

On the Limitation of Generalized Welch-Bound Equality Signals

Ateet Kapur, *Member, IEEE*,
Mahesh K. Varanasi, *Senior Member, IEEE*, and
Clifford T. Mullis

Abstract—This correspondence characterizes the performance limitation of the well-acclaimed generalized Welch-bound equality (WBE) signals under linear minimum mean-squared error (MMSE) detection. It is analytically proven, and experimentally verified, that when users in an overloaded but finite-size code-division multiple-access (CDMA) system are allocated such signals, the error rate of *at least one* user “floors” (i.e., it cannot be driven to zero even in the absence of additive noise), independently of the symbol energies. If, in addition, all users are received with equal energy, then the error rate of *every* user “floors.”

Index Terms—Code-division multiple access (CDMA), generalized Welch-bound equality (WBE) signals, multiuser detection, overloaded system.

I. INTRODUCTION

This correspondence is concerned with characterizing the effect of the interference limitation of linear minimum mean-squared error (MMSE) detection on the performance of overloaded code-division multiple-access (CDMA) systems when users are allocated the so-called generalized Welch-bound equality (WBE) signals. We consider the complex baseband model for the synchronous K -user CDMA channel with processing gain N which is given as

$$\mathbf{r} = \sum_{k=1}^K A_k b_k \mathbf{s}_k + \mathbf{n} \quad (1)$$

where A_k , b_k , and \mathbf{s}_k denote, respectively, the (complex) received amplitude, data, and spreading sequence (or simply signal) of user k . The vector \mathbf{n} denotes additive complex Gaussian noise and has distribution $\mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_N)$ with \mathbf{I}_N denoting the N -dimensional identity matrix. Without loss of generality, we normalize the data to have unit average energy and the signals to have unit norm. For simplicity, we assume that the b_k 's are drawn from a common modulation alphabet for all users but our results extend to distinct alphabets as well.

We focus on overloaded CDMA systems, i.e., when $K > N$, and on the case where the signals $\mathbf{s}_1, \dots, \mathbf{s}_K$ form a generalized WBE signal set. Overloaded CDMA systems are of particular interest when bandwidth is at a premium (recall that N is proportional to Shannon bandwidth), and they are nontrivial in the sense that orthogonal signals cannot be allocated to all users. Generalized WBE signals, on the other hand, are an attractive signal allocation in such systems. They are characterized mathematically (see, e.g., [1]) by properties of the

$N \times K$ signal matrix $\mathbf{S} = [\mathbf{s}_1, \dots, \mathbf{s}_K]$. First, users are partitioned in two groups as a function of the energy disparity and the processing gain. Specifically, user k is said to be *oversized* if

$$\left(N - \sum_{j=1}^K 1_{\{E_j \geq E_k\}} \right) E_k > \sum_{j=1}^K E_j 1_{\{E_k > E_j\}}$$

and *nonoversized* otherwise. If users are indexed in decreasing order of energy, and if \mathcal{O} and \mathcal{O}^c denote the subsets of oversized and nonoversized users, respectively, the signal matrix has the form

$$\mathbf{S} = \begin{bmatrix} \mathbf{I}_{|\mathcal{O}|} & \mathbf{0} \\ \mathbf{0} & \mathbf{S}_{\mathcal{O}^c} \end{bmatrix}. \quad (2)$$

Oversized users are allocated orthogonal signals. The submatrix $\mathbf{S}_{\mathcal{O}^c}$, of dimensions $(N - |\mathcal{O}|) \times |\mathcal{O}^c|$, represents the signals of nonoversized users and satisfies the following WBE-like property (see, e.g., [2]):

$$\mathbf{S}_{\mathcal{O}^c} \mathbf{E}_{\mathcal{O}^c} \mathbf{S}_{\mathcal{O}^c}^H = \mathbf{E}_{\mathcal{O}^c} \mathbf{I}_{N-|\mathcal{O}|} \quad (3)$$

where

$$\begin{aligned} \mathbf{E}_{\mathcal{O}^c} &= \text{diag}\{E_k, k \in \mathcal{O}^c\} \\ E_{\mathcal{O}^c} &= \sum_{k \in \mathcal{O}^c} E_k / (N - |\mathcal{O}|) \end{aligned}$$

and H stands for Hermitian transpose. For a given system triplet (N, K, \mathbf{E}) where $\mathbf{E} = \text{diag}\{E_k, k = 1, \dots, K\}$, we denote the ensemble of matrices that represents generalized WBE signals by $\mathcal{W}(N, K, \mathbf{E})$. In the equal-energy case, there are no oversized users and hence the matrix characterization reduces to $\mathbf{S} \mathbf{S}^H = (K/N) \mathbf{I}_N$. We denote the corresponding ensemble of matrices by $\mathcal{W}(N, K)$.

The main appeal of generalized WBE signals is their host of optimality properties in overloaded CDMA systems. They maximize sum capacity for arbitrary received energies [1], and simultaneously maximize symmetric capacity if the energies are equal [2]. Generalized WBE signals also minimize the total power with respect to the joint signal design and power control problem under quality of service (QoS) constraints [3]. We emphasize that these properties require that the receiver employs *nonlinear* detection (joint maximum likelihood, or successive cancellation with MMSE filtering as in [3]). By contrast, generalized WBE signals have also been investigated under *linear* MMSE detection. In particular, [4], [5] prove for different channel models that they solve the same QoS-based problem as in [3], with the difference that the receiver employs linear MMSE detection. Practical issues regarding their implementation under linear detection have been studied in [6]–[9].

Linear MMSE detection has an attractive user-separating structure (a bank of linear MMSE filters, followed by single-user decision rules), and is arguably the best practical detector among linear detectors ([10, Sec. 6.2]). Linearity, however, can be too limiting if one is to efficiently cope with high interference such as arises in overloaded systems. Specifically, users that are allocated signals that linearly depend on the interfering signals experience irreducible multiple-access interference (MAI) (in the limit of low noise). The effects of this interference limitation have been observed before. In [4], it is shown that in order for users to achieve certain signal-to-interference ratio (SIR) guarantees, the corresponding sum of effective bandwidths has to be less than the processing gain. Otherwise, the SIR requirements are inadmissible (no matter what powers are allocated). By contrast, when the receiver employs successive cancellation with MMSE filtering, every set of SIR requirements is admissible, and the power and signal allocation that minimize the total power are specified in [3]. In either case (MMSE detector with or without successive cancellation), generalized WBE signals are optimal. When the SIR requirements are admissible

Manuscript received December 19, 2003; revised November 22, 2004. This work was supported in part by the National Science Foundation under Grant CCR-0112977. The material in this correspondence was presented in part at the 38th Conference on Information Sciences and Systems, Princeton, NJ, March 2004.

A. Kapur was with the Department of Electrical Engineering, University of Colorado, Boulder, CO 80309 USA. He is now with the Communication Theory Group, Swiss Federal Institute of Technology (ETH) CH-8092 Zurich, Switzerland (e-mail: ateet@ee.ethz.ch).

M. K. Varanasi and C. T. Mullis are with the Department of Electrical Engineering, University of Colorado, Boulder, CO 80309-0425 USA (e-mail: varanasi@schof.colorado.edu; mullis@schof.colorado.edu).

Communicated by X. Wang, Associate Editor for Detection and Estimation. Digital Object Identifier 10.1109/TIT.2005.847695

under linear MMSE detection, the MMSE detector with successive cancellation requires a smaller total power than its counterpart without successive cancellation. Moreover, a large systems analysis (i.e., as K and $N \rightarrow \infty$ with the load factor K/N fixed) shows that the spectral efficiency of linear MMSE detection (and in fact of any linear detection) is severely limited in overloaded systems compared to nonlinear detection [11], [12].

In this correspondence, we analyze the joint error rate of the symbol-by-symbol linear MMSE detector in an overloaded CDMA system that uses generalized WBE signals, and show that it cannot be driven to zero with decreasing noise power, irrespectively of what the user powers are. Consequently, at least one user's symbol error probability floors. This result is not to be confused with the fact that the symbol error probability of the decorrelating detector of at least one user (with a linearly dependent signal) floors because the linear MMSE detector does *not* converge to the decorrelator for a linearly dependent user [13]. Note also that our result is stronger than saying that at least one (linearly dependent) user will have zero near-far resistance [10].

II. MAIN RESULT

Uncoded error rate has received much attention as a performance measure of multiuser detection. It is not tractable in general, but it is characterized in the low-noise limit by the asymptotic effective energy (AEE). The AEE for a user (denoted by e_k for user k) is defined in [14] as the energy required by the (optimum) matched-filter detector in a single-user channel to achieve in the low-noise regime the same error rate as the multiuser detector in the multiuser channel. The AEE is identically equal to zero if and only if the user's error rate floors. Similarly, the joint error rate (JER) is characterized asymptotically by the symmetric energy (denoted by e or $e(\mathbf{S})$ for the signal matrix \mathbf{S}), which is equal to the smallest AEE [14]. The symmetric energy is identically equal to zero if and only if the JER floors, i.e., the error rate of at least one user floors.

The AEE under linear MMSE detection depends on the signal space geometry as shown in [13]. It is equal to the AEE under decorrelation (defined as a detector that projects out the MAI) *if and only if* the desired signal is linearly independent of the interfering signals, and *otherwise* to the AEE under pseudodecorrelation, which only partially cancels the MAI. Specifically, a user experiences irreducible MAI in the linearly dependent case, even asymptotically (in particular, linear MMSE detection is not near-far resistant). This irreducible MAI does not necessarily translate, however, into a JER floor in general. Our main result characterizes its effect on the JER for the case when users are allocated generalized WBE signals.

Theorem 1: For any number of users, processing gain (with $N < K$), energies, and modulation size, generalized WBE signals have a symmetric energy under linear MMSE detection that is identically equal to zero. Specifically

$$\forall \mathbf{S} \in \mathcal{W}(N, K, \mathbf{E}), \quad \begin{cases} e_k = E_k, & \forall k \in \mathcal{O} \\ e(\mathbf{S}_{\mathcal{O}^c}) = 0. \end{cases}$$

In other words, no matter how the received energies are distributed, there is always *at least* one user whose error rate does not decay with vanishing noise. In particular, even power control, usually considered to be an effective interference-mitigation technique, cannot overcome the limitations of generalized WBE signals under linear MMSE detection. The result is in fact stronger in the equal-energy case.

Corollary 1: For any number of users, processing gain (with $N < K$), modulation size, and when the received energies are equal,

WBE signals yield an AEE that is identically equal to zero for all users.

III. PROOF

The proof uses the following “minimum eigenvalue” property of generalized WBE signals.

Proposition 1: Let $\mathbf{S} \in \mathcal{W}(N, K, \mathbf{E})$. For any $k = 1, \dots, K$, the k th column of \mathbf{S} is an eigenvector of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$ associated with the smallest eigenvalue, where \mathbf{S}_k is formed by deleting the k th column of \mathbf{S} and \mathbf{E}_k by deleting the k th column and row of \mathbf{E} .

Proof: The proof is in two steps. We first show that \mathbf{s}_k is an eigenvector of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$, $\forall k$, and then that it corresponds to the minimum eigenvalue.

From the characterization of generalized WBE signals in (2) and (3), it follows that the rows of the amplitude-scaled matrix $\mathbf{S} \mathbf{E}^{1/2}$ are mutually orthogonal. In addition, the n th row has norm equal to E_n if $n \in \mathcal{O}$ and to $E_{\mathcal{O}^c}$ otherwise. In other words, the outer product $\mathbf{S} \mathbf{E} \mathbf{S}^H$ is diagonal equal to $\mathbf{D} = \text{diag}\{E_1, \dots, E_{|\mathcal{O}|}, E_{\mathcal{O}^c}, \dots, E_{\mathcal{O}^c}\}$. Consequently, we have that

$$\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H + E_k \mathbf{s}_k \mathbf{s}_k = \mathbf{D}, \quad \forall k \quad (4)$$

and, therefore, that $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H \mathbf{s}_k = (\mathbf{D} - E_k \mathbf{I}_N) \mathbf{s}_k$. We now distinguish two cases. If user k is oversized, then clearly $(\mathbf{D} - E_k \mathbf{I}_N) \mathbf{s}_k = \mathbf{0}$ and the minimum eigenvalue property trivially holds. If user k is nonoversized, it is easily verified from (2) and (3) that $\mathbf{D} \mathbf{s}_k = E_{\mathcal{O}^c} \mathbf{s}_k$ and hence, that $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H \mathbf{s}_k = (E_{\mathcal{O}^c} - E_k) \mathbf{s}_k$. Therefore, \mathbf{s}_k is an eigenvector of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$ in this case as well.

To show that the corresponding eigenvalue is the smallest one, we completely characterize the spectrum of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$. Let $\mathbf{U} \mathbf{\Lambda}_k \mathbf{U}^H$ be the spectral decomposition of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$. Combining (4) with the result that \mathbf{s}_k is an eigenvector, i.e., $\mathbf{s}_k = \mathbf{U} \mathbf{e}$, where \mathbf{e} is a unit vector of dimension $N \times 1$, we have that $\mathbf{U} (\mathbf{\Lambda}_k + E_k \mathbf{e} \mathbf{e}^T) \mathbf{U}^H = \mathbf{D}$. Consequently, the eigenvalues of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$ are exactly the diagonal elements of \mathbf{D} , except for the eigenvalue associated with \mathbf{s}_k . This eigenvalue is equal to zero if $k \in \mathcal{O}$ (as noted earlier), and to $E_{\mathcal{O}^c} - E_k$ if $k \in \mathcal{O}^c$. In either case, it is obviously the smallest eigenvalue of $\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H$. Hence the result. \square

Next, we make two simplifying observations. Recall that the MMSE filter of any user, say user k , is given by $(\mathbf{S}_k \mathbf{E}_k \mathbf{S}_k^H + \sigma^2 \mathbf{I}_N)^{-1} \mathbf{s}_k$. From the “minimum eigenvalue” property, it is clear that this filter is equal to \mathbf{s}_k up to a multiplicative constant. Therefore, this fundamental property gives a more direct proof than in [4] of the following result.

Corollary 2: Linear MMSE detection collapses to matched-filter detection when $\mathbf{S} \in \mathcal{W}(N, K, \mathbf{E})$.

In particular, the two detectors have equal AEE. Second, we note that to prove our main result for an arbitrary modulation, we only need to consider the modulation with the largest minimum distance, i.e., quaternary phase-shift keying (QPSK) (binary phase-shift keying (BPSK)) for complex-valued (real-valued) modulations. Indeed, the symmetric energy for these modulations is an upper bound for any other modulation. Given these two simplifications, the AEE of any user is given as

$$\text{if } k \in \mathcal{O}, \quad e_k = E_k \quad (5)$$

¹Note the symmetry of the interference space for each user. In particular, the strength of the interference along the principal directions is the same for all nonoversized users. This symmetry in turn ensures a form of interference avoidance whereby each signal lies in the direction of least interference (see also [8]). It is therefore not surprising that generalized WBE signals minimize the total squared correlation (see [15]).

$$\text{if } k \in \mathcal{O}^c, \quad e_k = E_k \left[1 - E_k^{-1} \sum_{l \neq k} |R_{lk}| \right]_+^2 \quad (6)$$

where $\mathbf{R} = (\mathbf{S}\mathbf{A})^H \mathbf{S}\mathbf{A}$ is the weighted correlation matrix and $[a]_+ = \max(0, a)$. Equation (5) follows because oversized users are allocated orthogonal signals, and (6) is a direct application of ([10, Sec. 3.5]).

Let us first assume that there are no oversized users (i.e., $\sum_k E_k > N \max_k E_k$), and without loss of generality that $\sum_k E_k = K$. Consequently, the signal matrix satisfies $\mathbf{S}\mathbf{E}\mathbf{S}^H = (K/N)\mathbf{I}_N$, and every user's AEE is given as in (6). Proving that the symmetric energy is identically equal to zero is then equivalent to finding at least one index k for which $E_k^{-1} \sum_{l \neq k} |R_{lk}|$ is greater than one, i.e., the so-called closed-eye condition ([10, Sec. 3.5]). We prove that this inequality holds for the user with minimum energy (whose index we denote ν).

Recall that the matrix $\mathbf{S}\mathbf{A}$ has rows that are orthogonal and have equal norm (equal to K/N). These rows form an incomplete orthogonal set of vectors in \mathbb{C}^K . We complete them into an orthonormal basis of \mathbb{C}^K by scaling $\mathbf{S}\mathbf{A}$ with $\sqrt{N/K}$ and by solving for the "missing" rows. For the purpose of the proof, we write these "missing" rows as a scaled product of matrices. Specifically, let $\tilde{\mathbf{S}}\tilde{\mathbf{A}}$ be the $(K-N) \times K$ matrix such that

$$\mathbf{U}^T = \left[\sqrt{\frac{N}{K}} (\mathbf{S}\mathbf{A})^T, \sqrt{\frac{K-N}{K}} (\tilde{\mathbf{S}}\tilde{\mathbf{A}})^T \right]$$

is unitary (T denotes the transpose), that $\tilde{\mathbf{S}}$ is a $(K-N) \times K$ matrix with unit-norm columns, and that $\tilde{\mathbf{A}}$ is diagonal, positive definite.

Next, we show a key property of generalized WBE signals. Namely, if we interpret $\tilde{\mathbf{S}}$ and $\tilde{\mathbf{A}}$ as the signal and amplitude matrices of a fictitious overloaded CDMA system with K users and processing gain $K-N$, then $\tilde{\mathbf{S}}$ represents a generalized WBE signal set with respect to the system triplet $(K-N, K, \tilde{\mathbf{E}})$, where $\tilde{\mathbf{E}}$ denotes the diagonal energy matrix, i.e., $\tilde{\mathbf{E}} = \tilde{\mathbf{A}}^2$. Indeed, since \mathbf{U} is unitary, it follows that $\mathbf{I}_K = \mathbf{U}^H \mathbf{U}$, and hence that the Gramian $\tilde{\mathbf{R}} = (\tilde{\mathbf{S}}\tilde{\mathbf{A}})^H (\tilde{\mathbf{S}}\tilde{\mathbf{A}})$ is

$$\tilde{\mathbf{R}} = \frac{K}{K-N} \mathbf{I}_K - \frac{N}{K-N} \mathbf{R}. \quad (7)$$

Clearly, (7) uniquely specifies $\tilde{\mathbf{E}}$ and $\tilde{\mathbf{A}}$ from the diagonal elements of $\tilde{\mathbf{R}}$. Since $\mathbf{I}_K = \mathbf{U}\mathbf{U}^H$ also holds, it follows that the outer product matrix $(\tilde{\mathbf{S}}\tilde{\mathbf{A}})(\tilde{\mathbf{S}}\tilde{\mathbf{A}})^H$ is equal to $K/(K-N)\mathbf{I}_{K-N}$ and hence, that $\tilde{\mathbf{S}} \in \mathcal{W}(K-N, K, \tilde{\mathbf{E}})$. In fact, it is easy to verify that any set of L orthogonal vectors in \mathbb{C}^K where $L \leq K$, forms a generalized WBE signal set by suitably scaling these vectors and stacking up the scaled vectors as rows of a (short and large) matrix. The unitary completion of a given generalized WBE signal set specified by \mathbf{S} and \mathbf{A} as shown above, uniquely characterizes (up to rotations) the dual generalized WBE signal set by specifying the matrices $\tilde{\mathbf{S}}$ and $\tilde{\mathbf{A}}$.

Another consequence of $\mathbf{I}_K = \mathbf{U}\mathbf{U}^H$ is that the product $\mathbf{S}\tilde{\mathbf{S}}^H$ is identically equal to zero, i.e., that the rows of \mathbf{S} and $\tilde{\mathbf{S}}$ are orthogonal, and hence that the product $\mathbf{R}\tilde{\mathbf{R}}$ is identically equal to zero. In particular, $(\mathbf{R}\tilde{\mathbf{R}})_{\nu\nu} = 0$, and we have the series of equalities

$$\begin{aligned} R_{\nu\nu} \tilde{R}_{\nu\nu} &= - \sum_{l \neq \nu} R_{\nu l} \tilde{R}_{l\nu} \\ &= \left| \sum_{l \neq \nu} R_{\nu l} \tilde{R}_{l\nu} \right| = \sum_{l \neq \nu} |R_{\nu l}| |\tilde{R}_{l\nu}|. \end{aligned} \quad (8)$$

The last equality follows directly from (7). Finally, since

$$R_{\nu\nu} = E_\nu, \tilde{R}_{\nu\nu} = (K - NE_\nu)/(K - N)$$

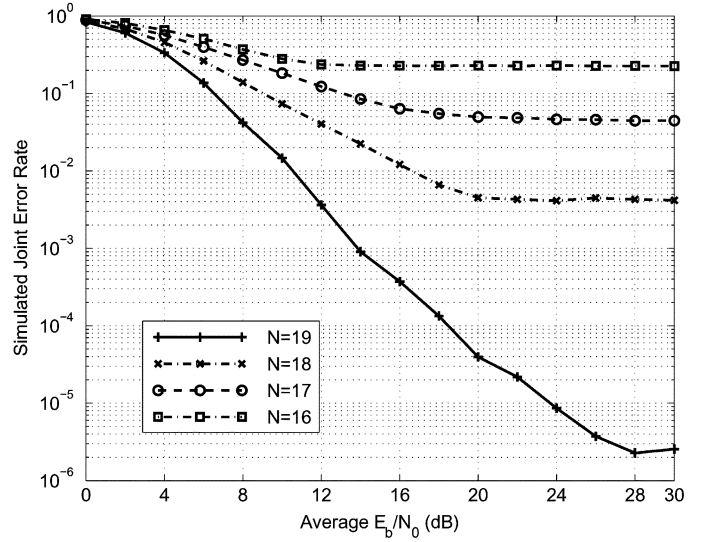


Fig. 1. The effect of the overload on the JER performance of WBE signals: $(K, \mathbf{E}) = (20, \mathbf{I}_K)$, BPSK modulation, and different values of N .

and from the Cauchy-Schwarz inequality applied to $\tilde{R}_{l\nu} = (\tilde{\mathbf{A}}_l \tilde{\mathbf{s}}_l)^H (\tilde{\mathbf{A}}_\nu \tilde{\mathbf{s}}_\nu)$

$$|\tilde{R}_{l\nu}| \leq \frac{\sqrt{(K - NE_l)(K - NE_\nu)}}{K - N}$$

the equality in (8) yields

$$1 \leq \frac{1}{E_\nu} \sum_{l \neq \nu} |R_{\nu l}| \sqrt{\frac{K - NE_l}{K - NE_\nu}} \leq \frac{1}{E_\nu} \sum_{l \neq \nu} |R_{\nu l}|$$

where the last step follows because $E_\nu = \min_k E_k$. Hence, the result that $e_\nu = 0$.

Finally, we extend the proof to the case when $\sum_k E_k \leq N \max_k E_k$. Oversized users obviously achieve single-user performance for all values of noise power, and in particular $e_k = E_k, \forall k \in \mathcal{O}$. On the other hand, the nonoversized users' submatrix $\mathbf{S}_{\mathcal{O}^c}$ represents a reduced generalized WBE signal set, i.e.,

$$\mathbf{S}_{\mathcal{O}^c} \in \mathcal{W}(N - |\mathcal{O}|, |\mathcal{O}^c|, \mathbf{E}_{\mathcal{O}^c})$$

in which there are no oversized users. Indeed, if user k is nonoversized with respect to the system parameters (N, K, \mathbf{E}) , then it is easy to show that it is also nonoversized with respect to $(N - |\mathcal{O}|, |\mathcal{O}^c|, \mathbf{E}_{\mathcal{O}^c})$. Consequently, we can appeal to our arguments above and conclude that $e(\mathbf{S}_{\mathcal{O}^c}) = 0$.

In summary, we have proved that there exist at least one user whose AEE is identically zero, no matter how the received energies are distributed. When the received energies are equal, it follows by symmetry that all users have the same AEE (6), and therefore the other users' AEE are also identically zero. Hence the corollary.

IV. NUMERICAL EXAMPLES

We illustrate the JER performance of generalized WBE signals under linear MMSE (and matched-filter) detection as a function of (K, N, \mathbf{E}) via numerical examples. We fix the modulation to BPSK, i.e., the best scheme in terms of achieving nonzero AEE and lowest bit-error rate (BER).

We first consider the effects on the JER of different processing gains by varying N while fixing $(K, \mathbf{E}) = (20, \mathbf{I}_K)$. The resulting JER versus average E_b/N_0 is plotted in Fig. 1. As predicted, the JER always floors, i.e., the BER of at least one user floors. In fact, we know that the BER of every user floors, but we emphasize that the BER floor can

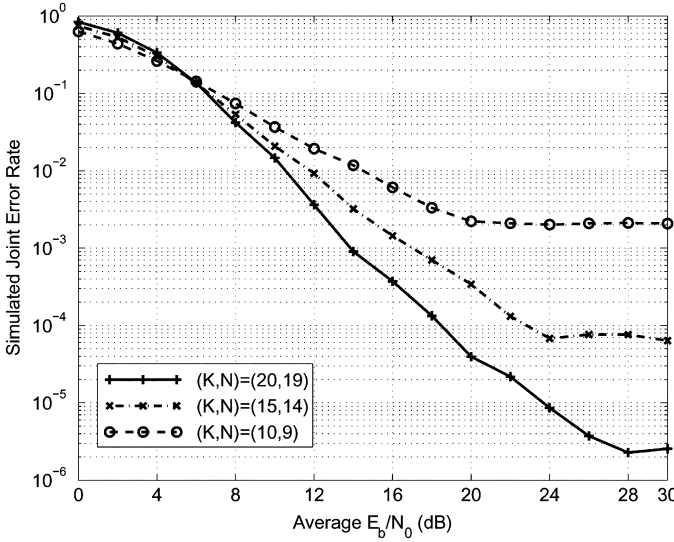


Fig. 2. The effect of variable system sizes on the JER performance of WBE signals: $\mathbf{E} = \mathbf{I}_K$, $N = K - 1$, BPSK modulation, and different values of K .

differ from one user to another in general. More interestingly, we note that the JER floor value critically depends on the load factor $\beta = K/N$: it rises very quickly as β increases. For instance, the load for $N = 17$ is only marginally larger than full-rank signaling (1.1765 instead of 1), but the JER floors at 0.05 for $E_b/N_0 \geq 20$ dB. Not surprisingly, the performance improves as the overload decreases, and is best when $N = K - 1$, i.e., for least overload.

Next, we study the effects of the size of the system on the JER performance by varying K for a fixed $\mathbf{E} = \mathbf{I}_K$ and $N = K - 1$ (least overload). It is easy to verify that, in this case, the WBE signals form a simplex set, and hence that every user achieves exactly the same BER for all E_b/N_0 . Fig. 2 summarizes our numerical simulations and illustrates that the JER floors again. More interestingly, we note that as the system grows i) the floor value decreases and ii) it is reached for higher E_b/N_0 . The decreasing floor value is a direct consequence of the decreasing load factor as K grows (in fact, the system becomes fully loaded in the limit). Consequently, the floor value might be acceptable when K is sufficiently large and assuming least overload (i.e., small values of β). This might require, however, an unacceptably high E_b/N_0 .

Given that the BER floors, it is of interest to compute the floor value. We first note that this value is a decreasing function of the load β only, i.e., it is independent of the absolute values of K and N . The BER floor of user k can be computed exactly by a counting argument. For any noise level, the BER is the average conditional error probabilities over all the interfering bit sequences. As noise vanishes, only those sequences that satisfy $\eta_k = E_k - \sum_{l \neq k} R_{kl} b_l \leq 0$ contribute to the BER floor. Specifically, the conditional error probability for such a sequence is equal, in the low-noise limit, to one if $\eta_k < 0$ or 0.5 if $\eta_k = 0$. The BER floor is then given by counting these sequences (and suitably weighting them by 1 or 0.5) and dividing the result by the total number of interfering bit sequences. This operation is computationally prohibitive unless we can exploit special properties of the weighted correlation matrix \mathbf{R} . While such properties are not apparent in general, the case of equal energies with $K = N + 1$ is particularly simple since WBE signals form a simplex set. In this case, $R_{kl} = -1/N, \forall k \neq l$, and it is easy to verify that the BER floor is equal to 2^{-K} . In fact, since the floor depends only on the load, any user in a K' -user, N' -dimension system such that $K'/N' = K/N$ achieves the same floor 2^{-K} .

Alternatively, we can estimate the BER floor using an SIR approximation. Indeed, recall that generalized WBE signals under linear

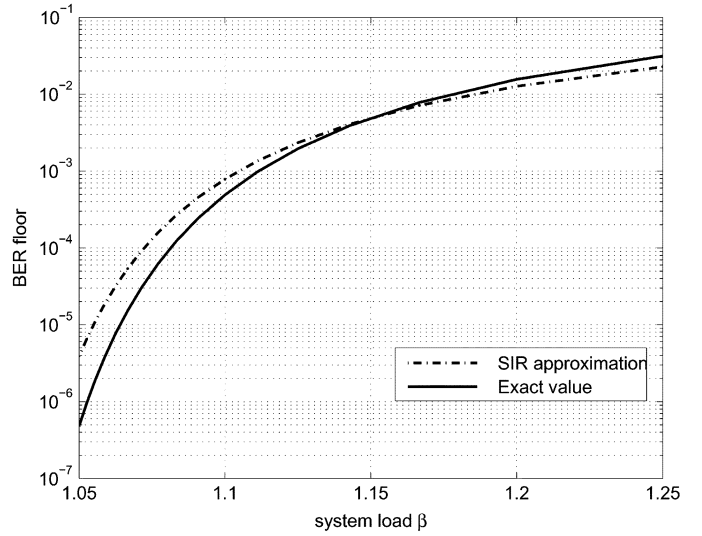


Fig. 3. Comparison of the exact BER floor and the SIR approximation as a function of the system load for the equal-power case.

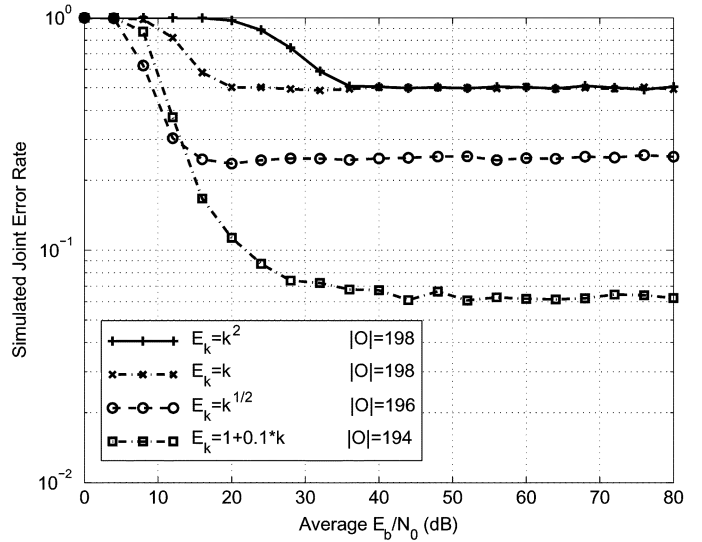


Fig. 4. The effect of the energy distribution on the JER performance of generalized WBE signals: $(K, N) = (200, 199)$, BPSK modulation, and different energy distributions.

MMSE detection also experience an asymptotic saturation in terms of maximum achievable SIR [4]. Namely, assuming equal energies, the SIR cannot be larger than $(\beta - 1)^{-1}$ even as noise vanishes. Using the classical approximation that the SIR in a multiuser system is roughly equal to the signal-to-noise ratio (SNR) in a single-user system, the BER floor is approximated by $Q((\beta - 1)^{-1/2})$. We compare the exact and SIR-predicted floors for different loads in Fig. 3. To compute the exact BER floor, we first consider loads β for which there exists an associated simplex signal set and then interpolate for other loads. Fig. 3 illustrates that the SIR approximation is roughly accurate for a narrow range of loads around $\beta = 1.15$. It gives only an order of magnitude estimate for higher loads (where the floor is high anyway), and it quickly breaks down for lower loads. This comparison underlines that an SIR approximation does not replace an error probability analysis in general.

Finally, we illustrate the effect of unequal energy distributions on the JER performance. Specifically, we fix $(K, N) = (200, 199)$ (least overload) and vary \mathbf{E} . Each energy distribution results in a generalized

WBE signal set with a corresponding number of oversized users $|\mathcal{O}|$. The values we used for numerical simulations are summarized in the following table.

E_k	$ \mathcal{O} $	E_k	$ \mathcal{O} $
k^2	198	\sqrt{k}	196
k	198	$1 + 0.1k$	194

Fig. 4 illustrates that even mild energy disparities yield very poor performance. For instance, the JER floors at 1/2 for the first two power distributions. Here, the 198 more powerful users are oversized and hence experience a single-user Gaussian channel; by contrast, the two remaining users share the only remaining direction in the signal space, and hence, interfere in such a way that the AEE of the weakest user is equal to zero. Finally, as the energy disparities decrease, there are fewer oversized users, and the floor decreases and is reached for higher E_b/N_0 . The JER is still unacceptably high for all practical purposes though. Consider for instance that when $E_k = 1 + 0.1k$, the JER floors at 0.06 for $E_b/N_0 \geq 35$ dB.

V. CONCLUSION

This correspondence has characterized exactly the severe limitation of generalized WBE signals under linear MMSE detection. Specifically, we have shown that such signals do not satisfy even the basic requirement that the error rate of every user decreases exponentially as noise vanishes. Our results hold for arbitrary overload, modulation, and received energies. Moreover, when the received powers are equal, the error rate of every user floors. Therefore, it appears that the full benefit of generalized WBE signals can only be leveraged by nonlinear detection. It remains an open problem as to whether there exists a signal set with nonzero symmetric energy under linear MMSE detection (and hence not the generalized WBE set) for overloaded CDMA systems.

REFERENCES

- [1] P. Viswanath and V. Anantharam, "Optimal sequences and sum capacity of synchronous CDMA systems," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1984–1991, Sep. 1999.
- [2] M. Rupf and J. L. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1261–1266, Jul. 1994.
- [3] T. Guess, "Optimal sequences for CDMA with decision-feedback receivers," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 886–900, Apr. 2003.
- [4] P. Viswanath, V. Anantharam, and D. N. C. Tse, "Optimal sequences, power control, and user capacity of synchronous CDMA systems with linear MMSE receivers," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1968–1983, Sep. 1999.
- [5] L. Gao and T. F. Wong, "Power control and spreading sequence allocation in a CDMA forward link," *IEEE Trans. Inf. Theory*, vol. 50, no. 1, pp. 105–124, Jan. 2004.
- [6] S. Ulukus and R. D. Yates, "Iterative construction of optimum signature sequence sets in synchronous CDMA systems," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1989–1998, Jul. 2001.
- [7] P. Anigstein and V. Anantharam, "Ensuring convergence of the MMSE iteration for interference avoidance to the global optimum," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 873–885, Apr. 2003.
- [8] C. Rose, S. Ulukus, and R. D. Yates, "Wireless systems and interference avoidance," *IEEE Trans. Wireless Commun.*, vol. 1, no. 3, pp. 415–428, Jul. 2002.
- [9] T. Strohmer, R. W. Heath Jr., and A. J. Paulraj, "On the design of optimal spreading sequences for CDMA systems," in *Proc. Asilomar Conf. Signals, Systems, and Computers*, Pacific Grove, CA, Nov. 2002, pp. 1434–1438.
- [10] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.
- [11] S. Verdú and S. Shamai (Shitz), "Spectral efficiency of CDMA with random spreading," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 622–640, Mar. 1999.

- [12] D. N. C. Tse and S. V. Hanly, "Linear multiuser receivers: Effective interference, effective bandwidth, and user capacity," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 641–657, Mar. 1999.
- [13] A. Kapur and M. K. Varanasi, "Multiuser detection for overloaded CDMA systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1728–1742, Jul. 2003.
- [14] M. K. Varanasi, "Decision feedback multiuser detection: A systematic approach," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 219–240, Jan. 1999.
- [15] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II, Methods in Communication, Security, and Computer Science*. New York: Springer-Verlag, 1993.

Extracting Randomness from Multiple Independent Sources

Chia-Jung Lee, Chi-Jen Lu, Shi-Chun Tsai, and Wen-Guey Tzeng

Abstract—We study the problem of deterministically extracting almost perfect random bits from multiple weakly random sources that are mutually independent. With two independent sources, we have an explicit extractor which can extract a number of random bits that matches the best construction currently known, via the generalized leftover hash lemma. We also extend our construction to extract randomness from more independent sources. One nice feature is that the extractor still works even with all but one source exposed. Finally, we apply our extractor for a cryptographic task in which a group of parties wants to agree on a secret key for group communication over an insecure channel, without using ideal local randomness.

Index Terms—Deterministic extractor, two-sources extractor, multi-sources-extractor, leftover hash lemma.

I. INTRODUCTION

Randomness has become a useful resource in computer science. For several important computational problems, randomized algorithms are simpler, run faster, or use smaller space than the known deterministic ones. In cryptography, randomness is essential for protocols to generate or hide the secret. Hence, how to obtain and manipulate randomness has become an important topic in computer science. However, random sources we have access to are usually imperfect. We say that a source has *min-entropy* k if every string occurs with probability at most 2^{-k} . From such a weakly random source, one would like to extract almost

Manuscript received August 16, 2004; revised January 38, 2005. The work of C.-J. Lee and S.-C. Tsai was supported in part by the National Science Council of Taiwan under Contract NSC-92-2213-E-009-024. The work of C.-J. Lu was supported in part by the National Science Council of Taiwan under Contract NSC-93-2213-E-001-004. The work of W.-G. Tzeng was supported in part by the National Science Council of Taiwan under Contract NSC-93-2213-E-009-009, and in part under a MediaTek Grant, 2003.

C.-J. Lee and S.-C. Tsai are with the Department of Computer Science and Info Engineering, National Chiao-Tung University, Hsinchu 30050, Taiwan, R.O.C. (e-mail: leecj@csie.nctu.edu.tw; sctsay@csie.nctu.edu.tw).

C.-J. Lu is with the Institute of Information Science, Academia Sinica, Taipei, Taiwan, R.O.C. (e-mail: cjlu@iis.sinica.edu.tw).

W.-G. Tzeng is with the Department of Computer and Info Science, National Chiao-Tung University, Hsinchu 30050, Taiwan, R.O.C. (e-mail: tzeng@cis.nctu.edu.tw).

Communicated by T. Johansson, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2005.847746