is represented using $d = 256 \times 256 = 62580$ parameters. We further assume that the source entropy rate is 0.5 bit per byte ($H^n(\theta)/n = 0.5$). This assumption is inspired by experiments on real network data traffic in [17, Section IV.A]. It is implied by [16,

² $f(n) = o(g(n))$ if and only if $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$.

³ $f(n) = O(g(n))$ if and only if $\lim_{n \rightarrow \infty} \sup \frac{f(n)}{g(n)} < \infty$.

Theorem 1] that the compression overhead is more than 75% for strings of length 256kB. We conclude that redundancy is significant in the compression of finite-length low-entropy sequences, such as the Internet traffic packets that are much shorter than 256kB. It is this redundancy that we hope to suppress using side information from a correlated source. The compression overhead becomes negligible for very long sequences (e.g., it is less than 2% for strings of length 64MB and above), and hence, the side information gain vanishes as $O(\log n/n)$ when the sequence length grows large.

It is also worth noting the scope of benefits expected from universal compression of network traffic with side information is significant since file sharing and web data comprise more than 50% of network traffic [20] for which, the correlation levels may be as high as 90% [1]. Further, universal compression with side information is applicable to storage reduction in cloud and distributed storage systems, traffic reduction for Internet Service Providers, and power and bandwidth reduction in wireless communications networks (e.g., wireless sensors networks, cellular mobile networks, hot spots). See [17], [21] for a more thorough investigation of such applications and also for practical coding schemes for network packet compression.

III. PROBLEM SETUP

Let \mathcal{X} be a finite alphabet. We assume that the server S comprises of two parametric sources $\theta^{(1)}, \theta^{(2)} \in \Theta_d$, where $\theta^{(1)} := (\theta_1^{(1)}, \dots, \theta_d^{(1)})$ and $\theta^{(2)} = (\theta_1^{(2)}, \dots, \theta_d^{(2)})$, and where Θ_d is a d -dimensional compact set. Denote $\mu_{\theta^{(1)}}^n$ and $\mu_{\theta^{(2)}}^n$ as the probability measures defined by the parameter vector θ on strings of length n . If the information sources are memoryless, we let $\theta^{(1)}$ be the stochastic vector associated with the categorical distribution over source characters, and Θ_d would be the d -dimensional probability simplex. In the memoryless case, $\mu_{\theta^{(1)}}^n$ would be a product distribution.

In this paper, we consider a Bayesian setting where we assume that $\theta^{(1)}$ is a priori unknown but its prior is known. Unless otherwise stated, we use the notation $X^n \in \mathcal{X}^n$ and $Y^m \in \mathcal{X}^m$ to denote random string of length n and m drawn from $\mu_{\theta^{(1)}}^n$ and $\mu_{\theta^{(2)}}^m$, respectively. See Assumption 1 (appendix) for a set of regularity conditions that we assume on the parametric family.

We put forth a notion of correlation between the parameter vectors $\theta^{(1)}$ and $\theta^{(2)}$, which are jointly drawn. As we shall see, the degree of correlation could be tuned using a hyperparameter t . We assume that the unknown (and unobserved) parameter vector $\theta^{(1)}$ follows a prior distribution q supported on Θ_d . Let Z^t be a random string of length t that is drawn from $\mu_{\theta^{(1)}}^t$. We assume that given Z^t , the parameter vectors $\theta^{(1)}$ and $\theta^{(2)}$ are independent and identically distributed. This is shown in the Markov chain represented in Fig. 2. We will state several nice properties of this proposed model in Section IV.

Note that this framework is fundamentally different from Slepian-Wolf coding that also targets the spatial correlation

$$\theta^{(1)} \longrightarrow Z^t \longrightarrow \theta^{(2)}$$

FIGURE 2. The correlation model between the two information sources.

between distributed information sources [22]–[25]. In Slepian-Wolf coding, the sequences from the distributed sources are assumed to have character-by-character correlation, which is also different from our correlation model that is due to the parameter vectors being unknown in a universal compression setup.

Let $H^n(\theta)$ denote the Shannon entropy of the source given θ , i.e.,

$$\begin{aligned} H^n(\theta) &\triangleq E \left\{ \log \left(\frac{1}{\mu_\theta(X^n)} \right) \right\} \\ &= \sum_{x^n \in \mathcal{X}^n} \mu_\theta(x^n) \log \left(\frac{1}{\mu_\theta(x^n)} \right). \end{aligned} \quad (1)$$

Throughout this paper expectations are taken over functions of the random sequence X^n with respect to the (unknown) probability measure μ_θ , and $\log(\cdot)$ denotes the logarithm in base 2, unless otherwise stated. We further use the notation $H(\theta)$ to denote the entropy rate, defined as $H(\theta) \triangleq \lim_{n \rightarrow \infty} \frac{1}{n} H^n(\theta)$.

Let $\mathcal{I}(\theta)$ be the Fisher information matrix, where each element is given by

$$\mathcal{I}(\theta)_{ij} \triangleq \lim_{n \rightarrow \infty} \frac{1}{n \log e} E \left\{ \frac{\partial^2}{\partial \theta_i \partial \theta_j} \log \left(\frac{1}{\mu_\theta^n(X^n)} \right) \right\}. \quad (2)$$

Fisher information matrix quantifies the amount of information, on the average, that a random string X^n from the source conveys about the source parameters. Let Jeffreys' prior on Θ_d be defined as

$$w_J(\theta) \triangleq \frac{|\mathcal{I}(\theta)|^{\frac{1}{2}}}{\int_{\phi \in \Theta_d} |\mathcal{I}(\phi)|^{\frac{1}{2}} d\phi}. \quad (3)$$

Roughly speaking, Jeffreys' prior is optimal in the sense that the average minimax redundancy is asymptotically achieved when the parameter vector θ is assumed to follow Jeffreys' prior (see [18] for a formalized statement and proof). This prior distribution is particularly interesting because it corresponds to the worst-case compression performance for the best compression scheme.

We consider the family of block codes that map any n -string to a variable-length binary sequence, which also satisfy Kraft's inequality [26]. Let

$$\begin{aligned} \mathcal{C} &\triangleq \mathcal{X}^n \times \{\varepsilon\}^m, \\ \mathcal{C}^E &\triangleq \mathcal{X}^n \times \mathcal{X}^m, \\ \mathcal{D} &\triangleq \{0, 1\}^* \times \{\varepsilon\}^m, \\ \mathcal{D}^D &\triangleq \{0, 1\}^* \times \mathcal{X}^m, \end{aligned} \quad (4)$$

where ε denotes an erasure. We use $c : \mathcal{C} \rightarrow \{0, 1\}^*$ and $c^E : \mathcal{C}^E \rightarrow \{0, 1\}^*$ to denote the encoder without and with side information, respectively. Similarly, we also use $d : \mathcal{D} \rightarrow \mathcal{X}^n$

and $d^D : \mathcal{D}^D \rightarrow \mathcal{X}^n$ to denote the decoder without and with side information, respectively. We use notations

$$\begin{aligned}
 \mathcal{C} &\triangleq (\mathcal{X}^n, \varepsilon^m) \in \mathcal{C}, \\
 \mathcal{C}^E &\triangleq (\mathcal{X}^n, y^m) \in \mathcal{C}^E, \\
 \mathcal{D} &\triangleq (c(\mathcal{C}), \varepsilon^m) \in \mathcal{D}, \\
 \mathcal{D}^E &\triangleq (c^E(\mathcal{C}^E), \varepsilon^m) \in \mathcal{D}, \\
 \mathcal{D}^D &\triangleq (c(\mathcal{C}), y^m) \in \mathcal{D}^D, \\
 \mathcal{D}^{ED} &\triangleq (c^E(\mathcal{C}^E), y^m) \in \mathcal{D}^D.
 \end{aligned} \tag{5}$$

Next, we present the notions of strictly lossless and almost lossless source codes, which will be needed in the sequel. While the definitions are only given for the case with no side information at the encoder and the decoder, it is straightforward to extend them using the above definitions. Our main focus is on prefix free codes that ensure unique decodability of concatenated code blocks (see [27, Chapter 5.1]).

Definition 1: The code $c : \mathcal{C} \rightarrow \{0, 1\}^*$ is called strictly lossless (also called zero-error) if there exists a reverse mapping $d : \mathcal{D} \rightarrow \mathcal{X}^n$ such that

$$\forall C \in \mathcal{C} : d(D) = x^n.$$

Definition 2: Let $\mu^{n,m}$ denote a joint probability distribution on (x^n, y^m) . The code $c_\varepsilon : \mathcal{C} \rightarrow \{0, 1\}^*$ is called almost lossless with permissible error probability $\varepsilon(n)$, if there exists a reverse mapping $d_\varepsilon : \mathcal{D} \rightarrow \mathcal{X}^n$ such that

$$E\{\mathbf{1}_e(X^n, Y^m)\} \leq \varepsilon(n),$$

where $\mathbf{1}_e(x^n)$ denotes the error indicator function, i.e.,

$$\mathbf{1}_e(x^n, y^m) \triangleq \begin{cases} 1 & d_\varepsilon(D) \neq x^n, \\ 0 & \text{otherwise,} \end{cases}$$

where D and E are defined in (5).

Most of the practical data compression schemes are examples of strictly lossless codes, namely, the arithmetic code [28], Huffman code [29], Lempel-Ziv codes [9], [10], and CTW code [11]. In almost lossless source coding, which is a weaker notion of the lossless case, we allow a non-zero error probability $\varepsilon(n)$ for any finite n while if $\varepsilon(n) = o_n(1)$ the code is almost surely asymptotically error free. The proofs of Shannon [30] for the existence of entropy achieving source codes are based on almost lossless random codes. The proof of the Slepian-Wolf theorem [22] also uses almost lossless codes. Further, all of the practical implementations of SW source coding are based on almost lossless codes (see [24], [25]).

We consider four coding strategies according to the orientation of the switches s_e and s_d in Fig. 3 for the compression of x^n drawn from $\mu_{\theta^{(1)}}^n$ provided that the sequence y^m drawn from $\mu_{\theta^{(2)}}^m$ is available to the encoder/decoder or not.⁴

⁴In this paper, we assume that m and n are a priori known to both the encoder and the decoder.

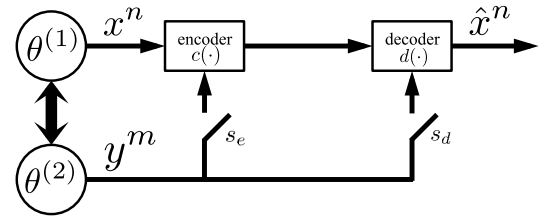


FIGURE 3. The compression model for universal source coding with two correlated parameter vectors.

- Ucomp (Universal compression without side information), where the switches s_e and s_d in Fig. 3 are both open. This corresponds to $C \in \mathcal{C}$ and $D \in \mathcal{D}$.
- UcompE (Universal compression with encoder side information), where the switch s_e in Fig. 3 is closed but the switch s_d is open. This corresponds to $C^E \in \mathcal{C}^E$ and $D^E \in \mathcal{D}$.
- UcompD (Universal compression with decoder side information), where the switch s_e in Fig. 3 is open but the switch s_d is closed. This corresponds to $C \in \mathcal{C}$ and $D^D \in \mathcal{D}^D$.
- UcompED (Universal compression with encoder-decoder side information), where the switches s_e and s_d in Fig. 3 are both closed. This corresponds to $C^E \in \mathcal{C}^E$ and $D^{ED} \in \mathcal{D}^D$.

IV. IMPLICATIONS OF THE CORRELATION MODEL

In this section, we study some implications of the proposed correlation model. This section may be skipped by the reader and only referred to when a particular lemma is needed in the subsequent proofs.

Lemma 1: The joint distribution of $(\theta^{(1)}, \theta^{(2)})$ for all $t \geq 0$ is given by

$$p^t(\theta^{(1)}, \theta^{(2)}) = w(\theta^{(1)})w(\theta^{(2)})f^t(\theta^{(1)}, \theta^{(2)}), \tag{6}$$

where $f^t(\theta^{(1)}, \theta^{(2)})$ is defined as

$$f^t(\theta^{(1)}, \theta^{(2)}) \triangleq \sum_{z^t \in \mathcal{X}^t} \left(\frac{\mu_{\theta^{(1)}}^t(z^t)\mu_{\theta^{(2)}}^t(z^t)}{\int_{\phi \in \Theta_d} \mu_{\phi}^t(z^t)w(\phi)d\phi} \right). \tag{7}$$

Proof: We have

$$p^t(\theta^{(2)}|\theta^{(1)}) = \sum_{z^t \in \mathcal{X}^t} p(\theta^{(2)}, z^t|\theta^{(1)}) \tag{8}$$

$$= \sum_{z^t \in \mathcal{X}^t} p(\theta^{(2)}|z^t)\mu_{\theta^{(1)}}^t(z^t) \tag{9}$$

$$= w(\theta^{(2)}) \sum_{z^t \in \mathcal{X}^t} \left(\frac{\mu_{\theta^{(1)}}^t(z^t)\mu_{\theta^{(2)}}^t(z^t)}{\int_{\phi \in \Theta_d} \mu_{\phi}^t(z^t)w(\phi)d\phi} \right), \tag{10}$$

where (9) follows from the fact that $\theta^{(2)}$ and $\theta^{(1)}$ are independent and identically distributed given Z^t , and (10) follows from the Bayes rule. Hence, the result follows. ■

Next, we find the marginal distribution of $\theta^{(2)}$, i.e., $p_{\theta^{(2)}}^t(\theta^{(2)})$.

Lemma 2: For all $t \geq 0$, we have

$$p^t(\theta^{(2)}) = w(\theta^{(2)}). \quad (11)$$

Proof: The proof follows from the following equations

$$\begin{aligned} p_{\theta^{(2)}}^t(\theta^{(2)}) &= \int_{\Theta_d} p_{\theta^{(2)}|\theta^{(1)}}^t(\theta^{(2)}|\theta^{(1)})w(\theta^{(1)})d\theta^{(1)} \\ &= w(\theta^{(2)}) \int_{\Theta_d} f^t(\theta^{(1)}, \theta^{(2)})w(\theta^{(1)})d\theta^{(1)} \quad (12) \\ &= w(\theta^{(2)}), \quad (13) \end{aligned}$$

where (12) follows from Lemma 8 (appendix). ■

Lemma 3: $\theta^{(2)}$ is independent of $\theta^{(1)}$ if and only if $t = 0$, i.e.,

$$p^0(\theta^{(1)}, \theta^{(2)}) = w(\theta^{(1)})w(\theta^{(2)}). \quad (14)$$

Proof: By definition of $f^t(\cdot, \cdot)$, and the fact that $\mu_{\theta^{(1)}}^0(z^0) = 1$, we have

$$f^0(\theta^{(1)}, \theta^{(2)}) = \left(\frac{1}{\int_{\phi \in \Theta_d} w(\phi)d\phi} \right) = 1. \quad (15)$$

Hence, the claim follows by invoking Lemma 1. ■

Lemma 4: $\theta^{(2)}$ converges in mean square to $\theta^{(1)}$ as $t \rightarrow \infty$, that is

$$\lim_{t \rightarrow \infty} E \left\{ \|\theta^{(2)} - \theta^{(1)}\|^2 \right\} = 0. \quad (16)$$

Proof: Let $\widehat{\theta}^{(1)}(Z^t)$ be the maximum likelihood estimator (MLE) of $\theta^{(1)}$ from the observation Z^t . By definition, $\widehat{\theta}^{(1)}(Z^t)$ also serves as the MLE for $\theta^{(2)}$. Then,

$$\begin{aligned} E\{\|\theta^{(2)} - \theta^{(1)}\|^2\} &\leq E\{\|\theta^{(2)} - \widehat{\theta}^{(1)}(Z^t)\|^2\} \\ &\quad + E\{\|\theta^{(1)} - \widehat{\theta}^{(1)}(Z^t)\|^2\} \quad (17) \\ &= 2E\{\|\theta^{(1)} - \widehat{\theta}^{(1)}(Z^t)\|^2\}, \quad (18) \end{aligned}$$

and the statement follows from the convergence of MLE in mean square for the parametric information source as assumed in the regularity conditions put forth in Assumption 1 (appendix). ■

Remark: The degree of correlation between the two parameter vectors $\theta^{(1)}$ and $\theta^{(2)}$ is determined by the hyperparameter t . This degree of correlation varies from independence of the two parameter vectors at $t = 0$ all the way to the vectors being equal (convergence in mean square) when $t \rightarrow \infty$. Further note that the covariance matrix of the parameter vectors $\theta^{(1)}$ and $\theta^{(2)}$ asymptotically as t grows large behaves like $\frac{2}{t}\mathcal{I}^{-1}(\theta^{(1)})$.

V. AVERAGE MAXIMIN REDUNDANCY

In this section, we investigate the average maximin redundancy in universal compression of correlated sources for different coding strategies put forth in Section III.

A. Ucomp CODING STRATEGY

Let $l^n : \mathcal{X}^n \rightarrow \mathbb{R}^+$ denote the universal (strictly lossless) length function for Ucomp.⁵ This is the length associated with a strictly lossless code. A necessary and sufficient condition for existence of a code that satisfies unique decodability is given by Kraft inequality:

$$\sum_{x^n \in \mathcal{X}^n} 2^{-l^n(x^n)} \leq 1. \quad (19)$$

Denote L^n as the set of all strictly lossless universal length functions that satisfy Kraft inequality. Denote $R^n(l^n, \theta)$ as the average redundancy of the code with length function $l^n(\cdot)$, defined as

$$R^n(l^n, \theta) \triangleq E_{X^n \sim \mu^n} \{l^n(X^n)\} - H^n(\theta). \quad (20)$$

Define \underline{R} as the minimax redundancy of Ucomp, i.e.,

$$\underline{R}^n = \max_{w \in \Omega_d} \min_{l^n \in L^n} \int_{\theta \in \Theta_d} R^n(l^n, \theta)w(\theta)d\theta. \quad (21)$$

It is well known that the maximum above is attained by Jeffreys' prior in the asymptotic limit as n grows large. Hence, in the rest of this paper we assume that $\theta^{(1)}, \theta^{(2)} \sim w_J$ follow Jeffreys' prior given in (3). On the other hand, the length function that achieves the inner minimization is simply the information random variable.

$$l^n(x^n) \triangleq -\log \left(\int_{\theta \in \Theta_d} \mu_{\theta}^n(x^n)w_J(\theta)d\theta \right). \quad (22)$$

Putting it all together, we have

$$\underline{R}^n = I(X^n; \theta), \quad (23)$$

where $I(\cdot; \cdot)$ denotes the mutual information. This is Gallager's redundancy-capacity theorem in [32].

Clarke and Barron [18] showed that the average maximin redundancy for strictly lossless Ucomp is

$$\underline{R}^n = \frac{d}{2} \log \left(\frac{n}{2\pi e} \right) + \log \int_{\phi \in \Theta_d} |\mathcal{I}(\phi)|^{\frac{1}{2}} d\phi + o_n(1).$$

This result states that the average maximin redundancy in Ucomp coding strategy is $O(\log n)$ and also is linearly proportional to the number of unknown source parameters, d .

It is straightforward to define $\underline{R}_{\epsilon}^n$ as the average redundancy when $\theta^{(1)}$ follows Jeffreys' prior when we are restricted to almost lossless codes with permissible error ϵ . Note that it is clear that $\underline{R}_{\epsilon}^n \leq \underline{R}^n$. A natural question that arises is how much reduction is achievable by allowing a permissible error probability in decoding. Our main result on Ucomp coding strategy with almost lossless codes is given in the following theorem.

Theorem 1: If $\epsilon(n) = O(\frac{1}{n})$, then

$$\underline{R}_{\epsilon}^n = \underline{R}^n - O_n(1). \quad (24)$$

⁵We ignore the integer constraint on the length functions in this paper, which will result in a negligible redundancy smaller than 1 bit and is exactly analyzed in [26], [31].

Proof: The proof is completed by invoking Lemma 12 in the appendix and noting that $\underline{R}^n = O(\log n)$. ■

The content of Theorem 1 is that if the permissible error, $\epsilon(n)$, in almost lossless compression vanishes fast enough as n grows, then asymptotically the maximin risk imposed by universality of compression dominates any savings obtained by allowing an $\epsilon(n)$ average error in decoding. Hence, in the rest of this paper we only focus on the family of strictly lossless codes.

B. UcompE CODING STRATEGY

Since the side information sequence y^m is not available to the decoder, then the minimum number of average bits required at the decoder to describe the random sequence X^n is indeed $H(X^n)$. On the other hand, it is straightforward to see that

$$H(X^n) = H^n(\theta^{(1)}) + I(X^n; \theta^{(1)}), \quad (25)$$

where $I(X^n; \theta^{(1)}) = \underline{R}^n$ by the redundancy-capacity theorem. Hence, in UcompE strategy, we establish that the side information provided by y^m only at the encoder does not provide any benefit on the strictly lossless universal compression of the sequence x^n .

C. UcompD CODING STRATEGY

Considering the UcompD strategy, by Assumption 1 (appendix), the two sources $\mu_{\theta^{(1)}}$ and $\mu_{\theta^{(2)}}$ are d -dimensional parametric ergodic sources. In other words, any pair $(x^n, y^m) \in \mathcal{X}^n \times \mathcal{Y}^m$ occurs with non-zero probability and the support set of (x^n, y^m) is equal to the entire $\mathcal{X}^n \times \mathcal{Y}^m$. Therefore, the knowledge of the side information sequence y^m at the decoder does not rule out any possibilities for x^n at the decoder. Hence, we conclude that side information provides no reduction in average codeword length (see [33] and the references therein for a discussion on zero-error coding). However, this is not the case in almost lossless source coding. See [21] for an almost lossless code in this case.

D. UcompED CODING STRATEGY

In the case of UcompED, let $l^{n,m} : \mathcal{X}^n \times \mathcal{Y}^m \rightarrow \mathbb{R}^+$ denote the universal prefix-free strictly lossless length function. Denote $L^{n,m}$ as the set of all possible such length functions. Denote $R^{n,m}(l^{n,m}, \theta^{(1)}, \theta^{(2)})$ as the expected redundancy of the code with length function $l^{n,m}(\cdot, \cdot)$:

$$R^{n,m}(l^{n,m}, \theta^{(1)}, \theta^{(2)}) \triangleq E_{X^n, Y^m \sim \mu_{\theta^{(1)}, \theta^{(2)}}^{n,m}} \{l^{n,m}(X^n, Y^m)\} - H^n(\theta^{(1)}), \quad (26)$$

where $\mu_{\theta^{(1)}, \theta^{(2)}}^{n,m}$ is the product distribution

$$\mu_{\theta^{(1)}, \theta^{(2)}}^{n,m}(x^n, y^m) \triangleq \mu_{\theta^{(1)}}^n(x^n) \mu_{\theta^{(2)}}^m(y^m). \quad (27)$$

Here we assume that $\theta^{(1)}, \theta^{(2)}$ follow the correlation model that we put forth in this paper with their marginals being Jeffreys' prior. Hence, we define

$$\underline{R}^{n,m,t} \triangleq E_{(\theta^{(1)}, \theta^{(2)}) \sim p^t} \left\{ \min_{l^{n,m} \in L^{n,m}} R^{n,m}(l^{n,m}, \theta^{(1)}, \theta^{(2)}) \right\}. \quad (28)$$

In this case, following the same lines of arguments in [32], we can conclude that

$$\underline{R}^{n,m,t} = I(X^n; \theta^{(1)} | Y^m). \quad (29)$$

The following intuitive inequality demonstrates that the redundancy decreases when side information is available.

Lemma 5: For all $n, m, t \geq 0$, we have

$$\underline{R}^{n,m,t} \leq \underline{R}^n. \quad (30)$$

with equality if and only if $\min\{n, m, t\} = 0$.

Proof: First notice that $\underline{R}^{n,m,t} = I(X^n; \theta^{(1)} | Y^m)$ and $\underline{R}^n = I(X^n; \theta^{(1)})$ and hence the inequality is achieved by applying Lemma 9 (appendix) and noticing the Markov chain $X^n \rightarrow \theta^{(1)} \rightarrow Y^m$.

Equality holds if and only if $I(X^n; Y^m) = 0$. We just need to show that $I(X^n; Y^m) = 0$ if and only if $\min\{n, m, t\} = 0$. If $n = 0$ or $m = 0$, then $I(X^n; Y^m) = 0$. If $t = 0$, then $\theta^{(1)}$ and $\theta^{(2)}$ are independent by Lemma 3. Hence, X^n and Y^m are also independent. Conversely, assume that $n, m > 0$, then by Lemma 3, $I(X^n; Y^m) = 0$ only if $t = 0$ completing the proof. ■

According to Lemma 5, side information cannot hurt, which is intuitively expected. However, there is no benefit provided by the side information when the two parameter vectors of the sources S_1 and S_2 are independent. This is not surprising as when $\theta^{(1)}$ and $\theta^{(2)}$ are independent, then X^n (produced by S_1) and Y^m (produced by S_2) are also independent. Thus, the knowledge of y^m does not affect the distribution of x^n . Hence, y^m cannot be used toward the reduction of the codeword length for x^n .

Next, we present our main result on the average maximin redundancy for strictly lossless UcompED coding.

Theorem 2: For strictly lossless UcompED coding, if $\min\{m, t\} = O_n(1)$, then

$$\underline{R}^{n,m,t} = \underline{R}^n - O_n(1),$$

and if $\min\{m, t\} = \omega_n(1)$, then⁶

$$\underline{R}^{n,m,t} = \widehat{R}(n, m, t) + o_n(1),$$

where $\widehat{R}(n, m, t)$ is defined as

$$\widehat{R}(n, m, t) \triangleq \frac{d}{2} \log \left(1 + \frac{n}{m^*(m, t)} \right), \quad (31)$$

and $m^*(\cdot, \cdot)$ is given by the following:

$$\frac{1}{m^*(m, t)} \triangleq \frac{1}{m} + \frac{2}{t}. \quad (32)$$

Proof: Recall that

$$\underline{R}^{n,m,t} = I(X^n; \theta^{(1)} | Y^m). \quad (33)$$

Further, note the following Markov chain

$$\widehat{\theta}^{(1)}(X^n) \rightarrow \theta^{(1)} \rightarrow Z^t \rightarrow \theta^{(2)} \rightarrow Y^m. \quad (34)$$

Assuming that $\min\{m, t\} = \omega_n(1)$, i.e., both grow unbounded with n . Then, we can rely on the asymptotic normality of all

⁶ $f(n) = \omega(g(n))$ if and only if $g(n) = o(f(n))$.

of the variables above and noting that $\widehat{\theta}^{(1)}(X^n)$ is a sufficient statistic for X^n , then $\theta^{(1)}$ is Gaussian distributed with mean $\widehat{\theta}(Y^m)$ with variance $\frac{1}{m^*} = \frac{2}{t} + \frac{1}{m}$ given Y^m . Hence, invoking Lemma 10 (appendix) we arrive at the desired result.

For $\min\{m, t\} = O_n(1)$, notice that from Lemma 9 we can deduce that

$$I(X^n; \theta^{(1)}) - I(X^n; \theta^{(1)}|Y^m) = I(X^n; Y^m) \leq I(\theta^{(1)}; Y^m). \quad (35)$$

Hence, the result is concluded by noting that $I(\theta^{(1)}; Y^m) = O_n(1)$. ■

Theorem 2 characterizes the average maximin redundancy in the case of UcompED with side information from a correlated source. If the sources are not sufficiently correlated or the side information string is not long enough, then not much performance improvement is expected and the redundancy is close to that of Ucomp strategy. On the other hand, for sufficiently correlated information sources with sufficiently long side information string, one expects that the redundancy would be significantly reduced. In a sense, $m^*(m, t)$ can be thought of as the effective length of the side information string. When $t \rightarrow \infty$, we see that $m^*(m, t) \approx m$ while for smaller t , we see that $m^*(m, t) < m$.

VI. SIDE INFORMATION GAIN

In this section, we define and characterize the side information gain in the different coding strategies described in Section III. Side information gain is defined as the ratio of the expected codeword length of the traditional universal compression (i.e., Ucomp) to that of the universal compression with side information from a correlated source (i.e., UcompED):

$$g^{n,m,t}(\theta) \triangleq \frac{H^n(\theta) + \underline{R}^n}{H^n(\theta) + \underline{R}^{n,m,t}}, \quad (36)$$

In other words, $g^{n,m,t}(\theta)$ is the side information gain on a string of length n drawn from μ_θ^n and compressed using UcompED coding strategy with a side information string of length m drawn from a correlated source with degree of correlation t .

The following is a trivial lower bound on the side information gain.

Lemma 6: For all $n, m, t \geq 0$, and $\theta \in \Theta_d$:

$$g^{n,m,t}(\theta) \geq 1. \quad (37)$$

Proof: This is proved by invoking Lemma 5. ■

Next, we present our main result on the side information gain in the next theorem.

Theorem 3: If $\min\{m, t\} = O_n(1)$, then $g^{n,m,t}(\theta) = 1 + O(\frac{1}{n})$. If $\min\{m, t\} = \omega_n(1)$:

$$g^{n,m,t}(\theta) = 1 + \frac{\underline{R}^n - \widehat{R}(n, m, t)}{H^n(\theta) + \widehat{R}(n, m, t)} + O\left(\frac{1}{n}\right), \quad (38)$$

where $\widehat{R}(n, m, t)$ is defined in (31).

Proof: The theorem is proved by invoking Theorem 2 and light algebraic manipulations. ■

Consider the case where the string length n grows to infinity. Intuitively, we would expect the side information gain to vanish in this case.

Lemma 7: For any $m, t \geq 0$ and any $\theta \in \Theta_d$, we have

$$\lim_{n \rightarrow \infty} g^{n,m,t}(\theta) = 1. \quad (39)$$

Let us demonstrate the significance of the side information gain through an example. We let the information source be a first-order Markov source with alphabet size $k = 256$. We also assume that the source is such that $H^n(\theta)/n = 0.5$ bit per source character (byte). In Fig. 4, the lower bound on the side information gain is demonstrated as a function of the sequence length n for different values of the memory size m . As can be seen, significant improvement in the compression may be achieved using memorization. For example, the lower bound on $g^{32\text{kB}, m, \infty}(\theta)$ is equal to 1.39, 1.92, 2.22, and 2.32, for m equal to 128kB, 512kB, 2MB, and 8MB, respectively. Further, $g^{512\text{kB}, \infty, \infty}(\theta) = 2.35$. Hence, more than a factor of two improvement is expected on top of traditional universal compression when network packets of lengths up to 32kB are compressed using side information. See [17, Section III] for practical compression methods that aim at achieving these improvements. As demonstrated in Fig. 4, the side information gain for memory of size 8MB is very close to $g^{n, \infty, \infty}(\theta)$, and hence, increasing the memory size beyond 8MB does not result in substantial increase of the side information gain. On the other hand, we further observe that as $n \rightarrow \infty$, the side information gain becomes negligible regardless of the length of the side information string. For example, at $n = 32\text{MB}$ even when $m \rightarrow \infty$, we have $g^{32\text{MB}, \infty, \infty} \approx 1.01$, which is a subtle improvement. This is not surprising as the redundancy that is removed via the side information is $O(\log n)$, and hence the gain in (38) is $O(\frac{\log n}{n})$ which vanishes as n grows.

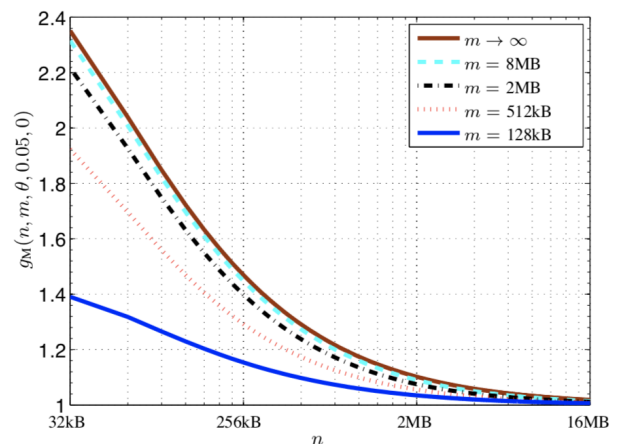


FIGURE 4. Theoretical lower bound on the side information gain $g_M(n, m, \theta, 0.05, 0)$ for the first-order Markov source with alphabet size $k = 256$ and entropy rate $H^n(\theta)/n = 0.5$.

Thus far, we have shown that significant performance improvement is obtained from side information on the compression of finite-length strings from low-entropy sources. As also was evident in the previous example, as the size of the memory increases the performance of the universal compression with side information is improved. However, there is a certain memory size beyond which increasing the side information length does not provide further compression improvement. In this section, we will quantify the required size of memory such that the benefits of the memory-assisted compression apply.

Then, the following theorem determines the size of the required memory for achieving $(1 - \delta)$ fraction of the gain for unlimited memory. Let $\widehat{g}^{n,t}(\theta)$ be defined as

$$\widehat{g}^{n,t}(\theta) \triangleq 1 + \frac{R^n}{H^n(\theta)}. \quad (40)$$

It is straightforward to see that $\widehat{g}^{n,t}(\theta)$ is the limit of side information gain as the effective side information string length $m^*(m, t) \rightarrow \infty$, where $m^*(\cdot, \cdot)$ is defined in (32).

Theorem 4: Let $m_\delta^n(\theta)$ be defined as

$$m_\delta^n(\theta) \triangleq \frac{1 - \delta}{\delta} \frac{n}{H^n(\theta)} \frac{d}{2} \log e. \quad (41)$$

Then, for any $m, t \geq 0$ such that $m^(m, t) \geq m_\delta^n(\theta)$, we have*

$$g^{n,m,t}(\theta) \geq (1 - \delta)\widehat{g}^{n,t}(\theta).$$

Proof: By invoking Theorem 3, we have

$$g^{n,m,t}(\theta) \geq \frac{H^n(\theta)}{H^n(\theta) + \widehat{R}(n, m, t)} \widehat{g}^{n,t}(\theta). \quad (42)$$

Hence, we need to show that for $m^*(m, t) > m_\delta^n(\theta)$, we have

$$\frac{H^n(\theta)}{H^n(\theta) + \widehat{R}(n, m, t)} \geq (1 - \delta). \quad (43)$$

By noting the definition of $m_\delta^n(\theta)$, for any $m^*(m, t) > m_\delta^n(\theta)$, we have

$$\frac{d}{2} \frac{n}{m^*(m, t)} \log e \leq \frac{\delta}{1 - \delta} H^n(\theta). \quad (44)$$

By noting that $\log\left(1 + \frac{n}{m}\right) \leq \frac{n}{m} \log e$, we have

$$\frac{d}{2} \log\left(1 + \frac{n}{m^*(m, t)}\right) \leq \frac{\delta}{1 - \delta} H^n(\theta), \quad (45)$$

and hence, the proof is completed by noting the definition of $\widehat{R}(n, m, t)$ in (31) and light algebraic manipulations. ■

Theorem 4 determines the size of the memory that is sufficient for the gain to be at least a fraction $(1 - \delta)$ of the gain obtained as $m \rightarrow \infty$. Considering our working example of the first-order Markov source in this section with $H^n(\theta)/n = 0.5$, with $\delta = 0.01$, we have $m_\delta(\theta) \approx 8.9\text{MB}$ is sufficient for the gain to reach 99% of its maximum confirming our previous observation. This also complements the practical observations reported in [17, Section IV.C].

VII. IMPACT OF PREFIX CONSTRAINT

Thus far, all of the results of the paper are on prefix-free codes that satisfy Kraft inequality in (19). However, we remind the reader that our main application is in network packet compression. In this case, the code need not be uniquely decodable (satisfy Kraft inequality) as the beginning and the end of each block is already determined by the header of the packet. Thus, the unique decodability condition is too restrictive and can be relaxed. It is only necessary for the mapping (the code) to be injective so as to ensure that *one* block of length n can be uniquely decoded. Such codes are known as one-to-one codes. These are also called nonsingular codes in [27, Chapter 5.1]. An interesting fact about one-to-one codes is that while the average codeword length of prefix-free codes can never be smaller than the Shannon entropy, the average codeword length of one-to-one codes can go below the entropy (cf. [34]–[38] and the references therein).

Let $l_*^n(\cdot)$ denote a strictly lossless one-to-one length function. Further, denote L_*^n as the collection of all one-to-one codes (bijective mappings to binary sequences) on sequences of length n . Let $R_*^n(l_*^n, \theta)$ denote the average redundancy of the one-to-one code, which is defined in the usual way as

$$R_*^n(l_*^n, \theta) \triangleq E\{l_*^n(X^n)\} - H_n(\theta). \quad (46)$$

Further, define

$$\underline{R}_*^n \triangleq \max_{w \in \Omega_d} \min_{l_*^n \in L_*^n} \int_{\theta \in \Theta_d} R_*^n(l_*^n, \theta) w(\theta) d\theta, \quad (47)$$

where Ω_d denotes the set of probability measures on Θ_d .

Theorem 5: The following bound holds:

$$\underline{R}_*^n \geq \frac{d - 2}{2} \log \frac{n}{2\pi e} - \log 2\pi e^2 + \int_{\theta \in \Theta_d} |\mathcal{I}(\theta)|^{\frac{1}{2}} d\theta + O\left(\frac{1}{\sqrt{n}}\right). \quad (48)$$

Proof: We have

$$H(X^n) = H(X^n|\theta) + I(X^n; \theta) \quad (49)$$

Assuming that θ follows Jeffreys' prior, we can get

$$H(X^n) = \underline{H}^n + \underline{R}^n, \quad (50)$$

where \underline{R}^n is the average minimax redundancy for prefix-free codes given in (24) and \underline{H}^n is given by

$$\underline{H}^n \triangleq \int_{\theta \in \Theta_d} H_n(\theta) w_J(\theta) d\theta. \quad (51)$$

We now invoke the main theorem in [34] to obtain a lower bound on $E\{l_*^n(X^n)\}$. The proof is completed by observing that $\log \underline{H}^n \leq \log n$ and noting that the average redundancy for the case where θ follows Jeffreys' prior provides a lower limit on the average maximin redundancy. ■

Theorem 5 shows that the compression overhead as measured against entropy is $\frac{d-2}{2} \log n + O_n(1)$. However, as discussed earlier, non-universal one-to-one codes achieve an average codeword length that can go below entropy. In particular, for the family of parametric sources studied in this paper,

for almost all $\theta \in \Theta_d$, it is shown that the average codeword length is given by $H^n(\theta) - \frac{1}{2} \log n + O_n(1)$ [35], [36], [38]. Hence, the cost of universality is $\frac{d-1}{2} \log n + O_n(1)$. See [39], [40] for a more complete study of the one-to-one universal compression problem. Additionally, see [41] for new insights on why the cost of universality scales with one less parameter in one-to-one compression, i.e., $\frac{d-1}{2}$, as compared to $\frac{d}{2}$ for prefix-free codes.

It is desirable to characterize how much reduction is offered by universal one-to-one compression compared with the prefix-free universal compression. We compare the performance of universal one-to-one codes with that of the universal prefix-free codes through the running numerical example from Section II. This example is based on a first-order Markov source with alphabet size $|\mathcal{X}| = 256$, where the number of source parameters is $d = 256 \times 255 = 62580$. Note that we have not provided an actual code for the one-to-one universal compression. We compare the converse bound of Theorem 5 with the average maximin redundancy of universal prefix-free codes.

Fig. 5 compares the minimum average number of bits per symbol required to compress the class of the first-order Markov sources normalized to the entropy of the sequence for different values of entropy rates in bits per source symbol (per byte). As can be seen, relaxing the prefix constraint at its best does not offer meaningful performance improvement on the compression performance as the curves for the prefix-free codes and one-to-one codes almost coincide. This leads to the conclusion that the universal one-to-one codes are not of much practical interest.

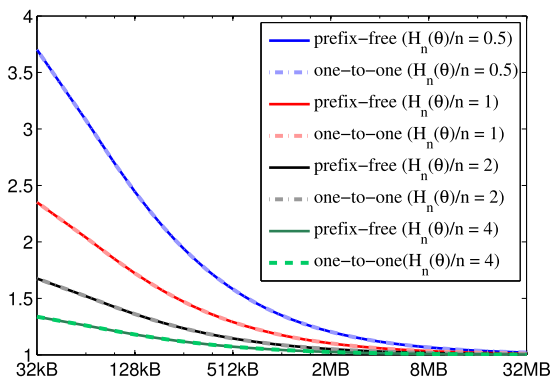


FIGURE 5. Average maximin redundancy as a function of string length for prefix-free and one-to-one universal codes for different values of entropy rate $H_n(\theta)/n$.

On the other hand, if the source entropy rate is 1 bit per byte ($H_n(\theta)/n = 1$), the compression rate on sequences of length 32kB (for both prefix-free and one-to-one codes) is around 2.25 times the entropy-rate, which results in more than 100% overhead on top of the entropy-rate for both prefix-free and one-to-one universal codes. Hence, we conclude that average redundancy poses significant overhead in the universal compression of finite-length low-entropy sequences, such as the Internet traffic, which cannot be compensated by dropping

the prefix constraint. Hence, the side information gain provided from a correlated information source is essential even if the prefix constraint is dropped.

VIII. A NETWORK CASE STUDY

In this section, we demonstrate how the side information gain could be leveraged in terms of the compression of network traffic. Assume that source S is the CNN server and the packet size is $n = 1\text{kB}$. Further, assume that the memory size is 4MB. In Section II, we demonstrated that for this source, the average compression ratio for Ucomp is $\frac{1}{n}E\{l^n(X^n)\} = 4.42$ bits per byte for this packet size. We further expected that the side information gain for such packet size be at least $g = 5$. Note that the rest of this discussion is concerned as to how the side information gain impacts the overall performance in the network.

We define the network-wide gain of side information measured in *bit* \times *hop* (BH) for the sample network presented in Fig. 6, where M denotes the memory element. Assume that the server S would serve the client C in the network. The intermediate nodes R_i are not capable of memorization. Recall that the side information gain g is only achievable on every link in a path where the encoder and the decoder both have access to the side information string.

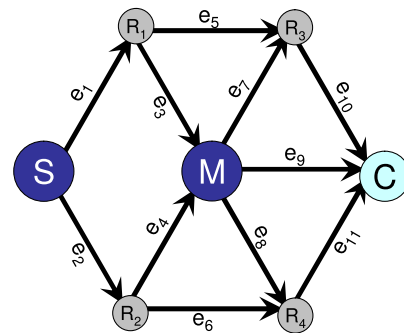


FIGURE 6. The sample network in case study.

Let $d(S, C)$ denote the length of the shortest path from S to C , which is clearly $d(S, C) = 3$, e.g., using the path e_1, e_5, e_{10} . Let $BH(S, C)$ denote the minimum bit-hop cost required to transmit the sequence (of length n) from S to C without any compression mechanism, which is $BH(S, C) = 24\text{kbits}$ (which is $1\text{kB} \times 8\text{bits/byte} \times 3$). In the case of end-to-end universal compression, i.e., using Ucomp, on the average we need to transmit $BH_{\text{Ucomp}} = E\{l^n(X^n)\}d(S, C)$ bit \times hop for the transmission of a packet of length n to the client.

On the other hand, in the case of universal compression with side information, i.e., using UcompED, for every information bit on the path from the server to the memory element M , we can leverage the side information, and hence, we only require $\frac{1}{n}E\{l^{n,m}(X^n, Y^m)\} = \frac{1}{ng}E\{l^n(X^n)\}$ bit transmissions per each source character that is transmitted to the memory element. Then, the memory element M will decode the received codeword using UcompED decoder and the side information string y^m . It will then re-encode the

result using Ucomp encoder for the final destination (the client C). In this example, this implies that we require to transmit $\frac{2}{n}E\{l^{n,m}(X^n, Y^m)\}$ bit \times hop on the average from S to M on links e_1 and e_3 (where $d(S, M) = 2$) for each source character. Then, we transmit the message using $E\{l^n(X^n)\}$ bit \times hop per source character from M to C on the link e_9 . Let $BH_{UcompED}$ be the minimum bit \times hop cost for transmitting the string (of length n) using network compression that leverages side information in the $S \rightarrow M$ path, i.e.,

$$\begin{aligned} BH_{UcompED} &= d(S, M)E\{l^{n,m}(X^n, Y^m)\} \\ &\quad + d(M, C)E\{l^n(X^n)\} \\ &= 2E\{l^{n,m}(X^n, Y^m)\} + E\{l^n(X^n)\}. \end{aligned} \quad (52)$$

Further, let \mathcal{G}_{BH} be the bit \times hop gain of network compression, defined as $\mathcal{G}_{BH} = \frac{BH_{Ucomp}}{BH_{UcompED}}$. Thus, $\mathcal{G}_{BH} = 2.14$ in this example by substituting $g = 5$. In other words, network compression (using UcompED in the $S \rightarrow M$ path) achieves more than a factor of 2 saving in bit \times hop over the traditional universal compression of the packet (using Ucomp from S to C) in the sample network.

In [17], we fully characterize the scaling of the bit \times hop gain, \mathcal{G}_{BH} , for scale-free networks (random power-law graphs) as a function of side information gain, g . We show that $\mathcal{G}_{BH} \approx g$ if the fraction of nodes in the network equipped with memorization capability is larger than a phase-transition cutoff. We refer the interested reader to [17] for more details.

IX. CONCLUSION

In this paper, we formulated and studied universal compression with side information from a correlated source. We showed that redundancy can impose a significant overhead in universal compression of finite-length sequences, such as network packets. We put forth a notion of correlation between information sources where the degree of correlation is controlled by a single hyperparameter. We showed that side information from a correlated source can significantly suppress the redundancy in universal compression. We defined the side information gain and showed that it can be large with reasonable side information size for small strings, such as network packets. We showed that this gain is largely preserved even if the code is allowed to be only almost lossless allowing a sufficiently small error that vanishes asymptotically. We also showed that dropping the prefix constraint would not remedy the universal compression problem either. Finally, we showed how these benefits are applicable in network compression in a case study.

ASSUMPTIONS AND PROOFS

Assumption 1 (regularity conditions): We need some regularity conditions to hold for the parametric model so that our results can be derived.

- 1) The parametric model is smooth, i.e., twice differentiable with respect to θ in the interior of Θ_d so that

the Fisher information matrix can be defined. Further, the limit in (2) exists.

- 2) The determinant of fisher information matrix is finite for all θ in the interior of Θ_d and the normalization constant in the denominator of (3) is finite.
- 3) The parametric model has a minimal d -dimensional representation, i.e., $\mathcal{I}(\theta)$ is full-rank. Hence, $\mathcal{I}^{-1}(\theta)$ exists.
- 4) We require that the central limit theorem holds for the maximum likelihood estimator $\hat{\theta}(x^n)$ of each θ in the interior of Θ_d so that $(\hat{\theta}(X^n) - \theta)\sqrt{n}$ converges to a normal distribution with zero mean and covariance matrix $\mathcal{I}^{-1}(\theta)$.

Lemma 8: For all $t \geq 0$, we have

$$\begin{aligned} E_{\theta^{(1)} \sim q} \left\{ f^t(\theta^{(1)}, \theta^{(2)}) \right\} &= \int_{\theta^{(1)} \in \Theta_d} f^t(\theta^{(1)}, \theta^{(2)}) w(\theta^{(1)}) d\theta^{(1)} \\ &= 1. \end{aligned} \quad (53)$$

Proof: Following the equations

$$\begin{aligned} &\int_{\theta^{(1)} \in \Theta_d} f^t(\theta^{(1)}, \theta^{(2)}) w(\theta^{(1)}) d\theta^{(1)} \\ &= \sum_{z^t \in \mathcal{X}^t} \left(\frac{\mu_{\theta^{(2)}}^t(z^t) \int_{\theta^{(1)} \in \Theta_d} \mu_{\theta^{(1)}}^t(z^t) w(\theta^{(1)}) d\theta^{(1)}}{\int_{\phi \in \Theta_d} \mu_{\phi}^t(z^t) w(\phi) d\phi} \right) \\ &= \sum_{z^t \in \mathcal{X}^t} \mu_{\theta^{(2)}}^t(z^t) \end{aligned} \quad (54)$$

$$= 1, \quad (55)$$

where (54) is obtained since the two integral terms in the numerator and denominator cancel each other out. ■

Lemma 9: Let $X \rightarrow Y \rightarrow Z$ form a Markov chain. Then,

$$I(X; Y) \geq I(X; Y|Z), \quad (56)$$

with equality if and only if $I(X; Z) = 0$. The gap in the inequality is also fully characterized by

$$I(X; Y) - I(X; Y|Z) = I(X; Z). \quad (57)$$

Proof: This is a well-known result on Markov chains and could be proved by applying the chain rule to $I(X; Y, Z)$ in different orders and noting that $I(X; Z|Y) = 0$ due to the Markov chain. ■

Lemma 10: Let $X \rightarrow Y \rightarrow Z$ form a Markov chain, where X, Y, Z are all Gaussian distributed and supported on \mathbb{R}^d . Further, let X follow a non-informative improper uniform distribution on \mathbb{R}^d . Let Y be a noisy observation of X with variance σ^2 , i.e., $Y = X + N_1$ where $N_1 \sim \mathcal{N}(\mathbf{0}_d, \sigma^2 I_d)$ is independent of X , and $\mathbf{0}_d$ and I_d denote the d -dimensional all-zero vector and identity matrix, respectively. In the same way, let Z be a noisy observation of Y with variance τ^2 . Then,

$$I(X; Y|Z) = \frac{d}{2} \log \left(1 + \frac{\tau^2}{\sigma^2} \right). \quad (58)$$

Proof: The proof is completed by following the following equations:

$$I(X; Y|Z) = h(X|Z) - h(X|Y, Z) \quad (59)$$

$$= h(X|Z) - h(X|Y) \quad (60)$$

$$= \frac{d}{2} \log(2\pi e(\sigma^2 + \tau^2)) - \frac{d}{2} \log(2\pi e\sigma^2) \quad (61)$$

$$= \frac{d}{2} \log\left(1 + \frac{\tau^2}{\sigma^2}\right). \quad (62)$$

where h denotes differential entropy. ■

Lemma 11: The following inequality holds:

$$H(X^n | \mathbf{1}_e(X^n), \widehat{X}^n) \leq \epsilon H(X^n). \quad (63)$$

Proof:

$$H(X^n | \mathbf{1}_e(X^n), \widehat{X}^n) = (1 - \epsilon)H(X^n | \mathbf{1}_e(X^n), 0, \widehat{X}^n) + \epsilon H(X^n | \mathbf{1}_e(X^n) = 1, \widehat{X}^n) \quad (64)$$

$$\leq \epsilon n \log |\mathcal{X}|. \quad (65)$$

The first term in (64) is zero since if $\mathbf{1}_e(X^n) = 0$, we have $X^n = \widehat{X}^n$ and hence

$$H(X^n | \mathbf{1}_e(X^n), 0, \widehat{X}^n) = 0.$$

The inequality in (65) then follows from the fact that x^n is supported on \mathcal{X}^n , and hence its entropy is bounded from above by $n \log |\mathcal{X}|$. ■

Lemma 12: The average minimax redundancy for the almost lossless Ucomp coding strategy is lower bounded by

$$\underline{R}_\epsilon^n \geq (1 - \epsilon)\underline{R}^n - h_b(\epsilon) - \epsilon n \log |\mathcal{X}|,$$

where $h_b(\epsilon)$ is the binary entropy function defined as:

$$h_b(\epsilon) \triangleq \epsilon \log\left(\frac{1}{\epsilon}\right) + (1 - \epsilon) \log\left(\frac{1}{1 - \epsilon}\right). \quad (66)$$

Proof: Consider $H(X^n, \widehat{X}^n, \mathbf{1}_e(X^n))$. Note that both \widehat{X}^n and $\mathbf{1}_e(X^n)$ are deterministic functions of X^n and hence

$$H(X^n, \widehat{X}^n, \mathbf{1}_e(X^n)) = H(X^n). \quad (67)$$

On the other hand, we can also use the chain rule in a different order to obtain

$$H(X^n, \widehat{X}^n, \mathbf{1}_e(X^n)) = H(\widehat{X}^n) + H(\mathbf{1}_e(X^n) | \widehat{X}^n) + H(X^n | \mathbf{1}_e(X^n), \widehat{X}^n). \quad (68)$$

Hence,

$$H(\widehat{X}^n) = H(X^n) - H(\mathbf{1}_e(X^n) | \widehat{X}^n) - H(X^n | \mathbf{1}_e(X^n), \widehat{X}^n) \geq H(X^n) - h_b(\epsilon) - H(X^n | \mathbf{1}_e(X^n), \widehat{X}^n) \quad (69)$$

$$\geq H(X^n) - h_b(\epsilon) - \epsilon n \log |\mathcal{X}|, \quad (70)$$

where the inequality in (69) is due to the fact that $H(\mathbf{1}_e(X^n) | \widehat{X}^n) \leq H(\mathbf{1}_e(X^n)) = h_b(\epsilon)$ and the inequality in (70) is due to Lemma 11. The proof of the lemma is completed by noting that $H(X^n) = H^n(\theta) + \underline{R}_\epsilon^n$. ■

REFERENCES

- [1] Z. Zhuang, C.-L. Tsao, and R. Sivakumar, "Curing the amnesia: Network memory for the Internet," Georgia Inst. Technol., Atlanta, GA, USA, Tech. Rep., 2009. [Online]. Available: https://www.researchgate.net/profile/Zhenyun_Zhuang/publication/267767740_Curing_the_amnesia_Network_memory_for_the_Internet/links/545cd47f0cf27487b44d40c1f/Curing-the-amnesia-Network-memory-for-the-Internet.pdf
- [2] A. Anand, A. Gupta, A. Akella, S. Seshan, and S. Shenker, "Packet caches on routers: The implications of universal redundant traffic elimination," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 4, pp. 219–230, 2008.
- [3] A. Anand, V. Sekar, and A. Akella, "SmartRE: An architecture for coordinated network-wide redundancy elimination," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 87–98, 2009.
- [4] A. Anand, C. Muthukrishnan, A. Akella, and R. Ramjee, "Redundancy in network traffic: Findings and implications," in *Proc. 11th Int. Joint Conf. Meas. Modelling Comput. Syst. (SIGMETRICS)*. New York, NY, USA: ACM, 2009, pp. 37–48.
- [5] N. Spring and D. Wetherall, "A protocol-independent technique for eliminating redundant network traffic," in *Proc. ACM SIGCOMM*, 2000, pp. 87–95.
- [6] S. Iyer, A. Rowstron, and P. Druschel, "Squirrel: A decentralized peer-to-peer Web cache," in *Proc. 21st Annu. Symp. Princ. Distrib. Comput. (PODC)*. New York, NY, USA: ACM, 2002, pp. 213–222.
- [7] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. C. Snoeren, "Cloud control with distributed rate limiting," in *Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun. (SIGCOMM)*. New York, NY, USA: ACM, 2007, pp. 337–348.
- [8] D. Qiu and R. Srikant, "Modeling and performance analysis of bittorrent-like peer-to-peer networks," in *Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun. (SIGCOMM)*. New York, NY, USA: ACM, 2004, pp. 367–378.
- [9] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 3, pp. 337–343, May 1977.
- [10] J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 5, pp. 530–536, Sep. 1978.
- [11] F. M. J. Willems, Y. M. Shtarkov, and T. J. Tjalkens, "The context-tree weighting method: Basic properties," *IEEE Trans. Inf. Theory*, vol. 41, no. 3, pp. 653–664, May 1995.
- [12] L. Davisson, "Universal noiseless coding," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 6, pp. 783–795, Nov. 1973.
- [13] J. Rissanen, "Universal coding, information, prediction, and estimation," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 4, pp. 629–636, Jul. 1984.
- [14] N. Merhav and M. Feder, "A strong version of the redundancy-capacity theorem of universal coding," *IEEE Trans. Inf. Theory*, vol. 41, no. 3, pp. 714–722, May 1995.
- [15] A. Barron, J. Rissanen, and B. Yu, "The minimum description length principle in coding and modeling," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2743–2760, Oct. 1998.
- [16] A. Beirami and F. Fekri, "Results on the redundancy of universal compression for finite-length sequences," in *Proc. IEEE Int. Symp. Inf. (ISIT)*, Jul. 2011, pp. 1604–1608.
- [17] A. Beirami, M. Sardari, and F. Fekri, "Packet-level network compression: Realization and scaling of the network-wide benefits," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1588–1604, Jun. 2016.
- [18] B. S. Clarke and A. R. Barron, "Information-theoretic asymptotics of Bayes methods," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 453–471, May 1990.
- [19] K. Atteson, "The asymptotic redundancy of Bayes rules for Markov chains," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2104–2109, Sep. 1999.
- [20] *Virtual Networking Index Forecast*, CISCO, San Jose, CA, USA, 2012.
- [21] A. Beirami, M. Sardari, and F. Fekri, "Wireless network compression via memory-enabled overhearing helpers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 176–190, Jan. 2016.
- [22] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.
- [23] D.-K. He, L. A. Lastras-Montano, E.-H. Yang, A. Jagmohan, and J. Chen, "On the redundancy of Slepian–Wolf coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5607–5627, Dec. 2009.
- [24] M. Sartipi and F. Fekri, "Distributed source coding using short to moderate length rate-compatible LDPC codes: The entire Slepian–Wolf rate region," *IEEE Trans. Commun.*, vol. 56, no. 3, pp. 400–411, Mar. 2008.

- [25] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar. 2003.
- [26] W. Szpankowski, "Asymptotic average redundancy of Huffman (and other) block codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2434–2443, Nov. 2000.
- [27] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.
- [28] G. G. Langdon, "An introduction to arithmetic coding," *IBM J. Res. Develop.*, vol. 28, no. 2, pp. 135–149, Mar. 1984.
- [29] D. Huffman, "A method for the construction of minimum-redundancy codes," *Proc. IRE*, vol. 40, no. 9, pp. 1098–1101, Sep. 1952.
- [30] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Aug. 1948.
- [31] M. Drmota and W. Szpankowski, "Precise minimax redundancy and regret," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2686–2707, Nov. 2004.
- [32] R. G. Gallager, "Source coding with side information and universal coding," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. LIDS-p-397, 1979.
- [33] N. Alon and A. Orlitsky, "Source coding and graph entropies," *IEEE Trans. Inf. Theory*, vol. 42, no. 5, pp. 1329–1339, Sep. 1996.
- [34] N. Alon and A. Orlitsky, "A lower bound on the expected length of one-to-one codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1670–1672, Sep. 1994.
- [35] W. Szpankowski, "A One-to-One code and its anti-redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4762–4766, Oct. 2008.
- [36] I. Kontoyiannis and S. Verdu, "Optimal lossless data compression: Non-asymptotics and asymptotics," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 777–795, Feb. 2014.
- [37] S. Leung-Yan-Cheong and T. Cover, "Some equivalences between Shannon entropy and Kolmogorov complexity," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 331–338, May 1978.
- [38] W. Szpankowski and S. Verdu, "Minimum expected length of fixed-to-variable lossless compression without prefix constraints," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4017–4025, Jul. 2011.
- [39] A. Beirami and F. Fekri, "Fundamental limits of universal lossless one-to-one compression of parametric sources," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014, pp. 212–216.
- [40] O. Kosut and L. Sankar, "Asymptotics and non-asymptotics for universal fixed-to-variable source coding," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3757–3772, Jun. 2017.
- [41] A. Beirami, R. Calderbank, M. M. Christiansen, K. R. Duffy, and M. Medard, "A characterization of guesswork on swiftly tilting curves," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 2850–2871, May 2019.



AHMAD BEIRAMI received the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, in 2014. His research interest includes fundamental limits of information processing systems. He was a recipient of the 2015 Sigma Xi Best Ph.D. Thesis Award from Georgia Tech.



FARAMARZ FEKRI (Fellow, IEEE) received the Ph.D. degree from the Georgia Institute of Technology, Atlanta, GA, USA, in 2000. Since 2000, he has been a Faculty Member with the School of Electrical and Computer Engineering, Georgia Institute of Technology, where he is currently a Professor position. He serves on the technical program committees of several IEEE conferences. His research interests include communications and signal processing, in particular, source and channel coding, information theory in biology, statistical inference in large data, information processing for wireless and sensor networks, and communication security. He received the National Science Foundation CAREER Award, in 2001, the Southern Center for Electrical Engineering Education (SCEEE) Young Faculty Development Award, in 2003, and the Outstanding Young Faculty Award of the School of ECE, in 2006. He is an Associate Editor of the *IEEE TRANSACTIONS ON MOLECULAR, BIOLOGICAL, AND MULTI-SCALE COMMUNICATIONS*. In the past, he has served on the Editorial Board for the *IEEE TRANSACTIONS ON COMMUNICATIONS*, and the Elsevier journal on *Physical Communication* (PHYCOM).

• • •