

Gallager Codes for CDMA Applications—Part I: Generalizations, Constructions, and Performance Bounds

Vladislav Sorokine, *Member, IEEE*, Frank R. Kschischang, *Member, IEEE*, and Subbarayan Pasupathy, *Fellow, IEEE*

Abstract—We focus on applications of low-rate Gallager (low-density parity-check) codes in code-division multiple-access schemes. The codes that we present here achieve good performance with relatively short frame-lengths in additive white Gaussian noise channels and, perhaps more importantly, in fading channels. These codes can be decoded with low complexity by using iterative decoding procedures. We present a construction that yields good short frame-length Gallager codes. Bounds on the frame-error probability for a maximum-likelihood decoder are obtained.

Index Terms—CDMA, iterative decoding, low-density parity-check codes.

I. INTRODUCTION

THE PARADIGM shift in coding theory toward suboptimal yet effective decoding procedures for powerful random-like codes, e.g., turbo codes [1], [2], has led to practical engineering advances. Turbo codes were shown to perform very close to the Shannon capacity of a Gaussian channel with an iterative turbo-decoding algorithm [3], and recently [4], highly optimized irregular low-density parity-check codes have been shown to come even closer to the Gaussian channel capacity than turbo codes. Remarkably, both families of codes are decoded using the same algorithm: the *sum-product algorithm*. (The sum-product algorithm is also known as the “forward/backward” [5] or “BCJR” [6] and is also related to the Baum–Welch [7] algorithm. See [8] for a tutorial treatment.) The excellent performance obtained with a practical decoding algorithm have made turbo codes extremely attractive in applications, and various integrated circuit solutions have already appeared, e.g., [9], or are in development.

Interestingly, the idea of combining long random codes with an iterative decoding algorithm was already present in Gallager’s pioneering work [10], in which he described and analyzed a class of random linear codes characterized by sparse parity-check matrices. Gallager showed that these codes are

“good,” i.e., with maximum-likelihood decoding they achieve arbitrarily small probability of error for rates bounded away from zero. Gallager also proposed a simple yet effective iterative decoding procedure for these codes. For a class of codes to be not just “good” but “very good,” it is required that the class contains codes that achieve arbitrarily small probability of error for all rates up to channel capacity. Gallager [10] showed that if the row weight of the parity-check matrix for a family of low-density parity-check codes is fixed, then such codes cannot be “very good.”

Zyablov and Pinsker [11] analyzed the error-correcting capabilities of Gallager codes and also proposed a simple “bit-flipping” decoding algorithm. MacKay and Neal independently rediscovered Gallager codes [12], [13] and proved that Gallager codes are “very good” for a variety of communications channels. Extensive simulation results [13] show that Gallager codes coupled with iterative decoding achieve excellent performance for Gaussian channels.

Iterative decoding is perhaps best understood as decoding on a graph that reflects the code’s structure [8], [14]–[20]. For example, a *Tanner graph* [14] describes the check structure of a code and plays a special role in iterative decoding algorithms. Certain instances of iterative decoding have been known for some time in the artificial intelligence community as *probability propagation* [16] in certain graphical models (see also [8] and [21]).

Powerful low-rate error-correcting codes that can be decoded with a relatively low complexity are of special interest in code-division multiple-access (CDMA) applications. Viterbi’s classic paper [22] showed that the use of powerful error correcting codes may significantly increase the capacity of a CDMA system. Developments following similar lines appeared in [23]–[25].

In this two-part paper, we present a family of low-rate, short-frame Gallager codes that have good performance both in additive white Gaussian noise (AWGN) channels and Rayleigh fading channels and can be used as an error protection scheme in CDMA systems.

The paper is organized as follows. In Section II, we introduce notations and definitions that will be useful throughout the paper. In Section III, we present a particular construction for low-rate, low-density parity-check codes that yields a significant performance improvement relative to other “candidate” constructions described in this section. This construction can be used to obtain codes with parameters suitable for application in IS-95-like CDMA systems. In Section IV, we study the

Paper approved by W. E. Ryan, the Editor for Modulation, Coding, and Equalization of the IEEE Communications Society. Manuscript received February 16, 1999; revised May 20, 1999 and August 31, 1999. This work was supported in part by the Natural Sciences and Engineering Research Council, Canada. This paper was presented in part at the 1997 Canadian Workshop on Information Theory, Toronto, ON, Canada, June 1997, the 1998 Information Theory Workshop, Killarney, Ireland, June 1998, and the Ninth International Symposium on Personal, Indoor and Mobile Communications (PIMRC), Boston, MA, September 1998.

The authors are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: vsorokin@qualcomm.com).

Publisher Item Identifier S 0090-6778(00)08781-X.

distance properties of the constructed subfamilies of Gallager codes. Bounds on the frame-error probability for a maximum-likelihood decoder are derived in Section V. Finally, we present a discussion of the main results in Section VI.

In Part II, we focus attention on codes with parameters compatible with the IS-95 cellular radio standard. We discuss low-complexity software and hardware decoder implementation issues. We also present simulation results for AWGN and fully interleaved Rayleigh fading channels with and without channel state information (CSI). We use the simulation results for a simplified analysis of the capacity of a single CDMA cell.

II. NOTATIONS AND DEFINITIONS

Let \mathcal{C} be a binary linear (N, K, D) code, i.e., a code of block length N , dimension K , and minimum Hamming distance D . Let $M = N - K$; then \mathcal{C} has an $M \times N$ parity-check matrix H , and every codeword $c \in \mathcal{C}$ satisfies the parity-check equation $c \cdot H^T = 0$.

Suppose a parity-check matrix H for a code \mathcal{C} exists with the property that H has some fixed number $j \in \mathbb{Z}^+$ of ones [that lie in the Galois field $GF(2)$] in each column (which we shall call *the column property*) and some fixed number $k \in \mathbb{Z}^+$ of ones in each row (*the row property*). We then call code \mathcal{C} an $\{N, j, k\}$ linear code [10]. If an H for \mathcal{C} exists with either the row property or the column property, then we denote such codes as $\{N, -, k\}$ or $\{N, j, -\}$ codes, respectively, where the “blank” is used instead of the corresponding parameter. Similarly, if the code’s minimum distance is unknown (or is not important), we may denote such code as an $(N, K, -)$ code.

Note that the parameters j and k in the notation $\{N, j, k\}$ characterize a particular parity-check matrix for \mathcal{C} . An equivalent parity-check matrix for the same code does not need to preserve them. The notation $\{N, j, k\}$ rather describes the structure of a particular parity-check matrix for \mathcal{C} .

Example. (7,4,3) Hamming Code: This is the Hamming code with parameters $(N = 7, K = 4, D = 3)$. One possible parity-check matrix is given by

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Note that H also qualifies as a parity-check matrix for a $\{7, -, 4\}$ code.

Historically, most studied linear codes have certain “structure,” such as the above (7,4,3) Hamming code. However, some results about ensembles of linear codes are also available. One can obtain a *random* linear code if H is generated randomly (with possible constraints). It is known that there exist long random linear codes that achieve capacity for many communications channels [26], [27].

In practice, however, one is also concerned with the complexity of the decoding algorithm. An arbitrary random linear code may have decoding complexity that is too high for most practical purposes, hence, one can consider a subclass of linear codes for which effective decoding algorithms can be devised.

One such subclass is *low-density parity-check* codes. A typical parity-check matrix for a binary low-density parity-check code is a very sparse matrix, i.e., a matrix with a very low density of nonzero matrix elements. This sparsity is precisely the property that makes effective and fast decoding of these codes possible.

One can further restrict the ensemble of linear codes by imposing certain “uniformity” constraints on H , such as the row and column properties ($\{N, j, k\}$ codes). These are the codes studied by Gallager [10]. Most codes that we consider have only the row property ($\{N, -, k\}$ codes), which one can view as a certain generalization of the codes studied by Gallager, though we still shall refer to them as *Gallager codes*. Depending on the particular procedure by which H is generated, it is possible to consider subfamilies of Gallager codes. We refer the reader to [10] and [13] where several explicit constructions for Gallager codes are given and analyzed.

In this paper, we restrict ourselves to low-rate, relatively short-frame Gallager codes for compatibility with typical CDMA cellular radio applications. In particular, if the data rate is 9600 bits/s and the (traffic) frame duration is 20 ms (as in IS-95), then the frame contains 192 bits of data. We assume this data frame length as a “target” frame length throughout the paper. We may note that IS-95 stipulates that these data bits are encoded with a rate-1/2 convolutional code to produce the modulation symbol stream at the rate of 19.2×10^3 symbols/s (this modulation symbol rate is kept constant across different rate sets in IS-95).

III. CONSTRUCTIONS FOR GALLAGER CODES

We considered various constructions for low-rate Gallager codes, some of which have been investigated previously in [10] and [13].

Gallager describes [10] a construction for $\{N, j, k\}$ codes in which a parity-check matrix consists of j blocks with N/k rows in each block, and furthermore, each column in a block having exactly one nonzero element. This construction can be further modified [10, p. 91] so that the parity-check matrix contains no short cycles. (A cycle in H is a sequence of distinct row-column indices $(r_1, c_1), (r_2, c_2), \dots, (r_n, c_n)$, n even, with $r_1 = r_2$, $c_2 = c_3$, $r_3 = r_4$, etc., and $c_n = c_1$, and for each index (r_i, c_i) , the corresponding entry in H is nonzero.)

Initially in [10], the existence of such cycles in H prevented the exact error-probability analysis of the iterative decoding procedure, and the shorter the cycles are, the sooner the exact analysis breaks down. Hence, an effort was made [10, p. 91] to eliminate them. However, the existence of a relatively small number of short cycles does not appear to be too damaging for iterative decoding [13].

In our search for good low-rate error-correcting codes, we investigated the following constructions.

Construction 1: (This construction is similar to the one considered by MacKay [13].) We generated H randomly, with column Hamming weight 3, and with row Hamming weight as uniform as possible. The following is an example

of a parity-check matrix generated by this construction [with parameters $(8, 2, -), \{8, 3, 4\}$]:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We found that the performance of rate-1/2 and rate-1/4 codes of relatively short block lengths of 512 bits obtained by this construction is similar to that reported in [10] and [13]. If the block length is decreased to 384 bits (to achieve an IS-95 compatible $K = 192$, rate-1/2 code), we observed a deterioration in the code's performance. Hence, our search did not yield codes with desired characteristics using this construction.

Construction 1A: We modified Construction 1 so that no two columns have an overlap greater than 1, thereby eliminating cycles of length 4 in H . The process of short cycle breaking is shown below. Elements enclosed in the boxes in the top matrix are the corners of a cycle.

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & \boxed{1} & \boxed{1} & 1 & 0 & 0 & 1 & 0 \\ 0 & \boxed{1} & \boxed{1} & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

↓

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & \boxed{1} & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & \boxed{1} & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & \boxed{1} & \boxed{1} & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

Note that in the matrix in (1), we *cannot* break all short cycles because the density of the matrix is high; however, breaking all such cycles is possible for low-density matrices. We obtained a slight improvement in performance (≈ 0.5 dB) compared with Construction 1 for all code rates (1/2, 1/4, and 1/8) but rate-1/8 codes (that, we hoped, could work for $K = 192$) were still poor.

After considerable experimental work, we discovered a construction similar to that in [10, Fig. 2.1], which we shall call *Construction 2*.

Construction 2: Let $k = 3$ be a divisor of N . The first row of the parity-check matrix H contains k ones in the first k positions and zeros in all other positions. Each of the next $N/k - 1$ rows is obtained by cyclic shifting of the immediately preceding row by k positions to the right, until column N contains a one. These rows form the *top* part of the parity-check matrix H . The dimensions of the top part of H are $N/k \times N$. Let $t = \lfloor kM/N \rfloor$.

Now $t - 1$ blocks of the parity-check matrix H are formed by a random permutation of the columns of the top block. Let $s = M \bmod N/k$. The bottom part of the matrix H is formed by permuting the columns of the first s rows of H .¹

The values of M and N in Construction 2 were restricted so as to be compatible with the desired code parameters ($K = 192$ and the code rate $R = 1/8$). This restriction causes the bottom part of H to contain fewer rows than the top part. The ramifications of this fact turn out to be very important for the code performance. We will further discuss this issue later in this section.

We compared the performances of Constructions 1A and 2. In these constructions, the code rates R and information block lengths K were assumed to be 1/8 and 192 bits, respectively. It is worth noting that Construction 2 produces parity-check matrices whose columns contain either 2 or 3 ones. (To be exact, for codes with parameters $M = 1344$, $N = 1536$, and $k = 3$, the parity-check matrix will contain 960 weight-3 columns and 576 weight-2 columns.) In this, Construction 2 differs (as it turns out, significantly) from both Constructions 1 and 1A. The performance improvement that Construction 2 yields is shown in Fig. 1.

Originally, we arrived at Construction 2 in an attempt to reduce the possibility of linear dependencies among rows of H by introducing the top block of H in a systematic-like form. Since the codes that we consider are low rate, parity check matrices for these codes are almost square (and sparse). We generated parity check matrices randomly, so we argued that, as the number of rows in H increases in order to achieve the desired low code rate, it is more and more likely that any new rows that are being added to H are linear combinations of rows already present in H , and hence, the effective code rate is greater than the target rate. It is possible, of course, but not easy to verify if all rows in H are linearly independent since it requires the rank determination of H .

However, the real reason for the good performance of the combination Construction 2–iterative decoder, lies (though we cannot prove this at the moment) in the “weak” parity-check structure of the code,² i.e., each column of H contains either two or three nonzero elements (we will say later [Part II] that each “site” is connected to two or three checks).

An example of the parity-check matrix H obtained by this construction (with $N = 9$ and $M = 7$) is shown below.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

¹Note that Construction 2 may be derived from the construction by Gallager for $\{N, j, k\}$ codes [10] by deleting some rows of H .

²MacKay has experimented extensively with similar parity-check matrices for Gallager codes [13]. Most recently, analysis and optimizations for irregular low-density parity-check codes with sum-product decoding have appeared in [4] and [28].

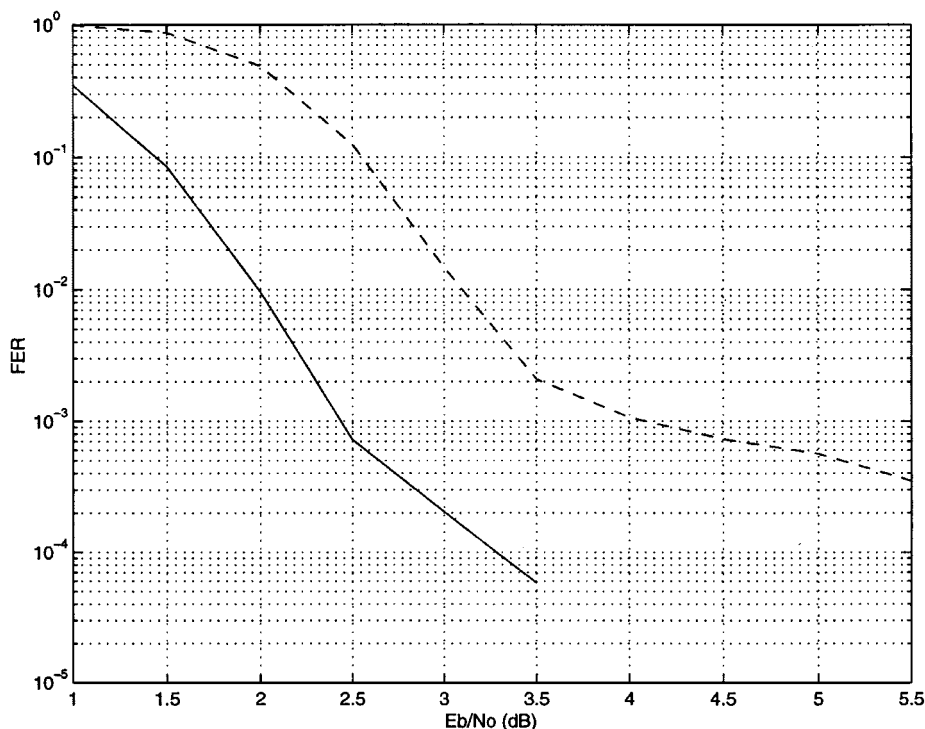


Fig. 1. Performance comparison of Constructions 1A and 2 for rate-1/8, block length 1536 Gallager codes. Construction 1A (dashed line). Construction 2 (solid line). Both curves are simulation results obtained by using the iterative sum-product decoding algorithm.

Note that in some instances the required block length N may not be a multiple of k . We bypass this difficulty by generating H with a slightly greater number of columns that is a multiple of k and then simply deleting extra columns in H .

IV. $\{N, -, 3\}$ GALLAGER CODES: MINIMUM HAMMING DISTANCE AND USEFUL BOUNDS

In this section, we analyze distance properties of rate-1/8 Gallager codes obtained by Construction 2. As before, we partition the parity-check matrix H for the Construction 2 into three blocks, where the upper two blocks of H have dimension $N/k \times N$ each, and the bottom block of H has dimensions $[(1 - R)N - 2N/k] \times N$. Gallager [10, p. 13] derived the following bound on the number of sequences with a given Hamming distance that are orthogonal to each block of H for an $\{N, j, k\}$ code.

For each code in an $\{N, j, k\}$ ensemble, the number $N_1(l)$ of sequences of weight l that satisfies any block of N/k parity-checks is bounded by

$$N_1 \left[\frac{N}{k} \mu'(s) \right] \leq \exp \left[\frac{N}{k} [\mu(s) + (k - 1) \ln 2 - s\mu'(s)] \right] \quad (3)$$

where

$$\mu(s) = \ln 2^{-k} [(1 + e^s)^k + (1 - e^s)^k] \quad (4)$$

$$\mu'(s) = \frac{d\mu(s)}{ds} \quad (5)$$

and s is an arbitrary real parameter.

The number of sequences of a certain Hamming weight that are orthogonal to the top two blocks of H for the $\{N, -, 3\}$

Gallager codes (for the remainder of this paper, whenever we refer to the $\{N, -, 3\}$ ensemble of codes, we will assume that they are produced by Construction 2) can also be bounded by (3) since these blocks have a structure identical with $\{N, j, 3\}$ Gallager codes. The proof of Gallager [10, p. 13] of the above proposition can be applied *mutatis mutandis* to compute the number of sequences with certain Hamming weight that are orthogonal to the bottom block of $(1 - R)N - 2N/k$ checks in an $\{N, -, 3\}$ code, thereby yielding the following result.

For a random block of $(1 - R)N - 2N/k$ parity-checks, the number $N_1(l)$ of sequences of weight l in an $\{N, -, 3\}$ code that satisfies the parity-checks is bounded by

$$N_1 \left[\frac{N}{k} \mu'(s) \right] \leq \frac{1}{2} \exp \left\{ \frac{N}{k} [\mu(s) + (k - 2) \ln 2 - s\mu'(s)] - RN[\mu(s) + (k - 1) \ln 2] + \eta(s) \right\} \quad (6)$$

where $s, \mu(s), \mu'(s)$ are the same as in (4) and (5), $k = 3$ and

$$\eta(s) = \ln [(1 + e^s)^{kRN} + (1 - e^s)^{kRN}]. \quad (7)$$

The probability that a randomly chosen weight l sequence of length N satisfies either one of the top complete blocks or the last incomplete block of parity-checks is $N_1(l)/\binom{N}{l}$, where $N_1(l)$ is bounded by either (3) (denote it N_1^c , where c stands for complete) or (6) (denote it N_1^i , where i stands for incomplete). Since the random permutations used to generate the second and third blocks of H are independent of each other, we can write

$$P(l) = [N_1^c(l)]^2 [N_1^i(l)] / \binom{N}{l}^3$$

for the probability that a randomly chosen binary N -tuple of weight l satisfies *all* of the parity checks. Then, we obtain the following result.

Over the ensemble of $\{N, -, 3\}$ codes obtained by Construction 2, the average³ number of codewords of (even⁴) weight l is given by

$$\overline{N(l)} = \binom{N}{l}^{-2} [N_1^c(l)]^2 [N_1^i(l)]. \quad (8)$$

The Stirling approximation gives the following bound on $\binom{N}{N\lambda}$ [29, p. 530]:

$$[2\pi N\lambda(1-\lambda)]^{-1/2} \exp\left[NH(\lambda) - \frac{1}{12N\lambda(1-\lambda)}\right] < \binom{N}{N\lambda} \quad (9)$$

where λ is l/N and $H(\lambda)$ is the natural entropy function.

From (8) and (9), we can derive the following bound on the number of weight l sequences in an $\{N, -, 3\}$ code:

$$\overline{N(l)} \leq C(\lambda, N) \exp[-NB(\lambda)] \quad (10)$$

where

$$C(\lambda, N) = \frac{1}{2} [2\pi N\lambda(1-\lambda)] \exp \frac{2}{12N\lambda(1-\lambda)}$$

$$B(\lambda) = 2H(\lambda) - (1-R)\mu(s) - 2(1-R) \ln 2 + 3\lambda s - \eta(s)/N$$

and $\lambda = l/N$.

One can obtain useful bounds on certain code parameters from the behavior of the function $B(\lambda)$. In particular, suppose $B(\lambda)$ has a zero crossing at $\lambda = \lambda_0$, and suppose for $\lambda < \lambda_0$, $B(\lambda) > 0$. Then, assuming that the bound (10) is tight, $\lambda_0 N$ is the typical minimum distance of the ensemble of $\{N, -, k\}$ codes, since for large enough N , the probability that a code contains a nonzero codeword of weight less than $\lambda_0 N$ tends to zero. Later in this section, using the special structure of H that arises when $k = 3$, we derive a "tighter" function $B(\lambda)$ by enumerating the sequences orthogonal to H directly.

In (7), $\eta(s)$ is dependent on N . We can remove the dependence by splitting the bound (10) into two parts and observing that only one part gives a significant contribution to the bound. Let us introduce the following functions:

$$\eta_1(s) = 3R \ln[1 + \exp(s)]$$

$$\eta_2(s) = 3R \ln[1 - \exp(s)]$$

$$B_1(\lambda) = 2H(\lambda) - (1-R)\mu(s) - 2(1-R) \ln 2 + 3\lambda s - \eta_1$$

and

$$B_2(\lambda) = 2H(\lambda) - (1-R)\mu(s) - 2(1-R) \ln 2 + 3\lambda s - \eta_2.$$

Then

$$\overline{N(l)} \leq C(\lambda, N) \{\exp[-NB_1(\lambda)] + \exp[-NB_2(\lambda)]\}. \quad (11)$$

³We count the number of occurrences of codewords of given weight in a code from the ensemble, and then average the number over all codes in the ensemble.

⁴Note that in Construction 2, the all-one codeword is in the code dual to \mathcal{C} , and can be generated by summing up the rows of the top block of H . Hence, any codeword in \mathcal{C} has to have an even weight to be orthogonal to the all-one codeword.

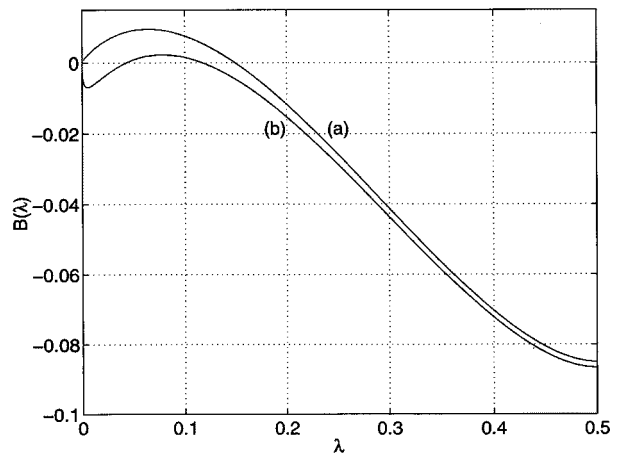


Fig. 2. (a) Function $B(\lambda)$ obtained by direct enumeration of sequences [expressions (12) and (13)] and (b) function $B_1(\lambda)$ obtained by bounding techniques of expressions (3) and (6).

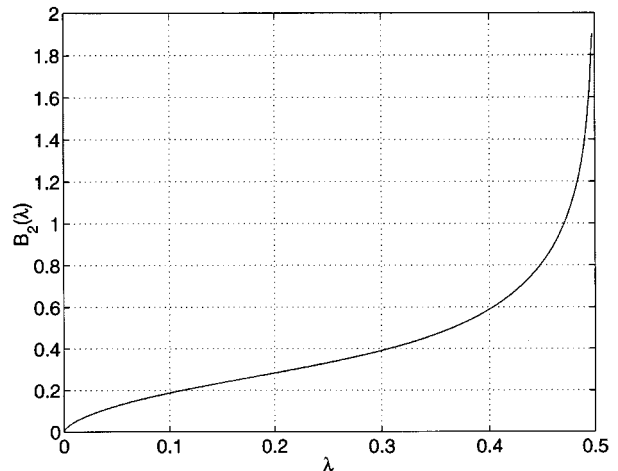


Fig. 3. Exponent $B_2(\lambda)$ in the upper bound on the average number of codewords of Hamming weight l in an $\{N, -, 3\}$ code.

A graph of the function $B_1(\lambda)$ is shown in Fig. 2 [curve (b)], and a graph of $B_2(\lambda)$ is shown in Fig. 3. Since $B_2(\lambda)$ is always positive, the contribution from $\exp[-NB_2(\lambda)]$ to the bound on $\overline{N(l)}$ in (11) can be neglected for large N .

It can be seen from Fig. 2 [curve (b)] that function $B_1(\lambda)$ assumes negative values in the neighborhood of the origin. However, for large N , an average $\{N, -, 3\}$ code does not contain very low weight codewords. To show this, we shall obtain a tighter bound on $\overline{N(l)}$ compared with (10). For relatively small values of N (such as $N = 1536$), it is possible to compute the number of sequences that are orthogonal to the parity-check matrix H by using combinatorial techniques.

Again, we consider the top two complete blocks and the last incomplete block of H separately.

Theorem 1: The number $N_1^c(l)$ of sequences of even weight $l \leq 2N/3$ that satisfy all the parity checks in any complete block of $N/3$ parity checks is

$$N_1^c(l) = 3^{l/2} \binom{N/3}{l/2}. \quad (12)$$

Proof: Because of the structure of top block, every word of even weight l that satisfies the top block can be obtained

by taking an arbitrary binary $N/3$ -tuple v with weight $l/2$, replacing each zero component with the sequence 000 and each nonzero component with one of the sequences {011, 101, 110}. Each distinct v gives rise to $3^{l/2}$ words, and since there are $\binom{N/3}{l/2}$ distinct weight $l/2$, $N/3$ -tuples v , a total of $N_1^c(l) = 3^{l/2} \binom{N/3}{l/2}$ sequences satisfy the parity checks in the top block. The other blocks are obtained by applying a permutation π to the top block; hence, there is a one-to-one correspondence via π between words that satisfy the top block and words that satisfy any other complete block. ■

Theorem 2: Let s be the number of rows in the last, incomplete block of the parity-check matrix H , $s > 0$. Then, the number $N_1^i(l)$ of sequences of even weight $l \leq N - s$ that satisfy the incomplete block of s parity-checks is

$$N_1^i(l) = \sum_{i=\max[0, (l-\{N-3s\})/2]}^{\min[l/2, s]} 3^i \binom{s}{i} \binom{N-3s}{l-2i}. \quad (13)$$

Proof: Without loss of generality, any word that satisfies the last (incomplete) block has $3s$ components constrained by parity-check equations and $N - 3s$ unconstrained components. By arguments identical to those used in the proof of Theorem 1, there are $3^i \binom{s}{i}$ ways to choose the constrained components to have weight $2i$; these can be combined freely with the unconstrained components. A word of weight l is obtained if the unconstrained component has weight $l - 2i$, which can be achieved in $\binom{N-3s}{l-2i}$ ways.

If l is greater than $N - 3s$, then the first term in (13) accounts for a sequence that has all ones in the “free” part plus additional ones in the parity-checked part. Hence, the lower limit of the sum in (13) is $\max[0, (l - \{N - 3s\})/2]$. On the other hand, the weight of the parity-checked part cannot exceed $2s$ since if $i = s$, all parity-checks are filled. Hence, the upper limit of the sum in (13) is $\min[l/2, s]$. In total, there are

$$N_1^i(l) = \sum_{i=\max[0, (l-\{N-3s\})/2]}^{\min[l/2, s]} 3^i \binom{s}{i} \binom{N-3s}{l-2i}$$

words of weight $l \leq N - s$ that satisfy the last incomplete block. ■

The probability that a random sequence of weight $l \leq N/2^s$ and length N satisfies any of the blocks of H is

$$P_1 = N_1(l) / \binom{N}{l}$$

where $N_1(l)$ is given by either (12) or (13). Since random permutations used to obtain the second and third blocks of H are chosen independently, the number of codewords of even weight $l \leq N/2$ in an $\{N, -, 3\}$ code, averaged over the ensemble of $\{N, -, 3\}$ codes, is

$$\overline{N(l)} = \binom{N}{l}^{-2} [N_1^c(l)]^2 [N_1^i(l)] \quad (14)$$

where $N_1^c(l)$ and $N_1^i(l)$ are given by (12) and (13).

⁵In the bounds that follow, most significant contributions come from lower weight codewords, so we restrict our computations to codewords of weight $l \leq N/2$.

We computed (14) for $N = 1536$ using Mathematica [30]. In order to relate this approach to previous results, we introduced the function $B(\lambda)$ which is now defined as

$$B(\lambda) = -1/N \ln \overline{N(l)}$$

where $\overline{N(l)}$ is given by (14) (and so $\overline{N(l)} = \exp[-NB(\lambda)]$).

The graph of $B(\lambda)$ is shown in Fig. 2 [curve (a)]. As we observe from Fig. 2, the function $B(\lambda)$ is indeed positive in the neighborhood of the origin. The large discrepancy in the neighborhood of the origin (and almost identical values as one moves away from the origin) between the bound on $B_1(\lambda)$ and its tighter counterpart is due to the fact that approximations introduced by applying the Chernoff bound in (3) and (6) tend to be close to the exact values for sequences of large Hamming weight but diverge apart for sequences of low Hamming weight.

It is also interesting to compare the average number of code-words of weight l for the codes obtained by Construction 2 and a random code with the same parameters ($R = 1/8$, $N = 1536$). We computed the number of sequences for the former class of codes by using expressions (12)–(14), and used [10, eq. (2.1)] to compute the expected number of weight- l sequences in the latter code. The result is shown in Fig. 4.

As one can observe from the figure, the minimum distance for typical codes obtained by Construction 2 is about half of the minimum distance for a random linear code with the same parameters. This is the price one has to pay for the availability of low-complexity decoding algorithms for the low-density Gallager codes. (Compare this with the observation of Gallager in [10, Fig. 2.4]. The figure shows the minimum distance ratios for few typical $\{N, j, k\}$ codes and the random code.)

V. AVERAGE PROBABILITY OF MAXIMUM-LIKELIHOOD DECODING ERROR

In this section, we derive upper bounds on the average (over the ensemble of codes) probability of maximum-likelihood decoding error for short frame $\{N, -, 3\}$ Gallager codes.

One of the most used techniques for obtaining an upper bound on the error probability is by using the union bound [31], [32]. Gallager derived in [10] bounds on the error probability that may be tighter than the union bound, but require simultaneous optimization of several independent parameters. Generally, these bounds are not easily applicable in the analysis of $\{N, -, 3\}$ Gallager codes.

Let us consider a Gaussian noise channel with the noise variance σ^2 and ± 1 antipodal signaling. If the Hamming distance between two code sequences is l , then the squared Euclidean distance between these sequences is $4l$. For any linear block code, the block-error probability is bounded by

$$P_e \leq \frac{1}{2} \sum_{l=d_{\min}}^N N(l) \operatorname{erfc}(\sqrt{l/2\sigma^2})$$

where

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-y^2} dy$$

$N(l)$ is the number of code sequences of weight l , d_{\min} is the code minimum Hamming distance, and N is the block length.

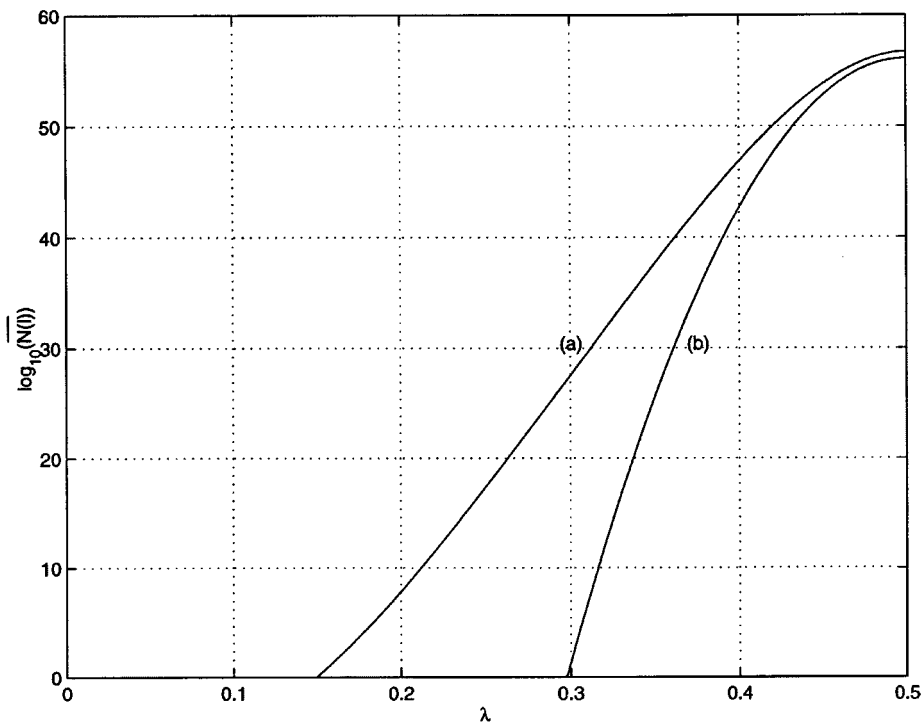


Fig. 4. Expected number of weight- l sequences in: (a) a code obtained by Construction 2 and (b) a random linear code. Both curves are for rate-1/8, block length $N = 1536$ codes. Horizontal axis: normalized sequence weight $\lambda = l/N$. Vertical axis: $\log_{10}(\overline{N(l)})$ (refer to (14) in the text). Note that both curves are shown as zeros if the computed number of sequences does not exceed 1.

Now averaging over all codes in the $\{N, -, 3\}$ ensemble, we obtain the following expression:

$$\overline{P_e} \leq \frac{1}{2} \sum_{l=0}^N \overline{N(l)} \operatorname{erfc} \left(\sqrt{l/2\sigma^2} \right) \quad (15)$$

where $\overline{N(l)}$ is the average number of codewords of weight l in the ensemble of $\{N, -, 3\}$ codes.

The graph of the bound on the average-error probability is shown in Fig. 5 (for $\overline{N(l)}$ we used the exact estimates obtained in Theorems 1 and 2 and $E_b/N_0 = 1/(2R\sigma^2)$).

The upper bound on the block-error probability for Gallager codes in Fig. 5 has two distinct types of behavior. Two different exponents apparently dominate the behavior of the upper bound for low and medium-to-high signal-to-noise ratios (SNRs). The two factors that determine these two types of behavior are the nearest neighbor multiplicity and the minimum Hamming distance. From the upper bound in Fig. 5, we may conclude that $\{N, -, 3\}$ Gallager codes have low average nearest neighbor multiplicity, and hence, we observe a sharp dropoff in the frame-error rate for lower SNR. As the SNR increases, the minimum Hamming distance becomes the dominant factor, and we observe that the bound becomes less steep since the typical minimum Hamming distance for $\{N, -, 3\}$ codes is not particularly good compared with the random code.

It is interesting to observe that in actual simulations for Gallager codes (Part II), the block-error rate exhibits a type of behavior similar to the theoretical findings, albeit the error rates are greater due to the suboptimal character of the iterative decoder. One could think of high performance iterative decoding as consisting of two essential parts: a good underlying code

and an iterative decoder that attempts to trace the good maximum-likelihood performance of the code. Hence, our analysis of $\{N, -, 3\}$ Gallager codes shows that the “underlying” codes have good maximum-likelihood performance, and in Part II, we will observe their good performance using iterative decoding.

VI. CONCLUSIONS

In this paper, we studied short frame Gallager codes that could be used as error-correcting codes for digital speech transmission in CDMA systems. A major feature that distinguishes the proposed scheme from similar applications of error-control coding in CDMA systems is the use of a suboptimal, yet highly effective iterative decoding algorithm. In this paper, we studied some of the theoretical properties of short frame Gallager codes. In Part II, we will investigate the actual performance of iterative decoders for this class of Gallager codes.

We discovered a class of low-rate Gallager codes, namely, $\{1536, -, 3\}$ codes, that, as we will see in Part II, exhibit strong performance in AWGN and fading channels for short frame-lengths. This class of low-rate Gallager codes maintains excellent performance even for short user data frames (192 bits), and hence, the delays associated with encoding and decoding of these codes are consistent with data delays in CDMA systems used for digital speech transmission.

We have attempted to correct the impression that one might obtain from [10] and [13] that only long frame-length Gallager codes may be of interest. In this paper, we attempted to show that short-frame Gallager codes may indeed be a focus of practical interest when one considers the entire range of factors involved in the realization of an error-correcting scheme, such

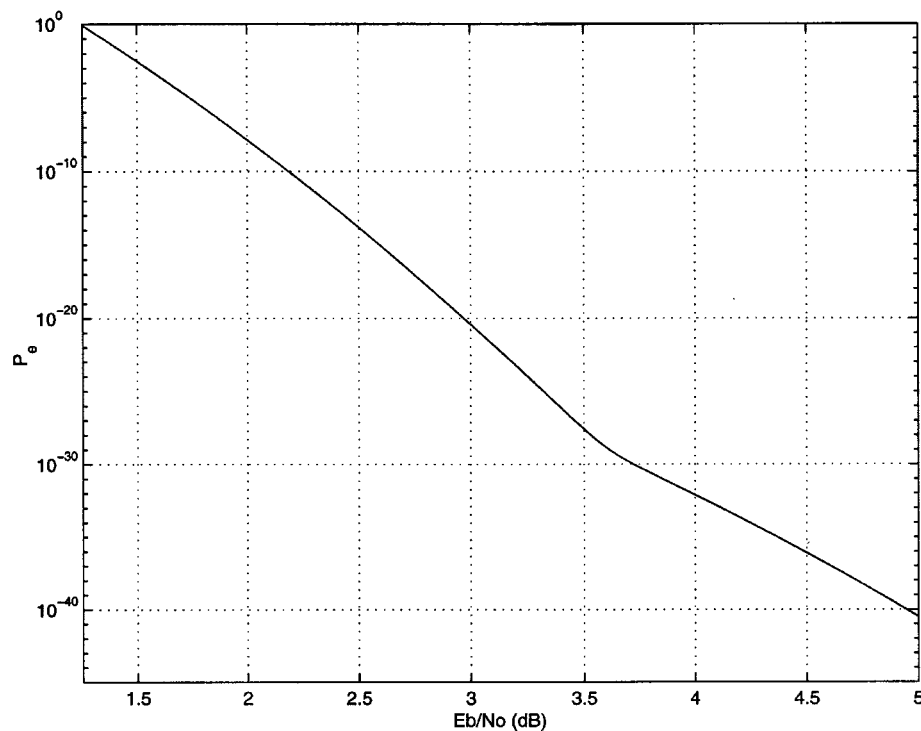


Fig. 5. Upper bound on the maximum-likelihood block error rate versus SNR for $\{1536, -, 3\}$ Gallager codes.

as encoding/decoding delays, implementation complexity, and error-correcting capabilities.

We investigated the distance properties of the ensemble of $\{N, -, 3\}$ Gallager codes and computed average upper bounds on the number of codewords with a certain Hamming weight in this ensemble. We applied these bounds in derivations of average upper bounds on the frame error rates for a maximum-likelihood decoder and showed that the resulting error probability bounds are small enough so that one could expect good performance for these codes even with suboptimal decoding schemes. This is shown in Part II where simulation results for iterative decoding of $\{N, -, 3\}$ Gallager codes are presented.

REFERENCES

- [1] G. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. IEEE Int. Conf. Communications (ICC'93)*, Geneva, Switzerland, May 1993, pp. 2.1064–2.1070.
- [2] S. Benedetto and G. Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 409–428, Mar. 1996.
- [3] G. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Trans. Commun.*, vol. 44, pp. 1261–1271, Oct. 1996.
- [4] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of provably good low-density parity check codes," *IEEE Trans. Inform. Theory*, to be published.
- [5] L. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proc. IEEE*, vol. 77, pp. 257–286, 1989.
- [6] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 284–287, 1974.
- [7] L. E. Baum, T. Petrie, G. Soules, and N. Weiss, "A maximization technique occurring in the statistical analysis of probabilistic functions in Markov chains," *Ann. Math. Statist.*, vol. 41, no. 1, pp. 164–171, 1970.
- [8] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, submitted for publication.
- [9] "CAS 5093 turbo-code codec," Comatlas, Chateaubourg, France, Tech. Rep. 3.7, Aug. 1994.
- [10] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
- [11] V. V. Zyablov and M. S. Pinsker, "Estimation of the error-correction complexity for Gallager low-density codes," *Problems of Information Transmission*, vol. 11, pp. 18–28, 1975. (translated from *Problemy Peredachi Informatsii*, vol. 11, no. 1, pp. 23–26).
- [12] D. J. C. MacKay and R. M. Neal, "Good codes based on very sparse matrices," in *Cryptography and Coding, 5th IMA Conference, in Lecture Notes in Computer Science*, C. Boyd, Ed., 1995, vol. 1025, pp. 110–111.
- [13] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, Mar. 1999.
- [14] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.
- [15] N. Wiberg, H.-A. Loeliger, and R. Kötter, "Codes and iterative decoding on general graphs," *Eur. Trans. Telecommun.*, vol. 6, pp. 513–525, Sept./Oct. 1995.
- [16] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. San Mateo, CA: Morgan Kaufmann, 1988.
- [17] R. J. McEliece, D. J. C. MacKay, and J.-F. Cheng, "Turbo decoding as an instance of Pearl's 'Belief Propagation' algorithm," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 140–152, Feb. 1998.
- [18] F. R. Kschischang and B. J. Frey, "Iterative decoding of compound codes by probability propagation in graphical models," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 219–230, Feb. 1998.
- [19] S. M. Aji and R. J. McEliece, "The generalized distributive law," *IEEE Trans. Inform. Theory*, vol. 46, pp. 325–343, Mar. 2000.
- [20] C. Heegard and S. B. Wicker, *Turbo Coding*. Norwell, MA: Kluwer Academic, 1998.
- [21] B. J. Frey, *Graphical Models for Machine Learning and Digital Communication*. Cambridge, MA: MIT Press, 1998.
- [22] A. J. Viterbi, "Very low rate convolutional codes for maximum theoretical performance of spread-spectrum multiple-access channels," *IEEE J. Select. Areas Commun.*, vol. 8, pp. 641–649, May 1990.
- [23] J. Chaib and H. Leib, "Benefits of error control coding for CDMA," in *Proc. 17th Biennial Symp. Communications*, Kingston, ON, Canada, 1994, pp. 88–91.
- [24] D. Divsalar and F. Pollara, "Turbo codes for PCS applications," *Proc. ICC*, pp. 54–59, 1995.
- [25] R. F. Ormondroyd and J. J. Maxey, "Performance of low-rate orthogonal convolutional codes in DS-SS applications," *IEEE Trans. Veh. Technol.*, vol. 46, pp. 320–328, May 1997.

- [26] P. Elias, "Coding for two noisy channels," in *Proc. Third London Symp. Information Theory*, C. Cherry, Ed., Sept. 1955.
- [27] B. Reiffen, "Sequential decoding for discrete input memoryless channels," *Proc. IRE.*, vol. IT-8, pp. 208–220, Apr. 1962.
- [28] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, to be published.
- [29] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
- [30] S. Wolfram, *Mathematica: A System for Doing Mathematics by Computer*, 2nd ed. Reading, MA: Addison-Wesley, 1991.
- [31] R. E. Blahut, *Digital Transmission of Information*. Reading, MA: Addison-Wesley, 1990.
- [32] S. Lin and D. J. Costello Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.



Vladislav Sorokine (M'98) received the degree of Engineer-Physicist with honors from Moscow Engineering Physics Institute (MIFI) in 1985, and the M.A.Sc. and Ph.D. degrees in electrical engineering from the University of Toronto, Toronto, ON, Canada, in 1993 and 1998, respectively.

He is a Systems Engineer with Qualcomm, Inc., San Diego, CA. His research interests include the area of coding theory and wireless communications. He is currently involved in the design and performance analysis of third generation wireless systems.



Frank R. Kschischang (M'91) received the B.A.Sc. degree with honors from the University of British Columbia, Vancouver, BC, Canada, in 1985, and the M.A.Sc. and Ph.D. degrees from the University of Toronto, Toronto, ON, Canada, in 1988 and 1991, respectively, all in electrical engineering. During his graduate studies, he held a variety of scholarships and fellowships, including the IEEE Communications Society Scholarship. He is a 1999 recipient of the Province of Ontario's Premier Research Excellence Award.

He is an Associate Professor of Electrical and Computer Engineering at the University of Toronto, Toronto, ON, Canada. His research interests include the area of coding theory, particularly in soft-decision decoding algorithms and codes defined on graphs.

Dr. Kschischang is currently an Associate Editor for Coding Theory of the *IEEE TRANSACTIONS ON INFORMATION THEORY*. He served as Publicity Chair of the 1998 IEEE International Symposium on Information Theory held in Cambridge, MA.



Subbarayan Pasupathy (M'73–SM'81–F'91) was born in Chennai (Madras), India, on September 21, 1940. He received the B.E. degree in telecommunications from the University of Madras in 1963, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Madras, India, in 1966, and the M.Phil. and Ph.D. degrees in engineering and applied science from Yale University, New Haven, CT, in 1970 and 1972, respectively.

He joined the faculty of the University of Toronto in 1973 and became a Professor of Electrical Engineering in 1983. He has served as the Chairman of the Communications Group and as the Associate Chairman of the Department of Electrical Engineering at the University of Toronto. His research interests are in the areas of communication theory, digital communications, and statistical signal processing.

Dr. Pasupathy is a Registered Professional Engineer in the Province of Ontario. He has served as a Technical Associate Editor for the *IEEE Communications Magazine* (1979–1982) and as an Associate Editor for the *Canadian Electrical Engineering Journal* (1980–1983). During 1982–1989, he was an Area Editor for Data Communications and Modulation for the *IEEE TRANSACTIONS ON COMMUNICATIONS*. Since 1984, he has been writing a regular column entitled "Light Traffic" for the *IEEE Communications Magazine*. He was elected Fellow of the IEEE in 1991 "for contributions to bandwidth-efficient coding and modulation schemes in digital communication."