Secure Cascade Channel Synthesis

Sanket Satpathy and Paul Cuff

Dept. of Electrical Engineering

Princeton University

Princeton, USA

Email: {satpathy,cuff}@princeton.edu

Abstract—We investigate channel synthesis in a cascade setting where nature provides an iid sequence X^n at node 1. Node 1 can send a message at rate R_1 to node 2 and node 2 can send a message at rate R_2 to node 3. Additionally, all 3 nodes share bits of common randomness at rate R_0. We want to generate sequences Y^n and Z^n along nodes in the cascade such that (X^n, Y^n, Z^n) appears to be appropriately correlated and iid even to an eavesdropper who is cognizant of the messages being sent. We characterize the optimal tradeoff between the amount of common randomness used and the required rates of communication. We also solve the problem for arbitrarily long cascades and provide an inner bound for cascade channel synthesis without an eavesdropper.

Fig. 1. The iid sequence X^n is given by nature. Messages J_1 and J_2 are sent along the cascade at rates R_1 and R_2. Common randomness at rate R_0 is shared by all 3 nodes. We want (X^n, Y^n, Z^n) iid correlated and independent of the messages (J_1, J_2).

I. INTRODUCTION

Since Shannon introduced the notion of mutual information, many attempts have been made to measure the correlation between random variables[1], [2], [3], [4]. Each of them is relevant in the context of the operational questions they address. New life has been breathed into these attempts by a line of inquiry into measures of correlation with a view to perform synthesis under a total variation constraint, known as strong coordination[3] or channel synthesis[5]. The optimal tradeoff between communication and common randomness was derived by Cuff[4] and Bennett et al.[6] for the case of two random variables and the results have been independently rediscovered and extended in other work[7], [8], [9], [10], [11], [5]. One particularly pleasing aspect of the above tradeoff was that it recovered two familiar measures of correlation as the required rate of communication - mutual information and Wyner's common information[2] in the presence of abundant and no common randomness, respectively.

Requiring that the synthesized joint distribution be close to the desired joint distribution in total variation is a more stringent constraint than empirical coordination[12], [3] i.e. jointly typical input and output sequences. On the other hand, we enjoy the benefit of the synthesized sequences being immune to statistical tests designed to detect iid correlated sequences[5]. This aspect of the results coupled with the nice properties of total variation as a metric such as a bound on entropy[13, Theorem 17.3.3] has led to applications in secrecy[14], [15], [16] and game theory[4], [17], [5]. We refer the interested reader to [5], [18] for a more thorough discussion of the properties of total variation and comparison with other metrics.

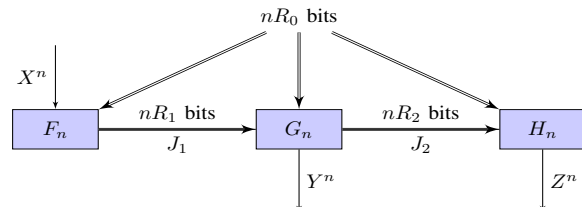This particular work is inspired by the suite of extensions presented in [5] with a focus on secrecy applications. To extend these applications to general networks, it is desirable to have a theory of strong coordination over arbitrary networks[7], [10]. The cascade channel synthesis problem shown in Fig.1 provides a starting point for such a theory. Distributed networks for control and sensing are seemingly ubiquitous - the power grid, road networks, server farms and the internet are a few prominent examples[19]. In many control settings, one would like the actions at various nodes to be independent of the communication so the actions cannot be anticipated by malicious eavesdroppers. We consider the problem of synthesizing sequences that appear to be iid and appropriately correlated even to an onlooker who can see messages sent over the communication channel, but does not have access to the source of common randomness.

The cascade structure for communication is especially relevant for large distributed networks where there is a cost per unit distance associated with sending messages. In such a setting, it would be more economical for nodes to forward appropriate messages locally in a cascade fashion rather than having a central node talk to all the other nodes. Also in some settings, there might be a hierarchy among the nodes that inherits the cascade structure (for example, in parallel computation interaction takes place in a master-slave hierarchy). In Section IV, we characterize the optimal rate region for the task assignment problem, where 3 out of $m \geq 3$ tasks have to be distributed uniformly at random to the 3 nodes, with the first node's tasks chosen at random by nature.

In this work, we assume that every node in the cascade has sufficient local randomness. We provide a precise description of the problem in Section II and present a characterization of the optimal rate region in Section III. One unexpected feature of the optimal region is that there is no loss of generality in

assuming that the second message is a function of the first i.e. the local randomness used in synthesizing Y^n is not essential to correlating Z^n with (X^n, Y^n). However, it is precisely this feature that proves to be our undoing for the corresponding scheme in the cascade channel synthesis problem with no eavesdropper as discussed in Section VII.

II. PRELIMINARIES AND PROBLEM DEFINITION

A. Notation

We represent both random variables and probability distribution functions with capital letters, but only letters P and Q are used for the latter. If it is not clear from context, we include subscripts to denote that $P_{Y|X}(y|x)$ is the conditional distribution of the random variable Y given the random variable X. We may abbreviate this as $P(y|x)$ or $P_{Y|X}$. Also, we use the script letter $\mathcal{X} \ni x$ to denote the alphabet of X. Sequences of random variables $X_1, \ldots, X_n$ are denoted by X^n. The set $\{1, \ldots, m\}$ is denoted by $[m]$.

Markov chains are denoted by $X - Y - Z$ implying the factorization $P_{XYZ} = P_{XY} P_{Z|Y}$. We define the total variation distance as

$$\|P_X - Q_X\|_{TV} \triangleq \frac{1}{2} \sum_x |P(x) - Q(x)|. \quad (1)$$

B. Problem-Specific Definitions

We have the iid source $X^n \sim \prod_{i=1}^n Q_X$ and we would like to *synthesize* the channel $Q_{YZ|X}$. Messages sent along the cascade communication links are denoted by $J_1 \in [2^{nR_1}]$ and $J_2 \in [2^{nR_2}]$. The common randomness shared by all nodes K is uniformly distributed on $[2^{nR_0}]$ and independent of X^n.

Definition 1. A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ *secure cascade channel synthesis (SCCS) code* consists of randomized encoding functions

$$F_n : \mathcal{X}^n \times [2^{nR_0}] \to [2^{nR_1}],$$
$$G_n^{(enc)} : [2^{nR_1}] \times [2^{nR_0}] \to [2^{nR_2}],$$

and randomized decoding functions

$$G_n^{(dec)} : [2^{nR_1}] \times [2^{nR_0}] \to \mathcal{Y}^n,$$
$$H_n : [2^{nR_2}] \times [2^{nR_0}] \to \mathcal{Z}^n.$$

We have $J_1 = F_n(X^n, K), J_2 = G_n^{(enc)}(J_1, K), Y^n = G_n^{(dec)}(J_1, K)$ and $Z^n = H_n(J_2, K)$.

Note that node 2 has both encoding and decoding capability. The *induced joint distribution* of a $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ SCCS code is the joint distribution $P_{X^n, Y^n, Z^n, K, J_1, J_2}$ as per the above specifications.

Definition 2. A sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ SCCS codes for $n \geq 1$ is said to *achieve* $Q_{YZ|X}$ if the induced joint distributions have marginals that satisfy

$$\lim_{n \to \infty} \left\| P_{X^n Y^n Z^n J_1 J_2} - P_{J_1 J_2} \prod_{t=1}^n Q(x_t, y_t, z_t) \right\|_{TV} = 0. \quad (2)$$

Definition 3. A rate triple (R_0, R_1, R_2) is said to be *achievable* if there exists a $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ SCCS code that achieves $Q_{YZ|X}$.

Definition 4. The *secure synthesis rate region* $\mathcal{C}$ is the closure of achievable triples (R_0, R_1, R_2).

III. MAIN RESULT

The characterization of the set of achievable rate triples is given in terms of the following set

$$\mathcal{S}_D \triangleq \left\{ \begin{array}{ll} (R_0, R_1, R_2) \in \mathbb{R}^3 & : \quad \exists P_{X,Y,Z,U,V} \in D \text{ s.t.} \\ \quad R_1 & \geq \quad I(X; U, V) \\ \quad R_2 & \geq \quad I(X; V) \\ \quad R_0 & \geq \quad I(X, Y, Z; U, V) \end{array} \right\}, \quad (3)$$

where

$$D \triangleq \left\{ \begin{array}{ll} P_{X,Y,Z,U,V} & : \quad (X, Y, Z) \sim Q_X Q_{YZ|X}, \\ & \quad X - (U, V) - Y, \\ & \quad (X, Y, U) - V - Z, \\ & \quad |\mathcal{V}| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{Z}| + 3, \\ & \quad |\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{Z}||\mathcal{V}| + 2 \end{array} \right\}. \quad (4)$$

Also, let $D' = D \cap \{P_{X,Y,Z,U,V} : H(V|U) = 0\}$ denote the restriction of D to joint distributions where V is a function of U.

Theorem 1.

$$\mathcal{C} = \mathcal{S}_D = \mathcal{S}_{D'}. \quad (5)$$

IV. OBSERVATIONS AND EXAMPLES

Note that the communication rate region of our result coincides with the rate region for empirical coordination in the cascade channel[3] since there must exist a realization of the shared randomness that yields good empirical coordination codes, in agreement with Theorem 2 of [3]. Also this observation consolidates the intuition that the onus of secrecy that we have taken on is borne primarily by the available common randomness.

The two node channel synthesis problem[4], [5] recovered mutual information and Wyner's common information as the required communication rates at the extremes of abundant and no common randomness, respectively. The problem we consider is that of secure coordination. We do not have constraints on the sum of communication and common randomness rates since we cannot afford to have public messages give away too much about our coordination scheme. The extremes of our region are not determined by the amount of common randomness available, but we see that the minimum rates follow the same trend as above.

By the data-processing inequality[13], the choice $(U, V) = (Y, Z)$ simultaneously minimizes both the communication rates at $R_1 \geq I(X; Y, Z)$ and $R_2 \geq I(X; Z)$. Also, the minimum achievable rate of common randomness is

$$C_c(X; Y; Z) = \min_{\substack{(U,V): X-(U,V)-Y, \\ (X,Y,U)-V-Z}} I(X, Y, Z; U, V), \quad (6)$$

which can be viewed as a generalization of Wyner's common information in the cascade setting. Another straightforward generalization of Wyner's common information that has been considered in the literature[20] is

$$C(X;Y;Z) = \min I(X,Y,Z;U), \qquad (7)$$

where the minimum is over random variables U such that given U, X,Y and Z are independent of each other. In fact, the two quantities are the same. This is because the minimizers of (7) and (6) are compatible with each other's Markov structures. For example, if $\hat{U}$ attains the minimum for (7), then $(U,V) = (\emptyset, \hat{U})$ satisfies the Markov chains in (6). Note that the communication and common randomness rates cannot be simultaneously minimized in general.

A. Task Assignment

We now compute our region for a toy problem of task assignment, where 3 out of $m \geq 3$ tasks are to be assigned to the 3 nodes uniformly at random. To be precise, we consider a channel $Q_{YZ|X}$ that acts on X uniformly distributed on $[m]$ i.e. $Q_X = m^{-1}$ and produces a pair $Y \neq Z$ uniformly distributed over all distinct pairs in $[m] \setminus \{X\}$. This is a generalization of the scatter channel example in [5].

As per (3), we consider joint distributions $P_{X,Y,Z,U,V} \in D$. The Markov chains ensure that for each pair (u,v) in the support of (U,V), the conditional distributions $P_{X,Y|U=u,V=v}$ and $P_{X,Y,Z|V=v}$ factor as $P_{X|U=u,V=v}P_{Y|U=u,V=v}$ and $P_{X,Y|V=v}P_{Z|V=v}$ respectively. Also, these distributions have the constraint that the supports of X,Y and Z cannot intersect.

The above constraint dictates that $|\text{support}(X,Y)| = a \in [m-1] \setminus \{1\}$ and that $|\text{support}(Y)| = b \in [a-1]$, enumerating all possible sparsity patterns. Since we seek U and V to enforce the above Markov chains, consider V to specify support(X,Y) and U to specify support(Y). For each of the above categories, we have trivial bounds on conditional entropy:

$$H(X|V=v) \leq \log a \qquad (8)$$
$$H(X|U=u,V=v) \leq \log(a-b) \qquad (9)$$
$$H(X,Y,Z|U=v,V=v) \leq \log(a-b)b(m-a). \quad (10)$$

The above inequalities give lower bounds on the required rates that are achieved by letting U and V be uniformly distributed over all appropriate supports of sizes b and a respectively, and selecting uniform distributions over supports. Thus, the rate region is given by the convex hull of the set

$$\left\{ \begin{array}{rcl} (R_0, R_1, R_2) \in \mathbb{R}^3 & : & \exists a \in [m-1], b \in [a-1] \text{ s.t.} \\ R_1 & \geq & \log\left(\frac{m}{a-b}\right) \\ R_2 & \geq & \log\left(\frac{m}{a}\right) \\ R_0 & \geq & \log\left(\frac{m(m-1)(m-2)}{(a-b)b(m-a)}\right) \end{array} \right\}. \quad (11)$$

The communication rates are minimized when $a = m-1$ and $b = 1$ i.e. given (U,V), the uncertainty is concentrated on X. On the other hand, the common randomness requirement is minimized when $b \approx \frac{m}{3}$ and $a \approx \frac{2m}{3}$ up to the nearest integer i.e. given (U,V), the uncertainty is shared equally by X,Y and Z. The tradeoff between information content of the messages and rate of common randomness is evident here.

V. Sketch of Converse

Let (R_0, R_1, R_2) be achievable. Then for $\epsilon \in (0, 1/4)$ there exists a $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ secure channel synthesis code with an induced joint distribution $P_{X^n, Y^n, Z^n, K, J_1, J_2}$ such that

$$\lim_{n\to\infty} \left\| P_{X^nY^nZ^nJ_1J_2} - P_{J_1J_2}\prod_{l=1}^{n}Q(x_l,y_l,z_l) \right\|_{TV} < \epsilon. \quad (12)$$

We shall use the random variable T uniformly distributed on $[n]$, as a time index. First, we use the triangle inequality and [5, Lemma V.1] to note that

$$\|P_{X^nY^nZ^nJ_1J_2} - P_{J_1J_2}P_{X^nY^nZ^n}\|_{TV} \leq \cdots$$

$$2\left\| P_{X^nY^nZ^nJ_1J_2} - P_{J_1J_2}\prod_{l=1}^{n}Q(x_l,y_l,z_l) \right\|_{TV} < 2\epsilon. \quad (13)$$

A. Entropy Bounds

We will need the following bounds on entropy in terms of total variation[5, Lemma VI.3]. If the joint distribution of (X^n, Y^n, Z^n) is close in total variation to an iid distribution as assumed, then we have

$$\sum_{t=1}^{n} I_P(X_t, Y_t, Z_t; X^{t-1}, Y^{t-1}, Z^{t-1}) \leq ng(\epsilon), \quad (14)$$

$$I_P(X_T, Y_T, Z_T; T) \leq ng(\epsilon), \quad (15)$$

where

$$g(\epsilon) \triangleq 4\epsilon \log\left(\frac{|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|}{\epsilon}\right). \quad (16)$$

Note that $\lim_{\epsilon\downarrow 0} g(\epsilon) = 0$.

B. Approximate Rate Region

We use standard information-theoretic inequalities, the physical constraint $X^n - (J_1, K) - J_2$ and the fact that X^n and K are independent to bound the communication rates:

$$nR_1 \geq H(J_1) \qquad \geq H(J_1|K) \qquad (17)$$
$$\geq I(X^n; J_1|K) = I(X^n; J_1, J_2, K), \quad (18)$$
$$nR_2 \geq H(J_2) \qquad \geq H(J_2|K) \qquad (19)$$
$$\geq I(X^n; J_2|K) = I(X^n; J_2, K). \quad (20)$$

Finally, we bound R_0:

$$nR_0 \geq H(K) \geq H(K|J_1, J_2) \qquad (21)$$
$$\geq I(X^n, Y^n, Z^n; K|J_1, J_2) \qquad (22)$$
$$\geq I(X^n, Y^n, Z^n; J_1, J_2, K) - g(2\epsilon) \qquad (23)$$
$$\geq \sum_{t=1}^{n} I(X_t, Y_t, Z_t; J_1, J_2, K) - g(2\epsilon) - ng(\epsilon) \quad (24)$$
$$\geq nI(X_T, Y_T, Z_T; J_1, J_2, K|T) - (n+1)g(\epsilon) \quad (25)$$
$$\geq nI(X_T, Y_T, Z_T; J_1, J_2, K, T) - (2n+1)g(\epsilon). \quad (26)$$

Theorem 17.3.3 of [13] coupled with (13) was used in the third line and the other steps follow from (14) and (15). The single-letterization for the communication rates is done similarly. Making associations $U' = J_1$ and $V' = (J_2, K, T)$, we see that the rates and Markov chains in (3) and (4) are satisfied up to the correction in (26).

Using a generalized Carathéodory theorem, we can show existence of a distribution Γ_{XYZUV} with (U, V) satisfying the cardinality bounds and Markov chains as in (4), but using [5, Lemma VI.2] we only have that

$$\left\| \Gamma_{XYZ} - Q_X Q_{YZ|X} \right\|_{TV} < \epsilon, \quad (27)$$

yielding approximate versions of $\mathcal{S}_D$ and D. The final step is to take $\epsilon \downarrow 0$ and use a compactness argument as in [5, Lemma VI.5] to conclude that the above region coincides with (3) in the limit.

C. Comment on Converse

Note that the above arguments go through with the associations $U = (J_1, J_2, K, T)$ and $V = (J_2, K, T)$, establishing that there is no loss of generality in assuming that V is a function of U in the rate region description. In the argument for the cardinality bound, we find it helpful to rewrite $(X, Y, U) - V - Z$ as the equivalent constraint $I(X, Y, U; Z|V) = 0$. This lets us first bound $|\mathcal{V}|$ without worrying about $|\mathcal{U}|$.

VI. Sketch of Achievability

A. Cloud-Mixing

Given a channel $Q_{V|U}$, we want to synthesize $V^n \sim \prod Q_V$ at the output. However, we would like to do it using a small codebook of $U^n \sim \prod Q_U$ codewords. How large does the codebook need to be? The cloud-mixing lemma provides the answer. It is implied by results on resolvability[21] and goes back to Wyner's work[2]. The key ingredients of our proof are the following lemmas.

Lemma 1 (Lemma IV.1 in [5]). For any discrete distribution Q_{UV} and $n \geq 1$, let $\mathcal{B}^{(n)} = \{U^n(m)\}_{m=1}^{2^{nR}}$ be a codebook of sequences each drawn independently from $\prod_{k=1}^n Q_U(u_k)$. For a fixed codebook, define

$$P(v^n) = 2^{-nR} \sum_{m=1}^{2^{nR}} \prod_{k=1}^n Q_{V|U}(v_k|U_k(m)). \quad (28)$$

Then if $R > I(V; U)$,

$$\lim_{n \to \infty} \mathbb{E} \left\| P(v^n) - \prod_{k=1}^n Q_V(v_k) \right\|_{TV} = 0, \quad (29)$$

where the expectation is with respect to the random codebook $\mathcal{B}^{(n)}$.

Lemma 2 (Lemma IV.17 in [5]). For any discrete distribution Q_{UVZ} and $n \geq 1$, let $\mathcal{B}_1^{(n)} = \{U^n(l)\}_{l=1}^{2^{nR_1}}$ and $\mathcal{B}_2^{(n)} = \{V^n(m, l)\}_{m=1}^{2^{nR_2}}$ for $l \in [2^{nR_1}]$ be codebooks of sequences drawn from $\prod_{i=1}^n Q_U$ and $\prod_{i=1}^n Q_{V|U_i(l)}$ respectively. For fixed codebooks, define

$$P(z^n) = 2^{-n(R_1+R_2)} \sum_{l=1}^{2^{nR_1}} \sum_{m=1}^{2^{nR_2}} \prod_{k=1}^n Q_{Z|UV}(z_k|U_k(l), V_k(m, l)). \quad (30)$$

If we have

$$R_1 > I(U; Z), \quad (31)$$

$$R_2 > I(U, V; Z) - H(U), \quad (32)$$

$$R_1 + R_2 > I(U, V; Z), \quad (33)$$

then

$$\lim_{n \to \infty} \mathbb{E} \left\| P(z^n) - \prod_{k=1}^n Q_Z(z_k) \right\|_{TV} = 0, \quad (34)$$

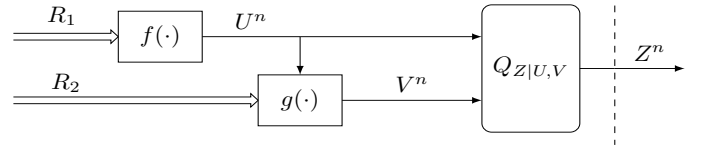where the expectation is with respect to the random codebooks.

Fig. 2. *Two-encoder Example:* Sufficient rates for producing an i.i.d. Z^n sequence in this two encoder system are given in Lemma 2.

B. Existence of Achievability Codes

Assume that (R_0, R_1, R_2) is in the interior of $\mathcal{S}_D$. Then there exists a distribution $Q_{XYZUV} \in D$ such that the rates in (3) are satisfied. For $n \geq 1$, let (K, J_1, J_2) be uniformly distributed on $[2^{nR_0}] \times [2^{n(R_1-R_2)}] \times [2^{nR_2}]$. Application of Lemma 1 with (U, V) in place of U and Lemma 2 with U, V interchanged and $(X, R_2, R_1 - R_2)$ in place of (Z, R_1, R_2) ensures the existence of codebooks $\mathcal{B}^{(n)} = \{U^n(k, j_1, j_2), V^n(k, j_2)\}_{(k, j_1, j_2) \in \mathcal{K} \times \mathcal{J}_1 \times \mathcal{J}_2}$ such that

$$\lim_{n \to \infty} \left\| P(x^n, y^n, z^n) - \prod_{t=1}^n Q(x_t, y_t, z_t) \right\|_{TV} = 0, \quad (35)$$

$$\lim_{n \to \infty} \left\| P(x^n, k) - 2^{-nR_0} \prod_{t=1}^n Q_X(x_t) \right\|_{TV} = 0 \quad (36)$$

respectively, where $P(x^n, y^n, z^n)$ and $P(x^n, k)$ are marginals derived from the joint distribution

$$P(x^n, y^n, z^n, k, j_1, j_2) = 2^{-n(R_0+R_1)} \times \cdots$$
$$\left(\prod_{t=1}^n Q(x_t, y_t|U_t(k, j_1, j_2), V_t(k, j_2)) Q(z_t|V_t(k, j_2)) \right).$$

Note that the Markov chains in place allow the separation of syntheses of Z^n from (X^n, Y^n, U^n), and of X^n from Y^n. The messages that determine the U^n, V^n codewords are compatible with the physical constraints imposed by the cascade structure. By satisfying all the individual demands of the problem, we have indirectly shown the existence of channel synthesis codes. Finally, note that fixing $(j_1, j_2) \in \mathcal{J}_1 \times \mathcal{J}_2$ still leaves us with a sufficient rate of common randomness $R_0 > I(X, Y, Z; U, V)$ for (35) to hold by Lemma 1. Thus, there must exist good codebooks for secure coordination such that

$$\lim_{n \to \infty} \left\| P_{X^n Y^n Z^n J_1 J_2} - 2^{-nR_1} \prod_{t=1}^n Q(x_t, y_t, z_t) \right\|_{TV} = 0.$$

Finally, note that given a secure strong coordination code, redefining (U, V) to be $((U, V), V)$ we see that the corresponding distribution in D' yields the same rates.

C. Comment on Achievability

Our scheme requires local randomization at all nodes - please refer to [5] for a quantitative treatment of local randomness in channel synthesis. Also, observe that while it is intuitive to think of the common randomness as a one-time pad on the messages, we do not need to use such a construction in our proof. On the other hand, it seems desirable to have a more direct achievability scheme for channel synthesis with explicit constructions. Some attempts have been made in this direction[22], [23].

VII. EXTENSIONS

A. Arbitrarily Long Cascades

Our main result of Theorem 1 can be readily extended to secure channel synthesis of a distribution $Q_{Y_1,\ldots,Y_{m-1}|X}$ for a cascade with $m \geq 3$ nodes, with communication rates $R_1, \ldots, R_{m-1}$ on the links of the cascade and common randomness shared by all nodes at rate R_0.

Let $C_k^m \triangleq (C_k, \ldots, C_m)$ for $C \in \{R, U, Y\}$, $1 \leq i \leq m-1$ and $1 \leq j \leq m-2$ below. The optimal rate region is

$$\mathcal{S}_{D_m} \triangleq \left\{ \begin{array}{rcl} R_0^{m-1} \in \mathbb{R}^m & : & \exists P_{X,Y_1^{m-1},U_1^{m-1}} \in D_m \text{ s.t.} \\ R_i & \geq & I(X;U_i^{m-1}) \\ R_0 & \geq & I(X,Y_1^{m-1};U_1^{m-1}) \end{array} \right\}, \quad (37)$$

where

$$D_m \triangleq \left\{ \begin{array}{rcl} P_{X,Y_1^{m-1},U_1^{m-1}} & : & (X,Y_1^{m-1}) \sim Q_X Q_{Y_1^{m-1}|X}, \\ & & X - U_1^{m-1} - Y_1, \\ & & (X,Y_1^j,U_1^j) - U_{j+1}^{m-1} - Y_{j+1}, \\ & & H(U_i^{m-1}|U_i) = 0, \end{array} \right. \quad (38)$$

with the cardinality bounds

$$|\mathcal{U}_i| \leq |\mathcal{X}| \left(\prod_{k=1}^{m-1} |\mathcal{Y}_k|\right) \left(\prod_{k=i+1}^{m-1} |\mathcal{U}_k|\right) + m + i - 2. \quad (39)$$

The proof follows the same steps as the main result, using an appropriate generalization of Lemma 2 to derive the communication rates - namely an application of Lemma 1 followed by repeated applications of [5, Corollary IV.8].

B. No Eavesdropper

The cascade channel synthesis problem with no eavesdropper does not ask that (X^n, Y^n, Z^n) and (J_1, J_2) are independent, but only that

$$\lim_{n \to \infty} \left\| P_{X^n Y^n Z^n} - \prod_{t=1}^n Q(x_t, y_t, z_t) \right\|_{TV} = 0. \quad (40)$$

Note that a good secure channel synthesis code is also a good channel synthesis code[5, Lemma V.1]. For the channel synthesis problem with two nodes, a simple modification of rates for the secure synthesis region is optimal for channel synthesis - namely that the rate constraint on common randomness can be shared by the communication rate as well. In the same spirit, we can replace the constraint on R_0 in (3) with the constraints

$$R_1 + R_0 \geq I(X,Y,Z;U,V) \quad (41)$$

$$R_2 + R_0 \geq I(X,Y,Z;V), \quad (42)$$

which can be shown to be achievable, but not optimal. Consider the case when X is independent of (Y,Z). An application of Lemma 1 implies that the constraint on $(R_2 + R_0)$ alone is sufficient. So let us select $U = \emptyset$ and V independent of X such that $Y - V - Z$. All rate constraints except (41) and (42) vanish so that using $R_2 > 0$ will force us to use $R_1 > 0$ at the optimal rates, since V is a function of U. This region is not optimal. We suspect that another random variable W such that $(X,Y,U) - (V,W) - Z$ and $U - V - W$ might be required in order to convey information about the local randomness used to synthesize Y^n.

REFERENCES

[1] P. Gács and J. Korner, "Common information is far less than mutual information," *Probl. Inform. Control*, vol. 2, no. 2, pp. 149–162, 1973.

[2] A. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theor.*, vol. 21, pp. 163–179, Sept. 2006.

[3] P. Cuff, H. H. Permuter, and T. M. Cover, "Coordination capacity," *IEEE Trans. on Info. Theory*, vol. 56, no. 9, pp. 4181–4206, 2010.

[4] P. Cuff, "Communication requirements for generating correlated random variables," in *ISIT*, pp. 1393–1397, 2008.

[5] P. Cuff, "Distributed channel synthesis," *CoRR*, vol. abs/1208.4415, 2012.

[6] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, "Quantum reverse shannon theorem," Tech. Rep. arXiv:0912.5537, Dec 2009.

[7] A. Gohari and V. Anantharam, "Generating dependent random variables over networks," in *ITW*, pp. 698 –702, Oct. 2011.

[8] A. Gohari, M. H. Yassaee, and M. R. Aref, "Secure channel simulation," *CoRR*, vol. abs/1207.3513, 2012.

[9] M. H. Yassaee, A. Gohari, and M. R. Aref, "Channel simulation via interactive communications," in *ISIT*, pp. 3053–3057, 2012.

[10] F. Haddadpour, M. H. Yassaee, A. Gohari, and M. R. Aref, "Coordination via a relay," in *ISIT*, pp. 3048–3052, 2012.

[11] A. Winter, "Compression of sources of probability distributions and density operators," *eprint arXiv:quant-ph/0208131*, Aug. 2002.

[12] T. M. Cover and H. H. Permuter, "Capacity of coordinated actions," in *ISIT*, pp. 2701 –2705, June 2007.

[13] T. M. Cover and J. A. Thomas, *Elements of information theory (2. ed.)*. Wiley, 2006.

[14] P. Cuff, "A framework for partial secrecy," in *GLOBECOM*, pp. 1–5, 2010.

[15] P. Cuff, "Using a secret key to foil an eavesdropper," in *Allerton*, pp. 1405 –1411, 29 2010-oct. 1 2010.

[16] A. Winter, "Secret, public and quantum correlation cost of triples of random variables," in *ISIT 2005*, pp. 2270–2274, 2005.

[17] P. Cuff, "State information in bayesian games," in *Allerton*, 2009.

[18] M. Bloch and J. N. Laneman, "Secrecy from resolvability," *CoRR*, vol. abs/1105.5419, 2011.

[19] R. Murray, K. Astrom, S. Boyd, R. Brockett, and G. Stein, "Future directions in control in an information-rich world," *Control Systems, IEEE*, vol. 23, pp. 20 – 33, apr 2003.

[20] W. Liu, G. Xu, and B. Chen, "The common info. of n dependent random variables," *CoRR*, vol. abs/1010.3613, 2010.

[21] T. Han and S. Verdu, "Approximation theory of output statistics," *Info. Theory, IEEE Trans. on*, vol. 39, pp. 752 –772, may 1993.

[22] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *CoRR*, vol. abs/1203.0730, 2012.

[23] M. R. Bloch, L. Luzzi, and J. Kliewer, "Strong coordination with polar codes," *CoRR*, vol. abs/1210.2159, 2012.