Capacity Bounds on the Downlink of Symmetric, Multi-Relay, Single-Receiver C-RAN Networks

Shirin Saeedi Bidokhti 1,*, Gerhard Kramer 2 and Shlomo Shamai 3

1 Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104, USA
2 Department of Electrical and Computer Engineering, Technical University of Munich, 80333 Munich, Germany; gerhard.kramer@tum.de
3 Department of Electrical Engineering, Technion, Haifa 3200003, Israel; sshlomo@ee.technion.ac.il

* Correspondence: saeedi@seas.upenn.edu; Tel.: +1-215-573-2225

Received: 17 July 2017; Accepted: 6 November 2017; Published: 14 November 2017

Abstract: The downlink of symmetric Cloud Radio Access Networks (C-RANs) with multiple relays and a single receiver is studied. Lower and upper bounds are derived on the capacity. The lower bound is achieved by Marton’s coding, which facilitates dependence among the multiple-access channel inputs. The upper bound uses Ozarow’s technique to augment the system with an auxiliary random variable. The bounds are studied over scalar Gaussian C-RANs and are shown to meet and characterize the capacity for interesting regimes of operation.

Keywords: capacity; coding; cloud radio access network

1. Introduction

Cloud Radio Access Networks (C-RANs) are expected to be a part of future mobile network architectures. In C-RANs, information processing is done in a cloud-based central unit that is connected to remote radio heads (or relays) by rate-limited fronthaul links. C-RANs improve energy and bandwidth efficiency and reduce the complexity of relays by facilitating centralized information processing and cooperative communication. We refer to [1–3] and the references therein for an overview of the challenges and coding techniques for C-RANs. Several coding schemes have been proposed in recent years for the downlink of C-RANs including message sharing [4], backhaul compression [5], hybrid schemes [6] and generalized data sharing using Marton’s coding [7,8]. The paper [9] gives an upper bound on the sum-rate of two-relay C-RANs with two users and numerically compares the performance of the aforementioned schemes with the upper bound.

We consider the downlink of a C-RAN with multiple relays and a single receiver. This network may be modeled by an $M$-relay diamond network where the broadcast component is modeled by rate-limited links and the multiaccess component is modeled by a memoryless Multiple Access Channel (MAC); see Figure 1. The capacity of this class of networks is not known in general, but lower and upper bounds were derived in [10–12] for two-relay networks. Moreover, the capacity was found for binary adder MACs [12] and for certain regimes of operation in Gaussian MACs [11,12]. In this work, we derive lower and upper bounds for C-RANs with multiple relays and find the capacity in interesting regimes of operation for symmetric Gaussian C-RANs.

This paper is organized as follows. Section 2 introduces the notation and the problem setup. In Section 3, we propose a coding strategy based on Marton’s coding and discuss simplifications for symmetric networks. In Section 4, we generalize the bounding technique in [11,12]. The case of symmetric Gaussian C-RANs is studied in Section 5, where we compute lower and upper bounds on the capacity and show that they meet in certain regimes of operation characterized in terms of power, number of users and broadcast link capacities.
2. Preliminaries and Problem Setup

2.1. Notation

Random variables are denoted by uppercase letters, e.g., $X$; their realizations are denoted by lowercase letters, e.g., $x$; and their corresponding probabilities are denoted by $p_X(x)$ or $p(x)$. The probability mass function (pmf) describing $X$ is denoted by $p_X$. $T^n_c(X)$ denotes the set of sequences that are $c$-typical with respect to $p_X$ ([13], p. 25). When $p_X$ is clear from the context, we write $T^n$. The entropy of $X$ is denoted by $H(X)$; the conditional entropy of $X$ given $Y$ is denoted by $H(X|Y)$; and the mutual information of $X$ and $Y$ is denoted by $I(X;Y)$. Similarly, differential entropies and conditional differential entropies are denoted by $h(X)$ and $h(X|Y)$.

Matrices are denoted by bold letters, e.g., $K$. We denote the entry of matrix $K$ in row $i$ and column $j$ by $K_{ij}$. Sets are denoted by script letters, e.g., $S$. The Cartesian product of $S_1$ and $S_2$ is denoted by $S_1 \times S_2$, and the $n$-fold Cartesian product of $S$ is denoted by $S^n$. The cardinality of $S$ is denoted by $|S|$.

Given the set $S = \{s_1, \ldots, s_k\}$, $X_S$ denotes the tuple $(X_{s_1}, \ldots, X_{s_k})$. We define $X^n = X_1, \ldots, X_n$, and (see [14], Equation (74)):

$$I(X_S) = \sum_{m \in S} H(X_m) - H(X_S).$$  \hspace{1cm} (1)

For example, when $S = \{s_1, s_2\}$, (1) becomes the mutual information $I(X_{s_1};X_{s_2})$. The conditional version of (1), $I(X_S|U)$, is defined similarly by conditioning all terms in (1) on $U$. Note that $I(X_S|U)$ is non-negative.

2.2. Model

Consider the C-RAN in Figure 1, where a source communicates a message $W$ with $nR$ bits to a sink with the help of $M$ relays. Let $\mathcal{M} = \{1, \ldots, M\}$ be the set of relays. The source encodes $W$ into descriptions $V_1, \ldots, V_M$ that are provided to relays $1, \ldots, M$, respectively, and where $V_m$ satisfies:

$$H(V_m) \leq nC_m, \hspace{1cm} m = 1, \ldots, M.$$  \hspace{1cm} (2)

Each relay $m, m = 1, \ldots, M$, maps its description $V_m$ into a sequence $X_m^n$, which is sent over a multiple access channel. The MAC is characterized by the input alphabets $\mathcal{X}_1, \ldots, \mathcal{X}_M$ and the output alphabet $\mathcal{Y}$ and the transitional probabilities $p(y|x_1, \ldots, x_M)$ for all $(x_1, \ldots, x_M, y) \in \mathcal{X}_1 \times \ldots \times \mathcal{X}_M \times \mathcal{Y}$. From the received sequence $Y^n$, the sink decodes an estimate $\hat{W}$ of $W$.

A coding scheme consists of an encoder, $M$ relay mappings and a decoder and is said to achieve the rate $R$ if, by choosing $n$ sufficiently large, we can make the error probability $Pr(\hat{W} \neq W)$ as small as desired. We are interested in characterizing the largest achievable rate $R$. We refer to the supremum of achievable rates as the capacity $C^{(M)}$ of the network.

In this work, we focus on symmetric networks.
Definition 1. The network in Figure 1 is symmetric if we have:

\[ C_1 = \ldots = C_M =: C \quad (3) \]

\[ \mathcal{X}_1 = \ldots = \mathcal{X}_M =: \mathcal{X} \quad (4) \]

and:

\[ p_{Y|X_1\ldots X_M}(y|x_1,\ldots,x_M) = p_{Y|X_1\ldots X_M}(y'|x'_1,\ldots,x'_M) \quad (5) \]

for all \( y \in \mathcal{Y}, (x_1,\ldots,x_M) \in \mathcal{X}^M \) and any of its permutations \((x'_1,\ldots,x'_M)\).

When the MAC is Gaussian, the input and output alphabets are the set of real numbers, and the output is given by:

\[ Y = \sum_{m=1}^{M} X_M + Z \quad (6) \]

where \( Z \) is Gaussian noise with zero mean and unit variance. We consider average block power constraints \( P_1,\ldots,P_M \):

\[ \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}(X_{m,i}^2) \leq P_m, \quad m = 1,\ldots,M. \quad (7) \]

The Gaussian C-RAN is symmetric if \( C_m = C \) and \( P_m = P \) for all \( m = 1,\ldots,M \).

3. A Lower Bound

We outline an achievable scheme based on Marton’s coding. We remark that this scheme can be improved for certain regimes of \( C \) by using superposition coding (e.g., see ([15], Theorem 2) and ([11], Theorem 2)).

Fix the pmf \( p(x_1,\ldots,x_M), \epsilon > 0 \), and the auxiliary rates \( R_m, R'_m, m = 1,\ldots,M \), such that:

\[ R_m, R'_m \geq 0 \quad (8) \]

\[ R_m + R'_m \leq C_m. \quad (9) \]

3.1. Codebook Construction

Set:

\[ R = \sum_{m=1}^{M} R_m. \quad (10) \]

For every \( m = 1,\ldots,M \), generate \( 2^{n(R_m+R'_m)} \) sequences \( x_m^n(w_m,w'_m) \), \( w_m = 1,\ldots,2^{nR_m}, w'_m = 1,\ldots,2^{nR'_m} \), in an i.i.d. manner according to \( \prod_{i} P_{X_i}(x_{m,i}) \), independently across \( m = 1,\ldots,M \). For each bin index \( (w_1,\ldots,w_M) \), pick a jointly typical sequence tuple:

\[ (x_1^n(w_1,w'_1),\ldots,x_M^n(w_M,w'_M)) \in T^n_{\epsilon}. \quad (11) \]

3.2. Encoding

Represent message \( w \) as a tuple \((w_1,\ldots,w_M)\), and send \((w_m,w'_m)\) to relay \( m, m = 1,\ldots,M \).

3.3. Relay Mapping at Relay \( m, m = 1,\ldots,M \)

Relay \( m \) sends \( X_m^n(w_m,w'_m) \) over the MAC.
3.4. Decoding

Upon receiving \(y^n\), the receiver looks for indices \(\hat{w}_1, \ldots, \hat{w}_M\) for which the following joint typicality test holds for some \(\hat{w}_1', \ldots, \hat{w}_M'\):

\[
(x^n_{1}(\hat{w}_1, \hat{w}_1'), \ldots, x^n_{M}(\hat{w}_M, \hat{w}_M'), y^n) \in T^n_{e}.
\] (12)

We show in Appendix A that the above scheme has a vanishing error probability as \(n \to \infty\) if, in addition to (8)–(10), we have:

\[\sum_{m \in S} R'_m \geq I(X_S), \quad \forall S \subseteq M \] (13)
\[\sum_{m \in S} R_m + R'_m \leq I(X_S; Y|X_S) + I(X_M) - I(X_S), \quad \forall S \subseteq M. \] (14)

One can use Fourier–Motzkin elimination to eliminate \(R_m, R'_m, m = 1, \ldots, M\), from (8)–(10), (13), (14), and characterize the set of achievable rates \(R\). For symmetric networks (see Definition 1), we bypass the above step and proceed by choosing \(p_{X_M}\) to be “symmetric”.

We say \(p_{X_M}\) is symmetric if:

\[X_1 = \ldots = X_M = X\] (15)
and, for all subsets \(S, S' \subseteq M\) with \(|S| = |S'|\), we have:

\[p_{X_M}(x_1, \ldots, x_{|S|}) = p_{X_M}(x_1, \ldots, x_{|S'|}), \quad \forall (x_1, \ldots, x_{|S|}) \in X^{|S|}. \] (16)

We simplify the problem defined by (8)–(10), (13), (14) for symmetric distributions and prove the following result in Appendix B.

**Theorem 1.** For symmetric C-RAN downlinks, the rate \(R\) is achievable if:

\[R \leq MC - I(X_M) \] (17)
\[R \leq I(X_M; Y) \] (18)

for some symmetric distribution \(p_{X_M}\).

4. An Upper Bound

Our upper bound is motivated by [11,12,14,16].

**Theorem 2.** The capacity \(C^{(M)}\) is upper bounded by:

\[
C^{(M)} \leq \max_{p(x)} \min_{-p(u|y)} \max_{p(i|x,y)} \left\{MC - (M - 1)H(U|Q) + \sum_{m=1}^{M} H(U|X_mQ) - H(U|X_M) \right\}
\] (19)

where \(Q - X_M - Y - U\) forms a Markov chain. Moreover, the alphabet size of \(Q\) may be chosen to satisfy \(|Q| \leq \prod_{i=1}^{M} |X_i| + 2^M - 1.\)

**Remark 1.** For \(M = 2\), Theorem 2 reduces to ([12], Theorem 3).
Proof outline. We start with the following $n$-letter upper bound (see Appendix C):

$$nR \leq nMC - I(X^n_M) \tag{20}$$

$$nR \leq n|S|C + I(X^n_M; Y^n|X^n_S), \quad \forall S \subseteq M. \tag{21}$$

For any sequence $U^n$, we have:

$$I(X^n_M) \geq I(X^n_M) - I(X^n_M|U^n)$$

$$= \left[ \sum_{m=1}^{M} I(X^n_m; U^n) \right] - I(X^n_M; U^n)$$

$$= (M - 1)H(U^n) - \left[ \sum_{m=1}^{M} H(U^n|X^n_m) \right] + H(U^n|X^n_M). \tag{22}$$

By substituting (22) into (20), we obtain:

$$nR \leq nMC - (M - 1)H(U^n) + \left[ \sum_{m=1}^{M} H(U^n|X^n_m) \right] - H(U^n|X^n_M). \tag{23}$$

We now choose $U_i, i = 1, \ldots, n$, to be the output of a memoryless channel $p_{U|Y}(u_i|y_i)$ with input $Y_i$. The auxiliary channel $p_{U|Y}(.,.)$ will be optimized later. With this choice, we single-letterize (21) and (23) and obtain:

$$R \leq MC - (M - 1)H(U|Q) + \sum_{m=1}^{M} H(U|X_mQ) - H(U|X_M) \tag{24}$$

$$R \leq |S|C + I(X_S; Y|X_SQ), \quad \forall S \subseteq M \tag{25}$$

where $Q = X_M - Y - U$ forms a Markov chain.

5. The Symmetric Gaussian C-RAN

We specialize Theorem 1 to the symmetric Gaussian C-RAN defined in (6) and (7) where $P_m = P$ for all $m = 1, \ldots, M$. Choose $(X_1, \ldots, X_M)$ to be jointly Gaussian with the covariance matrix:

$$K_M(\rho) = \begin{bmatrix} P & \rho P & \cdots & \rho P \\ \rho P & P & \cdots & \rho P \\ \vdots & \ddots & \ddots & \vdots \\ \rho P & \cdots & \rho P & P \end{bmatrix}. \tag{26}$$

Remark 2. Choosing $(X_1, \ldots, X_M)$ to be jointly Gaussian (and/or symmetric) is not necessarily optimal for (13) and (14), but it gives a lower bound on the capacity.

Theorem 3. The rate $R$ is achievable if it satisfies the following constraints for some non-negative parameter $\rho$, $0 \leq \rho \leq 1$:

$$R \leq MC - \frac{1}{2} \log \left( \frac{p^M}{\det(K_M(\rho))} \right) \tag{27}$$

$$R \leq \frac{1}{2} \log (1 + PM(1 + (M - 1)\rho)). \tag{28}$$
Remark 3. One can recursively calculate $\det(K_M(\rho))$:

$$
\det(K_M(\rho)) = p^M \left( 1 - \rho^2 \sum_{i=1}^{M-1} i(1 - \rho)^{i-1} \right)
= p^M (1 - \rho)^{M-1} (1 + (M - 1)\rho). 
$$

Let $R^{(\ell)}$ be the maximum achievable rate given by (27) and (28). The RHS of (27) is non-increasing in $\rho$, and the RHS of (28) is increasing in $\rho$. Therefore, we have the following two cases for the optimizing solution $\rho^{(\ell)}$:

- If $MC \leq \frac{1}{2} \log (1 + PM)$ then
  $$
  \rho^{(\ell)} = 0 \quad \text{and} \quad R^{(\ell)} = MC. 
  $$

- Otherwise, $\rho^{(\ell)}$ is the unique solution of $\rho$ in:
  $$
  \frac{1}{2} \log(1 + PM(1 + (M - 1)\rho)) = MC - \frac{1}{2} \log(\frac{1}{(1 - \rho)^{M-1} (1 + (M - 1)\rho)}) 
  $$
  and we have:
  $$
  R^{(\ell)} = \frac{1}{2} \log(1 + PM(1 + (M - 1)\rho^{(\ell)})). 
  $$

We next specialize Theorem 2 to symmetric Gaussian C-RANs.

Theorem 4. The rate $R$ is achievable only if there exists $\rho, 0 \leq \rho \leq 1$, such that the following inequalities hold for all $N \geq 0$:

$$
R \leq MC - (M - 1)\frac{1}{2} \log \left( 2^{2R} + N \right) - \frac{1}{2} \log(1 + N)
+ \frac{M}{2} \log (1 + N + P((M - 1)(1 - \rho)(1 + (M - 1)\rho))) 
$$

$$
R \leq \frac{1}{2} \log (1 + PM(1 + (M - 1)\rho)).
$$

Proof. Set:

$$
U_i = Y_i + Z_{N,i}, \quad i = 1, \ldots, n
$$

where $\{Z_{N,i}\}_{i=1}^n$ are identically distributed according to the normal distribution $\mathcal{N}(0, N)$ and are independent of each other and $X_1^n, \ldots, X_M^n$. The variance $N$ is to be optimized.

In order to find a computable upper bound in (19), we need to lower bound $h(U|Q)$. Recall that $U$ is a noisy version of $Y$. We thus use the conditional entropy power inequality ([17], Theorem 17.7.3):

$$
\begin{align*}
  h(U|Q) &\geq \frac{1}{2} \log \left( 2^{2h(Y|Q)} + 2\pi e N \right) \\
  &\geq \frac{1}{2} \log \left( 2\pi e \left( 2^{2R} + N \right) \right).
\end{align*}
$$

Substituting (36) into the first constraint of (19), we obtain:
\[ R \leq MC - (M - 1)\frac{1}{2} \log \left(2\pi e \left(2^{2R} + N\right)\right) + \sum_{m=1}^{M} h(U|X_mQ) - h(U|X_M) \leq MC - (M - 1)\frac{1}{2} \log \left(2\pi e \left(2^{2R} + N\right)\right) + \sum_{m=1}^{M} h(U|X_m) - h(U|X_M). \] (37)

Now, consider the second term in (19) with \(S = \emptyset\):

\[ R \leq I(X_M;Y|Q) \leq I(X_M;Y) = h(Y) - h(Y|X_M). \] (38)

Note that the RHSs of (37), (38) are both concave in \(p(x_M)\) and symmetric with respect to \(X_1, \ldots, X_M\). Therefore, a symmetric \(p(x_M)\) maximizes them. Let \(K\) denote the covariance matrix of an optimal symmetric solution. We have:

\[ K_{ii} = P, \quad K_{ij} = P\rho. \] (39)

Using the conditional version of the maximum entropy lemma [18], we can upper bound the differential entropies that appear with a positive sign in (37) and (38) by their Gaussian counterparts, and \(h(U|X_M)\) and \(h(Y|X_M)\) can be written explicitly because the channels from \(X_M\) to \(U\) and \(Y\) are Gaussian. We obtain (33) and (34). Note that the RHSs of both bounds are increasing in \(P\), and therefore there is no loss of generality in choosing \(K_{ii} = P\) (among \(K_{ii} \leq P\)). \(\square\)

The upper bound of Theorem 4 and the lower bound of Theorem 3 are plotted in Figure 2 for \(M = 3\) and \(P = 1\), and they are compared with the lower bounds of message sharing [4] and compression [5]. One sees that our lower and upper bounds are close, and they match over a wide range of \(C\). Moreover, establishing partial cooperation among the relays through Marton’s coding offers significant gains. Figure 3 plots the capacity bounds for \(P = 1\) and different values of \(M\).

![Figure 2. Capacity bounds as functions of \(C\) (\(M = 3\), \(P = 1\)).](image)
Figure 3. Capacity bounds as functions of $C$ for $P = 1$ and different values of $M$.

We next compare the lower and upper bounds. We define:

$$C_C = \frac{1}{2M} \log (1 + PM) \quad (40)$$

$$C_L = \frac{1}{2M} \log \left( \frac{1 + \frac{M^2 P}{2(M-1)}}{\frac{M}{2} M^{-1}} \right) \quad (41)$$

$$C_U = \frac{1}{2M} \log \left( \frac{1 + MP \left(1 + (M - 1)\rho^{(2)}\right)}{(1 - \rho^{(2)}) M^{-1} \left(1 + (M - 1)\rho^{(2)}\right)} \right) \quad (42)$$

where:

$$\rho^{(2)} = \frac{M - 2 - \frac{1}{P} + \sqrt{(M - 2 - \frac{1}{P})^2 + 4(M - 1)}}{2(M - 1)} \quad (43)$$

**Theorem 5.** The lower bound of Theorem 3 matches the upper bound of Theorem 4 if:

$$C \leq C_C \quad (44)$$

or if:

$$C_L \leq C \leq C_U \quad (45)$$

where $C_C, C_L, C_U$ are defined in (40)–(42).

**Remark 4.** Theorem 5 recovers ([12], Theorem 5), for $M = 2$.

**Remark 5.** For $C \leq C_C$, no cooperation is needed among the transmitters, and the capacity is equal to $MC$.

**Remark 6.** For $C$ large enough, full cooperation is possible through superposition coding, and the capacity is:

$$C^{(M)} = \frac{1}{2} \log \left(1 + M^2 P\right), \quad C \geq C_{\text{coop}} \quad (46)$$
where
\[
C_{\text{coop}} = \frac{1}{2} \log \left( 1 + M^2 p \right).
\] (47)
The rate (46) is not achievable by Theorem 3 except when \( C \to \infty \). This rate is achievable by message sharing.

**Proof of Theorem 5.** To find regimes of \( P \) and \( C \) for which the lower and upper bounds match, we mimic the analysis in ([12], Appendix F). Consider the lower bound in Theorem 3 and in particular its maximum achievable rate \( R^{(\ell)} \), which is attained by \( \rho^{(\ell)} \); see (30)–(32). If (44) holds, we have \( \rho^{(\ell)} = 0 \), \( R^{(\ell)} = MC \), and thus the cut-set bound is achieved. Otherwise, we proceed as follows.

Consider (33). Since \( R \geq R^{(\ell)} \) and using the definition of \( R^{(\ell)} \) in (32), we can further upper bound (33) and obtain:
\[
R \leq MC - \left( M - 1 \right) \frac{1}{2} \log \left( 1 + N + PM(1 + (M - 1)\rho^{(\ell)}) \right)
+ \frac{M}{2} \log \left( 1 + N + P((M - 1)(1 - \rho)(1 + (M - 1)\rho)) \right)
- \frac{1}{2} \log(1 + N).
\] (48)
Call the RHS of (48) \( g_1(\rho) \) and the RHS of (34) \( g_2(\rho) \). Fix \( N \) as a function of \( \rho^{(\ell)} \) such that:
\[
I^{(G,\rho^{(\ell)})}(X_M|U) = 0
\] (49)
where \( I^{(G,\rho^{(\ell)})}(X_M|U) \) is \( I(X_M|U) \) evaluated for a fully-symmetric Gaussian distribution with correlation factor \( \rho^{(\ell)} \). One can verify that the following choice of \( N \) satisfies (49):
\[
N = P \left( \frac{1 - \rho^{(\ell)}(1 + (M - 1)\rho^{(\ell)})}{\rho^{(\ell)}} \right) - 1.
\] (50)
The right inequality in (45) ensures \( N \geq 0 \).

With this choice of \( N \), \( g_1(\rho) \) is exactly equal to:
\[
MC - I^{(G,\rho^{(\ell)})}(X_M)
\]
at \( \rho = \rho^{(\ell)} \). Note that \( \rho^{(\ell)} \) is defined in (31), and thus, \( g_1(\rho) \) crosses \( g_2(\rho) \) at \( \rho^{(\ell)} \). Since \( g_2(\rho) \) is increasing in \( \rho \), the maximum admissible rate by (34) and (48) matches \( R^{(\ell)} \) if \( g_1(\rho) \) is non-increasing for \( \rho \geq \rho^{(\ell)} \). This is ensured by the left inequality in (45).

6. Concluding Remarks
We studied the downlink of symmetric C-RANs with multiple relays and a single receiver and established lower and upper bounds on the capacity. The lower bound uses Marton’s coding to establish partial cooperation among the relays and improves on schemes that are based on message sharing and compression for scalar Gaussian C-RANs (see Figure 2). The upper bound generalizes the bounding techniques of [11,12]. When specialized to symmetric Gaussian C-RANs, the lower and upper bounds meet over a wide range of \( C \), and this range gets large as \( M \) and/or \( P \) get large.

Future directions include generalizing the techniques to address C-RANs with multiple receivers (e.g., [5]), secrecy constraints at the receivers (e.g., [19]) and secrecy constraints at individual relays (e.g., [20]).
Appendix A. Analysis of the Achievable Scheme

The scheme fails only if one of the following events occurs:

- (11) does not hold for any index tuple \((w^*_1, \ldots, w^*_M)\). This event has a vanishing error probability as \(n \to \infty\) ([13], Lemma 8.2) if we have (13);
- (12) does not hold for the original indices \((w_1, w^*_1, \ldots, w_M, w^*_M)\). This event has a vanishing error probability as \(n \to \infty\) by (11) and the law of large numbers;
- (12) holds for indices \((\tilde{w}_1, \tilde{w}^*_1, \ldots, \tilde{w}_M, \tilde{w}^*_M)\) where \((\tilde{w}_1, \ldots, \tilde{w}_M) \neq (w_1, \ldots, w_M)\). We show that this event has a vanishing error probability as \(n \to \infty\) if we have (14). Since the codebook is symmetric with respect to all messages, we assume without loss of generality that \(w_1 = \ldots = w_M = 1\) and \(w'_1 = \ldots = w'_M = 1\). Fix the sets \(S_1, S_2, S_3 \subset M\) such that \(S_1 \cup S_2 \cup S_3 = M\).

Consider the case where

\[
\begin{align*}
\tilde{w}_i & = 1, \tilde{w}'_i = 1 \quad \forall i \in S_1 \\
\tilde{w}_i & = 1, \tilde{w}'_i \neq 1 \quad \forall i \in S_2 \\
\tilde{w}_i & \neq 1 \quad \forall i \in S_3.
\end{align*}
\]

We denote the set of index tuples satisfying (A1) by \(W(S^2_1)\). We have:

\[
\Pr \left( \bigcup_{W(S^2_1)} (X^1_1(\tilde{w}_1, \tilde{w}'_1), \ldots, X^M_1(\tilde{w}_M, \tilde{w}'_M), Y^n) \in T^n_\epsilon \right) \\
\leq 2^n \sum_{m \in S_1} (R_m + R'_m) + \sum_{m \in S_2} R'_m \\
\times \sum_{(x'_1, \ldots, x'_M, y^n) \in T^n_\epsilon} p_{X^n_1, \ldots, X^n_M, Y^n}(x'_1, \ldots, x'_M, y^n) \\
(a) \leq 2^n \sum_{m \in S_1} (R_m + R'_m) + n \sum_{m \in S_2} R'_m \\
\times 2^n (H(X_M Y) - H(X_M Y) - \sum_{m \in S_1 \cup S_2} H(X_M) - \delta(e))
\]

where \(X^n_{S_2}\) denotes \(\{X^*_m(\tilde{w}_m, \tilde{w}'_m)\}_{m \in S_2}\) and \(X^n_{S_3}\) denotes \(\{X^*_m(\tilde{w}_m, \tilde{w}'_m)\}_{m \in S_3}\). In Step (a), we use that (i) \(X^n_{S_1} Y^n\) is “almost independent” of \(X^n_{S_2}, X^n_{S_3}\) and (ii) the random sequences \(X^*_m(\tilde{w}_m, \tilde{w}'_m)\), \(m \in S_2\), and \(X^*_m(\tilde{w}_m, \tilde{w}'_m)\), \(m \in S_3\), are mutually “almost independent”. Note that we use the term “almost independent”, rather than independent, because we have assumed \(w_1 = \ldots = w_M = 1\) and \(w'_1 = \ldots = w'_M = 1\); i.e., we implicitly have a conditional probability and conditioned on \(w'_1 = \ldots = w'_M = 1\), claims (i)–(ii) may not hold if we insist on exact independence. This issue has been dealt with in [21–23], and following similar arguments, one can show that (i) and (ii) hold with “almost independence”. The probability of the considered error event is thus arbitrarily close to zero for large enough \(n\) if:

\[
\sum_{m \in S_3} (R_m + R'_m) + \sum_{m \in S_2} R'_m < I(X_M; Y | X_{S_1}) + I(X_M) - I(X_{S_3}).
\]

Inequality (A3) is satisfied by (14) when we choose \(S = S_1\). Note that the inequalities with \(S_2 \neq \emptyset\) are redundant.
Appendix B. Simplification for Symmetric Networks with Symmetric Distributions

Choose \( R_m = \bar{R} \) and \( R'_m = R' \) for all \( 1, \ldots, M \). The problem defined by (8)–(10), (13), (14) simplifies using the definition in (16):

\[
\begin{align*}
\bar{R}, \bar{R}' &\geq 0 \tag{A4} \\
\bar{R} + \bar{R}' &\leq C \tag{A5} \\
M \bar{R} &\leq R \tag{A6} \\
|S| \bar{R}' &\geq I(X_S) \quad \forall S \subseteq M \tag{A7} \\
|S| (\bar{R} + \bar{R}') &\leq I(X_S; Y | X_{S'}) + I(X_M) - I(X_S) \quad \forall S \subseteq M. \tag{A8}
\end{align*}
\]

We prove that the tightest inequality in (A7) and (A8) is given by \( S = M \). Eliminating \( \bar{R}' \) from the remaining inequalities concludes the proof.

Let \( S \) be any subset of \( M \) and \( s_0 \) be an element of \( M \) such that \( s_0 \notin S \). This is possible if \( S \neq M \). Define \( T = M \setminus \{S \cup s_0\} \). We show that:

\[
\frac{I(X_S)}{|S|} \leq \frac{I(X_{S \cup \{s_0\}})}{|S| + 1} \tag{A9}
\]

and:

\[
\begin{align*}
\frac{1}{|S| + 1} \left( I(X_{S \cup \{s_0\}}; Y | X_T) + I(X_M) - I(X_T) \right) \\
\leq \frac{1}{|S|} \left( I(X_S; Y | X_T X_{s_0}) + I(X_M) - I(X_{T \cup s_0}) \right). \tag{A10}
\end{align*}
\]

The following equalities come in handy in the proof:

\[
\begin{align*}
I(X_S; T) &= I(X_S) + I(X_T) + I(X_S; X_T) \tag{A11} \\
I(X_S) &= \sum_{j=1}^{\left| S \right| - 1} I(X_{s_1} \ldots X_{s_j}; X_{s_{j+1}}). \tag{A12}
\end{align*}
\]

Suppose \( S = \{s_1, \ldots, s_{|S|}\} \) and \( S' = \{s_0, s_1, \ldots, s_{|S| - 1}\} \). We have:

\[
|S| I(X_{S \cup s_0}) = |S| I(X_S) + |S| I(X_S; X_{s_0}) \geq |S| I(X_S) + \sum_{j=1}^{\left| S \right|} I(X_{s_1} \ldots X_{s_j}; X_{s_0}) \geq \sum_{j=0}^{\left| S \right| - 1} I(X_{s_0} \ldots X_{s_j}; X_{s_{j+1}}) \tag{A13}
\]

where (a) and (c) hold by (16) and (b) is by (A12), written for \( S' \).
Similarly, we have:

\[
(|S| + 1) \left( I(X_S; Y | X_T X_{\bar{S}}) + I(X_M) - I(X_{T \cup \bar{S}}) \right) - |S| \left( I(X_{S \cup \{s_0\}}; Y | X_T) + I(X_M) - I(X_T) \right) \\
= I(X_S; Y | X_T X_{\bar{S}}) - |S|I(X_{S_{\bar{S}}}; Y | X_T) + I(X_M) - (|S| + 1)I(X_{T \cup \bar{S}}) + |S|I(X_T) \\
\overset{(a)}{=} I(X_S; Y | X_T X_{\bar{S}}) - |S|I(X_{S_{\bar{S}}}; Y | X_T) + I(X_S) + I(X_{T \cup \bar{S}}) + I(X_S; X_{T \cup \bar{S}}) \\
- (|S| + 1)I(X_{T \cup \bar{S}}) + |S|I(X_T) \\
\overset{(b)}{=} I(X_S; Y | X_T X_{\bar{S}}) - |S|I(X_{S_{\bar{S}}}; Y | X_T) + I(X_S) + I(X_S; X_{T \cup \bar{S}}) - |S|I(X_T; X_{\bar{S}}) \\
= H(X_S) + I(X_S) - H(X_S; Y X_T X_{\bar{S}}) - |S| \left( H(X_{\bar{S}}) - H(X_{\bar{S}}; Y X_T) \right) \\
\overset{(c)}{=} |S|H(X_{\bar{S}}; Y X_T) - H(X_S; Y X_T X_{\bar{S}}) \\
\overset{(d)}{\geq} 0
\]  

(A14)

where (a) and (b) are by (A11), (c) follows from (16) and (d) follows from (16) and the symmetry of the channel in (5).

Appendix C. Proof of Theorem 2

We first prove the multi-letter bound in (20) using Fano’s inequality and the data processing inequality. For any \( \epsilon > 0 \), we have:

\[
nR \overset{(a)}{\leq} H(V_1, \ldots, V_M) + n\epsilon \\
= \sum_{m=1}^{M} H(V_m) - I(V_M) + n\epsilon \\
\leq \sum_{m=1}^{M} nC - I(V_M) + n\epsilon \overset{(b)}{\leq} \sum_{m=1}^{M} nC - I(X^n_M) + n\epsilon
\]  

(A15)

where (a) is by Fano’s inequality and (b) is by the data processing inequality as follows:

\[
I(V_M) = \sum_{m=1}^{n} I(V_1 \ldots V_m; V_{m+1}) \\
\leq \sum_{m=1}^{n} I(X^n_1 \ldots X^n_m; X^n_{m+1}) = I(X^n_M).
\]  

(A16)

Similarly, for any subset \( S \subset M \) and \( \epsilon > 0 \), we have:

\[
nR \leq I(W; Y^n) + n\epsilon \\
\leq I(W; Y^n V_S X^n_S) + n\epsilon \\
= I(W; V_S X^n_S) + I(W; Y^n | V_S X^n_S) + n\epsilon \\
\overset{(a)}{=} I(W; V_S) + I(W; Y^n | V_S X^n_S) + n\epsilon \\
\leq H(V_S) + I(W X^n_M; Y^n | V_S X^n_S) + n\epsilon \\
\overset{(b)}{\leq} n|S|C + I(X^n_M; Y^n | X^n_S) + n\epsilon
\]  

(A17)
where (a) is because $W - V_S - X_M^n$ forms a Markov chain and (b) is because conditioning does not increase entropy and because $WV_M - X_M^n - Y$ forms a Markov chain.

Next, we single-letterize (23) as follows:

$$nR \leq nMC - (M-1) \sum_{i=1}^{n} H(U_i|U^{i-1}) + \sum_{m=1}^{M} \sum_{i=1}^{n} H(U_i|X^n_M U^{i-1}) - \sum_{i=1}^{n} H(U_i|X^n_M U^{i-1})$$

$$\leq nMC - (M-1) \sum_{i=1}^{n} H(U_i|U^{i-1}) + \sum_{m=1}^{M} \sum_{i=1}^{n} H(U_i|X^n_m U^{i-1}) - \sum_{i=1}^{n} H(U_i|X^n_M U^{i-1})$$

$$= nMC - n(M-1)H(U_T|U^{T-1}T) + \sum_{m=1}^{M} \sum_{i=1}^{n} H(U_i|X^n_m U^{i-1}) - nH(U_T|X_M^n U^{T-1}T)$$

$$= n\left(MC - (M-1)H(U|Q) + \sum_{m=1}^{M} H(U|X^n_m Q) - H(U|X_M Q)\right)$$

where $T$ is a uniform random variable on the set $\{1, \ldots, n\}$ independent of everything in the system, $Q$ is defined by $(U^{T-1}T)$ and $X_1, \ldots, X_M, Y$ and $U$ are defined by $X_{i,T}, \ldots, X_{M,T}, Y_T$ and $U_T$, respectively. Note that $U - Y - X_M - Q$ forms a Markov chain.

Finally, we expand (21) as follows:

$$nR \leq n|S|C + \sum_{i=1}^{n} H(Y_i|X^n_S Y^{i-1}) - \sum_{i=1}^{n} H(Y_i|X^n_M Y^{i-1})$$

$$= n|S|C + \sum_{i=1}^{n} H(Y_i|X^n_S Y^{i-1}) - \sum_{i=1}^{n} H(Y_i|X^n_M Y^{i-1} U^{i-1})$$

(A19)

$$\leq n|S|C + \sum_{i=1}^{n} H(Y_i|X_S U^{i-1}) - \sum_{i=1}^{n} H(Y_i|X_{M,i} U^{i-1})$$

$$\leq n\left(|S|C + I(X_S; Y|X_S Q)\right)$$

where (a) is because $Y_i - X^n_S Y^{i-1} - U^{i-1}$ forms a Markov chain, (b) is because $Y_i - X_{M,i} - U^{i-1}$ forms a Markov chain and (c) is by a standard time sharing argument. The cardinality of $Q$ is bounded using the Fenchel–Eggleston–Carathéodory theorem ([13], Appendix A) (see also ([24], Appendix B)).

References


