Constructing and Decoding GWBE Codes Using Kronecker Products

Pedram Pad, *Student Member, IEEE,* Mohammad Javad Faraji, *Student Member, IEEE*,
and Farokh Marvasti, *Senior Member, IEEE*

***Abstract*—In this letter, we introduce a novel method for constructing large size Generalized Welch Bound Equality (GWBE) matrices. This method can also be used for the construction of large WBE matrices. The advantage of this method is its low complexity for constructing large size matrices and low computational complexity using Maximum Likelihood (ML) decoders for a subclass of these codes.**

***Index Terms*—GWBE, WBE, Kronecker product, maximum-likelihood.**

I. INTRODUCTION

WBE codes maximize the sum capacity when the user powers are equal [1]. In fact these codes have minimum correlation with respect to a criterion called Total Squared Correlation (TSC [2]). For practical conditions, Binary WBE (BWBE) codes are more attractive. For binary codes, the lower bounds of TSC are derived in [3], [4]. These bounds are known as Karystinos-Pados (KP) bounds. In some special cases, the KP bounds meet the Welch bounds. For unequal user powers, the sum capacity is maximized by assigning orthogonal signature sequences to high power users and Generalized WBE (GWBE) signatures to low power users [5]. Various methods for constructing WBE [6], BWBE [3], [4], [7], [8] and GWBE [5], [6] codes are proposed.

The maximum of the sum channel capacity occurs when the input data has Gaussian distribution. But for the binary cases, the channel capacity and design of optimum code/decoders are challenging problems [9], [10], [11], [12], [13].

In this letter, we wish to introduce a novel method for constructing large size GWBE codes from smaller ones. This method can also be applied to construct WBE codes. For a special class of such codes, the decoding problem can be reduced to the decoding of smaller size systems; thus their optimum decoders have a significant lower computational complexity. We have simulated large size codes with high over-loading factors with ML decoders for bit, symbol and Almost Symbol (ASML) levels. An iterative decoder is also simulated for comparison.

II. METHOD FOR ENLARGING GWBE MATRICES

For GWBE matrices, we assume that the columns of the signature matrices are normalized. There are two equivalent definitions of GWBE matrices that will be discussed here [1], [2], [5], [6], [14], [15]. In this section, we propose a new method for GWBE matrix construction. Suppose that we have an overloaded CDMA system with m chips and n users $(n > m)$ such that the ith user has power p_i. $\|\mathbf{A}\|_F = \left(\sum_{i,j} |a_{ij}|^2\right)^{1/2}$ is the Frobenius norm of the matrix $\mathbf{A}$ and $\otimes$ denotes the Kronecker product; the entries of a matrix are shown with small letters.

GWBE Definition Based on Sum Capacity: A GWBE matrix $\mathbf{S}$ that maximizes the sum channel capacity has the following property

$$\mathbf{SPS}^H = \frac{\sum_{i=1}^n p_i}{m}\mathbf{I}_m$$

where $\mathbf{P} = \operatorname{diag}(p_1, \ldots, p_n)$ is a diagonal matrix, $\mathbf{S}^H$ is the Hermition of $\mathbf{S}$ and $\mathbf{I}_m$ denotes the $m \times m$ identity matrix.

GWBE Definition Based on Correlation: Let $\hat{\mathbf{S}} = \mathbf{SP}^{1/2}$, where $\mathbf{P}$ is as defined before. The Generalized-TSC (GTSC) of $\hat{\mathbf{S}}$ is defined as

$$GTSC(\hat{\mathbf{S}}) := \frac{\sum_{i=1}^n \sum_{j=1}^n |\langle \hat{S}_i, \hat{S}_j \rangle|^2}{\left(\sum_{i=1}^n \langle \hat{S}_i, \hat{S}_i \rangle\right)^2}$$

where $\hat{S}_i$ is the i^{th} column of $\hat{\mathbf{S}}$ and $\langle ., . \rangle$ denotes the inner product. It is easy to show that

$$GTSC(\hat{\mathbf{S}}) = \frac{\|\hat{\mathbf{S}}^H\hat{\mathbf{S}}\|_F^2}{\|\hat{\mathbf{S}}\|_F^4}.$$

We know that $GTSC(\hat{\mathbf{S}}) \geq 1/m$ and $\hat{\mathbf{S}}$ is a GWBE matrix if its GTSC achieves this lower bound.

Theorem 1: If $\mathbf{S}$ is an $m_1 \times n_1$ GWBE matrix $(n_1 > m_1)$ for a CDMA system with user powers p_i's, and $\mathbf{T}$ is an $m_2 \times n_2$ GWBE matrix $(n_2 > m_2)$ for a CDMA system with user powers q_j's, then $\mathbf{S} \otimes \mathbf{T}$ is an $m_1m_2 \times n_1n_2$ GWBE matrix for a CDMA system with user powers p_iq_j's for $1 \leq i \leq n_1$ and $1 \leq j \leq n_2$.

We prove this theorem using both definitions of GWBE matrices.

Lemma 1: $\|\mathbf{A} \otimes \mathbf{B}\|_F = \|\mathbf{A}\|_F\|\mathbf{B}\|_F$.

Proof: Suppose $\mathbf{A}$ and $\mathbf{B}$ are $m_1 \times n_1$ and $m_2 \times n_2$ matrices and $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$.

$$\|\mathbf{C}\|_F^2 = \sum_{i=1}^{m_1m_2}\sum_{j=1}^{n_1n_2} |c_{ij}|^2 = \sum_{i=1}^{m_1}\sum_{j=1}^{n_1}\left(|a_{ij}|^2\sum_{r=1}^{m_2}\sum_{s=1}^{n_2}|b_{rs}|^2\right)$$

$$= \left(\sum_{i=1}^{m_1}\sum_{j=1}^{n_1}|a_{ij}|^2\right)\left(\sum_{r=1}^{m_2}\sum_{s=1}^{n_2}|b_{rs}|^2\right) = \|\mathbf{A}\|_F^2\|\mathbf{B}\|_F^2.$$

Proof 1 of Theorem 1: Because each column of $\mathbf{S} \otimes \mathbf{T}$ is the Kronecker product of a column of $\mathbf{S}$ by a column of $\mathbf{T}$, according to Lemma 1, the Frobenius norm of each column

Manuscript received September 22, 2009. The associate editor coordinating the review of this letter and approving it for publication was Y.-C. Wu.

The authors are with the Advanced Communication Research Institute (ACRI), Electrical Engineering Department, Sharif University of Technology, Tehran, Iran (e-mail: {pedram_pad, faraji}@ee.sharif.edu, marvasti@sharif.edu).

Digital Object Identifier 10.1109/LCOMM.2010.01.091900

1089-7798/10$25.00 © 2010 IEEE

of $\mathbf{S}\otimes\mathbf{T}$ equals the product of the Frobenius norms of the corresponding columns of $\mathbf{S}$ and $\mathbf{T}$. Thus the columns of $\mathbf{S}\otimes\mathbf{T}$ have norm 1 and satisfies the unit-norm property of the signature matrices. Let $\mathbf{P} = \text{diag}\,(p_1,\dots,p_{n_1})$ and $\mathbf{Q} = \text{diag}\,(q_1,\dots,q_{n_2})$, then $\mathbf{SPS}^H = \frac{\sum_{i=1}^{n_1} p_i}{m_1}\mathbf{I}_{n_1}$ and $\mathbf{TQT}^H = \frac{\sum_{j=1}^{n_2} q_j}{m_2}\mathbf{I}_{n_2}$. Thus, we have

$$(\mathbf{S}\otimes\mathbf{T})(\mathbf{P}\otimes\mathbf{Q})(\mathbf{S}\otimes\mathbf{T})^H = \left(\mathbf{SPS}^H\otimes\mathbf{TQT}^H\right)$$

$$= \frac{\left(\sum_{i=1}^{n_1} p_i\right)\left(\sum_{j=1}^{n_2} q_j\right)}{m_1 m_2}\mathbf{I}_{m_1 m_2}.$$

But $\mathbf{P}\otimes\mathbf{Q}$ is a diagonal matrix with diagonal entries as $p_i q_j$'s for $1\le i\le n_1$ and $1\le j\le n_2$. Thus the proof is complete.
For the second proof we use the second definition of the GWBE matrices. Firstly, we can easily prove the following lemma.

Lemma 2: $GTSC(\mathbf{A}\otimes\mathbf{B}) = GTSC(\mathbf{A})GTSC(\mathbf{B})$.
Proof 2 of Theorem 1: Let $\hat{\mathbf{S}} = \mathbf{SP}^{1/2}$ and $\hat{\mathbf{T}} = \mathbf{TQ}^{1/2}$, where $\mathbf{P}$ and $\mathbf{Q}$ are the matrices defined in the Proof 1. Since $\mathbf{S}$ and $\mathbf{T}$ are GWBE matrices, $GTSC(\hat{\mathbf{S}}) = 1/m_1$ and $GTSC(\hat{\mathbf{T}}) = 1/m_2$. According to Lemma 2, $GTSC(\hat{\mathbf{S}}\otimes\hat{\mathbf{T}}) = 1/(m_1 m_2)$. But

$$\hat{\mathbf{S}}\otimes\hat{\mathbf{T}} = \left(\mathbf{SP}^{1/2}\right)\otimes\left(\mathbf{TQ}^{1/2}\right) = (\mathbf{S}\otimes\mathbf{T})\left(\mathbf{P}^{1/2}\otimes\mathbf{Q}^{1/2}\right)$$

$$= (\mathbf{S}\otimes\mathbf{T})(\mathbf{P}\otimes\mathbf{Q})^{1/2}.$$

But according to Proof 1, $\mathbf{S}\otimes\mathbf{T}$ has normalized columns and $\mathbf{P}\otimes\mathbf{Q}$ is a diagonal matrix with $p_i q_j$'s as its diagonal entries which completes the second proof.

Corollary 1: Suppose $\mathbf{A}$ and $\mathbf{B}$ are matrices with normalized columns; we then have $TSC\,(\mathbf{A}\otimes\mathbf{B}) = TSC\,(\mathbf{A})\,TSC\,(\mathbf{B})$.
Proof: First we must show that $TSC\,(\mathbf{A}\otimes\mathbf{B})$ is well-defined; it means we must show that the columns of $\mathbf{A}\otimes\mathbf{B}$ are normalized. The proof is similar to that of the first step of Theorem 1. Now, suppose that $\mathbf{A}$ and $\mathbf{B}$ are $m_1\times n_1$ and $m_2\times n_2$ matrices, respectively. It is easy to show that $TSC(\mathbf{A}) = n_1^2 GTSC(\mathbf{A})$, $TSC(\mathbf{B}) = n_2^2 GTSC(\mathbf{B})$ and $TSC(\mathbf{A}\otimes\mathbf{B}) = (n_1 n_2)^2\, GTSC(\mathbf{A}\otimes\mathbf{B})$. Thus, according to Lemma 2, the proof is complete.

Corollary 2: Suppose $\mathbf{S}$ and $\mathbf{T}$ are $m_1\times n_1$ and $m_2\times n_2$ WBE matrices, respectively. If $m_1\ge n_1$ and $m_2\ge n_2$, then $\mathbf{S}\otimes\mathbf{T}$ is an $m_1 m_2\times n_1 n_2$ WBE matrix. The same statement is true for the case that $m_1\le n_1$ and $m_2\le n_2$.
Proof: The minimum TSC of an $m\times n$ matrix (the Welch bound) is n if $m\ge n$, and n^2/m if $m\le n$ [2]. Thus, if $m_1\ge n_1$ and $m_2\ge n_2$, then $TSC\,(\mathbf{S}) = n_1$ and $TSC\,(\mathbf{T}) = n_2$. By using Corollary 1, $TSC\,(\mathbf{S}\otimes\mathbf{T}) = TSC\,(\mathbf{S})\,TSC\,(\mathbf{T}) = n_1 n_2$. Since $\mathbf{S}\otimes\mathbf{T}$ is an $m_1 m_2\times n_1 n_2$ matrix and $m_1 m_2\ge n_1 n_2$, it is a WBE matrix. Similarly, if $m_1\le n_1$ and $m_2\le n_2$, then $TSC\,(\mathbf{S}) = n_1^2/m_1$ and $TSC\,(\mathbf{T}) = n_2^2/m_2$. By using Corollary 1, $TSC\,(\mathbf{S}\otimes\mathbf{T}) = TSC\,(\mathbf{S})\,TSC\,(\mathbf{T}) = (n_1 n_2)^2/(m_1 m_2)$. Since $\mathbf{S}\otimes\mathbf{T}$ is an $m_1 m_2\times n_1 n_2$ matrix and $m_1 m_2\le n_1 n_2$, it is a WBE matrix. Also, when $m_1\le n_1$ and $m_2\le n_2$, $\mathbf{S}$ and $\mathbf{T}$ are GWBE matrices with equal user powers and thus using Theorem 1, $\mathbf{S}\otimes\mathbf{T}$ is a WBE matrix.

Note 1: According to [16], the direct construction of an $m_1 m_2\times n_1 n_2$ GWBE matrix needs $6m_1 m_2 n_1 n_2$ operations. But using the method proposed in this letter, it only needs $6m_1 n_1 + 6m_2 n_2$ such operations and $m_1 m_2 n_1 n_2$ multiplications. Since some operations in direct construction of GWBE matrices are more complicated than a simple multiplication, this new method results in a significant reduction in the computational cost of constructing large size GWBE matrices.

This method can also be used for enlarging BWBE matrices. It is proved in [3], [4] that the TSC of a binary matrix is lower bounded by the KP bound which is greater than or equal to the Welch bound[3]. Note that for an $m\times n$ $\{\pm 1\}$-matrix, the KP bound meets the Welch bound when $\max(m,n)$ is a multiple of 4. According to Corollary 2, if $\mathbf{S}$ and $\mathbf{T}$ are binary matrices such that their TSC meets the Welch bound (i.e., BWBE matrices), then $\mathbf{S}\otimes\mathbf{T}$ is also a BWBE matrix (note that the entries of $\mathbf{S}\otimes\mathbf{T}$ is also binary antipodal).

III. GWBE Matrices with Low Cost ML Decoders

By bit ML decoders, we mean a decoder that extracts the user bits optimally. Also, by symbol ML decoders, we mean the decoder that extracts the symbols (the user data vectors) optimally. We use the average of the Bit Error Rate (BER) of the users as the measure of performance and thus the bit ML decoder is the optimum decoder and the symbol ML decoder is suboptimum.
Theorem 1 implies that if $\mathbf{U}$ is $k\times k$ unitary and $\mathbf{A}$ is an $m\times n$ GWBE matrix, then $\mathbf{C} = \mathbf{U}\otimes\mathbf{A}$ is a $km\times kn$ GWBE matrix. Now, consider a CDMA channel model $Y = \mathbf{C}X + N$ where $\mathbf{C}$ is the signature matrix, X is the input data vector and N is the noise vector with distribution $\mathcal{N}\left(0,\sigma^2\mathbf{I}_{km}\right)$. If we multiply both sides of (1) by $\mathbf{U}^T\otimes\mathbf{I}_m$, we have

$$\left(\mathbf{U}^T\otimes\mathbf{I}_m\right)Y = (\mathbf{I}_k\otimes\mathbf{A})\,X + \left(\mathbf{U}^T\otimes\mathbf{I}_m\right)N. \quad (1)$$

Since $\mathbf{U}^T\otimes\mathbf{I}_m$ is unitary, $\left(\mathbf{U}^T\otimes\mathbf{I}_m\right)N$ is a Gaussian random vector with the same distribution as N. By converting $Y = \mathbf{C}X + N$ to (1), we have decoupled a system of km-equations down to k systems of m-equations. This means a dramatic reduction in the decoding complexity. For example, if the input alphabet is binary, the direct implementation of the bit/symbol ML decoders need to calculate 2^{kn} Euclidean distances of km-dimensional vectors, but by using (1), we only need $k\times 2^n$ Euclidean distances of m-dimensional vectors.

Note 2: Since the correlation matrix is

$$(\mathbf{U}\otimes\mathbf{A})^T(\mathbf{U}\otimes\mathbf{A}) = \mathbf{I}_k\otimes\left(\mathbf{A}^T\mathbf{A}\right),$$

the columns of $\mathbf{U}\otimes\mathbf{A}$ are similar to the group orthogonal codes given in [11].
Almost Symbol ML (ASML) Decoder In addition, when the input alphabet is binary antipodal, another procedure can be performed for decreasing the complexity of the decoder even further. Suppose $\mathbf{A}_{m\times n} = [\mathbf{D}_{m\times m}|\mathbf{E}_{m\times(n-m)}]$ where $\mathbf{D}$ is an invertible matrix (existence of such an $m\times m$ sub-matrix of $\mathbf{A}$ is not a very restrictive condition). Assume that $X = [X_1^T\ X_2^T]^T$ such that $\mathbf{A}X = \mathbf{D}X_1 + \mathbf{E}X_2$, we thus have

$\mathbf{D}^{-1}Y = X_1 + \mathbf{D}^{-1}\mathbf{E}X_2 + \mathbf{D}^{-1}N$. Hence,

$$[\hat{X}_1^T\ \hat{X}_2^T]^T = \arg \min_{[X_1^T\ X_2^T]^T} \|\mathbf{D}^{-1}Y - X_1 - \mathbf{D}^{-1}\mathbf{E}X_2\|$$

is a suboptimum decoder ($\|\ \|$ denotes the Euclidean norm). In fact, if $\mathbf{D}$ is a unitary matrix, then the above decoder is the symbol ML decoder (because the $\mathbf{D}^{-1}N$ vector will be a random vector with the same distribution as N). However, since the binary vector derived from the signs of the entries of another vector is the nearest $\{\pm 1\}$-vector, the above decoder can be implemented with a very low complexity, i.e.,

$$\hat{X}_2 = \arg\min_{X_2}\{\left(\mathbf{D}^{-1}Y - \mathbf{D}^{-1}\mathbf{E}X_2\right) - \text{sign}\left(\mathbf{D}^{-1}Y - \mathbf{D}^{-1}\mathbf{E}X_2\right)\}$$

$$\hat{X}_1 = \text{sign}\left(\mathbf{D}^{-1}Y - \mathbf{D}^{-1}\mathbf{E}X_2\right)$$

which needs 2^{n-m} Euclidean norm calculations instead of 2^n such calculations for the direct implementation of symbol ML decoders. This method is called Almost Symbol ML (ASML). We have simulated two highly overloaded CDMA systems with 64 chips and 96 or 128 users in an AWGN channel. For the first system, the signature matrix is $\frac{1}{\sqrt{8}}\mathbf{H}_8 \otimes \mathbf{A}_{8\times 12}$ where $\mathbf{H}_8$ is an 8×8 Hadamard matrix and $\mathbf{C}_{8\times 12}$ is an 8×12 BWBE matrix that is constructed by the method proposed in [3]. For the second system, we have used the matrix $\frac{1}{\sqrt{16}}\mathbf{H}_{16} \otimes \mathbf{A}_{4\times 8}$ for $\mathbf{A}_{4\times 8} = [\mathbf{D}|\mathbf{E}]$ where $\mathbf{D} = \mathbf{I}_4$ and $\mathbf{E}$ is a random 4×4 real valued unitary matrix. It is easy to show that $\mathbf{A}_{4\times 8}$ is a random WBE matrix. From (2), the bit and symbol ML decoders are implemented with a complexity of 8×2^{12} and 16×2^8 Euclidean distance calculations of 8 and 4-dimensional vectors instead of 2^{96} and 2^{128} such calculations for 64-dimensional vectors, respectively. The ASML decoder can be implemented with even lower complexity. It respectfully needs $8\times 2^4 = 128$ and $16\times 2^4 = 256$ Euclidean norm calculations of 8 and 4-dimensional vectors. Note that because the first 8×8 sub-matrix of $\mathbf{A}_{8\times 12}$ is not unitary, the ASML is not equivalent to the symbol ML decoder for the first system. But since the first 4×4 matrix of $\mathbf{A}_{4\times 8}$ is unitary, the symbol ML decoder is equivalent to ASML for the second system. The iterative decoder with soft thresholding [12] is also used for comparison. The BER performance curves versus E_b/N_0 is depicted in Figs. 1 and 2. As seen in Fig. 2, the BER of the bit ML decoder nearly coincides with that of ASML. This shows that we can use the simpler ASML decoder.

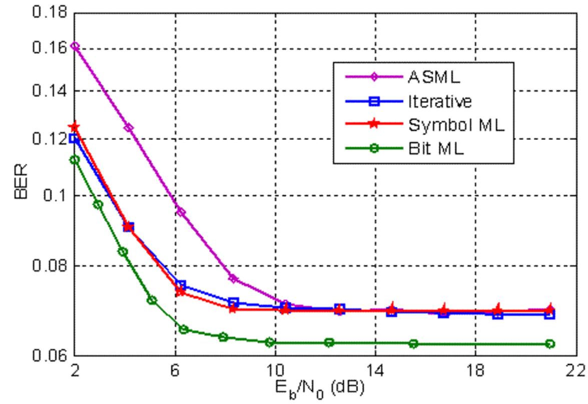

Fig. 1. BER versus E_b/N_0 for a 64×96 BWBE code with bit ML, symbol ML, ASML and iterative decoders.

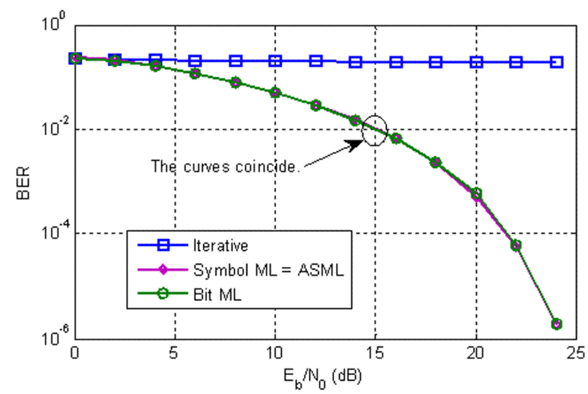

Fig. 2. BER versus E_b/N_0 for a 64×128 WBE code with real valued entries using bit ML, symbol ML, ASML and iterative decoders.

References

[1] M. Rupf and J. L. Massey, "Optimum sequences multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 40, pp. 1261–1266, July 1994.

[2] 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 Sciences*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds. New York: Springer-Verlag, 1993.

[3] G. N. Karystinos and D. A. Pados, "New bounds on the total squared correlation and optimum design of DS-CDMA binary signature sets," *IEEE Trans. Commun.*, vol. 51, no. 1, pp. 48–51, Jan. 2003.

[4] V. P. Ipatov, "On the Karystinos-Pados bounds and optimal binary DS-CDMA signature ensembles," *IEEE Commun. Lett.*, vol. 8, no. 2, pp. 81–83, Feb. 2004.

[5] P. Viswanath and V. Anantharam, "Optimum sequences and sum capacity of synchronous CDMA systems," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1984–1991, Sep. 1999.

[6] C. Rose, "CDMA codeword optimization: interference avoidance and convergence via class warfare," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2368–2382, Sep. 2001.

[7] C. Ding, M. Golin, and T. Klove, "Meeting the Welch and Karystinos-Pados bounds on DS-CDMA binary signature sets," *Designs, Codes and Cryptography*, vol. 30, pp. 73–84, Aug. 2003.

[8] G. N. Karystinos and D. A. Pados, "The maximum squared correlation, total asymptotic efficiency, and sum capacity of minimum total-squared-correlation binary signature sets," *IEEE Trans. Inf. Theory*, vol. 51, pp. 348–355, Jan. 2005.

[9] K. Alishahi, F. Marvasti, V. Aref, and P. Pad, "Bounds on the sum capacity of synchronous binary CDMA channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3577–3593, Aug. 2009.

[10] S. Verdu, *Multiuser Detection*. New York: Cambridge University Press, 1998.

[11] D. Djoinin and V. Bhagrava, "New results on low complexity detectors for over-saturated CDMA systems," in *Proc. Globecom'01*, Nov. 2001.

[12] F. Marvasti, M. Ferdowszadeh, and P. Pad, "Iterative synchronous and asynchronous multi-user detection with optimum soft limiter," patent applicaion 12/122668, May 2008.

[13] P. Pad, F. Marvasti, K. Alishahi, and S. Akbari, "A class of errorless codes for over-loaded synchronous wireless and optical CDMA systems," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2705–2715, June 2009.

[14] S. Waldron, "Generalized Welch bound equality sequences are tight frames," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2307–2309, Sep. 2003.

[15] P. Anigstein and V. Anantharam, "Ensuring convergence of the MMSE iteration for interference avoidance to the global optimum," *IEEE Trans. Inf. Theory*, vol. 49, pp. 873–885, Apr. 2003.

[16] J. A. Tropp, I. S. Dhillon, and R. W. H. Jr., "Finite-step algorithms for constructing optimal CDMA signature sequences," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2916–2921, Nov. 2004.