Reliable Computation over Multiple-Access Channels

Bobak Nazer and Michael Gastpar
Dept. of Electrical Engineering and Computer Sciences
University of California, Berkeley
Berkeley, CA, 94720-1770
{bobak, gastpar}@eecs.berkeley.edu

Abstract

In the standard multiple-access problem, a central access point needs to reconstruct the signals observed by each user separately. Suppose now that the access point only reconstructs the *sum* (or any other function) of these observed signals. For this problem, we develop strategies and information-theoretic performance bounds. It is shown that in general, separating source from channel coding leads to suboptimal performance. For linear functions, a scheme is developed, analyzed, and shown to perform optimally for a class of multiple-access channels.

1 Introduction

Computing and communicating functions in a distributed fashion is to date an unsolved problem. On top of taking advantage of source dependencies, there are potential gains to be made by using the structure of the function in the coding scheme. Solutions to this problem are of practical interest to distributed computation systems such as sensor networks. Sending functions using sensor network protocols was studied in [1]; however, their setting was not information theoretic.

As was shown in [2], separation is not always optimal for communication over MACs. In this paper, we will show that even when the sources are independent, joint source-channel encoding may be required for optimally communicating a function. We develop a joint source-channel strategy that exploits the natural operation of the channel to send linear functions. This technique was implicitly used in [3] to achieve asymptotically optimal distortion per unit cost with uncoded transmission and in [4] for asymptotically efficient parameter estimation. We focus on using block codes to send the desired function in an undistorted fashion across the channel.

We begin our analysis with a rather simple MAC with some nice properties. For this channel, we can easily give a full characterization of the separation and computation coding schemes. Afterwards, we extend the key ideas of the example to a larger class of MACS. Finally, we show some preliminary work for sending functions over unmatched channels and computation over Gaussian MACs.

2 The Mod-2 Adder MAC: An Inspiring Example

Our example centers on the mod-2 adder MAC (M2MAC) (Figure 1). The vector source (S_1, S_2) is generated iid from the following joint probability distribution function (pdf):

$$\Pr(S_1 = 0, S_2 = 0) = \Pr(S_1 = 1, S_2 = 1) = \frac{1-p}{2} \quad (1)$$

$$\Pr(S_1 = 0, S_2 = 1) = \Pr(S_1 = 1, S_2 = 0) = \frac{p}{2} \quad (2)$$

$$(3)$$

A simple calculation will show that S_1 and S_2 have uniform marginal distributions. Each source is seen by a block encoder:

$$f_1 : \{0,1\}^{k_1} \to \{0,1\}^n \quad (4)$$

$$f_2 : \{0,1\}^{k_2} \to \{0,1\}^n \quad (5)$$

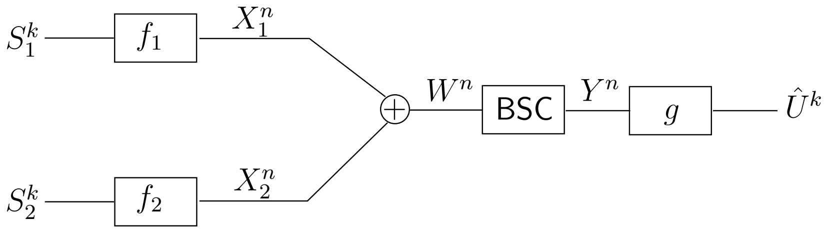

Figure 1: The Binary Mod-2 Adder MAC (M2MAC)

Our goal is to losslessly transmit $U = S_1 \oplus S_2$ across the channel at the highest rate possible. We denote the encoder outputs by X_1 and X_2. These are combined with a mod-2 addition to yield W and are passed through a binary symmetric channel (BSC) with crossover probability q to give Y. Finally, Y is decoded by a block decoder

$$g : \{0,1\}^n \to \{0,1\}^k \quad (6)$$

to give an estimate of the source parity, $\hat{U}$. We say that we can reliably communicate U over the MAC at a *computation rate* of $\kappa = \frac{k}{n}$ if we can guarantee:

$$\lim_{k\to\infty} \Pr(U^k \neq \hat{U}^k) \to 0 \quad (7)$$

2.1 Separation: Körner-Marton Revisited

We define separation to mean that successful transmission is guaranteed iff the rate region for distributed source coding (with respect to the computation distortion measure) intersects the MAC capacity region. In the case where the rates are symmetric throughout, only the sum rates are pertinent.

2.1.1 Channel Coding

The MAC capacity region is known [5, p.389]. The region is the closure of the convex hull of all rate pairs, (R_1, R_2), satisfying the following constraints:

$$R_1 < I(X_1; Y|X_2) \quad (8)$$

$$R_2 < I(X_2; Y|X_1) \quad (9)$$

$$R_1 + R_2 < I(X_1, X_2; Y) \quad (10)$$

for any distribution $p(x_1)p(x_2)$. See (pp.393-402, [5]) for the achievability and converse proofs. For the M2MAC, this region can easily be worked out to be:

$$R_1 + R_2 < 1 - h_B(q), \quad \text{where } h_B(q) = -q\log_2 q - (1-q)\log_2(1-q) \tag{11}$$

2.1.2 Source Coding

The rate region for distributed source coding of the mod-2 sum, $U = S_1 \oplus S_2$ was derived by Körner and Marton in [6]. Crucial to their proof is a linear source coding technique due to Wyner [7] which is given in the following lemma. First note that a lowercase, bold version of a random variable represents a length ℓ sequence in row form where ℓ can always be inferred from context. For example, $\mathbf{x} = (X[1], X[2], \ldots X[\ell])$.

Lemma 1. *For any iid $\mathcal{B}(p)$ source S, $\epsilon > 0$ and m large enough, there exists a binary $k \times m$ encoding matrix $\mathbf{H}$ with associated decoding function $b(.)$ such that $Pr(b(\mathbf{sH}) \neq \mathbf{s}) < \epsilon$ if $k < mh_B(p)$.*

See [7] for a complete proof. Korner and Marton [6] use Lemma 1 to give the distributed source coding region for the sum U. Their main result is reproduced below as Lemma 2.

Lemma 2. *S_1^k and S_2^k from the M2MAC are separately encoded by two source coders at rates R_1 and R_2. The mod-2 sum, U, can be reconstructed with $Pr(\hat{U}^k \neq U^k) < \epsilon \; \forall \epsilon > 0$ iff $R_1 > h_B(p)$ and $R_2 > h_B(p)$.*

Proof. (*Achievability.*) Choose an $k \times m$ source coding matrix, $\mathbf{H}$, appropriate for a $\mathcal{B}(p)$ source (see Lemma 1) and its associated decoding function $b(.)$. Apply this to both sources to get $\mathbf{z_1} = \mathbf{s_1 H}$ and $\mathbf{z_2} = \mathbf{s_2 H}$. At the decoder compute $\mathbf{z} = \mathbf{z_1} \oplus \mathbf{z_2} = (\mathbf{z_1} \oplus \mathbf{z_2})\mathbf{H} = \mathbf{uH}$ and $\hat{\mathbf{u}} = b(\mathbf{z})$. By Lemma 1, $\Pr(\hat{\mathbf{u}} \neq \mathbf{u}) < \epsilon \quad \forall \epsilon > 0$ and m large enough so long as $\frac{k}{m} < h_B(p)$.
(*Converse.*) Consider the relaxation where the decoder has full knowledge of S_2 and we would like to jointly encode S_1 and U to losslessly reconstruct U at the decoder. Note that any scheme that accomplishes this also gives the decoder a lossless reconstruction of S_1. Thus, it can be shown that for joint encoding, $R \geq H(S_1, U|S_2) = H(U|S_2) = H(U) = h_B(p)$ is required for a vanishing probability of error. This implies that for separate encoding of S_1 and U, $R_1 + R_U \geq h_B(p)$. Similarly, we can get that $R_2 + R_U \geq h_B(p)$. Setting $R_U = 0$ gives the desired result. □

We can now give the best possible rate available using separation. The sum source coding rate required is $2h_B(p)$ and the MAC sum capacity is $1 - h_B(q)$. Reliable communication requires that $k(2h_B(p)) < n(1 - h_B(q))$. This gives the optimal separation computation rate of:

$$\kappa_{\text{SEP}} = \frac{1 - h_B(q)}{2h_B(p)} - \delta \quad \forall \delta > 0 \tag{12}$$

Remark: The Körner-Marton scheme allows for a strictly lower sum rate than Slepian-Wolf coding of S_1 and S_2.

2.2 Computation Coding

We now present a block coding scheme, that we will refer to as *computation coding*, that takes advantage of the channel's natural operation and optimally trades off code rate for reliable communication of U. First, we will need the dual of the linear source coding scheme presented in Lemma 1. The lemma below was originally given by Elias in [8] and can also be found as Theorem 6.2.1 in [9].

Lemma 3. *Consider a BSC with crossover probability q, encoder input V, channel input X, channel output Y and decoder output $\hat{V}$. For any $\epsilon > 0$ and n large enough, there exists a binary $m \times n$ encoding matrix $\mathbf{G}$ with associated decoding function $c(.)$ such that when $\mathbf{x} = \mathbf{vG}$, $Pr(c(\mathbf{y}) \neq \mathbf{v}) < \epsilon$ if $m(1 - h_B(q)) < n$.*

See [9, §6.2] for a full proof. We are now prepared to combine our linear source and channel coding methods into a computation code.

Theorem 1. *There exists a linear block coding scheme for the M2MAC that can achieve any computation rate satisfying $\kappa < \frac{1-h_B(q)}{h_B(p)}$ with $Pr(\hat{U}^k \neq U^k) < \epsilon \quad \forall \epsilon > 0$ for n large enough. Furthermore, this is the best possible computation rate for lossless transmission of U over this channel.*

Proof. (*Achievability.*) By Lemma 1, there exists a $k \times m$ binary matrix $\mathbf{H}$ with associated decoding function $b(.)$ for linearly encoding an iid $\mathcal{B}(p)$ source to its entropy rate. Similarly, by Lemma 3, there exists an $m \times n$ binary matrix $\mathbf{G}$ with associated decoding function $c(.)$ for reliable communication approaching capacity over a BSC with crossover probability q. Let $\mathbf{x_1} = \mathbf{s_1HG}$ and $\mathbf{x_2} = \mathbf{s_2HG}$. Then $\mathbf{w} = \mathbf{s_1HG} \oplus \mathbf{s_2HG} = \mathbf{uHG}$. We decode using $\hat{\mathbf{u}} = c(b(\mathbf{y}))$. Select an $\epsilon > 0$. The error can be upper bounded by a simple union bound:

$$\Pr(\hat{\mathbf{u}} \neq \mathbf{u}) \leq \Pr(b(\mathbf{y}) \neq \mathbf{uH}) + \Pr(c(\mathbf{uH}) \neq \mathbf{u}) \tag{13}$$

$$\Pr(b(\mathbf{y}) \neq \mathbf{uH}) \overset{(a)}{<} \frac{\epsilon}{2} \tag{14}$$

$$\Pr(c(\mathbf{uH}) \neq \mathbf{u}) \overset{(b)}{<} \frac{\epsilon}{2} \tag{15}$$

$$\Pr(\hat{\mathbf{u}} \neq \mathbf{u}) < \epsilon \tag{16}$$

(a) for n large enough, so long as $m(1 - h_B(q)) < n$
(b) for m large enough, so long as $k < h_B(p)m$
Thus, we can drive the error to zero so long as $\frac{k}{n} < \frac{1-h_B(q)}{h_B(p)}$.
(*Converse.*) Consider any (n, k) block code. Since U is an iid $\mathcal{B}(p)$ sequence, then it requires that $I(U^k; \hat{U}^k) \geq kh_B(p)$ to attain a vanishing probability of error. Messages can only be sent reliably if the sum rate does not exceed the maximum mutual information available on the channel $I(X_1, X_2; Y) = 1 - h_B(q)$. By the data processing inequality, $I(U^k; \hat{U}^k) \leq I(X_1^n, X_2^n; Y^n)$. It can be shown that this implies that $\frac{k}{n} \leq \frac{1-h_B(q)}{h_B(p)}$ is required for a vanishing probability of error. This is actually also an upper bound on $\frac{k}{n}$ for joint encoding of U. □

Our distributed scheme achieves the best performance available for joint encoding. We can now conclude that computation codes achieve the best possible computation rate:

$$\kappa_{\text{COMP}} = \frac{1 - h_B(q)}{h_B(p)} - \delta \quad \forall \delta > 0 \tag{17}$$

Remark: Somewhat surprisingly, this strategy allows for a rate twice that of the separation scheme, regardless of the source statistics. Even if S_1 and S_2 are independent, our strategy provides a clear advantage over separation. This suggests that in general, optimal distributed computation over a MAC requires a joint-source channel strategy that focuses primarily on the desired function. The computation rate for computation coding, Körner-Marton optimal separation, and Slepian-Wolf suboptimal separation over a BSC with crossover probability $q = 0.1$ is shown in Figure 2.

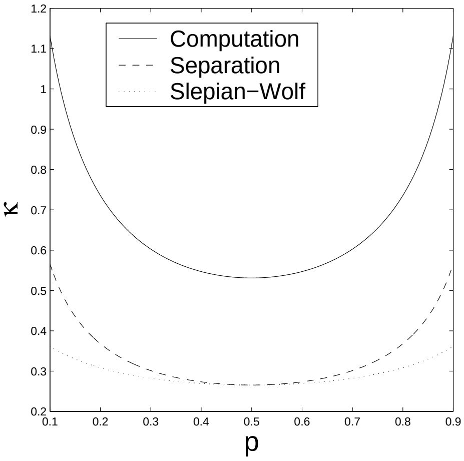

Figure 2: Comparison of schemes for sending U

3 Linear Functions over Discrete Linear MACs

Our first extension of the M2MAC is to a much larger class of MACs matched to linear functions, which we call discrete linear MACs (Figure 3). The computation code we developed can be extended to send any set of possibly dependent linear functions over these channels.

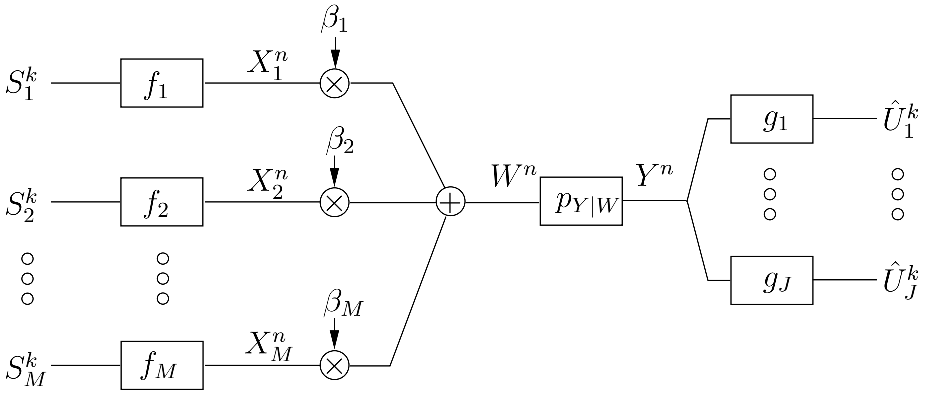

Figure 3: Discrete Linear MAC

3.1 Problem Statement

There are M sources $S_1, S_2, \ldots, S_M$ taking values on the Galois field $\mathcal{X}$. The sources are generated iid according to a joint probability distribution $p(S_1, S_2, \ldots, S_M)$. Each source S_i is seen by a separate source-channel encoder which outputs a channel symbol X_i at each time step according to an (n, k) block code:

$$f_i : \mathcal{X}^k \rightarrow \mathcal{X}^n, \quad i = 1, 2, \ldots, M \tag{18}$$

Note that the channel input alphabet for each user is also $\mathcal{X}$. We can represent the channel output Y as coming from a discrete memoryless channel (DMC), $p_{Y|W}$, where:

$$W = \sum_{i=1}^{M} \beta_i X_i \quad \text{for some } \beta_i \in \mathcal{X} \setminus \{0\} \text{ where 0 is the zero symbol in } \mathcal{X} \tag{19}$$

Our goal is to reliably communicate the linear functions $U_1, U_2, \ldots, U_J$ where:

$$U_j = \sum_{i=1}^{M} \alpha_{ji} S_i \qquad \alpha_{ji} \in \mathcal{X}, \quad j = 1, 2, \ldots, J \tag{20}$$

where we allow $\alpha_{ji} = 0$ for some i and j. There are J block decoders:

$$g_j : \mathcal{X}^n \rightarrow \mathcal{X}^k, \quad j = 1, 2, \ldots, J \tag{21}$$

each outputting an estimate of the j^{th} function, $g(Y^n) = \hat{U}_j$. We would like to maximize the computation rate, $\kappa = \frac{k}{n}$, while satisfying:

$$\lim_{k \rightarrow \infty} \Pr((\hat{U}_1^k, \hat{U}_2^k, \ldots, \hat{U}_J^k) \neq (U_1^k, U_2^k, \ldots, U_J^k)) \rightarrow 0 \tag{22}$$

Remark: The random variables $U_1, U_2, \ldots, U_J$ can be arbitrarily correlated. As a result, this setting is general enough to contain the problem of sending correlated sources over the MAC as a special case. (Set $\alpha_{ji} = \delta_{ji}$, the Kronecker delta, and $M = J$.)

Finally, we need the following definition from [9, p.94]:

Definition. We say that a DMC is *symmetric* if the output symbols can be placed into subsets such that for each subset the probability transition matrix satisfies the following two conditions:

1. Each row is a permutation of every other row.

2. Each column is a permutation of every other column.

It can easily be shown that the uniform distribution achieves capacity on symmetric DMCs. This concept can also be extended to channels with discrete inputs and continuous outputs such as a binary-input Gaussian channel. However, in the interests of space, we limit ourselves to discrete alphabets.

3.2 Computation Coding for Discrete Linear MACs

We now generalize the computation code used for the M2MAC for Galois fields. First, we will need a result of Csiszár's for linear Slepian-Wolf coding [10].

Lemma 4. *Let $(W_1, W_2, \ldots, W_L)$ be a vector source generated iid by some pdf on a discrete alphabet. For any point in the Slepian-Wolf rate region and k large enough, there are matrices $\mathbf{H_1}, \mathbf{H_2}, ..., \mathbf{H_L}$ of size $k \times m_i$, respectively, taking values over a Galois field with associated decoding function $b(.)$ that can be used to compress the sources in a distributed fashion with $Pr((\hat{W}_1^k, \hat{W}_2^k, \ldots, \hat{W}_L^k) \neq (W_1^k, W_2^k, \ldots, W_L^k)) < \epsilon \ \ \forall \epsilon > 0$.*

For a full proof, see [10]. The following lemma appears as Problem 2.1.11 in [11].

Lemma 5. *Consider a symmetric DMC with encoder input W, channel input X over Galois field $\mathcal{X}$, channel output Y, and capacity C. For any $\epsilon > 0$ and n large enough, there exists a matrix $\mathbf{G} \in \mathcal{X}^{m \times n}$ with associated decoding function $c(.)$ such that when $\mathbf{x} = \mathbf{wG}$, $Pr(c(\mathbf{y}) \neq \mathbf{w}) < \epsilon$ if $mC < n$.*

Due to space constraints, we do not include the proof here. See [9, §6.2] for the basic structure of one possible proof.

Corollary 1. *Lemma 5 also holds for asymmetric DMCs so long as C, the channel capacity, is replaced with $I(W;Y)$ where $p(W)$ is taken to be uniform.*

Theorem 2. *For the problem described in Section 3, if $p_{Y|W}$ is symmetric and has capacity C, then $\kappa = \frac{k}{n} = \frac{C}{H(U_1, U_2, \ldots, U_J)}$ is optimal.*

Proof. (*Achievability.*) Using Lemma 4, we choose matrices $\mathbf{H_1}, \mathbf{H_2}, ..., \mathbf{H_J}$ of size $k \times m_i$, respectively, to get $(U_1, U_2, \ldots, U_J)$ to some point in the Slepian-Wolf rate region with sum rate $H(U_1, U_2, \ldots, U_L)$. With these matrices form the following matrix for each $i \in M$:

$$\mathbf{H_i^{SW}} = [\alpha_{1i}\mathbf{H_1} \ \alpha_{2i}\mathbf{H_2} \ \cdots \ \alpha_{Ji}\mathbf{H_J}] \tag{23}$$

Using Lemma 5, we choose a matrix $\mathbf{G}$ of size $(\sum_{i=1}^{J} m_i) \times n$ to communicate over $p_{Y|W}$ at capacity. We note that each β_i has a multiplicative inverse β_i^{-1}. Let $\mathbf{B_i} = \beta_i^{-1}\mathbf{1}^{n \times n}$ and define: At each encoder we use the following encoding rule: $\mathbf{x} = \mathbf{A_i s_i H_i^{SW} G B_i}$. By linearity, $\mathbf{w} = [\mathbf{u_1 H_1} \ \mathbf{u_2 H_2} \ \cdots \ \mathbf{u_J H_J}]\,\mathbf{G}$. It is easy to show that using our ML decoders $b(.)$ and $c(.)$ we reach the desired rate point for any error $\epsilon > 0$ for n large enough.
(*Converse*). Consider any (n,k) block code. We now give an upper bound on the computation rate by using a joint encoding relaxation. The following condition is necessary for lossless reconstruction of our functions:

$$I(U_1, U_2, \ldots, U_J; \hat{U}_1, \hat{U}_2, \ldots, \hat{U}_J) \geq H(U_1, U_2, \ldots, U_J) \tag{24}$$

By the data processing inequality, we get that:

$$I(U_1^k, U_2^k, \ldots, U_J^k; \hat{U}_1^k, \hat{U}_2^k, \ldots, \hat{U}_J^k) \leq I(W^n; Y^n) \tag{25}$$

It can be shown that the above inequality implies:

$$kI(U_1, U_2, \ldots, U_J; \hat{U}_1, \hat{U}_2, \ldots, \hat{U}_J) \leq nI(W;Y) \tag{26}$$

We know that $I(W;Y) \leq C$ where C is the channel capacity. Finally, we get the desired upper bound:

$$\kappa = \frac{k}{n} \leq \frac{C}{H(U_1, U_2, \ldots, U_J)} \tag{27}$$

$\square$

Corollary 2. *For the problem described in Section 3, if $p_{Y|W}$ is asymmetric, then $\kappa = \frac{k}{n} = \frac{I(W;Y)}{H(U_1,U_2,\ldots,U_J)}$ is achievable where $p(W)$ is taken to be uniform.*

Remark: Ideally, we would like to compare computation coding with separation for this class of MACs. However, the Körner-Marton scheme does not seem to extend to higher alphabets as shown by the following simple example.

Example. Let S_1 and S_2 be independent random variables on GF(3) with mod-3 sum $U = S_1 \oplus S_2$. Their pdfs are given by the following table:

V	$P(S_1 = V)$	$P(S_2 = V)$	$P(U = V)$
0	0.5	0	0.25
1	0.5	0.5	0.25
2	0	0.5	0.5

It is easy to show that $H(S_1) = H(S_2) = 1$ and $H(U) = 1.5$. Clearly, a strategy that encodes S_1 and S_2 to $H(U)$ bits per symbol is wasteful as we can use the possibly suboptimal strategy of transmitting the sources separately at 1 bit per symbol.

We have developed a large class of function-matched channels, discrete linear MACS, for which computation codes allow us to optimally send any linear function.

4 Linear Functions over Unmatched Channels

We have shown that computation codes perform well over appropriately matched channels. Now, we give an example that demonstrates that linear functions can be communicated over unmatched channels at rates higher than those possible with separation.

Example. Our setting is the same as the M2MAC. For simplicity, we make S_1 and S_2 independent $\mathcal{B}(\frac{1}{2})$ processes. The only difference is the channel performs a real addition, $W = S_1 + S_2$, and passes the result through the following probability transition matrix to get Y.

$$P_{Y|W} = \begin{pmatrix} 1-\alpha-\beta & \alpha & \beta \\ \beta & 1-\alpha-\beta & \alpha \\ \alpha & \beta & 1-\alpha-\beta \end{pmatrix} \tag{28}$$

Let $\alpha = 0.05$ and $\beta = 0.1$. The computation rate for U under separation is 0.3928. We now adopt a suboptimal computation code by interpreting 2 as 0 at the channel output. Even with this crude relaxation, we can construct a computation code that achieves a computation rate of 0.4989 on the above channel. Note that values for α and β can be found for which separation beats the proposed computation code.

The above example shows that computation codes can provide benefits for sending functions over unmatched channels. However, a deeper understanding of the mismatch between the channel and desired functions is required before we can create an elegant scheme for the general problem.

5 Lossy Computation over MACs

So far we have only given results for lossless computation codes. We now study the case where some distortion is allowed in our computation. Although we would require linear distributed source codes to achieve any point on the rate distortion curve, we can use uncoded transmission to optimally achieve a non-zero point. One can show that an uncoded scheme is optimal over the M2MAC with respect to the Hamming distortion measure. Uncoded transmission also gives an elegant result in the Gaussian case.

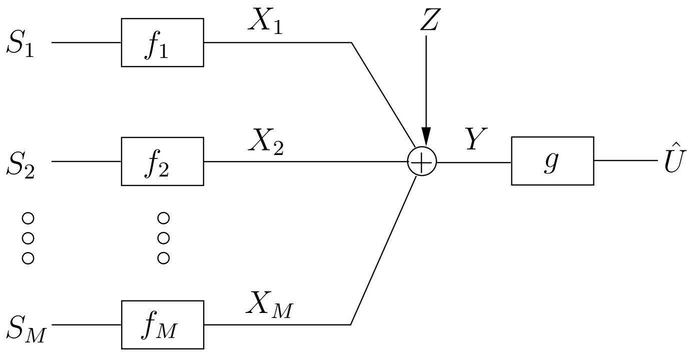

Figure 4: Gaussian MAC

There are M independent sources, $S_1, S_2, \ldots, S_M$, each generated iid from a $\mathcal{N}(0, \sigma_S^2)$ distribution. Each encoder, $f_i : \mathcal{R} \to \mathcal{R}$, takes in a source symbol, S_i, and outputs a channel input, X_i. The encoders must satisfy a joint power constraint:

$$E[tr(\mathbf{X}\mathbf{X}^T)] \leq MP \tag{29}$$

At each time step, the channel inputs, X_i, are added to the noise, Z, to produce the channel output Y. For simplicity, Z is assumed to be iid $\mathcal{N}(0, N)$ and independent of the sources.

$$Y[k] = \sum_{i=1}^{M} X_i[k] + Z[k] \tag{30}$$

Finally we have our decoder, $g : \mathcal{R} \to \mathcal{R}$. We would like to send $U = a_1 S_1 + a_2 S_2 + \ldots + a_M S_M$, $a_i \in \mathcal{R}$, across the channel. This estimate, $\hat{U}$, is subject to the standard mean-squared error constraint:

$$d(U, \hat{U}) = (U - \hat{U})^2 \tag{31}$$

$$E[d(U, \hat{U})] \leq D \tag{32}$$

Our goal is to achieve the lowest D for a given P.

Theorem 3. *Uncoded transmission is optimal for transmission of a linear function of $S_1, S_2, \ldots, S_M$ over a Gaussian MAC in the $\kappa = \frac{k}{n} = 1$ case. It achieves the following distortion:*

$$D = \sigma_S^2 \sum_{i=1}^{M} a_i^2 \frac{N}{P \sum_{i=1}^{M} a_i^2 + N} \tag{33}$$

Proof Sketch.(*Converse.*) Since the sources are independent, it can be shown that:

$$I(X_1, X_2, \ldots, X_M; Y) \leq C_{\text{MAC}}(P) \tag{34}$$

where $C_{\text{MAC}}(P)$ is the maximum sum rate achievable on the Gaussian MAC with total power MP. We can upper bound the sum rate needed to compress U to distortion D by joining the encoders. Call this $R_{\text{JOINT}}(D)$. It can be shown using the data processing inequality and some other information theoretic techniques that $R_{\text{JOINT}}(D) \leq C_{\text{MAC}}(P)$. Using this, we can lower bound the achievable distortion.

We have shown that uncoded transmission is optimal for lossy linear computation over Gaussian channels. It can be shown that uncoded transmission beats compressing the sources separately by a factor of M. The next step is to find a scheme to optimally tradeoff code rate for higher fidelity on the desired computation, real addition. This is still an open problem.

6 Conclusion

We have developed an example, the M2MAC, that shows that separation is not optimal for sending functions over multiple-access channels. Instead, we need a joint source-channel code that takes advantage of whatever match exists between the function performed by the channel and the desired function. For the case of linear functions over Galois fields, we have shown a strategy, computation coding, and a class of MACs for which it is optimal. Future work includes developing block codes for optimal real addition over the Gaussian MAC and developing a more general scheme for sending any function over any MAC.

References

[1] A. Giridhar and P. R. Kumar, "Computing and communicating functions over sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 755–764, April 2005.

[2] T. Cover, A. El Gamal, and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Transactions on Information Theory*, vol. 26, no. 6, pp. 648–657, November 1980.

[3] M. Gastpar and M. Vetterli, "Source-channel communication in sensor networks," in *2nd Int Workshop on Info Proc in Sensor Networks (IPSN '03)*, ser. Lecture Notes in Computer Science, L. J. Guibas and F. Zhao, Eds. New York, NY: Springer, April 2003, pp. 167–177.

[4] G. Mergen and L. Tong, "Type based estimation over multiaccess channels," *IEEE Transactions on Signal Processing*, to appear in 2005.

[5] T. Cover and J. Thomas, *Elements of Information Theory.* New York: Wiley-Interscience, 1991.

[6] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Transactions on Information Theory*, vol. 25, no. 2, pp. 219–221, March 1979.

[7] A. D. Wyner, "Recent results in the shannon theory," *IEEE Transactions on Information Theory*, vol. 20, no. 1, pp. 2–10, January 1974.

[8] P. Elias, "Coding for noisy channels," *IRE Convention Record*, vol. 4, pp. 37–46, 1955.

[9] R. Gallager, *Information Theory and Reliable Communication.* New York: John Wiley and Sons, Inc., 1968.

[10] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Transactions on Information Theory*, vol. 28, no. 4, pp. 585–592, July 1982.

[11] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* New York: Academic Press, 1982.