The 33rd Symposium on Information Theory
and its Applications (SITA2010)
Matsushiro, Nagano, Japan, Nov. 30–Dec. 3, 2010

Maximum likelihood detection for DS-CDMA using Gröbner bases

Shunsuke Horii * Tota Suko † Toshiyasu Matsushima * Shigeichi Hirasawa ‡

Abstract— Maximum likelihood (ML) multiuser detection for the direct sequence code division multiple access (DS-CDMA) channel is known to be NP-hard, i.e., its computational complexity increase exponentially with the number of users. Since the ML multiuser detection can be regarded as an integer quadratic programming, some optimization algorithms have been used to tackle the problem. Conti and Traverso have proposed an efficient algorithm to solve integer programming based on the Grobner bases. Conti-Traverso algorithm is originally used to solve the integer linear programming, we can not apply the algorithm to the multiuser detection problem in a straight-forward manner. On the other hand, Ikegami et. al. extended the Conti-Traverso algorithm to solve the integer linear programming with modulo arithmetic conditions. In this paper, we transform the ML multiuser detection problem into the integer linear programming with modulo arithmetic conditions and propose the multiuser detection algorithm based on the extended Conti-Traverso algorithm.

Keywords— Multiuser detection, Maximum Likelihood detection, Integer quadratic programming, Gröbner basis

1 Introduction

Multiuser detection (MUD) for interference cancellation in direct-sequence code-division multiple access (DS-CDMA) communication systems is very important and it have been studied deeply for a number of years [1].

Assuming an additive white Gaussian noise channel, Maximum-likelihood (ML) detection is optimum. ML detector minimizes the squared Euclidean distance between the received signal and hypothesized information-bit vector $\boldsymbol{b}$ which is constrained to the set $\{-1,1\}^K$, where K is the number of users. It has been shown that this problem is, in general, NP-hard problem [1] and therefore it is too complex to implement for practical DS-CDMA systems even for a moderate number of users.

For certain special cases, it has been shown that ML detection can be implemented in polynomial time [2]-[4]. For general cases, the A* algorithm is used in [5], where ML detection is restated as finding the optimal path in a tree, and it's computational complexity is fewer than the brute forth search in many cases.

Since the computational complexity of ML detection is the exponential order, many low complexity sub-optimal detectors have been developed. ML detection problem is considered as a binary constrained minimization problem which is known as a binary quadratic programming (BQP) in the area of optimization theory. Various optimization algorithms are used to solve the BQP approximately. The relaxation method is one of most effective methods to solve the BQP approximately. They relax the binary constraints and operate on continuous variables. The solution to the relaxed problem is used to provide an approximate solution. In [6][7], some relaxation methods has been applied to the multiuser detection problem. To obtain a better approximate solution for the ML detection problem, semidefinite relaxation has been also used to the multiuser detection problem [8]-[11].

In this paper, quite different algorithm for ML detection problem is proposed. The proposed algorithm is an exact algorithm, i.e., it output the most closest information-bit vector to the received signal. The algorithm is based on the Conti-Traverso algorithm [12]. The Conti-Traverso algorithm solves an integer programming using a *Gröbner basis*. The Conti-Traverso algorithm compute a Gröbner basis for an ideal of a polynomial ring which is defined from the constraints and then compute the optimum solution.

Since the Conti-Traverso algorithm can be used to solve the integer linear programming, and the ML detection problem is the integer quadratic programming, we can not apply the algorithm to the ML detection problem in a straight-forward manner. On the other hand, in [13] Ikegami et. al. extended the Conti-Traverso algorithm to solve the integer linear programming with modulo arithmetic conditions. In this paper, we transform the ML detection problem into the integer linear programming with modulo arithmetic conditions and apply the extended Conti-Traverso algorithm to the transformed problem. The complexity of the proposed detection algorithm is not as efficient as other ML detection algorithms such as A* algorithm. We think that the algebraic structure of the multiuser detection problem will be found out through this research.

The rest of the paper is organized as follows. In section 2, we establish the synchronous DS-CDMA channel model and maximum likelihood multiuser detection problem. In section 3, we review some basic notions about Gr"obner bases and the extended Conti-Traverso algorithm proposed in [13]. Section 4 contains the derivation of the proposed multiuser detection algorithm.

* The author is with the Department of Applied Mathematics, Waseda University, 3-4-1, Okubo, Shinjuku Tokyo 169-8555 Japan. E-mail: s.horii@aoni.waseda.jp

† The author is with the Media Network Center, Waseda University, 1-6-1, Nishiwaseda, Shinjuku Tokyo 169-8050 Japan.

‡ The author is with the Waseda Research Institute for Science and Engineering, Waseda University, 3-4-1, Okubo, Shinjuku Tokyo, 169-8555, and is with Cyber University, Japan.

2 DS-CDMA Channel Model

We consider a synchronous CDMA system employing BPSK modulation. The received signal in a K-user system is described by

$$r(t) = \sum_{k=1}^{K} \sqrt{e_k} b_k g_k(t) + n(t), \quad 0 \le t \le T \qquad (1)$$

where e_k is the signal energy, $b_k \in \{-1, +1\}$ is the value of the information bit, $n(t)$ is additive white Gaussian noise (AWGN) with power spectral density $N_0/2$, and $g_k(t)$ is the signature waveform for user k, given by

$$g_k(t) = \sum_{n=0}^{N-1} s_k(n) p(t - nT_c), \quad 0 \le t \le T, \qquad (2)$$

where T_c is the chip interval, $p(t)$ is a rectangular pulse of duration T_c, $\{s_k(n), 0 \le n \le N-1\} \in \{-1, +1\}^N$ is a sequence of pseudo random bits, and N is the number of pseudo random bits in one symbol period T.

The correlation matrix $\boldsymbol{W}$ is the $K \times K$ matrix, whose elements are

$$w_{kl} = \int_0^T g_k(t) g_l(t) dt = \sum_{n=0}^{N-1} s_k(n) s_l(n). \qquad (3)$$

The ML detector selects the hypothesized information bit vector $\boldsymbol{b}^* = \{b_1^*, b_2^*, \cdots, b_K^*\}$ that maximized the joint posterior distribution $P(\boldsymbol{b}|r(t))$. Assuming that all information sequences are equiprobable, the ML detector minimizes the squared Euclidean distance between the received signal and hypothesized information bit vector [1], i.e.,

$$\begin{aligned} \boldsymbol{b}^* &= \arg \min_{-1,+1}^{K} \int_0^T \left[r(t) - \sum_{k=1}^{K} \sqrt{a_k} b_k g_k(t) \right]^2 dt \qquad (4) \\ &= \arg \min_{\boldsymbol{b} \in \{-1,+1\}^K} \left(\boldsymbol{b}^T \boldsymbol{Q} \boldsymbol{b} - 2 \boldsymbol{r}^T \boldsymbol{b} \right) \qquad (5) \end{aligned}$$

where $\boldsymbol{r} = [r_1, r_2, \cdots, r_K]^T$ is the vector of matched filter outputs given by

$$r_k = \sqrt{e_k} \int_0^T r(t) g_k(t) dt, \quad 1 \le k \le K \qquad (6)$$

and $\boldsymbol{Q}$ is $K \times K$ matrix with $q_{kl} = \sqrt{e_k}\sqrt{e_l} w_{kl}$.

Let $\tilde{\boldsymbol{b}} = (\boldsymbol{1} - 2\boldsymbol{b})/2$, where $\boldsymbol{1}$ is an K-dimensional vector of all ones. Then we can convert the problem (5) to a 0-1 quadratic programming problem as

$$\tilde{\boldsymbol{b}}^* = \arg \min_{\tilde{\boldsymbol{b}} \in \{0,1\}^K} \tilde{\boldsymbol{b}}^T \boldsymbol{Q} \tilde{\boldsymbol{b}} - \boldsymbol{p}^T \tilde{\boldsymbol{b}} \qquad (7)$$

where $\boldsymbol{p} = \boldsymbol{R}\boldsymbol{1} - \boldsymbol{r}$. Note that the solutions of (5) and (7) are related by the one-to-one relationship $b_k^* = (1 - 2\tilde{b}_k^*)/2$, where b_k and b_l are the k-th element of $\boldsymbol{b}$ and $\tilde{\boldsymbol{b}}$, respectively.

3 Gröbner basis, Conti-Traverso algorithm and its extension

In [12] and [13], Conti and Traverso have been proposed an algorithm to solve the integer linear programming and Ikegami and Kaji have been proposed an algorithm to solve the integer linear programming with modulo arithmetic conditions, respectively. These algorithms are based on the theory of Gröbner bases, hence we review some basic notions in the following subsection.

3.1 Gröbner basis

Let F be a field and $F[X_1, \cdots, X_n]$ be the polynomial ring over F in n variables $X_1, \cdots, X_n$. For $f_1, \cdots, f_s \in F[X_1, \cdots, X_n]$, let $\langle f_1, \cdots, f_s \rangle$ be the collection

$$\langle f_1, \cdots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_i \in F[X_1, \cdots, X_n] \right\}. \qquad (8)$$

Then $\langle f_1, \cdots, f_s \rangle$ forms an ideal in $F[X_1, \cdots, X_n]$ and it is called the ideal generated by $f_1, \cdots, f_s$. The set of polynomials $\{f_1, \cdots, f_s\}$ is called a basis of the ideal I when $I = \langle f_1, \cdots, f_s \rangle$. According to the Hilbert's basis theorem, any ideal of $F[X_1, \cdots, X_n]$ has a finite basis.

A monomial of $X_1, \cdots, X_n$ is a product in the form of $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ with $\alpha_i \in \mathbf{Z}_+$ for $1 \le i \le n$, where $\mathbf{Z}_+$ denotes the set of nonnegative integers. We abbreviate the above monomial as $\boldsymbol{X}^{\boldsymbol{\alpha}}$, where $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbf{Z}_+^n$ is the vector of exponents in the monomial.

A monomial order $<$ on $F[X_1, \cdots, X_n]$ is a total order on the set of monomials in $F[X_1, \cdots, X_n]$ that satisfies following conditions:

- if $\boldsymbol{X}^{\boldsymbol{\alpha}_1} < \boldsymbol{X}^{\boldsymbol{\alpha}_2}$, then $\boldsymbol{X}^{\boldsymbol{\alpha}_1 + \boldsymbol{\beta}} < \boldsymbol{X}^{\boldsymbol{\alpha}_2 + \boldsymbol{\beta}}$ for all $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\beta} \in \mathbf{Z}_+^n$
- $\boldsymbol{X}^{\boldsymbol{0}} (= 1) < \boldsymbol{X}^{\boldsymbol{\alpha}}$ for all $\boldsymbol{\alpha} \in \mathbf{Z}_+^n$

For a monomial order $<$ and a nonzero polynomial $f = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{X}^{\boldsymbol{\alpha}} \in F[X_1, \cdots, X_n]$ with $c_{\boldsymbol{\alpha}} \in F$ for any $\boldsymbol{\alpha} \in \mathbf{Z}_+^n$, The leading term of f is the term which has the largest exponent in f with respect to $<$. The leading term of f is denoted by $\mathrm{LT}_<(f)$.

For an ideal I, we denote by $\mathrm{LT}_<(I)$ the set of leading terms of elements of I and by $\langle \mathrm{LT}_<(I) \rangle$ the ideal generated by the elements of $\mathrm{LT}_<(I)$. A nonempty finite subset $\mathcal{G} = \{g_1, \cdots, g_t\} \subset F[X_1, \cdots, X_n]$ is called a Gröbner basis of the ideal I with respect to $<$ if and only if

$$\langle \mathrm{LT}_<(g_1), \cdots, \mathrm{LT}_<(g_t) \rangle = \langle \mathrm{LT}_<(I) \rangle \qquad (9)$$

For a monomial order $<$ and a Gröbner basis $\mathcal{G}$ with respect to $<$, the remainder of a polynomial $f \in F[X_1, \cdots, X_n]$ divided by every elements of $\mathcal{G}$ with respect to $<$ is uniquely determined according to the division algorithm in $F[X_1, \cdots, X_n]$. The remainder is called the normal form of f by $\mathcal{G}$ and denote as $\bar{f}^{\mathcal{G}}$. We write $f \equiv h \bmod I$ if $\bar{f}^{\mathcal{G}} = \bar{h}^{\mathcal{G}}$.

3.2 Conti-Traverso algorithm

The Conti-Traverso algorithm can solve the following minimization problem:

$$\mathrm{IP}_{\boldsymbol{A},\boldsymbol{c}}(\boldsymbol{d}) = \min\left\{\boldsymbol{c}^T\boldsymbol{x} : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{d}\ \boldsymbol{x} \in \mathbf{Z}^n\right\}, \qquad (10)$$

where $\boldsymbol{A} = [\boldsymbol{a}_1\ \boldsymbol{a}_2\ \cdots\ \boldsymbol{a}_n] \in \mathbf{Z}^{m\times n}$, $\boldsymbol{c} \in \mathbf{R}_+^n$ and $\boldsymbol{d} \in \mathbf{Z}^m$, where $\mathbf{R}_+$ is the set of nonnegative real numbers. The algorithm first define an ideal I and a monomial order $<$ and a monomial f that are determined by $\boldsymbol{A}$, $\boldsymbol{c}$ and $\boldsymbol{d}$, respectively. Then the algorithm computes Groöbner basis of I with respect to $\boldsymbol{w}$ and computes the normal form of f. Then the exponent of the normal form of f is an optimal solution of $\mathrm{IP}_{\boldsymbol{A},\boldsymbol{c}}(\boldsymbol{d})$.

3.3 Extended Conti-Traverso algorithm

Here we consider the following minimization problem:

$$\mathrm{IP}_{\boldsymbol{A},\boldsymbol{c},q}(\boldsymbol{d}) = \min\left\{\boldsymbol{c}^T\boldsymbol{x} : \boldsymbol{A}\boldsymbol{x} \equiv \boldsymbol{d} \bmod q, \boldsymbol{x} \in \mathbf{Z}_q^n\right\}, \qquad (11)$$

where $\boldsymbol{A} = [\boldsymbol{a}_1\ \boldsymbol{a}_2\ \cdots\ \boldsymbol{a}_n] \in \mathbf{Z}_q^{m\times n}$, $\boldsymbol{d} \in \mathbf{Z}_q^m$, $\boldsymbol{c} \in \mathbf{R}_+^n$ and $\boldsymbol{Z}_q = \{0, 1, \cdots, q-1\}$.

Then we consider the polynomials $F[X_1, \cdots, X_n]$, $F[Y_1, \cdots, Y_m]$ and $F[X_1, \cdots, X_n, Y_1, \cdots, Y_m]$. We define the homomorphic mapping $\phi_{\boldsymbol{A}}$ as

$$\begin{aligned} \phi_{\boldsymbol{A}} : F[X_1, \cdots, X_n] &\rightarrow F[Y_1, \cdots, Y_m], \qquad (12)\\ X_i &\mapsto \boldsymbol{Y}^{\boldsymbol{a}_i} := Y_1^{a_{1i}} \cdots Y_m^{a_{mi}} \end{aligned}$$

Let $\phi_{\boldsymbol{A}}^i = \phi_{\boldsymbol{A}}(X_i) = Y_1^{a_{1i}} \cdots Y_m^{a_{mi}}$ for $1 \le i \le n$ and J and $I_{\boldsymbol{A}}$ be ideals defined by

$$\begin{aligned} J &= \langle Y_1^q - 1, \cdots, Y_m^q - 1\rangle \qquad (13)\\ I_{\boldsymbol{A}} &= \left\langle \phi_{\boldsymbol{A}}^1 - X_1, \cdots, \phi_{\boldsymbol{A}}^n - X_n, Y_1^q - 1, \cdots, Y_m^q - 1\right\rangle\\ &\subset F[X_1, \cdots X_m, Y_1, \cdots, Y_n]. \qquad (14) \end{aligned}$$

Then we introduce the following definition [13]:

Definition 1
A monomial order $<_{\boldsymbol{c}}$ on $F[X_1, \cdots, X_n, Y_1, \cdots, Y_m]$ is *adopted* to an integer programming $\mathrm{IP}_{\boldsymbol{A},\boldsymbol{c},q}(\boldsymbol{d})$ if it has the following properties:

- (Elimination) Any monomial containing at least one of $Y_j, 1 \le j \le m$ is greater than any monomial containing only X_i's
- (Compatibility with $\boldsymbol{c}$) For any $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbf{Z}_q^n$ with $\phi_{\boldsymbol{A}}(\boldsymbol{X}^{\boldsymbol{x}_1}) \equiv \phi_{\boldsymbol{A}}(\boldsymbol{X}^{\boldsymbol{x}_2}) \bmod J$, if $\boldsymbol{c}^T\boldsymbol{x}_1 < \boldsymbol{c}^T\boldsymbol{x}_2$, then $\boldsymbol{X}^{\boldsymbol{x}_1} <_{\boldsymbol{c}} \boldsymbol{X}^{\boldsymbol{x}_2}$.

Let $\psi := \boldsymbol{Y}^{\boldsymbol{d}} = Y_1^{d_1} \cdots Y_m^{d_m}$. Then the extended Conti-Traverso algorithm proposed in [13] is described as follows:

Algorithm 1
(**Extended Conti-Traverso Algorithm** [13])
1: Compute the Gröbner basis $\mathcal{G}$ of the ideal $I_{\boldsymbol{A}}$ with respect to a fixed adapted monomial order $<_{\boldsymbol{c}}$.
2: Compute the normal form $\bar{\psi}^{\mathcal{G}}$
3: Return the exponent of $\bar{\psi}^{\mathcal{G}}$

When the cost coefficient $\boldsymbol{c} = (c_1, \cdots, c_n)$ contains a negative value, we cannot apply the above algorithm. The way to avoid the problem have been also indicated in [13].

For a given matrix $\boldsymbol{A} \in \mathbf{Z}_q^{m\times n}$, consider an enlarged matrix

$$\boldsymbol{A'} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{O}\\ \boldsymbol{E} & \boldsymbol{E}\end{pmatrix}, \qquad (15)$$

where $\boldsymbol{O}$ is the $m \times n$-zero matrix and $\boldsymbol{E}$ is the $n \times n$-identity matrix. The matrix $\boldsymbol{A'}$ is called the Lawrence Lifting of A. Let $\bar{\boldsymbol{d}} = (q-1, \cdots, q-1) \in \mathbf{Z}_q^n$ and $\tilde{\boldsymbol{d}} = (\boldsymbol{d}, \bar{\boldsymbol{d}}) \in \mathbf{Z}_q^{m+n}$. We define the μ as

$$\mu = \max\left[\{|c_i| : c_i < 0, i = 1, \cdots, n\} \cup \{0\}\right], \qquad (16)$$

and let $\boldsymbol{c}_1 = (c_1 + \mu, \cdots, c_n + \mu) \in \mathbf{R}_+^n$ and $\boldsymbol{c}_2 = (\mu, \mu, \cdots, \mu) \in \mathbf{R}_+^n$ and $\boldsymbol{c'} = (\boldsymbol{c}_1, \boldsymbol{c}_2) \in \mathbf{R}_+^{2n}$. Then following theorem is valid [13].

Theorem 1 [13]
Let $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbf{Z}_q^n$. If $\boldsymbol{x} = (\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathbf{Z}_q^{2n}$ is an optimal solution of $\mathrm{IP}_{\boldsymbol{A'},\boldsymbol{c'},q}(\boldsymbol{d'})$ then $\boldsymbol{x}_1$ is an optimal solution of $\mathrm{IP}_{\boldsymbol{A},\boldsymbol{c},q}(\boldsymbol{d})$.

Since the problem $\mathrm{IP}_{\boldsymbol{A'},\boldsymbol{c'},q}(\tilde{\boldsymbol{d}})$ contains no negative cost coefficient and the above algorithm is applicable.

4 Multiuser detection based on the Extended Conti-Traverso algorithm

Unfortunately, ML multiuser detection problem described in (7) is quadratic programming problem, we can not apply the Conti-Traverso algorithm or Extended Conti-Traverso algorithm directly. Then we transform the problem (7) to the integer linear programming problem with modulo arithmetic condition.

4.1 Transformation of the ML detection problem

The problem (7) can be reformulated as

$$\begin{aligned} \tilde{\boldsymbol{b}}^* = \arg \min_{\tilde{\boldsymbol{b}}\in\{0,1\}^K} & 4\sum_{k=1}^{K} r_k\tilde{b}_k\\ &+ \sum_{(k,l)\in\mathcal{K}} (1-\tilde{b}_k)(1-\tilde{b}_l)q_{k,l}, \qquad (17) \end{aligned}$$

where $q_{k,l}$ denotes the (k,l) element of $\boldsymbol{Q}$ and $\mathcal{K} = \{(k,l) : k, l = 1, \cdots, K,\ k < l\}$.

Then we define the variables

$$z_{k,l} = \tilde{b}_k \oplus \tilde{b}_l \quad (k,l) \in \mathcal{K}. \qquad (18)$$

These variable satisfy the following equations for all $(k,l) \in \mathcal{K}$:

$$\begin{aligned} \tilde{b}_k + \tilde{b}_l + z_{k,l} &\equiv 0 \mod 2, \qquad (19)\\ 1 - 2z_{k,l} &= (1-2\tilde{b}_k)(1-2\tilde{b}_l). \qquad (20) \end{aligned}$$

Substituting (20) to (17) and eliminating the constant factor, we obtain the following problem.

$$\begin{array}{ll} \text{minimize} & 2\sum_{k=1}^{K} r_k x_k - \sum_{(k,l)\in\mathcal{K}} q_{k,l} z_{k,l} \\ \text{subject to} & x_k \in \{0,1\} \quad \forall k = 1,\cdots,K \\ & z_{k,l} \in \{0,1\} \quad \forall (k,l) \in \mathcal{K} \\ & x_k + x_l + z_{k,l} \equiv 0 \bmod 2 \quad \forall (k,l) \in \mathcal{K} \end{array} \tag{21}$$

Let $n = (K^2+K)/2$, $m = (K^2-K)/2$ and $\pi : \{1,\cdots,m\} \to \mathcal{K}$ be the mapping such that $\pi(1) = (1,2)$, $\pi(2) = (1,3)$, $\cdots$, $\pi(m) = (K-1,K)$. Then we define the variable $\boldsymbol{x} \in \mathbf{Z}_2^n$, $\boldsymbol{c} \in \mathbf{R}^n$ and $\boldsymbol{A} \in \mathbf{Z}_2^{m\times n}$ as

$$\boldsymbol{x} = [x_1,\cdots,x_K,z_{(1,2)},\cdots,z_{(K-1,K)}] \tag{22}$$

$$\boldsymbol{c} = [2r_1,\cdots,2r_K,q_{(1,2)},\cdots,q_{(K-1,K)}] \tag{23}$$

$$a_{i,j} = \begin{cases} 1 & \text{if } j \in \pi(i) \text{ or } j = K+i \\ 0 & \text{otherwise} \end{cases}, \tag{24}$$

where $a_{i,j}$ is the (i,j)-element of $\boldsymbol{A}$. Then we can write the problem (21) in the form of $\mathrm{IP}_{\boldsymbol{A},\boldsymbol{c},2}(\boldsymbol{0})$. The cost coefficient $\boldsymbol{c}$ does not always has only nonnegative values, hence when it has any negative value, we should solve the problem $\mathrm{IP}_{\boldsymbol{A}',\boldsymbol{c}'2}$ as described in the previous section.

Example 1
Suppose a two-user system with signature sequences characterized by the correlation matrix

$$\boldsymbol{W} = \begin{bmatrix} 1 & 0.7 \\ 0.7 & 1 \end{bmatrix} \tag{25}$$

and amplitudes are $e_1 = 1, e_2 = 1$. If the output of matched filter is $\boldsymbol{r} = (-1, 0.6)$, the problem we should solve is described as

$$\begin{array}{ll} \text{minimize} & -2x_1 + 1.2x_2 - 0.7x_3 \\ \text{subject to} & x_1,x_2,x_3 \in \{0,1\} \\ & x_1 + x_2 + x_3 \equiv 0 \bmod 2 \end{array} \tag{26}$$

Now $\mu = 2$ and $\boldsymbol{c}' = (0, 3.2, 1.3, 2, 2, 2)$ and transformed problem is

$$\begin{array}{ll} \text{minimize} & 3.2x_2' + 1.3x_3' + 2x_4' + 2x_5' + 2x_6' \\ \text{subject to} & x_i' \in \{0,1\}, i = 1,\cdots,6 \\ & x_1' + x_2' + x_3' \equiv 0 \bmod 2 \\ & x_1' + x_4' \equiv 1 \bmod 2 \\ & x_2' + x_5' \equiv 1 \bmod 2 \\ & x_3' + x_6' \equiv 1 \bmod 2 \end{array} \tag{27}$$

We can compute the Gröbner basis using the Buchberger algorithm. We find the Gröbner basis consists of 9 polynomials and the normal form of $\boldsymbol{Y}^{\boldsymbol{d}} = Y_2Y_3Y_4$ by the Gröbner basis turns out to be $X_1X_3X_5$. The exponent of the monomial is $(1,0,1,0,1,0)$ and the output of the ML detector is $\tilde{\boldsymbol{b}} = (1,0)$ and hence $\boldsymbol{b} = (-1,1)$.

Example 2
Suppose a three-user system with correlation matrix

$$\boldsymbol{W} = \begin{bmatrix} 1 & -1/7 & 3/7 \\ -1/7 & 1 & 3/7 \\ 3/7 & 3/7 & 1 \end{bmatrix} \tag{28}$$

and amplitudes are $e_1 = 1, e_2 = 1, e_3 = 1$. Let assume that the output of matched filter is $\boldsymbol{r} = (0.5, 1.8, -2.2)$. In this case, the Gröbner basis consists of 19 polynomials and the normal form of $\boldsymbol{Y}^{\boldsymbol{d}}$ by the Gröbner basis turns out to be $X_3X_5X_6X_7X_8X_{10}$. The exponent of the monomial is $(0,0,1,0,1,1,1,1,0,1,0,0)$ and the output of the ML detector is $\tilde{\boldsymbol{b}} = (0,0,1)$ and hence $\boldsymbol{b} = (1,1,-1)$.

4.2 Discussions

Here we discuss the complexity of the ML detection algorithm based on the proposed algorithm. The complexity depends on the calculation of the Gröbner basis and the calculation of the normal form. It is very difficult to estimate the complexity for these operations. In general, it requires enormous amounts of time to compute a Gröbner basis using the Buchberger algorithm and it is difficult to implement the proposed algorithm even for the moderate number of users.

As described in section 2, the ML multiuser detection problem can be formulated as the 0-1 quadratic programming problem, and it is generally NP-hard problem. On the other hand, the ML detection can be implemented in polynomial time when the off-diagonal elements of correlation matrix are all non-positive [2]-[4]. They transform the ML multiuser detection problem to the minimum cut problem. The minimum cut problem can be solved by the the cycle-canceling algorithm. We conjecture that there are some kind of relations between those algorithm and proposed algorithm.

5 Conclusion

In this paper, we proposed the ML multiuser detection algorithm based on the Gröbner bases. The key idea is that the ML detection problem can be transformed to the integer linear programming with modulo arithmetic conditions and it can be solved by the extended Conti-Traverso algorithm. The complexity of the proposed detection algorithm is not as efficient as other ML detection algorithms such as A* algorithm because the complexity to calculate the Gröbner bases is very large in general. The algebraic structure of the multiuser detection problem will be found out through this research. It includes the relation between the cycle-canceling algorithm and proposed algorithm for a certain special cases of multiuser detection problem. It is the future work.

Acknowledgment

One of the authors, Shunsuke Horii, would like to acknowledge all members of Matsushima Lab. and Hirasawa Lab. in Waseda Univ. for their helpful suggestions to this work. This research is partially supported by No.20200044 of Grant-in-Aid for Scientific Research on Innovative Areas. and No.22560395 of Grant-in-Aid for Scientific Research Category (C), Japan Society for the Promotion of Science.

References

[1] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[2] C. Sankaran and T. Ephremides, "Solving a class of optimum multiuser detection problems with polynomial complexity," IEEE Trans. Inf. Theory, vol. 44, pp. 1958-1961, Sept. 1998.

[3] S. Ulukus and R.D. Yates, "Optimum multiuser detection is tractable for synchronous CDMA using m-sequences," IEEE Commun. Lett., vol. 2, pp. 89-91, Apr. 1998.

[4] C. Schlegel and A. Grant, "Polynomial complexity optimal detection of certain multiple-access systems," IEEE Trans. Inf. Theory, vol. 46, pp. 2246-2248, Sept. 2000.

[5] P. Németh, L. K. Rasmussen, and T. M. Aulin, "Maximum-likelihood detection of block coded CDMA using A* algorithm," in Proc. Int. Symp. Inf. Theory, Washington, DC, June 2001, p. 88.

[6] A. Yener, R. D. Yates, and S. Ulukus, "A nonlinear programming approach to CDMA multiuser detection," in Proc. Asilomar Conf. Signals, Systems, Computing, Pacific Grove, CA, Oct. 1999, pp. 1579-1583.

[7] S. Ito, T. Wadayama and I. Takumi, "A convex optimization based multiuser detection algorithm for synchronous CDMA systems," IEICE Technical Report, vol. 109, No. 143, IT2009-19, pp. 79-84. July, 2009.

[8] X. F. Wang, W. S. Lu, and A. Antoniou, "A near-optimal multiuser detection for CDMA channels using semidefinite programming relaxation," in Proc. Int. Symp. Circuits System, 2001, pp. 298-301.

[9] P. H. Tan and L. K. Rasmussen, "The application of semidefinite programming for detection in CDMA," IEEE J. Select. Areas Commun., vol. 19, pp. 1442-1449, Aug. 2001.

[10] W. K. Ma, T. N. Davidson, K. M. Wong, Z. Q. Luo, and P. C. Ching, "Quasi-maximum-likelihood multiuser detection by semi-definite relaxation with application to synchronous CDMA," IEEE Trans. Signal Processing, vol. 50, pp. 912-922, Apr. 2002.

[11] M. Abdi, H. E. Hahas, A. Jard, and E. Moulines, "Semidefinite positive relaxation of the maximum-likelihood criterion applied to multiuser detection in a CDMA context," IEEE Signal Processing Lett., vol. 9, pp. 165-167, June 2002.

[12] P. Conti and C. Traverso, "Buchberger algorithm and integer programming," in Proc. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-9), ed. H. F. Mattson, T. Mora, and T. R. N. Rao, LNCS, no. 539, pp. 130-139, Springer-Verlag, Oct. 1991.

[13] D. Ikegami, Y. Kaji, "Maximum Likelihood Decoding for Linear Block Codes Using Gröbner Bases," IEICE Trans. Fundamentals, vol. E86-A, No. 3, pp. 643-651, March 2003.