Structured Random Codes and Sensor Network Coding Theorems

Bobak Nazer and Michael Gastpar
University of California, Berkeley
Wireless Foundations Center, Department of EECS
Berkeley, CA 94720-1770, USA
Email: {bobak,gastpar}@eecs.berkeley.edu

***Abstract*—In the Shannon-theoretic analysis of joint source-channel coding problems, achievability is usually established via a two-stage approach: The sources are compressed into bits, and these bits are reliably communicated across the noisy channels. Random coding arguments are the backbone of both stages of the proof. This "separation" strategy not only establishes the optimal performance for stationary ergodic point-to-point problems, but also for a number of simple network situations, such as independent sources that are communicated with respect to separate fidelity criteria across a multiple-access channel. Beyond such simple cases, for general networks, separation-based coding is suboptimal. For instance, for a simple Gaussian sensor network, uncoded transmission is exactly optimal and performs exponentially better than a separation-based solution. In this note, we generalize this sensor network strategy by employing a lattice code. The underlying linear structure of our code is crucial to its success.**

I. Introduction

Structured code constructions have been at the forefront of interest in communication systems research for at least fifty years, some of the most prominent examples including the Reed-Solomon codes and the low-density parity-check (LDPC) codes. The chief reason for this is implementability: for a code to be efficiently encodable and decodable, it must have some structure.

In parallel, researchers have investigated the fundamental limits of communication systems. Some of these limits can be established via structured codes, but not all. A much more versatile tool was developed by Shannon, the so-called *random coding argument*. In its simplest incarnation, the letters of each codeword of a codebook are drawn independently of each other from a fixed scalar probability distribution. Clearly, the resulting codebook will not have any particular (algebraic) structure. It turns out that such codebooks can establish the capacity of all (stationary, memoryless, ergodic) point-to-point channels. It is now apparent that this fact must be considered an isolated case of luck. More generally, i.e., for networks, no similar theorem seems to hold.

To be more precise, it has become more and more clear that these completely unstructured codes will be insufficient to establish the best possible capacity results. In well-matched cases, uncoded transmission can perform much better than standard separation-based strategies. This is often due to using the additive operation of the channel to compute a sufficient statistic: something a separation-based code cannot do. As we will show, by employing a structured code, we can continue to reap some of the benefits of uncoded transmission beyond perfectly matched cases.

II. Structured Codes

The apparent necessity of structured codes was first observed by Körner and Marton [1]. In their problem, a decoder wishes to reconstruct the parity of two correlated binary sources seen by separate encoders. By employing the same linear code at each encoder, the decoder can sum the received codewords to recover the parity at the lowest possible rate. A standard strategy, such as random binning, would require a higher sum rate.

More recently, we have studied the problem of reliable computation over multiple-access channels and have found that here, too, structured codes are a very important part of the puzzle [2]. By letting each encoder use the same linear codebook, we can take advantage of the natural operation of the channel while still protecting against channel noise. This can result in huge gains over a separation-based strategy, often proportionally to the number of users (even if the underlying sources are independent). In previous work, we applied this technique to a sensor network that required a filtered, downsampled version of the sources [3].

There has also been a great deal of recent interest in using structured codes for proving new network capacity theorems. Due to space limitations, we refer the interested reader to our recent survey paper for a more comprehensive treatment and pointers to related work [4]. Of particular note is an analogue of the Körner-Marton problem developed by Krithivasan and Pradhan [5]. They show that for recovering the difference of correlated Gaussian sources, a lattice code can reduce the sum rate.

III. A Sensor Network Example

In this section, we will illustrate the significance of structured codes in a sensor network scenario. For the purpose of this note, the goal will not be generality but illustrative quality.

A. The Model

Consider the "sensor" network illustrated in Figure 1. The underlying source $\{S[n]\}_{n=1}^{N}$ is a sequence of N independent and identically distributed (i.i.d.) real-valued Gaussian random

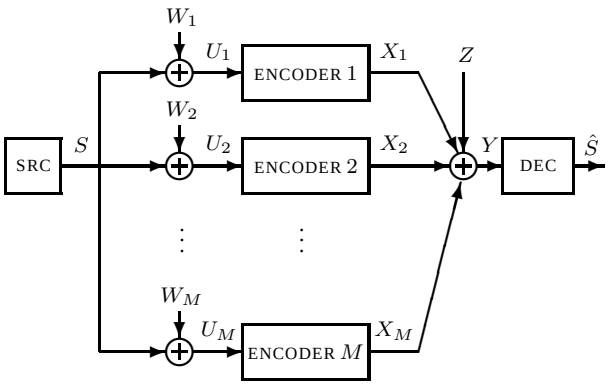

Fig. 1. The decoder (DEC) needs to reconstruct S, i.e., the underlying source (SRC). Each encoder is allowed to pool together an arbitrary number of observations $\{U_m[n]\}_{n=1}^N$, and encode them into ℓN channel uses via an arbitrarily complex encoding procedure. For the purpose of this note, ℓ is a positive integer.

variables of mean zero and variance σ_S^2. Sensor m observes a sequence $\{U_m[n]\}_{n=1}^N$ defined as

$$U_m[n] \quad = \quad S[n] + W_m[n], \tag{1}$$

where $\{W_m[n]\}_{n=1}^N$ is a sequence of i.i.d. Gaussian random variables of mean zero and variance σ_W^2. Sensor m can apply an *arbitrary* coding function to the observation sequence such as to generate a sequence of ℓN channel inputs, $\{X_m[k]\}_{k=1}^{\ell N} = f_m(\{U_m[n]\}_{n=1}^N)$. For the purpose of this note, we assume that ℓ is a positive integer. The only constraint is that the function $f_m(\cdot)$ be chosen to ensure that

$$\lim_{N\to\infty} \frac{1}{\ell N} \sum_{k=1}^{\ell N} \mathbb{E}\left[(X_m[k])^2\right] \quad \leq \quad P. \tag{2}$$

The channel output is then given as

$$Y[k] \quad = \quad Z[k] + \sum_{m=1}^{M} X_m[k], \tag{3}$$

where $\{Z[k]\}_{k=1}^{\ell N}$ is an i.i.d. sequence of Gaussian random variables of mean zero and variance σ_Z^2. Upon observing the channel output sequence $\{Y[k]\}_{k=1}^{\ell N}$, the decoder (or fusion center) must produce a sequence $\{\hat{S}[n]\}_{n=1}^N = g(\{Y[k]\}_{k=1}^{\ell N})$, and we consider the distortion

$$D \quad = \quad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbb{E}\left[(S[n] - \hat{S}[n])^2\right]. \tag{4}$$

This note concerns the determination of the smallest attainable distortion D_ℓ, for fixed power P (per terminal), over all possible encoding and decoding functions, $f_m(\cdot)$ ($m = 1, 2, \ldots, M$) and $g(\cdot)$. A particular interest concerns the dependence of the results on ℓ, the average number of channel uses per source symbol (i.e., the "bandwidth expansion factor").

B. Separate Source and Channel Coding

An obvious first candidate is to let each encoder first compress its respective observation stream in the best possible fashion into a bit stream, and then communicate this bit stream reliably to the decoder. The source coding problem corresponding to our sensor network example has been well studied, under the name of *CEO problem*. This problem was introduced in [6], [7] and the quadratic Gaussian version described above was solved by Oohama [8], with some recent refinements [9], [10]. From this work, the *sum* rate (i.e., the total rate over all M encoders) in order to achieve a certain distortion D is determined as

$$R(D) = \log_2^+ \left(\frac{\sigma_S^2}{D} \left(\frac{D\sigma_S^2 M}{D\sigma_S^2 M - \sigma_S^2\sigma_W^2 + D\sigma_W^2} \right)^M \right). \tag{5}$$

For the purpose of this note, we use Oohama's simpler lower bound, which can be obtained easily from the above, noting that $\sigma_S^2/D \geq 1$,

$$R(D) \geq M \log_2^+ \left(\frac{D\sigma_S^2 M}{D\sigma_S^2 M - \sigma_S^2\sigma_W^2 + D\sigma_W^2} \right). \tag{6}$$

Conversely, the smallest achievable distortion satisfies

$$D(R) \geq \frac{\sigma_S^2\sigma_W^2}{\sigma_S^2 M \left(1 - 2^{-R/M}\right) + \sigma_W^2}. \tag{7}$$

By noting that $1 - 2^{-R/M} \leq R/M$, this implies the lower bound

$$D(R) \geq \frac{\sigma_S^2\sigma_W^2}{\sigma_S^2 R + \sigma_W^2}. \tag{8}$$

The total communication rate across the multiple-access channel in our system can be somewhat generously bounded by

$$R_{tot} \quad \leq \quad \frac{\ell}{2} \log_2 \left(1 + \frac{M^2 P}{\sigma_Z^2} \right), \tag{9}$$

where we recall that ℓ is the (average) number of channel uses per source sample. This leads to the following result:

Theorem 1: For the Gaussian "sensor" network, using *separate source and channel code design* incurs a distortion of at most

$$D_\ell^{(\text{separation})} \geq \frac{\sigma_S^2\sigma_W^2}{\ell\frac{\sigma_S^2}{2} \log_2 \left(1 + M^2 P/\sigma_Z^2\right) + \sigma_W^2}. \tag{10}$$

C. Uncoded Transmission

For the special case $\ell = 1$ (equal bandwidth), the simple sensor network has been thoroughly investigated. Somewhat surprisingly, it has been shown in [11], [12], [13] that an optimal strategy is for each sensor to transmit

$$X_m[n] \quad = \quad \sqrt{\frac{P}{\sigma_S^2 + \sigma_W^2}} U_m[n]. \tag{11}$$

It is easily verified that this satisfies the power constraint (Equation (2)). We refer to this communication strategy as *uncoded transmission*. The performance of this simple scheme

can be evaluated by straightforward calculations. We summarize the result in the following theorem.

Theorem 2: For the Gaussian "sensor" network with $\ell = 1$, *uncoded transmission* attains the smallest possible distortion, given by

$$D_1 = \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2+\sigma_W^2}\left(1+\frac{M(\sigma_S^2\sigma_Z^2/\sigma_W^2)}{\frac{M\sigma_S^2+\sigma_W^2}{\sigma_S^2+\sigma_W^2}MP+\sigma_Z^2}\right). \quad (12)$$

For a proof, see [11], [12], [13].

An interesting question is: What to do with further channel uses, i.e., if $\ell > 1$? This is indeed unclear. One candidate may be repetition coding, which would lead to the following distortion:

$$D_\ell^{(\text{uncoded})} = \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2+\sigma_W^2}\left(1+\frac{M(\sigma_S^2\sigma_Z^2/\sigma_W^2)}{\frac{M\sigma_S^2+\sigma_W^2}{\sigma_S^2+\sigma_W^2}\ell MP+\sigma_Z^2}\right). \quad (13)$$

Before studying further code construction, we will provide a converse bound.

D. A Converse Bound

We can slightly extend a bound first presented in [14] to obtain the following theorem:

Theorem 3: For the Gaussian "sensor" network, the incurred distortion must satisfy

$$D_\ell \geq \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2+\sigma_W^2}\cdot \left(1+M\frac{\sigma_S^2}{\sigma_W^2}\left(\frac{\sigma_Z^2}{\frac{M\sigma_S^2+\sigma_W^2}{\sigma_S^2+\sigma_W^2}MP+\sigma_Z^2}\right)^\ell\right). \quad (14)$$

E. Structured Codes

As the converse bound in Theorem 3 shows, we would ideally like the distortion to fall *exponentially* with increasing channel bandwidth (or increasing ℓ). However, repetition coding only provides a linear descent so we must turn to more clever strategies for $\ell > 1$.

Just like the uncoded strategy, we would like to use the additive operation of the channel to our advantage. Furthermore, we would like our transmissions to be uncorrelated with the current estimate of the source at the decoder. By using a lattice code for distributed Wyner-Ziv coding, we can simultaneously satisfy both requirements. The lattice will allow us to only decode the sum of codewords and the Wyner-Ziv strategy will ensure uncorrelatedness with the previous estimate.

We have developed just such a lattice code in [2]. First, we will need some basic facts about lattices. Note that in this section a bold-faced variable is often used to denote the appropriate N-length vector (i.e. $\mathbf{u}_m = \{U_m[n]\}_{n=1}^N$)

Definition 1: An N-dimensional *lattice*, Λ, is a set of points in $\mathbb{R}^N$ such that if $\mathbf{x}, \mathbf{y} \in \Lambda$, then $\mathbf{x}+\mathbf{y} \in \Lambda$, and if $\mathbf{x} \in \Lambda$, then $-\mathbf{x} \in \Lambda$. A lattice can always be written in terms of a generator matrix $\mathbf{G} \in \mathbb{R}^{N\times N}$:

$$\Lambda = \{\mathbf{x} = \mathbf{z}\mathbf{G} : \mathbf{z} \in \mathbb{Z}^N\} \quad (15)$$

where $\mathbb{Z}$ represents the integers.

Definition 2: A *lattice quantizer* is a map, $Q : \mathbb{R}^N \to \Lambda$, that sends a point, $\mathbf{x}$, to the nearest lattice point in Euclidean distance:

$$\mathbf{x_q} = Q(\mathbf{x}) = \arg\min_{\mathbf{l}\in\Lambda} ||\mathbf{x}-\mathbf{l}||_2 \quad (16)$$

Definition 3: Let $[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q(\mathbf{x})$. The mod Λ operation satisfies:

$$[[\mathbf{x}] \bmod \Lambda + \mathbf{y}] \bmod \Lambda = [\mathbf{x}+\mathbf{y}] \bmod \Lambda \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^N \quad (17)$$

We now give our achievable scheme which is a multiterminal generalization of the scheme presented by Erez and Zamir in [15].

Theorem 4: For the Gaussian "sensor" network, the following distortion is achievable for any $\ell > 1$:

$$D_\ell^{(\text{lattice})} = \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2+\sigma_W^2}\cdot \left(1+\left(\frac{M(\sigma_S^2\sigma_Z^2/\sigma_W^2)}{\frac{M\sigma_S^2+\sigma_W^2}{\sigma_S^2+\sigma_W^2}MP+\sigma_Z^2}\right)\left(\frac{M\sigma_Z^2}{MP+\sigma_Z^2}\right)^{\ell-1}\right).$$

Proof: (Sketch.) We first use uncoded transmission to communicate our observation sequences across the channel to get an MMSE estimate of their sum at distortion $D_1^{(U)}$ where

$$D_1^{(U)} = \frac{(M^2\sigma_S^2+M\sigma_W^2)\sigma_Z^2}{\frac{P}{\sigma_S^2+\sigma_W^2}(M^2\sigma_S^2+M\sigma_W^2)+\sigma_Z^2} \quad (18)$$

Denote this MMSE estimate of the sum of observations, $\sum_{m=1}^M U_m[n]$, by $V^{(1)}[n]$.

Now we employ our lattice-based scheme from Theorem 3 in [2] to refine this estimate of our sum with the remaining $(\ell-1)N$ channel uses. We can reduce our distortion down to $D_\ell^{(U)}$ where

$$D_\ell^{(U)} = D_1^{(U)}\left(\frac{M\sigma_Z}{MP+\sigma_Z^2}\right)^{\ell-1} \quad (19)$$

The lattice scheme essentially works as follows. We choose a lattice Λ in $\mathbb{R}^N$ that is good for both source coding and channel coding using the results of [16]. For a block of N channel uses, each encoder transmits:

$$\mathbf{x}_m = [\gamma\mathbf{u}_m + \mathbf{d}_m] \bmod \Lambda \quad (20)$$

where $\mathbf{d}_m$ is a random vector available as common randomness which is used as a dither and γ is a constant in $\mathbb{R}^N$. For details, see [2]. The decoder combines the received signal $\mathbf{y}$ with the previous estimate $\mathbf{v}^{(1)}$ to get a new estimate $\mathbf{v}^{(2)}$:

$$\mathbf{v}^{(2)} = \beta\left[\alpha\mathbf{y} - \left(\sum_{m=1}^M \mathbf{d}_m + \gamma\mathbf{v}^{(1)}\right)\right] \bmod \Lambda + \mathbf{v}^{(1)} \quad (21)$$

where α and β are appropriately chosen constants in $\mathbb{R}^N$. This process is iterated until we have expended all ℓN channel uses to give us the estimate at distortion $D_\ell^{(U)}$. We then use this estimate of the sum of observations to make

an MMSE estimate $E[\mathbf{s}|\mathbf{v}^{(1)}]$ of the original source S. Let $\mathbf{u}_{\text{SUM}} = \sum_{m=1}^{M} \mathbf{u}_m$. The distortion for this estimate is given by:

$$D_\ell = \frac{1}{N} E\left[\|\mathbf{s} - E[\mathbf{s}|\mathbf{v}^{(\ell)}]\|_2^2\right] \tag{22}$$

$$= \frac{1}{N} E\left[\|\mathbf{s} - E[\mathbf{s}|\mathbf{u}_{\text{SUM}}] + E[\mathbf{s}|\mathbf{u}_{\text{SUM}}] - E[\mathbf{s}|\mathbf{v}^{(\ell)}]\|_2^2\right]$$

$$\stackrel{\text{(a)}}{=} \frac{1}{N} E\left[\|\mathbf{s} + E[\mathbf{s}|\mathbf{u}_{\text{SUM}}]\|_2^2\right] \cdots \tag{23}$$

$$+ \frac{1}{N} E\left[\|E[\mathbf{s}|\mathbf{u}_{\text{SUM}}] - E[\mathbf{s}|\mathbf{v}^{(\ell)}]\|_2^2\right]$$

$$\stackrel{\text{(b)}}{=} \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2 + \sigma_W^2} \cdots \tag{24}$$

$$+ \left(\frac{\sigma_S^2}{M\sigma_S^2 + \sigma_W^2}\right)^2 \frac{1}{N} E\left[\|\mathbf{u}_{\text{SUM}} - E[\mathbf{u}_{\text{SUM}}|\mathbf{v}^{(\ell)}]\|_2^2\right]$$

$$= \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2 + \sigma_W^2} + \left(\frac{\sigma_S^2}{M\sigma_S^2 + \sigma_W^2}\right)^2 D_\ell^{(U)} \tag{25}$$

where $\|\cdot\|_2^2$ denotes the square of the ℓ_2 norm, (a) follows by the orthogonality principle, and (b) is due to the fact that MMSE estimation for Gaussian sources is just a rescaling. ∎

As desired, we now have a scheme for which distortion falls exponentially with increasing ℓ. Unfortunately, its performance does not match that of our lower bound from Theorem 3. It is unclear whether our scheme can be significantly improved upon or that there is a fundamental penalty for distributed encoding beyond the $\ell = 1$. It seems likely that any scheme that employs quantization at the encoders will face a penalty that keeps it away from the lower bound.

It is interesting to note that the performance attained by our lattice code is not accessible to an i.i.d. random code even if we do not enforce the notion of separation. This is due to the fact that the sum of any two codewords is a valid codeword in a lattice code (and hence potentially decodable) but almost surely not in an i.i.d. random code.

IV. Generalizations and Extensions

One shortcoming of our scheme is that it only results in a reduction in distortion for $\ell > 1$ if an SNR requirement is satisfied ($\frac{P}{\sigma_Z^2} > 1 - \frac{1}{M}$). This can be overcome by combining repetition coding with the lattice scheme in Theorem 4. For instance, if each transmission is repeated $\theta \in \mathbb{Z}_+$ times then we can run $\frac{\ell-1}{\theta}$ refinements to get the following distortion (assume $\frac{\ell-1}{\theta} \in \mathbb{Z}_+$):

$$D_\ell = \frac{\sigma_S^2\sigma_W^2}{M\sigma_S^2 + \sigma_W^2} \cdot \cdot \left(1 + \left(\frac{M(\sigma_S^2\sigma_Z^2/\sigma_W^2)}{\frac{M\sigma_S^2+\sigma_W^2}{\sigma_S^2+\sigma_W^2} MP + \sigma_Z^2}\right)\left(\frac{M\sigma_Z^2}{\theta MP + \sigma_Z^2}\right)^{\frac{\ell-1}{\theta}}\right).$$

An interesting open problem would be to improve the performance of the lattice scheme so that it is not SNR limited. Another open problem is to allow the underlying correlations of the sources to help in the transmission of the lattice points. In the current scheme, correlations provide a large boost in the uncoded step but are not involved in the lattice refinements.

In a more general setting, the channel may be a noisy scaled sum of its inputs and the sufficient statistic will be a different linear function of the sources. Just like uncoded transmission [13], structured coding will be useful in the general case, although there may be some penalties for mismatch between the desired function and that performed by the channel. Further investigations will focus on characterizing its performance in these scenarios.

Acknowledgment

The authors would like to thank A.D. Sarwate and K. Eswaran for valuable discussions. B. Nazer was supported by an NSF Graduate Fellowship and M. Gastpar was supported by an NSF CAREER Grant CCF-0347298.

References

[1] 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.

[2] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Trans. Inform. Theory*, vol. IT-53, pp. 3498–3516, October 2007.

[3] A. D. Sarwate, B. Nazer, and M. Gastpar, "Spatial filtering in sensor networks with computation codes," in *SSP 2007, Madison, WI, August, 2007*.

[4] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," *Euro. Trans. Telecomm.* To appear.

[5] D. Krithivasan and S. Pradhan, "Lattices for distributed source coding: Jointly Gaussian sources and reconstruction of a linear function," *IEEE Trans. Inform. Theory*. Submitted July 2007. See http://arxiv.org/abs/0707.3461.

[6] T. Berger, Z. Zhang, and H. Viswanathan, "The CEO problem," *IEEE Trans. Inform. Theory*, vol. IT–42, pp. 887–902, May 1996.

[7] H. Viswanathan and T. Berger, "The quadratic Gaussian CEO problem," *IEEE Trans. Inform. Theory*, vol. IT–43, pp. 1549–1559, September 1997.

[8] Y. Oohama, "The rate-distortion function for the quadratic Gaussian CEO problem," *IEEE Trans. Inform. Theory*, vol. IT–44, pp. 1057–1070, May 1998.

[9] V. Prabhakaran, D. Tse, and K. Ramchandran, "Rate region of the quadratic Gaussian CEO problem," in *Proc IEEE Int Symp Info Theory*, (Chicago, IL), July 2004.

[10] J. Chen, X. Zhang, T. Berger, and S. Wicker, "An upper bound on the sum-rate distortion function and its corresponding rate allocation schemes for the CEO problem," *IEEE Jour. Sel. Areas Comm.*, vol. 22, pp. 977–987, Aug 2004.

[11] M. Gastpar and M. Vetterli, "On the capacity of wireless networks: The relay case," in *Proc IEEE Infocom 2002*, vol. 3, (New York, NY), pp. 1577 – 1586, June 2002.

[12] M. Gastpar and M. Vetterli, "Source-channel communication in sensor networks," in *IPSN'03* (L. J. Guibas and F. Zhao, eds.), pp. 162–177, New York, NY: Lecture Notes in Computer Science, Springer, April 2003.

[13] M. Gastpar and M. Vetterli, "Power, spatio-temporal bandwidth, and distortion in large sensor networks," *IEEE Jour. Sel. Areas Comm.*, vol. 23, pp. 745–754, April 2005.

[14] M. Gastpar, "Uncoded transmission is exactly optimal for a simple Gaussian sensor network," in *Proc. 2007 ITA Workshop*, (San Diego, CA), February 2007.

[15] Y. Kochman and R. Zamir, "Joint Wyner-Ziv/dirty-paper coding by analog modulo-lattice modulation," *IEEE Trans. Inform. Theory*. Submitted Jan 2008. See http://arxiv.org/abs/0801.0815.

[16] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inform. Theory*, vol. IT-51, pp. 3401–3416, October 2005.