Welch's Bound and Sequence Sets for Code-Division Multiple-Access Systems

James L. Massey and Thomas Mittelholzer

Signal and Information Processing Laboratory
Swiss Federal Institute of Technology
CH-8092 Zürich

Abstract

Welch's bound for a set of M complex equi-energy sequences is considered as a lower bound on the sum of the squares of the magnitudes of the inner products between all pairs of these sequences. It is shown that, when the sequences are binary (±-1 valued) sequences assigned to the M users in a synchronous code-division multiple-access (S-CDMA) system, precisely such a sum determines the sum of the variances of the interuser interference seen by the individual users. It is further shown that Welch's bound, in the general case, holds with equality if and only if the array having the M sequences as rows has orthogonal and equi-energy columns. For the case of binary (±-1 valued) sequences that meet Welch's bound with equality, it is shown that the sequences are uniformly good in the sense that, when used in a S-CDMA system, the variance of the interuser interference is the same for all users. It is proved that a sequence set corresponding to a binary linear code achieves Welch's bound with equality if and only if the dual code contains no codewords of Hamming weight two. Transformations and combination of sequences sets that preserve equality in Welch's bound are given and used to illustrate the design and analysis of sequence sets for non-synchronous CDMA systems.

1 Introduction

The aim of this paper is to show the central role played by Welch's bound [1] in the synthesis and/or analysis of sequence sets or multi-sets (in which the same sequence can appear more than once) for use in code-division multiple-access (CDMA) systems.

Section 2 motivates the interest in the sum of the squares of the magnitudes of the inner products between the sequences in a sequence (multi-)set by showing that this sum determines the sum of the variances of the interuser interference experienced by the individual users in a synchronous CDMA (S-CDMA) system. Welch's bound on the sum of the magnitudes of the squares of the inner products between the sequences in a complex sequence (multi-)set is introduced in Section 3 where the apparently new necessary and sufficient condition for equality is derived. It is further shown that (multi-)sets of equi-energy sequences that achieve Welch's bound with equality enjoy an interesting "uniformly good" property that, for the S-

user is the same for all users. Section 4 treats the construction of sequence sets from binary linear codes and gives the necessary and sufficient condition for such a sequence set to achieve equality in Welch's bound. In Section 5, transformations and combination of sequence (multi-)sets are considered that preserve equality in Welch's bound and that are useful in synthesizing and/or analyzing sequence (multi-)sets for use in non-synchronous CDMA systems. Section 6 contains some concluding remarks.

2 Synchronous CDMA Systems

In most spread-spectrum multiple-access systems of the CDMA type, each of the users, say user i, is assigned a binary (±1 valued) *spreading sequence* of length L, say

$$\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}, \ldots, x_L^{(i)}],$$

where L is the *spreading factor* of the spread-spectrum system. The binary (±1 valued) data sequence

$$\ldots, B_{-1}^{(i)}, B_0^{(i)}, B_1^{(i)}, \ldots$$

of user i is then expanded to a binary (±1 valued) sequence at L times the original data rate by using the original data symbols to control the polarity of the spreading sequence $\mathbf{x}^{(i)}$. Each component of the expanded binary (±1 valued) data symbol

$$B_k^{(i)}\,\mathbf{x}^{(i)} = [B_k^{(i)} x_1^{(i)}, B_k^{(i)} x_2^{(i)}, \ldots, B_k^{(i)} x_L^{(i)}]$$

is called a *chip*. In this manner, one creates the binary (±1 valued) sequence

$$\ldots, B_{-1}^{(i)}\,\mathbf{x}^{(i)}, \; B_0^{(i)}\,\mathbf{x}^{(i)}, \; B_1^{(i)}\,\mathbf{x}^{(i)}, \; \ldots$$

that forms the input to the modulator of user i. This modulator might, for instance, be a binary phase-shift-keyed modulator, and all users would use the same carrier frequency.

In a synchronous CDMA (S-CDMA) system, all users are in exact synchronism (relative to the receiver) in the sense that not only are their carrier frequencies and phases the same, but also their expanded data symbols are aligned in time. With the usual assumption of additive white Gaussian noise, this implies that the demodulator output for the k-th data symbol interval can be written as the L-chip sequence

$$\mathbf{r}_k = \sum_{j=1}^{M} B_k^{(j)}\,\mathbf{x}^{(j)} + \mathbf{n}_k \qquad (2.1)$$

where the L-chip noise sequence

$$\mathbf{n}_k = [n_{k1}, n_{k2}, \ldots, n_{kL}],$$

random variables, each with mean 0 and variance $1/\gamma$, where γ is the signal-to-noise ratio defined as the received energy of an expanded data symbol divided by the two-sided noise power spectral density of the additive white Gaussian noise.

In a *conventional CDMA receiver*, the sequence $\mathbf{r}_k$ is further processed separately for each user in the manner that, say for user i, $\mathbf{r}_k$ is *matched-filtered* (or "correlated") with the spreading sequence $\mathbf{x}^{(i)}$ of that user to produce the detection statistic $S_k^{(i)}$ for the data symbol $B_k^{(i)}$. Mathematically, matched filtering is just the operation of computing the inner product so that

$$S_k^{(i)} = \langle \mathbf{r}_k, \mathbf{x}^{(i)} \rangle = \sum_{l=1}^{L} r_{kl}\, x_l^{(i)}$$

where

$$\mathbf{r}_k = [r_{k1}, r_{k2}, \ldots, r_{kL}].$$

With the help of (2.1) and the fact that

$$\langle \mathbf{x}^{(j)}, \mathbf{x}^{(j)} \rangle = L \tag{2.2}$$

for all j, the data symbol detection statistic for user i becomes

$$S_k^{(i)} = L\, B_k^{(i)} + \sum_{\substack{j=1 \\ j \neq i}}^{M} B_k^{(j)} \langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle + \eta_k^{(i)}, \tag{2.3}$$

where

$$\eta_k^{(i)} = \langle \mathbf{n}_k, \mathbf{x}^{(i)} \rangle = \sum_{l=1}^{L} n_{kl}\, x_l^{(i)}$$

is a Gaussian random variable with mean 0 and variance L/γ that is independent of the data symbols. Because the data symbols of the M users are themselves statistically independent and each has mean 0 and variance 1, the sum

$$\xi_k^{(i)} = \sum_{\substack{j=1 \\ j \neq i}}^{M} B_k^{(j)} \langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle \tag{2.4}$$

in (2.3), which represents the *interuser interference experienced by user i*, has mean 0 and variance

$$\sigma^2(i) = \sum_{\substack{j=1 \\ j \neq i}}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2. \tag{2.5}$$

It is common in the analysis of CDMA systems to make the so-called *Gaussian assumption* that the interuser interference experienced by user i is a Gaussian random variable; the central-limit theorem ensures that this assumption is generally valid when the number M of users is large.

Summarizing, we have seen that, in a conventional S-CDMA system, the detection statistic for the data symbol $B_k^{(i)}$ of user i can be written as

$$S_k^{(i)} = L\, B_k^{(i)} + \xi_k^{(i)} + \eta_k^{(i)} \tag{2.6}$$

where $\xi_k^{(i)}$ and $\eta_k^{(i)}$, under the Gaussian assumption, are independent zero-mean Gaussian random variables. The noise $\eta_k^{(i)}$ has variance L/γ, while the interuser interference $\xi_k^{(i)}$ has variance given by (2.5), which we write here in the more convenient form

$$\sigma^2(i) = \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 - L^2. \tag{2.7}$$

It follows that the sequence design problem for S-CDMA, when a conventional receiver is used and when the system is judged by the *worst interuser interference* σ^2_{wc} *experienced by any user*, can be phrased as follows:

Problem 1: Choose the binary (±1 valued) sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ of length L to minimize

$$\sigma^2_{wc} = \max_i \sigma^2(i) = \max_i \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 - L^2. \tag{2.8}$$

The optimally fair solution to Problem 1 will result from a solution, when it exists, to the following problem.

Problem 2: Choose the binary (±1 valued) sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ of length L to minimize

$$\sigma^2_{TOT} = \sum_{i=1}^{M} \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 - M L^2 \tag{2.9}$$

over all choices of such sequences and then (if possible) to satisfy the further condition that, for $1 \le i \le M$,

$$\sigma^2(i) = \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 - L^2 = \frac{1}{M}\, \sigma^2_{TOT}. \tag{2.10}$$

It is primarily this second problem that we will address in the remainder of this paper. To place our later results into better perspective, we first consider here the

Condition for No Interuser Interference: The binary (±1 valued) length L sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ give $\sigma^2_{TOT} = 0$ [and hence also $\sigma^2(i) = 0$ for $1 \leq i \leq M$] if and only if $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are orthogonal, i.e., if and only if

$$\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle = 0, \quad \text{all } i \neq j.$$

Proof:

$$\sum_{i=1}^{M} \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 \geq \sum_{i=1}^{M} |\langle \mathbf{x}^{(i)}, \mathbf{x}^{(i)} \rangle|^2 = M L^2$$

with equality if and only if $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are orthogonal. o

It follows immediately that $\sigma^2_{TOT} = 0$ is possible only when $M \leq L$, since there can be at most L orthogonal non-zero sequences of length L. Thus, $\sigma^2_{TOT} = 0$ when $M = L$ is possible if and only if the $L \times L$ matrix having $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ as rows is a *Hadamard matrix* [2, p. 129]. Except for the trivial cases L = 1 and L = 2, Hadamard matrices exist only when L is divisible by 4; they may exist for all L divisible by 4 but this has not been proved. Hadamard matrices are known to exist whenever L is a power of 2 [2, p. 130-131]. However, the case $M \leq L$ is not of real interest in S-CDMA systems. The motivation for attaining the complete synchronization that characterizes an S-CDMA system is that this should allow the system to accomodate many more users than one can tolerate with non-synchronous CDMA.

3 Welch's Bound

The starting point for our finding solutions to Problem 2 above will be the bound on the sum of the squares of the magnitudes of inner products given by Welch in 1974 [1]. Because this bound applies generally to sequences with complex components and because the general case is as easy to treat as the special case of sequences with ±1 components, we will hereafter allow the sequences

$$\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}, \ldots, x_L^{(i)}]$$

to be in C^L, the vector space of L-tuples over the complex field C with the inner product defined as

$$\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle = \sum_{k=1}^{L} x_k^{(j)} \, x_k^{(i)*} \tag{3.1}$$

where the asterisk denotes complex conjugation.

We first derive an elementary property of squares of inner products in C^L that is the key not only to a simple derivation of Welch's bound, but also and more interestingly to a recognition of when equality holds in that bound.

Lemma 1: (Row-Column Equivalence) Let $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, \ldots, \mathbf{y}^{(L)}$ denote the columns of the $M \times L$ array whose rows are the sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ in C^L, then

$$\sum_{i=1}^{M} \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 = \sum_{k=1}^{L} \sum_{l=1}^{L} |\langle \mathbf{y}^{(l)}, \mathbf{y}^{(k)} \rangle|^2. \tag{3.2}$$

Proof: Because $\langle \mathbf{x}^{(i)}, \mathbf{x}^{(j)} \rangle = \langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle^*$, we have

$$\begin{aligned}
\sum_{i=1}^{M} \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 &= \sum_{i=1}^{M} \sum_{j=1}^{M} \langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle \langle \mathbf{x}^{(i)}, \mathbf{x}^{(j)} \rangle \\
&= \sum_{i=1}^{M} \sum_{j=1}^{M} \sum_{k=1}^{L} x_k^{(j)} x_k^{(i)*} \sum_{l=1}^{L} x_l^{(i)} x_l^{(j)*} \\
&= \sum_{k=1}^{L} \sum_{l=1}^{L} \sum_{i=1}^{M} x_l^{(i)} x_k^{(i)*} \sum_{j=1}^{M} x_k^{(j)} x_l^{(j)*} \\
&= \sum_{k=1}^{L} \sum_{l=1}^{L} \langle \mathbf{y}^{(l)}, \mathbf{y}^{(k)} \rangle \langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle \\
&= \sum_{k=1}^{L} \sum_{l=1}^{L} |\langle \mathbf{y}^{(l)}, \mathbf{y}^{(k)} \rangle|^2,
\end{aligned}$$

where we have used the fact that the column vector $\mathbf{y}^{(k)}$ is just

$$\mathbf{y}^{(k)} = (x_k^{(1)}, x_k^{(2)}, \ldots, x_k^{(M)}). \text{ o}$$

We will also have need for the following simple result.

Lemma 2: If $a_1, a_2, \ldots, a_L$ are real numbers, then

$$\sum_{k=1}^{L} (a_k)^2 \geq \frac{1}{L} \left(\sum_{k=1}^{L} a_k \right)^2 \tag{3.3}$$

with equality if and only if $a_1 = a_2 = \ldots = a_L$.

Proof: Consider a random variable X that takes on the value a_k with probability $1/L$ for $1 \leq k \leq L$. Because the square function x^2 is strictly convex-$\cup$ on the whole real line, it follows from Jensen's inequality that

$$E[X^2] = \sum_{k=1}^{L} \frac{1}{L}(a_k)^2 \geq E[X]^2 = (\sum_{k=1}^{L} \frac{1}{L} a_k)^2$$

with equality if and only if $a_1 = a_2 = ... = a_L$. Multiplying both sides of this inequality by L gives the lemma. o

We are now ready for the proof of Welch's bound.

Welch's Bound: If $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, ... , \mathbf{x}^{(M)}$ are sequences in C^L and all have the same "energy" L, i. e., if

$$\| \mathbf{x}^{(i)} \|^2 = \langle \mathbf{x}^{(i)}, \mathbf{x}^{(i)} \rangle = L \tag{3.4}$$

for $1 \leq i \leq M$, then

$$\sum_{i=1}^{M} \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 \geq M^2 L \tag{3.5}$$

with equality if and only if the *columns* $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, ... , \mathbf{y}^{(L)}$ of the $M \times L$ array whose rows are $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, ... , \mathbf{x}^{(M)}$ are *orthogonal* and all columns have the same energy, i.e.,

$$\| \mathbf{y}^{(k)} \|^2 = M \tag{3.6}$$

for $1 \leq k \leq L$.

Remark: Welch's bound was originally stated, and is usually treated, as a lower bound on the maximum value of $|\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|$ for $i \neq j$. This form of the bound is easily obtained from (3.5), but it seems to us that Welch's bound is more fundamentally a bound on the sum of the squares of the magnitudes of the inner products between the sequences. The condition for equality in (3.5) appears not to have been given previously.

Proof:

$$\sum_{k=1}^{L} \sum_{l=1}^{L} |\langle \mathbf{y}^{(l)}, \mathbf{y}^{(k)} \rangle|^2 \geq \sum_{k=1}^{L} |\langle \mathbf{y}^{(k)}, \mathbf{y}^{(k)} \rangle|^2 = \sum_{k=1}^{L} (\| \mathbf{y}^{(k)} \|^2)^2$$

with equality if and only if $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, ... , \mathbf{y}^{(L)}$ are orthogonal. But Lemma 2 now gives

$$\sum_{k=1}^{L} (\| \mathbf{y}^{(k)} \|^2)^2 \geq \frac{1}{L}(\sum_{k=1}^{L} \| \mathbf{y}^{(k)} \|^2)^2 = \frac{1}{L}(\sum_{k=1}^{L} \sum_{i=1}^{M} |x_k^{(i)}|^2)^2 = \frac{1}{L}(\sum_{i=1}^{M} \sum_{k=1}^{L} |x_k^{(i)}|^2)^2$$

$$= \frac{1}{L}(\sum_{i=1}^{M} \| \mathbf{x}^{(i)} \|^2)^2 = \frac{1}{L}(M L)^2 = M^2 L$$

this value must be M.) o

We now show a rather surprising consequence of the situation when equality holds in (3.5), i.e., when the *columns* $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, \ldots, \mathbf{y}^{(L)}$ of the $M \times L$ array whose rows are the equi-energy sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are *orthogonal*.

Proposition 1: (The Uniformly-Good Property) If $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are sequences in C^L such that $\| \mathbf{x}^{(i)} \|^2 = L$ for $1 \le i \le M$ and such that equality holds in (3.5), then

$$\sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 = M L$$

for $1 \le i \le M$.

Proof:

$$\sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 = \sum_{j=1}^{M} \langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle \langle \mathbf{x}^{(i)}, \mathbf{x}^{(j)} \rangle = \sum_{j=1}^{M} \sum_{k=1}^{L} x_k^{(j)} x_k^{(i)*} \sum_{l=1}^{L} x_l^{(i)} x_l^{(j)*}$$

$$= \sum_{k=1}^{L} \sum_{l=1}^{L} x_k^{(i)*} x_l^{(i)} \sum_{j=1}^{M} x_k^{(j)} x_l^{(j)*} = \sum_{k=1}^{L} \sum_{l=1}^{L} x_k^{(i)*} x_l^{(i)} \langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle.$$

But equality in (3.5) implies $\langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle = 0$ for all $k \ne l$ and $\langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle = M$ for $k = l$ so that

$$\sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 = \sum_{k=1}^{L} x_k^{(i)*} x_k^{(i)} M = \| \mathbf{x}^{(i)} \|^2 M = L M. \text{ o}$$

We next consider the special case when all components of all sequences have unit magnitude, i.e., when $|x_k^{(i)}| = 1$ for $1 \le i \le M$ and $1 \le k < L$. [We note that this special case includes the case of interest for CDMA systems where the sequences have ± 1 components.] For this special case, equalities (3.4) and (3.6) are automatically fulfilled so that Welch's bound simplifies as follows.

Welch's Bound for Sequences with Unit-Amplitude Components: If $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are sequences in C^L such that $|x_k^{(i)}| = 1$ for $1 \le i \le M$ and $1 \le k < L$, then

$$\sum_{i=1}^{M} \sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 \ge M^2 L \tag{3.7}$$

with equality if and only if the *columns* $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, \ldots, \mathbf{y}^{(L)}$ of the $M \times L$ array whose rows are $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are *orthogonal*. Moreover (by Proposition 1), if equality holds in (3.7), then

$$\sum_{j=1}^{M} |\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|^2 = M L \tag{3.8}$$

4 Optimum S-CDMA Sequence Sets from Linear Codes

We will call the binary (±1 valued) sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ of length L a *Welch-Bound-Equality* (WBE) sequence set (or sequence multi-set if these M sequences are not all distinct) if equality holds in (3.7) or, equivalently from (2.9), if

$$\sigma^2_{TOT} = M\,L\,(M - L). \tag{4.1}$$

It follows further from Proposition 1 that, for a WBE sequence (multi-)set, the variance of the interuser interference experienced by user i is

$$\sigma^2(i) = L\,(M - L) \tag{4.2}$$

for $1 \le i \le M$. In other words, *WBE sequence (multi-)sets are optimal for S-CDMA systems in that they provide a solution to Problem 2* that was formulated in Section 2. In this section, we will give a simple, but powerful, construction of WBE sequence sets based on linear error-correcting codes. First, we note that the number M of sequences in a WBE sequence (multi-)set must be even, because the parity of $\langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle$ equals the parity of M and hence cannot vanish for $k \ne l$ unless M is even (where here and hereafter we exclude the trivial case where $L = 1$). Moreover, because L non-zero vectors can be orthogonal only if their length M is at least L, it follows that equality in (3.7) is possible only when $M \ge L$. Thus, for a given L, we see that it will generally be easier to satisfy the orthogonality condition on $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, \ldots, \mathbf{y}^{(L)}$ as M becomes larger. Thus, the minimization of the variance of interuser interference when $M \ge L$ is quite the reverse of the problem of complete elimination of interuser interference that was discussed at the end of Section 2.

With a binary (±1 valued) sequence $\mathbf{x} = [x_1, x_2, \ldots, x_L]$, we can and will associate a binary (GF(2) valued) sequence $\mathbf{b} = [b_1, b_2, \ldots, b_L]$ where b_k is 0 or 1 according as x_k is +1 or -1, respectively. In this manner, we can and will associate to any set of vectors in $GF(2)^L$ a corresponding set of binary (±1 valued) sequences of length L. For ease of later reference, we note here that if $\mathbf{x}$ and $\mathbf{x}'$ are any two binary (±1 valued) sequences of length L and if $\mathbf{b}$ and $\mathbf{b}'$ are the corresponding vectors in $GF(2)^L$, then

$$\langle \mathbf{x}', \mathbf{x} \rangle = \sum_{k=1}^{L} x_k' x_k = L - 2\,d(\mathbf{b}', \mathbf{b}) \tag{4.3}$$

where d(.,.) denotes the *Hamming distance* between the indicated vectors, i.e., the number of components in which these vectors differ.

We recall that a binary (L, K) *linear code* V is just a K-dimensional subspace of $GF(2)^L$ considered as a vector space of dimension L over the finite field GF(2) and that such a code contains 2^K codewords [2, p. 40]. We recall also that the *dual code* $V^{\perp}$ is the set of all $\mathbf{b}' = [b_1', b_2', \ldots, b_L']$ in $GF(2)^L$ such that $b_1 b_1' + b_2 b_2' + \ldots + b_L b_L' = 0$ for all $\mathbf{b} = [b_1, b_2, \ldots, b_L]$ in V, and that this dual code is a binary linear (L, L - K) code [2, p. 44].

We now relate vectors in $GF(2)^L$ to the WBE sequences corresponding to linear

codes.

Proposition 2: The binary (±1 valued) sequence set corresponding to the binary linear code V is a WBE sequence set if and only if the *dual code* $V^{\perp}$ contains no codewords of Hamming weight two, i. e., with exactly two non-zero components.

Proof: Consider any positions k and l, $1 \le k < l \le L$. We will determine the condition such that columns $\mathbf{y}^{(k)}$ and $\mathbf{y}^{(l)}$ of the array with rows $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ are *not* orthogonal when this sequence set corresponds to the binary linear code V. Now the subset of codewords $\mathbf{b} = [b_1, b_2, \ldots, b_L]$ in V such that $b_k = b_l$ or, equivalently, such that $b_k + b_l = 0$ is a subspace U of V, where we note that the codeword $\mathbf{0} = [0, 0, \ldots, 0]$ is always in this subspace U. If $U \neq V$, then this subspace has a single coset in V distinct from itself, namely the set of all codewords $\mathbf{b} = [b_1, b_2, \ldots, b_L]$ such that $b_k \neq b_l$ or, equivalently, such that $b_k + b_l = 1$. Thus, if $U \neq V$, $\mathbf{y}^{(k)}$ and $\mathbf{y}^{(l)}$ will disagree in exactly half of their components and hence $\langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle = 0$. But if $U = V$, then $\mathbf{y}^{(k)}$ and $\mathbf{y}^{(l)}$ will agree in all their components and hence $\langle \mathbf{y}^{(k)}, \mathbf{y}^{(l)} \rangle = M \neq 0$. Thus $\mathbf{y}^{(k)}$ and $\mathbf{y}^{(l)}$ will not be orthogonal for all $k \neq l$ if and only if, for some $k \neq l$, $b_k + b_l = 0$ in all codewords $\mathbf{b}$. But this latter condition is just the condition that the dual code contains the weight two vector whose 1's are in positions k and l. o

The interesting WBE sequence sets specified by Proposition 2 are those of the following corollary, whose truth follows from the fact that the *minimum distance* of a linear code is equal to the minimum Hamming weight of its non-$\mathbf{0}$ codewords [2, p. 41].

Corollary to Proposition 2: The binary (±1 valued) sequence set corresponding to the binary linear code V is a WBE sequence set if the minimum distance $d^{\perp}$ of the dual code $V^{\perp}$ is at least three.

The dual code $V^{\perp}$ of a linear code V contains a word of Hamming weight one whose 1 is in position k if and only if $b_k = 0$ in all codewords $\mathbf{b} = [b_1, b_2, \ldots, b_L]$ of V, i.e., if and only if the k-th component of the codewords in V is *idle*. If $V^{\perp}$ contains no weight two codewords, then, because $V^{\perp}$ is also a linear code, it can contain at most one codeword of Hamming weight one. Moreover, deleting the corresponding idle component from all codewords of V will then give a linear code V' whose dual code $V'^{\perp}$ contains no codewords with Hamming weights one or two, and thus, unless the dual code is the linear dual code $V'^{\perp}$ has minimum distance $d^{\perp} \ge 3$. It follows that *the Corollary to Proposition 2 actually gives all the linear codes corresponding to WBE sequence sets except for the trivial generalization to linear codes obtained by inserting exactly one idle component into all the codewords of one of the former codes.*

Recall from the discussion in Section 2 that the i-th user in a CDMA system will transmit in every expanded data symbol period either his spreading sequence $+\mathbf{x}^{(i)}$ or its negative $-\mathbf{x}^{(i)}$ according as his corresponding data bit is +1 or -1, respectively. Thus, it is often desired that no sequence in a CDMA sequence set be the negative of another sequence, i. e., that $\mathbf{x}^{(i)} \neq -\mathbf{x}^{(j)}$ for all $i \neq j$ or, equivalently for the corresponding sequences in $GF(2)^L$, $\mathbf{b}^{(i)} \neq \mathbf{b}^{(j)} + \mathbf{1}$ for all $i \neq j$ where $\mathbf{1} = [1, 1, \ldots, 1]$ is the all-one

for all $i \neq j$ a *unipolar* sequence set. The following characterization is immediate.
Characterization of Unipolar Sequence Sets Corresponding to Linear Codes: The binary (±1 valued) sequence set correponding to a binary linear code V is unipolar if and only if the all-one word $\mathbf{1} = [1, 1, \ldots, 1]$ is *not* a codeword in V.

We illustrate the ideas of this section with two simple examples.

Example 1: Let $\mathbf{v}$ be a binary *maximal-length sequence* (or *m-sequence* or *pseudo-noise sequence*) of length $L = 2^m - 1$ where $m \geq 2$ [2, p. 222]. Let T denote the left cyclic shift operator. Then $\mathbf{0}, \mathbf{v}, T(\mathbf{v}), \ldots, T^{L-1}(\mathbf{v})$ are the codewords in a binary linear code V (for which $\mathbf{1}$ is not a codeword) with minimum distance $d = 2^{m-1}$ whose dual code $V^{\perp}$ is a Hamming code with minimum distance $d^{\perp} = 3$ [2, p. 223]. It follows from the Corollary that the binary (±1 valued) sequence set corresponding to V is a unipolar WBE sequence set of $M = L + 1$ sequences. It follows further from (4.2) that, when this sequence set is used in an S-CDMA system, the interuser interference experienced by user i has variance

$$\sigma^2(i) = L \tag{4.4}$$

for $1 \leq i \leq M$. [We note that the results in this simple example could also have been obtained by conventional arguments. The code V is an equidistant code in the sense that the Hamming distance between any of its two codewords is the same [2, p. 223], namely 2^{m-1}. This implies from (4.3) that

$$\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle = L - 2 \cdot 2^{m-1} = -1 \tag{4.5}$$

for all $i \neq j$, which then with the aid of the definition (2.5) gives (4.4).]

Example 2: Let α be a primitive element of the finite field $GF(2^4)$ [2, p. 158] and let V be the (L = 15, K = 6) Bose-Chaudhuri-Hocquenghem (BCH) code such that $\alpha^0 = 1$, α, and α^3 are zeroes of the generator polynomial g(X) of this code [2, p. 271]. This BCH code has minimum distance d = 6 [2, Appendix D] and the all-one vector $\mathbf{1}$ is not a codeword in this code. The dual code $V^{\perp}$ is a (15, 9) cyclic code with minimum distance $d^{\perp} = 3$ [2, Appendix D]. It follows from the Corollary that the binary (±1 valued) sequence set corresponding to V is a unipolar WBE sequence set of M = 64 sequences of length 15. It follows further from (4.2) that, when this sequence set is used in a S-CDMA system, the interuser interference experienced by user i has variance

$$\sigma^2(i) = 15\,(64 - 15) = 735 \tag{4.6}$$

for $1 \leq i \leq M$.

5 WBE-Preserving Transformation and Combination of Sequence Sets

We first consider operations on a sequence (multi-)set that preserve the WBE

Proposition 3: If the binary (±1 valued) sequences $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ of length L form a WBE sequence set or multi-set, then the sequence set or multi-set obtained by performing any of the following operations on the former set or multiset is also a WBE sequence set or multi-set:

(i) Replacing $\mathbf{x}^{(i)}$ by $-\mathbf{x}^{(i)}$ for any i;

(ii) Replacing $\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}, \ldots, x_L^{(i)}]$ by its left cyclic shift $T(\mathbf{x}^{(i)}) = [x_2^{(i)}, \ldots, x_L^{(i)}, x_1^{(i)}]$ for $1 \le i \le M$;

(iii) Replacing $\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}, \ldots, x_L^{(i)}]$ by its left *negacyclic shift* $N(\mathbf{x}) = [x_2^{(i)}, \ldots, x_L^{(i)}, -x_1^{(i)}]$ for $1 \le i \le M$;

(iv) Deleting the k-th component $x_k^{(i)}$ of $\mathbf{x}^{(i)}$ for $1 \le i \le M$ and for any k; and

(v) Replacing $\mathbf{x}^{(i)}$, which corresponds to $\mathbf{b}^{(i)}$ in $GF(2)^L$, by the binary (±1 valued) sequence corresponding to $\mathbf{b}^{(i)} + \mathbf{u}$ for $1 \le i \le M$ and any $\mathbf{u}$ in $GF(2)^L$.

Proof: Operation (i) changes only the sign of $\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle$ for all $j \ne i$ and hence does not alter the sum in (3.8). Operation (ii) causes the columns of the $M \times L$ array whose rows are $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ to be cyclically shifted, but this does not alter the orthogonality of the columns nor their equi-energy. Operation (iii) additionally changes the sign of one column in this array, but again this does not alter the orthogonality of the columns nor their equi-energy. Operation (iv) deletes one column of this array but again this does not alter the orthogonality nor the equi-energy of the remaining columns. Finally, operation (v) changes only the signs of those columns of the $M \times L$ array whose rows are $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ corresponding to positions in which $\mathbf{u}$ contains a 1, which clearly does not alter the orthogonality of the columns nor their equi-energy. o

Example 3: Adding any vector $\mathbf{u}$ in $GF(2)^L$ to the codewords of the linear code V of length $L = 2^m - 1$ considered in Example 1 gives the coset

$$\mathbf{u} + V = \{\mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{u} + T(\mathbf{v}), \ldots, \mathbf{u} + T^{L-1}(\mathbf{v})\},$$

which by Proposition 3(v) also corresponds to a WBE sequence set S of $M = 2^m$ sequences. We note that if m is not divisible by 4 and if the sequence $\mathbf{u}$ is the $(2^e + 1)$-st decimation of the m-sequence $\mathbf{v}$, then $\mathbf{u}$ is also an m-sequence and the corresponding binary (±1 valued) sequence set, when augmented with the sequence corresponding to $\mathbf{v}$ is a so-called *Gold sequence set* where the name honors the originator of these sequence sets [3]. Note however, that, for any choice of $\mathbf{u}$, the sequence set S is WBE. Note also that the full Gold sequence set cannot be WBE because it contains an odd number of sequences.

sets to produce larger ones.

Proposition 4: If $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ and $\mathbf{x}'^{(1)}, \mathbf{x}'^{(2)}, \ldots, \mathbf{x}'^{(M')}$ are both WBE sequence (multi-)sets containing M and M', respectively, binary (±1 valued) sequences of the same length L, then their "union" $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}, \mathbf{x}'^{(1)}, \mathbf{x}'^{(2)}, \ldots, \mathbf{x}'^{(M')}$ is a WBE sequence (multi-)set with M + M' sequences.

Proof: Let $\mathbf{y}^{(k)}$ and $\mathbf{y}'^{(k)}$ denote the k-th columns of the $M \times L$ and the $M' \times L$ arrays whose rows are $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ and $\mathbf{x}'^{(1)}, \mathbf{x}'^{(2)}, \ldots, \mathbf{x}'^{(M')}$, respectively. Then the k-th column of the $(M + M') \times L$ array for the "union" sequence set is $\mathbf{Y}^{(k)} = (\mathbf{y}^{(k)}, \mathbf{y}'^{(k)})$. Thus,

$$\langle \mathbf{Y}^{(l)}, \mathbf{Y}^{(k)} \rangle = \langle \mathbf{y}^{(l)}, \mathbf{y}^{(k)} \rangle + \langle \mathbf{y}'^{(l)}, \mathbf{y}'^{(k)} \rangle = 0$$

for $k \neq l$ so that the "union" of these two sequence sets in indeed WBE. o

Propositions 3 and 4 are very useful when constructing and/or analyzing sequence sets for various types of non-synchronous CDMA systems. We will illustrate this applicability with an example for so-called *quasi-synchronous CDMA*, which is defined in the same manner as S-CDMA in Section 2 except that there can now be a relative time misalignment of at most one chip between the symbols of any two users. Again we take the worst-case interuser interference experienced by any user over all admissible misalignments as the quantity to be minimized. A rather tedious argument that we will not repeat here shows that, for any user i, the worst interuser interference experienced by that user will occur when his symbol edge is either first or last among those of all M users and those other users are each either in full symbol synchronization with the specified user or exactly one chip misaligned with that user [4]. Assuming that L is large so that we can ignore whether the single chip from an adjacent expanded data symbol that overlaps the expanded data symbol of a specified user corresponds to a data bit with the same or with the opposite sign as that for the adjacent expanded data symbol whose L - 1 chips overlap the same expanded data symbol of the specified user, it follows that the worst interuser interference experienced by user i will have a variance

$$\sigma^2_{wc}(i) = \max_{\Delta \in \{-1,+1\}} \sum_{\substack{j=1 \\ j \neq i}}^{M} \max_{\theta \in \{0, \Delta\}} |\langle T^{\theta}(\mathbf{x}^{(j)}), \mathbf{x}^{(i)} \rangle|^2 \qquad (5.1)$$

where again T is the (left) cyclic shift operator. The sequence set should thus be chosen to minimize

$$\sigma^2_{wc} = \max_i \sigma^2_{wc}(i). \qquad (5.2)$$

Example 4: Let S be the WBE sequence set with $M = L + 1 = 2^m$ sequences corresponding to $\mathbf{u} + V$ in Example 3, where $\mathbf{u}$ is an arbitrary vector in $GF(2)^L$.

corresponding to T(V) be the set of left cyclic shifts of the sequences in S. By Proposition 4, the union sequence set U = S ∪ T(S) containing 2M sequences is also WBE. For the WBE sequence set U, (3.7) gives

$$2\sum_{i=1}^{M}\sum_{j=1}^{M}|\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)}\rangle|^2 + 2\sum_{i=1}^{M}\sum_{j=1}^{M}|\langle T(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 = (2M)^2 L, \tag{5.3}$$

where we have used the fact that $\langle T(\mathbf{x}^{(j)}), T(\mathbf{x}^{(i)})\rangle = \langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)}\rangle$. Now the first double sum on the left in (5.3) is just $M^2 L$, as follows from the fact that S is a WBE sequence set of M sequences. Moreover,

$$\sum_{j=1}^{M}|\langle T(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2$$

is independent of i, as follows from (4.3) and the fact that the linear code V is closed under cyclic shifting so that the Hamming distances from any vector in $\mathbf{u}$ + V to all the vectors in $T(\mathbf{u} + V) = T(\mathbf{u}) + T(V) = T(\mathbf{u}) + V$ does not depend on the particular choice of the former vector. It thus follows from (5.3) that

$$\sum_{j=1}^{M}|\langle T(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 = M L \tag{5.4}$$

for $1 \le i \le M$. But, because $\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)}\rangle = -1$ for all $i \ne j$ according to (4.5) and because $\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)}\rangle$ must have odd parity since L is odd, it follows that

$$\max_{\theta \in \{0, +1\}} |\langle T^{\theta}(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 = |\langle T(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 \tag{5.5}$$

holds for all $j \ne i$. An entirely similar argument for $\Delta = -1$, which again exploits the fact that V is closed under cyclic shifting, shows that

$$\sum_{j=1}^{M}|\langle T^{-1}(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 = M L \tag{5.6}$$

and that

$$\max_{\theta \in \{0, -1\}} |\langle T^{\theta}(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 = |\langle T^{-1}(\mathbf{x}^{(j)}), \mathbf{x}^{(i)}\rangle|^2 \tag{5.7}$$

also holds for all $j \ne i$. Because of (5.1), (5.4)-(5.7) and the fact that $|\langle T^{-1}(\mathbf{x}^{(i)}), \mathbf{x}^{(i)}\rangle| = |\langle T(\mathbf{x}^{(i)}), \mathbf{x}^{(i)}\rangle|$, it follows that

$$\sigma^2_{wc}(i) = M L - |\langle T(\mathbf{x}^{(i)}), \mathbf{x}^{(i)}\rangle|^2 \tag{5.8}$$

for $1 \le i \le M$. We see from (5.8) that the worst user will be that user i for which the "autocorrelation" magnitude $|\langle T(\mathbf{x}^{(i)}), \mathbf{x}^{(i)}\rangle|$ is *smallest*. But, for every i, the fact that L

$$1 \leq |\langle T(\mathbf{x}^{(i)}), \mathbf{x}^{(i)} \rangle| \leq L \tag{5.9}$$

with equality on the left when $\mathbf{x}^{(i)}$ corresponds to an m-sequence, as it would, for instance, for that user whose sequence corresponds to the additive vector $\mathbf{u}$ when $\mathbf{u}$ is an m-sequence (as it is in the Gold sequence set). We conclude then from (5.2), (5.8), (5.9) and the fact that $M = L + 1$ that

$$L \leq \sigma^2_{wc} \leq L^2 + L - 1 \tag{5.10}$$

with equality on the right if $\mathbf{u}$ is an m-sequence (and hence if S is the Gold sequence set). It may come as a small surprise to some readers that the Gold sequence set gives the poorest worst-case performance among the sequence sets corresponding to different choices of the vector $\mathbf{u}$. What is more significant is that (5.10) applies for any $L = 2^m - 1$ with $m \geq 2$; there is no requirement that m not be divisible by 4 as is required for the Gold sequence set to exist.

6 Remarks

We have given rather abundant evidence to show the importance of sequence (multi-)sets that achieve equality in Welch's bound and we have shown that such sequence sets are surprisingly easy to construct. There seems no reason, in most CDMA systems, to settle for a sequence (multi-)set that does not achieve equality in Welch's bound.

It may come as a major surprise to some readers that the sequence set corresponding to *any* binary linear code V whose dual code has minimum distance at least 3 corresponds to a WBE sequence set and hence is optimum for use in S-CDMA systems. There is no requirement that the code V have any other special distance properties, as would be required for instance if one attempted to make the "crosscorrelation" magnitude $|\langle \mathbf{x}^{(j)}, \mathbf{x}^{(i)} \rangle|$ small for all $j \neq i$. Such an attempt requires, by (4.3), that the Hamming distance $d(\mathbf{b}^{(j)}, \mathbf{d}^{(i)})$ between the corresponding codewords in V be made as near to $L/2$ as possible for all $j \neq i$, or equivalently that the Hamming weights of the non-$\mathbf{0}$ codewords be made as near as possible to $L/2$. The reader may object that if these crosscorrelations are not as nearly uniformly small in magnitude as possible, then the validity of invoking the central-limit theorem to justify the assumption that the interuser interference $\xi_k^{(i)}$ in (2.4) is Gaussian becomes suspect. We would counter by pointing out that, for a given variance, a Gaussian random variable has the maximum possible entropy [5, Section 20.5]. Thus, the channel created for user i by the S-CDMA system and in which $\xi_k^{(i)}$ is an additive noise term actually has its *minimum capacity* when $\xi_k^{(i)}$is Gaussian. For a given variance of the interuser interference, its non-Gaussianness (if properly exploited) is a virtue, not a vice!

Acknowledgment

The research reported here was supported by the European Space Research and Technology Centre (ESTEC) in Noordwijk, The Netherlands, under ESTEC Contract

DeGaudenzi of ESTEC are gratefully acknowledged.

References

[1] L. R. Welch, "Lower Bounds on the Maximum Cross Correlation of Signals," *IEEE Trans. on Information Theory*, vol. IT-20, pp. 397-399, May 1974.

[2] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes* (2nd Ed.). Cambridge, Mass.: M.I.T. Press, 1972.

[3] R. Gold, "Optimal Binary Sequences for Spread-Spectrum Multiplexing," *IEEE Trans. on Information Theory*, vol. IT-13, pp. 619-621, October 1967.

[4] J. L. Massey and T. Mittelholzer, Final Report ESTEC Contract No. 8696/89/NL/US: Technical Assistance for the CDMA Communication System Analysis, Signal and Information Processing Laboratory, Swiss Federal Institute of Technology, Zürich, Switzerland, 19 March 1991.

[5] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, pp. 379-423 and pp. 623-656, July and October, 1948.