On the Performance of Independently Designed LDPC Codes for the Relay Channel

Jérémie Ezri Ecole Polytechnique Fédérale de Lausanne, EPFL Coding Theory Laboratory CH-1015 Lausanne, Switzerland E-mail: jeremie.ezri@epfl.ch

*Abstract***— A decode-and-forward LDPC-based coding and decoding scheme is proposed and applied to the BAWGN singlerelay channel. The source broadcasts information to both the relay and the destination. The relay is able to simultaneously receive and transmit. Both the relay and the destination apply successive iterative decoding using belief propagation. In the proposed scheme, the LDPC code used by the source and the LDPC code used by the relay are designed independently of each other. Optimality properties of this approach are established via information-theoretic upper and lower bounds.**

Asymptotic analysis shows that the performance of the proposed scheme can be as close as 0.02 **dB away from the theoretical limit for any decode-and-forward scheme, and simulation results** show that its performance for a block code of length 2^{14} can be **within** 0.65 **dB away from the same limit with a corresponding bit error probability of** $\sim 10^{-6}$.

I. INTRODUCTION

Iterative decoding has recently attracted a lot of interest due to its ability to approach the ultimate channel capacity of various single-user channels. It turns out that the *Low-Density Parity-Check codes* (LDPC codes) introduced by Gallager in [1] are among the best such codes. Efficient tools to analyze LDPC codes are developed in [2] and [3], as well as efficient encoding. It has also been shown in [4] that LDPC codes approach capacity on the multiple access channel.

In a wireless multiple access network, each node has to broadcast the data in the network. Consequently, other transmitters have access to the data and can possibly collaborate to convey the information to the base station. The simplest network model that enables collaboration is the relay channel. Two important coding theorems for the single relay channel were established in [5]. Several coding strategies that exploit terminal cooperation for *relay networks* were developed in [6].

Unfortunately, the capacity of the general relay channel is still an open problem. Nevertheless, an upper bound and several achievable lower bounds are known. Driven by the practical interest of collaborative communication, new research challenges consist in achieving the theoretical lower bounds via efficient and practical coding schemes. As far as we know, only [7] and [8] have addressed this issue by studying the performance of a turbo-based scheme for the relay channel. A particular LDPC-based scheme was analyzed in [9], where the codes used by the source and the relay have the same rate.

Michael Gastpar Department of EECS University of California, Berkeley Berkeley, CA 94720, USA E-mail: gastpar@eecs.berkeley.edu

When the source and relay power budgets are fixed (no power allocation), this generally incurs a rate penalty, but it enables an interesting mode of operation at the relay, namely simply to transmit the codeword that is closest to the received signal. A more general discussion of LDPC codes for Gaussian relay channels appears in [10].

In this work, we consider the *Binary input Additive White Gaussian Noise* (BAWGN) single-relay channel and propose a decode-and-forward strategy in which the LDPC codes used by the source and the relay, respectively, are designed independently of each other. While this generally incurs a rate penalty, there is an interesting regime where it is optimal. We characterize this regime using information-theoretic bounds. We then evaluate our scheme's performance for both infinite and finite length, and compare its achievable rate to the corresponding information-theoretical bounds developed in [5].

II. PRELIMINARIES

A. Model and Problem Statement

Fig. 1. BAWGN relay channel.

The BAWGN relay channel is depicted in Fig. 1. The source sends X to the relay and the destination at the same time. The relay receives Y_1 and sends X_1 , which depends only on the past values of Y_1 , to the destination which receives Y. We consider a BPSK modulation for the inputs with two power constraints $\mathbb{E}X^2 \leq P$ and $\mathbb{E}X_1^2 \leq P_1$, i.e., $X \in {\{\pm\sqrt{P}\}}$ and $X_1 \in {\pm \sqrt{P_1}}$. Let $Z_1 \sim \mathcal{N}(0, \sigma_1^2)$ be the noise added at the relay and $Z_1 \sim \mathcal{N}(0, \sigma_1^2)$ the noise added at the destination relay and $Z \sim \mathcal{N}(0, \sigma^2)$ the noise added at the destination.

In order to gain insight, and to have a simple parametrization, we will consider in the following the geometrically inspired example depicted in Fig. 2, in which the relay is on a line between the source and the destination. We fix the distance between the source and the destination to one and we let d be the distance between the source and the relay. We only consider the case in which $0 \le d \le 1$. Moreover we assume that the two receivers are identical and thus Z and Z_1 have the same variance σ^2 . In a similar fashion, we assume that the transmitter at the source and the transmitter at the relay have the same power constraint, i.e., $P = P_1$. In this case, the received signals can be expressed as:

$$
Y_1 = \frac{1}{d^{\frac{\alpha}{2}}}X + Z_1 \tag{1}
$$

$$
Y = X + \frac{1}{(1-d)^{\frac{\alpha}{2}}} X_1 + Z \tag{2}
$$

where α is a fixed and assumed to be known attenuation exponent, typically around two or three.

$$
\begin{array}{c}\n a \\
 \bigcirc \\
 S \\
 \hline\n 1\n \end{array}\n \qquad\n \begin{array}{c}\n \bigcirc \\
 O \\
 D \\
 \hline\n 0\n \end{array}
$$

Fig. 2. Relay on a line between the source and the destination.

The channel is assumed to be memoryless and the transition density is thus

$$
p(y, y_1 | x, x_1) = \frac{1}{2\pi\sigma^2} e^{-\frac{\left(y - x - \frac{1}{(1 - d)\frac{\alpha}{2}} x_1\right)^2 + \left(y_1 - \frac{1}{d\frac{\alpha}{2}} x\right)^2}{2\sigma^2}}.
$$
 (3)

Finally, let us define the signal-to-noise ratio (SNR) to be $\frac{P}{\sigma^2}$ in dB.

B. Capacity Upper Bound

The following upper bound on the capacity for the relay channel is a particular case of the more general max-flow mincut theorem in [11, Theorem 14.10.1].

Proposition 1: The capacity of the relay channel is upper bounded by:

$$
C \le \sup_{p(x,x_1)} \min\{I(X,X_1;Y), I(X;Y,Y_1|X_1)\} \tag{4}
$$

C. Capacity Lower Bound

Cover and El Gamal proposed in [5, Theorem 1] the *decodeand-forward* strategy which provides a lower bound to the capacity.

Proposition 2: The capacity of the relay channel is lowerbounded by:

$$
C \ge R_{\text{DF}} \triangleq \sup_{p(x,x_1)} \min\{I(X,X_1;Y), I(X;Y_1|X_1)\} \tag{5}
$$

Remark 1: We can even show that for any strategy which allows the relay to decode completely the message sent by the source, the maximum achievable rate is R_{DF} .

Two naive lower bounds can be found by only considering either the link between the source and the destination or the way trough the relay.

If the relay is not used, we obtain the lower bound:

$$
C \ge \max_{p(x)} \max_{x_1} I(X;Y|X_1 = x_1)
$$
 (6)

that we call the *point-to-point* lower bound.

If we consider that the direct channel is ignored, i.e., the source sends information to the relay, and the relay to the destination, but the destination no longer attempts to decode anything that comes directly from the source, we obtain:

$$
C \ge \max_{p(x)p(x_1)} \min\{I(X;Y_1), I(X_1;Y)\}.\tag{7}
$$

We will call this lower bound the *two-hop* lower bound.

III. BOUNDS EVALUATION FOR THE BAWGN RELAY CHANNEL.

In the BAWGN relay channel case, we have to maximize (4) and (5) over the joint input distribution $p_{X,X_1}(x, x_1)$ which can be parametrized as follows

$$
\begin{array}{c|c|c}\nX_1 \setminus X & 1 & -1 \\
\hline\n1 & \alpha & \beta \\
\hline\n-1 & \gamma & 1 - \alpha - \beta - \gamma\n\end{array} \tag{8}
$$

where $0 \le \alpha \le 1$, $0 \le \beta \le 1 - \alpha$, $0 \le \gamma \le 1 - \alpha - \beta$.

Lemma 1: A joint distribution $p_{X,X_1}(x, x_1)$ which maximizes the upper bound (4) on the capacity and R_{DF} (5) is of the form

$$
\begin{array}{c|cc}\nX_1 \setminus X & 1 & -1 \\
\hline\n1 & \frac{1}{2} \rho & \frac{1}{2}(1 - \rho) \\
\hline\n-1 & \frac{1}{2}(1 - \rho) & \frac{1}{2} \rho\n\end{array} (9)
$$

where $0 \leq \rho \leq 0.5$.

The proof can be found in [12].

Let us examine more carefully the lower bound R_{DF} given by (5). The first mutual information $I(X, X_1; Y)$ is imposed by the destination and the second one $I(X; Y_1|X_1)$ by the relay. It is thus interesting to compare the behavior of these two mutual informations when we vary the parameters ρ (the dependence between X and X_1), d and σ , in order to know where the bottleneck of the scheme is in a given situation.

Fig. 3. Mutual informations $I(X, X_1; Y)$ and $I(X; Y | X_1)$ as a function of ρ for a) $d = 0.25$ and b) $d = 0.45$.

As we can see in Fig. 3, for $\rho = 0$, i.e., $X = X_1$, we have $I(X, X_1; Y) \ge I(X; Y_1 | X_1) = 0$. Moreover these two mutual informations are concave in ρ and $I(X; Y_1|X_1)$ is even symmetric, centered in $\rho = 0.5$. We can identify two regimes:

- 1) When the relay is sufficiently close to the source, there will be a maximizing ρ^* , with $0 \le \rho^* < 0.5$ (Fig. 3.a).
When the relay is sufficiently far from the source (this
- 2) When the relay is sufficiently far from the source (this increases $I(X, X_1; Y)$ and decreases $I(X; Y_1|X_1)$, the two curves no longer intersect in the interval $0 \leq$

¹It is more relevant to only consider the case in which the two inputs X and X_1 are independent. Indeed, if we put effort in designing a scheme with dependent codes, there is no reason not to use the decode-and-forward strategy, since it cannot decrease the rate.

Fig. 4. Bounds for the BAWGN relay channel: $\alpha = 2$, SNR= 0 dB.

 ρ < 0.5 (Fig. 3.b). Since $I(X; Y_1|X_1)$ is concave and symmetric, the maximum is thus simply

$$
R_{\text{DF}} = I_{\rho=0.5}(X; Y_1 | X_1) = I(X; Y_1). \tag{10}
$$

Since $\rho = 0.5$ means $X \perp X_1$, we will call this the *independent codes* regime. It is important to note that in this regime, the relay is the only bottleneck.

Let us call *the cut-off point* (d_{co}) , the distance corresponding to the limit case in which $R_{\text{DF}} = I_{\rho=0.5}(X; Y_1 | X_1)$ = $I_{\rho=0.5}(X,X_1;Y).$

Now it is interesting to compare the upper bound (4) and R_{DF} (5). These two bounds are plotted in Fig. 4 versus the distance d for SNR = 0 dB and $\alpha = 2$. We can see that when the relay is close to the source, the two bounds are almost identical and thus they are both very tight and close to the capacity. When the relay moves from the cut-off point d_{co} to the destination, we see that the gap between the two bounds increases and thus R_{DF} is less and less tight.²

The two naive lower bounds of Section II-C are labeled R_{II} for the point-to-point one and R_{12} for the two-hop one.

As we will see in the following, we are particularly interested in the case in which we restrain ourselves to using independent codes. So, we have also plotted the maximum achievable rate of the decode-and-forward strategy (R_{DFI}) for this particular case.

Finally, Fig. 5 shows the cut-off point d_{co} as a function of the SNR. It also depicts the other limit distance, d_l , above which $R_{\text{DF}} = R_{\text{12}}$.

Note that for high SNR, one would select a larger modulation constellation, rather than binary inputs. This is discussed in part in [10].

Fig. 5. Evolution of d_{co} and d_l as a function of the SNR for $\alpha = 2$.

²We can say that because we know other tighter lower bounds in this regime. See [6].

IV. DECODE-AND-FORWARD STRATEGY

The strategy that we used in this paper is based on the decode-and-forward one proposed by Cover and El Gamal in [5] when we restrain it to independent inputs, i.e., $X \perp X_1$. Let W be the set of possible messages with $|\mathcal{W}| = 2^{nR}$ and S the set of bins with $|\mathcal{S}| = 2^{nR_1}$. We partition W into S. To that end, each $w \in \mathcal{W}$ is assigned uniformly and independently to a bin $s \in S$. Let w_i be the message picked by the source at time *i*, by convention we say that $w_i \in s_{i+1}$. The procedure depicted in Table I works as follows:

In block i: the source picks a message $w_i \in \mathcal{W}$ and computes the corresponding codeword $x(w_i)$.

Upon receiving $y_1(i)$, the relay computes its estimate $x(\tilde{w}_i)$ and thus \tilde{s}_{i+1} such that $x(\tilde{w}_i) \in \tilde{s}_{i+1}$. Given its previous estimate \tilde{s}_i , it computes and sends $x_1(\tilde{s}_i)$.

Upon receiving $y(i)$, the destination computes the estimate \hat{s}_i (this can be done correctly if $n \to \infty$ and $R_1 < I(X_1; Y)$).

In block $i + 1$ **:** same things happen at the source and at the relay. Upon receiving $y(i + 1)$, the destination computes the estimate \hat{s}_{i+1} and uses \hat{s}_i , \hat{s}_{i+1} and $y(i)$ in order to compute the estimate $\hat{\mathbf{x}}(w_i)$.

Let R be the rate of the code used by the source. In the original decode-and-forward strategy, we send $B - 1$ blocks of information over B blocks of transmission. Moreover, two consecutive codewords are selected in a dependent fashion at the source. This implies two drawbacks:

- 1) If the relay makes a decoding error in block i , the destination will be unable to correctly decode blocks i to $B-1$.
- 2) The actual rate of the original strategy is $R' = \frac{B-1}{B}R$.
Thus to have R' close to R, we must choose R large Thus, to have R' close to R, we must choose B large and this is not desired because of point 1.

Our designed independent input scheme avoids these two problems. Indeed, since the source selects independently the codewords to be sent given the messages, an error at the relay at time i will certainly affect the decoding of block i and $i + 1$ at the destination, but not the following ones. We can thus perform a infinite successive decoding at the destination with no need to consider B blocks, which implies that R is the actual rate of the scheme.

V. BINNING WITH LDPC CODES

We work over $\mathbb{F} \triangleq GF(2)$. Consider a set of messages $W = \mathbb{F}^l$ and a set of bins $S \subseteq \mathbb{F}^m$. Consider an LDPC code of rate R and length n , and its corresponding parity-check matrix H specified by its degree distribution.

Fig. 6. Factor graph for the decoding of $x(w_i)$ when the corresponding bin s_{i+1} is known.

In order to do the binning, i.e., to partition W into S , each $w \in W$ is assigned to a bin $s \in S$. To this end we compute the codeword $x(w)$ and we pass it trough a hash function M, which is a sparse $m \times n$ matrix specified by its degree distribution of rate R_M . We say that $w \in s$ if and only if

$$
Mx(w) = s.
$$
 (11)

Now consider that $x(w)$ is transmitted through a channel which outputs *y*. Moreover assume that the destination knows *s* as side information. According to (11), the destination decoder uses its knowledge of *s* in order to increase the number of constraints on the codeword $x(w)$. By doing that the decoder transforms the rate R of $x(w)$ into an artificial *lower-rate* R^*
which is given by which is given by

$$
n(1 - R^*) = n(1 - R) + n(1 - R_M)
$$

\n
$$
\implies R^* = R + R_M - 1.
$$
 (12)

The decoding can thus be performed over the graph depicted in Fig. 6.

VI. LDPC CODE IMPLEMENTATION

Since we will use LDPC codes, it is important to note that linear codes can achieve the theoretical limit of our model.

Theorem 1: Linear codes can achieve R_{DF} in the independent codes regime of a BAWGN relay channel. For the proof, see [12].

A. Encoding

Code generation: We consider two parity-check matrices H and H_1 of rate R and R_1 respectively and specified by their degree distribution. Moreover we assume that the code corresponding to H_1 is systematic.

Given a message w the source computes the corresponding codeword $x(w)$, such that it satisfies

$$
\text{Hx}(w) = \mathbf{0} \tag{13}
$$

The relay encodes a given bin *s* into $x_1(s)$ such that it satisfies

$$
H_1 \mathbf{x}_1(s) = \mathbf{0}.\tag{14}
$$

To perform this encoding, we use the algorithm proposed by Richardson and Urbanke in [3].

Fig. 7. Factor graph for the decoding of $x_1(s_i)$ at the destination.

Binning: We do the binning as proposed in Section V by considering a hash function matrix M specified by its degree distribution of rate R_M . This means, that at time *i*:

$$
M\mathbf{x}(w_i) = \mathbf{s}_{i+1}.\tag{15}
$$

We thus have the relation:

$$
R_1 = \frac{m}{n} = \frac{n(1 - R_M)}{n} = 1 - R_M.
$$
 (16)

B. Decoding

As has been widely used elsewhere, the decoders employ the belief propagation algorithm over factor graphs. The decoding at the relay is straightforward. Upon receiving $y_1(i)$ = $\frac{1}{d\alpha}$ **x**(w_i) + **z**₁(*i*), the relay decodes **x**(w_i) using a single-user factor graph.

Because of the encoding block Markov property, $I(X_k^i; Y(1), \ldots, Y(i), Y(i+1), \ldots) = I(X_k^i; Y(i), Y(i+1))$
where X^i is the *k*th bit of the *i*th block. Thus the factor where X_k^i is the k^{th} bit of the i^{th} block. Thus, the factor graphs used at the destination are derived from the MAP rule (see [13])

$$
\arg\max_{X_k^i \in \{\pm\sqrt{P}\}} p_{X_k^i | Y(i), Y(i+1)}(x_k^i | y(i), y(i+1)).\tag{17}
$$

Upon receiving $y(i)$, the destination decodes $x_1(s_i)$ using the graph depicted in Fig. 7. An iteration consists in simultaneous decoding rounds through the constraints corresponding to H and H_1 and then in passing information from one side of the graph to the other through the middle nodes which receive the channel observation $y(i)$. Thus, since $R \geq R_1$, the information-theoretic bound on R_1 is given by

$$
R_1 \le I(X_1;Y). \tag{18}
$$

Upon receiving $y(i+1)$, the destination decodes $x_1(s_i+1)$ in the same way and uses its estimate \hat{s}_{i+1} to fix the constraints corresponding to M in the previous graph of block ⁱ. According to (12) and (16), this transforms the rate R of $x(w_i)$ into R^* such that

$$
R^* = R - R_1. \tag{19}
$$

In order to maximize R , we thus have to maximize the sum rate $R^* + R_1$.
Next the de

Next, the decoder decodes $x(w_i)$ using the decoding graph depicted in Fig. 6, where $\mathbf{x}(w_i)$ has an artificial lower-rate R^*
and the input observation depends on the received sequence and the input observation depends on the received sequence $y(i)$, but also on the estimate $\hat{x}_1(s_i)$.

VII. DENSITY EVOLUTION

Under the decoding procedure discussed in Section VI-B and since H , H_1 and M are chosen randomly, the decoding of a specific bit is asymptotically tree like if we let the block length grow to infinity and we assume a finite number of iterations. Therefore we can employ the density evolution method in order to analyze the performance of our scheme (see [2]).

We consider our BAWGN model expressed by (1) and (2) , with SNR = 0 dB and $\alpha = 2$ in the independent codes regime. In order to optimize the decoding at the relay, we have to use a good single-user code for H. Following Section III, the relay is the only bottleneck in this regime, the choice of H_1 and M for the decoding at the destination is less crucial. We have thus decided to use some good single-user codes for H_1 and M, without doing any LDPC degree distribution optimization.

It turns out that the theoretical results of Section III are confirmed for our practical scheme and the density evolution shows that we can achieve rates that are ~ 0.02 to 0.03 dB away from R_{DE} in the independent codes regime. In particular, if the relay is at a distance $d = 0.3544$ from the source, we can achieve a rate $R = 0.99$ for $\sigma = 1.0$, which is only 0.0248 dB away from the R_{DF} limit $\sigma_{\text{DF}} = 1.0029$.

VIII. SIMULATION RESULTS

We saw in Section IV that errors made by the relay affect the decoding at the destination. This problem does not appear in density evolution, since the error probability at the relay tends to zero when we are under threshold. However, when we work with finite length codes, the probability of error at the relay increases as R approaches R_{DF} and these errors are propagated to the destination.

Fig. 8. Bit error probability at the relay and at the destination for a block length $n = 2^{14}$, $R = 0.95$, $R_M = 0.46$, $R_1 = 0.54$ and $d = 0.446$ with $\alpha = 2$.

Fig. 8 depicts the bit error probability at the relay and at the destination for the triple rates $R = 0.95, R_M = 0.46, R_1 =$ 0.54 and $d = 0.446$ over the model corresponding to (1) and (2) with $n = 2^{14}$ and $\alpha = 2$. We see that the bit error probability at the destination can be reasonably small $(P_{\text{b}}^{\text{BP}} \simeq 10^{-6})$ if we are around 0.65 dB within the theoretical $\lim_{h \to 0} \tau$ limit σ_{DF} .

Fig. 9 compares three achievable points to R_{DF} in a rate perspective for a fixed bit error probability $P_b^{\text{BP}} \simeq 10^{-5}$.

IX. CONCLUSION

In this work, a decode-and-forward LDPC-based coding and decoding scheme has been proposed and applied to the single

Fig. 9. Three achievable rates for SNR=0.915 dB, with $P_b^{\rm BP} \simeq 10^{-5}$ and Fig. 9.
 $n = 2^{14}$

BAWGN relay channel. We have assumed that the relay is able to simultaneously receive and transmit. Both the relay and the destination apply successive iterative decoding using belief propagation.

We have evaluated the max-flow min-cut upper bound and the Cover and El Gamal decode-and-forward lower bound for the BAWGN relay channel. We have shown that uniformly distributed input marginals achieve these two bounds and that there is an important regime in which the maximizing joint input distribution is the independent one.

We have shown that in this regime, the performance of the proposed scheme can be as close as 0.02 dB away to the theoretical decode-and-forward limit for infinite length and 0.65 dB for block codes of length 2^{14} , with a corresponding bit error probability $P_b^{\text{BP}} \simeq 10^{-6}$.

ACKNOWLEDGMENT

Fruitful discussions with Prof. Rüdiger Urbanke (EPFL) are gratefully acknowledged.

REFERENCES

- [1] R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA, 1963.
- [2] T. Richardson, A. Shokrollahi, R. Urbanke, "Design of capacityapproaching irregular low-density prity-check codes", *IEEE Trans. Inform. Theory*, vol. 47, pp. 619-637, Feb. 2001.
- [3] T. Richardson, R. Urbanke, "Efficient encoding of low-density paritycheck codes", *IEEE Trans. Inform. Theory*, vol. 47, pp. 638-656, Feb. 2001.
- [4] A. Amraoui, S. Dusad, R. Urbanke, "Achieving general points in the 2-user gaussian mac without time-sharing or rate-splitting by means of iterative coding", *IEEE ISIT*, p. 334, Lausanne, Switzerland, July 2002.
- [5] T. M. Cover, A. A. El Gamal, "Capacity theorems for the relay channel", *IEEE Trans. Inform.Theory*, vol. 25, pp. 572-584, Sept. 1979.
- [6] G. Kramer, M. Gastpar, P. Gupta, "Cooperative strategies and capacity theorems for relay networks", *IEEE Trans. Inform.Theory*, vol. 51, pp. 3037-3063 , Sept. 2005.
- [7] B. Zhao, M. C. Valenti, "Distributed turbo coded diversity for relay channel", *IEE Electron. Lett.*, vol. 39, no. 10, pp. 786 787, May 2003.
- [8] Z. Zhang, I. Bahceci, T. M. Duman, "Capacity approaching codes for relay channels", *IEEE ISIT*, p. 2, Chicago, USA, June 2004.
- [9] M.A. Khojastepour, N. Ahmed, B. Aazhang, "Code design for the relay channel and factor graph decoding", *Signals, Systems and Computers*, Vol.2, pp. 2000 - 2004, Nov. 2004.
- [10] G. Kramer, "Communication strategies and coding for relaying", Inst. for Math. and its Appl. (IMA) 2005 Summer Program on Wireless Comm., Univ. of Minnesota, Minneapolis, MN, June 22-July 1, 2005, *to appear*.
- [11] T. Cover, J. Thomas, *Elements of Information Theory.* Wiley, New-York, 1991.
- [12] J. Ezri, '*LDPC Codes for the Relay Channel*, Master's Thesis, Univ. of California, Berkeley, CA and EPFL, Lausanne, Switzerland, Sept. 2005.
- [13] F. Kschischang, B. Frey, H.-A. Loeliger, "Factor graphs and the sumproduct algorithm", *IEEE Trans. Inform. Theory*, vol. 47, pp. 491-519, Feb. 2001.