Relaying Simultaneous Multicasts via Structured Codes

D. Gündüz[1,2], O. Simeone[3], A. Goldsmith[1], H. V. Poor[2] and S. Shamai (Shitz)[4]
[1]Dept. of Electrical Engineering, Stanford Univ., Stanford, CA 94305, USA
[2]Dept. of Electrical Engineering, Princeton Univ., Princeton, NJ 08544, USA
[3]CWCSPR, New Jersey Institute of Technology, Newark, NJ 07102, USA
[4]Dept. of Electrical Engineering, Technion, Haifa, 32000, Israel

***Abstract*—Simultaneous multicasting of messages with the help of a relay is studied. A two-source two-destination network is considered, in which each destination can receive directly only the signal from one of the sources, so that the reception of the message from the other source (and multicasting) is enabled by the presence of the relay. An outer bound is derived, which is shown to be achievable in the case of finite-field modulo-additive channels by using linear codes, highlighting the benefits of structured codes in exploiting the underlying physical-layer structure of the network. Results are extended to the Gaussian channel model as well, providing achievable rate regions based on nested lattice codes. It is shown that for a wide range of power constraints, the performance with lattice codes approaches the upper bound and surpasses the rates achieved by the standard random coding schemes.**

I. Introduction

Consider non-cooperating base stations multicasting to mobile users in different cells. The coverage area of each base station is generally limited to its cell. To extend coverage, to increase capacity or to improve robustness, a standard solution is that of introducing relays on the cell boundaries that help each base station reach users in the neighboring cells. A model for this scenario is shown in Fig. 1, where two sources (e.g., base stations) simultaneously multicast independent information to two destinations (e.g., mobile users), assisted by a relay station. The model under study is a *compound multiple access channel with a relay* (cMACr) and can be seen as an extension of several fundamental channel models, such as the multiple access channel (MAC), the broadcast channel (BC) and the relay channel (RC). The cMACr is studied in [1], where decode-and-forward (DF) and amplify-and-forward (AF) based protocols are analyzed, and in [10], where we study a more general cMACr model with an additional relay message and provide achievable rate regions using DF and compress-and-forward (CF) schemes. Both works show the advantages of leveraging the network structure, and specifically the available side information at the different nodes, when designing the coding strategies. For instance, DF at the relay may exploit the fact that the users may have already decoded one of the two messages at a certain block [1].

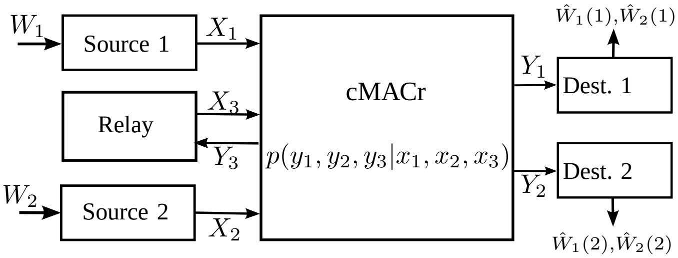
W_1
Source 1
X_1
Relay
X_3
Y_3
W_2
Source 2
X_2
cMACr
$p(y_1, y_2, y_3|x_1, x_2, x_3)$
Y_1
Dest. 1
$\hat{W}_1(1), \hat{W}_2(1)$
Y_2
Dest. 2
$\hat{W}_1(2), \hat{W}_2(2)$

Fig. 1. A compound MAC with a relay (cMACr).

In this paper, we focus on a special cMACr in which each source's signal is received directly by only one of the destinations, while the other destination is reached through the relay. This special model is called the *cMACr without cross-reception*. Extending the previous work reviewed above, here we are interested in further leveraging the network structure by exploiting structured codes [2] [5] [6]. We first present an upper bound for this model and review achievable rates with DF and CF (based on random coding). Then, we study a modulo-additive binary cMACr, and characterize its capacity region, showing that it is achieved by binary linear block codes, while the random coding schemes fall short of the capacity. Finally, we extend these considerations to the Gaussian channel by proposing an achievable scheme based on nested lattice codes. We compare the symmetric rate achievable through lattice coding with the random coding rates and the outer bound and show that lattice coding significantly improves the achievable symmetric rate compared to the random coding schemes in the moderate to high power regime.

II. System Model

A cMACr consists of three input alphabets $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{X}_3$ of source 1, source 2 and the relay, respectively, and three output alphabets $\mathcal{Y}_1$, $\mathcal{Y}_2$ and $\mathcal{Y}_3$ of destination 1, destination 2 and the relay, respectively. We consider a discrete memoryless time-invariant channel without feedback characterized by $p(y_1, y_2, y_3|x_1, x_2, x_3)$ (see Fig. 1). Source i has message $W_i \in \mathcal{W}_i$, $i = 1, 2$, both of which need to be transmitted reliably to both destinations.

This work was supported by U.S. National Science Foundation under grants CNS-06-26611 and CNS-06-25637, the DARPA ITMANET program under grant 1105741-1-TFIND, the U.S. Army Research Office under MURI award W911NF-05-1-0246 and by the Israel Science Foundation and the European Commission in the framework of the FP7 Network of Excellence in Wireless COMmunications NEWCOM++.

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

Definition 2.1: A $(2^{nR_1}, 2^{nR_2})$ code for the cMACr consists of two sets $\mathcal{W}_i = \{1, \ldots, 2^{nR_i}\}$ for $i = 1, 2$, two encoding functions f_i at the sources, $i = 1, 2$, $f_i : \mathcal{W}_i \rightarrow \mathcal{X}_i^n$, a set of (causal) encoding functions g_j at the relay, $j = 1, \ldots, n$, $g_j : \mathcal{Y}_3^{j-1} \rightarrow \mathcal{X}_3$, and two decoding functions h_i at the destinations, $i = 1, 2$, $h_i : \mathcal{Y}_i^n \rightarrow \mathcal{W}_1 \times \mathcal{W}_2$.

We assume that the relay is capable of full-duplex operation, i.e., it can receive and transmit at the same time instant. The average error probability, P_e^n, is defined as

$$\frac{1}{2^{n(R_1+R_2)}} \sum_{W_1, W_2} \Pr\left[\bigcup_{i=1,2} \{h_i(Y_i^n) \neq (W_1, W_2)\} \right].$$

Definition 2.2: A rate pair (R_1, R_2) is said to be *achievable* for the cMACr if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^n \rightarrow 0$ as $n \rightarrow \infty$.

Definition 2.3: The *capacity region* $\mathcal{C}$ for the cMACr is the closure of the set of all achievable rate pairs.

We are interested in a special cMACr model, called the cMACr without cross-reception, in which each source can reach only one of the destinations directly. This is modeled by the following (symbol-by-symbol) Markov chain conditions:

$$Y_1 - (X_1, X_3) - X_2 \text{ and } Y_2 - (X_2, X_3) - X_1, \qquad (1)$$

which state that the output at destination i, $i = 1, 2$, depends only on the inputs of source i and the relay.

III. Bounds on the Capacity Region

A single-letter capacity characterization for the cMACr is open in the most general case. The following proposition presents an outer bound for the cMACr without cross reception.

Proposition 3.1: Assuming that the Markov chain conditions (1) hold for any channel input distribution, a rate pair (R_1, R_2) with $R_j \geq 0$, $j = 1, 2$, is achievable only if

$$\begin{aligned} R_1 &\leq \min\{I(X_1; Y_3|U_1, X_2, X_3, Q), I(X_1, X_3; Y_1|U_2, Q), \\ &\qquad I(X_3; Y_2|X_2, U_2, Q)\} \\ R_2 &\leq \min\{I(X_2; Y_3|U_2, X_1, X_3, Q), I(X_3; Y_1|X_1, U_1, Q), \\ &\qquad I(X_2, X_3; Y_2|U_1, Q)\} \text{ and} \\ R_1 + R_2 &\leq \min\{I(X_1, X_3; Y_1|Q), I(X_2, X_3; Y_2|Q)\} \end{aligned}$$

for some auxiliary random variables U_1, U_2 and Q with joint distribution $p(q)p(x_1, u_1|q)p(x_2, u_2|q)p(x_3|u_1, u_2, q)$ $p(y_1, y_2, y_3|x_1, x_2, x_3)$.

Proof: The proof can be found in [10]. ■

Next, we review the achievable rate regions of the well-known random coding schemes of DF and CF. The proofs of these regions for a general cMACr with additional relay message are given in [10] .

Proposition 3.2: For the cMACr without cross reception, any rate pair (R_1, R_2) with $R_j \geq 0$, $j = 1, 2$, satisfying

$$\begin{aligned} R_1 &\leq \min\{I(X_1; Y_3|U_1, X_2, X_3, Q), I(X_1, X_3; Y_1|U_2, Q), \\ &\qquad I(X_3; Y_2|X_2, U_2, Q)\} \\ R_2 &\leq \min\{I(X_2; Y_3|U_2, X_1, X_3, Q), I(X_3; Y_1|X_1, U_1, Q), \\ &\qquad I(X_2, X_3; Y_2|U_1, Q)\} \text{ and} \\ R_1 + R_2 &\leq \min\{I(X_1, X_2; Y_3|U_1, U_2, X_3, Q), \\ &\qquad I(X_1, X_3; Y_1|Q), I(X_2, X_3; Y_2|Q)\} \end{aligned}$$

for auxiliary random variables U_1, U_2 and Q with a joint distribution of the form $p(q)p(x_1, u_1|q)p(x_2, u_2|q)p(x_3|u_1, u_2, q)$ $p(y_1, y_2, y_3|x_1, x_2, x_3)$ is achievable by DF.

Proposition 3.3: For the cMACr without cross reception, any rate pair (R_1, R_2) with $R_j \geq 0$, $j = 1, 2$, satisfying

$$\begin{aligned} R_1 &\leq \min\{I(X_1; Y_1, \hat{Y}_3|X_2, X_3, Q), I(X_1; Y_2, \hat{Y}_3|X_2, X_3, Q)\}, \\ R_2 &\leq \min\{I(X_2; Y_2, \hat{Y}_3|X_1, X_3, Q), I(X_2; Y_1, \hat{Y}_3|X_1, X_3, Q)\}, \\ R_1 + R_2 &\leq \min\{I(X_1, X_2; Y_1, \hat{Y}_3|X_3, Q), \\ &\qquad I(X_1, X_2; Y_2, \hat{Y}_3|X_3, Q)\}, \text{ such that} \\ &I(Y_3; \hat{Y}_3|X_3, Y_i, Q) \leq I(X_3; Y_i|Q), \text{ for } i = 1, 2, \end{aligned}$$

for random variables $\hat{Y}_3$ and Q with a joint distribution $p(q, x_1, x_2, x_3, y_1, y_2, y_3, \hat{y}_3) = p(q)p(x_1|q)p(x_2|q)p(x_3|q)$ $p(\hat{y}_3|y_3, x_3, q)p(y_1, y_2, y_3|x_1, x_2, x_3)$ is achievable by CF with $\hat{Y}_3$ having bounded cardinality.

Note that the only difference between the outer bound in Prop. 3.1 and the achievable region with DF in Prop. 3.2 is that the latter contains an additional sum-rate constraint, which reduces the rate region in general. This sum-rate constraint accounts for the fact that the DF scheme requires both messages W_1 and W_2 to be decoded at the relay. Due to this requirement, apart from some special cases, DF is in general suboptimal. In fact, in certain cases simply decoding a function of the messages at the relay might suffice. To illustrate this point, consider the special case of the cMACr characterized by $X_i = (X_{i,1}, X_{i,2})$, $Y_i = (Y_{i,1}, Y_{i,2})$ and $Y_{i,1} = X_{i,1}$ for $i = 1, 2$ and the channel given as $p(y_1, y_2, y_3) = p(y_3|x_{1,2}, x_{2,2})p(y_{1,1}|x_{1,1})p(y_{2,1}|x_{2,1})$ $p(y_{1,2}, y_{2,2}|x_3)$. In this model, each source has an error-free orthogonal channel to its destination. Assuming that these channels have enough capacity to transmit the corresponding messages reliably (i.e., message i is available at destination i), the channel at hand resembles the two-way relay channel. In the two-way relay channel, as shown in [6], [7] and [8], DF relaying is suboptimal while using a structured code achieves the capacity in the case of finite field additive channels and might improve the achievable rate region in the case of Gaussian channels. In the following section, we show that linear block codes achieve the capacity for the modulo additive cMACr as well, which cannot be achieved by either DF or CF.

IV. Binary cMACr

Random coding arguments have been highly successful in proving the existence of capacity-achieving codes for many source and channel coding problems in multi-user information theory. However, there are various multi-user scenarios for which random coding fails to achieve the capacity, while *structured codes* can be shown to perform optimally. The best known such example is given by Körner and Marton in [2], which considers encoding the modulo sum of two binary random variables. See [5] for more examples and references.

Here, we consider a binary symmetric (BS) cMACr model and show that structured codes achieve its capacity, while the rate regions achievable with DF or CF schemes are both suboptimal. We model the BS cMACr as follows:

$$Y_i = X_i \oplus X_3 \oplus Z_i, i = 1, 2, \text{ and} \tag{2a}$$

$$Y_3 = X_1 \oplus X_2 \oplus Z_3, \tag{2b}$$

where $\oplus$ denotes binary addition, and the noise components Z_i are independent and identically distributed (i.i.d.) with[1] $\mathcal{B}(\varepsilon_i)$, $i = 1, 2, 3$, $0 \leq \varepsilon_i \leq 0.5$, and they are independent of each other and the channel inputs. Notice that this channel satisfies the Markov condition given in (1). The capacity region for this BS cMACr, which can be achieved by structured codes, is characterized in the following proposition.

Proposition 4.1: For the binary symmetric cMACr characterized in (2), the capacity region is the union of all rate pairs (R_1, R_2) satisfying

$$R_i \leq 1 - H_b(\varepsilon_3), i = 1, 2, \text{ and} \tag{3a}$$

$$R_1 + R_2 \leq \min\{1 - H_b(\varepsilon_1), 1 - H_b(\varepsilon_2)\}, \tag{3b}$$

where $H_b(\varepsilon)$ is the binary entropy function defined as $H_b(\varepsilon) \triangleq -\varepsilon \log \varepsilon - (1 - \varepsilon) \log(1 - \varepsilon)$.

Proof: The proof can be found in Appendix A. ■

For comparison, the rate region achievable with DF of Proposition 3.2 is given by (3) with the additional constraint $R_1 + R_2 \leq 1 - H_b(\varepsilon_3)$, showing that the DF scheme achieves the capacity (3) only if $\varepsilon_3 \leq \min\{\varepsilon_1, \varepsilon_2\}$. As discussed in the previous section, the suboptimality of DF follows from the fact that, while the latter requires decoding of the individual messages, with binary linear codes only the binary sum is decoded at the relay, still guaranteeing decoding at the destinations (see Appendix A for details).

V. Gaussian cMACr

A Gaussian cMACr satisfying the Markov conditions in (1) is given by

$$Y_i = X_i + \eta X_3 + Z_i, i = 1, 2 \tag{4a}$$

$$Y_3 = \gamma(X_1 + X_2) + Z_3, \tag{4b}$$

where $\gamma \geq 0$ is the channel gain from the users to the relay and $\eta \geq 0$ is the channel gain from the relay to both destinations. The noise components Z_i, $i = 1, 2, 3$ are i.i.d. zero-mean unit variance Gaussian random variables. We assume average power constraints: $\frac{1}{n}\sum_{i=1}^{n} E[X_{ji}^2] \leq P_j$ for $j = 1, 2, 3$. We define $C(x) = \frac{1}{2}\log(1 + x)$ for $x \in \mathbb{R}^+$.

For simplicity, we focus on a symmetric scenario with $P_1 = P_2 = P_3 = P$ and consider the achievable symmetric rate $R_1 = R_2 = R$. Under such assumptions, the outer bound of Proposition 3.1 reduces to

$$R \leq \max_{\substack{0 \leq \alpha \leq 1 \\ 0 \leq \alpha_3 \leq 1}} \min\left\{\frac{1}{2}C\left(P\left(1 + \eta^2 + 2\eta\sqrt{\alpha\alpha_3}\right)\right),\right.$$

$$\left. C\left(P + \eta^2 P(1 - \alpha_3)\right), C\left(\gamma^2 P\left(\frac{1 - 2\alpha\alpha_3}{1 - \alpha\alpha_3}\right)\right)\right\}, \tag{5}$$

whereas the rate achievable with DF is given by the right hand side of (5) with an additional term in $\min\{\cdot\}$ given by $\frac{1}{2}C\left(2\gamma^2 P\left(1 - 2\alpha\alpha_3\right)\right)$. The following symmetric rate is instead achievable by CF from Proposition 3.3:

$$R \leq \min\left\{C\left(\frac{\gamma^2\alpha P}{1 + N_q}\right), \frac{1}{2}\left[C(\alpha P) + C\left(\frac{2\gamma^2\alpha P}{1 + N_q}\right)\right]\right\}$$

where $N_q = \frac{1+\gamma^2(\alpha^2P^2+2\alpha P)+\alpha P}{\eta^2 P_3}$ for all $0 \leq \alpha \leq 1$.

In Sec. IV, we have shown that for a binary additive compound MAC with a relay, it is optimal to use structured (block linear) codes rather than conventional unstructured (random) codes. The reason for this performance advantage is that linear codes, when received by the relay over an additive channel, enable the latter to decode the sum of the original messages with no rate loss, without requiring joint decoding of the messages. As is well known, the counterpart of binary block codes over binary additive channels in the case of Gaussian channels is given by lattice codes which can achieve the Gaussian channel capacity in the limit of infinite block lengths [3]. A lattice is a discrete subgroup of the Euclidean space $\mathbb{R}^n$ with the vector addition operation, and hence provides us a modulo sum operation at the relay similar to the binary case.

For the Gaussian cMACr setting given in (4), we use the same nested lattice code at both sources. Similar to the transmission structure used in the binary setting, we want the relay to decode only the modulo sum of the messages, where the modulo operation is with respect to a coarse lattice as in [7], whereas the messages are mapped to a fine lattice. The relay then broadcasts the modulo sum of the message points to both destinations. Each destination decodes the message from the source that it hears directly, and the modulo sum of the messages from the relay as explained in Appendix B. Using these two, each destination can also decode the remaining message. We have the following rate region that can be achieved by the proposed lattice coding scheme.

Proposition 5.1: For the symmetric Gaussian cMACr characterized by (4), an equal rate R can be achieved using a lattice encoding/decoding scheme if

$$R \leq \min\left\{C\left(\gamma^2 P - \frac{1}{2}\right), C\left(P\min\{1, \eta^2\}\right),\right.$$

$$\left.\frac{1}{2}C(P(1 + \eta^2))\right\}. \tag{6}$$

Proof: The proof can be found in Appendix B. ■

Remark 5.1: Achievability of (6), discussed in Appendix B, requires transmission at rates corresponding to the symmetric rate point on the boundary of the MAC regions from each source and the relay to the corresponding destination. However, here, of the two senders over each MAC, one employs lattice coding, and hence the standard joint typicality argument fails to prove achievability of these rate points. The problem is solved by noticing that, even in this scenario, it is straightforward to operate at the corner points of the MAC region by using single user encoding and successive decoding. In general, two different techniques can achieve

[1] $X \sim \mathcal{B}(\varepsilon)$ denotes a Bernoulli distribution for which $p(X = 1) = \varepsilon$ and $p(X = 0) = 1 - \varepsilon$.

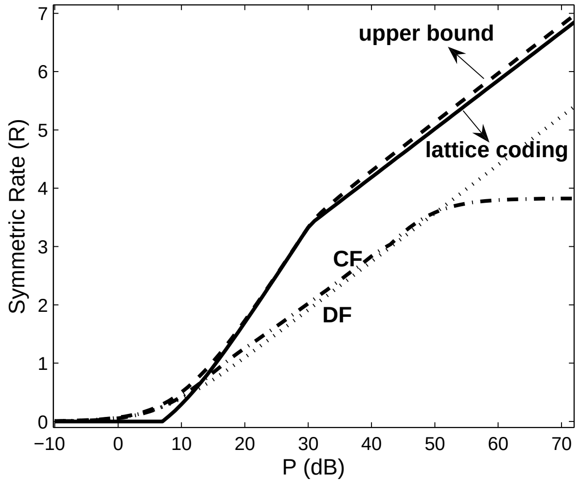

Fig. 2. Equal rate achievable with lattice codes (6) compared with the upper bound (5) and the rates achievable with DF and CF for $\gamma^2 = 1/10$ and $\eta^2 = 10$ versus $P_1 = P_2 = P_3 = P$.

any boundary rate point by using point-to-point codes, namely time-sharing and rate-splitting [9]. In our case, time-sharing would generally cause a rate reduction with respect to (6), due to the constraint arising from decoding at the relay. In contrast, rate-splitting does not have such a drawback: the relay splits its message and power into two parts and acts as two virtual users, while single-user coding is applied for each virtual relay user as well as the message from the source. Since lattice coding achieves the optimal performance for single user decoding, we can achieve any point on the boundary.

1) Numerical example: In Fig. 2, the equal rate achievable with lattice codes (6) is compared with the upper bound (5) and the symmetric rates achievable with DF and CF for $\gamma^2 = 1/10$ and $\eta^2 = 10$ versus $P_1 = P_2 = P_3 = P$. We see that, for sufficiently large P, the lattice-based scheme is close to optimal, whereas for smaller P, CF or DF have better performance. The performance loss of lattice-based schemes with respect to the upper bound is due to the fact that lattice encoding does not enable coherent power combining gains at the destination. It is also noted that both DF and lattice-based schemes have the optimal multiplexing gain of $1/2$ (in terms of equal rate).

VI. Conclusions

We have studied a compound multiple access channel with a relay, in which the relay simultaneously assists both sources to multicast their messages. In particular, we have considered a special case, called the cMACr without cross-reception, in which the destinations can receive the signal directly only from one of the sources. Our focus in this paper has been on the performance of structured codes, rather than random coding schemes. We have proved that the capacity can be achieved by linear block codes in the case of finite-field modulo-additive channels. In the Gaussian setting we have shown that the achievable rate can be improved by nested lattice coding at moderate to high SNRs.

Appendix A
Proof of Proposition 4.1

We first prove the converse showing that (3) serves as an outer bound, and prove the direct part describing a structured coding scheme that achieves the outer bound.

To prove the converse, we consider the outer bound in Prop. 3.1, and show that an input distribution with $X_1, X_2, X_3, U_1, U_2 \sim \mathcal{B}(1/2)$ and independent of each other maximizes all the mutual information terms. To this end, notice that ignoring all the constraints involving auxiliary random variables in the outer bound can only enlarge the region, so that we have the conditions:

$$R_1 \le I(X_1; Y_3 | X_2, X_3, Q), \tag{7}$$

$$R_2 \le I(X_2; Y_3 | X_1, X_3, Q), \text{ and} \tag{8}$$

$$R_1 + R_2 \le \min\{I(X_1, X_3; Y_1 | Q), I(X_2, X_3; Y_2 | Q)\}. \tag{9}$$

We can further write

$$\begin{aligned} I(X_1; Y_3 | X_2, X_3, Q) &= H(Y_3 | X_2, X_3, Q) \\ &\quad - H(Y_3 | X_1, X_2, X_3, Q) \\ &\le H(Y_3) - H_b(\varepsilon_3) \le 1 - H_b(\varepsilon_3), \\ I(X_1, X_3; Y_1 | Q) &= H(Y_1 | Q) - H(Y_1 | X_1, X_3, Q) \\ &\le H(Y_1) - H_b(\varepsilon_1) \le 1 - H_b(\varepsilon_1). \end{aligned}$$

These inequalities hold with equality under the above stated input distribution, which concludes the proof of the converse.

We now prove the direct part of the proposition. First, consider $R_1 \ge R_2$. Transmission is organized into B blocks of size n bits. In each of the first $B-1$ blocks, say the bth, the j-th source, $j = 1, 2$, sends nR_j new bits, organized into a $1 \times \lfloor nR_j \rfloor$ vector $\mathbf{u}_{j,b}$. Moreover, encoding at the sources is done using the same binary linear code characterized by a $\lfloor nR_1 \rfloor \times n$ random binary generator matrix $\mathbf{G}$ with i.i.d. entries $\mathcal{B}(1/2)$. Specifically, as in [8], source 1 transmits $\mathbf{x}_{1,b} = \mathbf{u}_{1,b}\mathbf{G}$ and source 2 transmits $\mathbf{x}_{2,b} = [\mathbf{0}\ \mathbf{u}_{2,b}]\mathbf{G}$ where the all-zero vector is of size $1 \times \lfloor nR_1 \rfloor - \lfloor nR_2 \rfloor$ (zero-padding). Since capacity-achieving random linear codes exist for BS channels, we assume that $\mathbf{G}$ is the generating matrix for such a capacity achieving code.

We define $\mathbf{u}_{3,b} \triangleq \mathbf{u}_{1,b} \oplus [\mathbf{0}\ \mathbf{u}_{2,b}]$. The relay can then decode $\mathbf{u}_{3,b}$ from the received signal $\mathbf{y}_{3,b} = \mathbf{u}_{3,b}\mathbf{G} + \mathbf{z}_3$ since $\mathbf{x}_{1,b} \oplus \mathbf{x}_{2,b}$ is also a codeword of the code generated by $\mathbf{G}$. This occurs with vanishing probability of error if (3a) holds. In the following $(b+1)$-th block, the relay encodes $\mathbf{u}_{3,b}$ using an independent binary linear code with an $\lfloor nR_1 \rfloor \times n$ random binary generator matrix $\mathbf{G}_3$ as $\mathbf{x}_{3,b+1} = \mathbf{u}_{3,b}\mathbf{G}_3$. We use the convention that the signal sent by the relay in the first block is $\mathbf{x}_{3,1} = \mathbf{0}$ or any other known sequence.

At the end of the first block ($b = 1$), where the relay sends a known signal, the j-th destination can decode the current nR_j bits $\mathbf{u}_{j,1}$ from the jth source if $R_j \le 1 - H_b(\varepsilon_j)$. Under this condition, we can now consider the second block, or any other

$(b+1)$-th block, assuming that the j-th destination already knows $\mathbf{u}_{j,b}$. In the $(b+1)$-th block, the first destination sees the signal $\mathbf{y}_{1,b+1} = \mathbf{u}_{1,b+1}\mathbf{G} \oplus \mathbf{u}_{3,b}\mathbf{G}_3 \oplus \mathbf{z}_1$. However, since $\mathbf{u}_{1,b}$ is known at the first destination, it can be canceled from the received signal, leading to $\mathbf{y}'_{1,b+1} = \mathbf{u}_{1,b+1}\mathbf{G} \oplus \mathbf{u}_{2,b}\mathbf{G}'_3 \oplus \mathbf{z}_1$, where $\mathbf{G}'_3$ is a $\lfloor nR_2 \rfloor \times n$ matrix that contains the last $\lfloor nR_2 \rfloor$ rows of $\mathbf{G}_3$. $\mathbf{u}_{1,b+1}$ and $\mathbf{u}_{2,b}$ are correctly decoded by the first destination if $R_1 + R_2 \leq 1 - H_b(\varepsilon_1)$. Repeating this argument for the second destination and then considering the case $R_1 \geq R_2$ concludes the proof.

Appendix B
Proof of Proposition 5.1

We first give a brief overview of lattice codes (see [3], [7] for further details). An n-dimensional lattice Λ is defined as $\Lambda = \{GX : X \in \mathbb{Z}^n\}$, where $G \in \mathbf{R}^n$ is the generator matrix. For any $x \in \mathbb{R}^n$, the quantization of X maps X to the nearest lattice point in Euclidean distance:$Q_\Lambda(X) \triangleq \arg\min_{Q\in\Lambda} \|X - Q\|$. The mod operation is defined as $X \mod \Lambda = X - Q_\Lambda(X)$. The fundamental Voronoi region $\mathcal{V}(\Lambda)$ is defined as $\mathcal{V}(\Lambda) = \{X : Q_\Lambda(X) = 0\}$, whose volume is denoted by $V(\Lambda)$ and is defined as $V(\Lambda) = \int_{\mathcal{V}(\Lambda)} dX$. The second moment of lattice Λ is given by $\sigma^2(\Lambda) = \frac{1}{nV(\Lambda)}\int_{\mathcal{V}(\Lambda)} \|X\|^2 dX$, while the normalized second moment is defined as $G(\Lambda) = \frac{\sigma^2(\Lambda)}{V(\Lambda)^{1/n}} = \sigma^2(\Lambda) = \frac{1}{nV(\Lambda)}\int_{\mathcal{V}(\Lambda)} \|X\|^2 dX$.

We use a nested lattice structure as in [4], where Λ_c denotes the coarse lattice and Λ_f denotes the fine lattice and we have $\Lambda_c \subseteq \Lambda_f$. Both sources use the same coarse and fine lattices for coding. We consider lattices such that $G(\Lambda_c) \approx \frac{1}{2\pi e}$ and $G(\Lambda_f) \approx \frac{1}{2\pi e}$, whose existence is shown in [4]. In nested lattice coding, the codewords are the lattice points of the fine lattice that are in the fundamental Voronoi region of the coarse lattice. Moreover, we choose the coarse lattice (i.e., the shaping lattice) such that $\sigma^2(\Lambda_c) = P$ to satisfy the power constraint. The fine lattice is chosen to be good for channel coding, i.e., it achieves the Poltyrev exponent [4].

We use a block Markov coding structure; that is the messages are coded into B blocks, and are transmitted over $B+1$ channel blocks. The relay forwards the information relating to the messages from each block over the next channel block. The relay is kept silent in the first channel block, while the sources are silent in the last one. The destinations decode the messages from the sources and the relay right after each block. Since there is no coherent combining, sources send only new messages at each channel block, thus sequential decoding with a window size of one is sufficient. We explain the coding scheme for two consecutive channel blocks dropping the channel block index in the expressions.

Each source i maps its message W_i to a fine lattice point $V_i \in \Lambda_f \cap \mathcal{V}(\Lambda_c)$, $i = 1, 2$. Each user employs a dither vector U_i which is independent of the dither vectors of the other users and of the messages and is uniformly distributed over $\mathcal{V}(\Lambda_c)$. We assume all the terminals in the network know the dither vectors. Now the transmitted codeword from source i is given by $X_i = (V_i - U_i) \mod \Lambda_c$. It can be shown that X_i is also uniform over $\mathcal{V}(\Lambda_c)$.

At the end of each block, we want the relay to decode $V \triangleq (V_1 + V_2) \mod \Lambda_c$ instead of decoding both messages. Following [7] (with proper scaling to take care of the channel gain γ), it is possible to show that V can be decoded at the relay if

$$R \leq \frac{1}{n}\log_2 |\Lambda_f \cap \mathcal{V}(\Lambda_c)| < \frac{1}{2}\log\left(\frac{1}{2} + \gamma^2 P\right). \tag{10}$$

Then in the next channel block, while the sources send new information, the relay broadcasts the index of V to both destinations. The relay uses rate-splitting [9], and transmits each part of the V index using a single-user random code (see Remark 5.1). Let R_1 and R_2 be the rates of the two codes the relay uses, with power allocation δ and $P - \delta$, respectively. Each destination applies successive decoding; the codes from the relay are decoded using a single-user typicality decoder, while the signal from the source is decoded by a Euclidean lattice decoder. Successful decoding is possible if

$$\begin{aligned} R_1 &\leq C\left(\eta^2\delta\right), \\ R &\leq C\left(\frac{P}{1+\eta^2\delta}\right) \text{ and} \\ R_2 &\leq C\left(\frac{\eta^2(P-\delta)}{1+\eta^2\delta+P}\right), \end{aligned}$$

where $R_1 + R_2 = R$. This is equivalent to having

$$R \leq \left\{C\left(\eta^2 P\right), C\left(P\right), \frac{1}{2}C\left((1+\eta^2)P\right)\right\}.$$

Combining this with (10), we obtain the rate constraint given in the theorem.

References

[1] I. Maric, A. Goldsmith and M. Médard, "Information-theoretic relaying for multicast in wireless networks," *Proc. IEEE Military Communications Conference (MILCOM)*, Orlando, FL, Oct. 2007.

[2] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Inform. Theory*, vol. 25, pp. 219-221, March 1979.

[3] U. Erez and R. Zamir, "Achieving 1/2 log(1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2293–2314, October 2004.

[4] R. Zamir, S. Shamai and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250-1276, June 2002.

[5] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," *European Trans. Telecommun.*, vol. 19, no. 4, pp. 455-474, Apr. 2008.

[6] R. Knopp, "Two-way wireless communication via a relay station," *The 3 Ms of Future Mobile Communications: Multi-user, Multi-antenna, Multi-hop Systems*, Paris, France, March 2007.

[7] M. P. Wilson, K. Narayanan, H. Pfister and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," submitted to *IEEE Trans. Inform. Theory* [arXiv:0805.0012v2].

[8] W. Nam, S. Y. Chung and Y. H. Lee, "Capacity bounds for two-way relay channels," *Proc. Int'l Zurich Seminar on Communications*, pp. 144-147, Zurich, Switzerland, March 2008.

[9] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 364-375, March 1996.

[10] D. Gündüz, O. Simeone, A. J. Goldsmith, H. V. Poor and S. Shamai, "Multiple multicasts with the help of a relay," submitted to *IEEE Trans. Inform. Theory* [arXiv:0902.3178v1].