On Compute-and-Forward with Feedback

Or Ordentlich
Tel Aviv University
ordent@eng.tau.ac.il

Uri Erez
Tel Aviv University
uri@eng.tau.ac.il

Bobak Nazer
Boston University
bobak@bu.edu

***Abstract*—We consider a Gaussian multiple-access channel where each user's message is identified with a vector of elements from a finite field, and the receiver's goal is to decode a linear combination of these finite field vectors. It is further assumed that each transmitter can causally observe the channel's output through a clean feedback link. We propose a novel coding scheme for this setup, which can be seen as an extension of the Cover-Leung scheme for the computation problem. This scheme is shown to achieve computation rates higher than the best known computation rates for the same scenario without feedback. In particular, for the symmetric two-user Gaussian multiple-access channel, the proposed scheme attains a symmetric computation rate greater than $1/2\log(3/4+\mathsf{SNR})$.**

I. Introduction

In the compute-and-forward framework [1], a receiver is interested in decoding a linear function of messages, rather than the individual messages themselves, from the output of a Gaussian multiple-access channel (MAC). This setup was originally motivated by considering a network where only a small subset of the nodes is interested in decoding the messages while the other nodes act as relays. In this scenario, a possible strategy for the relays is to decode functions of the messages and forward them down the network [1]. See the chapter [2] in the recent textbook of Zamir [3] for an overview of compute-and-forward and its applications.

Sometimes, the transmitters may have access to (a noisy version of) the signal seen by the receiver, through a feedback link. It is therefore natural to ask if and how the feedback link can be used to obtain improved performance. In this paper we propose a novel coding scheme for the noiseless feedback setup. This scheme can be seen as a variant of the Cover-Leung scheme [4], which was developed for communication over a MAC with feedback, under the standard setting where the receiver is interested in decoding the individual messages. Our scheme is based on the use of lattice codes and operates in two phases. In the first phase the receiver decodes a list of candidates for the desired linear function that contains the true value with high probability. This is enabled by invoking the lattice list decoder proposed by Song and Devroye [5]. Further, each transmitter uses its feedback link for decoding the message transmitted by the other user, which together with its own message allows it to compute the desired function. In the second phase, both users coherently transmit to the receiver information about the value of the function, that allows it to resolve the ambiguity from the first phase. The two phases are superimposed in block Markov fashion. It is shown that the computation rate achieved by the scheme above is higher than the best known computation rate without feedback.

For simplicity of exposition we consider a two-user MAC with clean feedback. However, our results can be easily extended to handle noisy feedback as well as more than two users, as briefly described in Section VI.

The work of O. Ordentlich was supported by the Admas Fellowship Program of the Israel Academy of Science and Humanities, a fellowship from The Yitzhak and Chaya Weinstein Research Institute for Signal Processing at Tel Aviv University, and the Feder Family Award. The work of U. Erez was supported by the Israel Science Foundation (ISF). The work of B. Nazer was supported by the National Science Foundation under grant CCF-1253918.

II. Problem Statement

We consider a discrete-time, real-valued, Gaussian multiple-access channel with two users

$$Y[t] = h_1 X_1[t] + h_2 X_2[t] + Z[t], \tag{1}$$

where $h_1, h_2 \in \mathbb{R}$ and $Z[t] \sim \mathcal{N}(0,1)$ is additive white Gaussian noise (AWGN). We assume that clean causal feedback is available for both users, i.e., before transmitting $X_i[t]$, each user has access to $\{Y[\ell]\}_{\ell=1}^{t-1}$.

Each user has a message vector $\mathbf{w}_i \in \mathbb{F}_p^k$, $i = 1, 2$, from a finite field of prime cardinality p. The message vectors are statistically independent and uniformly distributed over $\mathbb{F}_p^k$. The receiver is interested in decoding the linear combination

$$\mathbf{u} = \mathbf{w}_1 \oplus \mathbf{w}_2 \tag{2}$$

of the message vectors, where $\oplus$ denotes componentwise addition over $\mathbb{F}_p$. To that end, the channel (1) is used n times. The input of the ith user to the channel at time t is produced by an encoding function $\mathcal{E}_i^t : \mathbb{F}_p^k \times \mathbb{R}^{t-1} \mapsto \mathbb{R}$, such that $X_i[t] = \mathcal{E}_i^t\left(\mathbf{w}_i, \{Y[\ell]\}_{\ell=1}^{t-1}\right)$. The encoders are required to satisfy the power constraint $\sum_{t=1}^n \mathbb{E}(X_i^2[t]) \le n\mathsf{SNR}$. The receiver has a decoding function $\mathcal{D} : \mathbb{R}^n \mapsto \mathbb{F}_p^k$ that maps the channel outputs to an estimate $\hat{\mathbf{u}} = \mathcal{D}\left(\{Y[t]\}_{t=1}^n\right)$. The error probability is defined as $P_e \triangleq \Pr(\hat{\mathbf{u}} \neq \mathbf{u})$. A computation rate R is achievable if for any $\epsilon > 0$ and n large enough there exists an integer k, a prime number p, encoders $\{\mathcal{E}_1^t\}_{t=1}^n, \{\mathcal{E}_2^t\}_{t=1}^n$ and decoder $\mathcal{D}$ such that $P_e < \epsilon$ and $R = \frac{k}{n}\log p$.

Remark 1: In general, the receiver may be interested in a linear combination $\mathbf{u} = q_1\mathbf{w}_1 \oplus q_2\mathbf{w}_2$ for some $q_1, q_2 \in \mathbb{F}_p$. We claim, however, that there is no loss of generality in our assumption that $q_1 = q_2 = 1$, as the transmitters can simply encode $\tilde{\mathbf{w}}_i = q_i\mathbf{w}_i$ instead of $\mathbf{w}_i$.

III. Preliminaries

In this section, we recall several results that will be used in the derivation of our main result.

A. Compute-and-Forward

When feedback is not available, the problem defined in Section II reduces to the standard compute-and-forward problem introduced in [1], where a lattice-based transmission scheme was developed for this setup. Let $\Lambda \subseteq \Lambda_c \subset \mathbb{R}^n$ be a pair of n-dimensional nested lattices and denote the Voronoi region of Λ by $\mathcal{V}$ (see [3] for a comprehensive overview of lattice definitions). The codebook $\mathcal{C}$ is constructed as $\mathcal{C} = \Lambda_c \cap \mathcal{V}$ and its rate is $R = \log|\Lambda_c \cap \mathcal{V}| = \log\left(\frac{\mathrm{Vol}(\Lambda)}{\mathrm{Vol}(\Lambda_c)}\right)$.

In [1] it was shown that for any $R > 0$ and p large enough one can construct a sequence of nested lattice pairs where Λ is Rogers good with second moment $\sigma^2(\Lambda) = \mathsf{SNR}$, while Λ_c is Poltyrev good and Rogers good, and in addition there exists a one-to-one mapping function $\phi : \mathbb{F}_p^k \mapsto \mathcal{C}$ with the property that for any $a_1, a_2 \in \mathbb{Z}$

$$\phi^{-1}\left([a_1\phi(\mathbf{w}_1) + a_2\phi(\mathbf{w}_2)] \bmod \Lambda\right) = q_1\mathbf{w}_1 \oplus q_2\mathbf{w}_2, \quad (3)$$

where $q_i = [a_i] \bmod p$.

It follows that in order to decode a finite field linear combination $\mathbf{u} = q_1\mathbf{w}_1 \oplus q_2\mathbf{w}_2$, it suffices to decode an integer-linear combination $[a_1\phi(\mathbf{w}_1) + a_2\phi(\mathbf{w}_2)] \bmod \Lambda$ of the lattice points $\phi(\mathbf{w}_1)$ and $\phi(\mathbf{w}_2)$. In the sequel, we will therefore consider the problem of decoding integer-linear combinations of the lattice points transmitted by the two users, and bear in mind that this corresponds to decoding a finite field linear combination.

In the compute-and-forward scheme, each user maps its message $\mathbf{w}_i$ to a lattice point $\mathbf{t}_i = \phi(\mathbf{w}_i) \in \mathcal{C}$ and transmits $\mathbf{x}_i = [\mathbf{t}_i - \mathbf{d}_i] \bmod \Lambda$ over n consecutive channel uses, where $\mathbf{d}_1, \mathbf{d}_2$ are dither vectors uniformly distributed over $\mathcal{V}$, statistically independent of one another and of $(\mathbf{w}_1, \mathbf{w}_2)$. By the Crypto Lemma [3], [6], $\mathbf{x}_i$ is uniformly distributed on $\mathcal{V}$ and statistically independent of $\mathbf{t}_i$. In order to decode the integer-linear combination $\mathbf{v} = [a_1\mathbf{t}_1 + a_2\mathbf{t}_2] \bmod \Lambda$, the receiver computes

$$\mathbf{s} = [\alpha\mathbf{y} + a_1\mathbf{d}_1 + a_2\mathbf{d}_2] \bmod \Lambda = [\mathbf{v} + \mathbf{z}_{\text{eff}}] \bmod \Lambda$$

where

$$\mathbf{z}_{\text{eff}} = (\alpha h_1 - a_1)\mathbf{x}_1 + (\alpha h_2 - a_2)\mathbf{x}_2 + \alpha\mathbf{z}$$

is a mixture of dither vectors and Gaussian noise which is statistically independent of $\mathbf{v}$, whose effective variance is

$$\sigma^2_{\text{eff}} \triangleq \frac{1}{n}\mathbb{E}\|\mathbf{z}_{\text{eff}}\|^2 = \left((\alpha h_1 - a_1)^2 + (\alpha h_2 - a_2)^2\right)\mathsf{SNR} + \alpha^2.$$

In [1], [6] it is shown that if

$$R < \frac{1}{2}\log\left(\frac{\mathsf{SNR}}{\sigma^2_{\text{eff}}}\right) \quad (4)$$

then $\Pr(\mathbf{z}_{\text{eff}} \notin \mathcal{V}_c) \to 0$ as n increases. Subsequently, if we set $\hat{\mathbf{v}} = Q_{\Lambda_c}(\mathbf{s})$, where $Q_{\Lambda_c}(\cdot)$ is the nearest neighbor quantizer w.r.t. the lattice Λ_c, we have that $\Pr(\hat{\mathbf{v}} \neq \mathbf{v}) \to 0$ as long as (4) is satisfied. Minimizing σ^2_{eff} w.r.t. α we see that $\mathbf{v} = [a_1\mathbf{t}_1 + a_2\mathbf{t}_2] \bmod \Lambda$ can be reliably decoded if [1], [7]

$$\begin{aligned} R &< R_{\text{comp}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR}) \\ &\triangleq \frac{1}{2}\log\left(1 + \|\mathbf{h}\|^2\mathsf{SNR}\right) \\ &\quad - \frac{1}{2}\log\left(\|\mathbf{a}\|^2 + \mathsf{SNR}(\|\mathbf{a}\|^2\|\mathbf{h}\|^2 - (\mathbf{a}^T\mathbf{h})^2)\right) \end{aligned} \quad (5)$$

where $\mathbf{h} = [h_1 \ h_2]$ and $\mathbf{a} = [a_1 \ a_2]$.

B. Lattice List Decoding

We have seen that it is possible to reliably decode $\mathbf{v}$ if $R < R_{\text{comp}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR})$. If $R > R_{\text{comp}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR})$, the compute-and-forward scheme does not allow for reliable decoding. Instead, in this case we would like to decode a list of candidates that contains $\mathbf{v}$ with high probability and whose size is as small as possible. This problem was studied by Song and Devroye in [5] (see also the related work [8], [9]) and the following theorem was proved.

Theorem 1: [5, Thm. 3 rephrased] Let $\mathcal{C} = \Lambda_c \cap \mathcal{V}$ be a lattice codebook with rate R, based on the nested lattice pair $\Lambda \subseteq \Lambda_c \subset \mathbb{R}^n$ with $\sigma^2(\Lambda) = \mathsf{SNR}$. Let $\mathbf{v} \in \mathcal{C}$, and let $\mathbf{z}_{\text{eff}}$ be a linear combination of AWGN and statistically independent dither vectors uniformly distributed over $\mathcal{V}$ whose effective variance is $\sigma^2_{\text{eff}} = \frac{1}{n}\mathbb{E}\|\mathbf{z}_{\text{eff}}\|^2$. Further, let $R_c = \frac{1}{2}\log\left(\frac{\mathsf{SNR}}{\sigma^2_{\text{eff}}}\right)$. For any $\epsilon > 0$, $\delta > 0$, $R > R_c$, SNR and n large enough there exists a nested lattice pair $\Lambda \subseteq \Lambda_c \subset \mathbb{R}^n$ such that one can use the observation $\mathbf{s} = [\mathbf{v} + \mathbf{z}_{\text{eff}}] \bmod \Lambda$ to produce a list L of no more than $2^{n(R-R_c+\delta)}$ codewords from $\mathcal{C}$ that contains $\mathbf{v}$ with probability greater than $1 - \epsilon$, where

Sketch of proof. The full proof can be found in [5]. For completeness, we provide a proof sketch. Construct a chain of nested lattices $\Lambda \subseteq \Lambda_s \subseteq \Lambda_c$ such that Λ_c, Λ_s are Rogers and Poltyrev good and Λ is Rogers good and in addition

$$\frac{1}{n}\log\left(\frac{\mathrm{Vol}(\Lambda)}{\mathrm{Vol}(\Lambda_c)}\right) = R, \qquad \frac{1}{n}\log\left(\frac{\mathrm{Vol}(\Lambda)}{\mathrm{Vol}(\Lambda_s)}\right) = R_c - \delta$$

which implies that $\frac{1}{n}\log\left(\frac{\mathrm{Vol}(\Lambda_s)}{\mathrm{Vol}(\Lambda_c)}\right) = R - R_c + \delta$. We construct the codebook $\mathcal{C} = \Lambda_c \cap \mathcal{V}$ and the virtual codebook $\mathcal{C}_s = \Lambda_s \cap \mathcal{V}$. The list L consists of all points in $\mathcal{C}$ that fall inside $[\mathbf{s} + \mathcal{V}_s] \bmod \Lambda$, i.e.,

$$L = \{\mathbf{c} \in \mathcal{C} : \mathbf{c} \in [\mathbf{s} + \mathcal{V}_s] \bmod \Lambda\}.$$

Since $\mathbf{s} = [\mathbf{v} + \mathbf{z}_{\text{eff}}] \bmod \Lambda$, we have that a sufficient condition for $\mathbf{v} \in L$ is that $\mathbf{z}_{\text{eff}} \in -\mathcal{V}_s$. Recalling that a Voronoi region is centro-symmetric, this is equivalent to the condition $\mathbf{z}_{\text{eff}} \in \mathcal{V}_s$. Since the virtual codebook $\mathcal{C}_s$ with rate $R_c - \delta$ is constructed from a good nested lattice pair, we have from (4) that $\Pr(\mathbf{z}_{\text{eff}} \notin \mathcal{V}_s) \to 0$. Thus, $\mathbf{v} \in L$ with high probability. Moreover, $[\mathbf{s} + \mathcal{V}_s] \bmod \Lambda$ is a fundamental cell of Λ_s, and since $\Lambda_s \subseteq \Lambda_c$, we have that $\frac{1}{n}|L| = \frac{1}{n}\log\left(\frac{\mathrm{Vol}(\Lambda_s)}{\mathrm{Vol}(\Lambda_c)}\right) = R - R_c + \delta$. ■

Remark 2: It can be shown that the nested lattice chain $\Lambda \subseteq \Lambda_s \subseteq \Lambda_c$ from the proof can be constructed such that there

will exist a one-to-one mapping function $\phi : \mathbb{F}_p^k \mapsto \mathcal{C}$ with the property (3). Moreover, the requirements that the lattices in the chain are Poltyrev and Rogers good is over restrictive. Instead of Rogers goodness, it suffices to require MSE goodness, and instead of Poltyrev goodness, it suffices to require goodness under nearest neighbor coset decoding, see [10].

We will need the following corollary of Theorem 1.

Corollary 1: For any $\epsilon > 0$, $\delta > 0$, $R > R_{\text{comp}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR})$ and n large enough it is possible to use the output of the channel (1) to decode a list of size no greater than $2^{n(R-R_{\text{comp}}(\mathbf{h},\mathbf{a},\mathsf{SNR})+\delta)}$ that contains $\mathbf{v} = [a_1\mathbf{t}_1 + a_2\mathbf{t}_2] \bmod \Lambda$ with probability greater than $1-\epsilon$.

IV. Main Result

In this section, we propose a coding scheme for compute-and-forward with feedback. This scheme can be seen as an extension of the Cover-Leung scheme [4] for the MAC with feedback. The scheme works in a block Markov fashion, where at each block each of the transmitters sends a superposition of a codeword that corresponds to new information, and a codeword that correspond to the finite field sum of both users' messages from the previous block. The latter codeword is sent coherently by both users, which is enabled through the available feedback. The following theorem describes the computation rate achieved by this scheme.

Theorem 2 (Computation rate with feedback): Consider the MAC (1) with clean feedback and assume w.l.o.g. that $0 < h_2 \le h_1$. For any $0 < \rho \le 1$ let

$$\rho_1 = 1 - (1-\rho)\left(\frac{h_2}{h_1}\right)^2,$$
$$R_c = \frac{1}{2}\log^+\left(\frac{1}{2} + (1-\rho)h_2^2\mathsf{SNR}\right),$$
$$R' = \frac{1}{2}\log\left(1 + \frac{(h_1\sqrt{\rho_1} + h_2\sqrt{\rho})^2\mathsf{SNR}}{1 + 2(1-\rho)h_2^2\mathsf{SNR}}\right).$$

Any computation rate satisfying

$$R < \max_{0<\rho\le 1} \min\left(R' + R_c, \frac{1}{2}\log\left(1 + (1-\rho)h_2^2\mathsf{SNR}\right)\right) \quad (6)$$

is achievable.

Proof. Let $\Lambda \subseteq \Lambda_c \subset \mathbb{R}^{\tilde{n}}$ be a nested lattice pair satisfying the conditions of Theorem 1, and let $\mathcal{C} = \Lambda_c \cap \mathcal{V}$ be the corresponding codebook of rate $R = \frac{\tilde{k}}{\tilde{n}}\log p$ with a one-to-one mapping function $\phi : \mathbb{F}_p^{\tilde{k}} \mapsto \mathcal{C}$ that satisfies (3).[1] In addition, we will use another "good" nested lattice codebook $\mathcal{C}' = \Lambda_c' \cap \mathcal{V}'$ with rate R' based on the nested lattice pair $\Lambda' \subseteq \Lambda_c' \subset \mathbb{R}^{\tilde{n}}$ where $\sigma^2(\Lambda') = \mathsf{SNR}$. We further define a random binning function $\mathbf{B} : \mathbb{F}_p^{\tilde{k}} \mapsto \{1, \ldots, 2^{\tilde{n}R'}\}$ for $0 < R' < R$ as follows: for each $\mathbf{w} \in \mathbb{F}_p^{\tilde{k}}$ draw the value of $\mathbf{B}(\mathbf{w})$ from the uniform distribution over $\{1, \ldots, 2^{\tilde{n}R'}\}$ in a statistically independent manner. As usual, we will show that the expected error probability achieved by the scheme described below w.r.t. the ensemble of binning functions is small, and then deduce that there exists a fixed binning function that achieves a small error probability.

Our scheme operates in a block Markov fashion, and the feedback is also only used in blocks. Each user has N finite field messages $\{\mathbf{w}_i^{(m)}\}_{m=1}^N$, $i = 1, 2$, each uniform on $\mathbb{F}_p^{\tilde{k}}$. Let $0 < \rho_1 \le 1$, $0 < \rho_2 \le 1$. For the first block, user i encodes its message $\mathbf{w}_i^{(1)}$ to $\tilde{\mathbf{x}}_i^{(1)} = [\mathbf{t}_i^{(1)} - \mathbf{d}_i^{(1)}] \bmod \Lambda$ where $\mathbf{t}_i^{(1)} = \phi(\mathbf{w}_i^{(1)})$ and all dither vectors $\{\mathbf{d}_i^{(m)}\}$ are statistically independent and uniformly distributed over $\mathcal{V}$. It then transmits

$$\mathbf{x}_i^{(1)} = \sqrt{1-\rho_i}\tilde{\mathbf{x}}_i^{(1)}. \quad (7)$$

The receiver observes

$$\mathbf{y}^{(1)} = \sqrt{1-\rho_1}h_1\tilde{\mathbf{x}}_1^{(1)} + \sqrt{1-\rho_2}h_2\tilde{\mathbf{x}}_2^{(1)} + \mathbf{z}^{(1)}, \quad (8)$$

from which it decodes a list of candidates for $\mathbf{v}^{(1)} = [\mathbf{t}_1^{(1)} + \mathbf{t}_2^{(1)}] \bmod \Lambda$.[2] By Theorem 1, assuming that $R > \tilde{R}_c = R_{\text{comp}}([\sqrt{1-\rho_1}h_1 \ \sqrt{1-\rho_2}h_2], [1\ 1], \mathsf{SNR})$ it can decode a list $L^{(1)}$ of size

$$|L^{(1)}| = 2^{\tilde{n}(R-\tilde{R}_c+\delta)} \quad (9)$$

codewords, that contains $\mathbf{v}^{(1)}$ with high probability. Applying the inverse mapping $\phi^{-1}(\cdot)$ to each codeword in the list, we get a list of members in $\mathbb{F}_p^{\tilde{k}}$ of size $|L^{(1)}|$, that contains $\mathbf{u}^{(1)} = \mathbf{w}_1^{(1)} \oplus \mathbf{w}_2^{(1)}$ with high probability.

Let $\bar{i} = \{1,2\} \setminus \{i\}$. Since user i obtains $\mathbf{y}^{(1)}$ by the feedback link, it can cancel out its own signal from it and construct the observation

$$\mathbf{y}_i(1) = \sqrt{1-\rho_{\bar{i}}}h_{\bar{i}}\tilde{\mathbf{x}}_{\bar{i}}^{(1)} + \mathbf{z}^{(1)} \quad (10)$$

from which it can decode the other user's message $\mathbf{w}_{\bar{i}}^{(1)}$ as long as

$$R < \frac{1}{2}\log\left(1 + (1-\rho_{\bar{i}})h_{\bar{i}}^2\mathsf{SNR}\right). \quad (11)$$

It follows that, if (11) holds, before the second block begins each user should have access to both $\mathbf{w}_1^{(1)}$ and $\mathbf{w}_2^{(1)}$, and consequently both users have access to $\mathbf{u}^{(1)} \in \mathbb{F}_p^{\tilde{k}}$. Each user then applies the binning function on $\mathbf{u}^{(1)}$ to obtain $\mathbf{b}^{(1)} = B(\mathbf{u}^{(1)}) \in \{1, \ldots, 2^{\tilde{n}R'}\}$, maps it to a codeword $\mathbf{t}'^{(1)} \in \mathcal{C}'$ and produces $\mathbf{x}_{\text{cohr}}^{(1)} = [\mathbf{t}'^{(1)} - \mathbf{d}'^{(1)}] \bmod \Lambda$, where the dither vector $\mathbf{d}'^{(1)}$ is common to both users and is uniformly distributed on $\mathcal{V}'$. In addition, each user encodes its new message $\mathbf{w}_i^{(2)}$ to $\tilde{\mathbf{x}}_i^{(2)}$ in the same manner as in the first block, and transmits

$$\mathbf{x}_i^{(2)} = \sqrt{\rho_i}\mathbf{x}_{\text{cohr}}^{(1)} + \sqrt{1-\rho_i}\tilde{\mathbf{x}}_i^{(2)} \quad (12)$$

[1] We use the notation $\tilde{n}$ and $\tilde{k}$, rather than n and k, to emphasize the fact that these integers correspond to the length and rate of one block in our block Markov scheme, rather than the length and rate of the whole transmission scheme.

[2] Equivalently, the receiver could have attempted to decode a list for a different linear combination $[a_1\mathbf{t}_1^{(1)} + a_2\mathbf{t}_2^{(1)}] \bmod \Lambda$, $a_1, a_2 \neq 0$. However, the choice $a_1 = a_2 = 1$ allows for using smaller values of ρ_1, ρ_2 than other choices, and this leaves more available power for coherent transmission.

The receiver therefore obtains

$$\mathbf{y}^{(2)} = (\sqrt{\rho_1}h_1 + \sqrt{\rho_2}h_2)\mathbf{x}_{\text{cohr}}^{(1)} + \sqrt{1-\rho_1}h_1\tilde{\mathbf{x}}_1^{(2)} + \sqrt{1-\rho_2}h_2\tilde{\mathbf{x}}_2^{(2)} + \mathbf{z}^{(2)}. \quad (13)$$

The term

$$\tilde{\mathbf{z}}^{(2)} = \sqrt{1-\rho_1}h_1\tilde{\mathbf{x}}_1^{(2)} + \sqrt{1-\rho_2}h_2\tilde{\mathbf{x}}_2^{(2)} + \mathbf{z}^{(2)} \quad (14)$$

is a mixture of AWGN and independent dither vectors from Rogers good lattices, with effective variance

$$\tfrac{1}{n}\mathbb{E}\|\tilde{\mathbf{z}}^{(2)}\|^2 = 1 + \left((1-\rho_1)h_1^2 + (1-\rho_2)h_2^2\right)\mathsf{SNR}. \quad (15)$$

Thus, the receiver can decode $\mathbf{t}'^{(1)}$ from $\mathbf{y}^{(2)}$ provided that

$$R' \le \frac{1}{2}\log\left(1 + \frac{(\sqrt{\rho_1}h_1 + \sqrt{\rho_2}h_2)^2\mathsf{SNR}}{1 + ((1-\rho_1)h_1^2 + (1-\rho_2)h_2^2)\,\mathsf{SNR}}\right). \quad (16)$$

After decoding $\mathbf{t}'^{(1)}$ the receiver has access to $\mathbf{b}^{(1)}$, and from the previous block it also has access to a list of candidates $L^{(1)}$ for $\mathbf{u}^{(1)}$. The receiver now intersects the list $L^{(1)}$ with the set $B^{-1}(\mathbf{b}^{(1)})$ of all vectors in $\mathbb{F}_p^{\tilde{k}}$ that are mapped to $\mathbf{b}^{(1)}$ by the binning function $B(\cdot)$. If it finds a unique vector in the intersection it outputs it as $\hat{\mathbf{u}}^{(1)}$ and otherwise it declares an error. Assume the following events occurred:

1) the list $L^{(1)}$ contains $\mathbf{u}^{(1)}$;
2) each user i decoded the other user's message $\mathbf{w}_{\tilde{i}}^{(1)}$ correctly from $\mathbf{y}_i^{(1)}$;
3) The receiver decoded $\mathbf{t}'^{(1)}$ correctly from $\mathbf{y}^{(2)}$.

In this case, the true linear combination $\mathbf{u}^{(1)}$ is guaranteed to be in the intersection. The probability that all three events occur approaches 1 with the dimension if (9), (11) and (16) hold. The probability that some $\mathbf{u}' \neq \mathbf{u}^{(1)}$ falls in the intersection of the two lists can be bounded using the union bound and the uniform independent assignment of bins to message vectors as

$$\Pr\left(\bigcup_{\mathbf{w}\in L^{(1)}}\left\{B(\mathbf{w}) = \mathbf{b}^{(1)}\right\}\right) \le |L^{(1)}|2^{-\tilde{n}R'} = 2^{\tilde{n}(\delta + R - \tilde{R}_c - R')}$$

which vanishes as long as

$$R < R' + \tilde{R}_c - \delta. \quad (17)$$

If $\mathbf{u}^{(1)}$ is decoded successfully, the decoder can cancel out the contribution of $\mathbf{x}_{\text{cohr}}^{(1)}$ from $\mathbf{y}^{(2)}$ and produce

$$\tilde{\mathbf{y}}^{(2)} = \sqrt{1-\rho_1}h_1\tilde{\mathbf{x}}_1^{(2)} + \sqrt{1-\rho_2}h_2\tilde{\mathbf{x}}_2^{(2)} + \mathbf{z}^{(2)} \quad (18)$$

from which it can decode a new list $L^{(2)}$ that contains $\mathbf{u}^{(2)}$ with high probability. Similarly, each encoder can use the feedback link to decode $\mathbf{w}_{\tilde{i}}^{(2)}$ such that $\mathbf{u}^{(2)}$ can be produced, binned, and coherently transmitted by both users in the next block, superimposed on a new message. This process goes on until the $(N+1)$th block where the users only transmit coherently the bin of $\mathbf{u}^{(N)}$ without superimposing new information. Thus, after $N+1$ blocks the receiver can decode N linear combination vectors, meaning that the effective rate is reduced to $RN/(N+1)$ which can be made as close as desired to R by increasing N.

Equations (11), (16) and (17) give an achievable computation rate as a function of ρ_1, ρ_2. In general, we may optimize this rate over all $0 < \rho_1, \rho_2 \le 1$. To simplify the expressions, we choose a possibly suboptimal assignment of ρ_1, ρ_2 that satisfies $(1-\rho_1)h_1^2 = (1-\rho_2)h_2^2$. This assignment ensures that both coefficients in the effective channel (8) are equal, which results in a high computation rate, and in addition balances the constraints (11) for correct decoding of the other user's message via the feedback link. Setting $\rho_2 = \rho$, our achievable computation rate takes the form of the solution to the single parameter optimization problem described in the theorem. ■

V. Performance Comparison

A. Compute-and-Forward with Full CSI

In order to compare the performance our scheme to compute-and-forward with no feedback, we will need to develop a suitable benchmark. The computation rate $R_{\text{comp}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR})$ given in (4) does not require channel state information (CSI) at the transmitters. However, if CSI is available at the transmitters, they can scale their signals prior to transmission in order to make the channel gains more favorable. In our setting, it is assumed that clean feedback from the receiver is available for both users, and in particular this implies that the transmitters should have the same CSI as the receiver. Thus, we will use the performance of compute-and-forward with full CSI at the transmitters as our benchmark for evaluating the gains obtained by our feedback scheme. We now derive an expression for the computation rate achieved by compute-and-forward with optimal scaling of the signals prior to transmission.

First note that each user can scale its signal by a factor $0 < g_i \le 1$ prior to transmission without violating the power constraint. Therefore, the transmitters can induce any effective channel in the rectangle

$$\tilde{\mathcal{H}} \triangleq \left\{\tilde{h} = [\tilde{h}_1\ \tilde{h}_2]\ :\ 0 < \tilde{h}_1 \le h_1,\ 0 < \tilde{h}_2 \le h_2\right\}.$$

and the computation rate with CSI can be increased to

$$R_{\text{comp}}^{\text{CSI}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR}) \triangleq \max_{\tilde{\mathbf{h}}\in\tilde{\mathcal{H}}} R_{\text{comp}}(\tilde{\mathbf{h}}, \mathbf{a}, \mathsf{SNR}). \quad (19)$$

We can rewrite (5) as

$$R_{\text{comp}}(\mathbf{h}, \mathbf{a}, \mathsf{SNR}) = \frac{1}{2}\log\left(\frac{1 + \|\mathbf{h}\|^2\mathsf{SNR}}{\|\mathbf{a}\|^2(1 + \|\mathbf{h}\|^2\mathsf{SNR}\sin^2(\theta))}\right),$$

where $\theta \in [-\pi, \pi)$ is the angle between the vectors $\mathbf{a}$ and $\mathbf{h}$, i.e., $\cos(\theta) = (\mathbf{a}^T\mathbf{h})/(\|\mathbf{a}\| \cdot \|\mathbf{h}\|)$. Note that for a fixed θ the computation rate above is monotonically increasing in $\|\mathbf{h}\|^2$. This implies that the maximum in the RHS of (19) is obtained on the boundary of $\tilde{\mathcal{H}}$ defined as

$$\bar{\mathcal{H}} = \{[h_1\ y]\ :\ 0 < y \le h_2\} \bigcup \{[x\ h_2]\ :\ 0 < x \le h_1\}.$$

To summarize, we obtained[3]

$$R_{\text{comp}}^{\text{CSI}}(\mathbf{h},\mathbf{a},\mathsf{SNR}) = \max_{\bar{\mathbf{h}}\in\mathcal{H}} R_{\text{comp}}(\bar{\mathbf{h}},\mathbf{a},\mathsf{SNR}). \quad (20)$$

B. Numerical Evaluation of the Obtained Rate

Figure 1 shows the achievable computation rate with feedback given in Theorem 2. For reference we also plot three additional curves: The computation rate with full CSI, given by (20), optimized over all integer vectors $\mathbf{a}\in\mathbb{Z}^2$ where both a_1 and a_2 are different than zero; The symmetric capacity of the MAC (1) with clean feedback [11]

$$C_{\text{sym}}^{\text{feed}} = \max_{0\le\rho\le 1} \min\left(\frac{1}{2}\log\left(1+\mathsf{SNR}(1-\rho^2)\min\{h_1^2,h_2^2\}\right), \frac{1}{4}\log\left(1+\mathsf{SNR}(h_1^2+h_2^2+2\rho|h_1h_2|)\right)\right).$$

Clearly, the linear combination $\mathbf{u}$ can be decoded by first decoding both messages and then computing their sum, which we refer to as *separation*; An upper bound on the computation rate with feedback, given by $\frac{1}{2}\log(1+\mathsf{SNR}\min\{h_1^2,h_2^2\})$. To see why this is an upper bound on the computation rate with feedback observe that if the receiver can decode $\mathbf{u}$, then due to the feedback link so can each of the users. But since each user sees the other user's signal through an AWGN channel, the computation rate with feedback cannot exceed the capacity of the corresponding AWGN channel (which is not increased when feedback is available).

We note that in the special case where $h_1 = h_2 = 1$ the computation rate without feedback is $\frac{1}{2}\log^+(\frac{1}{2}+\mathsf{SNR})$. Taking the suboptimal choice $\rho = 1/4\mathsf{SNR}$ in (6) yields $R \ge \frac{1}{2}\log^+(\frac{3}{4}+\mathsf{SNR})$.

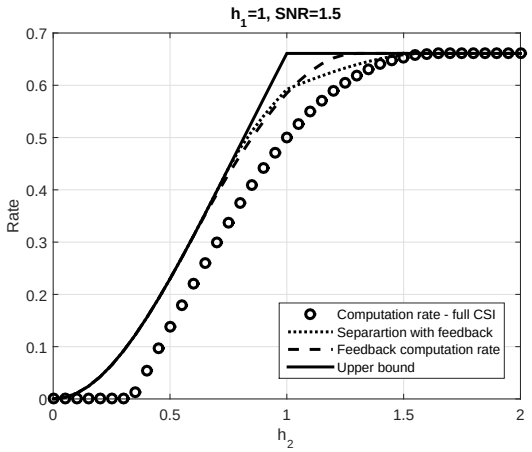

Fig. 1. Numerical evaluation of the computation rate without feedback but with full CSI, the symmetric capacity for decoding both messages when clean feedback is available, the computation rate with feedback from Theorem 2, and an upper bound

[3]We note that some improvement may be obtained by time-sharing between different power allocations. This, however, is outside the scope of this paper.

VI. Summary and Extensions

We have presented a scheme for decoding a linear combination of finite field messages over a Gaussian two-user MAC with clean feedback. Our scheme outperforms the best achievable computation rates without feedback, and for certain regimes of parameters, it also outperforms a separation strategy over the MAC with clean feedback.

We now comment on two possible extensions of our results. First, we have assumed throughout that the feedback is clean. However, since the feedback link is only exploited in blocks by each user for decoding the other user's message, Theorem 2 can be generalized to the case of noisy feedback by modifying the rate constraint (11) to allow for decoding over a more noisy channel. Second, we can consider a Gaussian MAC with K-users, $K>2$, where each user has the channel's output as feedback, and the receiver is interested in decoding the finite field sum of all messages. Here, each user can exploit the feedback link for decoding the finite field sum of the remaining $K-1$ users. In this case, the rate constraint (11) should be modified to the compound computation rate of the finite field sum over all different K possible multiple-access channels with $K-1$ users, obtained by removing one of the users from the original K-user MAC.

An interesting question for future research is whether it is possible to develop a low-complexity scalar scheme (à la [12], [11], [13]) for compute-and-forward with clean feedback, that achieves higher rates than a separation based MAC feedback scheme.

References

[1] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. IT*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[2] B. Nazer and R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge University Press, 2014, ch. Gaussian Networks.

[3] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge: Cambridge University Press, 2014.

[4] T. M. Cover and C. S. K. Leung, "An achievable rate region for the multiple-access channel with feedback," *IEEE Trans. IT*, vol. 27, no. 3, pp. 292–298, May 1981.

[5] Y. Song and N. Devroye, "Lattice codes for the gaussian relay channel: Decode-and-forward and compress-and-forward," *IEEE Trans. IT*, vol. 59, no. 8, pp. 4927–4948, Aug. 2013.

[6] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans IT*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[7] U. Niesen and P. Whiting, "The degrees of freedom of compute-and-forward," *IEEE Trans. IT*, vol. 58, no. 8, pp. 5214–5232, Aug. 2012.

[8] M. Nokleby and B. Aazhang, "Cooperative compute-and-forward," 2012, available online: http://arxiv.org/abs/1203.0695.

[9] M. Nokleby, B. Nazer, B. Aazhang, and N. Devroye, "Relays that cooperate to compute," in *Proceedings of ISWCS*, 2012, pp. 266–270.

[10] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," in *Proceedings of IEEEI*, 2012, pp. 1–12.

[11] L. H. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. IT*, vol. 30, no. 4, pp. 623–629, July 1984.

[12] J. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback–i: No bandwidth constraint," *IEEE Trans. IT*, vol. 12, no. 2, pp. 172–182, Apr 1966.

[13] L. Ozarow and S. Leung-Yan-Cheong, "An achievable region and outer bound for the Gaussian broadcast channel with feedback (corresp.)," *IEEE Trans. IT*, vol. 30, no. 4, pp. 667–671, Jul 1984.