A New Method for Variable Elimination in Systems of Inequations

Farhad Shirani Chaharsooghi, Mohammad Javad Emadi, Mahdi Zamanighomi and Mohammad Reza Aref

Electrical Engineering Department, Sharif University of Technology, Tehran, Iran.
Email: fshirani@ee.sharif.edu, emadi@ee.sharif.edu, m_zamani@ee.sharif.edu, aref@sharif.edu

Abstract—In this paper, we present a new method for variable elimination in systems of inequations which is much faster than the Fourier-Motzkin Elimination (FME) method. In our method, a linear Diophantine problem is introduced which is dual to our original problem. The new Diophantine system is then solved, and the final result is calculated by finding the dual inequations problem. We introduce a problem in the interference channel with multiple nodes and solve it with our new method. Next, we generalize our method to all problems involving FME and in the end we compare our method with the previous method. We show that our method has many advantages in comparison to the previous method. It does not produce many of the redundant answers of the FME method. It also solves the whole problem in one step whereas the previous method uses a step by step approach in eliminating each auxiliary variable.

I. INTRODUCTION

The FME Method was first introduced by Fourier [1] in 1827 and was rediscovered in Motzkin’s thesis in 1936 [2]. Considering the set of inequations $Ax \leq b$, $A \in \mathbb{R}^{m,n}$, $b \in \mathbb{R}^n$ the method provides a scheme for determining the existence of a real or integer solution to the given problem. The method uses a step by step algorithm, in which each step reduces the dimension of the answer space by projecting the answer space on a hyperplane. The procedure continues until the dimension is reduced to one; if the one dimensional answer is feasible, then the solution exists. A dual mode for FME was introduced in 1972 by Dantzik [3].

The FME method is widely used in solving rate region problems since there is often the need to eliminate the auxiliary variables introduced into the problem from the resulting inequations and hence reduce the dimension of the solution space by finding its projection on a given plane. The complexity of calculation in each step is of the order of $k^2 \frac{n^2}{4}$, with $k$ being the number of constraints in the system of inequations. This complexity makes the method unfeasible for high dimensional problems. There have been many attempts to decrease the calculation time of the method. In 1996, Kebler [4] introduced a parallel computation method which was more efficient when solving the elimination problem on a computer.

In this paper, we present a new method for eliminating auxiliary variables in inequations which is much faster than the FME method. In our method, we first introduce a linear Diophantine problem which is dual to the original problem. We then proceed by solving this new Diophantine system, next we calculate the final result by finding the dual inequations system. Our new method uses the algorithm Normaliz to find the Hilbert basis of the solution space of the given Diophantine problem.

Normaliz was first introduced as a program in 1997 by R. Koch. In 2003, the algorithm was presented in Koch’s thesis [5]. Normaliz was originally introduced to compute the lattice points in a lattice polytope and the integral closure of a monomial ideal. Koch mentions in his thesis that the algorithm may be extended to find the Hilbert basis of the solution space of a system of linear Diophantine equations. However, applying the algorithm introduced in [5] to information theoretic problems is still time-consuming. In 2010, Bruns and Ichim [6] introduced a dual algorithm which is much faster when applied to problems with a greater number of constraints than auxiliary variables. Since this is the case in almost all information theory problems, we use this method to find the desired Hilbert Basis solution.

One of the most important fundamental channels in communication systems is the Interference Channel (IC). The IC was initiated by Shannon [7]. Simple outer bounds for the IC were established by Ahlswede [8]. Later, Carleial [9], using superposition encoding and sequential decoding, characterized an achievable rate region for general discrete memoryless IC. In the IC each receiver is only interested in the message from its corresponding sender. However, it might decode messages from other senders to reduce the interference effect. Han and Kobayashi (HK) utilized rate splitting techniques in [10], and applied simultaneous superposition coding techniques to establish the largest inner bound introduced for the general IC to date. Computing the capacity region of general IC is still an open problem, but in special cases such as strong interference regime the capacity region has been established, and the region was the same as the HK rate region [11]. In the method used to achieve the HK rate region, the messages are split into two parts, the private and common parts; private messages are decoded by the corresponding receiver, while the common messages are decoded by all receivers.

Rate splitting has become a prominent tool for solving rate region problems. However, there is a drawback to the method in that solving the channel with the new split messages yields a system of inequations based on the split-rates. Since we are interested in each sender’s total rates, the auxiliary variables must be eliminated. The FME method is needed to eliminate
these auxiliary rates.

The rest of the paper is organized as follows: In Section II, we first introduce our model of an $l$ transmitter-receiver interference channel. In Section III, we introduce a problem in the IC. In this section, we use some simplifying assumptions, since the goal of the section is to explain the new elimination method. In Section IV, we solve the problem with our new method. In Section V, we present a generalized algorithm for our new method which could be applied to any problem involving FME. In Section VI, we present results of applying our new method to several problems which were solved previously using the FME method. Section VII concludes the paper.

II. CHANNEL MODEL

In this section, we introduce our model of IC. We denote random variables by upper case letters e.g. $X$, their realizations are presented by lower case letters e.g. $x$ in finite sets denoted by $x$. We use $x_k^l$ to denote the vector $x_i, x_{i+1}, \ldots, x_k$. We denote $x^n_i$ if $i=1$, while for $i=1$ and $k=l$, we show the vector by $x$. Also, if $i=1$ and $k=l$, we show the vector by $x^n_i$. Furthermore, $x^n_{i \to l}$ is the compact form of $(x_i, x_{i+1}, \ldots, x_n)$ where $x_i = (x_{i1}, \ldots, x_{id})$.

A discrete Interference Channel, with $l$ senders and $l$ receivers is the $2l+1$ tuple $(x, p(y|x), y')$ where $x_i$ are the input alphabets, $y_i$ are the output alphabets for $i=1,2,\ldots,l$ and $p(y|x)$ is the conditional probability of the channel. Each decoder is only interested in decoding its corresponding sender’s message; however, in order to reduce the interference effect, receivers might decode the message from other senders as well. The channel is memoryless and time invariant in the sense that

$$p(y|x^n_{i\to l}) = p(y|x|y^n_{i\to l}).$$

A $(2^nR_1, 2^nR_2, \ldots, 2^nR_l, n)$ code consists of (i) $l$ message sets $w_i = 1, 2, \ldots, 2^nR_i, i \in [1:l]$, (ii) $l$ encoding functions $f_u = w_u \to x^n_u, u \in [1:l]$, (iii) $l$ decoding functions $g_u(\cdot)$ where $W_i = g_u(Y^n_u), u \in [1:l]$.

We define the average probability of error for this code as $P(e^{(n)}) = Pr(\bigcup_{i=1}^{l} (W_i \neq W_i))$. A nonnegative rate $l$-tuple $(R_1, R_2, \ldots, R_l)$ is said to be achievable if there exists a code $(2^nR_1, 2^nR_2, \ldots, 2^nR_l, n)$ for which $P(e^{(n)}) \to 0$ as $n$ tends to infinity.

III. PROBLEM STATEMENT

In this section, we present our coding strategy which is a generalization of the method used in [10]. We describe the problem in solving the resulting inequations with the conventional FME method. After stating the problem, we introduce our method and compare the results with the former procedure.

Since our goal in this paper is to introduce an alternative elimination method for the FME method, we use some simplifying assumptions in the channel. We consider the channel to be symmetric in the sense that the $i$th sender sends the same amount of information to all receivers other than its own corresponding receiver. This allows each sender to send the same common message to all receivers. We split each message $W_i$ into common and private parts $(W_{ic}, W_{ip})$. The common part of the message is decoded by all receivers while the private part is decoded only by the $i$th receiver. Another suitable assumption would have been to assume a sense of degradedness between the receivers in the following way: assume that receiver $i_1$ receives all the common massages sent by sender $i$; receiver $i_2$ receives all the common messages received by the receivers other than $i_1$, and so on. In this case we had to split the message in each sender to $l$ common parts and one private part in the following way: split the message $W_i$ into $(W_{ic_1}, W_{ic_2}, \ldots, W_{ic_l}, W_{ip})$. $W_{ic_l}$ is decoded by the receiver with the least information about the massage from sender $i$; the receiver with the second least information about this message decodes $W_{ic_{l-1}}$, $W_{ic_{l-2}}$, and so on. The rest of the solution would stay the same. Clearly, the symmetric case mentioned above is a special case of this latter case. Since the two cases have the same solution, and for the sake of simplicity, we solve the channel for the symmetric case in this paper.

Codebook Generation:

Let $Z_1 = \{U_1, U_2, \ldots, U_l, X_1, X_2, \ldots, X_l, Y_1, Y_2, \ldots, Y_l, Q\}$, where $Q$ is the time-sharing variable. Let $x_l$ denote the set of all joint p.m.f.s $p_1$ on $Z_1$, which can be written in the form

$$p(z_1) = p(q) \prod_{i=1}^{l} (p(u_i|q)p(x_i|u_i,q)p(y_1,y_2,\ldots,y_l|x_1,x_2,\ldots,x_l))$$

For any $p_1$ defined above, generate $2^{nR_{ic}}$, $i \in [1:l]$, i.i.d $u_{ic}^n(w_{ic})$ where $w_{ic} \in [1:2^{nR_{ic}}]$. For each $u_{ic}^n(w_{ic})$, generate $2^{nR_{ip}}$, i.i.d $x_{ip}^n(w_{ip}, w_{ic})$. The time-sharing variable has no impact on the rest of the proof and for the sake of brevity, we ignore it until the end of the proof where we bound its cardinality.

Encoding:

At the beginning of each block, the $i$th sender picks related $(u_{ic}^n, x_{ip}^n)$ according to $\prod_{i=1}^{l} p(u_{ic,j}|p(x_{ic,j}|u_{ic,j})$ and sends it.

Decoding:

At the end of each block, the $i$th receiver finds $(x_{ic}^n, u_{ic}^n, u_{ip}^n, \ldots, u_{ip}^n)$ such that:

$$(x_{ic}^n(w_{ip}, w_{ic}), u_{ic}^n(w_{ic}), u_{ip}^n(w_{ip}), \ldots, u_{ip}^n(w_{ic})) \in A_e$$

Without loss of generality we consider the case where all senders have sent index 1 as their messages. We investigate all possible scenarios in the first decoder. The decoder must decode messages $(w_{1p}, w_{ic}, w_{2p}, \ldots, w_{ic})$, the decoding is errorless if $\hat{w} = (\hat{w}_{1p}, \hat{w}_{ic}) = (1, 1)$. Using the same method as in [12] and by the AEP rule, it is clear that the probability of error approaches zero as $n \to \infty$ (e.g. rate $l$-tuple is achievable) if the rates satisfy the following set of equations:

$$R_{1p} + \alpha_1 R_{1c} + \alpha_2 R_{2c} + \ldots + \alpha_l R_{lc} \leq I_{1,\alpha_1,\alpha_2,\ldots,\alpha_l} \quad (1)$$

where

$$\alpha_i \in \{0, 1\}$$

$$I_{1,\alpha_1,\alpha_2,\ldots,\alpha_l} = I(X_1, U_S; Y_1|U_{S'}$$
and \( U_1 \in U_S \) if \( \alpha_1 = 1 \); also, for \( \alpha_1 = 0 \), we have \( U_1 \in U_{S'} \). We note that \( R_1 - R_{1c} = R_{1p} \), substituting into (1) we have

\[
R_1 - \alpha_1 R_{1c} + \alpha_2 R_{2c} + \ldots + \alpha_l R_{lc} \leq I_{1, \alpha_1, \alpha_2, \ldots, \alpha_l}, \quad \alpha_i \in \{0, 1\}
\]

These are the inequations for decoder 1. We rewrite the inequations for all decoders in matrix form:

\[
\begin{pmatrix}
1 & 0 & \ldots & 0 & 0 \\
1 & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 1 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & 1 \\
0 & 0 & \ldots & 0 & 1 \\
\end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_l \\ \vdots \\ \vdots \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_l \\ \vdots \\ \vdots \end{pmatrix} \leq \begin{pmatrix} I_{1,00} \\ I_{1,01} \\ \vdots \\ I_{1,11} \\ I_{2,00} \\ \vdots \\ I_{2,11} \end{pmatrix}
\]

If we denote \( A \) as the matrix whose rows are all possible binary \( l \)-tuples starting from \((0, 0, \ldots, 0)\) in an increasing order, then \( A_i \) is the matrix formed by multiplying the \( i \)th column in \( A \) by \(-1\). We show the rate coefficients matrix in (2) with \( C_l \). We show the rate vector with \( R^l \), and the mutual information vector with \( I_l \), so we may write (2) in compact form as \( C_l R^l \leq I_l \). To clarify the method of forming the above mentioned inequations, we give the following example, which illustrates the inequations for a two sender-receiver interference channel:

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 \\
1 & 0 & -1 & 0 \\
1 & 0 & -1 & 1 \\
0 & 1 & 0 & 0 \\
0 & 1 & 0 & -1 \\
0 & 1 & 1 & 0 \\
0 & 1 & 1 & -1 \\
\end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \\ R_{1c} \\ R_{2c} \end{pmatrix} \leq \begin{pmatrix} I_{1,00} \\ I_{1,01} \\ I_{1,11} \\ I_{2,00} \\ I_{2,01} \\ I_{2,10} \\ I_{2,11} \end{pmatrix}
\]

Note that these are the same inequations given in (12). To solve this system with the conventional FME method, one must eliminate all of the variables \( R_{ic}, i \in [1 : l] \); this process takes \( l \) rounds of applying FME to the matrix. According to (12), the size of the matrix grows at a worst case rate of \( \frac{c^l}{2} \) each round. This complexity renders the aforementioned method impractical for \( l \) larger than 2, since, after applying FME, one must eliminate the redundant inequations in the resulting matrix using an exhaustive search. Finding the redundant inequations often needs more time than eliminating the auxiliary variables, which itself is a time-consuming process.

IV. OUR NEW METHOD

Here, we present a new method for solving (2) which not only requires much less calculation in comparison with the FME but also produces no redundant inequations assuming the mutual-informations on the right side of the inequations are independent. Before proceeding with the solution, we present some definitions. We show the matrices resulting from \( l \) rounds of FME by \( C^*_l \) and \( I^*_l \), so the resulting inequations can be written in the form \( C^*_l R^l \leq I^*_l \). Note that the second \( l \) columns of \( C^*_l \) are zero. It is also clear that if we show the rows of \( C_l \) by \( C_l(I_1, \alpha_1, \alpha_2, \ldots, \alpha_l) \), then all rows of \( C^*_l \) and \( I^*_l \) can be shown by

\[
C^*_l(k) = \sum_{i, \alpha_1, \alpha_2, \ldots, \alpha_l} a_k(i, \alpha_1, \alpha_2, \ldots, \alpha_l) C_l(I_1, \alpha_1, \alpha_2, \ldots, \alpha_l),
\]

\[
I^*_l(k) = \sum_{i, \alpha_1, \alpha_2, \ldots, \alpha_l} a_k(i, \alpha_1, \alpha_2, \ldots, \alpha_l) I_l(I_1, \alpha_1, \alpha_2, \ldots, \alpha_l),
\]

where

\[
\alpha_i \in \{0, 1\}, i \in [1 : l], a_k(i, \alpha_1, \alpha_2, \ldots, \alpha_l) \geq 0
\]

Let \( G_{C_l} \) be the solution space of the inequations in (2) for rates \( R_1, R_2, \ldots, R_l \), and let \( G_{C^*_l} \) be the solution space of \( C^*_l R^l \leq I^*_l \). Furthermore, we define the matrix \( D \) as the matrix whose rows are formed by all of the linear combinations of \( C_l(I_1, \alpha_1, \alpha_2, \ldots, \alpha_l) \) with positive coefficients and with the property that the second \( l \) columns of \( D \) are zero. In other words, \( D \) is a row of \( D \) if

\[
D = \sum_{i, \alpha_1, \alpha_2, \ldots, \alpha_l} a_i(i, \alpha_1, \alpha_2, \ldots, \alpha_l) C_l(I_1, \alpha_1, \alpha_2, \ldots, \alpha_l)
\]

with the following conditions:

\[
a_k(i, \alpha_1, \alpha_2, \ldots, \alpha_l) \geq 0
\]

\[
D^2_{l+1} = 0;
\]

We define \( G_{D_l} \) as the solution space of the following inequations:

\[
D^2_l R^l \leq I_{D_l}
\]

where

\[
I_{D_l} = \sum_{i, \alpha_1, \alpha_2, \ldots, \alpha_l} a_i(i, \alpha_1, \alpha_2, \ldots, \alpha_l) I_l(I_1, \alpha_1, \alpha_2, \ldots, \alpha_l)
\]

Theorem 1: \( G_{C^*_l} \) is equal to \( G_{D_l} \).

Proof: The proof is straightforward. Since all rows of \( D_l \) are linear combinations of rows of \( C_l \) with positive coefficients, all inequations in (5) result from inequations in (2). Hence, we have \( G_{C_l} \subseteq G_{D_l} \), and by the FME, we know that \( G_{C_l} \) is equal to \( G_{C^*_l} \) for \( (R_1, R_2, \ldots, R_l) \), we have \( G_{C^*_l} \subseteq G_{D_l} \). On the other hand, since all the rows of \( C^*_l \) are linear combinations of rows of \( C_l \) with the property that for each row \( C^*_l \), \( C^*_l^{2l+1} = 0 \), any row \( C^*_l \) of \( C^*_l \) is a row of \( D_l \), and so \( G_{D_l} \subseteq G_{C^*_l} \) and the proof is complete. ■
Now, we propose that instead of finding \( G_{C_1} \), we try to find \( G_{D_i} \). From (4), we know that for every \( D \) in (3) we have
\[
\sum_{i, \alpha_1 \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_l} \sum_{i, \alpha_1 \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_l} \alpha_{i, \alpha_1 \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_l} = \sum_{\alpha_{i, \alpha_1 \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_l}} a_{j, \alpha_1 \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_l} (6)
\]

Now we need to choose inequations in (5) whose linear combinations with positive coefficients produce all inequations in (5). Without loss of generality, we consider \( a_{j, \alpha_1 \alpha_2, \ldots, \alpha_l} \in \mathbb{Z}^+ \). We give the following definition as in [13].

**Definition:** We call a set of vectors \( H \), generator vectors of \( S \), if every vector in \( S \) can be expressed as a linear combination of vectors in \( H \) with positive coefficients and no vector in \( H \) may be expressed in such a way by other vectors in \( H \). Such a set of vectors is called the Hilbert Basis of the vector space \( S \).

The problem of finding a Hilbert Basis for the solutions of a Diophantine system of equations such as (6) has many solutions. One solution is to use an algorithm called Normaliz introduced by Koch in [5]. We use this method to solve (6). If the set of \( a_{j, \alpha_1 \alpha_2, \ldots, \alpha_l} \), \( j = 1, \ldots, l, \alpha_i \in \{0, 1\} \) is an answer for (6), then we have the following inequation for \( R_1, \ldots, R_l \):
\[
\sum_{j=1}^{l} \left( \sum_{\alpha_i} a_{j, \alpha_1 \alpha_2, \ldots, \alpha_l} R_j \right) \leq \sum_{\alpha_{i, \alpha_1 \alpha_2, \ldots, \alpha_l}} a_{j, \alpha_1 \alpha_2, \ldots, \alpha_l} I_{j, \alpha_1 \alpha_2, \ldots, \alpha_l}
\]

Since Normaliz provides a Hilbert Basis solution for the equations in (6), and since each solution for (6) represents a unique equation in (5) and adding two answers from (6) with positive coefficients is equivalent to adding two inequations in (5) with positive coefficients, the resulting inequations contain all the non-redundant inequations in (5). Hence, by applying Normaliz, we can calculate the solution to our original problem. Since the dimension of the Diophantine space in (4) is much greater than the number of constraints we have, it is better to use Normaliz Dual as suggested in [6]. Our results for the two sender-receiver IC are the same as HK rate region in [10].

To this point, we have found the rate region by eliminating the auxiliary variables. Since, in the case of the above channel, all the mutual-informations \( I_{l, \alpha_1 \alpha_2, \ldots, \alpha_l} \) are independent of each other (i.e. they don’t have a clear relation with each other), there are no redundant inequations in our final system of inequations and so by the Caratheodory theorem [13] \( Q \) is bounded by the number of resulting inequations after applying Normaliz and finding the dual system.

**V. Generalization to Other Problems**

The method proposed above may be used in any other problem which could be solved using the FME. The following algorithm is used:
1. Define the encoding and decoding schemes.
2. Find the inequalities matrix corresponding to the defined schemes.
3. Write the Diophantine equations of the matrix.
4. Use Normaliz to solve the Diophantine problem.
5. For each answer vector for the Diophantine problems, write the corresponding inequation.

**VI. Simulation and Results**

Here, we use our method to solve some problems which have been solved using the FME method previously. The simulation results are illustrated in Table I.

<table>
<thead>
<tr>
<th>Name</th>
<th>Number of constraints</th>
<th>Number of aux. variables</th>
<th>Basis Elements</th>
<th>Non-Redundant Elements</th>
<th>t (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HK</td>
<td>l=2</td>
<td>8</td>
<td>2</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>HK</td>
<td>l=3</td>
<td>24</td>
<td>3</td>
<td>153</td>
<td>153</td>
</tr>
<tr>
<td>HK</td>
<td>l=4</td>
<td>64</td>
<td>4</td>
<td>56384</td>
<td>56384</td>
</tr>
<tr>
<td>Ref. 15</td>
<td></td>
<td>29</td>
<td>6</td>
<td>286</td>
<td>60</td>
</tr>
<tr>
<td>Ref. 18</td>
<td></td>
<td>12</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

The results are obtained from running Normaliz 2.2 on a 2.4 i5 CPU. The 4th column indicates the number of inequations resulting from applying our method while the 5th column indicates the number of non-redundant constraints. Note that in cases such as [15] and [16] where there are certain relations between mutual-informations on the right side of the inequations, there may be redundant answers in our method. However all these redundant answers will be present in the FME case as well. Table I shows the efficiency of our method in comparison to the FME method. There are several features of our method that make it more efficient in comparison with the former method. One feature is that the FME method eliminates one variable at a time, while our method eliminates all variables in one step. Another feature is that our method is much faster compared to the previous method. Another important advantage of the new method is that it doesn’t introduce many of the redundant inequation present in the FME solution. Note that one of the most time-consuming parts of the FME method is the removal of inequations which are linear combinations of previous inequations with positive coefficients. This process uses an exhaustive search and is very inefficient. Our method doesn’t introduce any such redundant answers.

**VII. Conclusion**

In this paper, we introduced a new method for performing variable elimination in systems of inequations. We illustrated the implementation of our new method on a special case of IC. A generalization of the method was presented and in the end some simulation results were compared with the actual results after applying FME and removing redundant answers. It was shown that our new method is much faster and more efficient than the FME method. Our method eliminates all variables in one step while the FME method uses a step by step approach.
Also, our method produces fewer redundant inequations in comparison to the FME method.

ACKNOWLEDGMENTS

We would like to express our appreciation for the ISSL Group of Sharif University of Technology and specially B. Akhbari and M. Mirmohseni for their valuable comments.

REFERENCES


