International Symposium on Information Theory and Its Applications
Honolulu, Hawaii, U.S.A., November 5–8, 2000

Coding Theorems for Generalized Repeat Accumulate Codes

Henry D. Pfister and Paul H. Siegel

Signal Transmission and Recording Group
Department of Electrical and Computer Engineering
University of California, San Diego
La Jolla, CA 92093-0407, USA
Email: {hpfister,psiegel}@ucsd.edu

Abstract

In this paper, we present a coding theorem for the ensemble of Generalized Repeat Accumulate (GRA^m) codes. These codes are the serial concatenation of a terminated convolutional code and m interleaved rate-1 "accumulate" codes. This theorem generalizes the results of [1] and [2] by considering outer codes with $d_{free} = 2$ and multiple "accumulate" codes. For outer codes with $d_{free} \geq 2$, it proves the Interleaver Gain Exponent Conjecture for GRA^m codes. This leads to the new result that GRA^m codes will have vanishing word error probability for outer codes with $d_{free} = 2$, if and only if $m \geq 2$. Finally, we compute E_b/N_0 thresholds for selected GRA^m codes on the additive white Gaussian noise channel, and we observe that they are very close to the Shannon limit for $m \geq 3$.

1. Introduction

It is well-known that long random codes achieve reliable communication at noise levels up to the Shannon limit, but they provide no structure for efficient decoding. The introduction and analysis of Repeat Accumulate (RA) codes by Divsalar, Jin, and McEliece [1] shows that the concatenation of a repetition code and a rate-1 code, through a random interleaver, can also achieve reliable communication at noise levels near the Shannon limit. A more general analysis of serially concatenated rate-1 codes [3] implies that using more than one interleaved rate-1 code may yield further improvement.

The coding theorem for the ensemble of RA codes under maximum likelihood decoding, given in [1], states that, for all E_b/N_0 greater than a threshold which depends only on the repeat order $q \geq 3$, the serial concatenation of a repetition code and a rate-1 "accumulate" code will have vanishing word error probability as the block length goes to infinity. In [2], this theorem was extended to serial turbo codes, for outer codes with $d_{free} \geq 3$.

In this paper, we consider Generalized Repeat Accumulate (GRA^m) codes, which are the serial concatenation of a terminated convolutional code (TCC) and m interleaved rate-1 "accumulate" codes [3]. Following the approach pioneered in [1], we prove a coding theorem for ensembles of GRA^m codes on a memoryless channel with maximum likelihood decoding. The theorem states that if the outer code has $d_{free} \geq 2$ and the channel parameter z is less than some threshold z^*, then the probability of word error is $O(N^\nu)$, where ν is determined solely by m and d_{free}. The proof, based on the union bound, also gives loose lower bounds on the threshold z^*. A new tighter bound by Jin and McEliece [4] allows us to compute very accurate E_b/N_0 thresholds for the additive white Gaussian noise (AWGN) channel. For $m = 3$, many of these thresholds are virtually identical to the Shannon limit.

2. Weight Enumerators and the Union Bound

In this section, we review weight enumerators for linear block codes and the union bound on error probability for maximum likelihood decoding. The *input output weight enumerator* (IOWE) $A_{w,h}$ of an (N, K) linear block code is the number of codewords with input weight w and output weight h, and the *weight enumerator* (WE) A_h is the number of codewords with output weight h and any input weight. Using these definitions, the probability of word error is upper bounded by

$$P_W \leq \sum_{h=1}^{N} \sum_{w=1}^{K} A_{w,h} z^h = \sum_{h=1}^{N} A_h z^h, \tag{1}$$

and the probability of bit error is upper bounded by

$$P_B \leq \sum_{h=1}^{N} \sum_{w=1}^{K} \frac{w}{K} A_{w,h} z^h = \sum_{h=1}^{N} B_h z^h. \tag{2}$$

The term z^h, which depends on the channel of interest, represents an upper bound on the pairwise er-

This work was supported in part by NSF Grant NCR-9612802 and by the National Storage Industry Consortium.

ror probability for any two codewords differing in h positions. The parameter z can be defined for any memoryless channel; for the AWGN channel it is $z = e^{-(K/N)(E_b/N_0)}$.

3. Generalized Repeat Accumulate Codes

3.1. Description

A GRA^m code is the serial concatenation of a TCC and m interleaved rate-1 “accumulate” codes, and the ensemble of GRA^m codes is formed by using uniform random interleavers [5]. The ensemble averaged WE is

$$\overline{A}_{h_{m+1}}(N) = \sum_{(h_1,\ldots h_m)=(1,\ldots,1)}^{(N,\ldots,N)} A^{(o)}_{h_1}(N) \prod_{i=1}^{m} P^{(acc)}_{h_i,h_{i+1}}(N), \quad (3)$$

where $A^{(o)}_h$ is the WE of the outer TCC and $P^{(acc)}_{w,h}$ is the *input output weight transition probability* (IOWTP) [3] of the “accumulate” code. Using the IOWE given in [1], we have

$$P^{(acc)}_{w,h}(N) = \frac{\binom{N-h}{\lfloor w/2 \rfloor}\binom{h-1}{\lceil w/2 \rceil - 1}}{\binom{N}{w}} \text{ for } 1 \le w \le N. \quad (4)$$

Our main result is a theorem which characterizes the ensemble behavior of GRA^m codes. The theorem and proof make use of the asymptotic notation defined in [6]. Specifically, we write $O(f(n))$ for functions of order at most $f(n)$, $\Omega(f(n))$ for functions of order at least $f(n)$, and $\Theta(f(n))$ for functions of order exactly $f(n)$. The notation $o(f(n))$ refers to functions that, when divided by $f(n)$, converge to zero as n goes to infinity.

Theorem. *Consider the average performance of an ensemble of GRA^m codes, based on an outer TCC with $d_{free} \ge 2$, transmitted over a memoryless channel with channel parameter z. Let $\nu = 1 - \sum_{i=1}^{m} \lceil d_{free}/2^i \rceil$. Then, there exists a positive threshold z^* such that, for any $z < z^*$, the probability of word error under maximum likelihood decoding is $P_W = \Theta(N^\nu)$. If the outer code also has the property that, for all input-output weight pairs, $w \le th$ for some constant t, then the probability of bit error is $P_B = \Theta(N^{\nu-1})$.*

3.2. Proof of the lower bound $P_W(N) = \Omega(N^\nu)$

An important property of the “accumulate” code is that it never maps an input word of weight w to an output word of weight $h < \lceil w/2 \rceil$. This property can be seen mathematically by the fact that (4) is zero whenever $h < \lceil w/2 \rceil$. Let us consider the *multiplicity*, or the number of codewords, generated by any distinct *weight path* $(h_1, \ldots, h_{m+1})$ in (3). It will be identically zero if $h_{i+1} < \lceil h_i/2 \rceil$ for any $i = 1, \ldots, m$.

We can use this property to find the minimum distance, d_{min}, of the overall code and its multiplicity, $A_{d_{min}}$. Minimizing h_{m+1}, using the constraints $h_{i+1} \ge \lceil h_i/2 \rceil$, results in a weight path which starts at $h_1 = d_{free}$ and continues with $h_{i+1} = \lceil h_i/2 \rceil$ for $i = 1, \ldots, m$. This path leads to the overall minimum distance,

$$d_{min} = \lceil d_{free}/2^m \rceil . \quad (5)$$

It is well-known that a TCC has $\Theta(N)$ codewords with weight d_{free}. Using simple upper and lower bounds for the binomial coefficients, we can show that, for fixed $w, h \ge 1$ satisfying $N - \lfloor w/2 \rfloor \ge h \ge \lceil w/2 \rceil$,

$$P^{(acc)}_{w,h}(N) = \Theta(N^{-\lceil w/2 \rceil}).$$

Combining these results with (3) gives

$$A_{d_{min}} = \Theta(N^\nu) \text{ with } \nu = 1 - \sum_{i=1}^{m} \lceil d_{free}/2^i \rceil , \quad (6)$$

and applying the union bound gives $P^{UB}_W(N) = \Omega(N^\nu)$ and $P^{UB}_B(N) = \Omega(N^{\nu-1})$.

Furthermore, it is possible to show that the probability that any code in the ensemble has a codeword of weight d_{min} is $\Theta(N^\nu)$. The exact probability of decoding error due to any particular fixed weight codeword is $\Theta(1)$, so we can lower bound the exact probability of decoding error with

$$P_W(N) = \Omega(N^\nu) \text{ and } P_B(N) = \Omega(N^{\nu-1}).$$

3.3. Proof of the upper bound $P_W(N) = O(N^\nu)$

Using a similar strategy to [1], we break the proof into two parts. The first part considers the WE $\overline{A}^{\le h_N}_{h_{m+1}}(N)$ for output weights $h_{m+1} \le h_N$ and their contribution, $P^{\le h_N}_W(N)$, to the probability of error. The second part considers a weaker bound on the WE $\overline{A}_{h_{m+1}}(N)$ and the contribution, $P^{> h_N}_W(N)$, of output weights $h_{m+1} > h_N$ to the probability of error. The weight h_N is a function of N, and can always be chosen so that $P^{\le h_N}_W$ dominates the overall performance. Both parts involve bounds on binomial coefficients and the WE derived using the methods of [7].

3.3.1. Small output weights

The following two bounds, based on results taken from [7], assume that $h_{m+1} \le h_N$ and that we have chosen h_N in such a way that $\ln h_N / \ln N = o(1)$. Under those conditions, the WE of a TCC is

$$A^{(o)}_h(N) = O\left(N^{\lfloor h/d_{free} \rfloor}\right), \quad (7)$$

and the IOWTP of the “accumulate” code is

$$P^{(acc)}_{w,h}(N) = O\left(N^{-\lceil w/2 \rceil (1 - O(\ln h / \ln N))}\right). \quad (8)$$

Using the constraint $h_i \leq 2h_{i+1}$ for the limits of the sum, and applying (7) and (8) to (3) gives

$$\overline{A}^{\leq h_N}_{h_{m+1}}(N) = \sum_{(h_1,\ldots,h_m)=(1,\ldots,1)}^{(2^m h_N,\ldots,2h_N,h_N)} O\left(N^{\kappa(h_1,\ldots,h_{m+1})}\right),$$

where

$$\kappa(h_1,\ldots,h_{m+1}) = \lfloor h_1/d_{free} \rfloor - \sum_{i=1}^{m} \lceil h_i/2 \rceil (1-\epsilon_{i+1})$$

and $\epsilon_i = O(\ln h_i / \ln N) \to 0$. It is relatively simple to show that, ignoring the ϵ's, the weight path of the overall minimum distance (5) also maximizes $\kappa(h_1,\ldots,h_{m+1})$. For each h_{m+1}, there are multiple weight paths which maximize $\kappa(h_1,\ldots,h_{m+1})$ and, ignoring the case of $d_{free}=2$ and $m=1$, it is possible to show that the number of such paths is $O(1)$. For any h_{m+1}, let $\nu(h_{m+1})$ be the maximum of $\kappa(h_1,\ldots,h_{m+1})$ over all weight paths with non-zero multiplicity. Then

$$\nu(h_{m+1}) = \nu + O(\ln h_{m+1} / \ln N)$$

where ν is defined by (6). This is because all of the h_i, for $i=1,\ldots,m$, are constrained to be $O(1)$ by this maximization. Therefore all of the ϵ_i, for $i=1,\ldots,m$, can be included in the asymptotic constant. This leaves h_{m+1}, which is not constrained by the maximization, whose ϵ_{m+1} is retained as $O(\ln h_{m+1} / \ln N)$. Also, we can ignore all of the weight paths which do not maximize $\kappa(h_1,\ldots,h_{m+1})$, because their total contribution is $o(N^{\nu})$ (at most $O(h_N^m)$ terms each contributing $O(N^{\nu-1})$). Using the fact that $N^{O(\ln h_{m+1}/\ln N)} = O(h_{m+1}^k)$ for some k, we have the WE

$$\overline{A}^{\leq h_N}_{h_{m+1}}(N) = O\left(N^{\nu}(h_{m+1})^k\right). \tag{9}$$

Assuming that $z<1$, the substitution of (9) into the union bounds (1) and (2) gives geometric sums which result in $P_W^{\leq h_N}(N) = O(N^{\nu})$ and $P_B^{\leq h_N}(N) = O(N^{\nu-1})$. For the case of $d_{free}=2$ and $m=1$, these arguments do not hold, but as we will see in Section 3.3.3, the bounds on $P_W(N)$ and $P_B(N)$ still do.

3.3.2. Large output weights

We derive upper bounds for the WE of GRA^m codes which are sufficiently tight, for large output weights, to show that $P_W^{\leq h_N}(N)$ and $P_B^{\leq h_N}(N)$ are the asymptotically dominant terms of $P_W(N)$ and $P_B(N)$. The bounds are inductive in the sense that we use a parametric bound on the WE of GRA^m codes for $m=1$, and then show that each added "accumulate" stage leaves the form of the bound unchanged.

Using bounds from [7], it is possible to show that

$$P^{(acc)}_{w,h}(N) \leq \left(5e^2 h/N\right)^{\lceil w/d \rceil} \tag{10}$$

for any $d \geq 2$, and also that

$$A^{(o)}_h(N) \leq (N/h)^{\lfloor h/d_{free} \rfloor} g^h \tag{11}$$

where g is a constant which depends only on the particular code. For $m=1$, we apply to (3) the bound (10), with $d=d_{free}$, and the bound (11) . Using $h_1 \leq 2h_2$ for the limits of the sum gives

$$\overline{A}_{h_2}(N) \leq \sum_{h_1=d_{free}}^{2h_2} \left(\frac{Ng^{d_{free}}}{h_1}\frac{5e^2h_2}{N}\right)^{\lceil h_1/d_{free} \rceil}.$$

Finally, we upper bound this sum by $2h_2$ times the maximum value of its summand to get

$$\overline{A}_{h_2}(N) \leq 2h_2 a^{h_2} \tag{12}$$

where $\ln a = 5eg^{d_{free}}/d_{free}$. In general, this bound is reasonably accurate for small h_2 when $d_{free}=2$, and fairly weak otherwise.

Starting with $\overline{A}_{h_i}(N) \leq Ch_i a^{h_i}$, a more general form of (12), we consider the effect of adding another "accumulate" code. We can write (3) in an incremental form using the bound (10), with $d=2$, to see that

$$\overline{A}_{h_{i+1}}(N) \leq \sum_{h_i=1}^{2h_{i+1}} Ch_i a^{h_i} \left(5e^2 h_{i+1}/N\right)^{\lceil h_i/2 \rceil}.$$

This sum can be upper bounded by twice the sum of the terms with even h_i, so we let $b=5e^2a^2$ and take the dominant terms to get

$$\overline{A}_{h_{i+1}}(N) \leq \begin{cases} \frac{4Cbh_{i+1}/N}{(1-bh_{i+1}/N)^2} & \text{if } bh_{i+1} < N \\ 2C\left(h_{i+1}^2+h_{i+1}\right) & \text{if } bh_{i+1} = N \\ \frac{4Ch_{i+1}(bh_{i+1}/N)^{h_{i+1}+2}}{(1-bh_{i+1}/N)^2} & \text{if } bh_{i+1} > N \end{cases},$$

which, for large enough N, can be weakly upper bounded by

$$\overline{A}_{h_{i+1}}(N) \leq \widetilde{C} h_{i+1} \widetilde{a}^{h_{i+1}}. \tag{13}$$

for $\widetilde{a}=b$ and some $\widetilde{C}$. This is the same bound we started with, so by induction this bound holds for any fixed number of "accumulate" stages. In fact, this bound shows that the WE of GRA^m codes, with $m>1$, is $O(1)$ for all $h_{i+1} \leq N/b$, which gives us hope that choosing interleavers carefully could give a minimum distance that grows like $O(N)$.

Now we upper bound $P_W^{>h_N}(N)$ by combining (1) and (13) to get

$$P_W^{>h_N}(N) \leq \sum_{h_{m+1}=h_N+1}^{N} Ch_{m+1} a^{h_{m+1}} z^{h_{m+1}}.$$

Rate	γ^*	γ_1	γ_2	γ_3	ρ_1	ρ_2	ρ_3
1/3	-0.495	0.739	-0.478	-0.495	0.50	1.65	3.76
1/4	-0.794	-0.078	-0.790	-0.794	0.12	2.20	4.61
1/5	-0.964	-0.494	-0.962	-0.963	0.06	2.69	5.31
1/6	-1.073	-0.742	-1.072	-1.073	0.11	3.13	5.90
1/7	-1.150	-0.905	-1.149	-1.150	0.19	3.52	6.41

Table 1: E_b/N_0 thresholds in dB for RA^m codes.

For all z satisfying $az < 1$, we can upper bound the geometric sum to get

$$P_W^{>h_N}(N) \le \frac{C(h_N+1)(az)^{h_N}}{(1-az)^2}.$$

Letting $h_N = (\ln N)^2$ and $\delta = \ln az < 0$, we have

$$P_W^{>h_N}(N) = O\left((\ln N)^2\right) N^{\delta \ln N} = o(N^{\nu-1}). \qquad (14)$$

So our threshold $z^* = 1/a$ and, for any $z < z^*$, this proves that $P_W^{\le h_N}(N)$ dominates $P_W^{>h_N}(N)$ for all GRA^m codes. Combining (14) with the fact that $P_B \le P_W$ also makes it clear that $P_B^{\le h_N}(N)$ dominates $P_B^{>h_N}(N)$.

3.3.3. The special case of $d_{free} = 2$ and $m = 1$

It turns out that GRA^m codes with $d_{free} = 2$ and $m = 1$ have a WE (12) which grows exponentially in h_2. The WE is not growing with N, however, and is $O(1)$ for fixed h_2. Applying the union bound (1) to (12) gives

$$P_W(N) \le \sum_{h_2=1}^{N} \left(2h_2 a^{h_2}\right) z^{h_2}. \qquad (15)$$

Even as $N \to \infty$, this sum is upper bounded by a constant if $az < 1$. So our threshold $z^* = 1/a$ and, for all $z < z^*$, we have $P_W(N) = O(1)$. This bound is trivial though, because all probabilities are upper bounded by a constant. Examining (15) more carefully, however, shows that the constant will be less than 1 for sufficiently small z. Using the input-output weight pair condition from the theorem and the inequality $h_i \le 2h_{i+1}$, we have the bound $w \le th_1 \le 2th_2$. Applying the union bound (2), we get

$$P_B(N) \le O\left(N^{-1}\right) \sum_{h_2=1}^{N} h_2 \left(2h_2 a^{h_2}\right) z^{h_2}.$$

Once again, if $az < 1$, the sum is upper bounded by a constant for all N. So, for all $z < z^*$, we have $P_B(N) = O(N^{-1})$. This completes the proof of the theorem.

4. The IGE Conjecture

The IGE conjecture considers the growth rate of the WE $\overline{A}_{h_{m+1}}(N)$ in N for fixed h_{m+1} as the block length goes to infinity. Following [1], we define

Rate	γ^*	γ_1	γ_2	γ_3	ρ_1	ρ_2	ρ_3
1/2	0.187	3.419	0.327	0.188	3.42	1.23	2.72
4/5	2.040	4.388	2.206	2.044	4.39	2.62	3.36
8/9	3.033	5.034	3.187	3.037	5.03	3.49	4.04
12/13	3.591	5.425	3.736	3.596	5.43	3.99	4.46
16/17	3.971	5.700	4.109	3.976	5.70	4.33	4.77

Table 2: E_b/N_0 thresholds in dB for PA^m codes.

$$\alpha(h_{m+1}) = \limsup_{N \to \infty} \log_N \overline{A}_{h_{m+1}}(N) \qquad (16)$$

and

$$\beta_M = \max_{h_{m+1} \ge 1} \alpha(h_{m+1}). \qquad (17)$$

The IGE Conjecture [1] predicts that there exists a threshold channel parameter z^* such that, for any $z < z^*$, the probability of word error is $P_W = O(N^{\beta_M})$. Another commonly cited variation of the IGE Conjecture also predicts that, under the same conditions, the probability of bit error is $P_B = O(N^{\beta_M - 1})$.

For GRA^m codes, it follows from (6), (9), (12), and the definitions (16) and (17) that

$$\beta_M = \max_{h_{m+1} \ge 1} \limsup_{N \to \infty} \log_N \overline{A}^{\le h_N}_{h_{m+1}}(N) = \nu.$$

Therefore, the IGE Conjectures for P_W and P_B of GRA^m codes are corollaries of the theorem.

5. Computing the Threshold

The results of Section 3.3.2 give an analytical method to compute the threshold z^* for GRA^m codes, but the thresholds computed are quite loose. In this section, we outline a method which computes tight bounds on the spectral shape of an ensemble of GRA^m codes. Using these bounds, we apply the techniques of [8] and [4] to calculate very accurate E_b/N_0 thresholds for the AWGN channel.

5.1. Tight bounds on the spectral shape

Let us consider the *spectral shape* of the WE, $r_N(x) = (\log A_{\lfloor Nx \rfloor})/N$, as defined by [8]. For TCCs with no memory, we can use the method of [9, p. 15] to compute tight bounds on the spectral shape of the outer code. Using similar bounds on (4), we can track the evolution of the spectral shape of the WE as it passes through each "accumulate" encoder. Let $r_N^{(0)}(x_0)$ be the spectral shape of the outer code's WE, and let $r_N^{(i)}(x_i)$ be the spectral shape of the WE after the ith "accumulate" encoder. Then, we can show that

$$r_N^{(i+1)}(x_{i+1}) \le \frac{O(\log N)}{N} + \max_{0 \le x_i \le 1} \left[r_N^{(i)}(x_i) + f(x_i, x_{i+1}) \right]$$

where

$$f(x,y) = (1-y)H\left(\frac{x}{2(1-y)}\right) + yH\left(\frac{x}{2y}\right) - H(x).$$

5.2. Thresholds for typical pairs decoding

In Section 3.3.2, we bounded $P_W^{>h_N}(N)$ using the union bound for maximum likelihood decoding. This allows us to compute loose lower bounds on the threshold z^* for a wide variety of memoryless channels. The methods in [4] and [8], based upon an analysis of the "typical pairs" decoder, yield very good threshold estimates for binary linear codes on memoryless, symmetric channels, including the BSC and AWGN channel. Using the results of Section 5.1, we applied these methods to compute E_b/N_0 thresholds for Repeat Accumulate (RA^m) and Parity Accumulate (PA^m) codes. Tables 1 and 2 show the results for $m = 1, 2,$ and 3.

In the tables, γ^* denotes the Shannon limit and γ_m denotes the typical pairs decoding threshold. Note that the thresholds are very close to the Shannon limit for $m=3$. The value ρ_m denotes an upper bound to the iterative decoding threshold using a message passing decoder. The iterative decoding analysis, based on [10], holds for all asymptotically long GRA^m codes that have an asymptotically large number of independent decoding iterations.

6. Concluding remarks

In this paper, we proved a coding theorem for the ensemble of Generalized Repeat Accumulate (GRA^m) codes. This theorem extends the results of [1] and [2] to serial concatenations that incorporate outer codes with $d_{free}=2$ and multiple interleaved "accumulate" codes. As a corollary, we confirmed the validity of the Interleaver Gain Exponent (IGE) Conjecture for GRA^m codes where the outer code satisfies $d_{free} \geq 2$. We also computed E_b/N_0 thresholds for selected GRA^m codes on the AWGN channel.

The theorem implies that, for suitably high E_b/N_0, GRA^m codes will have vanishing word error probability for outer codes with $d_{free}=2$, if and only if $m \geq 2$. As an illustration of this result, Figure 1 compares word-error-rate (WER) simulation results for a rate 1/2 RA code and a rate 1/2 RA^2 code. The $m=1$ code shows no interleaving gain, while the $m=2$ code clearly does.

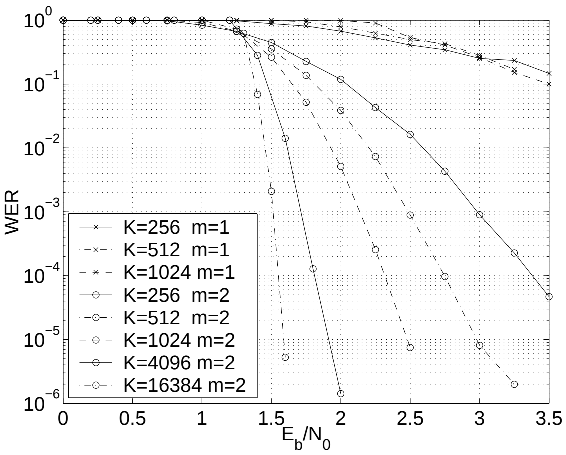

Figure 1: Simulation results for rate 1/2 RA^m codes.

References

[1] Dariush Divsalar, Hui Jin, and Robert J. McEliece, "Coding theorems for "turbo–like" codes," in *Proc. 36th Annual Allerton Conf. on Commun., Control, and Comp.*, Monticello, IL, USA, Sept. 1998, pp. 201–210.

[2] Hui Jin and Robert J. McEliece, "AWGN coding theorems for serial turbo codes," in *Proc. 37th Annual Allerton Conf. on Commun., Control, and Comp.*, Monticello, IL, USA, Sept. 1999, pp. 893–894.

[3] Henry D. Pfister and Paul H. Siegel, "The serial concatenation of rate 1 codes through uniform random interleavers," in *Proc. 37th Annual Allerton Conf. on Commun., Control, and Comp.*, Monticello, IL, USA, Sept. 1999, pp. 260–269.

[4] Hui Jin and Robert J. McEliece, "Typical pairs decoding on the AWGN channel," in *Int. Symp. on Inform. Theory and its Applications*, Honolulu, HI, USA, Nov. 2000, To appear.

[5] Sergio Benedetto and Guido Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 409–428, March 1996.

[6] Donald E. Knuth, "Big omicron and big omega and big theta," *SIGACT News*, vol. 8, no. 2, pp. 18–24, April 1976.

[7] Nabil Kahale and Rudiger Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. IEEE Int. Symposium on Inform. Theory*, Cambridge, MA, USA, Aug. 1998, IEEE, p. 31.

[8] Srinivas Aji, Hui Jin, Aamod Khandekar, David J. C. MacKay, and Robert J. McEliece, "BSC thresholds for code ensembles based on "typical pairs" decoding," in *IMA 1999 Summer Program: Codes, Systems and Graphical Models*, Aug. 1999, To appear in the proceedings.

[9] Robert G. Gallager, "Low-density parity-check codes," Research Monograph 21, The M.I.T. Press, Cambridge, MA, USA, 1963.

[10] Thomas Richardson and Rudiger Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," Submitted to IEEE Trans. Inform. Theory, Nov. 1998.