Compute–Forward Multiple Access (CFMA) with Nested LDPC Codes

Erixhen SulaJingge ZhuAdriano PastoreSung Hoon LimMichael GastparEPFLUC BerkeleyCTTC/CERCAKIOSTEPFLerixhen.sula@epfl.chjingge.zhu@berkeley.eduadriano.pastore@cttc.catshlim@kiost.ac.krmichael.gastpar@epfl.ch

Abstract—Inspired by the compute-and-forward scheme from Nazer and Gastpar, a novel multiple-access scheme introduced by Zhu and Gastpar makes use of nested lattice codes and sequential decoding of linear combinations of codewords to recover the individual messages. This strategy, coined *computeforward multiple access* (CFMA), provably achieves points on the dominant face of the multiple-access capacity region while circumventing the need of time sharing or rate splitting. For a two-user multiple-access channel (MAC), we propose a practical procedure to design suitable codes from off-the-shelf LDPC codes and present a sequential belief propagation decoder with complexity comparable with that of point-to-point decoders. We demonstrate the potential of our strategy by comparing several numerical evaluations with theoretical limits.

I. INTRODUCTION

The promise of non-orthogonal multiple-access communication schemes is to operate at rate points beyond the convex combinations of single-user capacities (attained by orthogonal resource sharing) in an attempt to achieve the MAC capacity region. Several encoding and decoding schemes have been proposed in the literature: simultaneous joint decoding, which recovers all messages at once, is optimal in terms of achievable rates but suffers from high complexity; successive cancellation decoding is also first-order optimal but requires time sharing to obtain all rate points on the dominant face; rate splitting as proposed by Rimoldi and Urbanke [1] is also optimal but requires superposition coding and additional decoding steps, which in practical systems may entail some complexity overhead.

Recently, the CFMA strategy proposed in [2], which is based on nested and scaled lattice codes, was shown to achieve the full capacity region of the Gaussian MAC when the SNR is greater than $1 + \sqrt{2}$. The underlying idea behind CFMA in the two-user case is to first recover a weighted sum of the lattice codewords, which is accomplished by extending the compute–forward strategy originally proposed by Nazer and Gastpar [3]. In the second stage, using the recovered linear combination as side information, the decoder recovers any one of the messages. Finally, since the receiver knows one linear combination and one of the two messages, it can recover the remaining message.

Based on the theoretical findings of [2], which uses random lattice codes and lattice decoding as proof techniques following ideas from [3], [4], the goal of this paper is to design practical codes and efficient decoding algorithms that can operate close to the boundary of the multiple access channel capacity at reasonably low error probability without the need of time sharing. With this goal in mind, we present a practical CFMA strategy based on nested *linear* codes constructed from off-the-shelf low-density parity check (LDPC) codes that are originally designed for point-to-point communications. From details presented in Section III, it will become apparent that our proposed decoding algorithms for each of the two decoding steps are only slight variations of the classical single-user point-to-point belief propagation decoder, and as such, enjoy similarly low complexity.

Boldface lower-case and upper-case denote vectors and matrices respectively. The operator ' \oplus ' denotes the binary (XOR) addition. The bracket [a : b] stands for the set of integers contained in the interval [a; b].

II. SYSTEM MODEL AND THEORETICAL BACKGROUND

We consider the two-user Gaussian MAC, with input alphabets X_1 , X_2 and output alphabet \mathcal{Y} . For input symbols x_1 , x_2 , the output symbol is given by

$$Y = h_1 x_1 + h_2 x_2 + Z, (1)$$

where $h_1, h_2 \in \mathbb{R}$ denote the constant channel and $Z \sim \mathcal{N}(0, 1)$ is the additive white Gaussian noise (AWGN).

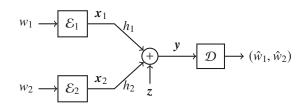


Fig. 1. Block diagram of the two-user Gaussian MAC communication system

A $(2^{nR_1}, 2^{nR_2}, n)$ code for the MAC consists of:

- two message sets $[1:2^{nR_1}]$ and $[1:2^{nR_2}]$;
- two encoding functions \mathcal{E}_1 and \mathcal{E}_2 which respectively assign codewords $x_k \in \mathcal{X}_k^n$ to each message $w_k \in [1 : 2^{nR_k}]$, k = 1, 2, with average power constraint

$$\|\boldsymbol{x}_k\|^2 \le nP; \tag{2}$$

a decoding function D which assigns an estimate (ŵ₁, ŵ₂) of the message pair based on y ∈ Yⁿ.

Assuming that the messages w_1 and w_2 are drawn uniformly at random from the message sets $[1:2^{nR_1}]$ and $[1:2^{nR_2}]$, respectively, the average probability of error is defined as

$$P_{\rm e}^{(n)} = \operatorname{Prob}\left\{ (\hat{w}_1, \hat{w}_2) \neq (w_1, w_2) \right\}.$$
 (3)

A rate pair (R_1, R_2) is said to be *achievable* if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$.

In the remainder of this section, we will briefly review some theoretical results on the multiple–access channel and the compute–forward multiple access (CFMA) scheme.

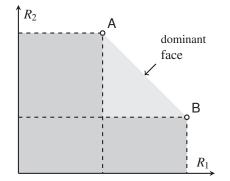


Fig. 2. The MAC rate region achievable for a fixed input distribution $p(x_1)p(x_2)$ (light and dark shaded gray combined). The corner points A and B are achievable by successive cancellation decoding, whereas points located on the dominant face (i.e., the segment connecting A and B) can be achieved by time sharing between A and B.

The capacity region of the MAC [5] is given by the set of rate pairs (R_1, R_2) that satisfies

$$R_1 < I(X_1; Y | X_2)$$
 (4a)

$$R_2 < I(X_2; Y|X_1)$$
 (4b)

$$R_1 + R_2 < I(X_1, X_2; Y)$$
(4c)

for some joint distribution $(X_1, X_2) \sim p(x_1)p(x_2)$. When input alphabets are set to $X_1 = X_2 = \mathbb{R}$ and the codewords are subject to a power constraint (2), the capacity region [5] is attained by setting $X_k \sim \mathcal{N}(0, P)$, k = 1, 2. Throughout this paper, we will refer to the rate region (4) with uniform discrete input distributions as \mathcal{R}_{MAC-UI} .

The so-called *corner points*, labeled in Figure 2 as A and B, are achievable by means of successive cancellation decoding [5]. The remaining points on the dominant face (that is, the segment that connects the corner points) can be achievable by time sharing.

More recently, the authors of [6] presented a generalization of compute–forward which is based on nested linear codes and joint typicality encoding and decoding, rather than on lattice codes as in [2], [3]. Assuming that the constellation size q is a prime power, one defines field mappings φ_1^{-1} and φ_2^{-1} which bijectively map constellation points $x_1 \in X_1$ and $x_2 \in X_2$ to finite field elements $u_1 \in \mathbb{F}_q$ and $u_2 \in \mathbb{F}_q$, respectively. In analogy to the procedure with lattice codes described above, the receiver first decodes a weighted field sum

$$s = a_1 \boldsymbol{u}_1 \oplus_q a_2 \boldsymbol{u}_2$$

= $a_1 \varphi_1^{-1}(\boldsymbol{x}_1) \oplus_q a_2 \varphi_2^{-1}(\boldsymbol{x}_2)$

(where $u_k = \varphi_k^{-1}(x_k)$ stands for the vector resulting from a symbol-by-symbol application of φ_k^{-1} on the coordinates of x_k) and then uses the decoded *s* as side information to decode either u_1 or u_2 .

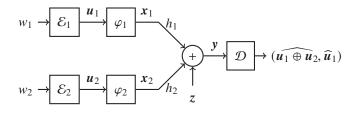


Fig. 3. Block diagram for the MAC channel with CFMA decoding.

By specializing [6, Theorem 1], we can readily establish the following theorem which describes a rate region achievable with CFMA.

Let X_1 and X_2 have equal cardinality q, which we assume to be a prime power. Let \mathbb{F}_q denote a q-ary finite field. Fix the input distribution $p(x_1)p(x_2)$.

Theorem 1: A rate pair (R_1, R_2) is achievable with nested linear codes and under the CFMA decoding strategy¹ if for some non-zero coefficient vector $(a_1, a_2) \in \mathbb{F}_q^2$ and for some bijective field mappings φ_1^{-1} and φ_2^{-1} , we have either

$$R_{1} \leq H(X_{1}) - \max\{H(S|Y), H(X_{1}, X_{2}|Y, S)\},\$$

$$R_{2} \leq H(X_{2}) - H(S|Y),$$
(5a)

or

$$R_{1} \leq H(X_{1}) - H(S|Y),$$

$$R_{2} \leq H(X_{2}) - \max\{H(S|Y), H(X_{1}, X_{2}|Y, S)\},$$
(5b)

where $S = a_1 \varphi_1^{-1}(X_1) \oplus_q a_2 \varphi_2^{-1}(X_2)$.

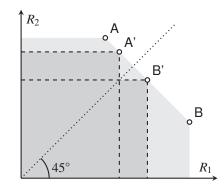


Fig. 4. For some fixed $(a_1, a_2) \in \mathbb{F}_q^2$, inequalities (5a) and (5b) yield rate points A' and B', respectively. If $H(S|Y) \leq \frac{1}{2}H(X_1, X_2|Y)$, they lie on the dominant face (as in the figure). Points dominated by A' and B' (in dark gray) can be achieved without time sharing, using nested linear codes and the CFMA decoding strategy. The uniform-input rate region \mathcal{R}_{MAC-UI} is shaded in light gray.

Throughout the paper, we will refer to the rate region (5) evaluated with uniform discrete inputs as $\mathcal{R}_{CFMA-UI}$. Note that

¹The reader is referred to [6] for a precise description of the nested linear code construction, and the encoding and decoding strategies used for the proof of achievability.

Theorem 1 can be extended by a discretization approach [6, Theorem 3] to infinite constellations and continuous signal distributions, by way of which, in particular, Zhu and Gastpar's original achievability result proved using lattice codes [2, Theorem 2] can be recovered.

Figure 4 illustrates the rates achievable with CFMA according to Theorem 1, for some fixed coefficient pair $(a_1, a_2) \in \mathbb{F}_q^2$. The coordinates of points A' and B' are given by the right-hand sides of Equations (5a) and (5b), respectively.

III. CFMA WITH BINARY CODES

In this section we devise a practical design of CFMA for a two-user Gaussian MAC, inspired by the theoretically achievable rate region established by Theorem 1, and based on off-the-shelf binary linear error-correcting codes. One important feature of the proposed implementation is that while operating near the dominant face of the achievable rate region (other than the two corner points), we keep the decoding algorithm essentially the same as that for a point-to-point system. This low complexity design makes it attractive for practical implementations.

A. Code construction and encoding

Let (R_1, R_2) be the target rate pair $(R_1, R_2 \le 1$ for binary codes) and assume $R_1 \ge R_2$ without loss of generality. We need to find two linear channel codes C_1, C_2 with respective rates R_1, R_2 and satisfying the inclusion $C_2 \subseteq C_1$.

Code construction with binary LDPC codes: Assuming $R_1 \ge R_2$, we pick an LDPC code C_2 of rate R_2 for user 2, with its parity check matrix $H \in \mathbb{F}_2^{(n-k_2)\times n}$. To construct the code C_1 for user 1 while ensuring $C_2 \subseteq C_1$, a "merging" technique is used. For example, let $h_i^T, h_j^T \in \mathbb{F}_2^{1\times n}$ be two rows of the parity-check matrix H. Since any codeword u from C_2 satisfies

$$\boldsymbol{h}_i^{\mathsf{T}}\boldsymbol{u}=0, \qquad \boldsymbol{h}_j^{\mathsf{T}}\boldsymbol{u}=0,$$

it also satisfies

$$(\boldsymbol{h}_i \oplus \boldsymbol{h}_i)^{\mathsf{T}} \boldsymbol{u} = 0.$$

Replacing two rows $\mathbf{h}_i^{\mathsf{T}}, \mathbf{h}_j^{\mathsf{T}}$ in \mathbf{H} by the new row $(\mathbf{h}_i \oplus \mathbf{h}_j)^{\mathsf{T}}$ we obtain a new code C'. The parity check matrix \mathbf{H}' of C' is of dimension $(n - k_2 - 1) \times n$ hence has a higher rate. Obviously, any codeword $\mathbf{u} \in C_2$ satisfies $\mathbf{H}'\mathbf{u} = \mathbf{0}$, hence is a codeword of C'. This merging procedure is illustrated in Figure 5 using the Tanner graph of the LDPC code, where two check nodes are merged into one.

Example 1: We give an example of constructing two nested LDPC codes in Figure 5 by merging check nodes. The original LDPC code is shown in Figure 5a with four check nodes f_1 , f_2 , f_3 , f_4 where check nodes f_3 and f_4 impose the constraints:

$$x_3 \oplus x_5 \oplus x_6 \oplus x_8 = 0$$
$$x_4 \oplus x_5 \oplus x_6 \oplus x_7 = 0$$

We merge the check nodes f_3 and f_4 to obtain a new code in Figure 5b with three check nodes f'_1, f'_2, f'_3 . Since f'_3 is formed by merging f_3 and f_4 , it imposes the constraint:

$$x_3 \oplus x_4 \oplus x_7 \oplus x_8 = 0$$

The check nodes f'_1 and f'_2 give the same constraints as f_1 and f_2 respectively. The rate of the new code is increased to 5/8 from the original code with a rate 1/2.

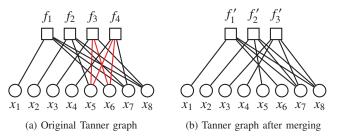


Fig. 5. How to construct nested linear codes by parity-check merging. Tanner graph and parity-check matrix of the original code (a); of the derived supercode (b).

Encoding and modulation: Given two messages w_1, w_2 , the binary codewords u_1, u_2 are generated using nested codebooks C_1, C_2 . The codeword bits $u_{1,i}$ and $u_{2,i}$ are each mapped to real-valued BPSK symbols using the constellation mappings φ_1 and φ_2 , i.e.,

$$(x_{1,i}, x_{2,i}) = (\varphi_1(u_{1,i}), \varphi_2(u_{2,i})), \qquad i = 1, \dots, n$$
 (6)

where $\varphi_k \colon \mathbb{F}_2 \to X$ is defined as $\varphi_k(u_{k,i}) = \sqrt{P}(2u_{k,i} - 1)$ for k = 1, 2.

B. Decoding algorithm

Now we derive the decoding algorithm for the CFMA scheme using binary LDPC codes, and show that the same sum-product algorithm for the point-to-point LDPC decoding can be directly applied to our scheme with only a slight modification to the initialization step. We set $a_1 = a_2 = 1$, which is the only non-trivial choice for binary codes, since setting either a_1 or a_2 to zero will reduce the decoder to plain successive cancellation. Hence, we define $s = u_1 \oplus u_2$ and choose to derive the algorithm for decoding the pair (s, u_1) . The decoding of (s, u_2) is similar. Ideally, we target a bit-wise maximum *a posteriori* (MAP) estimation, i.e., $\operatorname{argmax}_{s_i \in \{0,1\}} p(s_i | y)$. However, since p(y|s) is not memoryless, the sum-product algorithm does not directly approximate the bit-wise MAP in this case. Nonetheless, as an approximation to the bit-wise MAP rule, we perform a bit-wise MAP estimation as follows:

$$\hat{s}_i = \underset{s_i \in \{0,1\}}{\operatorname{argmax}} \sum_{\sim s_i} \prod_{i=1}^n p(y_i | s_i) \mathbb{1} \big\{ \tilde{\boldsymbol{H}} \boldsymbol{s} = \boldsymbol{0} \big\},$$
(7)

where the summation is over all coordinates of s except s_i . Here, we have made use of the fact $s = u_1 \oplus u_2$ is uniformly distributed over \tilde{C} as a consequence of u_1 and u_2 being uniform over the nested codebooks C_1 and C_2 , respectively, hence $p(s) = \mathbb{1}\{\tilde{H}s = 0\}/|\tilde{C}|$ where \tilde{C} is the code with the larger rate among C_1, C_2 and \tilde{H} is its parity check matrix.

As shown in [7], the formulation in (7) already permits a low-complexity sum-product algorithm for the bit-wise MAP estimation of the sum codewords s. Also notice that the complexity of this algorithm is the same as for a point-to-point system where the receiver decodes one codeword from the code described by \tilde{H} .

Similarly, given the sum codeword $s = u_1 \oplus u_2 \in \tilde{C}$, the bit-wise MAP decoding of one codeword, say u_1 , is given by

$$\hat{u}_{1,i} = \underset{u_{1,i} \in \{0,1\}}{\operatorname{argmax}} p(u_{1,i} | \mathbf{y}, \mathbf{s})$$
$$= \underset{u_{1,i} \in \{0,1\}}{\operatorname{argmax}} \sum_{\sim u_{1,i}} \prod_{i=1}^{n} p(y_i | u_{1,i}, s_i) \mathbb{1} \{ \mathbf{H}_1 \mathbf{u}_1 = \mathbf{0} \}.$$
(8)

For the above equality we have used the fact that the channel is memoryless, as well as the fact that (u_1, s) is uniform over $C_1 \times \tilde{C}$, hence

$$p(\boldsymbol{u}_1, \boldsymbol{s}) = \frac{\mathbb{I}\{\boldsymbol{u}_1 \in C_1\}\mathbb{I}\{\boldsymbol{s} \in \tilde{C}\}}{|C_1| |\tilde{C}|},\tag{9}$$

where we recall that *s* is the decoded codeword from \tilde{C} hence it always holds that $s \in \tilde{C}$, namely $\mathbb{1}\left\{s \in \tilde{C}\right\} = 1$. Furthermore $u_1 \in C_1$ is equivalent to $H_1u_1 = 0$.

It is important to realize that both decoding steps (7) and (8) can be tackled by standard sum-product algorithms like those commonly used for LDPC decoding in point-to-point systems. Thus, CFMA decoding can be implemented efficiently using a standard sum-product algorithm, albeit with modified initial log-likelihood ratio (LLR) values:

LLR₁ :=
$$\log \frac{p(y_i|s_i = 0)}{p(y_i|s_i = 1)}$$

= $\log \frac{\cosh(y_i\sqrt{P}(h_1 + h_2))}{\cosh(y_i\sqrt{P}(h_1 - h_2))} - 2Ph_1h_2$ (10a)

$$LLR_{2} \coloneqq \log \frac{p(y_{i}|u_{1,i} - 0, s_{i})}{p(y_{i}|u_{1,i} = 1, s_{i})} \\ = \begin{cases} -2y_{i}\sqrt{P}(h_{1} + h_{2}) & \text{for } s_{i} = 0\\ -2y_{i}\sqrt{P}(h_{1} - h_{2}) & \text{for } s_{i} = 1 \end{cases}$$
(10b)

Algorithm 1 describes the decoding procedure for the CFMA scheme with binary LDPC codes. The function SPA(H, LLR) executes the standard sum-product algorithm on the Tanner graph given by the parity-check matrix H with initial input value LLR. Details and efficient implementations of this standard algorithm can be found in the literature, e.g. [8].

Algorithm 1 CFMA: Decoding algorithm with binary LDPC codes. LLR_1 and LLR_2 are given in (10).

1: $\hat{s} = \text{SPA}(\tilde{H}, \text{LLR}_1)$	\triangleright Decode the sum codeword <i>s</i>
2: $\hat{\boldsymbol{u}}_1 = \text{SPA}(\boldsymbol{H}_1, \text{LLR}_2)$	▶ Decode the codeword u_1
3: $\hat{\boldsymbol{u}}_2 = \hat{\boldsymbol{s}} \oplus \hat{\boldsymbol{u}}_1$	▶ Decode the codeword u_2

IV. NUMERICAL SIMULATIONS

In this section, we provide numerical simulations of our proposed CFMA codes and compare them with the theoretical limits described by Theorem 1. As regards the latter, we evaluate Theorem 1 with different discrete inputs.

Throughout our simulations we use the sum-product algorithm with maximum number of iterations set to 25. We assume that a rate pair (R_1, R_2) is achieved for a given power and channel gains if the bit-error rate (BER) is below 10^{-3} over 500 independent trials. We compare the corresponding value of transmit power against the value that achieves the target rate pair in Theorem 1 evaluated with discrete inputs.

For ease of presentation, for a fixed input distribution, we will reference the corner points of \mathcal{R}_{MAC-UI} as points A and B, and the corner points of $\mathcal{R}_{CFMA-UI}$ (for fixed coefficients a_1 and a_2) by A' and B' (cf. Figure 4).

A. CFMA: binary codes with BPSK modulation

In this scenario we set the pair of channel gains to $(h_1, h_2) = (1, \sqrt{3})$. The target rate pair is $(R_1, R_2) = (0.9742, 0.9355)$ which corresponds to the point B' shown in Figure 6 (evaluated based on Theorem 1). The LDPC blocksize is 4376. For this particular setup, points B and B' coincide with one of the corner points of rate region (4). The theoretical rate regions and performance evaluation for this case is given in Figures 6 and 7, respectively. We use the base LDPC code to construct our CFMA code rate R = 0.9355, and under the point-to-point AWGN channel, the code has 0.66 dB gap from the Shannon limit. On the other hand, our CFMA strategy has 0.846 dB gap from the corresponding theoretical bound.

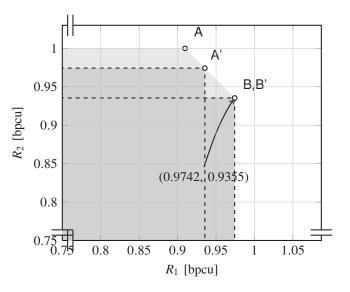


Fig. 6. Target rate pair B' for case of BPSK modulation. The point B' in this case achieves the corner point B of \mathcal{R}_{MAC-UI} . Note that axes are cropped.

B. CFMA: binary codes with 4-QAM modulation

In this scenario, we assume that the input symbols are complex-valued and set both channel gains to unity, i.e., $h_1 = h_2 = 1$. The target rate pair is $(R_1, R_2) = (1.885, 1.871)$,

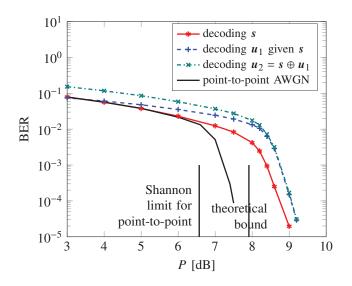


Fig. 7. Bit error rate simulation results for each decoding step for BPSK modulation and target rate pair $(R_1, R_2) = (0.9742, 0.9355)$. For reference, we include the base code performance (solid black line) and the corresponding Shannon limit for the binary-input AWGN channel.

and the LDPC blocksize is 4376. The theoretical rate regions and performance evaluation for this case is given in Figures 8 and 9, respectively. The base code is the same as in section IV-A. In the simulation for this case, we observe that our CFMA strategy has 1.57 dB gap from the corresponding theoretical bound.

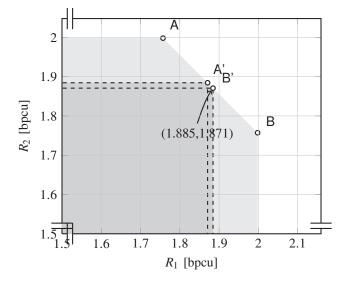


Fig. 8. Target rate pair B' for the 4-QAM modulation case. The achievable rate pair B' of the CFMA strategy achieves a non-endpoint on the dominant face of \mathcal{R}_{MAC-UI} . Note that axes are cropped.

V. CONCLUDING REMARKS

In this paper, we presented a practical CFMA coding strategy with sequential decoders that has low complexity comparable with that of point-to-point decoders. We have shown that the CFMA strategy achieves additional points on the dominant face of the joint decoding rate regions unlike the conventional successive cancellation strategy which is

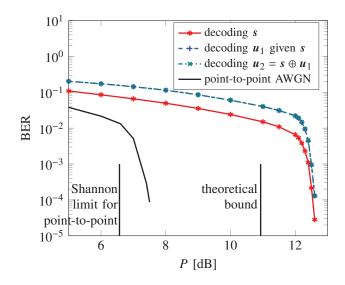


Fig. 9. Bit error rate simulation results for each decoding step for 4-QAM modulation and target rate pair $(R_1, R_2) = (1.885, 1.871)$. For reference, we include the base code performance (solid black line) and the corresponding Shannon limit for the binary-input AWGN channel.

restricted to the corner points. Several case studies have been presented with off-the-self point-to-point LDPC codes that show the potential of our strategy. This property itself can be desirable in many cases where backward compatibility is an issue. As future work, it would be interesting to see how the performance of the CFMA strategy can be improved by further optimization of the codes.

ACKNOWLEDGMENT

The authors would like to thank Chen Feng for his helpful discussions. This work was supported in part by the Swiss National Science Foundation under Grant 169294, Grant P2ELP2_165137 and by the Spanish government grant TEC2014-59255-C3-1-R.

References

- B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 364–375, 1996.
- [2] J. Zhu and M. Gastpar, "Gaussian Multiple Access via Compute-and-Forward," *IEEE Trans. Inf. Theory*, vol. 63, no. 5, May 2017.
- [3] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.
- [4] U. Erez and R. Zamir, "Achieving ¹/₂ log(1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.
- [5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.
- [6] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar, "A joint typicality approach to algebraic network information theory," *ArXiv eprints*, Jun. 2016, preprint available at http://arxiv.org/abs/1606.09548.
- [7] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge: Cambridge University Press, 2008.
- [8] X.-Y. Hu, E. Eleftheriou, D.-M. Arnold, and A. Dholakia, "Efficient implementations of the sum-product algorithm for decoding LDPC codes," in *IEEE Global Communications Conference (GLOBECOM)*, 2001.