Published in IET Communications
Received on 15th July 2012
Revised on 16th August 2013
Accepted on 20th August 2013
doi: 10.1049/iet-com.2013.0344

ISSN 1751-8628

Generalisation of code division multiple access systems and derivation of new bounds for the sum capacity

Shayan Dashmiz[1], Mohammad Reza Takapoui[2], Sajjad Moazeni[3], Mehrdad Moharrami[4], Melika Abolhasani[5], Farokh Marvasti[4]

[1]*Department of Finance, London School of Economics and Political Sciences, London WC2A 2AE, UK*
[2]*Electrical Engineering Department, Stanford University, Stanford, CA 94305, USA*
[3]*Electrical Engineering and Computer Science Department, University of California at Berkeley, Berkeley, CA 94720-1770, USA*
[4]*Advanced Communication Research Institute (ACRI), Department of EE, Sharif University of Technology, Tehran 1455618181, Iran*
[5]*Department of Computer Science, University of Maryland, College Park, MA 20742, USA*
E-mail: smoazeni@berkeley.edu

Abstract: In this study, the authors explore a generalised scheme for the synchronous code division multiple access (CDMA). In this scheme, unlike the standard CDMA systems, each user has different codewords for communicating different messages. Two main problems are investigated. The first problem concerns whether uniquely detectable overloaded matrices (an injective matrix, i.e. the inputs and outputs are in one-to-one correspondence depending on the input alphabets) exist in the absence of additive noise, and if so, whether there are any practical optimum detectors for such input codewords. The second problem is about finding tight bounds for the sum channel capacity. In response to the first problem, the authors have constructed uniquely detectable matrices for the generalised scheme and the authors have developed practical maximum likelihood detection algorithms for such codes. In response to the second problem, lower bounds and conjectured upper bounds are derived. The results of this study are superior to other standard overloaded CDMA codes since the generalisation can support more users than the previous schemes.

1 Introduction

Multiple access communication systems were first studied by Shannon. Moreover, different schemes of multiple access systems such as code division multiple access (CDMA) systems were introduced and explored in [1].

In general, users for CDMA systems send either binary or non-binary data. In our present paper, we use a more generalised concept of user data. Each user has a set of codewords which do not necessarily construct a linear code. We intend to study two main issues related to such generalised CDMA (GCDMA) systems. The first problem is to find uniquely detectable overloaded GCDMA matrices and the second issue is related to the development of tight lower and upper bounds for the sum channel capacity of such a GCDMA system. We, as well as other authors [2, 3], have already studied these two issues for the standard binary and non-binary CDMA systems:

In [2, 4, 5], a class of overloaded uniquely detectable matrices for binary multiuser and binary/ternary signatures for wireless and optical applications were developed. Mow [4] presented a unifying approach to find one-to-one binary and ternary matrices for binary inputs for multiuser applications. He also applied constructive theorems developed by the previous authors [6, 7] to enlarge such matrices; this paper also discusses asymptotic behaviour of such matrices. In [2], the authors have also developed uniquely detectable overloaded matrices for binary inputs independently. In the continuation of [2], the authors extended these matrices in [2] to non-binary finite real and complex signature codes [8].

The theoretical developments in CDMA sum capacity have been limited to users with Gaussian inputs where Welch Bound Equality (WBE) codes achieve the theoretical capacity [9, 10]. For binary CDMA, only asymptotic results were known [11, 12] prior to our recent papers [2, 8, 13]. For non-binary finite input and signature alphabets, asymptotic sum capacity results were developed in [3].

The GCDMA scheme consists of a family of codes (S_1, S_2, …, S_n). Each S_i is a set of $m \times 1$ vectors, which are called codewords, namely $S_i = \left\{A^{(i1)}, A^{(i2)}, ..., A^{(il_i)}\right\}$, where $A^{(ij)}$ is an $m \times 1$ vector. At synchronous time slots, the ith user transmits one of the vectors from the set S_i. A code family (S_1, S_2,…, S_n) is said to be 'uniquely decodable' if all the sums of n vectors $A^{(ij)}$ $(1 \le j \le l_i)$, each from a different

© The Institution of Engineering and Technology 2014

code, are distinct. In the absence of noise, the transmitted user vectors can be detected uniquely from the received vector. Binary version of this scheme is also known as T-user and is studied by the authors in [14, 15]. In [14], a class of uniquely decodable codes is introduced for the binary case using iterative methods and the proposed decoder was only for the noiseless case which is not computationally practical. Also, the lower and upper bounds for the sum capacity of such a scheme are derived for the binary signature. In [15], the authors introduced a tighter upper bound for the T-user binary case. Ferguson [16] introduced a generalised code construction method for binary T-user.

In our present paper, we will construct a class of uniquely decodable overloaded codes with practical maximum likelihood (ML) decoders. Unlike the previous authors on the T-user schemes that only considered binary and noiseless cases, we will also propose tighter lower bounds for the sum capacity of our generalised systems that include non-binary and noisy cases. We will also demonstrate that higher sum capacities can be achieved using our proposed scheme as opposed to the standard CDMA systems.

The rest of the paper is organised as follows: in Section 2, the main characteristics of a GCDMA system are defined. In Section 3, the uniquely decodable codes and their ML decoding schemes are introduced and compared with the previous methods. In Section 4, we will develop tight lower and upper bounds for a GCDMA system with some numerical results. In Section 5, the conclusion and future works will be presented.

2 Preliminaries

In a CDMA system, each of the n users multiplies its data by an m-chip vector, namely the signature vector, in order to transmit the user data. The signature vectors belong to the set $\mathcal{S}^m$, where $\mathcal{S}$ is the set of signature alphabets. Since the baseband information spreads over the frequency spectrum by a factor of m in CDMA systems, m is also called the spreading factor or the gain. The channel model, under the assumption of user synchronisation, is

$$\boldsymbol{Y} = \frac{1}{\sqrt{m}}\boldsymbol{C}\boldsymbol{W} + \boldsymbol{N} \tag{1}$$

where $\boldsymbol{C}$ is the signature matrix whose columns are the signature vectors of the users, $\boldsymbol{W}$ is the input vector, $\boldsymbol{Y}$ is the observed vector at the receiver end and $\boldsymbol{N} = [N_1, N_2, ..., N_m]^{\mathrm{T}}$, where N_i's are independent and identically distributed (i.i.d) random variables of variance σ_f^2 with pdf $f(.)$, is the noise vector. Since the total user powers and the noise in the above model are, respectively, equal to $\mathrm{tr}\left(\mathbb{E}\left(\frac{1}{m}\boldsymbol{C}\boldsymbol{W}\boldsymbol{W}^*\boldsymbol{C}^*\right)\right)$ and $\mathbb{E}\left(\boldsymbol{N}^*\boldsymbol{N}\right)$ (the symbol * stands for the Hermitian transpose), the multiuser signal-to-noise ratio (SNR) is defined as

$$\mathrm{SNR} = \frac{\mathrm{tr}\left(\mathbb{E}\left((1/m)\boldsymbol{C}\boldsymbol{W}\boldsymbol{W}^*\boldsymbol{C}^*\right)\right)}{\mathbb{E}(\boldsymbol{N}^*\boldsymbol{N})} \tag{2}$$

Since $\mathbb{E}\left(\boldsymbol{N}^*\boldsymbol{N}\right) = m\sigma_f^2$, the SNR definition can be written as

$$\mathrm{SNR} = \frac{1}{m\sigma_f^2}\mathrm{tr}\left(\mathbb{E}\left(\frac{1}{m}\boldsymbol{C}\boldsymbol{W}\boldsymbol{W}^*\boldsymbol{C}^*\right)\right) \tag{3}$$

Now, we define the normalised SNR as

$$\eta = \frac{m}{n}\mathrm{SNR} \tag{4}$$

The sum capacity for a CDMA system is defined as

$$\mathcal{C}\left(m, n, \mathcal{I}, \mathcal{S}, \eta\right) = \max_{C\in\mathcal{M}_{m\times n}(\mathcal{S})} \max_{p(w_1),p(w_2),\ldots,p(w_n)} \mathbb{I}(\boldsymbol{W}; \boldsymbol{Y}) \tag{5}$$

where $\mathcal{I}$ is the set of input alphabets, $\mathcal{M}_{m\times n}(\mathcal{S})$ is the set of all $m\times n$ matrices with entries from $\mathcal{S}$, and $\boldsymbol{W} = [w_1, w_2, \ldots, w_n]^{\mathrm{T}} \in \mathcal{I}^n$.

If $t = |\mathcal{I}|$, where $|.|$ stands for the cardinality of the set, we define a GCDMA system to be a system with n users in which the ith user has a set of t signature vectors, namely $S_i = \left\{A^{(i1)}, A^{(i2)}, ..., A^{(it)}\right\}$ such that $A^{(ij)} \in \mathcal{S}^m$ for $1 \le j \le t$ and $1 \le i \le n$. In order to transmit the jth symbol, the ith user sends $A^{(ij)}$. Our channel model for this system, assuming synchronisation, is

$$\boldsymbol{Y} = \frac{1}{\sqrt{m}}\boldsymbol{A}\boldsymbol{X} + \boldsymbol{N} \tag{6}$$

where $\boldsymbol{N} = [N_1, N_2, ..., N_m]^{\mathrm{T}}$, and N_i's are i.i.d random variables with pdf $f(.)$. Also, $\boldsymbol{Y}$ is the observed vector at the receiver and $\boldsymbol{A}$ is an $m\times nt$ signature matrix in which the column numbers from $(i-1)t+1$ to it for $1 \le i \le n$ are the elements of S_i, respectively. The input vector $\boldsymbol{X}$ is an $nt\times 1$ vector. The ith block in the input vector is defined to be the entries with indices $(i-1)t+1$ to it for $1 \le i \le n$. The entries in each block are all zero except in one position, which is equal to one. The index of the non-zero entry in the ith block represents the transmitted signature vector of the ith user. Hence, the output is the sum of n signature vectors.

In the noiseless case, a signature matrix $\boldsymbol{A}$ is called 'uniquely detectable', if all the t^n observed vectors are distinct. The sum capacity of GCDMA systems is defined as

$$\mathcal{GC}\left(m, n, \mathcal{S}, |\mathcal{I}|, \eta\right) = \max_{\boldsymbol{A}\in\boldsymbol{M}_{m\times nt}(\mathcal{S})} \max_{p(X)} \mathbb{I}(\boldsymbol{X}; \boldsymbol{Y}) \tag{7}$$

where the normalised SNR (η) is defined as shown in (4). In the noiseless case, η in the above channel capacity function is omitted.

3 Codes for GCDMA systems

In this section, we extend the class of generalised codes for overloaded CDMA systems (GCO) defined in [8] to GCDMA systems; these uniquely decodable codes for GCDMA scheme are called the generalised user CDMA (GUC) codes. An $m\times n$ matrix $\boldsymbol{C}$, with entries in $\mathcal{S}$ is called a GCO($m, n, \mathcal{I}, \mathcal{S}$) matrix if the mapping of $\boldsymbol{Y} = \boldsymbol{C}\boldsymbol{W}$ is injective when it is restricted to the input vectors with entries in $\mathcal{I}$. The proposed codes are uniquely decodable in the absence of noise. We will discuss the construction of GUC codes with the ML decoding and demonstrate some numerical results.

3.1 Construction of GUC codes

Suppose we have n users, where each user has t vectors with entries from the signature $\mathcal{S}$ with a chip rate of m. Each user uses one of the t vectors in order to send one of the t

© The Institution of Engineering and Technology 2014

doi: 10.1049/iet-com.2013.0344

messages. If such uniquely decodable codes exist, it is called GUC(n, m, t, $\mathcal{S}$). In this section, we will provide theorems for constructing GUC's for GCDMA systems.

The following theorem completely relates the case $t=2$ in GUC codes to the previous GCO codes discussed in [8].

Theorem 1: A GCO(m, n, $\{\pm 1\}$, $\mathcal{S}-\mathcal{S}$) matrix exists if and only if a GUC(m, n, 2, $\mathcal{S}$) code exists, where $\mathcal{S}-\mathcal{S}=\{x-y|x,y\in\mathcal{S}\}$.

Proof: Let $\boldsymbol{C}\in\mathcal{M}_{m\times n}(\mathcal{S}-\mathcal{S})$ be a GCO matrix with $\mathcal{I}=\{\pm 1\}$. Hence the ith column of $\boldsymbol{C}$ can be written as $\boldsymbol{v}_i-\boldsymbol{u}_i$, where $\boldsymbol{v}_i$ and $\boldsymbol{u}_i$ belong to $\mathcal{S}^m$. If we construct $\boldsymbol{A}\in\mathcal{M}_{m\times 2n}(\mathcal{S})$ such that $\boldsymbol{v}_i$ and $\boldsymbol{u}_i$ are the vectors of the ith user, then $\boldsymbol{A}$ will be a GUC matrix. We simply note that the ith user vectors are equal to $(\boldsymbol{v}_i+\boldsymbol{u}_i)/2+w_i(\boldsymbol{v}_i-\boldsymbol{u}_i)/2$, where w_i can be ± 1. Then we can model the channel as

$$\boldsymbol{Y}=\boldsymbol{C}\boldsymbol{W}+Y_0 \tag{8}$$

where $Y_0=\sum_{i=1}^{n}\dfrac{\boldsymbol{v}_i+\boldsymbol{u}_i}{2}$. Since $\boldsymbol{C}$ is injective on $\pm 1^n$, the transmission is uniquely decodable. Thus, $\boldsymbol{v}_i$ and $\boldsymbol{u}_i$ form a GUC matrix. Inversely, a GCO matrix with $\mathcal{I}=\{\pm 1\}$ can be obtained from a GUC code by putting the ith column equal to $\boldsymbol{v}_i-\boldsymbol{u}_i$. □

Example 1: Assume $\mathcal{S}=\{\pm 1\}$ and $m=64$. Applying Theorem 1 on a GCO(64, 256, $\{\pm 1\}$, $\{0, \pm 1\}$) matrix, we can obtain a GUC(64, 256, 2, $\mathcal{S}$). By comparing with the GCO(64, 193, $\{\pm 1\}$, $\mathcal{S}$), for a fixed chip rate and signature set, the total number of users is increased as expected.

In the next theorem, a recursive method is proposed for constructing large GUC codes from smaller ones. With this theorem, it is easy to show that the overloading factor n/m tends to infinity for large values of m for a fixed value of t and alphabets of $\mathcal{S}$.

Theorem 2: Assume a GUC(m, n, t, $\mathcal{S}$) exists. Then, we can obtain a GUC($2m$, $2n+l$, t, $\mathcal{S}$) if $l\times\log_2 t\le m$.

Proof: We first present a simpler case as a lemma:

Lemma 1: Let $\boldsymbol{C}$ be a GUC(m, n, t, $\{\pm 1\}$) and let $\boldsymbol{D}=H_w\otimes\boldsymbol{C}$ for $w=2^k$. Then, $\boldsymbol{D}$ is a GUC(mw, nw, t, $\{\pm 1\}$) matrix.

Proof of lemma 1: The lemma can be proved by induction on k. If $k=1$, then $\boldsymbol{D}=\begin{bmatrix}\boldsymbol{C} & \boldsymbol{C}\\ \boldsymbol{C} & -\boldsymbol{C}\end{bmatrix}$. Suppose $\boldsymbol{D}\boldsymbol{X}_1=\boldsymbol{D}\boldsymbol{X}_2$ where $\boldsymbol{X}_1=\begin{bmatrix}X_{1_1} & X_{1_2}\end{bmatrix}^{\mathrm{T}}$ and $\boldsymbol{X}_2=\begin{bmatrix}X_{2_1} & X_{2_2}\end{bmatrix}^{\mathrm{T}}$ are input vectors, according to definition, such that $\boldsymbol{X}_{i_j}$ is an $nt\times 1$ vector. Hence

$$\boldsymbol{C}\left(X_{1_1}+X_{1_2}\right)=\boldsymbol{C}\left(X_{2_1}+X_{2_2}\right)$$
$$\boldsymbol{C}\left(X_{1_1}-X_{1_2}\right)=\boldsymbol{C}\left(X_{2_1}-X_{2_2}\right)$$

By adding and subtracting the two equations and using the fact that $\boldsymbol{C}$ is a GUC matrix, results in $\boldsymbol{X}_1=\boldsymbol{X}_2$. This proves the case for $k=1$.

Now by induction and according to the fact $H_{2^k}=H_2\otimes H_2\otimes H_2\otimes\ldots\otimes H_2$, it arises that $\boldsymbol{D}$ is a GUC ($2m$, $2n$, t, ± 1) matrix. □

From this lemma we conclude the following. Consider the new l users and suppose $V_{i,j}$ is the jth signature of the ith new user ($i\le l, j\le t$). Let $V_{ij}=\left[V_{i,j,1}^{\mathrm{T}}, V_{i,j,2}^{\mathrm{T}}, \ldots, V_{i,j,w}^{\mathrm{T}}\right]^{\mathrm{T}}$ such that $\boldsymbol{V}_{i,j,p}$ is an$m\times 1$ vector and $V_{i,j,\mathrm{sum}}=\sum_t V_{i,j,t}$. Now suppose that $V_i=[V_{i,1}, V_{i,2}, V_{i,3}, \ldots, V_{i,\ t}]$, satisfies the following conditions for each i:

(1) The $(i-1)\times\lceil\log_w t\rceil+1$ to $i\times\lceil\log_w t\rceil$ elements of $V_{i_{j_{\mathrm{sum}}}}$ are from set $\mathcal{B}$ for different values of j.

$$\mathcal{B}=\{-w+2,\ -w+4,\ \ldots,0,\ \ldots,w-2,w\}$$

(2) For different values of j, the subvectors consisting of $(i-1)\times\lceil\log_w t\rceil+1$ to $i\times\lceil\log_w t\rceil$ entries of $V_{i,j,\mathrm{sum}}$ are all different.

(3) $V_{i,\ j,\mathrm{sum}}$ is zero in other elements for every j.

Note that according to Lemma 1 such V_{i_j}'s exist.

To prove Theorem 2, it is sufficient to show that if $\boldsymbol{D}=[\boldsymbol{H}_w\otimes\boldsymbol{C}/Z]$, where $Z=[V_1, V_2, V_3,\ldots, V_l]$ and $\boldsymbol{C}$ is a GUC(m, n, t, $\{\pm 1\}$) matrix, then $\boldsymbol{D}$ is GUC(wm, $wn+l$, t, $\{\pm 1\}$).

Suppose that there are two different input vectors $\boldsymbol{X}_1$ and $\boldsymbol{X}_2$ such that

$$\boldsymbol{D}\boldsymbol{X}_1=\boldsymbol{D}\boldsymbol{X}_2$$

Note that

$$\boldsymbol{D}\boldsymbol{X}_1=\begin{bmatrix}\boldsymbol{C} & \boldsymbol{C} & \ldots & \boldsymbol{C} & Z_1\\ \boldsymbol{C} & \boldsymbol{C} & \ldots & \boldsymbol{C} & Z_2\\ \boldsymbol{C} & \boldsymbol{C} & \ldots & \boldsymbol{C} & Z_3\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \boldsymbol{C} & \boldsymbol{C} & \ldots & \boldsymbol{C} & Z_w\end{bmatrix}\begin{bmatrix}X_1\\ X_2\\ X_3\\ \vdots\\ X_w\\ Y\end{bmatrix}$$

such that Z_i contains $(i-1)\times m$th row to $i\times m$th row of Z and $\boldsymbol{X}_i$ is $nt\times 1$ vectors for each i ($1\le i\le w$) and $\boldsymbol{Y}$ is a $lt\times 1$ vector. It results in

$$\boldsymbol{D}\boldsymbol{X}_1=\begin{bmatrix}X_{1,1}+X_{1,2}+\ldots+X_{1,w}+Y_{1,1}\\ X_{1,1}-X_{1,2}+\ldots-X_{1,w}+Y_{1,2}\\ X_{1,1}+X_{1,2}-\ldots-X_{1,w}+Y_{1,3}\\ \vdots\qquad\vdots\qquad\vdots\qquad\vdots\qquad\vdots\\ X_{1,1}-X_{1,2}+\ldots+X_{1,w}+Y_{1,w}\end{bmatrix}$$

Such that $X_{1,i}=\boldsymbol{C}\times\boldsymbol{X}_i$ and $Y_{1,i}=Z_i\times\boldsymbol{Y}$. Then if $\boldsymbol{D}\boldsymbol{X}_1=\boldsymbol{D}\boldsymbol{X}_2$

$$\begin{array}{ccccccccc}A_1+A_2+\ldots+A_w+B_1=0\\ A_1-A_2+\ldots-A_w+B_2=0\\ A_1+A_2-\ldots-A_w+B_3=0\\ \vdots\qquad\vdots\qquad\vdots\qquad\vdots\qquad\vdots\qquad\vdots\\ A_1-A_2+\ldots+A_w+B_w=0\end{array}$$

Such that $A_i=X_{1,i}-X_{2,i}$ and $B_i=Y_{1,i}-Y_{2,i}$. Note that

$$\begin{bmatrix}A_1 & A_2 & A_3 & \ldots & A_w\end{bmatrix}\times H'_w=\begin{bmatrix}B_1 & B_2 & B_3 & \ldots & B_w\end{bmatrix}$$
$$\Rightarrow\begin{bmatrix}A_1 & A_2 & A_3 & \ldots & A_w\end{bmatrix}\times wI_n$$
$$=\begin{bmatrix}B_1 & B_2 & B_3 & \ldots & B_w\end{bmatrix}\times H_w$$

© The Institution of Engineering and Technology 2014

Hence, we obtain that term $\sum_i (-1)^{\alpha} B_i$ for $\alpha \in \{0, 1\}$ is divisible by $2w$. However, according to the construction of B_i's each element of them is less than $2w$. Thus, the summation must be zero. However, we know that $H_w \otimes \boldsymbol{C}$ is GUC(wm, wn, t, $\{\pm 1\}$) as mentioned in theorem. □

Example 2: Applying Theorem 2, we deduce that a GUC($2m$, $2n + \lceil m/\log_2 3 \rceil$, 3, $\{\pm 1\}$) can be obtained from GUC(m, n, 3, $\{\pm 1\}$). By starting from $n = 1$ and $m = 2$, we achieve a GUC (64, 112, 3, $\{\pm 1\}$). Comparing GCO codes with $m = 64$ and $n = 103$, we conclude that GCDMA systems codes can support more users than traditional CDMA systems.

In the next section, we provide an ML decoding of the proposed codes for GCDMA systems.

3.2 ML decoding scheme for a subclass of GUC codes

In this section, we propose an ML decoding algorithm for the cases $t = 2$ and $t = 3$, which correspond to the binary and ternary inputs, respectively.

(1) *Case 1.* $t = 2$: As stated in Theorem 1, a GCDMA system using a GCO matrix can be modelled as

$$\boldsymbol{Y} = \boldsymbol{C}\boldsymbol{W} + Y_0 + \boldsymbol{N} \tag{9}$$

where $\boldsymbol{C}$ is an $m \times n$ matrix with $(\boldsymbol{v}_i - \boldsymbol{u}_i)/2$ as its ith column, $Y_0 = \sum (\boldsymbol{v}_i + \boldsymbol{u}_i)/2$ and $\boldsymbol{N}$ is the noise vector which has a Gaussian distribution with zero mean and auto-covariance matrix $\boldsymbol{\sigma}^2 \boldsymbol{I}$ ($\boldsymbol{I}$ denotes the identity matrix). If the codes are made according to Theorem 1, then $\boldsymbol{C}$ is a ternary GCO (GCO(n, m, $\{\pm 1\}$, $\{0, \pm 1\}$)) matrix and can be obtained from smaller ternary GCO matrices. To implement ML decoding, the term $\|\boldsymbol{Y} - \boldsymbol{C}\hat{W} - Y_0\|_2$ must be minimised, where $\hat{W} \in \{\pm 1\}^n$.

In the first step, we reduce the problem into a set of decoding problems with smaller code matrices. Consider a GCO matrix $\boldsymbol{C}_{wl \times wk} = \boldsymbol{H}_w \otimes \boldsymbol{D}_{l \times k}$ generated by the Kronecker product of a Hadamard matrix $\boldsymbol{H}$ with a smaller ternary GCO matrix $\boldsymbol{D}$. The received vector is

$$\boldsymbol{Y} = \boldsymbol{C}\boldsymbol{W} + Y_0 + \boldsymbol{N} = (\boldsymbol{H}_w \otimes \boldsymbol{D})\boldsymbol{W} + Y_0 + \boldsymbol{N} \tag{10}$$

Then we multiply both sides by

$$\left(\boldsymbol{H}_w^{-1} \otimes \boldsymbol{I}\right)\boldsymbol{Y} = (\boldsymbol{I} \otimes \boldsymbol{D})\boldsymbol{W} + \left(\boldsymbol{H}_w^{-1} \otimes \boldsymbol{I}\right)\left(Y_0 + \boldsymbol{N}\right) \tag{11}$$

depends only on the first k elements of $\boldsymbol{W}$ and the first l elements of $\left(\boldsymbol{H}_w^{-1} \otimes \boldsymbol{I}\right)(Y_0 + \boldsymbol{N})$; the second l elements of $\left(\boldsymbol{H}_w^{-1} \otimes \boldsymbol{I}\right)\boldsymbol{Y}$depends only on the second k elements of $\boldsymbol{W}$ and the second l elements of $\left(\boldsymbol{H}_w^{-1} \otimes \boldsymbol{I}\right)(Y_0 + \boldsymbol{N})$ and so on. Hence, we have divided the problem of decoding a GUC system with $m = rl$ and $n = rk$ to decoding r GUC systems with $m = l$ and $n = k$. If the decoding of smaller systems is ML, then the decoding of larger matrix is also ML.

In the second step, we will further reduce the complexity of the decoding. By permutation of $\boldsymbol{D}$, we can assume that $\boldsymbol{D} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \end{bmatrix}$, where $\boldsymbol{A}$ is an $l \times l$ unitary matrix and $\boldsymbol{B}$ is an $l \times (k - l)$ matrix. We have

$$\begin{aligned} \boldsymbol{Y} = \boldsymbol{D}\boldsymbol{W} + Y_0 + \boldsymbol{N} &= \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \end{bmatrix}\begin{bmatrix} \boldsymbol{W}_1 & \boldsymbol{W}_2 \end{bmatrix}^{\mathrm{T}} \\ &+ Y_0 + \boldsymbol{N} = \boldsymbol{A}\boldsymbol{W}_1 + \boldsymbol{B}\boldsymbol{W}_2 + Y_0 + \boldsymbol{N} \end{aligned} \tag{12}$$

where $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are column vectors of length l and $k - l$, respectively. Multiplying both sides by $\boldsymbol{A}^{-1}$, we obtain

$$\boldsymbol{A}^{-1}\left(\boldsymbol{Y} - Y_0\right) = \boldsymbol{W}_1 + \boldsymbol{A}^{-1}\boldsymbol{B}\boldsymbol{W}_2 + \boldsymbol{A}^{-1}\boldsymbol{N} \tag{13}$$

Thus, the decoding algorithm leads to solving the following optimisation problem

$$\min_{\hat{W}_1, \hat{W}_2} \left\| \boldsymbol{A}^{-1}\left(\boldsymbol{Y} - Y_0\right) - \boldsymbol{A}^{-1}\boldsymbol{B}\hat{W}_2 - \hat{W}_1 \right\|_2 \tag{14}$$

Instead of looking through all possibilities for $\boldsymbol{W} = [\boldsymbol{W}_1 \boldsymbol{W}_2]^{\mathrm{T}}$, we can search among 2^{k-l} possibilities of $\hat{W}_2$ and obtain

$$\hat{W}_1 = \mathrm{sign}\left(\boldsymbol{A}^{-1}\left(\boldsymbol{Y} - Y_0\right) - \boldsymbol{A}^{-1}\boldsymbol{B}\hat{W}_2\right) \tag{15}$$

where sign(z) is obtained by substituting the positive entries of z by 1 and the negatives by -1. Since $\boldsymbol{A}$ is unitary, this decoding algorithm is ML.

Example 3: The direct implementation of the ML decoding of a GUC matrix $\boldsymbol{C}_{64 \times 160} = \boldsymbol{H}_8 \otimes \boldsymbol{D}_{8 \times 20}$ requires about 2^{160} comparisons of vectors, which is an NP-hard problem. However, using the stated scheme, the complexity of decoding is $8 \times 2^{12} = 2^{15}$.

(2) *Case 2.* $t = 3$: In this case, each user has three signature vectors, namely $\boldsymbol{v}_i$, $\boldsymbol{u}_i$, and $\boldsymbol{w}_i$. Thus, each user vector can be written as $(\boldsymbol{v}_i + \boldsymbol{w}_i)/2 + x_i(\boldsymbol{v}_i - \boldsymbol{u}_i)/2 + y_i(\boldsymbol{w}_i - \boldsymbol{u}_i)/2$, where $\begin{bmatrix} x_i & y_i \end{bmatrix}^{\mathrm{T}}$ can be $\begin{bmatrix} 1 & -1 \end{bmatrix}^{\mathrm{T}}$, $\begin{bmatrix} -1 & -1 \end{bmatrix}^{\mathrm{T}}$ or $\begin{bmatrix} -1 & 1 \end{bmatrix}^{\mathrm{T}}$ to form $\boldsymbol{v}_i$, $\boldsymbol{u}_i$, and $\boldsymbol{w}_i$, respectively.

Hence, we model the channel as $\boldsymbol{Y} = \boldsymbol{C}\boldsymbol{W} + Y_0 + \boldsymbol{N}$, which is similar to the previous case except that $\boldsymbol{C}$ is an $m \times 2n$ matrix with columns of $(\boldsymbol{v}_i - \boldsymbol{u}_i)/2$ and $(\boldsymbol{w}_i - \boldsymbol{u}_i)/2$; $\boldsymbol{W}$ is in the form of $[z_1, \ldots, z_n]^{\mathrm{T}}$, where each $z_i = \begin{bmatrix} x_i & y_i \end{bmatrix}^{\mathrm{T}}$ can be $\begin{bmatrix} 1 & -1 \end{bmatrix}^{\mathrm{T}}$, $\begin{bmatrix} -1 & -1 \end{bmatrix}^{\mathrm{T}}$ or $\begin{bmatrix} -1 & 1 \end{bmatrix}^{\mathrm{T}}$. The first step in Case 1 can be also implemented here, but the second step must be modified to suit this case.

$\boldsymbol{A}$ and $\boldsymbol{B}$ are $m \times m$ and $m \times (2n - m)$ matrices; also $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are $m \times 1$ and $(2n - m) \times 1$ vectors, respectively. Instead of obtaining $\boldsymbol{W}_1$ from (15), we have to find the nearest vector of the form $[z_1, \ldots, z_{m/2}]^{\mathrm{T}}$ from $E = \boldsymbol{A}^{-1}(\boldsymbol{Y} - Y_0) - \boldsymbol{A}^{-1}\boldsymbol{B}\boldsymbol{W}_2$. To find such a vector we have to decompose E into $[e_1, \ldots, e_{m/2}]^{\mathrm{T}}$, where e_i consists of the $(2i - 1)$th and $(2i)$th elements of E. Thus, z_i can be obtained from

$$z_i = \begin{cases} [-1 \quad 1]^{\mathrm{T}}, & \text{if } 0 \le y_i \quad \text{and } x_i < y_i \\ [-1 \quad -1]^{\mathrm{T}}, & \text{if } x_i \le 0 \quad \text{and } y_i \le 0 \\ [1 \quad -1]^{\mathrm{T}}, & \text{if } 0 \le x_i \quad \text{and } y_i < x_i \end{cases}$$

The rest of the algorithm is the same as the one in Case 1. Hence, we can decode a GUC(wm, wn, 3, $\{\pm 1\}$) (which is formed by Kronecker product of a Hadamard matrix of size w with a GUC(m, n, 3, $\{\pm 1\}$)) with the complexity of

© The Institution of Engineering and Technology 2014

doi: 10.1049/iet-com.2013.0344

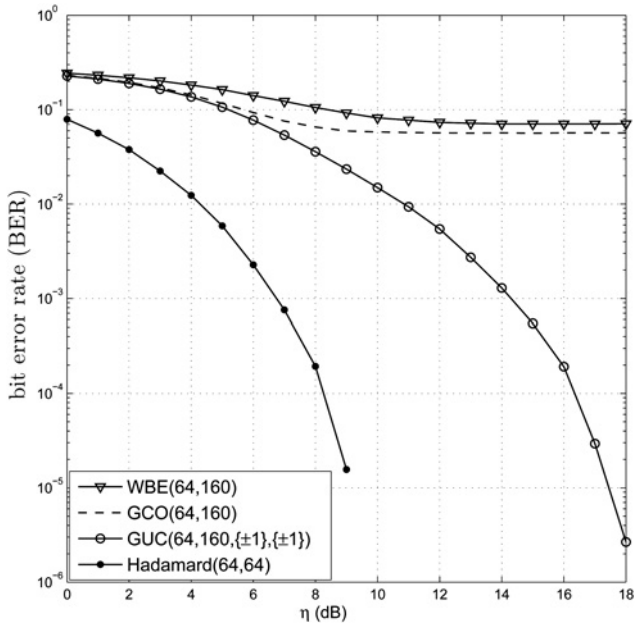

Fig. 1 *Bit error rate against normalised SNR (η) for a GCDMA system with m = 64, S = {±1} and t = 2*

$3^{n-m/2}$. However, the implementation of the direct ML decoding scheme has the complexity of 3^n.

Example 4: Using Theorem 2, we can obtain a GUC(16, 20, 3, {±1}) from a small GUC with $m=2$ and $n=1$. Then, we can achieve a system with $m=64$ and $n=80$ by the Kronecker product of this system with a Hadamard matrix of size 4. The decoder of this system with an exhaustive search is an NP-hard problem (about 3^{80} computations). However, using the above decoder, only 4×3^{12} computations are required, which is nearly 3^{68} times simpler than the direct approach of decoding.

3.3 Numerical results

To evaluate the performance of the GUC codes in noisy environments, we compare it to WBE and Hadamard codes assuming additive Gaussian noise. Fig. 1 confirms that GUC, similar to GCO, are superior to WBE codes. To compare GUC with GCO with the same number of chips and users ($m=64$, $n=120$), we first add eight random vectors to GCO(8, 12, {±1}, {±1}), and then derive a GCO (64, 160, {±1}, {±1}) matrix from the Kronecker product of this matrix with a Hadamard matrix of size 8. Simulation results confirm that a GUC code performs better that GCO as we expected since GCO matrices are special cases of GUC matrices.

4 Bounds for the sum capacity of GCDMA systems

In this section, we shall derive some lower and upper bounds for the sum capacity of GCDMA systems and compare them to the capacity bounds for CDMA systems. The following theorem relates the GCDMA capacity for the case $t=2$ to the CDMA capacity.

Theorem 3: For the noiseless case, the GCDMA sum capacity can be derived from the following equality

$$\mathcal{GC}(m, n, \mathcal{S}, t=2) = \mathcal{C}(m, n, \{\pm 1\}, \mathcal{S}-\mathcal{S}) \qquad (16)$$

The proof is given in Appendix 1.

Corollary 1:

$$\mathcal{GC}(m, n, \mathcal{S}=\{\pm 1\}, t=2) = \mathcal{C}(m, n, \{\pm 1\}, \{0, \pm 1\}) \geq \sup_{\pi_0, \pi_1} \left\{ -\log\left(\sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^n} \left(\sum_{\alpha=0}^{k} \binom{k}{\alpha,\ \alpha,\ k-2\alpha} \pi_0^{k-2\alpha} \pi_1^{2\alpha} \right)^m \right) \right\} \qquad (17)$$

where $\pi(.)$ is the distribution function on $\{0, \pm 1\}$, such that $\pi(0)=\pi_0$ and $\pi(+1)=\pi(-1)=\pi_1$.
In [8], the lower and upper bounds for $\mathcal{C}(m, n, \{0, \pm 1\}, \{\pm 1\})$ are derived, which can also be used for $\mathcal{GC}(m, n, \{\pm 1\}, t=2)$. With comparison to the lower bound of $\mathcal{C}(m, n, \{\pm 1\}, \{\pm 1\})$, it is seen that the generalised binary CDMA systems have tighter lower bounds as those of the binary CDMA cases.

For the noisy case, the following theorem gives a lower bound for the sum capacity of GCDMA codes for the case of $t=2$.

Theorem 4: For the noisy case, we have

$$\mathcal{GC}(m, n, \{\pm 1\}, 2, \eta) \geq \sup_{\rho} \sup_{\gamma} \Big\{ -m\big(\gamma \log e - \log(1+\gamma)\big) - \log\left\{ \sum_{k=0}^{n} \frac{1}{2^n} \binom{n}{k} \left\{ \sum_{i=0}^{k} \binom{k}{i} \frac{1}{2^k} \sum_{\alpha=0}^{i} \binom{i}{\alpha} \left(\frac{1-\rho}{2}\right)^{\alpha} \left(\frac{1+\rho}{2}\right)^{i-\alpha} \left(\sum_{\beta=0}^{k-i} \binom{k-i}{\beta} \left(\frac{1-\rho}{2}\right)^{\beta} \left(\frac{1+\rho}{2}\right)^{k-i-\beta} \left(e^{(-\gamma\eta/((1+\gamma)m))|2\alpha-2\beta|^2} \right) \right)^m \right\} \right\} \qquad (18)$$

The proof is given in Appendix 2. Also note that when $\eta=\infty$, the above inequality reduces to the bound represented in (17).

In a GCDMA code with $t=2$, the parameter ρ is introduced to represent the correlation between signature vectors of any user. That is, $\rho=-1$ corresponds to a CDMA system, and $\rho=1$ is the trivial case in which the two signature vectors are equal. Moreover, $\rho=0$ represents the case in which the signatures of a user are uncorrelated. To find the maximum capacity, different values of ρ should be examined. The numerical results show that the optimum ρ is not always equal to -1, which represents a classical binary CDMA system.

Fig. 2 shows the bounds of the sum capacity against the number of users for the noiseless case with $m=32$ and 64.

© The Institution of Engineering and Technology 2014

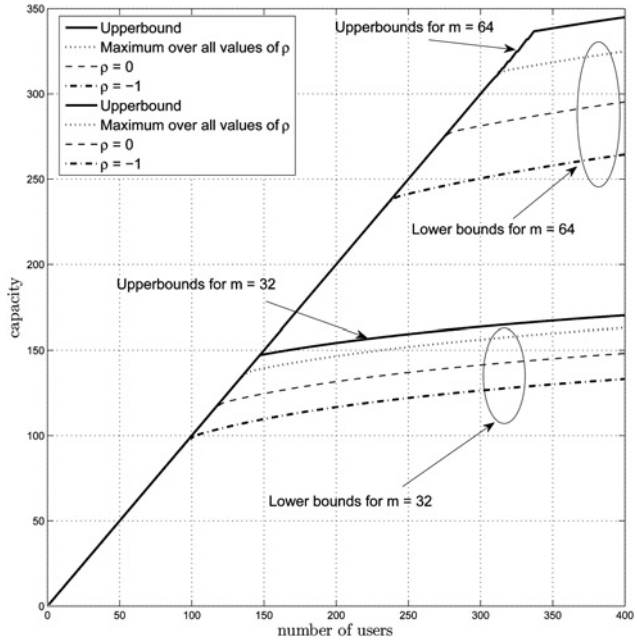

Fig. 2 *Sum capacity bounds against the number of users for the noiseless case in which m = 32, 64, $\mathcal{S} = \{\pm 1\}$ and t = 2*

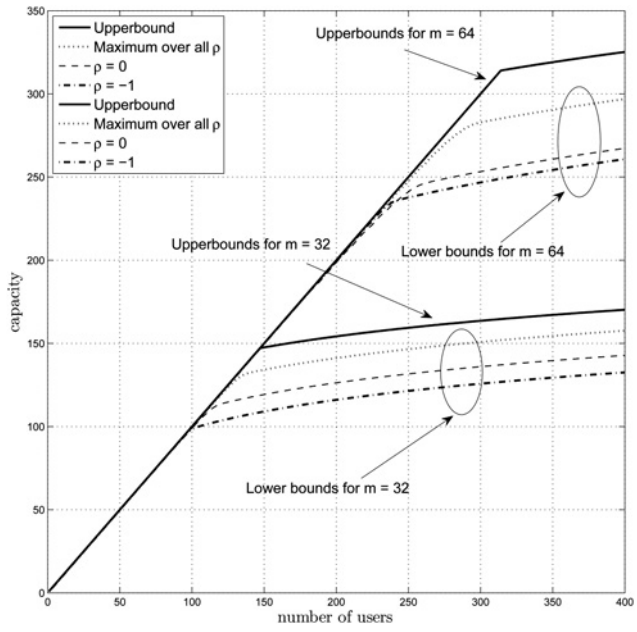

Fig. 3 *Sum capacity bounds against the number of users for the noisy case when m = 32, 64, η = 10, $\mathcal{S} = \{\pm 1\}$ and t = 2*

The plots with $\rho = -1$ can be interpreted as the lower bound of a CDMA system whereas the plots which are the maximisation over all the values of ρ represent lower bound for a GCDMA system. It can be seen that in a GCDMA system, tighter bounds can be achieved. This figure

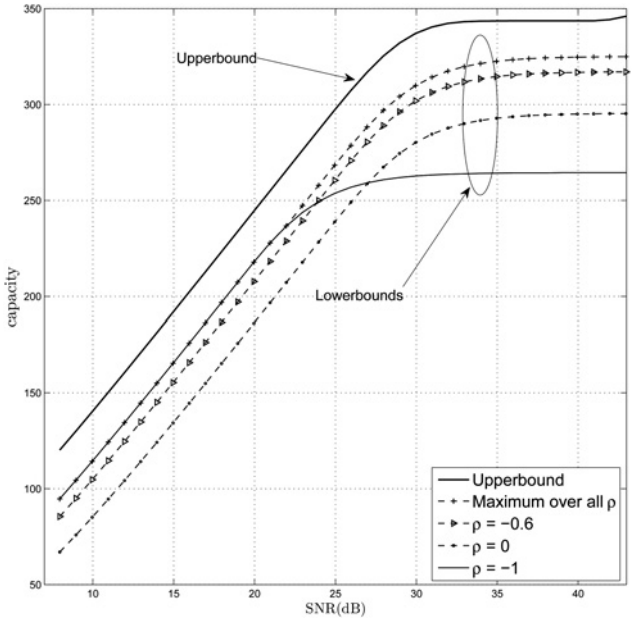

Fig. 4 *Sum capacity bounds against SNR for n = 400 users, m = 64, $S = \{\pm 1\}$ and t = 2*

suggests that the number of users in GCDMA systems maybe higher than that of CDMA systems. This figure also shows the upper bound of a GCDMA system according to (7) for both $m = 32$ and $m = 64$. Fig. 3 shows the same results for the noisy case when $\eta = 10$. This figure also shows that the bounds become less tight when the channel becomes noisy.

Fig. 4 shows the numerical results for the bounds of the sum capacity against SNR when $n = 400$ and $m = 64$. The lower bounds are plotted for various values of ρ. It can be seen that the bounds are linear with respect to SNR values in decibel up to a point and then saturates at high SNR values when interference because of the number of users become significant.

For the general case when $\mathcal{S} = \{\pm 1\}$, the sum capacity lower bounds can be derived from the following theorem.

Theorem 5: For arbitrary t and η, the following inequality holds (see (19))

The proof is given in Appendix 3.

Fig. 5 shows the numerical results for the normalised sum capacity lower bounds of a binary noiseless GCDMA system with $m = 64$, against the number of users for different values of t. The plots correspond to cases $t = 2, 4, 8$. The capacity per user is almost equals to log$t$ when the number of users is less than a threshold value, and it decreases exponentially afterwards.

For the general noiseless case when $\mathcal{S} = \{0, \pm 1, \ldots, \pm p\}$, the lower bound is shown in the theorem given below.

$$\mathcal{GC}(m, n, \mathcal{S} = \{\pm 1\}, t, \eta) \geq \sup_{\gamma} \left\{ -m\left(\gamma \log e - \log(1+\gamma)\right) - \log\left(\sum_{k=0}^{n} \binom{n}{k} \frac{(t-1)^k}{t^n} \left(\sum_{i=0}^{2k} \binom{2k}{i} \frac{1}{2^{2k}} \left(e^{\left(-\gamma\eta/((1+\gamma)m)\right)|2k-2i|^2} \right) \right)^m \right) \right\} \tag{19}$$

© The Institution of Engineering and Technology 2014

doi: 10.1049/iet-com.2013.0344

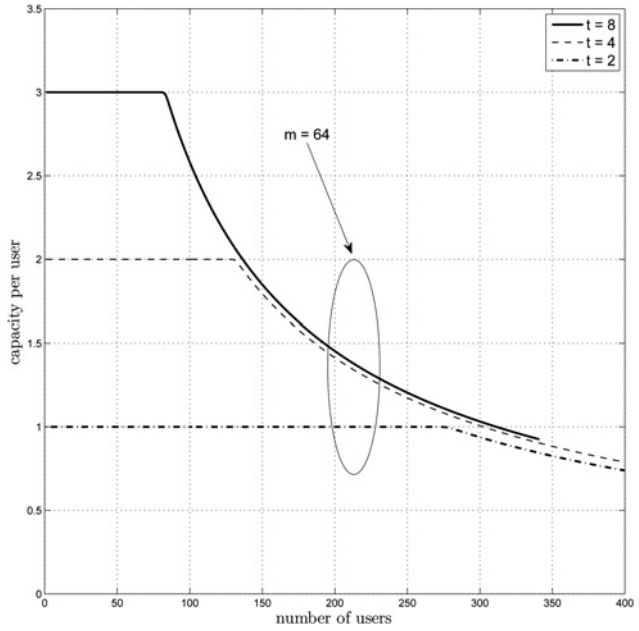

Fig. 5 *Normalised sum capacity lower bounds against the number of users for m = 64 and various values of t for the noisy case and $\mathcal{S} = \{\pm 1\}$*

Theorem 6: In the absence of noise for $\mathcal{S} = \{0, \pm 1, \ldots, \pm p\}$, the following inequality holds

$$\mathcal{GC}(m, n, \{0, \pm 1, ..., \pm p\}, t) \geq -\log \sum_{k=0}^{n} \binom{n}{k} \frac{(t-1)^k}{t^n} \left(A_p(2k)\right)^m \tag{20}$$

where $A_p(2k)$ is the probability of the event when $\sum_{i=1}^{2k} a_i = 0$ such that a_i's belong to the set $\{0, \pm 1, ..., \pm p\}$ with uniform distribution.
The proof is given in Appendix 4.

The numerical results for the normalised sum capacity lower bound for GCDMA systems with $m = 64$ and various values of t for $p = 1$ and $p = 2$ are shown in Figs. 6 and 7, respectively. As expected, the numerical results show that when $p = 2$, the system is saturated at a larger number of users than the case where $p = 1$.

Incidentally, from Theorem 3, the upper bounds of a GCDMA system are exactly the same as the CDMA system for the case when $t = 2$ and $\mathcal{S} = \{\pm 1\}$.

Theorem 7 (conjectured upper bound): Let f be a symmetric probability distribution function, that is, $f(x) = f(-x)$. Define the function $\tilde{f}$ by $\tilde{f}(x) = \sum_{j=0}^{n} \frac{\binom{n}{j}}{2^n} f\left(x - \frac{2j-n}{\sqrt{m}}\right)$; we have

$$\mathcal{GC}(m, n, \mathcal{S} = \{\pm 1\}, t = 2, f) \leq \min\left(n, m\left(h(\tilde{f}) - h(\tilde{f})\right)\right) \tag{21}$$

where $h(.)$ is the differential entropy.

Proof: From Theorem 3 and the upper bounds of corresponding CDMA in [8], the above inequality can be derived trivially. □

Below we shall give two examples for the upper bounds of specific GCDMA systems.

Example 5 (Noisy Case): For a Gaussian distribution, we have

$$\tilde{f}(x) = \frac{1}{\sigma\sqrt{2\pi}} \sum_{j=0}^{n} \frac{\binom{n}{j}}{2^n} \exp\left(-\frac{x - \left((2j-n)/(\sqrt{m})\right)}{2\sigma^2}\right) \tag{22}$$

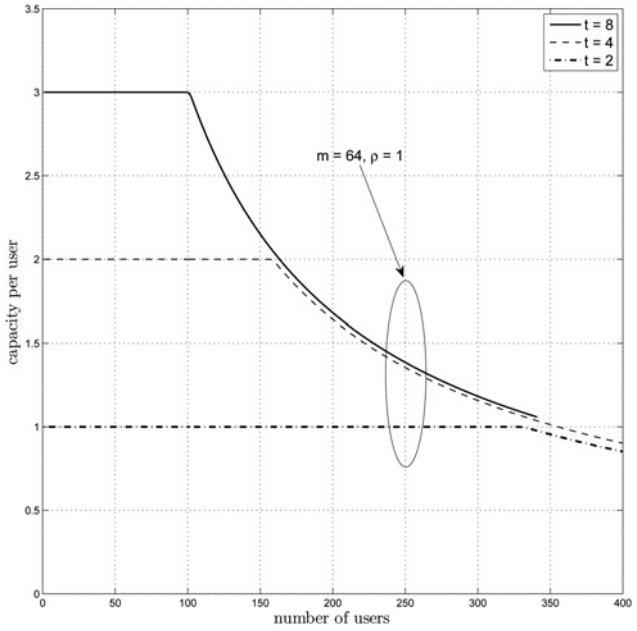

Fig. 6 *Normalised sum capacity lower bounds against the number of users for m = 64, p = 1, S = {0, ±1} and several values of t*

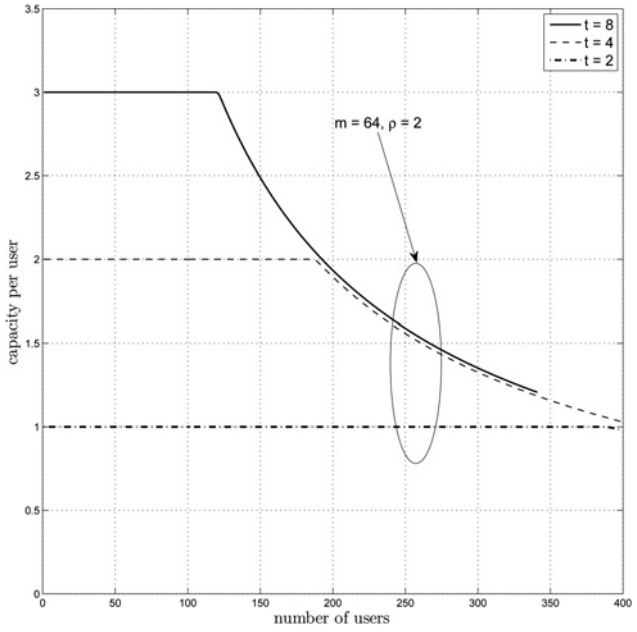

Fig. 7 *Normalised sum capacity lower bounds against the number of users for m = 64, p = 2, S = {0, ±1 ±2} different values of t*

© The Institution of Engineering and Technology 2014

Thus

$$\begin{aligned}&\mathcal{GC}\left(m, n, \mathcal{S}=\{\pm 1\}, t=2, \sigma^2\right)\\&\leq \min\left(n, m\left(h\left(\tilde{f}\right)-\log\left(\sqrt{2\pi e}\sigma\right)\right)\right)\end{aligned} \tag{23}$$

Example 6 (Noiseless Case): For the noiseless case, we assume that the pdf of the noise is an impulse, therefore

$$\tilde{f}(x)=\sum_{j=0}^{n}\frac{\binom{n}{j}}{2^n}\delta\left(x-\frac{2j-n}{\sqrt{m}}\right) \tag{24}$$

This is a discrete probability distribution. Hence, we use the usual entropy instead of the differential entropy, and the upper bound becomes

$$\mathcal{GC}\left(m, n, \mathcal{S}=\{\pm 1\}, t=2, \sigma^2\right)\leq \min\left(n, m\left(H\left(\tilde{f}\right)\right)\right) \tag{25}$$

5 Conclusion and future work

In this paper, we introduced a new framework for GCDMA systems in which each user uses a set of signature vectors for sending its data. In this new framework, we have addressed two main problems. The first concern was related to the development of uniquely detectable matrices (GUC matrices), which were constructed for finite users and signature matrices. Also, practical ML detection algorithms were suggested. The constructions showed that with the suggested GCDMA system, one may support more users in comparison with the classical CDMA systems. Numerical results for special cases showed that GUC matrices outperformed the codes proposed in previous works for overloaded CDMA systems. Our second concern was on the evaluation of the bounds for the sum capacity. We explored the problem by deriving general theorems and examples for special cases.

As for future work, we suggest to study the effects of fading because of multipath and near far effects on injectivity of GUC matrices and the evaluation of the sum capacity bounds. Also the generalisation of the new scheme to an asynchronous system is another interesting problem. In addition, the consideration of sparse active users in a GCDMA system is a good topic for future work.

6 Acknowledgment

This work was partially funded by INSF (Iran National Science Foundation). The authors also thank IPM (Institute for Research in Fundamental Sciences) for providing logistical support.

7 References

1 Liao, H.: 'Multiple access channels', *IEEE Trans. Inf. Theory*, 1973, **19**, (2), p. 253
2 Pad, P., Marvasti, F., Alishahi, K., Akbari, S.: 'A class of errorless codes for overloaded synchronous wireless and optical CDMA systems', *IEEE Trans. Inf. Theory*, 2009, **55**, (6), pp. 2705–2715
3 Guo, D., Verdu, S.: 'Randomly spread CDMA: asymptotics via statistical physics', *IEEE Trans. Inf. Theory*, 2005, **51**, (6), pp. 1983–2010
4 Mow, W.: 'Recursive constructions of detecting matrices for multiuser coding: a unifying approach', *IEEE Trans. Inf. Theory*, 2009, **55**, (1), pp. 93–98
5 Pad, P., Soltanolkotabi, M., Hadikhanlou, S., Enayati, A., Marvasti, F.: 'Errorless codes for over-loaded CDMA with active user detection'. IEEE International Conference on communications (ICC'09), 2009, pp. 1–6
6 Soderberg, S., Shapiro, H.: 'A combinatory detection problem', *Am. Math. Mon.*, 1963, **70**, (10), pp. 1066–1070
7 Lindstrom, B.: 'On Mobius functions and a problem in combinatorial number theory', *Can. Math. Bull.*, 1971, **14**, (10), pp. 513–516
8 Alishahi, K., Dashmiz, S., Pad, P., Marvasti, F.: 'Design of signature sequences for overloaded CDMA and bounds on the sum capacity with arbitrary symbol alphabets', *IEEE Trans. Inf. Theory*, 2012, **58**, (3), pp. 1441–1469
9 Verdu, S.: 'Multiuser detection' (Cambridge University Press, 1998)
10 Welch, L.: 'Lower bounds on the maximum cross correlation of signals (Corresp.)', *IEEE Trans. Inf. Theory*, 1974, **20**, (3), pp. 397–399
11 Tanaka, T.: 'A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors', *IEEE Trans. Inf. Theory*, 2002, **48**, (11), pp. 2888–2910
12 de Miguel, R., Shental, O., Mller, R.R., Kanter, I.: 'Information and multiaccess interference in a complexity-constrained vector channel', *J. Phys. A, Math. Theor.*, 2007, **40**, (20), pp. 5241–5260
13 Alishahi, K., Marvasti, F., Aref, V., Pad, P.: 'Bounds on the sum capacity of synchronous binary CDMA channels', *IEEE Trans. Inf. Theory*, 2009, **55**, (8), pp. 3577–3593
14 Chang, S.-C., Weldon, E.: 'Coding for T-user multiple-access channels', *IEEE Trans. Inf. Theory*, 1979, **25**, (6), pp. 684–691
15 Bross, S., Blake, I.: 'Upper bound for uniquely decodable codes in a binary input N-user adder channel', *IEEE Trans. Inf. Theory*, 1998, **44**, (1), pp. 334–340
16 Ferguson, T.: 'Generalized T-user codes for multiple-access channels', *IEEE Trans. Inf. Theory*, 1982, **28**, pp. 775–778

8 Appendix

8.1 Appendix 1: Proof of Theorem 3

Each of these capacity functions is the maximum of $I(X;Y)$ over all possible matrices and input distributions. In the absence of noise, $I(X;Y)=H(Y)$.

First, suppose that $\mathcal{GC}(m, n, \mathcal{S}, 2)=H(AX)$ for an $m\times 2n$ fixed matrix $\boldsymbol{A}\in\mathcal{M}_{m\times 2n}(\mathcal{S})$ and a probability distribution p on inputs $\{(1, 0), (0, 1)\}^n$. We construct a new $m\times 2n$ matrix $\boldsymbol{B}$ from matrix $\boldsymbol{A}$ by substituting columns A_{2k-1}, A_{2k} with $A_{2k-1}+A_{2k}$, $A_{2k-1}-A_{2k}$, respectively. By substituting the input pairs (1, 0), (0, 1) with pairs (1, 1), (1, −1), respectively, we obtain new input vectors which can transfer the same data when multiplied by $\boldsymbol{B}$. Note that input entries with odd indices are always 1. By removing the columns of matrix $\boldsymbol{B}$ with odd indices and the corresponding entries in the new input vectors, we obtain matrix $\boldsymbol{C}\in\mathcal{M}_{m\times n}(\mathcal{S}-\mathcal{S})$ and the new input vectors $\boldsymbol{X}\in\{\pm 1\}^n$ with the same input probability distribution, which are appropriate for the CDMA case and yield the same entropy. Thus, we have

$$\mathcal{C}(m, n, \{\pm 1\}, \mathcal{S}-\mathcal{S})\geq\mathcal{GC}(m, n, \mathcal{S}, 2) \tag{26}$$

Conversely, if $\mathcal{C}(m, n, \{\pm 1\}, \mathcal{S}-\mathcal{S})=\boldsymbol{H}(\boldsymbol{AX})$ for a fixed $m\times n$ matrix $\boldsymbol{C}$ and a probability distribution p' on the set $\{\pm 1\}$, we follow the reverse steps mentioned in the previous paragraph to obtain the same entropy for GCDMA case and conclude that

$$\mathcal{GC}(m, n, \mathcal{S}, 2)\geq\mathcal{C}(m, n, \{\pm 1\}, \mathcal{S}-\mathcal{S}) \tag{27}$$

Considering (26), (27), we can derive (17). □

© The Institution of Engineering and Technology 2014

doi: 10.1049/iet-com.2013.0344

8.2 Appendix 2: Proof of Theorem 4

In [8], the authors proved that for a given $\mathcal{I}$ and $\mathcal{S}$, the following equation holds

$$\mathcal{C}(m, n, \mathcal{I}, \mathcal{S}, \eta) \geq \sup_{\pi,p} \sup_{\gamma} \left\{ -m(\gamma \log e - \log(1+\gamma)) - \log \mathbb{E}_{\tilde{X}} \left(\left(\mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \right) \right)^m \right) \right\} \tag{28}$$

where $\boldsymbol{r} = \sqrt{2\eta / \left(\left(\sigma_p^2 + n\mu_p^2 \right) \left(\sigma_\pi^2 + \mu_\pi^2 \right) \right)}$, $\boldsymbol{b}$ and $\tilde{\boldsymbol{X}}$ are, respectively, vectors of length n with i.i.d. entries of distributions $\pi(\cdot)$ and $\tilde{p}(\cdot)$.

In our theorem, we consider a special case of this theorem, where $\boldsymbol{b}$ is a vector of length $2n$ representing an arbitrary row of the signature matrix in GCDMA. Therefore, b_{2k-1} and b_{2k} are the entries of signature vectors of user number k in that specific row. We consider b_{2k}, b_{2k-1} to be correlated by a factor of ρ. In other words $(b_{2k-1}, b_{2k}) = (+1 \quad +1)$ or $(-1 \quad -1)$ with probability $(1+\rho)/4$ and $(b_{2k-1}, b_{2k}) = (+1 \quad -1)$ or $(-1 \quad +1)$ with probability $(1-\rho)/4$.

Hence, $\tilde{p}$ and π in (28) are replaced by ρ and $\boldsymbol{r}^2$ in exponential function is replaced by 2η. In our case, $\tilde{\boldsymbol{X}}$ is a vector of length $2n$ defined as follows

$$\tilde{\boldsymbol{X}} = \{ \boldsymbol{X} - \boldsymbol{Y} | \boldsymbol{X}, \boldsymbol{Y} \quad \text{are input vectors} \} \tag{29}$$

As we previously mentioned, each pair X_{2k-1}, X_{2k} in the input vector $\boldsymbol{X}$ belongs to a user and is either $\begin{pmatrix} 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \end{pmatrix}$. Hence, each pair in $\tilde{\boldsymbol{X}}$ is either $(0 \quad 0)$ with probability 0.5 or one of the pairs $\begin{pmatrix} 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 1 \end{pmatrix}$, each with probability 0.25. The total number of $\tilde{x} \in \tilde{\boldsymbol{X}}$ with k non-zero pairs is $\binom{n}{k}$. Note that

$$\begin{aligned} &\mathbb{E}_{\tilde{X}} \left(\left(\mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \right) \right)^m \right) \\ &= \sum_{\text{every possible } \tilde{x}} p(\tilde{\boldsymbol{X}} = \tilde{x}) \mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \middle| \tilde{\boldsymbol{X}} = \tilde{x} \right)^m \\ &= \sum_{k=0}^{n} \binom{n}{k} \left(\frac{1}{2} \right)^n \mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \middle| \tilde{\boldsymbol{X}} = \boldsymbol{Z}_k \right)^m \end{aligned} \tag{30}$$

where $\boldsymbol{Z}_k$ for $0 \leq k \leq n$ is a vector of length $2n$, which begins with k pairs of $\begin{pmatrix} 1 & -1 \end{pmatrix}$ and ends with $n-k$ pairs of zero.

The last part in this equation is derived from the fact that replacing a $\begin{pmatrix} -1 & 1 \end{pmatrix}$ pair with a $\begin{pmatrix} 1 & -1 \end{pmatrix}$ pair in $\tilde{\boldsymbol{X}}$ or changing the order of pairs does not change the value of $\mathbb{E}_{\boldsymbol{b}}$.

Fixing $\tilde{\boldsymbol{X}}$ to $\boldsymbol{Z}_k$, we have

$$\left| \boldsymbol{b}^{\mathrm{T}} \tilde{\boldsymbol{X}} \right| = \sum_{i=1}^{k} b_{2i-1} - b_{2i} \tag{31}$$

As we mentioned before, there are four pairs of b_{2i-1}, b_{2i} for $1 \leq i \leq k$, and the value in exponential function in (28) is independent of the order of pairs in $\boldsymbol{b}$.

Thus, we can choose $0 \leq i \leq k$ pairs of k non-zero pairs to begin with 1, so that the other $k-i$ pairs begin with -1. $0 \leq \alpha \leq i$ pairs of these i pairs are $\begin{pmatrix} 1 & -1 \end{pmatrix}$, while $0 \leq \beta \leq k-i$ pairs of the $k-i$ pairs beginning with -1 are $\begin{pmatrix} -1 & 1 \end{pmatrix}$. Hence, in this case $\left| \boldsymbol{b}^{\mathrm{T}} \tilde{\boldsymbol{X}} \right|$ is equal to $|2\alpha - 2\beta|$ which yields

$$\begin{aligned} &\mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \middle| \tilde{\boldsymbol{X}} = \tilde{x} \right) \\ &= \sum_{i=0}^{k} \binom{k}{i} \frac{1}{2^k} \sum_{\alpha=0}^{i} \binom{i}{\alpha} \left(\frac{1-\rho}{2} \right)^{\alpha} \left(\frac{1+\rho}{2} \right)^{i-\alpha} \\ &\quad \sum_{\beta=0}^{k-i} \binom{k-i}{\beta} \left(\frac{1-\rho}{2} \right)^{\beta} \left(\frac{1+\rho}{2} \right)^{k-i-\beta} \\ &\quad \left(e^{\left((\gamma r^2)/(2(1+\gamma)m)\right) |2\alpha - 2\beta|^2} \right) \end{aligned} \tag{32}$$

From (28), (30) and (32) the proof is complete. □

8.3 Appendix 3: Proof of Theorem 5

Again, we take the advantage of (28). However, we consider $\boldsymbol{b}$ and $\tilde{\boldsymbol{X}}$ to be of length nt. The probability distributions on $\tilde{\boldsymbol{X}}$ and $\boldsymbol{b}$ are specified in our case. Hence, the following inequality can be derived from (28)

$$\mathcal{GC}(m, n, \{\pm 1\}, t) \geq \sup_{\gamma} \left\{ -m(\gamma \log e - \log(1+\gamma)) - log \mathbb{E}_{\tilde{X}} \left(\left(\mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \right) \right)^m \right) \right\} \tag{33}$$

It is easy to see that each user block of length t in $\tilde{\boldsymbol{X}}$ is either completely zero or has exactly one entry equal to 1 and one entry equal to -1. Without loss of generality, we assume that all non-zero blocks are in the beginning of the vector and the first two entries of a non-zero block are $(1, -1)$, respectively. To simplify (33), we suppose that exactly $0 \leq k \leq n$ blocks in $\tilde{\boldsymbol{X}}$ are non-zero and the other blocks are zero. Therefore we have

$$\begin{aligned} \mathbb{E}_{\tilde{X}} \left(\left(\mathbb{E}_{\boldsymbol{b}} \left(e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} \right) \right)^m \right) &= \sum_{k=0}^{n} \binom{n}{k} \left(\frac{1}{t} \right)^{n-k} \\ &\times \left(\frac{t-1}{t} \right)^k \mathbb{E}_{\boldsymbol{b}} (e^{\left((-\gamma r^2)/(2(1+\gamma)m)\right) \left| \boldsymbol{b}^{\mathrm{T}} \tilde{X} \right|^2} | \tilde{\boldsymbol{X}} = \boldsymbol{Z}_k)^m \end{aligned} \tag{34}$$

where $\boldsymbol{Z}_k$ is defined as in proof of Theorem 4. As each entry in

© The Institution of Engineering and Technology 2014

$\boldsymbol{b}$ is either 1 or -1 with probability 0.5, we have

$$\begin{aligned}&\mathbb{E}_{\boldsymbol{b}}\left(\mathrm{e}^{\left(\left(-\gamma r^2\right)/(2(1+\gamma)m)\right)\left|\boldsymbol{b}^{\mathrm{T}}\tilde{\boldsymbol{X}}\right|^2}\middle|\tilde{\boldsymbol{X}}=Z_k\right)\\&=\sum_{i=0}^{2k}\binom{2\ k}{i}\frac{1}{2^{2k}}\left(\mathrm{e}^{\left(\left(-\gamma r^2\right)/((1+\gamma)m)\right)|2k-2i|^2}\right)\end{aligned}\tag{35}$$

By considering (33), (34) and (36), the proof is complete. □

8.4 Appendix 4: Proof of Theorem 6

Using (33) and (34) from the previous proof, we can prove Theorem 6. The only step left to complete the proof is to show that

$$\Pr\left(\sum_{i=0}^{k-1}\left(b_{ik+1}-b_{ik+2}\right)=0\right)=A_p(2\ k)\tag{36}$$

According to the symmetry in ?

$$\Pr\left(\sum_{i=0}^{k-1}\left(b_{ik+1}-b_{ik+2}\right)=0\right)=\Pr\left(\sum_{i=0}^{k-1}\left(b_{ik+1}+b_{ik+2}\right)=0\right)\tag{37}$$

The right-hand side of the upper equality is exactly the definition of $A_p(2k)$. □

© The Institution of Engineering and Technology 2014

doi: 10.1049/iet-com.2013.0344