Common Information of Random Linear Network Coding Over A 1-Hop Broadcast Packet Erasure Channel

Chih-Chun Wang, Jaemin Han; {chihw, han83}@purdue.edu
Center of Wireless Systems and Applications (CWSA)
School of Electrical and Computer Engineering, Purdue University, USA

***Abstract*—Random linear network coding (RLNC) is widely used in practical network coding (NC) protocol design. Recent results show that RLNC also plays an important role in capacity-achieving *intersession NC* schemes for erasure-based 1-hop relay networks. This work quantifies the *common information* of RLNC over a 1-hop broadcast packet erasure channel. Several potential applications are discussed, including source coding, intersession NC, and broadcasting with common and private information.**

I. Problem Formulation

For any positive integer K, we define $[K] \triangleq \{1, \cdots, K\}$ and use $2^{[K]}$ to denote the collection of all subsets of $[K]$. We consider a 1-hop wireless broadcast channel with a single source s and multiple destinations d_k, $k \in [K]$. Source s has N information packets to transmit, denoted by a row vector $\mathbf{W} \triangleq (W_1, \cdots, W_N) \in (\mathsf{GF}(q))^N$. Random linear network coding (RLNC) [6] is used. That is, for each time slot t, source s sends a packet $Y_t = \mathbf{v}_t \mathbf{W}^{\mathrm{T}}$ through a broadcast erasure channel, where $\mathbf{v}_t$ is an N-dimensional row vector chosen independently and uniformly randomly from $(\mathsf{GF}(q))^N$. We assume that $\{\mathbf{v}_t : \forall t\}$ are known to all destinations d_k. This can be achieved either by generating $\{\mathbf{v}_t : \forall t\}$ via a pseudo random number generator with a common seed; or by the generation-based construction in [3].

In the end of time t, destination d_k either receives an erasure $Z_{k,t} = *$ or the transmitted packet $Z_{k,t} = Y_t$. We assume whether the packet is erased or not is independent of $\mathbf{W}$ and $\{Y_t : \forall t\}$. We use $\mathbf{Z}_k \triangleq \{Z_{k,t} : \forall t\}$ to denote what d_k has received/observed. For any t, we use $\mathcal{R}_t \in 2^{[K]}$ to denote the set of destinations that successfully receive Y_t. Define

$$\Omega_k \triangleq \mathsf{span}(\mathbf{v}_t : \forall t \text{ satisfying } k \in \mathcal{R}_t)$$

as the linear span of all vectors corresponding to the packets successfully received by d_k. The information available at d_k can now be characterized by the linear space Ω_k, and one can quickly verify that the mutual information $I(\mathbf{W}; \mathbf{Z}_k) = \mathrm{Rank}(\Omega_k)$, assuming the logarithm in $I(\cdot, \cdot)$ is of base q.

Some other notations are also useful for our discussion. For any two linear spaces A and B, we define the *sum space* $A \oplus B \triangleq \mathsf{span}(\mathbf{v} : \forall \mathbf{v} \in A \cup B)$. For any $S \in 2^{[K]}$, define

$$\pi_S \triangleq |\{t : \forall t \text{ satisfying } S \subseteq \mathcal{R}_t\}|$$

as the number of packets successfully received by all $d_k \in S$ (but may or may not be received by any $d_i \notin S$). For simplicity, we often use π_k as shorthand for $\pi_{\{k\}}$. The classic results of RLNC [6] prove that when a sufficiently large $\mathsf{GF}(q)$ is used, with close-to-one probability we must have

$$\mathrm{Rank}(\Omega_k) = \min(N, \pi_k). \quad (1)$$

Since Ω_k is the *information space* at d_k, the *common information* among d_1 to d_K can be expressed as the intersection $\bigcap_{k\in[K]} \Omega_k$. The question we would like to answer is

Given the receiving status $\{\mathcal{R}_t : \forall t\}$ of a RLNC scheme, what is the value of $\mathrm{Rank}\left(\bigcap_{k\in[K]} \Omega_k\right)$ when a sufficiently large $\mathsf{GF}(q)$ is used?

Remark 1: For $K = 2$, one can easily prove that

$$\begin{aligned}&\mathrm{Rank}(\Omega_1 \cap \Omega_2)\\ &= \mathrm{Rank}(\Omega_1) + \mathrm{Rank}(\Omega_2) - \mathrm{Rank}(\Omega_1 \oplus \Omega_2)\\ &= \min(N, \pi_1) + \min(N, \pi_2) - \min(N, \pi_1 + \pi_2 - \pi_{\{1,2\}}).\end{aligned} \quad (2)$$

The case of $K \geq 3$ quickly becomes non-trivial and cannot be derived by iteratively applying (2). One reason is that although the cardinality equality $|(S_1 \cap S_2) \cup S_3| = |(S_1 \cup S_3) \cap (S_2 \cup S_3)|$ holds for arbitrary sets S_1 to S_3, when focusing on ranks and sum spaces, we may have $\mathrm{Rank}((\Omega_1 \cap \Omega_2) \oplus \Omega_3)$ being strictly smaller than $\mathrm{Rank}((\Omega_1 \oplus \Omega_3) \cap (\Omega_2 \oplus \Omega_3))$. As a result, one cannot derive the results for $K \geq 3$ by iteratively applying (2), and the expression of $\mathrm{Rank}\left(\bigcap_{k\in[K]} \Omega_k\right)$ no longer admits the inclusion-exclusion form as in the simplest case of $K = 2$.

Remark 2: [6] proves that if $\min_{k\in[K]} \pi_k \geq N$, then $\mathrm{Rank}\left(\bigcap_{k\in[K]} \Omega_k\right) = N$, i.e., *all destinations* can decode *all packets*. This paper explores the *transient behavior* of RLNC (in terms of $\mathrm{Rank}\left(\bigcap_{k\in[K]} \Omega_k\right)$) when individual d_k has not received enough packets (when $\min_{k\in[K]} \pi_k < N$).

Remark 3: We deliberately choose not to specify the total number of time slots used in transmission so that our setting is compatible to that of the *rate-less codes* [1]. For readers interested in fixed-length codes over i.i.d. broadcast erasure channels [12], [13], one can view $\pi_S = n \prod_{k\in S} p_k$, where n is the total number of time slots and p_k is the marginal success probability that d_k receives a transmission.

II. Connections to Other Areas/Applications

RLNC is widely used in system-level research due to its distributed nature [2], [9] and optimal performance for *single*

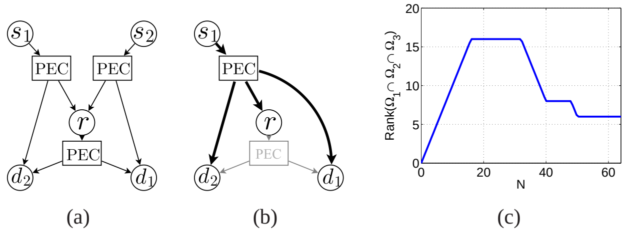

Fig. 1. (a) A 1-hop relay network without 2-hop transmission. (b) Allowing direct overhearing at d_k. (c) An illustration of $\mathrm{Rank}(\Omega_1 \cap \Omega_2 \cap \Omega_3)$ vs. N.

multicast [10]. Studying the *common information* of RLNC will deepen our understanding and have impact on both the information theory and the networking societies. In the following, we highlight three such connections to other areas.

1) Gács-Körner Common Information: In [5], [7], the Gács-Körner common information (GKCI) between two random variables (RVs) X and Y is defined as the supremum of the entropy $H(V)$ over all RVs V, taking values in some finite set $\mathcal{V}$, that can be written as $V = f(X) = g(Y)$ for some functions $f(\cdot)$ and $g(\cdot)$. The GKCI can also be generalized[1] for K random variables X_1 to X_K by finding the supremum of $H(V)$ for all $V = f_1(X_1) = \cdots = f_K(X_K)$. In our RLNC setting, the GKCI among $\mathbf{Z}_1$ to $\mathbf{Z}_K$ is indeed quantified by $\mathrm{Rank}\left(\bigcap_{k\in[K]} \Omega_k\right)$. Some relationships of the GKCI to other source coding problems can be found in [7].

2) Broadcast With Private And Common Messages: Under a wireline setting, [4] derives the capacity when a single source s would like to send two private messages to d_1 and d_2 with rates R_1 and R_2, respectively, and send one common message to both d_1 and d_2 with rate R_0. [4] proves that (R_0, R_1, R_2) is achievable if there exists an N such that the corresponding RLNC-based information spaces Ω_k, $k = 1, 2$, satisfy

$$\begin{cases} R_1 = \tilde{R}_1 + \hat{R}_1, \quad R_2 = \tilde{R}_2 + \hat{R}_2 \\ R_0 + \tilde{R}_1 + \tilde{R}_2 = \mathrm{Rank}(\Omega_1 \cap \Omega_2) \\ \hat{R}_1 \leq \mathrm{Rank}(\Omega_1) - \mathrm{Rank}(\Omega_1 \cap \Omega_2) \\ \hat{R}_2 \leq \mathrm{Rank}(\Omega_2) - \mathrm{Rank}(\Omega_1 \cap \Omega_2) \end{cases} \tag{3}$$

for some rate vector $(\tilde{R}_1, \hat{R}_1, \tilde{R}_2, \hat{R}_2)$. The interpretation of (3) is straightforward: we first break the rate R_k into two sub-rates $\tilde{R}_k$ and $\hat{R}_k$ for $k = 1, 2$. The sub-rates $\tilde{R}_1$, $\tilde{R}_2$, and the common message rate R_0 are then communicated to both d_1 and d_2 through the *common information* of RLNC. For each k, the sub-rate $\hat{R}_k$ is communicated to d_k through the information space Ω_k that is not in the common information space $\Omega_1 \cap \Omega_2$, and is thus upper bounded by the difference of the ranks. Combining the expressions in (1) and (2), [4] further proves that the achievable region (3) is indeed the capacity.

A natural question is whether we can extend the above RLNC-based results for $K \geq 3$. Characterizing the corresponding performance requires quantifying the common information $\mathrm{Rank}\left(\bigcap_{k\in[K]} \Omega_k\right)$ for arbitrary K values.

3) Combination of Intersession Network Coding And Opportunistic Routing: Consider a wireless relay network in Fig. 1(a) with two source-destination pairs (s_1, d_1) and (s_2, d_2) and a relay r interconnected by broadcast packet erasure channels (PECs), which models the widely-studied *intersession network coding (INC)* protocol in [8]. Recently the capacity of Fig. 1(a) has been characterized under a *1-time-reception-report setting* [13]. In the capacity-achieving scheme of [13] each s_i simply performs RLNC that broadcasts packets to r and the other destination d_j, $j \neq i$. The relay r later intelligently mixes the s_1-packets overheard by d_2 and the s_2-packets overheard by d_1, which achieves the capacity.

On the other hand, in practice, a packet transmission may be heard directly by its 2-hop neighbors. The *opportunistic routing* scheme in [2] shows that by exploiting this observation alone (without INC), one can substantially enhance the throughput. An interesting question is thus how much throughput enhancement one can achieve when combining both INC and opportunistic routing. For example, Fig. 1(b) illustrates the scenario in which a packet sent by s_1 may be overheard by d_1. Assume RLNC is used by s_1, and let Ω_r, Ω_{d_1}, and Ω_{d_2} denote the *information spaces* received by r, d_1, and d_2, respectively. Then relay r needs to transmit additional

$$\mathrm{Rank}(\Omega_r) - \mathrm{Rank}(\Omega_r \cap \Omega_{d_1}) \tag{4}$$

packets to d_1, where the first term quantifies the overall information at r, and the second term quantifies the corresponding (sub-) information already known at d_1. By similar reasonings,

$$\mathrm{Rank}(\Omega_r \cap \Omega_{d_2}) - \mathrm{Rank}((\Omega_r \cap \Omega_{d_2}) \cap \Omega_{d_1}) \tag{5}$$

corresponds to the amount of information possessed by r and also overheard by d_2 while being beneficial to d_1. Since (5) describes how many s_1-packets at r are overheard by d_2 and can later be mixed with the s_2-packets overheard by d_1, the INC performance depends on the values of (4) and (5). See [12], [13] for detailed discussion. The common information $\mathrm{Rank}\left(\bigcap_{k\in S} \Omega_k\right)$ is thus critical to the throughput analysis when combining INC and opportunistic routing.

III. Main Results for $K \geq 3$

For any $S \in 2^{[K]}$, we say a collection of subsets $\{S_1, S_2, \cdots, S_M\}$ is a partition of S if $S_m \neq \emptyset$ for all $m \in [M]$, $S_i \cap S_j = \emptyset$ for all $i \neq j$, and $\bigcup_{m=1}^{M} S_m = S$. We use $\{S_m\}$ as shorthand for a partition $\{S_1, S_2, \cdots, S_M\}$. For any N, we define a function $f_N : 2^{[K]} \mapsto \mathbb{R}^+$

$$f_N(S) \triangleq \max\left\{ N - \sum_{m=1}^{M} (N - \pi_{S_m})^+ : \forall \text{ partition } \{S_m\} \right\}, \tag{6}$$

where $(\cdot)^+ = \max(0, \cdot)$ is the projection to non-negative reals.

Proposition 1: Assume RLNC on a finite field $\mathsf{GF}(q)$. For any given receiving sets $\{\mathcal{R}_t : \forall t\}$ and the corresponding $\{\pi_T : \forall T \in 2^{[K]}\}$, we have

$$\lim_{q\to\infty} \mathsf{Prob}\left(\mathrm{Rank}\left(\bigcap_{\forall i\in S} \Omega_i \right) = f_N(S) \right) = 1.$$

Example: When $S = \{1\}$, there is only one partition $\{\{1\}\}$. $\mathrm{Rank}(\Omega_1)$ is thus $f_N(\{1\}) = N - (N - \pi_1)^+ = \min(\pi_1, N)$

[1]Other common information metrics for K RVs can be found in [11].

as predicted in (1). When $S=\{1,2\}$, there are two partitions $\{\{1,2\}\}$ and $\{\{1\},\{2\}\}$. The rank of $\Omega_1\cap\Omega_2$ is thus

$$f_N(\{1,2\})=\max\left(N-(N-\pi_1)^+-(N-\pi_2)^+,\right.\\ \left. N-(N-\pi_{\{1,2\}})^+\right).$$

By simple arithmetics, one can prove that $f_N(\{1,2\})$ is equivalent to (2). Note that for any fixed S, $f_N(S)$ depends on the value of N. Fig. 1(c) plots $f_N(S)$ versus N when $S=\{1,2,3\}$ for some fixed receiving status $\{\mathcal{R}_t:\forall t\}$. As can be seen, the resulting curve is neither concave nor convex.

IV. Outlines of The Proof of Proposition 1

The proof of Proposition 1 is outlined in this section. The detailed proofs are omitted due to the space limit.

Step 0.1: Conversion to a simpler setting. For any given $S\in 2^{[K]}$, N, receiving sets $\{\mathcal{R}_t:\forall t\}$, and the corresponding $\{\pi_T:\forall T\in 2^{[K]}\}$, consider the following two inequalities:

$$N\geq\max_{\forall i\in S}\pi_i \tag{7}$$

$$\forall S_0\subseteq S, S_0\neq S,\quad \left(\sum_{\forall i\in S_0}\pi_i\right)-(|S_0|-1)N\geq\pi_{S_0}. \tag{8}$$

Lemma 1: If both (7) and (8) are satisfied, then $f_N(S)$ in (6) can be rewritten as

$$f_N(S)=\max\left(\left(\sum_{\forall i\in S}\pi_i\right)-(|S|-1)N,\pi_S\right). \tag{9}$$

Lemma 2: Fix S and N. Consider any receiving sets $\{\mathcal{R}_t:\forall t\}$, which may not satisfy (7) and (8). We can always construct a new RLNC system with $\check{K}$ destinations such that the corresponding $\check{S}\in 2^{[\check{K}]}$, $\{\check{\mathcal{R}}_t:\forall t\}$, and $\{\check{\pi}_T:\forall T\in 2^{[\check{K}]}\}$ satisfy (7) and (8) for the original N and the new $\check{S}$; and simultaneously the following two equalities are satisfied

$$f_N(S)=\check{f}_N(\check{S}) \tag{10}$$

$$\lim_{q\to\infty}\mathsf{Prob}\left(\mathrm{Rank}\left(\bigcap_{\forall k\in S}\Omega_k\right)=\mathrm{Rank}\left(\bigcap_{\forall k\in\check{S}}\check{\Omega}_k\right)\right)=1, \tag{11}$$

where $\{\Omega_k\}$ (resp. $\{\check{\Omega}_k\}$) are the information spaces of RLNC according to the receiving sets $\{\mathcal{R}_t:\forall t\}$ (resp. $\{\check{\mathcal{R}}_t:\forall t\}$). $f_N(\cdot)$ and $\check{f}_N(\cdot)$ are the function (6) evaluated corresponding to $\{\mathcal{R}_t:\forall t\}$ and $\{\check{\mathcal{R}}_t:\forall t\}$, respectively.

Combining Lemmas 1 and 2, we thus only need to prove that when both (7) and (8) are satisfied, $\mathrm{Rank}\left(\bigcap_{k\in S}\Omega_k\right)$ can be computed by (9). In our proof, we also use the induction assumption that $\mathrm{Rank}\left(\bigcap_{k\in S'}\Omega_k\right)$ can be computed by (6) for any S' satisfying $|S'|<|S|$.

Step 0.2: Generalized linear network coding theorem for the intersection of spaces. We now introduce a lemma and a proposition that will be the theoretic foundation of Step 1.

Fix any N_1, N_2, and N that satisfy $\max(N_1,N_2)\leq N$ and $N_1+N_2\geq N$. For any $i\in[N_1]$, consider $2N$ multi-variable polynomials $g^{[1]}_{i,n}(\mathbf{x})$ and $h^{[1]}_{i,n}(\mathbf{x})$ for all $n\in[N]$ where $\mathbf{x}$ is the finite collection of input variables, each taking values in $\mathsf{GF}(q)$. For those $\mathbf{x}$ values such that $h^{[1]}_{i,n}(\mathbf{x})\neq 0$ for all $i\in[N_1]$ and $n\in[N]$, we can construct N_1 row vectors

$$\mathbf{w}^{[1]}_i(\mathbf{x})\triangleq\left(\frac{g^{[1]}_{i,1}(\mathbf{x})}{h^{[1]}_{i,1}(\mathbf{x})},\frac{g^{[1]}_{i,2}(\mathbf{x})}{h^{[1]}_{i,2}(\mathbf{x})},\cdots,\frac{g^{[1]}_{i,N}(\mathbf{x})}{h^{[1]}_{i,N}(\mathbf{x})}\right),\ \forall i\in[N_1].$$

Similarly, for any $j\in[N_2]$, consider $2N$ multi-variable polynomials $g^{[2]}_{j,n}(\mathbf{x})$ and $h^{[2]}_{j,n}(\mathbf{x})$ for all $n\in[N]$. For those $\mathbf{x}$ values such that $h^{[2]}_{j,n}(\mathbf{x})\neq 0$ for all $j\in[N_2]$ and $n\in[N]$, we can construct N_2 row vectors

$$\mathbf{w}^{[2]}_j(\mathbf{x})\triangleq\left(\frac{g^{[2]}_{j,1}(\mathbf{x})}{h^{[2]}_{j,1}(\mathbf{x})},\frac{g^{[2]}_{j,2}(\mathbf{x})}{h^{[2]}_{j,2}(\mathbf{x})},\cdots,\frac{g^{[2]}_{j,N}(\mathbf{x})}{h^{[2]}_{j,N}(\mathbf{x})}\right),\ \forall j\in[N_2].$$

We then have the following results.

Lemma 3: Let $\mathcal{A}$ denote the collection of all $\mathbf{x}$ values satisfying $\prod_{i\in[N_1]}\prod_{n\in[N]}h^{[1]}_{i,n}(\mathbf{x})\neq 0$ and

$$\mathrm{Rank}(\mathsf{span}(\mathbf{w}^{[1]}_i(\mathbf{x}):\forall i\in[N_1]))=N_1.$$

If $\mathcal{A}$ is non-empty, then when we choose each coordinate of $\mathbf{x}$ independently and uniformly randomly from $\mathsf{GF}(q)$, we have

$$\lim_{q\to\infty}\mathsf{Prob}(\mathbf{x}\in\mathcal{A})=1. \tag{12}$$

Lemma 3 is a simple extension of the RLNC results in [6].

Some further notation is needed before describing the next proposition. For any $(\tilde{N}_1,\tilde{N}_2)$ satisfying $\tilde{N}_1+\tilde{N}_2=N$ and $\tilde{N}_k\leq N_k$ for all $k\in\{1,2\}$, we use $\mathcal{B}_{\tilde{N}_1,\tilde{N}_2}$ to denote the collection of all $\mathbf{x}$ values satisfying

$$\prod_{\forall i\in[N_1]}\prod_{\forall j\in[N_2]}\prod_{\forall n\in[N]}h^{[1]}_{i,n}(\mathbf{x})h^{[2]}_{j,n}(\mathbf{x})\neq 0,\quad\text{and}$$

$$\mathrm{Rank}(\mathsf{span}(\mathbf{w}^{[1]}_i(\mathbf{x}),\mathbf{w}^{[2]}_j(\mathbf{x}):\forall i\in[\tilde{N}_1],\forall j\in[\tilde{N}_2]))=N. \tag{13}$$

For any $\mathbf{x}\in\mathcal{B}_{\tilde{N}_1,\tilde{N}_2}$ we define the "marginal spaces" by

$$\Omega^{[1]}(\mathbf{x})=\mathsf{span}(\mathbf{w}^{[1]}_i(\mathbf{x}):\forall i\in[N_1])$$
$$\Omega^{[2]}(\mathbf{x})=\mathsf{span}(\mathbf{w}^{[2]}_j(\mathbf{x}):\forall j\in[N_2]).$$

Proposition 2: Suppose $\mathcal{B}_{\tilde{N}_1,\tilde{N}_2}$ is not empty. For any given $\mathbf{x}_0\in\mathcal{B}_{\tilde{N}_1,\tilde{N}_2}$ and any fixed vector $\mathbf{w}_0\in\Omega^{[1]}(\mathbf{x}_0)\cap\Omega^{[2]}(\mathbf{x}_0)$, we can construct $2N$ polynomials $g_n(\mathbf{x})$ and $h_n(\mathbf{x})$ for all $n\in[N]$, such that for all $\mathbf{x}\in\mathcal{B}_{\tilde{N}_1,\tilde{N}_2}$, we have

$$\begin{cases}\prod_{n\in[N]}h_n(\mathbf{x})\neq 0\\ \mathbf{w}(\mathbf{x})\triangleq\left(\frac{g_1(\mathbf{x})}{h_1(\mathbf{x})},\cdots,\frac{g_N(\mathbf{x})}{h_N(\mathbf{x})}\right)\in\Omega^{[1]}(\mathbf{x})\cap\Omega^{[2]}(\mathbf{x})\\ \mathbf{w}_0=\mathbf{w}(\mathbf{x}_0)\end{cases}.$$

Step 1: Characterizing a *typical solution* of RLNC-based spaces through a merging process. The preliminary Step 0.1 ensures that we can focus only on those $\{\mathcal{R}_t:\forall t\}$ satisfying (7) and (8). Given such $\{\mathcal{R}_t:\forall t\}$, the goal in this step is to find a fixed, deterministic coding vector assignment $\{\mathring{\mathbf{v}}_t:\forall t\}$ that satisfies some "typicality" conditions such that with close-to-one probability, a randomly constructed $\{\mathbf{v}_t:\forall t\}$ will have the same "rank" property as that of the deterministic $\{\mathring{\mathbf{v}}_t:\forall t\}$.

Consider $S=[K]$. In addition to (7) and (8), we further assume (8) is satisfied even for $S_0=S$. We call it the (8+)

condition, which will be relaxed later. We will construct a fixed coding vector assignment $\{\mathring{\mathbf{v}}_t\colon \forall t\}$ satisfying the following. Define $\mathring{\Omega}_k$ as the information space at d_k generated by $\{\mathring{\mathbf{v}}_t\colon \forall t\}$. The typicality conditions to be satisfied are

$$\forall k \in [K-1],\ \text{Rank}\left(\bigcap_{i=1}^{k} \mathring{\Omega}_i\right) = f_N(\{1,\cdots,k\}), \quad (14)$$

$$\forall k \in [K-1],\ \text{Rank}\left(\left(\bigcap_{i=1}^{k} \mathring{\Omega}_i\right) \oplus \mathring{\Omega}_{k+1}\right) = N. \quad (15)$$

To see why (14) and (15) characterize typicality, consider the following merging process from $k=1$ to $k=K-1$. When $k=1$, (14) guarantees $\text{Rank}(\mathring{\Omega}_1) = f_N(\{1\}) = \pi_1$, which is indeed a typical rank value for a RLNC scheme (see (7)).

Consider the case $k=k_0$ sequentially for $k_0 = 2,\cdots,K-1$. With $k=k_0$, by (14) we can construct $f_N([k_0])$ linearly independent coding vectors from $\left(\bigcap_{i\in[k_0]} \mathring{\Omega}_i\right)$. Note that with $k=k_0-1$, (15) guarantees that $\left(\bigcap_{i\in[k_0-1]} \mathring{\Omega}_i\right)$ and $\mathring{\Omega}_{k_0}$ satisfy (13). *Therefore, Proposition 2 ensures that we can express the above deterministic $f_N([k_0])$ coding vectors as* fractions of polynomials *with the input variables being the choices of the RLNC vectors* $\{\mathbf{v}_t : \forall t\}$. Then we can use Lemma 3 (with $N_1 = f_N([k_0])$) to prove that even when we randomly choose $\{\mathbf{v}_t : \forall t\}$, the random $f_N([k_0])$ coding vectors, computed from the fractions of polynomials, are linearly independent with close-to-one probability. By the construction in Proposition 2, these $f_N([k_0])$ coding vectors are in $\left(\bigcap_{i\in[k_0-1]} \Omega_i\right) \cap \Omega_{k_0}$ with close-to-one probability.

By the induction assumption for all S' with $|S'| < |S| = K$ discussed in the end of Step 0.1, we also know that with close-to-one probability, we can have at most $f_N([k_0])$ linearly independent coding vectors from $\left(\bigcap_{i\in[k_0]} \Omega_i\right)$. *As a result, the deterministic $f_N([k_0])$ linearly independent coding vectors from $\left(\bigcap_{i\in[k_0]} \mathring{\Omega}_i\right)$ and the corresponding expressions based on fractions of polynomials are a typical solution of the basis vectors of the intersection $\bigcap_{k\in[k_0]} \Omega_k$ of a RLNC scheme.*

The final construction is to notice that

$$\begin{aligned}\text{Rank}\left(\bigcap_{\forall i\in[K]} \Omega_i\right) =&\text{Rank}\left(\bigcap_{\forall i\in[K-1]} \Omega_i\right) + \text{Rank}\left(\Omega_K\right)\\ &- \text{Rank}\left(\left(\bigcap_{\forall i\in[K-1]} \Omega_i\right) \oplus \Omega_K\right)\\ \overset{\text{typically}}{=}&\text{Rank}\left(\bigcap_{\forall i\in[K-1]} \mathring{\Omega}_i\right) + \text{Rank}\left(\mathring{\Omega}_K\right)\\ &- \text{Rank}\left(\left(\bigcap_{\forall i\in[K-1]} \mathring{\Omega}_i\right) \oplus \mathring{\Omega}_K\right) \quad (16)\\ =&f_N([K-1]) + f_N(\{K\}) - N = f_N([K]) \quad (17)\end{aligned}$$

where (16) follows from Lemma 3 and our aforementioned typicality arguments; the first equality of (17) follows from (14) and (15); and the last equality of (17) follows from (7), (8+), and Lemma 1.

Step 2: Explicitly constructing a typical solution. Given $\{\mathcal{R}_t : \forall t\}$ satisfying (7) and (8+), Step 1 converts the problem of quantifying $\text{Rank}\left(\bigcap_{i\in[K]} \Omega_i\right)$ of randomly assigned $\{\mathbf{v}_t : \forall t\}$ to that of finding one deterministic assignment $\{\mathring{\mathbf{v}}_t\colon \forall t\}$ satisfying (14) and (15). To solve the latter, we provide a *structured random construction* of $\{\mathring{\mathbf{v}}_t\colon \forall t\}$ that satisfies (14) and (15) with close-to-one probability.

Assume that (7) and (8+) hold. Consider $(K+1)$ integer values $u_{[K]}$, $u_{[K]\backslash 1}$, $u_{[K]\backslash 2}, \cdots, u_{[K]\backslash K}$ defined by

$$u_{[K]} \triangleq \left(\sum_{\forall k\in[K]} \pi_k\right) - (K-1)N$$
$$\forall k \in [K], \quad u_{[K]\backslash k} \triangleq N - \pi_k.$$

By (7) and (8+), all u values are non-negative and $u_{[K]} + \sum_{\forall k\in[K]} u_{[K]\backslash k} = N$. We use δ_1 to δ_N to represent N elementary basis vectors of $(\mathsf{GF}(q))^N$ such that each δ_n is an N-dimensional row vector with the n-th coordinate being 1 and all other coordinates being 0. Construct $(K+1)$ matrices $\mathbf{U}_{[K]}$, $\mathbf{U}_{[K]\backslash 1}$, $\mathbf{U}_{[K]\backslash 2}, \cdots, \mathbf{U}_{[K]\backslash K}$ as follows. $\mathbf{U}_{[K]}$ is a $u_{[K]} \times N$ matrix constructed by vertically concatenating the first $u_{[K]}$ basis vectors δ_1 to $\delta_{u_{[K]}}$. For each k, $\mathbf{U}_{[K]\backslash k}$ is a $u_{[K]\backslash k} \times N$ matrix constructed by vertically concatenating the next $u_{[K]\backslash k}$ basis vectors δ_n, $n \in \left\{u_{[K]} + \sum_{i=1}^{k-1} u_{[K]\backslash i} + 1, \cdots, u_{[K]} + \sum_{i=1}^{k} u_{[K]\backslash i}\right\}$.

For any $T \in 2^{[K]}$, consider all the packets that are received *by and only by* the users in T. We slightly abuse the notation and use $\pi_{T\overline{[K]\backslash T}}$ to denote the number of such packets. Let $\mathbf{V}_T$ denote a $\pi_{T\overline{[K]\backslash T}} \times N$ matrix that contains all $\mathbf{v}_t$ vectors satisfying $\mathcal{R}_t = T$. We construct a specific $\mathring{\mathbf{V}}_T$ by

$$\mathring{\mathbf{V}}_T = \Gamma_{[K];T}\mathbf{U}_{[K]} + \sum_{\forall i: i\notin T} \Gamma_{[K]\backslash i;T}\mathbf{U}_{[K]\backslash i}, \quad (18)$$

where $\Gamma_{[K];T}$ (resp. $\Gamma_{[K]\backslash i;T}$) is a $\pi_{T\overline{[K]\backslash T}} \times u_{[K]}$ (resp. $\pi_{T\overline{[K]\backslash T}} \times u_{[K]\backslash i}$) mixing matrix for which each entry is chosen independently and uniformly from $\mathsf{GF}(q)$. Repeat the above construction for all $T \in 2^{[K]}$ and we have constructed a coding vector assignment $\{\mathring{\mathbf{v}}_t\colon \forall t\}$.

The following lemma characterizes the typical behavior of the above random construction and implies the existence of one deterministic $\{\mathring{\mathbf{v}}_t\colon \forall t\}$ satisfying (14) and (15).

Lemma 4: For sufficiently large $\mathsf{GF}(q)$, the following three events hold with close-to-one probability for any $k \in [K-1]$:

(i) $$\text{Rank}\left(\bigcap_{i\in[k]} \mathring{\Omega}_i\right) = f_N([k]) = \left(\sum_{i\in[k]} \pi_i\right) - (k-1)N;$$

(ii) The elementary basis vectors contained in $\mathbf{U}_{[K]}$, $\mathbf{U}_{[K]\backslash(k+1)}$, $\mathbf{U}_{[K]\backslash(k+2)}$ to $\mathbf{U}_{[K]\backslash K}$ are also the basis vectors of $\left(\bigcap_{i\in[k]} \mathring{\Omega}_i\right)$; and

(iii) $$\text{Rank}\left(\left(\bigcap_{i\in[k]} \mathring{\Omega}_i\right) \oplus \mathring{\Omega}_{k+1}\right) = N.$$

Remark: Our structured random construction of $\{\mathring{\mathbf{v}}_t\colon \forall t\}$ has delicate structures (18) that are quite different from the uniformly random construction of $\{\mathbf{v}_t : \forall t\}$. The readers may think why not use a uniformly random construction for $\{\mathring{\mathbf{v}}_t : \forall t\}$. The reason is that if we use a uniformly random construction, then proving "$\{\mathring{\mathbf{v}}_t : \forall t\}$ satisfies (15) with $k = (K-1)$" is no easier than directly proving Proposition 1 for $\{\mathbf{v}_t : \forall t\}$, which becomes a tautology. In contrast, our structured random construction enables a clean proof for the existence of $\{\mathring{\mathbf{v}}_t\colon \forall t\}$ satisfying (14) and (15), which circumvents the difficulty of directly proving Proposition 1.

Step 3: Relaxing the condition (8+). In this following, we let $S = [K]$ and discuss how to relax condition (8+) back to condition (8). Assume the receiving sets $\{\mathcal{R}_t : \forall t\}$ satisfy (7) and (8) but not (8+). It thus means that

$$\Delta \stackrel{\Delta}{=} \pi_{[K]} - \left(\left(\sum_{\forall i\in[K]} \pi_i\right) - (K-1)N\right) > 0$$

Since (8) is satisfied, we also have

$$\begin{aligned}\pi_K + \Delta &= \pi_{[K]} - \left(\left(\sum_{\forall i\in[K-1]} \pi_i\right) - (K-2)N\right) + N \\ &\leq \pi_{[K-1]} - \left(\left(\sum_{\forall i\in[K-1]} \pi_i\right) - (K-2)N\right) + N \leq N.\end{aligned}$$

We temporarily let destination d_K hear additional Δ new coded packets $\mathbf{u}_1\mathbf{W}^{\mathrm{T}}$ to $\mathbf{u}_\Delta\mathbf{W}^{\mathrm{T}}$, where each coordinate of $\mathbf{u}_i$ is chosen independently and uniformly from $\mathsf{GF}(q)$. After d_K receiving additional Δ new packets, we have a new $\pi'_K = \pi_K + \Delta$ and all other π_T remain unchanged for all $T \neq \{K\}$. Since both (7) and (8+) are now satisfied, our previous proof shows that

$$\lim_{q\to\infty} \mathsf{Prob}\left(\mathrm{Rank}\left(\left(\bigcap_{i=1}^{K-1}\Omega_i\right)\oplus\Omega'_K\right) = N\right) = 1$$

where Ω'_K is the new space generated by the original packets and the new extra packets. Since we add Δ new packets, for the original space Ω_K we must have

$$\mathrm{Rank}\left(\left(\bigcap_{i=1}^{K-1}\Omega_i\right)\oplus\Omega_K\right) \geq N - \Delta \tag{19}$$

with close-to-one probability. Therefore

$$\begin{aligned}\mathrm{Rank}\left(\bigcap_{i=1}^{K}\Omega_i\right) &= \mathrm{Rank}\left(\bigcap_{i=1}^{K-1}\Omega_i\right) + \mathrm{Rank}(\Omega_K) \\ &\quad -\mathrm{Rank}\left(\left(\bigcap_{i=1}^{K-1}\Omega_i\right)\oplus\Omega_K\right) \\ &\leq \left(\left(\sum_{i=1}^{K-1}\pi_i\right) - (K-2)N\right) + \pi_K - (N-\Delta) \qquad (20) \\ &= \pi_{[K]}\end{aligned}$$

with close-to-one probability, where (20) follows from the induction assumption and from (19). By the classic results of RLNC (similar to (1)), we can also prove that

$$\lim_{q\to\infty} \mathsf{Prob}\left(\mathrm{Rank}\left(\bigcap_{i=1}^{K}\Omega_i\right) \geq \pi_{[K]}\right) = 1.$$

As a result, when only (7) and (8) are satisfied but not (8+), with close-to-one probability

$$\mathrm{Rank}\left(\bigcap_{i=1}^{K}\Omega_i\right) = \pi_{[K]} = f_N([K]).$$

The proof of Proposition 1 is thus complete.

V. Conclusion and Future Work

We have quantified the common information of random linear network coding (RLNC) over 1-hop broadcast erasure channels for an arbitrary number of K destinations. In our future work, we will quantify the common information of RLNC of K destinations over h-hop erasure networks for arbitrary h values. Such results need to further take into account the topology of the underlying network.

This work was supported in parts by NSF grants CCF-0845968 and CNS-0905331.

References

[1] J. Byers, M. Luby, and M. Mitzenmacher, "A digital fountain approach to asynchronous reliable multicast," *IEEE J. Select. Areas Commun.*, vol. 20, no. 8, pp. 1528–1540, Oct. 2002.

[2] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *Proc. ACM Special Interest Group on Data Commun. (SIGCOMM)*. Kyoto, Japan, August 2007.

[3] P. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. 41st Annual Allerton Conf. on Comm., Contr., and Computing*. Monticello, IL, October 2003.

[4] E. Erez and M. Feder, "Capacity region and network codes for two receivers multicast with private and common data," in *Proc. Workshop on Coding, Cryptography and Combinatorics*. Huangshen City, China, 2003.

[5] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems of Control and Information Theory*, vol. 2, no. 2, pp. 119–162, 1972.

[6] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.

[7] S. Kamath and V. Anantharam, "A new dual to the Gács-Körner common information defined via the Gray-Wyner system," in *Proc. 48th Annual Allerton Conf. on Comm., Contr., and Computing*, September 2010.

[8] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: Practical wireless network," in *Proc. ACM Special Interest Group on Data Commun. (SIGCOMM)*, 2006.

[9] D. Koutsonikolas, C.-C. Wang, and Y. Hu, "Efficient network coding based opportunistic routing through cumulative coded acknowledgment," *IEEE/ACM Trans. Netw.*, 2011, accepted in January 2011 and the conference version appeared in INFOCOM2010.

[10] S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, February 2003.

[11] W. Liu, G. Xu, and B. Chen, "The common information of n dependent random variables," in *Proc. 48th Annual Allerton Conf. on Comm., Contr., and Computing*, September 2010.

[12] C.-C. Wang, "Capacity of 1-to-K broadcast packet erasure channels with channel output feedback," in *Proc. 48th Annual Allerton Conf. on Comm., Contr., and Computing*. Monticello, Illinois, USA, September 2010.

[13] ——, "On the capacity of wireless 1-hop intersession network coding — a broadcast packet erasure channel approach," in *Proc. IEEE Int'l Symp. Inform. Theory*. Austin, TX, USA, June 2010.