Modulation and Coding for the Gaussian Collision Channel

Giuseppe Caire, *Member, IEEE*, Emilio Leonardi, *Member, IEEE*, and Emanuele Viterbo, *Member, IEEE*

***Abstract*—We study signal-space coding for coherent slow frequency-hopped communications over a Gaussian multiple-access collision channel (G-MACC). We define signal sets and interleavers having maximum *collision resistance*. The packet-error probability and the spectral efficiency obtained by these signal sets concatenated with outer block coding and hard (error-only) decoding is evaluated without assuming perfect interleaving. Closed-form expressions are provided and computer simulations show perfect agreement with analysis. The structure of good interleavers is also discussed.**

More generally, we present expressions for the information outage probability and for the achievable (ergodic) rate of the G-MACC at hand, under various assumptions on user coding and decoding strategies. Outage probability yields the limiting packet-error probability with finite interleaving depth (delay-limited systems). The achievable rate yields the limiting system spectral efficiency for large interleaving depth (delay-unconstrained systems). Comparisons with other classical multiple-access schemes are provided.

***Index Terms*—Coding and modulation, frequency-hopped communications, information outage probability, multiple-access collision channel.**

I. Introduction

In the Gaussian multiple-access channel (G-MAC), several senders (users) encode their information messages independently into sequences of real numbers and transmit their signals at the same time. A common receiver gets the superposition of all users signals plus additive Gaussian background noise and detects the individual messages [1]. This channel model serves as perhaps the simplest example of wireless network, where a common resource has to be shared by a population of users (examples are the uplink of a satellite system or the mobile-to-base link of a terrestrial cellular system, in the idealized case of isolated cells and no fading [2]).

The capacity region of the G-MAC is well known [1] and the modern research trend in the field is to devise low-complexity coding and decoding schemes to approach this limit. For example, [3] shows that all capacity region boundary points can be achieved by single-user coding/decoding and "stripping," provided that the users split their signals into at most two components whose rate sum is equal to the users' own rate (the rate-splitting approach). A more classical (and generally suboptimal) approach consists of eliminating multiple-access interference (MAI) by making the user signals orthogonal, like in TDMA/FDMA. The capacity region of the G-MAC with orthogonal access is strictly included in the general capacity region, and it is optimal in the case of equal-rate equal-energy users (symmetric capacity) [1].

In practice, both optimal and orthogonal multiple access require a good deal of coordination among users, in order to accommodate changing traffic conditions, access requests from new users entering the network, and re-allocation of resources (bandwidth and power) of users leaving the network. Users coordination can be achieved at the expenses of additional overhead and complexity, by implementing some protocol on top of the basic G-MAC mechanism.

A simple alternative to user coordination is random access, where no effort is made in order to avoid MAI and other countermeasures are taken to mitigate its effects. A G-MAC with random access shall be referred to as the *Gaussian multiple-access collision channel* (G-MACC). For example, in some packet radio networks users may "collide" (i.e., their signals may overlap in time–frequency) and are informed about an unsuccessful transmission by a feedback channel, so that a retransmission protocol can be implemented (e.g., the ALOHA protocol [4]–[6]). In other applications, retransmissions are undesirable or impossible. Then, the effect of collisions can be mitigated by a combination of coding, interleaving, and signal processing (see [8]–[15] and reference therein).

The capacity region of a noiseless collision channel without feedback was determined in [16]. In the channel model of [16], users cannot coordinate their transmissions because of unknown transmission delays, that cannot be estimated because of the lack of a feedback channel. Therefore, in [16] collisions are unavoidable. In this work, we do not place this restriction. On the contrary, we just assume that a "lazy" system designer did not implement any user coordination protocol or retransmission protocol. Moreover, we constrain the network to be equipped with conventional single-user matched filters (SUMF), which treat MAI as additional (white) noise without implementing stripping decoding or other signal–space interference cancellation techniques. Obviously, we do not claim any optimality of this approach. Nevertheless, devising modulation and coding schemes for this channel might be of some interest. Applications are, for example, simple indoor wireless networks with limited-mobility terminals, mobile satellite systems serving a large population of users with "bursty" traffic, or low-rate random-access channels for auxiliary operations in cellular systems, such as handoffs and call requests. Moreover, several partially ordered protocols

Manuscript received July 1, 1998; revised October 1, 1999. the material in this paper was presented in part at the IEEE International Symposium on Information Theory, MIT, Cambridge, MA, August 16–21, 1998.

G. Caire is with the Institute Eurocom, 06904 Sophia-Antipolis, France (e-mail: caire@eurocom.fr).

E. Leonardi and E. Viterbo are with the Dipartimento Elettronica, Politecnico di Torino, 10129 Torino, Italy (e-mail: leonardi@polito.it; viterbo@polito.it).

Communicated by M. L. Honig, Associate Editor for Communications.

Publisher Item Identifier S 0018-9448(00)06998-4.

(e.g., PRMA [17], [18]) have been proposed for integrated voice and data in wireless systems, so that the study of the underlying G-MACC may provide useful insight into more evolved applications [19].

In this paper, we consider a slotted G-MACC with coherent detection and equal-rate equal-energy users. The time–frequency plane is organized in *frames*, and each frame is divided in time–frequency *slots*. Users interleave and transmit their codewords over M (pseudo-)randomly selected slots. Previous analysis of time–frequency hopped systems considered perfect interleaving and infinite signal-to-noise ratio (SNR) [13], [14]. On the contrary, we distinguish delay-limited systems, for which M is finite, from delay-unconstrained systems, where perfect interleaving is allowed (i.e., M can be made arbitrarily large). Moreover, we take into account the effect of noise.

For this channel, we define a class of multidimensional signal sets having *collision resistance*, i.e., such that even if some signal components are transmitted during collided slots, correct signal detection is still possible from the uncollided components. A necessary condition for collision resistance is that the components of the signal point are transmitted on different slots. Then, we define a class of interleavers meeting this constraint and we select *good* interleavers in this class. Under some assumptions, the slotted G-MACC belongs to the class of block-interference channels studied in [20], in the case of no delay constraints. In fact, collisions can be regarded as an extreme case of *block fading*, studied in [21], [22]. Thus it is not surprising that high-diversity signal sets for the fading channel [23], [24] have good collision resistance. We provide a new algebraic construction of high-diversity signal sets based on $\mathbb{Z}$-modules, and an interesting four-dimensional example.

The idea of improving the performance of slotted ALOHA by introducing "packet redundancy" is not new (e.g., multicopy ALOHA and its generalizations [25], [26]). Replicating the same packet, as done in previous work, can be seen as the concatenation of an outer code with a trivial repetition inner code and a trivial interleaver. Here, we consider the concatenation of collision-resistant signal sets (which can be regarded as inner signal-space coding) with outer block coding (e.g., Reed–Solomon codes) and nontrivial interleaving (Sections II and III). The performance analysis of this scheme is inspired by the work of [14], with the fundamental difference that in our case, because of the finite interleaving depth, symbol errors at the decoder input are statistically dependent, so that the standard analysis of bounded-distance hard decoding [27] does not apply. Nevertheless, we find simple closed-form expressions for the word error probability and for the spectral efficiency achievable by Reed–Solomon outer coding. Our analysis of the error probability provides some useful hints on the design of good interleavers (Section IV).

Finally, we look at the G-MACC from a more idealized point of view and we derive closed-form expressions for its information outage probability [21] (for finite interleaving depth) and for its achievable symmetric rate (for ideal interleaving). We provide comparisons with other conventional access schemes for the G-MACC, such as slotted ALOHA, "Naive" code-division multiple access (CDMA) (NCDMA) with SUMF, and linear minimum mean-square error (MMSE) receivers[1] and ideal orthogonal access (Section V).

Proofs and mathematical details are collected in Appendices A–D and conclusions and future research directions are pointed out in Section VI.

Notations and Definitions:

- Φ_k^n denotes the *combinations set*, i.e., the set of subsets $\phi \subseteq \{1,\dots,n\}$ of cardinality k (referred to as "n-combinations of size k"). If $n \geq k$, $|\Phi_k^n| = \binom{n}{k}$, otherwise Φ_k^n is empty.
- Π_k denotes the set of permutations π of k elements.
- Ξ_k^n denotes the *ordered combinations set*, i.e., the set of vectors $\boldsymbol{\xi}$ of length k whose components are distinct elements of $\{1,\dots,n\}$. If $n \geq k$, $|\Xi_k^n| = k!\binom{n}{k}$, otherwise Ξ_k^n is empty. Moreover, there exists a (not unique) one-to-one correspondence $\Xi_k^n \leftrightarrow \Phi_k^n \times \Pi_k$.
- $B(n,k,p) \triangleq \binom{n}{k} p^k (1-p)^{n-k}$.
- "p" and "a.e." denote convergence in probability and almost everywhere, respectively [29].
- $\binom{0}{h} = 0^h = \delta_{h,0}$.
- $1\{A\}$ denotes the indicator function of the event A.
- $\mathcal{N}(\mu,\sigma^2)$ denotes the Gaussian probability density function (pdf) with mean μ and variance σ^2.
- $Q(x) \triangleq \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\,dt'$.
- $\mathcal{H}(p) \triangleq -p\log_2 p - (1-p)\log_2(1-p)$ and for a probability vector $\boldsymbol{p}$, $\mathcal{H}(\boldsymbol{p}) \triangleq -\sum_i p_i \log_2 p_i$.

II. Slotted Gaussian Multiple-Access Collision Channel

We consider a G-MACC with N_u users and slotted random access. The time–frequency plane is organized in *frames*. Each frame is partitioned in N_s time–frequency *slots*. User signals are divided into *bursts* which occupy one slot. Guard bands and guard intervals are inserted in order to make signal bursts approximately time- and band-limited over the slots. Each slot has L_s *real dimensions* (or *components*) available for transmission. Users occupy an average number g of slots per frame and transmit with *information rate*[2] R bits per dimension, so that all users have the same average bit rate $R_b = gRL_s/T$ bits per second, where T denotes the frame duration. Users select their slots randomly and independently, according to a given

[1]Following the terminology of [2], we denote by Naive CDMA an access scheme where all signals overlap in time and frequency and where users are decoded independently. The receiver for NCDMA is formed by a soft-output detector device (e.g., a bank of single-user matched filters, a bank of linear MMSE interference cancelers [10], or a bank of decorrelators [9]) which produces sequences of soft-decision variables for each user encoded data stream, followed by a bank of single-user decoders acting independently. No information from a decoder can be fed back to other decoders, as done in a stripping procedure [3], [28].

[2]In a real system, R should also take into account the overhead due to guard bands, guard intervals, training sequences for synchronization, and channel estimation and suitable higher level protocol overhead, like user address identifiers, packet numbering, acknowledgment, etc. For simplicity, in the following we shall assume an ideally synchronized system with Nyquist band-limited signals and perfect coherent reception.

(pseudo-)random time–frequency hopping code known to the receiver. Following [14], the transmission of each user is modeled as a Bernoulli process [29] with probability $p = g/N_s$ that a user occupies any given slot. The slot collision probability (i.e., the probability that more than one user transmits over the same slot) is given by $1 - (1-p)^{N_u - 1}$ [14]. We study the system performance under the assumption of infinite user population $(N_u \to \infty)$ for a fixed ratio $N_u/N_s = \beta$. Then, the number of transmitting users in each slot is Poisson-distributed [29] with mean $G = g\beta$ (G is referred to as the *channel load*), collisions in different slots are independent and identically distributed (i.i.d.), and the limiting collision probability is given by

$$P_{\text{col}} \triangleq 1 - \lim_{N_u \to \infty} \left(1 - \frac{g\beta}{N_u}\right)^{N_u - 1} = 1 - e^{-G}. \quad (1)$$

Let W denote the system bandwidth. The *system spectral efficiency* is defined as $\eta \triangleq \frac{N_u R_b}{W}$ bits per second per hertz. In this work, we are interested in the limiting η for $N_u \to \infty$ and constant $N_u/N_s = \beta$. According to the "$2WT$-Theorem," we can approximate $L_s \approx 2WT/N_s$ and write

$$\eta = 2RG. \quad (2)$$

A. Channel Models

Because of the complete symmetry of the problem with respect to any user, we can focus on the transmission of a given reference user (say, user 1). As discussed in Section I, in the G-MACC under analysis the receiver treats MAI as additional noise and does not take any advantage of its structure.

An optimistic assumption is that the demodulator for user 1 behaves as a linear device irrespectively of the MAI power and, for each received burst, provides a sequence of L_s samples taken at the symbol rate

$$y_j = x_j + \nu_j + n_j, \qquad j = 1, \ldots, L_s \quad (3)$$

where x_j is the jth component of the signal of user 1, ν_j is the jth MAI sample, and n_j is the jth additive white Gaussian noise (AWGN) sample, i.i.d. $\sim \mathcal{N}(0, N_0/2)$. The variance of ν_j depends on the number K of interfering users transmitting over the current slot, which is Poisson-distributed with mean G. The channel model defined by (3) will be referred to as the *variable-power additive noise* (VPAN) channel.

On the contrary, a pessimistic assumption (very common in the analysis of packet-radio networks [5]) is that the demodulator for user 1 is totally impaired by collisions. In this case, the demodulated sample sequence during the current slot can be written as

$$y_j = \alpha(x_j + n_j) \qquad j = 1, \ldots, L_s \quad (4)$$

where $\alpha \in \{0, 1\}$ is the *collision* random variable, defined by

$$\alpha = \begin{cases} 0, & \text{if } K > 0 \\ 1, & \text{if } K = 0. \end{cases} \quad (5)$$

The channel model defined by (4) will be referred to as the *on–off* channel.

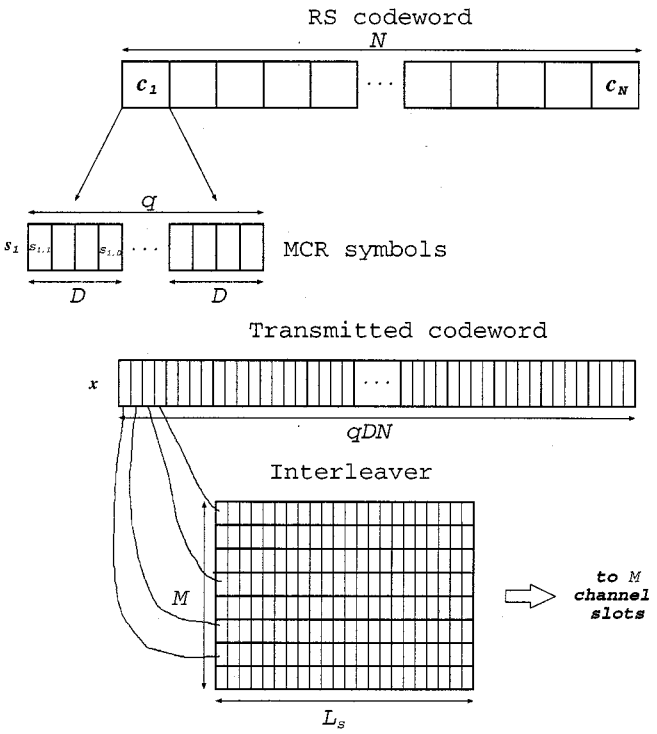

Fig. 1. Encoding and interleaving.

Coherent demodulation is assumed in the channel models (3) and (4). The real channel models derive from treating separately the in-phase and quadrature components of the signal complex envelope. In model (3), the MAI circular symmetry (i.i.d. in-phase and quadrature components) derives from assuming independent and uniformly distributed carrier phases for all interfering users.

B. Encoding and Interleaving

User information is organized in *packets*. Each packet is independently block-encoded, interleaved, transmitted over a given sequence of slots, demodulated, deinterleaved, and decoded. Then, packet-error probability and word-error probability (WER) coincide. Encoding and interleaving is sketched in Fig. 1 and described in the following.

Encoding: Without loss of generality, we consider signal-space codes $\mathcal{X}$ obtained by the concatenation of a block code over an abstract symbol alphabet with a signal set through a labeling map [30]. Let $\mathcal{C}$ be a block code of length N defined over a discrete and finite alphabet $\mathcal{A}$ and let $\mathcal{S}$ be a D-dimensional signal set (i.e., a discrete and finite set of vectors (signal points) in $\mathbb{R}^D$). Assume that $|\mathcal{A}| = |\mathcal{S}|^q$ and let $\boldsymbol{\mu} = \{\mu_i\}_{i=1}^N$ be a sequence of labeling maps $\mathcal{A} \to \mathcal{S}^q$ of $\mathcal{A}$ onto the q-fold Cartesian product of $\mathcal{S}$ by itself. Then, the code $\mathcal{X}$ is given by

$$\mathcal{X} = \{\boldsymbol{x} \in \mathbb{R}^{qDN} : \boldsymbol{x} = \boldsymbol{\mu}(\boldsymbol{c}), \forall \boldsymbol{c} = (c_1, \ldots, c_N) \in \mathcal{C}\} \quad (6)$$

where $\boldsymbol{\mu}(\boldsymbol{c}) = (\mu_1(c_1), \ldots, \mu_N(c_N))$ and where the image of c_i under μ_i is the qD-dimensional real vector

$$\mu_i(c_i) = (\boldsymbol{s}_{q(i-1)+1}, \ldots, \boldsymbol{s}_{q(i-1)+q})$$

(the $\boldsymbol{s}_{q(i-1)+j}$'s are D-dimensional vectors, or signal points, in $\mathcal{S}$). Codes $\mathcal{X}$ obtained in this way will be denoted briefly by $\mathcal{X} = \mathcal{C} \rightarrow \boldsymbol{\mu} \rightarrow \mathcal{S}$.

Interleaving: In general, system requirements impose a maximum transmission *delay*. Then, the interleaving depth, i.e., the number of slots over which a coded packet (codeword) is transmitted, cannot be arbitrarily large [21]. We assume that each user codeword is interleaved and transmitted over M distinct slots, we consider a particular codeword of the reference user and we number the M slots over which this is transmitted by $m = 1, \ldots, M$. Clearly, because of the block-interference model, the word error probability is independent of the actual position of signal components in the slots. Also, slots may contain signal components belonging to several codewords, so that the slot length L_s, the interleaving depth M, and the codesword length qDN can be chosen quite freely.[3] For the following analysis, all that matters is the unordered assignment of the qDN signal components of the transmitted codesword to the corresponding M slots. Thus for codes $\mathcal{X} \rightarrow \boldsymbol{\mu} \rightarrow \mathcal{S}$, we represent interleavers by an associated array $\boldsymbol{M}$ of size $qN \times D$ with elements in $\{1, \ldots, M\}$ such that the ℓth component of the kth signal in the codesword, denoted by $s_{k,\ell}$, is sent over the slot indexed by the (k, ℓ)th element of $\boldsymbol{M}$. The kth row of $\boldsymbol{M}$ specifies the sequence of slots over which signal $\boldsymbol{s}_k$ is transmitted.

Table I gives an array $\boldsymbol{M}$ for $M = 6$, $D = 3$, $q = 1$, and $N = 20$, and an interleaver associated with $\boldsymbol{M}$. For example, the components of signal $\boldsymbol{s}_{13}$ are transmitted over slots 2, 3, and 6, as specified by the 13th row of $\boldsymbol{M}$. By permuting arbitrarily the order of the signal components in each slot, we obtain equivalent interleavers all corresponding to the array $\boldsymbol{M}$ (we can say that an array $\boldsymbol{M}$ is representative of a class of equivalent interleavers).

TABLE I
EXAMPLE OF INTERLEAVER STRUCTURE WITH $M = 6$, $D = 3$, $q = 1$, AND $N = 20$

$\mathbf{s}_1$	1	2	3
$\mathbf{s}_2$	1	2	4
$\mathbf{s}_3$	1	2	5
$\mathbf{s}_4$	1	2	6
$\mathbf{s}_5$	1	3	4
$\mathbf{s}_6$	1	3	5
$\mathbf{s}_7$	1	3	6
$\mathbf{s}_8$	1	4	5
$\mathbf{s}_9$	1	4	6
$\mathbf{s}_{10}$	1	5	6
$\mathbf{s}_{11}$	2	3	4
$\mathbf{s}_{12}$	2	3	5
$\mathbf{s}_{13}$	2	3	6
$\mathbf{s}_{14}$	2	4	5
$\mathbf{s}_{15}$	2	4	6
$\mathbf{s}_{16}$	2	5	6
$\mathbf{s}_{17}$	3	4	5
$\mathbf{s}_{18}$	3	4	6
$\mathbf{s}_{19}$	3	5	6
$\mathbf{s}_{20}$	4	5	6

M

M										
1	$s_{1,1}$	$s_{2,1}$	$s_{3,1}$	$s_{4,1}$	$s_{5,1}$	$s_{6,1}$	$s_{7,1}$	$s_{8,1}$	$s_{9,1}$	$s_{10,1}$
2	$s_{1,2}$	$s_{2,2}$	$s_{3,2}$	$s_{4,2}$	$s_{11,1}$	$s_{12,1}$	$s_{13,1}$	$s_{14,1}$	$s_{15,1}$	$s_{16,1}$
3	$s_{1,3}$	$s_{5,2}$	$s_{6,2}$	$s_{7,2}$	$s_{11,2}$	$s_{12,2}$	$s_{13,2}$	$s_{17,1}$	$s_{18,1}$	$s_{19,1}$
4	$s_{2,3}$	$s_{5,3}$	$s_{8,2}$	$s_{9,2}$	$s_{11,3}$	$s_{14,2}$	$s_{15,2}$	$s_{17,2}$	$s_{18,2}$	$s_{20,1}$
5	$s_{3,3}$	$s_{6,3}$	$s_{8,3}$	$s_{10,2}$	$s_{12,3}$	$s_{14,3}$	$s_{16,2}$	$s_{17,3}$	$s_{19,2}$	$s_{20,2}$
6	$s_{4,3}$	$s_{7,3}$	$s_{9,3}$	$s_{10,3}$	$s_{13,3}$	$s_{15,3}$	$s_{16,3}$	$s_{18,3}$	$s_{19,3}$	$s_{20,3}$

III. COLLISION-RESISTANT SIGNAL SETS

In this section we analyze the system from the point of view of a single reference user. We focus on the transmission of D-dimensional signals $\boldsymbol{s} \in \mathcal{S}$ over the on–off channel. We consider the channel output $\boldsymbol{y}_k$ corresponding to the transmission of a single signal $\boldsymbol{s}_k$ without specifically indexing the user and, for simplicity of notation, we drop the time index k. Moreover, we assume that the components $(s_1, \ldots, s_D)$ of $\boldsymbol{s}$ are transmitted over D different slots, indexed by $j = 1, \ldots, D$, and we denote by $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_D)$ the collision pattern over these slots. Then, we can rewrite (4) as

$$y_j = \alpha_j(s_j + n_j), \qquad j = 1, \ldots, D \tag{7}$$

We assume that the receiver has perfect knowledge of $\boldsymbol{\alpha}$ (perfect channel state information (CSI)). Then, the maximum-likelihood (ML) decision rule for the detection of $\boldsymbol{s}$ is

$$\hat{\boldsymbol{s}} = \arg \min_{\boldsymbol{s} \in \mathcal{S}} \sum_{j=1}^{D} |y_j - \alpha_j s_j|^2. \tag{8}$$

This corresponds to selecting the minimum distance of the received point from the points of a signal set $\mathcal{S}(\boldsymbol{\alpha})$ obtained by projecting $\mathcal{S}$ over a $(D-k)$-dimensional subspace generated by the $D-k$ axes corresponding to the nonzero α_j's. In order to avoid systematic errors (i.e., detection errors even for arbitrarily large SNR) in the presence of $k < D$ collisions, we require that the points in $\mathcal{S}(\boldsymbol{\alpha})$ are distinct, for all $\boldsymbol{\alpha}$ with Hamming weight

$$W(\boldsymbol{\alpha}) \triangleq \sum_{j=1}^{D} \alpha_j > 0.$$

Then, we have the following definition.

Definition: A D-dimensional signal set $\mathcal{S}$ has *collision resistance* k if its projections on all $(D-k)$-dimensional coordinate subspaces have $|\mathcal{S}|$ points, i.e., $|\mathcal{S}(\boldsymbol{\alpha})| = |\mathcal{S}|$ for all $\boldsymbol{\alpha}$ of weight $W(\boldsymbol{\alpha}) \geq D - k$. □

In this paper, we are interested in maximum collision resistant (MCR) D-dimensional signal sets, i.e., with collision resistance equal to $D-1$. The minimum Hamming distance of such signal sets must be D. A similar requirement is imposed in the design of *high-diversity* signal sets for the fading channel where the

[3]For example, in the GSM full-rate standard, encoded packets corresponding to speech frames of 20 ms are interleaved over $M = 8$ TDMA slots, and each slot contains symbols from four different packets [31].

minimum Hamming distance between any two signal vectors is called *modulation diversity* [23], [24].

A desirable property of interleavers is that the components of each signal $\boldsymbol{s}$ in the codesword are transmitted over D distinct slots. We have the following definition.

Definition: Consider the $qN \times D$ array $\boldsymbol{M}$ associated with an interleaver. The interleaver is MCR if all rows of $\boldsymbol{M}$ are (not necessarily distinct) vectors from the ordered combinations set Ξ_D^M. □

In the following, we restrict our treatment to MCR interleavers. The array $\boldsymbol{M}$ of an MCR interleaver can be generated randomly, by selecting i.i.d. with uniform probability qN vectors $\boldsymbol{\xi} \in \Xi_D^M$ and by writing them by rows. We refer to randomly generated MCR interleavers as RMCR interleavers. We shall make use of the following fact, which is an immediate consequence of the *Strong Law of Large Numbers* [29]

Fact 1: For given D and $M \geq D$, consider a sequence of RMCR interleavers for increasing block length N, with associated array $\boldsymbol{M}_N$. For any given $\boldsymbol{\xi} \in \Xi_D^M$, let $f_N(\boldsymbol{\xi})$ be the fraction of rows of $\boldsymbol{M}_N$ equal to $\boldsymbol{\xi}$. Then, $f_N(\boldsymbol{\xi}) \stackrel{\text{a.e.}}{\to} 1/(D!\binom{M}{D})$ as $N \to \infty$. □

A. Error Probability of MCR Signal Sets

The error probability analysis is complicated by the fact that, in general, $\mathcal{S}$ and its projections $\mathcal{S}(\boldsymbol{\alpha})$ are not *geometrically uniform* [32]. We can *symmetrize* the problem with respect to all collision patterns of the same weight by averaging over all possible component permutations $\pi \in \Pi_D$. A component permutation π, if applied to a vector $\boldsymbol{s} = (s_1, \ldots, s_D)$, yields the permuted vector $\pi\boldsymbol{s} = (s_{\pi(1)}, \ldots, s_{\pi(D)})$. The *union bound* [7] on the symbol error probability $\overline{P}(e|k)$ conditioned on the number k of collided components and averaged over all $\boldsymbol{s} \in \mathcal{S}$ and $\pi \in \Pi_D$ is given by

$$\overline{P}(e|k) \leq \min\left\{ \frac{1}{|\mathcal{S}|D!} \sum_{\boldsymbol{s}\in\mathcal{S}} \sum_{\pi\in\Pi_D} \sum_{\hat{\boldsymbol{s}}\neq\boldsymbol{s}} P(\pi\boldsymbol{s} \to \pi\hat{\boldsymbol{s}}|k),\ 1 - \frac{1}{|\mathcal{S}|} \right\} \tag{9}$$

where the second term of the above minimum corresponds to the error probability with random selection of a signal in $\mathcal{S}$, and where we define the conditional *pairwise error probability* [7]

$$P(\pi\boldsymbol{s} \to \pi\hat{\boldsymbol{s}}|k) \triangleq Q\left(\sqrt{\frac{\mathcal{E}\sum_{j=1}^{D-k} |s_{\pi(j)} - \hat{s}_{\pi(j)}|^2}{2N_0}} \right). \tag{10}$$

In (10), we assume that $\mathcal{S}$ has unit average energy per dimension and that each signal component is scaled by $\sqrt{\mathcal{E}}$ before transmission, so that the SNR is $\mathcal{E}/N_0$.

Notice that $\overline{P}(e|k)$ depends on $\boldsymbol{\alpha}$ only through its weight $W(\boldsymbol{\alpha}) = D - k$. Since k is binomially distributed, the average symbol error probability is given by

$$P(e) = \sum_{k=0}^{D} B(D, k, P_{\text{col}}) \overline{P}(e|k). \tag{11}$$

By using (9) in (11) we obtain an upper bound on $P(e)$.

B. Construction of MCR Signal Sets

Good MCR signal sets have large squared Euclidean distance (SED) between points $\boldsymbol{s}$ and $\hat{\boldsymbol{s}}$ projected on the $W(\boldsymbol{\alpha})$-dimensional coordinate subspace determined by $\boldsymbol{\alpha}$, for all $\boldsymbol{\alpha}$. In particular, we define the (normalized) minimum SED given k collided components as

$$d_k^2 \triangleq \min_{\pi\in\Pi_D} \min_{\boldsymbol{s}\neq\hat{\boldsymbol{s}}} \sum_{j=1}^{D-k} |s_{\pi(j)} - \hat{\boldsymbol{s}}_{\pi(j)}|^2. \tag{12}$$

For each k, the exponential behavior as $\mathcal{E}/N_0 \to \infty$ of $\overline{P}(e|k)$ is determined by d_k^2, in the sense that

$$\overline{P}(e|k) = O(e^{-d_k^2 \mathcal{E}/(4N_0)}).$$

Hence, a practical design criterion for good MCR signal sets is to maximize d_k^2 for all $k = 0, \ldots, D-1$. We now give some examples of four-dimensional MCR signal sets of size 16, having spectral efficiency 1 bit/dim.

Example 1—The PAM$(16, 4)$ Signal Set: A simple MCR signal set is a repetition code of length 4 over the one-dimensional 16-PAM signal set $1/\sqrt{85}\{\pm1, \pm3, \ldots, \pm15\}$. The resulting four-dimensional constellation with normalized average energy per dimension, denoted by PAM$(16, 4)$, is made of 16 points equally spaced along the main diagonal of a hypercube. The minimum SED of the projections are $d_0^2 = 0.188, d_1^2 = 0.141, d_2^2 = 0.094$ and $d_3^2 = 0.047$. ♢

Example 2—The RH$(16, 4)$ Signal Set: An MCR signal set can be obtained by applying a suitable rotation to a four-dimensional hypercube with vertex coordinates $(\pm1, \pm1, \pm1, \pm1)$. In particular, the rotation matrix

$$\boldsymbol{R} = \begin{pmatrix} 0.4857 & 0.7859 & -0.2012 & -0.3255 \\ -0.7859 & 0.4857 & 0.3255 & -0.2012 \\ 0.2012 & 0.3255 & 0.4857 & 0.7859 \\ -0.3255 & 0.2012 & -0.7859 & 0.4857 \end{pmatrix} \tag{13}$$

was found in [24] to give maximum collision resistance and to maximize the minimum *product distance* within a certain family of rotation matrices. The obtained signal set, denoted by RH$(16, 4)$, has minimum SED 4. It is interesting to note that not all the $(D-k)$-dimensional projected constellations are equivalent. The four one-dimensional projections have minimum SED $= 0.003$. The six two-dimensional projections, shown in Fig. 2, have three minimum SEDs, namely $0.586, 0.422$, and 0.205 and the four three-dimensional projections all have minimum SED $= 1.530$. ♢

Example 3—The Z$(16, 4)$ signal set: Here, we show an example of a general algebraic construction which enables to obtain good MCR signal sets. Further details and examples can be found in [33]. Let $\mathbb{Z}_{16}$ be the ring of integers modulo 16 and consider the $\mathbb{Z}_{16}$-module $\Lambda = \mathbb{Z}_{16}G$, with $G = [g_1, g_2, g_3, g_4]$ (i.e., the set of vectors $\boldsymbol{z} = zG$, with $z \in \mathbb{Z}_{16}$, which can be seen as a $(4, 1)$ linear code over $\mathbb{Z}_{16}$ with generator matrix G [34]). If the elements of G have a multiplicative inverse in $\mathbb{Z}_{16}$, then the minimum Hamming distance of Λ is 4. The resulting MCR signal set $\mathcal{S}$ is obtained by applying componentwise the mapping $\mathbb{Z}_{16} \to \mathbb{R}$ defined by $s = 2z - 15$ to all $\boldsymbol{z} \in \Lambda$, and by normalizing the average energy per component.

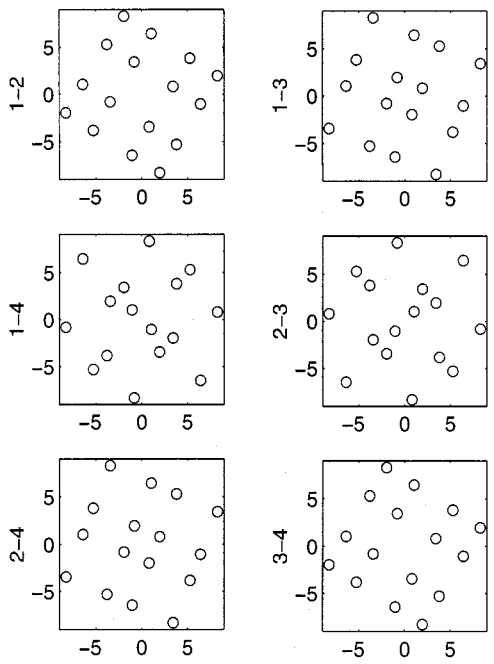

Fig. 2. The six two-dimensional projections of RH $(16,\ 4)$ of Example 2.

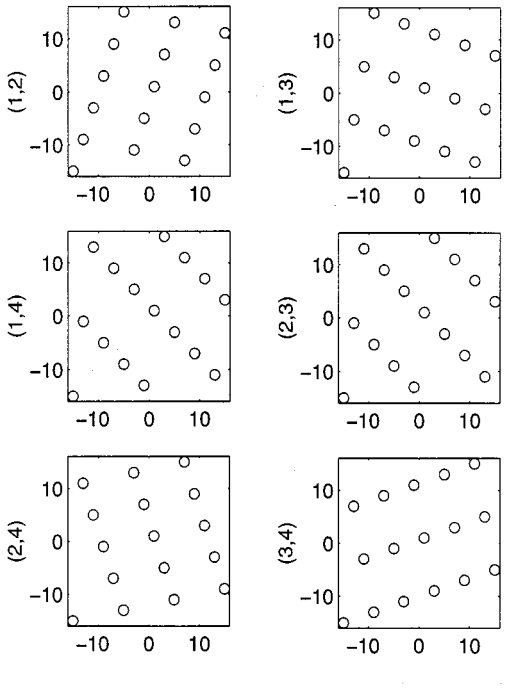

Fig. 3. The six two-dimensional projections of Z $(16,\ 4)$ of Example 3.

The signal set can be optimized by selecting G (e.g., with $G = [1,1,1,1]$ we obtain PAM $(16,\ 4)$). The choice $G = [1,3,5,7]$ proves to be particularly good. The resulting signal set, denoted by Z $(16,\ 4)$, has minimum SED$= 3.012$. The four one-dimensional projections have minimum SED $= 0.047$. The six two-dimensional projections, shown in Fig. 3, have two different minimum SEDs, namely, 0.471 and 0.377 and the four three-dimensional projections all have minimum SED $= 1.647$. $\diamondsuit$

Fig. 4 shows $\overline{P}(e|k)$ versus E_b/N_0 for the signal sets PAM $(16,\ 4)$, RH $(16,\ 4)$, and Z $(16,\ 4)$, for $k = 0,1,2,3$. The error curves of Z $(16,4)$ are more uniformly spaced in the useful SNR range, thus resulting in a more graceful performance degradation as the number of collisions increases.

IV. Concatenated Coding with Hard Decoding

In this section we evaluate the word-error probability of concatenated coding schemes $\mathcal{X} = \mathcal{C} \rightarrow \boldsymbol{\mu} \rightarrow \mathcal{S}$ over the on–off channel, where $\mathcal{S}$ is a D-dimensional MCR signal set, MCR interleaving with finite depth M is employed, and the receiver is formed by a symbol-by-symbol hard detector (SBSHD) followed by a t-error correcting decoder.[4] In the following, $\boldsymbol{c} \in \mathcal{C}$ denotes the transmitted codesword, $\boldsymbol{x} = (\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{qN})$ is the corresponding signal sequence, $\hat{\boldsymbol{x}} = (\hat{\boldsymbol{s}}_1, \ldots, \hat{\boldsymbol{s}}_{qN})$ is the sequence of detected signals at the output of the SBSHD, and $\hat{\boldsymbol{a}} = (\hat{a}_1, \ldots, \hat{a}_N)$ is the corresponding symbol sequence at the decoder input.

[4]Schemes making use of side reliability information on the SBSHD outputs, and/or error and erasures decoding are left for future investigation.

The WER $P(w)$ after bounded-distance error-only hard decoding is given by [27]

$$P(w) = \sum_{h=t+1}^{N} P(h) \tag{14}$$

where $P(h)$ is the probability that $\hat{\boldsymbol{a}}$ and $\boldsymbol{c}$ differ in h positions. Then, the key quantity to be evaluated next is $P(h)$.

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_M)$ be the collision pattern occurring over the M slots spanned by the transmission of $\boldsymbol{x}$. Consider the ith detected symbol $\hat{a}_i$ and the corresponding detected signals $(\hat{\boldsymbol{s}}_{q(i-1)+1}, \ldots, \hat{\boldsymbol{s}}_{q(i-1)+q})$. The detection error events $\{\boldsymbol{s}_{q(i-1)+j} \neq \hat{\boldsymbol{s}}_{q(i-1)+j}\}$ (for $i = 1, \ldots, N$ and $j = 1, \ldots, q$) are statistically independent if conditioned on $\boldsymbol{\alpha}$. Then, the probability of h errors given $\boldsymbol{\alpha}$ can be written in general as

$$P(h|\boldsymbol{\alpha}) = \sum_{\phi \in \Phi_h^N} \prod_{i \in \phi} P(e_i|\boldsymbol{\alpha}) \prod_{i \notin \phi} (1 - P(e_i|\boldsymbol{\alpha})) \tag{15}$$

where the events $e_i = \{\hat{a}_i \neq c_i\}$ have conditional probability

$$P(e_i|\boldsymbol{\alpha}) \triangleq 1 - \prod_{j=1}^{q} (1 - P(\boldsymbol{s}_{q(i-1)+j} \neq \hat{\boldsymbol{s}}_{q(i-1)+j}|\boldsymbol{\alpha})). \tag{16}$$

The desired $P(h)$ can be obtained by averaging $P(h|\boldsymbol{\alpha})$ over $\boldsymbol{\alpha}$ and over $\boldsymbol{c} \in \mathcal{C}$.

In general, $P(h|\boldsymbol{\alpha})$ is difficult to evaluate. Then, we shall compute the expectation of $P(h|\boldsymbol{\alpha})$ over the ensemble of all labeling maps $\boldsymbol{\mu}$ and over all sequences of random component permutations $\pi \in \Pi_D$. From a standard random-coding argument [1], there exist a sequence of labeling maps and component permutations such that the resulting concatenated coding

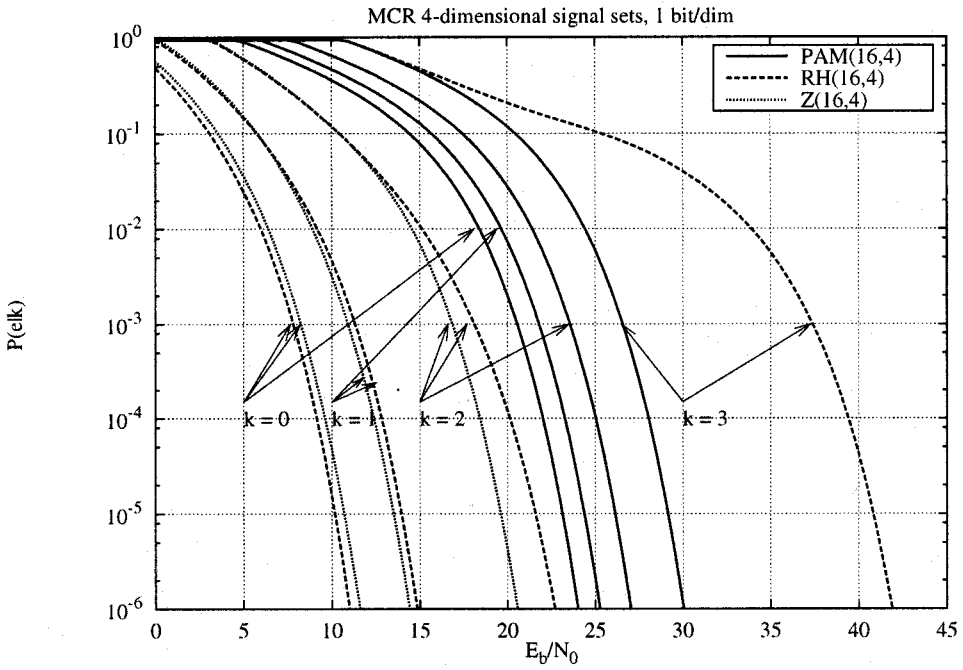

Fig. 4. $\overline{P}(e|k)$ versus E_b/N_0 for the MCR signal sets PAM $(16,\ 4)$, RH $(16,\ 4)$, and Z $(16,\ 4)$, for $k = 0, 1, 2, 3$. The curves of PAM $(16,\ 4)$ and Z $(16, 4)$ for $k = 3$ coincide, as these signal sets have the same one-dimensional projections.

scheme performs at least as good as the average. It is immediate to check that the expected $P(h|\boldsymbol{\alpha})$ is given by

$$\overline{P}(h|\boldsymbol{\alpha}) = \sum_{\phi\subset\Phi_h^N} \prod_{i\in\phi} \left[1 - \prod_{j=1}^{q}(1-\overline{P}(e|k_{q(i-1)+j}))\right] \cdot \prod_{i\notin\phi}\prod_{j=1}^{q}(1-\overline{P}(e|k_{q(i-1)+j})) \quad (17)$$

where $\overline{P}(e|k)$ is upper-bounded in (9) and where $k_{q(i-1)+j}$ is the number of collided components for the signal transmitted in position $q(i-1)+j$ of the coded sequence. Clearly, $k_{q(i-1)+j}$ is a function of $\boldsymbol{\alpha}$. For a given interleaver, the evaluation of (17) is still prohibitively complex for large N. Moreover, the result would depend on the particular interleaver. In order to overcome these difficulties, we shall consider the average performance over all RMCR interleavers and an easily computable expression which closely approximate the performance of *good* MCR interleavers (we will clarify the concept of good interleavers later on).

A. Average over RMCR Interleavers

By averaging $\overline{P}(h|\boldsymbol{\alpha})$ over the ensemble of RMCR interleavers we obtain an upper bound on the performance of the best MCR interleaver. With RMCR interleaving, the slots over which each signal $\boldsymbol{s}_{q(i-1)+j}$ is transmitted are given by the $(q(i-1)+j)$th row of the interleaver array, independently randomly selected from the ordered combinations set Ξ_D^M. It is immediate to show that, for a given $\boldsymbol{\alpha}$ of weight $W(\boldsymbol{\alpha}) = M - c$, the number of collisions $k_{q(i-1)+j}$ is a random variable conditionally distributed as $P_{M,D}(k|c)$, given by

$$P_{M,D}(k|c) = \begin{cases} \frac{\binom{c}{k}\binom{M-c}{D-k}}{\binom{M}{D}}, & \text{if } \max\{0, D-M+c\} \le \\ & \le k \le \min\{c, D\} \\ 0, & \text{otherwise.} \end{cases} \quad (18)$$

Since the slot selection for different signals is independent, the $k_{q(i-1)+j}$'s in (17) are conditionally independent. Then, by averaging over the RMCR interleaver ensemble, after some algebra we obtain

$$\overline{P}_{\text{ave}}(h|\boldsymbol{\alpha}) = B(N, h, 1-(1-\overline{P}(e|c))^q) \quad (19)$$

where $\overline{P}(e|c)$ is given by

$$\overline{P}(e|c) = \sum_{k=0}^{D} P_{M,D}(k|c)\overline{P}(e|k). \quad (20)$$

Finally, since $\overline{P}_{\text{ave}}(h|\boldsymbol{\alpha})$ depends only on the number of collisions c rather than on the particular collision pattern $\boldsymbol{\alpha}$ and since c is binomially distributed, we have

$$\overline{P}_{\text{ave}}(h) = \sum_{c=0}^{M} B(M, c, P_{\text{col}})\, B(N, h, 1-(1-\overline{P}(e|c))^q). \quad (21)$$

By using (21) in (14), we obtain the desired WER average bound.

For small M this bound might be loose, in the sense that it is easy to find interleavers performing significantly better than the average. Intuitively, good interleavers are such that, for all

$\boldsymbol{\alpha}$ of weight $M-c$ with $c \geq D$, the number of positions i for which $k_{q(i-1)+j} = D$ (for $j = 1, \ldots, q$) is minimum. In fact, if $k_{q(i-1)+j} = D$, the signal $\boldsymbol{s}_{q(i-1)+j}$ has all collided components and the SBSHD chooses at random $\hat{\boldsymbol{s}}_{q(i-1)+j} \in \mathcal{S}$ with uniform probability, so that the probability that $\hat{a}_i \neq c_i$ is large. Then, a good interleaver minimizes the number of "very probable" symbol errors at the decoder input. In the random ensemble with small M, bad interleavers dominate the average performance. However, as $M \to \infty$, from Lemma 2 of Appendix A, we have that

$$\lim_{M\to\infty} \overline{P}_{\text{ave}}(h) = B(N, h, 1-(1-P(e))^q) \triangleq \overline{P}_{\text{i.i.d.}}(h) \quad (22)$$

where $P(e)$ is given in (11). $\overline{P}_{\text{i.i.d.}}(h)$ corresponds to independent collisions, i.e., perfect interleaving and can be obviously obtained if $M \geq qND$. The limit (22) shows shows that the average interleaver performs as well as the best one for large interleaving depth, and that bad interleavers in the ensemble are asymptotically irrelevant.

B. Approximation for Good Interleavers

If the block length N of $\mathcal{C}$ satisfies $N = L\binom{M}{D}$ for some integer L, a good interleaver can be explicitly constructed by writing the elements ϕ of the combinations set Φ_D^M as a row of $\boldsymbol{M}$, for all $\phi \in \Phi_D^M$, and by repeating each row formed in this way exactly qL times.[5] In this way, exactly qL signals are transmitted over the same set of D out of M slots, such that the q signals $(\boldsymbol{s}_{q(i-1)+1}, \ldots, \boldsymbol{s}_{q(i-1)+q})$ corresponding to the ith symbol are transmitted over the same set of D slots. The number of symbols having signal completely collided is equal to $NP_{M,D}(D|c)$ for all patterns $\boldsymbol{\alpha}$ of weight $M-c$. In this way, the maximum number of "very probable" symbol errors over the ensemble of all collision patterns is minimized (a minimax approach to the interleaving design).

Example 4—Good Interleaver: Table I gives an example of such situation with $M=6$, $D=3$, $q=1$, and $N=\binom{M}{D}=20$. If one collision occurs in any one of the six slots, then exactly $NP_{M,D}(1|1) = \binom{5}{2} = 10$ symbols are hit in one component. If two collisions occur in any two slots, then exactly $NP_{M,D}(1|2) = 2\binom{4}{2} = 12$ symbols are hit in one component and $NP_{M,D}(2|2) = \binom{4}{1} = 4$ symbols are hit in two components. If three collisions occur, nine symbols are hit in one component, nine in two components, and one in three. With four collisions, 4, 12, and 4 symbols are hit, respectively, in one, two, and three components. With five collisions, 10 symbols are hit in two components and 10 in three. With six collisions no symbol is received. ♢

The WER for interleavers of the above type can be computed *exactly* as follows. For a given $\boldsymbol{\alpha}$, define the index set

$$\mathcal{J}_k(\boldsymbol{\alpha}) \triangleq \{i \in \{1, \ldots, N\}: k_{q(i-1)+j} = k, j = 1, \ldots, q\}.$$

$\mathcal{J}_k(\boldsymbol{\alpha})$ contains the indices of symbols whose corresponding signals have exactly k collided components. By construction, $|\mathcal{J}_k(\boldsymbol{\alpha})| = NP_{M,D}(k|c)$, which depends on $\boldsymbol{\alpha}$ only through its weight $M-c$. Define $L_{k|c} \triangleq |\mathcal{J}_k(\boldsymbol{\alpha})|$ and let H_k be the number of symbol error events $\{\hat{a}_i \neq c_i\}$ for $i \in \mathcal{J}_k(\boldsymbol{\alpha})$. Then, since after conditioning with respect to $\boldsymbol{\alpha}$ the symbol error events are statistically independent, H_k is binomially distributed as

$$P(H_k = h|\boldsymbol{\alpha}) = B(L_{k|c}, h, 1-(1-\overline{P}(e|k))^q). \quad (23)$$

Moreover, the H_k are conditionally statistically independent, given $\boldsymbol{\alpha}$. Since $\{\mathcal{J}_k(\boldsymbol{\alpha})\colon k = 0, \ldots, D\}$ is a partition of the index set $\{1, \ldots, N\}$ for all $\boldsymbol{\alpha}$, the total number of symbol errors is given by the sum $H = \sum_{k=0}^{D} H_k$. Then

$$\overline{P}_{\text{good}}(h|\boldsymbol{\alpha}) \triangleq P(H = h|\boldsymbol{\alpha}) \quad (24)$$

can be computed easily by convolving the binomial distributions given in (23) for $k = 0, \ldots, D$ and given c.

Unfortunately, the condition that $\binom{M}{D}$ divides N is often too restrictive. Then, for general N, M, and D, a search for optimized interleavers is needed. Intuitively, we expect that good interleavers behave as close as possible to the case where $\binom{M}{D}$ divides N, even if this condition is not satisfied. Driven by this argument, we can approximate the performance of any good interleaver by assuming the existence of an interleaver such that, for all $\boldsymbol{\alpha}$ of weight $M-c$, the size of $\mathcal{J}_k(\boldsymbol{\alpha})$ is as close as possible to $NP_{M,D}(k|c)$ (that in general is not integer). In particular, let

$$L_{k|c} = [NP_{M,D}(k|c)] + e_{k|c} \quad (25)$$

where $[\cdot]$ denotes rounding to the closest integer and $e_{k|c} \in \mathbb{Z}$ is chosen such that $\sum_{k=0}^{D} L_{k|c} = N$ and $\sum_{k=0}^{D} |e_{k|c}|$ is minimum. Then, from the same argument leading to (24), by convolving the binomial distributions defined by (23) for the $L_{k|c}$'s given in (25) we obtain the desired approximation for good interleavers.

As a consequence of Fact 1 in Section III, for RMCR interleavers with large N, any given M-combination of size D appears on the rows of the interleaver array approximately the same number $qN/\binom{M}{D}$ of times. Then, for large block length N any RCMR interleaver can be turned into a good interleaver (i.e., an interleaver such that its actual $\overline{P}(h|\boldsymbol{\alpha})$ is close to $\overline{P}_{\text{good}}(h|\boldsymbol{\alpha})$ for all $\boldsymbol{\alpha}$) by simple row reordering.

Example 5: Consider $\mathcal{X} = \mathcal{C} \to \boldsymbol{\mu} \to \mathcal{S}$ where $\mathcal{C}$ is the Reed–Solomon (RS) code with parameters $(15, 11, 5)$ over GF(16) and $\mathcal{S} = \text{Z}(16, 4)$ (in this case, $q = 1$). Fig. 5 shows WER versus E_b/N_0 obtained by Monte Carlo simulation and closed-form analysis, with interleaving depth $M = 8$ and $P_{\text{col}} = 0.1$. The average bound (AVE) agrees perfectly with the simulation (SIM) obtained by generating a different RMCR interleaver for each transmitted codesword. The bad interleaver of Table II (left) performs significantly worse than the average, while the hand-designed good interleaver of Table II (right) outperforms the average. The approximation (GOOD) obtained via (25) is very close to the actual performance of the good interleaver. ♢

Example 6: Fig. 6 shows the WER versus E_b/N_0 for $\mathcal{X} = \mathcal{C} \to \boldsymbol{\mu} \to \mathcal{S}$ where $\mathcal{C}$ is the shortened RS code with parameters $(210, 168, 43)$ over GF(256) and $\mathcal{S} = \text{Z}(16, 4)$ (in this case, $q = 2$). The code information rate is $R = 0.8$ bit/dim. The curves for finite M are obtained by the approximation for

[5]Actually, ϕ is an *unordered* set while the rows of $\boldsymbol{M}$ are *ordered* vectors. Without loss of generality, we may assume that the elements of ϕ are written in lexicographic order. By permuting the rows elements, we obtain different interleavers with the same MCR property.

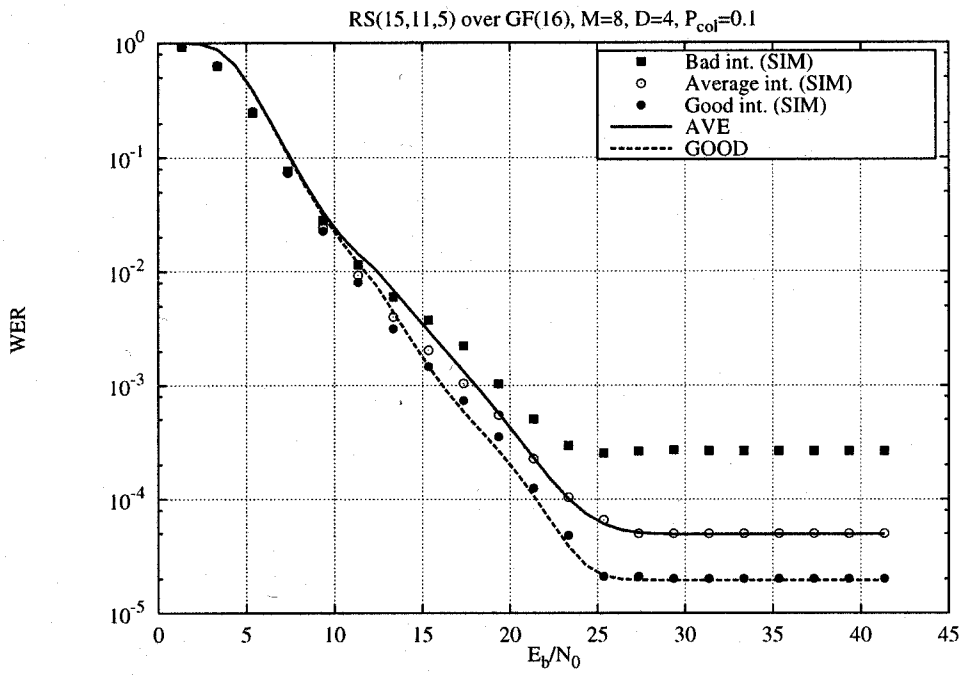

Fig. 5. WER versus E_b/N_0 for the RS-encoded scheme of Example 5, with $M = 8$ and $P_{\rm col} = 0.1$.

TABLE II
ARRAYS $\boldsymbol{M}$ FOR THE BAD (LEFT) AND THE GOOD (RIGHT) INTERLEAVERS OF EXAMPLE 5

8	7	6	4
8	7	6	4
8	7	6	4
8	7	5	3
8	7	5	3
8	7	5	3
8	7	5	3
8	7	5	3
8	7	5	3
8	6	5	2
8	6	4	2
8	6	4	2
8	6	4	2
7	6	4	1
7	6	4	1

2	5	1	4
5	3	6	7
1	4	6	8
5	1	8	6
1	5	4	6
6	7	3	1
3	2	8	7
3	5	2	6
5	4	3	7
1	7	3	8
8	5	6	7
1	5	4	8
6	5	2	4
2	1	7	8
7	5	1	8

good interleavers described above. For $M = D = 4$, the error probability curve presents five flat regions ("plateaus") and four rapidly decreasing regions ("steps"). The cth plateau, for $c = 0, 1, 2, 3, 4$, corresponds to the SNR region where the signals experiencing $\geq c$ collided components are wrongly detected with high probability, and the signals with $< C$ collided components are correctly detected with high probability. The zeroth and the fourth plateaus correspond to the regions where the system is either completely noise-limited or completely interference-limited, respectively. As M becomes larger than D, the number of plateaus and steps increases until they become indistinguishable, since there are more and more ways of placing c collisions over M slots, each of which occurs with smaller and smaller probability. We observe that, by increasing M, both a coding gain at intermediate SNR and a lower error floor at large SNR are achieved, at the price of a larger delay.

The WER obtained by the same RS code with conventional binary antipodal modulation (2PAM) can be computed, for any interleaving depth M, by one of the methods described in [35]. For comparison, Fig. 6 shows the case of $M = 4, 16$, and of perfect interleaving. It is apparent that the use of MCR signal sets yields very large performance improvements with respect to conventional noncollision resistant signal sets. Such bad performance of RS-coded 2PAM might be surprising, but it can be easily understood if we notice that, in the case of perfect interleaving and large SNR, the probability of a symbol error at the decoder input is close to the collision probability $P_{\rm col} = 0.1$, and that high-rate RS codes are efficient for much smaller symbol error probabilities (normally, $\leq 10^{-3}$). On the contrary, with D-dimensional MCR signal sets, perfect interleaving, and large SNR, the symbol error probability is close to $P_{\rm col}^D$ (in our case, 10^{-4}).

C. Spectral Efficiency of RS-Encoded MCR Signal Sets

In this section we study the spectral efficiency η of RS-encoded MCR signal sets used over the G-MACC, in the limit for large SNR. Let $\mathcal{S}$ be a D-dimensional MCR signal set of size $|\mathcal{S}|$. Then, from the MCR property, assuming that the SBSHD

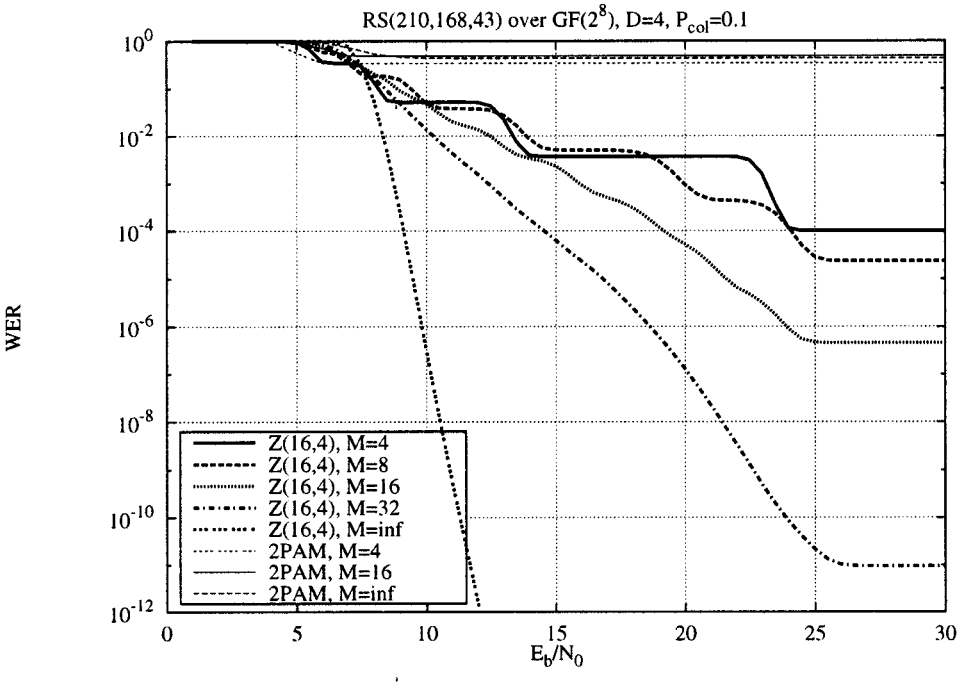

Fig. 6. WER versus E_b/N_0 for the RS-encoded scheme of Example 6, with $M = 4, 8, 16, 32,$ and ∞ (perfect interleaving) and $P_{\rm col} = 0.1$. For comparison, the WER of the same RS code with conventional 2PAM is shown for $M = 4, 16,$ and ∞.

makes a random choice if all components of the received signal are collided, we have

$$\lim_{\rm SNR\to\infty} \overline{P}(c|k) = \begin{cases} 0, & \text{if } k < D \\ 1 - 1/|\mathcal{S}|, & \text{if } k = D. \end{cases} \tag{26}$$

Since we are interested in the performance of long codes with good interleavers, we shall use the WER approximation described in the previous section, which can be achieved asymptotically as N increases. From the convolution of the binomial distributions defined by (23) and from (26), we can show that

$$\lim_{\rm SNR\to\infty} \overline{P}(h|\boldsymbol{\alpha}) = B(L_{D|c}, h, p_q) \tag{27}$$

for all $\boldsymbol{\alpha}$ of weight $M - c$, where we define $p_q \stackrel{\Delta}{=} 1 - |\mathcal{S}|^{-q}$. Consider an RS code with parameters $(N, N-2t, 2t+1)$. Then, as SNR $\to \infty$, the limiting WER is given by

$$\lim_{\rm SNR\to\infty} P(w) = \sum_{c=0}^{M} B(M, c, P_{\rm col}) \sum_{h=t+1}^{L_{D|c}} B(L_{D|c}, h, p_q). \tag{28}$$

As in [14], we may compute the WER limit for large block length and fixed code rate. Since the RS code alphabet size increases with N, for fixed $|\mathcal{S}|$ the number q of signals for each code symbol grows to infinity as $N \to \infty$. Then, $\lim_{q\to\infty} p_q = 1$ and

$$B(L_{D|c}, h, 1) = 1\{h = L_{D|c}\}. \tag{29}$$

In other words, for large SNR and block length, a codesword having c collided slots is affected by exactly $L_{D|c}$ symbol errors. Let $r = 1 - 2t/N$ be the RS code rate. From (25),

$$\frac{1}{N} L_{D|c} \to P_{M,D}(D|c), \qquad \text{as } N \to \infty.$$

Then

$$\begin{aligned} \lim_{N\to\infty} & \sum_{h=N(1-r)/2+1}^{L_{D|c}} 1\{h = L_{D|c}\} \\ &= \lim_{N\to\infty} 1\{N(1-r)/2 + 1 \le L_{D|c}\} \\ &= \lim_{N\to\infty} 1\left\{(1-r)/2 + \frac{1}{N} \le \frac{1}{N} L_{D|c}\right\} \\ &= 1\{(1-r)/2 < P_{M,D}(D|c)\}. \end{aligned} \tag{30}$$

Finally, by using the above limit in (28) we get

$$\begin{aligned} \lim_{N\to\infty} \lim_{\rm SNR\to\infty} & P(w) \\ &= \sum_{c=0}^{M} B(M, c, P_{\rm col}) 1\{(1-r)/2 < P_{M,D}(D|c)\}. \end{aligned} \tag{31}$$

In the case of perfect interleaving ($M \to \infty$), from Lemma 2 of Appendix A we obtain

$$\lim_{M\to\infty} \lim_{N\to\infty} \lim_{\rm SNR\to\infty} P(w) = 1\{(1-r)/2 < P_{\rm col}^D\} \tag{32}$$

(the above limit holds for all $P_{\rm col}^D \neq (1-r)/2$. If $P_{\rm col}^D = (1-r)/2$ with $0 < P_{\rm col} < 1$, it can be shown that the limit of $P(w)$ is equal to $1/2$).

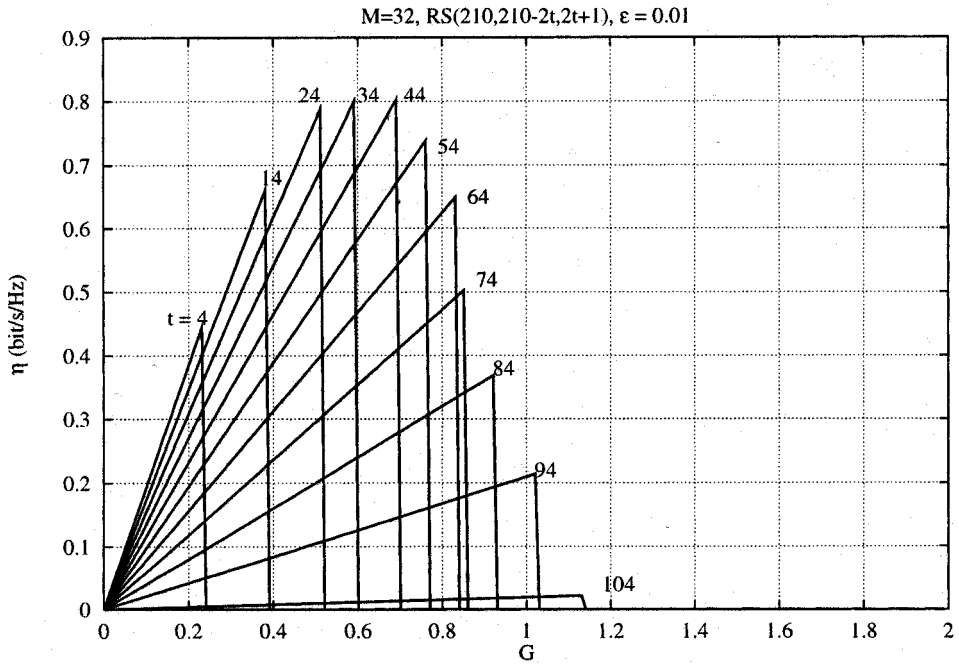

Fig. 7. η versus G for the shortened RS family with parameters $(210, 210-2t, 2t+1)$ over GF(256), with a four-dimensional MCR signal set of size 16, maximum WER constraint $\epsilon = 10^{-2}$, and interleaving $M = 32$. The value of t is reported next to each curve.

The asymptotic spectral efficiency for large SNR, subject to a WER (i.e., packet-error) probability not larger than ϵ, is given by

$$\eta = \begin{cases} 2G\frac{\log_2|\mathcal{S}|}{D}\, r, & \text{if } P_\infty(w) \le \epsilon \\ 0, & \text{if } P_\infty(w) > \epsilon \end{cases} \tag{33}$$

where $P_\infty(w)$ is given either by (28) for finite N, M, or by (31) for $N \to \infty$ and finite M or by (32) when $N, M \to \infty$. For given G, there exists an optimal code rate $r^*(G)$ maximizing η. The maximum η versus G can be obtained graphically, by taking the envelope of all the curves defined by (33), for $r \in [0, 1]$. In the case of perfect interleaving, from (32) and (1) we get explicitly the optimum code rate as

$$r^*(G) = \max\{1 - 2(1 - e^{-G})^D, 0\}. \tag{34}$$

D. Results

Fig. 7 shows η versus G for the shortened RS family with parameters $(210, 210-2t, 2t+1)$ over GF(256) concatenated with an MCR signal set with $D = 4$ and $|\mathcal{S}| = 16$ (e.g., any of the signal sets of Examples 1, 2 and 3), for t ranging from 0 to 104, $M = 32$ and the desired maximum WER $\epsilon = 10^{-2}$. As expected, the optimum code rate $r^*(G)$ is a decreasing function of G.

Fig. 8 shows the maximum η versus G for asymptotically large N, MCR signal sets with $D = 4$, and $|\mathcal{S}| = 16$, different values of M and desired maximum WER $\epsilon = 10^{-2}$. These curves are obtained from (31) and (33), by optimizing r for each G. The curve for $M \to \infty$ (obtained from (34)) is shown for comparison.

V. Outage Probability and Achievable Rate

Both channel models (3) and (4) fall in the class of *block-interference channels* studied in [20]–[22]. These channels may or may not behave ergodically (or more generally, be *information-stable*) depending on the delay constraint. In particular, ergodicity does not hold if $M < \infty$ [21].

From the very general approach of [36] (details are given in Appendix B), by letting the code block length $N \to \infty$ and M fixed and finite, we obtain the *instantaneous mutual information* I_M of the M-slot channel spanned by the transmission of a user codesword. Being a function of the collision pattern, I_M is a random variable. Following [21], we define the *information outage probability* as

$$P_{\text{out}}(R) \triangleq P(I_M < R). \tag{35}$$

$P_{\text{out}}(R)$ is equal to the WER averaged over the random coding ensemble of rate R and over all collision patterns, for $N \to \infty$ and fixed $M < \infty$ [37], [36]. In our system, $P_{\text{out}}(R)$ yields the limiting packet-error probability under a given delay constraint.

From the same general approach, by letting first $N \to \infty$ and then $M \to \infty$, we obtain the achievable rate ergodic I_∞. This yields the limiting spectral efficiency of delay-unconstrained systems.

In the rest of this section, we present expressions for I_M, $P_{\text{out}}(R)$, and I_∞ under different assumptions on the user signal set (or input distribution) and on the type of decoding. Proofs

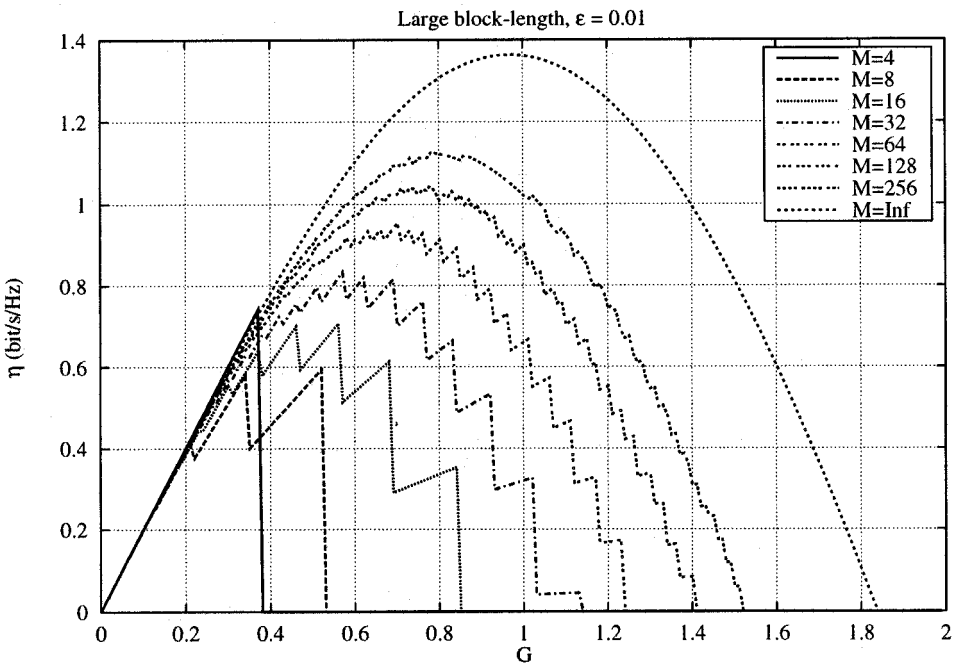

Fig. 8. Maximum η versus G for infinitely long RS codes, with a four-dimensional MCR signal set of size 16, maximum WER constraint $\epsilon = 10^{-2}$, and different interleaving depths. The code rate is optimized for each value of G.

are collected in Appendix C. These results serve as a baseline comparison of different coding and decoding schemes.

A. VPAN Channel with Gaussian Inputs

User codes are independently generated according to a Gaussian distribution $\mathcal{N}(0, \mathcal{E})$. With the channel model (3) and perfect CSI, the instantaneous mutual information is given by

$$I_M = \frac{1}{M}\sum_{m=1}^{M} \frac{1}{2}\log_2\left(1 + \frac{\mathcal{E}}{K_m\mathcal{E} + N_0/2}\right) \tag{36}$$

where the K_m's are i.i.d. Poisson-distributed with mean G. The exact evaluation of the outage probability is difficult if not impossible in general. However, we can find upper and lower bounds by defining two appropriate lattice random variables [29] I_{up} and I_{lo} such that

$$\begin{aligned} P(I_{\text{up}} \le x) &\ge P\left(\frac{1}{2M}\log_2(1 + \mathcal{E}/(K_1\mathcal{E} + N_0/2)) \le x\right) \\ &\ge P(I_{\text{lo}} \le x) \end{aligned}$$

and by computing the M-fold convolution of their probability mass distributions. We shall not give further details about this method because of space limitations. Also, from Jensen's inequality we can write

$$I_M \ge \frac{1}{2}\log_2\left(1 + \frac{\mathcal{E}}{\frac{1}{M}\sum_{m=1}^{M} K_m\mathcal{E} + N_0/2}\right) \tag{37}$$

so that $P_{\text{out}}(R)$ can be upper-bounded by the probability that the right-hand side (RHS) of the above inequality is less than R.

The delay-unconstrained achievable rate is given by

$$I_\infty = E\left[\frac{1}{2}\log_2\left(1 + \frac{\mathcal{E}}{K_1\mathcal{E} + N_0/2}\right)\right]. \tag{38}$$

B. On–Off Channel with Gaussian Inputs

User codes are generated as before. With the channel model (4) and perfect CSI, the instantaneous mutual information is given by

$$I_M = \frac{M - c}{2M}\log_2\left(1 + \frac{2\mathcal{E}}{N_0}\right) \tag{39}$$

where $W(\boldsymbol{\alpha}) = M - c$ and c is the number of collisions in the pattern $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_M)$. Since I_M is a nonincreasing function of c, and c is binomially distributed, the outage probability can be computed as

$$P_{\text{out}}(R) = 1 - \sum_{c=0}^{c'} B(M, c, P_{\text{col}}) \tag{40}$$

where c' is the largest c such that $I_M \ge R$.

The delay-unconstrained achievable rate is given by

$$I_\infty = \frac{1 - P_{\text{col}}}{2}\log_2\left(1 + \frac{2\mathcal{E}}{N_0}\right). \tag{41}$$

C. On-Off Channel, MCR Signal Sets with Soft Decoding

In this case, user codes $\mathcal{X} = \mathcal{C} \to \boldsymbol{\mu} \to \mathcal{S}$ are obtained by randomly generating $\mathcal{C}$ with i.i.d. components, uniformly

distributed on $\mathcal{A}$, and $\boldsymbol{\mu}$ with i.i.d. components, uniformly distributed on the set of all one-to-one mappings $\mathcal{A} \to \mathcal{S}^q$. With RMCR interleaving, we obtain

$$I_M = \frac{1}{D}\left\{\log_2|\mathcal{S}| - \sum_{k=0}^{D} P_{M,D}(k|c) F_{\mathcal{S}}(\mathcal{E}/N_0, k)\right\} \quad (42)$$

where $P_{M,D}(k|c)$ is given in (18), and where we define

$$F_{\mathcal{S}}(\mathcal{E}/N_0,k) \triangleq E_{\boldsymbol{s},\boldsymbol{n},\pi}\left[\log_2\left(\sum_{\boldsymbol{s}'\in\mathcal{S}} \exp\left(\frac{1}{N_0}\sum_{j=1}^{D-k} (2\sqrt{\mathcal{E}}(s'_{\pi(j)} - s_{\pi(j)})n_j - \mathcal{E}|s'_{\pi(j)} - s_{\pi(j)}|^2)\right)\right)\right] \quad (43)$$

($E_{\boldsymbol{s},\boldsymbol{n},\pi}[\cdot]$ denotes expectation with respect to $\boldsymbol{s} \sim$ uniform over $\mathcal{S}$, $n_j \sim \mathcal{N}(0, N_0/2)$, and $\pi \sim$ uniform over Π_D). The expectation in (43) can be evaluated numerically (e.g., by Monte Carlo simulation). Again, I_M depends only on the number of collisions c. Since I_M is nonincreasing in c, $P_{\text{out}}(R)$ can be computed by (40).

The delay-unconstrained achievable rate is given by

$$I_\infty = \frac{1}{D}\left\{\log_2|\mathcal{S}| - \sum_{k=0}^{D} B(D,k,P_{\text{col}}) F_{\mathcal{S}}(\mathcal{E}/N_0,k)\right\}. \quad (44)$$

D. On–Off Channel, MCR Signals with Hard Decoding

User codes are generated as before. The concatenation of a modulator for the discrete and finite signal set $\mathcal{S}$ with the G-MACC and with a SBSHD, conditioned on the collision pattern $\boldsymbol{\alpha}$, can be regarded as a discrete conditionally memoryless channel (DMC). In order to simplify the problem, we may consider the average of all transition probabilities with respect to all labeling maps and component permutations, for given $\boldsymbol{\alpha}$. It is immediate to show that the resulting *average* DMC is symmetric [1] with transition probabilities

$$P_k(\hat{\boldsymbol{s}}|\boldsymbol{s}) = \begin{cases} 1 - \overline{P}(e|k), & \text{if } \hat{\boldsymbol{s}} = \boldsymbol{s} \\ \frac{1}{|\mathcal{S}|-1}\overline{P}(e|k), & \text{if } \hat{\boldsymbol{s}} \neq \boldsymbol{s}. \end{cases} \quad (45)$$

From the convexity of the information density with respect to the channel transition probability and from Jensen's inequality, this yields a lower bound on I_M and I_∞.

We can interpret (45) as the transition probability assignment of a DMC depending on the channel "state" k, i.e., on the number of collisions k that occurred in the transmission of signal $\boldsymbol{s}$. If the knowledge of k for each transmitted $\boldsymbol{s}$ is available, we say that the decoder has perfect CSI. The instantaneous mutual information is given by

$$I_M = \frac{1}{D}\left\{\log_2|\mathcal{S}| - \overline{P}(e|c)\log_2(|\mathcal{S}|-1) - \sum_{k=0}^{D} P_{M,D}(k|c)\mathcal{H}(\overline{P}(e|k))\right\} \quad (46)$$

where $\overline{P}(e|c)$ is defined in (20). The resulting outage probability can be computed again from (40).

The delay-unconstrained achievable rate is given by

$$I_\infty = \frac{1}{D}\left\{\log_2|\mathcal{S}| - P(e)\log_2(|\mathcal{S}|-1) - \sum_{k=0}^{D} B(D,k,P_{\text{col}})\mathcal{H}(\overline{P}(e|k))\right\} \quad (47)$$

where $P(e)$ is given in (11).

Interestingly, in Appendix D we show that the same I_M and I_∞ are achieved by a decoder having no CSI. This is in agreement with the result of [20], showing that for a block-interference channel with $M \to \infty$ blocks of length $N/M < \infty$, the capacity without CSI converges to the capacity with perfect CSI as the ratio N/M increases. However, the result of [20] cannot be used in our case since it holds under an ergodic assumption ($M \to \infty$ and N/M finite), while our result needs no ergodicity (M finite and $N \to \infty$).

E. Results

Fig. 9 shows $P_{\text{out}}(R)$ versus E_b/N_0 in the cases of VPAN channel with Gaussian inputs (G–vpan, upper (UB) and lower (LB) bounds), on–off channel with Gaussian inputs (G-onoff), MCR signals with soft decoding (MCR-soft) and MCR signals with hard decoding (MCR-hard), for $R = 0.8$, $P_{\text{col}} = 0.1$, and $M = 4$. Fig. 10 shows analogous results for $M = 32$. In the case of MCR-soft and MCR-hard, we consider $\mathcal{S} = \text{Z}\,(16, 4)$. Then, $P_{\text{out}}(R)$ in the case of MCR-hard can be compared with the actual performance of RS-encoded schemes given in Fig. 6. For $M = 4$, $P_{\text{out}}(R)$ is very close to the actual WER attained by RS codes, while for $M = 32$ optimum coding and decoding yields a potential gain of about 3 dB at WER $= 10^{-2}$ and 5 dB at WER $= 10^{-4}$.

The spectral efficiency with finite interleaving, subject to a maximum outage (i.e., packet-error) probability constraint ϵ, is given by $\eta = 2GR^*(G)$, where $R^*(G)$ is the maximum information rate for which $P_{\text{out}}(R) \leq \epsilon$. Figs. 11 and 12 show η versus G for $M = 4$ and 32, respectively, $E_b/N_0 = 20$ dB, and $\epsilon = 10^{-2}$. The curves labeled by "G-vpan (JLB)" are obtained by using the Jensen's inequality lower bound (37).

The spectral efficiency with perfect interleaving is given by $\eta = 2GI_\infty(G)$, where $I_\infty(G)$ is I_∞ calculated for channel load equal to G. We can compare the performance of the schemes considered in this paper with other simple multiple-access schemes such as 1) ideal orthogonal access; 2) slotted (S-) ALOHA; and 3) NCDMA with SUMF or linear MMSE receiver.

The spectral efficiency of ideal orthogonal access with Gaussian inputs is

$$\eta_{\text{orth}} = \min\{G, 1\}\log_2(1 + 2\mathcal{E}/N_0). \quad (48)$$

This is also the symmetric capacity of the system. With S-ALOHA and infinite user population, the average number of delivered packets per slot is Ge^{-G} [5]. With Gaussian inputs, the resulting spectral efficiency is

$$\eta_{\text{aloha}} = Ge^{-G}\log_2(1 + 2\mathcal{E}/N_0). \quad (49)$$

Finally, NCDMA with direct-sequence spreading has spectral efficiency $\eta = N_u R_b/W = 2N_u R/L$, where L is the number of chips per symbol. As $N_u \to \infty$ with $N_u/L = G$, under

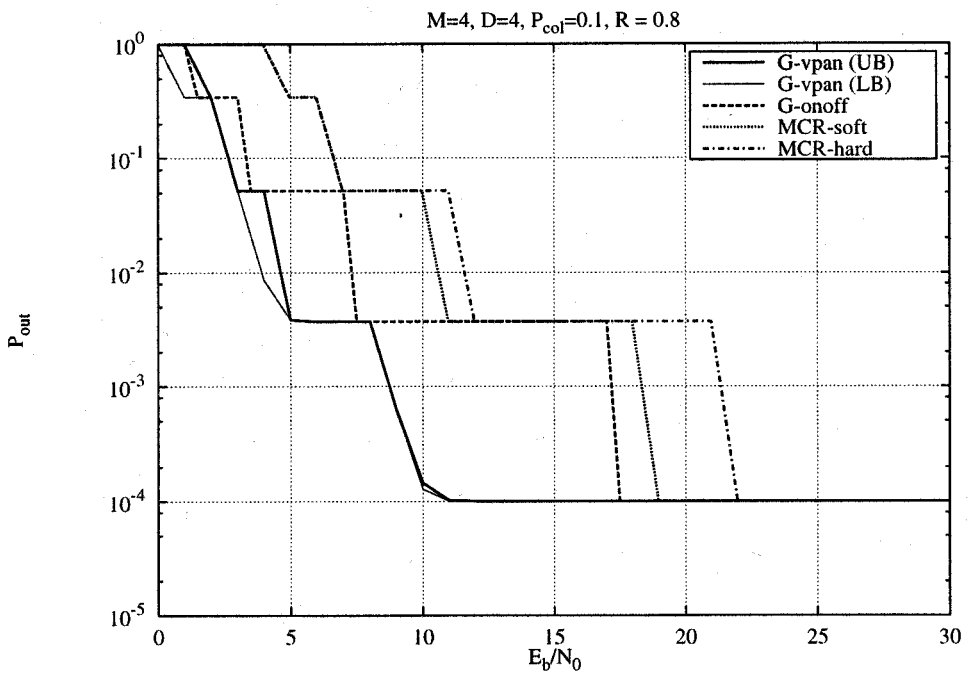

Fig. 9. $P_{\rm out}(R)$ versus E_b/N_0 for $R = 0.8$ bit/dim, $P_{\rm col} = 0.1$, and $M = 4$.

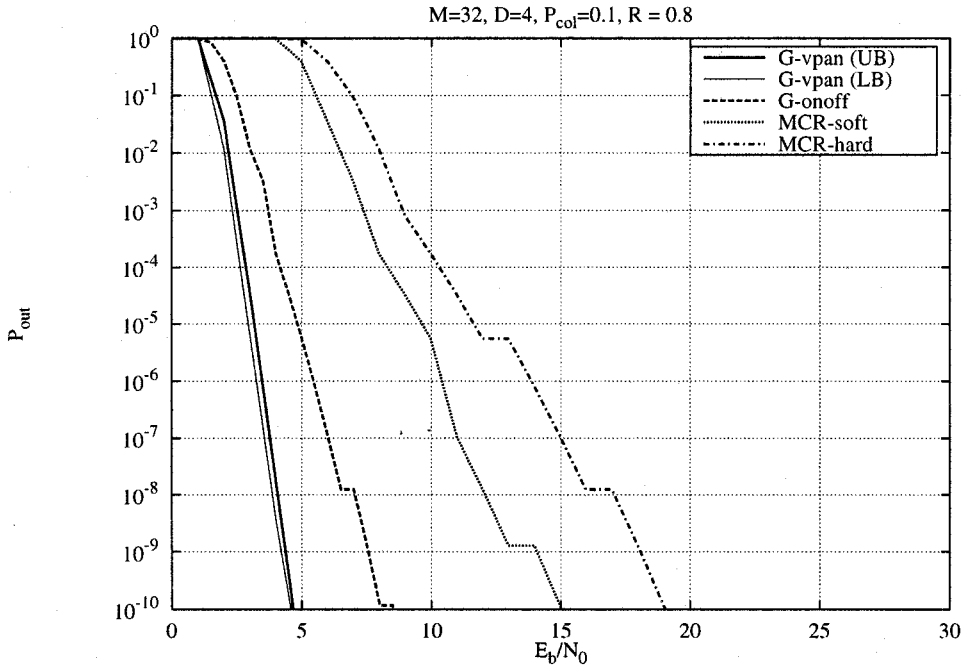

Fig. 10. $P_{\rm out}(R)$ versus E_b/N_0 for $R = 0.8$ bit/dim, $P_{\rm col} = 0.1$, and $M = 32$.

the assumption of independent and random selection of the spreading sequences and of Gaussian inputs, the spectral efficiency of NCDMA can be obtained in closed form from the results of [12]. For the SUMF receiver we have

$$\begin{cases} G = \frac{1}{\gamma} - \frac{N_0}{E_b \log_2(1+\gamma)} \\ \eta_{\rm sumf} = G \log_2(1+\gamma) \end{cases} \tag{50}$$

and for the linear MMSE receiver we have

$$\begin{cases} G = (1+\gamma)(\frac{1}{\gamma} - \frac{N_0}{E_b \log_2(1+\gamma)}) \\ \eta_{\rm mmse} = G \log_2(1+\gamma). \end{cases} \tag{51}$$

The above equations give η versus G in parametric form, where the parameter γ is the signal-to-interference ratio at the SUMF

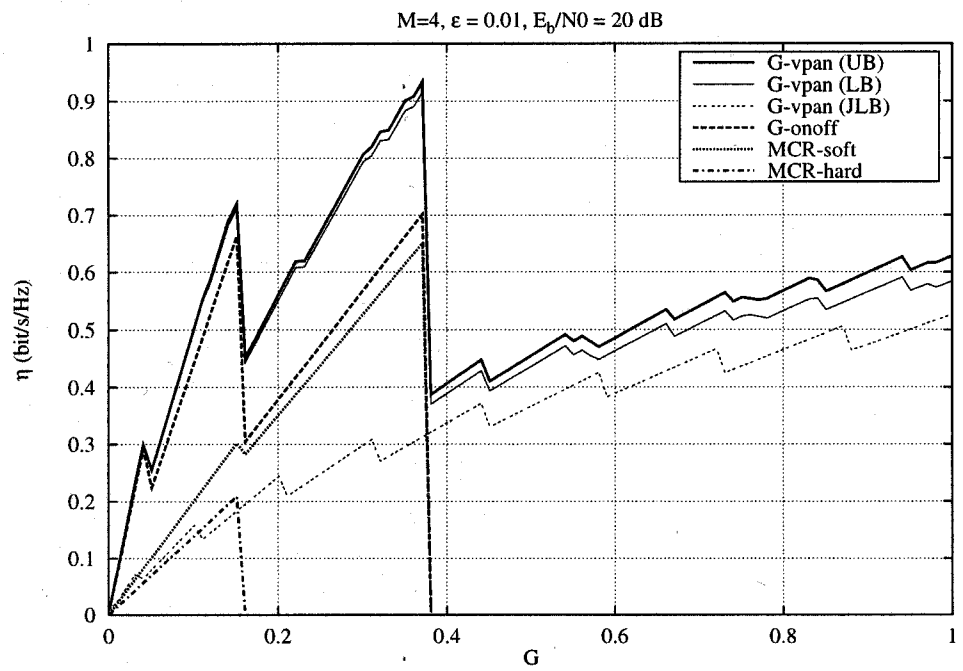

Fig. 11. η versus G for $M = 4$, maximum outage probability $\epsilon = 10^{-2}$, and $E_b/N_0 = 20$ dB.

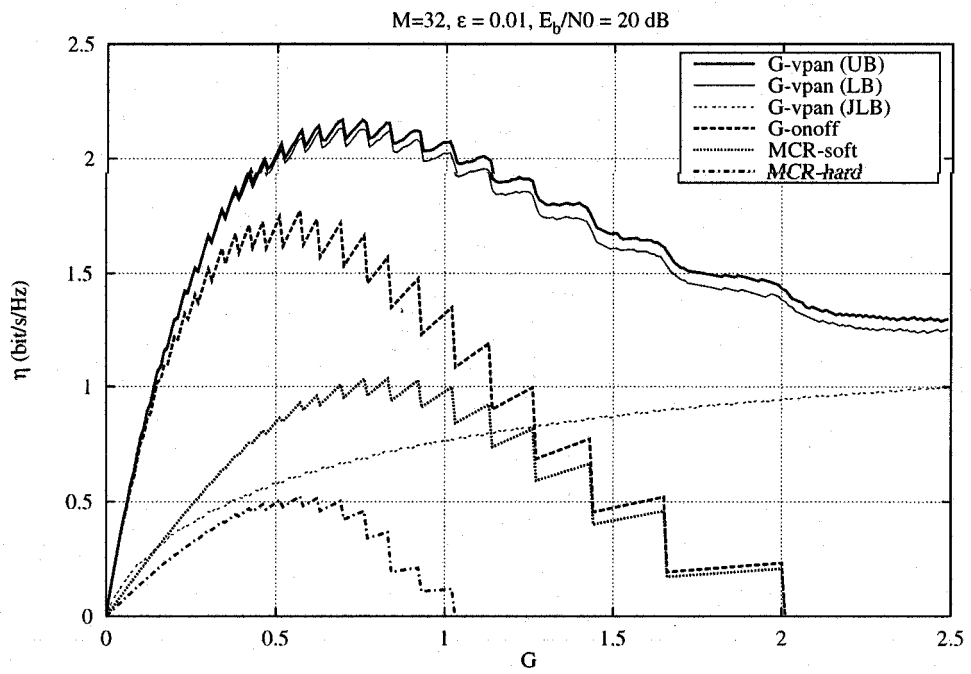

Fig. 12. η versus G for $M = 32$, maximum outage probability $\epsilon = 10^{-2}$, and $E_b/N_0 = 20$ dB.

or MMSE receiver output, respectively. For a given E_b/N_0, the spectral efficiency limit for high channel load (i.e., for $G \to \infty$ or, equivalently, for $\gamma \to 0$) is

$$\lim_{G\to\infty} \eta_{\text{sumf}} = \lim_{G\to\infty} \eta_{\text{mmse}} = \frac{1}{\log 2} - \frac{1}{E_b/N_0}. \qquad (52)$$

Fig. 13 shows the spectral efficiencies $\eta_{\text{G-vpan}}, \eta_{\text{G-onoff}}, \eta_{\text{MCR-soft}}, \eta_{\text{MCR-hard}}, \eta_{\text{orth}}, \eta_{\text{aloha}}, \eta_{\text{sumf}}$, and η_{mmse} versus G for perfect interleaving and $E_b/N_0 = 20$ dB. Fig. 14 shows analogous results for $E_b/N_0 = 30$ dB. $\eta_{\text{MCR-soft}}$ and $\eta_{\text{MCR-hard}}$ have been computed for Z $(16, 4)$.

The spectral efficiency loss of collision-type access with respect to (optimal) orthogonal access is evident. Interestingly,

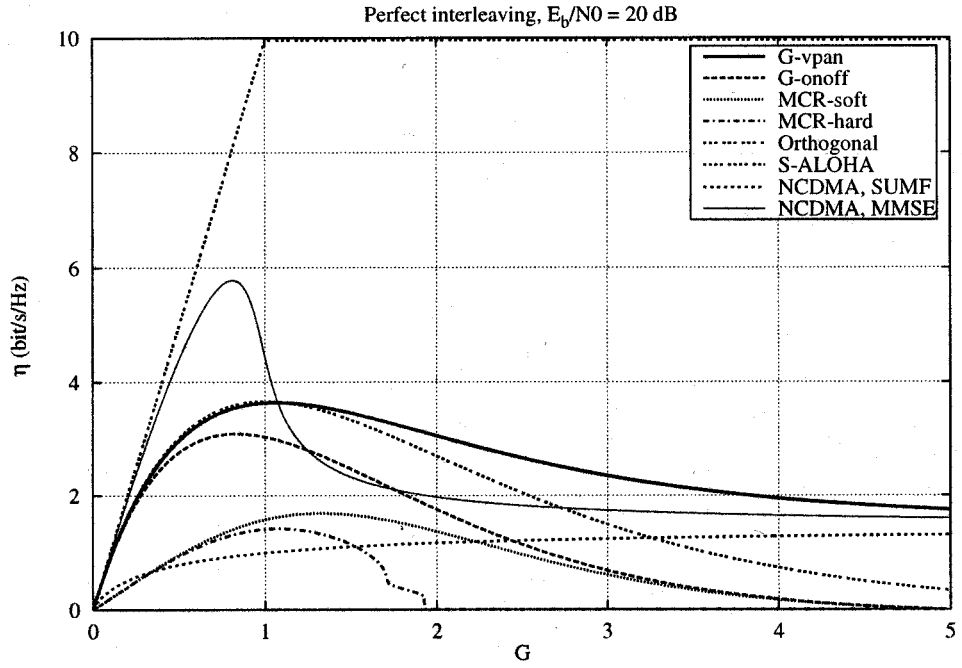

Fig. 13. η versus G for perfect interleaving and $E_b/N_0 = 20$ dB.

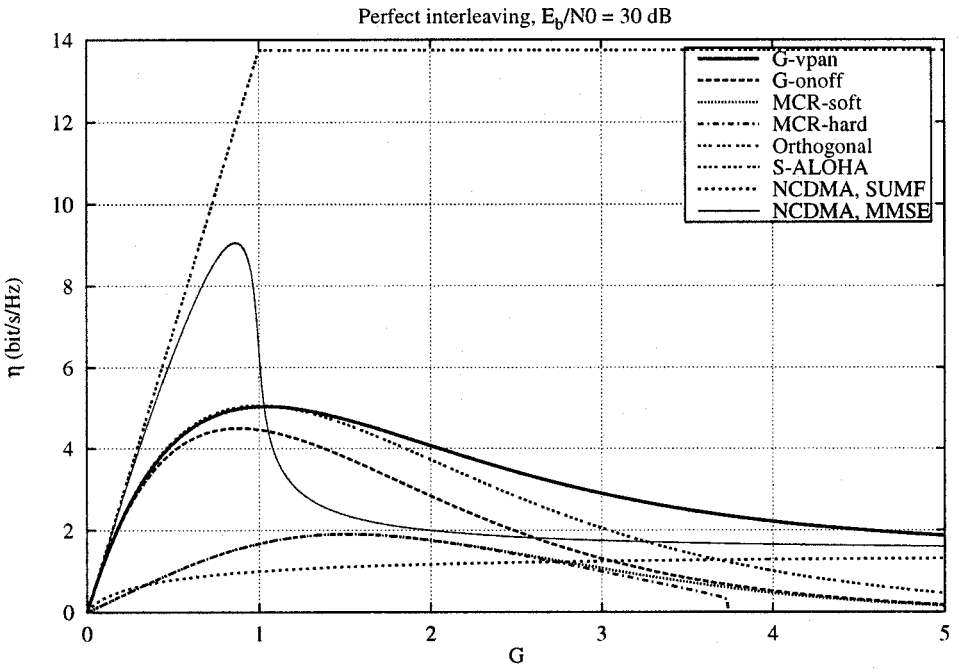

Fig. 14. η versus G for perfect interleaving and $E_b/N_0 = 30$ dB.

S-ALOHA and the VPAN channel with Gaussian inputs have very similar maximum η. As $G \to \infty$, η_{aloha} is vanishing while $\eta_{\text{G-vpan}}$ converges to a positive value. This limit is hard to compute. However, from Jensen's inequality we have that it is lower-bounded by the limit spectral efficiency of NCDMA given in (52). NCDMA with linear an MMSE receiver approaches optimal orthogonal access for $G < 1$, while its performance is close to the SUMF for $G > 1$.

Encoded MCR signals achieve a large fraction of the maximum spectral efficiency achievable with signal sets carrying 1 bit/dim and ideal orthogonal access (about 84% (MRC-soft) and 70% (MRC-hard) for $E_b/N_0 = 20$ dB, and about 98% for both schemes for $E_b/N_0 = 30$ dB). Interestingly, there exists a range of G such that η_{sumf} is below both $\eta_{\text{MCR-soft}}$ and $\eta_{\text{MCR-hard}}$. Then, for sufficiently large interleaving, encoded MCR signals with slotted random access (without

retransmissions) can compete with conventional CDMA with SUMF receiver in terms of spectral efficiency.

VI. Conclusions

In this paper we studied signal-space coding and interleaving for coherent slow frequency-hopped communications over a G-MACC. We characterized signal sets and interleavers having maximum *collision resistance* and we gave some explicit constructions. We analyzed the performance of these signal sets concatenated with outer block coding and hard (error-only) decoding in terms of packet-error probability and spectral efficiency, without assuming perfect interleaving. Computer simulations show perfect agreement with analysis. Our error probability analysis yields some useful intuitions about the structure of good interleavers.

Also, we obtained expressions for the information outage probability and for the achievable (ergodic) rate of the G-MACC under various assumptions on coding and decoding. Outage probability yields the achievable packet-error probability with finite interleaving and large block length. The achievable rate yields the system spectral efficiency for large interleaving depth.

From these results we can conclude that slow frequency-hopped random access with appropriate signal-space coding and interleaving might be a valid alternative to other conventional multiple-access schemes, like S-ALOHA and NCDMA with SUMF receiver. In particular, the spectral efficiency of slow frequency-hopped random access is very similar to that of S-ALOHA, without requiring feedback and retransmission (but at the expenses of a much longer interleaving delay). NCDMA with SUMF is suited for a high channel load with low-rate uniform traffic (its maximum spectral efficiency is achieved for $G \to \infty$). On the contrary, frequency-hopped random access, S-ALOHA, and NCDMA with the MMSE receiver achieve their maximum spectral efficiency for finite G. Hence, these schemes are more suited for lower channel load with high-rate traffic.

We conclude by listing a few topics for further research:

- By comparing the MCR-hard outage probability with the WER of actual RS-encoded MCR signals we see that there is a significant potential coding gain of optimal schemes with respect to bounded-distance error-only decoding, that increases as the interleaving depth gets large. Then, more advanced hard-decoding schemes (e.g., involving errors and erasures) should be considered and the analysis presented in this work should be extended to such schemes.
- By comparing MCR-soft and MCR-hard outage probabilities, we observe the potential gain obtained by soft decoding. In particular, trellis codes [30], suited for soft Viterbi decoding, could be constructed over MCR signal sets.
- Actual wireless channels are affected by time- and frequency-selective fading. Extensions of the results of this work to fading channels would be of great interest. Preliminary results can be found in [38].
- In fading channels the users are not received with the same power. Then, a signal burst may survive to a collision provided that the interference signal is sufficiently faded. This so-called "capture effect" has been investigated for S-ALOHA [39], [40] and should be taken into account in an extension of this work.
- Both the results in terms of WER of actual RS-encoded schemes and in terms of outage probability show that the user code information rate must be optimized depending on the channel load G. Then, adaptive coding schemes which vary the user code rate depending on the channel load should be considered.
- In partially ordered reservation protocols like PRMA [1], users access the channel randomly on the unreserved slots and place reservations in order to transmit a sequence of packets, then release their slots. These protocols are particularly sensitive to collisions in the first slot (the one with random access), since these usually cause an unsuccessful reservation request. Then, adding signal-space redundancy in order to protect this slot might improve the overall protocol performance, as shown in [19]. In general, the joint optimization of partially ordered protocols and signal-space coding is a very interesting problem.

Appendix A
Useful Limits

In this appendix we state two lemmas and a corollary which are extensively used throughout this paper. Because of space limitations and since they are mainly technical, we only sketch the proofs.

Lemma 1: For all $x \in (0,1)$ and $0 \le k \le D$, we have

$$\lim_{M\to\infty} \frac{\binom{xM}{k}\binom{M(1-x)}{D-k}}{\binom{M}{D}} = B(D,k,x). \qquad \square$$

The proof follows by upper and lower bounding the binomial coefficients using Stirling's approximations (see [41, Appendix A.3]).

Lemma 2: Let $f(x_0,\ldots,x_D)$ be a piecewise-continuous function $\mathbb{R}^{D+1} \to \mathbb{R}$. Then, for all $p \in (0,1)$, such that f is continuous in $(B(D,0,p),\ldots,B(D,D,p))$, we have

$$\lim_{M\to\infty} \sum_{c=0}^{M} B(M,c,p) f(P_{M,D}(0|c),\ldots,P_{M,D}(D|c)) = f(B(D,0,p),\ldots,B(D,D,p)). \qquad \square$$

The proof follows by applying Lemma 1 and the Laplace–DeMoivre theorem [29], and by noting that $B(D,k,p)$ is continuous for all $p \in [0,\ 1]$.

Corollary 1: Let $f(x_0,\ldots,x_D)$ be a continuous function $\mathbb{R}^{D+1} \to \mathbb{R}$, let X be a binomial random variable distributed as $P(X=c) = B(M,c,p)$, and define

$$g(X) \triangleq f(P_{M,D}(0|X),\ldots,P_{M,D}(D|X))$$

and

$$\overline{g}(p) \triangleq f(B(D,0,p),\ldots,B(D,D,p)).$$

Then

$$\lim_{M\to\infty} g(X) \stackrel{\mathrm{p}}{=} \overline{g}(p). \qquad \square$$

The proof follows from Chebyshev inequality [29], by showing that

$$\lim_{M\to\infty} E[g(X)] = \overline{g}(p)$$

and that

$$\lim_{M\to\infty} E[|g(X) - \overline{g}(p)|^2] = 0.$$

Both these limits follow from the continuity of f and from Lemma 2.

Appendix B
Achievable Rates

The achievable rates R for a channel with input n-sequence $\boldsymbol{x} \sim q(\boldsymbol{x})$, output $\boldsymbol{y}$, and transition probability $p(\boldsymbol{y}|\boldsymbol{x})$ satisfy [36]

$$R \le \underline{I}(\boldsymbol{x};\boldsymbol{y}) \tag{53}$$

where $\underline{I}(\boldsymbol{x};\boldsymbol{y})$ is the *inf-information rate*, defined as the *liminf in probability* of the normalized *information density* [36]

$$i(\boldsymbol{x};\boldsymbol{y}) = \frac{1}{n}\log_2 \frac{p(\boldsymbol{y}|\boldsymbol{x})}{p(\boldsymbol{y})}. \tag{54}$$

Consider the case where a codesword $\boldsymbol{x} = (\boldsymbol{s}_1,\ldots,\boldsymbol{s}_N)$, with $\boldsymbol{s}_i \in \mathcal{S}$ (a D-dimensional signal set), is transmitted on the G-MACC with an arbitrary deterministic MCR interleaver of depth M slots, and denote by $\boldsymbol{z}_i$ the received D-dimensional channel output corresponding to the transmission of $\boldsymbol{s}_i$, so that $\boldsymbol{y} = (\boldsymbol{z}_i,\ldots,\boldsymbol{z}_N)$. For a fixed collision pattern, let $p_{\boldsymbol{\xi}}(\boldsymbol{z}|\boldsymbol{s})$ denote the transition pdf of the channel with input $\boldsymbol{s}$ and output $\boldsymbol{z}$, where $\boldsymbol{\xi} \in \Xi_D^M$ defines the D slots over which $\boldsymbol{s}$ is transmitted. If the signals $\boldsymbol{s}_i$ are selected i.i.d. over $\mathcal{S}$ according to an arbitrary probability distribution $q(\boldsymbol{s})$, the information density can be written as

$$i(\boldsymbol{x};\boldsymbol{y}) = \sum_{\boldsymbol{\xi}} \in \Xi_D^M \; f_N(\boldsymbol{\xi}) i_{\boldsymbol{\xi}}(\boldsymbol{s}_1,\ldots,\boldsymbol{s}_{N_{\boldsymbol{\xi}}};\boldsymbol{z}_1,\ldots,\boldsymbol{z}_{N_{\boldsymbol{\xi}}}) \tag{55}$$

where $f_N(\boldsymbol{\xi})$ is the fraction of the occurrences of $\boldsymbol{\xi}$ in the interleaver array, where $N_{\boldsymbol{\xi}} = f_N(\boldsymbol{\xi})N$ and where we define

$$i_{\boldsymbol{\xi}}(\boldsymbol{s}_1,\ldots,\boldsymbol{s}_{N_{\boldsymbol{\xi}}}\boldsymbol{z}_1,\ldots,\boldsymbol{z}_{N_{\boldsymbol{\xi}}}) \triangleq \frac{1}{DN_{\boldsymbol{\xi}}}\sum_{i=1}^{N_{\boldsymbol{\xi}}}\log_2\frac{p_{\boldsymbol{\xi}}(\boldsymbol{z}_i|\boldsymbol{s}_i)}{\sum_{\boldsymbol{s}'\in\mathcal{S}} p_{\boldsymbol{\xi}}(\boldsymbol{z}_i|\boldsymbol{s}')q(\boldsymbol{s}')}.$$

For all $f_N(\boldsymbol{\xi}) > 0$, from the *Weak Law of Large Numbers* [29], as $N \to \infty$

$$i_{\boldsymbol{\xi}}(\boldsymbol{s}_1,\ldots,\boldsymbol{s}_{N_{\boldsymbol{\xi}}}\boldsymbol{z}_1,\ldots,\boldsymbol{z}_{N_{\boldsymbol{\xi}}}) \stackrel{\mathrm{p}}{\to} E\left[\frac{1}{D}\log_2\frac{p_{\boldsymbol{\xi}}(\boldsymbol{z}|\boldsymbol{s})}{\sum_{\boldsymbol{s}'\in\mathcal{S}} p_{\boldsymbol{\xi}}(\boldsymbol{z}|\boldsymbol{s}')q(\boldsymbol{s}')}\right] \triangleq I_{\boldsymbol{\xi}}(\boldsymbol{s};\boldsymbol{z}). \tag{56}$$

We define the *instantaneous mutual information* I_M as the limit in probability as $N \to \infty$ of the information density for given collision pattern and M. From Fact 1 in Section III, (55), and (56) we obtain

$$I_M = \frac{1}{D!\binom{M}{D}}\sum_{\boldsymbol{\xi}\in\Xi_D^M} I_{\boldsymbol{\xi}}(\boldsymbol{s};\boldsymbol{z}). \tag{57}$$

The achievable ergodic rate I_∞ is obtained as the limit in probability (if it exists) of I_M as $M \to \infty$.

Appendix C
Proofs

Proof of (36) and (38): In this case, $D = 1$ and $\mathcal{S} = \mathbb{R}$. With the channel model (3), the collision pattern is defined by the $(K_1,\ldots,K_M)$, where K_ξ is the number of interferers in slot $\xi = 1,\ldots,M$. We have $p_\xi(z|s) = \mathcal{N}(s, K_\xi\mathcal{E} + N_0/2)$, so that

$$I_\xi(s;z) = \frac{1}{2}\log_2\left(1 + \frac{\mathcal{E}}{K_\xi\mathcal{E} + N_0/2}\right). \tag{58}$$

Then (36) follows immediately. Since the K_ξ's are i.i.d. Poisson-distributed with mean G, we have

$$\lim_{M\to\infty} I_M \stackrel{\mathrm{p}}{=} E[I_1]$$

and (38) follows.

Proof of (39) and (41): Again, $D = 1$ and $\mathcal{S} = \mathbb{R}$. With the channel model (4), the collision pattern is defined by the $(\alpha_1,\ldots,\alpha_M)$, where $\alpha_\xi = 0$ if slot $\xi = 1,\ldots,M$ is collided and $\alpha_\xi = 1$ if it is not. We have $p_\xi(z|s) = \mathcal{N}(\alpha_\xi s, N_0/2)$, so that

$$I_\xi(s;z) = \frac{\alpha_\xi}{2}\log_2(1 + 2\mathcal{E}/N_0). \tag{59}$$

Then (39) follows immediately. Since the α_ξ's are i.i.d. Bernoulli-distributed with mean P_{col}, we have

$$\lim_{M\to\infty} I_M \stackrel{\mathrm{p}}{=} E[I_1]$$

and (41) follows.

Proof of (42), (44), (46), and (47): In this case, $\mathcal{S}$ is an MCR D-dimensional signal set. The channel transition pdfs are D-variate Gaussian

$$p_{\boldsymbol{\xi}}(\boldsymbol{z}|\boldsymbol{s}) = \prod_{j=1}^{D}\mathcal{N}(\alpha_{\xi_j}s_j, N_0/2) \tag{60}$$

where $\boldsymbol{\xi} = (\xi_1,\ldots,\xi_D) \in \Xi_D^M$. For $\boldsymbol{s}$ uniform over $\mathcal{S}$, we have

$$I_{\boldsymbol{\xi}}(\boldsymbol{s};\boldsymbol{z}) = \frac{1}{D}\left\{\log_2|\mathcal{S}| - E_{\boldsymbol{s},\boldsymbol{n}}\left[\log_2\left(\sum_{\boldsymbol{s}'\in\mathcal{S}} \cdot\exp\left(\frac{\alpha_{\xi_j}}{N_0}\sum_{j=1}^{D}(2\sqrt{\mathcal{E}}(s_j' - s_j)n_j - \mathcal{E}|s_j' - s_j|^2)\right)\right)\right]\right\}. \tag{61}$$

By summing over all $\boldsymbol{\xi} \in \Xi_D^M$ and dividing by $D!\binom{M}{D}$ we immediately obtain (42). The convergence in probability of I_M to I_∞ given in (44) follows immediately from Corollary 1 of Appendix A, since I_M is a continuous (linear) function of the probabilities $P_{M,D}(k|c)$ for $k = 0,\ldots,D$.

The proof of (46) and of (47) follows the same path as that of (42) and (44), provided that we use the symmetric DMC transition probabilities (45) instead of the transition pdf (60).

APPENDIX D
MUTUAL INFORMATION WITHOUT CSI

In this section we prove the claim made in Section V that I_M and I_∞ given in (46) and in (47) are obtained also if the decoder ignores the number of collided components k for each transmitted D-dimensional signal.

Let L_ϕ denote the number of signals transmitted over the slots indexed by $\phi \in \Phi_D^M$. Clearly, for each RMCR interleaver and block length N we have $\sum_{\phi\in\Phi_D^M} L_\phi = N$. Given a collision pattern $\boldsymbol{\alpha}$ of weight $W(\boldsymbol{\alpha}) = M - c$, all the signals suffering from k collisions are transmitted over a DMC with transition probability given by (45).

The decoder is not allowed to use this information for decoding (no CSI). However, it can group the L_ϕ signals corresponding to the ϕ and use the fact that all the signals belonging to the same group have the same (unknown) number of collided components. Because of this grouping, a codesword can be seen as a sequence of *super-symbols* of dimension DL_ϕ, for $\phi \in \Phi_D^M$. Each super-symbol is transmitted over the *super-channel* obtained by the L_ϕth extension of the original DMC.

For simplicity, we let $q_k = \overline{P}(e|k)$ and $p_k = q_k/(|\mathcal{S}|-1)$. Since the DMCs treated here are symmetric, we identify their channel transition probability matrix by its first row (the other rows are permutations of the first). Then, the transition probability of the DMC defined by (45) has first row

$$\boldsymbol{p}_k = (1-q_k, \underbrace{p_k, \ldots, p_k}_{|S|-1 \text{ times}})$$

The first row of the transition probability matrix of the Lth extension of this DMC is given by the L-fold Kronecker product of $\boldsymbol{p}_k$ by itself, denoted by $\boldsymbol{p}_k^{\otimes L}$. With no knowledge of k at the decoder, the super-channel transition probability is a mixture of the possible transition probabilities for $k = 0, \ldots, D$, where the mixing is with respect to the conditional distribution of k given c, i.e., with respect to $P_{M,D}(k|c)$ given in (18). The resulting transition probability of the ϕth super-channel is given by

$$\boldsymbol{p}^{(L_\phi)} \triangleq \sum_{k=0}^{D} \boldsymbol{p}_k^{\otimes L_\phi} P_{M,D}(k|c). \tag{62}$$

From Fact 1, with RMCR interleaving $L_\phi/N \overset{\text{a.e.}}{\to} 1/\binom{M}{D}$ as $N \to \infty$, for all ϕ. Then, the transition probabilities (62) are asymptotically equal. By letting $L = N/\binom{M}{D}$ and $\boldsymbol{p}^{(L)}$ denoting this common transition probability, we obtain

$$I_M = \frac{1}{D}\left\{\log_2|\mathcal{S}| - \lim_{L\to\infty}\frac{1}{L}\mathcal{H}(\boldsymbol{p}^{(L)})\right\}. \tag{63}$$

After some algebra, by applying the Laplace–DeMoivre theorem [29], we can write

$$\begin{aligned}\lim_{L\to\infty}\frac{1}{L}H(\boldsymbol{p}^{(L)}) &= \overline{P}(e|c)\log_2(|\mathcal{S}|-1) + \lim_{L\to\infty}\sum_{k=0}^{D} P_{M,D}(k|c)\log_2 \\ &\quad\cdot\left[\sum_{k'=0}^{D}(q_{k'}^{q_k}(1-q_{k'})^{1-q_k})^L P_{M,D}(k'|c)\right]^{1/L}. \end{aligned}\tag{64}$$

The above limit can be computed by noting that for all $k' \neq k$

$$q_{k'}^{q_k}(1-q_{k'})^{1-q_k} \le q_k^{q_k}(1-q_k)^{1-q_k}$$

since the relative entropy $D((1-q_k, q_k)||(1-q_{k'}, q_{k'}))$ is nonnegative [1]. Then, for each k, the term with $k' = k$ exponentially dominates the sum inside the logarithm in (64). We obtain

$$\lim_{L\to\infty}\frac{1}{L}H(\boldsymbol{p}^{(L)}) = \overline{P}(e|c)\log_2(|\mathcal{S}|-1) + \sum_{k=0}^{D} P_{M,D}(k|c)\mathcal{H}(q_k).$$

By using the above result in (63) we obtain (46). Consequently, also (47) can be achieved without CSI.

REFERENCES

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

[2] A. Wyner, "Shannontheoretic approach to a Gaussian cellular multiple access channel," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1713–1727, Nov. 1994.

[3] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Trans. Inform. Theory*, vol. 42, pp. 364–375, Mar. 1996.

[4] N. Abramson, "THE ALOHA SYSTEM—Another alternative for computer communications," in *AFIPS Conf. Proc., 1970 Fall Joint Computer Conf.*, vol. 37, 1970, pp. 281–285.

[5] L. Kleinrock and S. Lam, "Packet switching in a multiaccess broadcast channel: Performance evaluation," *IEEE Trans. Commun.*, vol. COM-23, pp. 410–423, Apr. 1975.

[6] E. Lutz, "Slotted ALOHA multiple access and error control coding for the land mobile satellite networks," *Int. J. Satellite Commun.*, vol. 10, pp. 275–281, 1992.

[7] J. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.

[8] A. Viterbi, *CDMA—Principles of Spread Spectrum Communications*. Reading, MA: Addison-Wesley, 1995.

[9] R. Lupas and S. Verdú, "Linear multiuser detectors for synchronous code-division multiple access," *IEEE Trans. Inform. Theory*, vol. 35, pp. 123–136, Jan. 1989.

[10] U. Madhow and M. Honig, "MMSE interference suppression for direct-sequence spread-spectrum CDMA," *IEEE Trans. Commun.*, vol. 42, pp. 3178–3188, Dec. 1994.

[11] S. Verdú and S. Shamai (Shitz), "Spectral efficiency of CDMA with random spreading," *IEEE Trans. on Imform. Theory*, vol. 45, pp. 622–640, Mar. 1999.

[12] D. Tse and S. Hanly, "Linear multiuser receivers: Effective interference, effective bandwidth and capacity," *IEEE Trans. Inform. Theory*, vol. 45, pp. 641–657, Mar. 1999.

[13] M. Pursley, "Frequency-hop transmission for satellite packet switching and terrestrial packet radio networks," *IEEE Trans. Imform. Theory*, vol. IT-32, pp. 652–667, Sept. 1986.

[14] S. Kim and W. Stark, "Optimum rate Reed-Solomon codes for frequency-hopped spread-spectrum multiple-access communication systems," *IEEE Trans. Commun.*, vol. 37, pp. 138–144, Feb. 1989.

[15] A. Grant and C. Schlegel, "Collision-type multiple-user communications," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1725–1735, Sept. 1997.

[16] J. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 192–206, Mar. 1985.

[17] D. Goodman, R. Valenzuela, K. Gayliard, and B. Ramamurthi, "Packet reservation multiple access for local wireless communications," *IEEE Trans. Commun.*, vol. 37, pp. 885–890, Aug. 1989.

[18] S. Nanda, D. Goodman, and U. Timor, "Performance of PRMA: A packet voice protocol for cellular systems," *IEEE Trans. Vehic. Technol.*, vol. 40, pp. 585–598, Aug. 1991.

[19] G. Caire, E. Leonardi, and E. Viterbo, "Improving performance of wireless networks using collision resistant modulations," in *Proc. Globecom '98*, Sidney, Australia, Nov. 8–12, 1998.

[20] R. McEliece and W. Stark, "Channels with block interference," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 44–53, Jan. 1984.

[21] L. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Vehic. Technol.*, vol. 43, pp. 359–378, May 1994.
[22] G. Kaplan and S. Shamai (Shitz), "Error probabilities for the block-fading Gaussian channel," *Arch. lrktr. Übertragung*, vol. 49, no. 4, pp. 192–205, 1995.
[23] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channel," *IEEE Trans. Inform. Theory*, vol. 42, pp. 502–518, Mar. 1996.
[24] J. Boutros and E. Viterbo, "Signal space diversity: A power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1453–1467, July 1998.
[25] E. Wong and T.-S. Yum, "The optimal multicopy ALOHA," *IEEE Trans. Automat. Contr.*, vol. 39, pp. 1233–1236, June 1994.
[26] Y. Leung, "Generalized multicopy ALOHA," *IEE Electron. Lett.*, vol. 31, no. 2, pp. 82–83, Jan. 1995.
[27] G. Clark and J. Cain, *Error-Correction Coding for Digital Communications*. New York: Plenum, 1981.
[28] M. Varanasi and T. Guess, "Bandwidth-efficient multiple-access via signal design for decision-feedback receivers: Toward and optimal spreading-coding trade-off," in *Proc. Globecom '97, Communication Theory Mini-Conf.*, Phoenix, AZ, Nov. 3–8, 1997.
[29] P. Billingsley, *Probability and Measure*. New York: Wiley, 1986.
[30] D. Forney Jr. and M. Trott, "The dynamics of linear codes over groups: State spaces, trellis diagram and canonical encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1491–1514, Sept. 1993.
[31] T. Rappaport, *Wireless Communications*. Englewood Cliffs, NJ: Prentice-Hall, 1996.
[32] D. Forney, Jr., "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, Sept. 1991.
[33] M. Graferath and E. Viterbo, "Algebraic construction of good collision resistant signal sets," in *Proc. Workshop on Coding and Cryptography*, Paris, France, Jan. 1999, pp. 213–224.
[34] G. Caire and E. Biglieri, "Linear block codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1246–1256, Sept. 1995.
[35] M. Chiani, "Error probability for block codes with block interference," in *Proc. ICC '96*, London, UK, Nov. 1996, pp. 97–100.
[36] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1147–1157, July 1994.
[37] G. Caire, R. Knopp, and P. Humblet, "System capacity of F-TDMA cellular systems," *IEEE Trans. Commun.*, vol. 46, pp. 1649–1661, Dec. 1998.
[38] G. Caire, E. Leonardi, and E. Viterbo, "Collision resistant modulation," in *Proc. ICT '98*, Porto Carrras, Greece, June 22–25, 1998.
[39] I. Habbab, M. Kaverhad, and C.-E. Sundberg, "ALOHA with capture over slow and fast fading radio channels with coding and divesity," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 79–88, Jan. 1989.
[40] J. Arnbak and W. van Blitterswjik, "Capacity of slotted ALOHA in Rayleigh-fading channels," *IEEE J. Select. Areas Commun.*, vol. 5, pp. 261–269, Feb. 1987.
[41] S. Roman, *Coding and Information Theory*. New York: Springer-Verlag, 1992.