Lecturas Matemáticas
Volumen **27** *(2006), páginas 5–16*

Short solutions for a linear Diophantine equation

H. Esmaeili
Bu-Ali Sina University, Hamedan, Iran

Abstract. It is known that finding the shortest solution for a linear Diophantine equation is a NP problem. In this paper we have devised a method, based upon the basis reduction algorithm, to obtain short solutions to a linear Diophantine equation. By this method we can obtain a short solution (not necessarily the shortest one) in a polynomial time. Numerical experiments show superiority to other methods which use generalizations of the Euclid's algorithm.

Key words and phrases. Linear Diophantine Equation, Short Solution, Basis Reduction Algorithm.

2000 AMS Mathematics Subject Classification. 11D04.

Resumen. En este artículo establecemos un método, basado en el algoritmo de reducción de las bases, para obtner soluciones cortas de una ecuación diofántica lineal en tiempo polinomio. Los resultados numéricos obtenidos muestran cierta superioridad sobre otros métodos que usan generalizaciones del algoritmo euclídeo.

Palabras y frases clave. Ecuaciones diofánticas lineales, soluciones cortas, algoritmo de reducción de la base.

1. Introduction

One can solve the linear Diophantine equation

$$a^T x = b, \quad x \in \mathbb{Z}^n, \tag{1}$$

where $a \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$, in a polynomial time. There are some methods for solving (1) [2], all of which try to construct a unimodular matrix M (an integer matrix with $|\det M| = 1$) such that $a^T M = de_1^T$, where d is the g.c.d. of components of a, $d = \text{g.c.d.}\,(a)$, and e_1 is the first column of the identity matrix I. Then, $\frac{b}{d} M e_1$ is a special solution to (1) and the other columns of M consist

of a basis to the integer solution space for the homogeneous equation $a^T x = 0$. From a computational point of view, it is important that absolute values of components of M be small (it can be theoretically proved that matrices M with absolutely small components do exist). There are algorithms that provide a unimodular matrix M with a small first column, while the other columns can grow rapidly [2]. Indeed, the main difficulty in working with integers is the rapid growth of the intermediate results [1, 5]. Hence, it is important to provide algorithms that restrain the growth of intermediate results. Some algorithms for computing g.c.d. can be found in [2], where they are compared from a numerical point of view.

In this paper, we have provided an algorithm to find a short solution to the linear Diophantine equation (1) based upon the basis reduction algorithm for integer lattices.

An (integer) lattice in $\mathbb{Z}^m$ is the set of all integer linear combinations of the columns of an integer $m \times n$ matrix, say A. In this case, columns of A are said to be a generating set for the lattice. Suppose $L(A)$ is the lattice generated by the columns of A. Then $L(A) = \{y \in \mathbb{Z}^m \mid y = Ax, \quad x \in \mathbb{Z}^n\}$.

In lattice words, solving the system of linear Diophantine equations

$$Ax = b, \quad x \in \mathbb{Z}^n, \tag{2}$$

is the "existence problem", namely:

Is $b \in L(A)$? If so, we must write b as an integer linear combinations of columns of A.

Note that (1) is a special case of (2), corresponding to $m = 1$. By finding the shortest solution to (1), we mean to solve the integer least squares problem

$$\min \parallel y \parallel \quad s.t. \quad y \in L(A), \quad y \neq 0. \tag{3}$$

The main difference between the above problems is related to complexity. There is a polynomial algorithm for solving (2) while the other algorithms proposed in the literature are NP. The algorithm given in this paper for solving (3) approximately is based upon finding an appropriate representation of $L(A)$, for an adequate A, using the basis reduction algorithm. Since the basis reduction algorithm gives a basis with short and nearly orthogonal vectors, then we are expected to get a short solution to (1), albeit not the shortest one.

Section 2 presents the basis reduction algorithm and some of its properties. Section 3 shows how we can obtain a general solution to a linear Diophantine equation using the basis reduction algorithm. Then we use again the basis reduction algorithm to get a general solution containing shorter vectors. We compare numerically this method to other methods based upon a generalization of the Euclid's algorithm. Our numerical experiments show some superiority to other methods.

We should note that the solution of a single Diophantine equation as (1) is a step in the ABS algorithms for solving a system of Diophantine equations, providing some used parameters. So our result may also be useful for ABS methods.

2. The Basis Reduction Algorithm

A lattice in R^n is defined as follows.

Definition 1. A set $L \subseteq \mathbb{R}^n$ is called a lattice when there exists a basis $\{b_1, b_2, \ldots, b_k\}$ for L such that

$$L = \left\{ \sum_{j=1}^{k} \alpha_j b_j \,|\, \alpha_j \in \mathbb{Z}\, 1 \leq j \leq k \right\}. \tag{4}$$

Let A be a nonsingular matrix of order n and L be the lattice generated by the columns of A. If B is another nonsingular matrix, whose columns also generate L, then $|\det A| = |\det B|$. So this number is independent the choice of the basis, and is called the determinant of L, denoted by $\det L$. It is equal to the volume of the parallelepiped

$$\{\lambda_1 b_1 + \cdots + \lambda_n b_n \,|\, 0 \leq \lambda_j \leq 1, \quad j = 1, \ldots, n\},$$

where $b_1, \ldots, b_n$ is any basis for L. This gives the well-known Hadamard inequalitiy

$$\det L \leq \prod_{j=1}^{n} \parallel b_j \parallel .$$

It is trivial that equality occurs only if $b_1, \ldots, b_n$ are orthogonal, and that not every lattice has an orthogonal basis. A classic theorem of Hermite states that for each n there exists a number $c(n)$ such that every n-dimensional lattice L has a basis $b_1, \ldots, b_n$ with

$$\prod_{j=1}^{n} \parallel b_j \parallel \leq c(n)\, \det L.$$

Such a basis may be viewed as an approximation of an orthogonal basis. Hermite showed that we could take

$$c(n) = \left(\frac{4}{3}\right)^{n(n-1)/4}.$$

Minkowski improved this result by showing that even

$$c(n) = \frac{2^n}{V_n} \approx \left(\frac{2n}{\pi e}\right)^{n/2}$$

works, where V_n denotes the volume of the n-dimensional unit ball. However, for this choice of $c(n)$, there has not been found any polynomial algorithm

which can give us a basis satisfying the Hermite result. For $c(n) = 2^{n(n-1)/4}$, LENSTRA, LENSTRA & LOVĂSZ [6] designed a polynomial algorithm which gave such a basis (if the lattice is given by generators). For this purpose, they used the Gram-Schmidt orthogonalization.

Gram-Schmidt orthogonalization is an algorithm for deriving orthogonal vectors b_j^*, $1 \leq j \leq n$, from linearly independent vectors b_j, $1 \leq j \leq n$. Let $B = (b_1, \ldots, b_n)$ and $B^* = (b_1^*, \ldots, b_n^*)$ be matrices with columns b_j and b_j^*, respectively. The vectors b_j^* are defined as follow:

$$b_j^* = b_j - \sum_{k=1}^{j-1} r_{kj} b_k^*, \quad j = 1, \ldots, n, \tag{5}$$

where

$$r_{kj} = b_k^{*T} b_j \,/\, b_k^{*T} b_k^*, \quad k = 1, \ldots, j-1. \tag{6}$$

Theorem 1. [8]

i) *The Gram-Schmidt procedure constructs an orthogonal basis* $b_1^*, \ldots, b_n^*$ *for* R^n.
ii) b_k^* *is the component of* b_k *orthogonal to the subspace generated by* $\{b_1^*, \ldots, b_{k-1}^*\}$.
iii) $|\det B| = |\det B^*| = \prod_{j=1}^{n} \| b_j^* \|$.

Let $B = (b_1, \ldots, b_n)$ be a basis for L and $B^* = (b_1^*, \ldots, b_n^*)$ the basis obtained from the Gram-Schmidt orthogonalization procedure. We note that B^* is typically not a basis for L because the numbers r_{kj} are not all integer. A nearly orthogonal basis is defined as follows.

Definition 2. Let B be a basis for L, and B^* the basis obtained from the Gram-Schmidt orthogonalization procedure. B is called a reduced basis if

$$|r_{kj}| \leq \frac{1}{2}, \quad 1 \leq k < j \leq n, \tag{7}$$

and

$$\| b_{j+1}^* + r_{j,j+1} b_j^* \|^2 \geq \frac{3}{4} \| b_j^* \|^2, \quad j = 1, \ldots, n-1. \tag{8}$$

Theorem 2. [8] *Let* B *be a reduced basis for* L. *Then,*

i) $\| b_j^* \| \leq \sqrt{2} \, \| b_{j+1}^* \|$
ii) $\| b_1 \| \leq 2^{(n-1)/4} (\det L)^{1/n}$
iii) $\| b_1 \| \leq 2^{(n-1)/2} \min\{\| y \| \mid y \in L, \ y \neq 0\}$
iv) $\prod_{j=1}^{n} \| b_j \| \leq 2^{n(n-1)/4} \det L$

A polynomial time algorithm to obtain a reduced basis for a lattice, given by an initial basis, can be found in [3,4,6,7]. The algorithm consists of a sequence of size reduction and interchanges as described below.

Size reduction: If for any pair of indices k and j, $1 \leq k < j \leq n$, condition (7) is violated, then b_j is replaced by $b_j - \widehat{r}_{kj}\, b_k$, where $\widehat{r}_{kj} = \lceil r_{kj} \rfloor$ is the integer nearest to r_{kj}.

Interchange: If condition (8) is violated for an index j, $1 \leq j < n$, then b_j and b_{j+1} are interchange.

Therefore, the basis reduction algorithm is as follow.

Basis reduction algorithm

1) Let B be a basis for the lattice L.
2) Let B^* be the Gram-Schmidt orthogonalization of B.
3) For $j = 2, \ldots, n$ and for $k = j-1, \ldots, 1$, replace b_j by $b_j - \widehat{r}_{kj}\, b_k$, where $\widehat{r}_{kj} = \lceil r_{kj} \rfloor$ is the integer closest to r_{kj}.
4) If
$$\| b^*_{j+1} + r_{j,j+1} b^*_j \|^2 < \frac{3}{4} \| b^*_j \|^2 ,$$
for some j, b_j and b_{j+1} are interchange and we return to step 1 with the new basis B.

Note. In matrix notation, we have $B = B^* V$, for some upper triangular matrix V with 1 on the main diagonal. In step 2, by elementary column operations one can change V into a matrix W in upper triangular form, with 1 on the main diagonal and all other entries at most $\frac{1}{2}$ in absolute value. Then, the columns of $B^* W$ form the basis B as it is after applying step 2.

Note. Let, at step 3, us interchange b_j and b_{j+1}. Also, let $\tilde{b}_1, \ldots, \tilde{b}_n$ be the new basis (after application of step 3), and $\tilde{b}^*_1, \ldots, \tilde{b}^*_n$ be the new Gram-Schmidt orthogonalization. Then $\tilde{b}_i = b_i$, for $i \neq j, j+1$, $\tilde{b}_j = b_{j+1}$ and $\tilde{b}_{j+1} = b_j$. So $\tilde{b}^*_i = b^*_i$, for $i \neq j, j+1$, and

$$\begin{aligned} \tilde{b}_j = b_{j+1} \quad &= r_{1,j+1} b^*_1 + \cdots + r_{j-1,j+1} b^*_{j-1} + r_{j,j+1} b^*_j + b^*_{j+1} \\ &= r_{1,j+1} \tilde{b}^*_1 + \cdots + r_{j-1,j+1} \tilde{b}^*_{j-1} + r_{j,j+1} b^*_j + b^*_{j+1}, \end{aligned}$$

where $|r_{k,j+1}| \leq \frac{1}{2}$. Since $r_{j,j+1}\, b^*_j + b^*_{j+1}$ is orthogonal to vectors $b_1, \ldots, b_{j-1}$, then

$$\tilde{b}^*_j = r_{j,j+1}\, b^*_j + b^*_{j+1}.$$

Therefore, by interchanging b_j and b_{j+1}, $\det B_i^T B_i$, where $B_i = (b_1, \ldots, b_i)$, is multiplied by a factor β, $\beta < \frac{3}{4}$.

Theorem 3. [3] *The above algorithm finds a reduced basis for L in a polynomial time.*

The following program present the basis reduction algorithm [3].

$for\ i = 1\ to\ n\ do$
$\quad b_i^* = b_i$
$\quad for\ j = 1\ to\ i-1\ do$
$\quad\quad \mu_{ij} = b_i^{*T} b_j^* / B_j$
$\quad\quad b_i^* = b_i^* - \mu_{ij} b_j^*$
$\quad end$
$\quad B_i = b_i^{*T} b_i^*$
end
$k := 2$
(1) $for\ l = k-1\ do\ (*)$
$if\ B_k < \left(0.75 - \mu_{k,k-1}^2\right) B_{k-1}\ then\ goto\ (2)$
$for\ l = k-2\ downto\ 1\ do\ (*)$
$if\ k = n+1\ then\ stop$
$k := k+1$
$goto\ (1)$
(2) $\mu := \mu_{k,k-1}$
$B := B_k + \mu^2 B_{k-1}$
$\mu_{k,k-1} := \mu B_{k-1} / B$
$B_k := B_{k-1} B_k / B$
$B_{k-1} := B$
$(b_{k-1}, b_k) := (b_k, b_{k-1})$
$for\ j = 1\ to\ k-2\ do$
$\quad (\mu_{k-1,j}\ ,\ \mu_{kj}) := (\mu_{kj}\ ,\ \mu_{k-1,j})$
end
$for\ i = k+1\ to\ n\ do$

$$\begin{pmatrix} \mu_{i,k-1} \\ \mu_{ik} \end{pmatrix} := \begin{pmatrix} 1 & \mu_{k,k-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{i,k-1} \\ \mu_{ik} \end{pmatrix}$$

end
$if\ k > 2\ then\ k := k-1$
$goto\ (1)$

$(*)$ *if* $|\mu_{kl}| > 0.5$ *then*
$r := nearest\ integer\ to\ \mu_{kl}$
$b_k := b_k - rb_l$
for $j = 1$ *to* $l-1$ *do*
$\mu_{kj} := \mu_{kj} - r\mu_{lj}$
end
$\mu_{kl} := \mu_{kl} - r$
end

3. Solving a linear Diophantine equation using the basis reduction algorithm

In this section, we use the basis reduction algorithm for solving a linear Diophantine equation. For this purpose, consider the linear Diophantine equation

$$a^T x = b, \quad x \in \mathbb{Z}^n, \tag{9}$$

where $a \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$. Let L be the lattice consisting of all integer vectors orthogonal to $(p^T, -1)^T$, where $p^T = (a^T, -b)$. To solve (9) by using the basis reduction, first we construct an initial basis B that generates L and then we apply the basis reduction algorithm to it to obtain the reduced basis $\mathcal{B}$. Then we use $\mathcal{B}$ to obtain the general solution of (9).

Suppose that B is the matrix

$$B = \begin{bmatrix} I_{n+1} \\ p^T \end{bmatrix},$$

where I_{n+1} is the identity matrix of order $n+1$. Note that columns of B form a basis for lattice L. The lattice L consists of all vectors of the form

$$(\alpha^T; \beta) = (\alpha_1, \ldots, \alpha_{n+1}; \beta) \in \mathbb{Z}^{n+2},$$

where $\beta = p^T \alpha$.

Let $\mathcal{B}$ be the reduced basis obtained from B. Here, B is a basis for L, so is $\mathcal{B}$. Therefore $(p^T, -1)\{\mathcal{B}\} = 0$. Using Euclid's algorithm or a generalization of it (see [2]), we reduce the last row of $\mathcal{B}$ to de_1^T, where $d \in \mathbb{Z}$ and e_1 is the first column of I_{n+1}. Apply those operations to all other rows of $\mathcal{B}$ too. Assume $\mathcal{B}'$ is the resulting matrix. Hence

$$\mathcal{B}' = \begin{bmatrix} Q \\ de_1^T \end{bmatrix},$$

for some unimodular matrix, say Q. We note that d is the g.c.d. of the entries of the last row of $\mathcal{B}$, that is, indeed, the g.c.d. of components of p. Moreover,

$(p^T, -1)\mathcal{B}' = 0$. Let z be the first column of Q and denote the other columns by M, $Q = (z, M)$. Since

$$0 = (p^T, -1)\mathcal{B}' = (p^T, -1) \begin{bmatrix} z & M \\ d & 0^T \end{bmatrix},$$

then $p^T M = 0$. Let $M = (\overline{M}^T, u)^T$. Then, we have the following theorem.

Theorem 4. *The Diophantine equation (9) is consistent if and only if* g.c.d.$(u) = 1$.

Proof. First of all, we note that $p^T M = 0$ implies $a^T \overline{M} = b\, u^T$. Assume g.c.d.$(u) = 1$. Then $u^T N = e_1^T$, for some unimodular matrix N, [2]. By multiplying from right $a^T \overline{M} = b\, u^T$ by N, we have $a^T \overline{M} N = b\, e_1^T$. Hence, $\tilde{x} = \overline{M} N e_1$ is a solution to (9).

Conversely, suppose that $\overline{x}$ is a solution to (9). Since

$$(a^T \ -b \ -1) \begin{bmatrix} \overline{x} \\ 1 \\ 0 \end{bmatrix} = 0,$$

we get

$$\begin{bmatrix} \overline{x} \\ 1 \\ 0 \end{bmatrix} \in L.$$

Since $\mathcal{B}'$ is a basis for L, then for some

$$y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \in \mathbb{Z}^{n+1},$$

where $y_1 \in \mathbb{Z}$ and $y_2 \in \mathbb{Z}^n$, we have

$$\begin{bmatrix} \overline{x} \\ 1 \\ 0 \end{bmatrix} = \mathcal{B}' y = \begin{bmatrix} z & M \\ d & 0^T \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix},$$

or

$$\begin{bmatrix} \overline{x} \\ 1 \end{bmatrix} = y_1 z + M y_2, \tag{10}$$

$$0 = d\, y_1. \tag{11}$$

From (11) we have $y_1 = 0$, meaning that the first column of $\mathcal{B}'$ has no role in the above representation and hence we can delete it. Since $y_1 = 0$ then

$$\begin{bmatrix} \overline{x} \\ 1 \end{bmatrix} = M y_2 = \begin{bmatrix} \overline{M} \\ u^T \end{bmatrix} y_2 = \begin{bmatrix} \overline{M} y_2 \\ u^T y_2 \end{bmatrix}.$$

and then $u^T y_2 = 1$. Therefore, y_2 is an integer vector satisfying the Diophantine equation $u^T \eta = 1$. It shows that g.c.d.$(u) = 1$, see [2]. ☑

Corollary. *Let (9) be consistent. Then the general solution of (9) is*

$$x = t + Uq, \quad q \in \mathbb{Z}^{n-1},$$

where $t = \overline{M}Ne_1$ is the first column of $\overline{M}N$, and U is the matrix consisting of the other columns of it, $\overline{M}N = (t, U)$. ☑

Example. Consider the Diophantine equation

$$6758323\,x_1 + 98756042\,x_2 + 434402\,x_3 + 5676\,x_4 + 436285\,x_5 = 877965345. \quad (12)$$

The initial basis B is as follows

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 6758323 & 98756042 & 434402 & 5676 & 436285 & -877965345 \end{bmatrix}.$$

After applying the basis reduction algorithm on B, we have the reduced basis $\mathcal{B}$ as

$$\mathcal{B} = \begin{bmatrix} 0 & -13 & -16 & -14 & 33 & -2 \\ 0 & 1 & 1 & 1 & -2 & 7 \\ 3 & -20 & 24 & 8 & 8 & 122 \\ 1 & -5 & -31 & 42 & -34 & 29 \\ -3 & -5 & -2 & -18 & -66 & 337 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 27 & -2 & -4 & -2 & -3 & -4 \end{bmatrix}.$$

Using Euclid's algorithm to obtain the g.c.d. of the last row of $\mathcal{B}$, we can obtain matrix $\mathcal{B}'$:

$$\mathcal{B}' = \begin{bmatrix} 35 & -56 & -1 & -81 & 14 & -63 \\ -9 & 17 & 0 & 12 & 6 & 4 \\ -114 & 220 & 28 & 86 & 98 & 155 \\ -63 & 84 & 47 & 92 & 60 & -219 \\ -403 & 824 & -13 & 464 & 339 & -81 \\ -1 & 2 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Matrix 6×5 in the right corner of $\mathcal{B}'$ is the matrix M:

$$M = \begin{bmatrix} -56 & -1 & -81 & 14 & -63 \\ 17 & 0 & 12 & 6 & 4 \\ 220 & 28 & 86 & 98 & 155 \\ 84 & 47 & 92 & 60 & -219 \\ 824 & -13 & 464 & 339 & -81 \\ 2 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Again, apply Euclid's algorithm on M to obtain the g.c.d. of the last row of it. The resulting matrix is

$$M' = \begin{bmatrix} 14 & -95 & 106 & -1 & -63 \\ 6 & 6 & -7 & 0 & 4 \\ 98 & -12 & 48 & 28 & 155 \\ 60 & 32 & -100 & 47 & -219 \\ 339 & 125 & -104 & -13 & -81 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since the g.c.d. of the last row of M is equal to 1, then (12) is consistent. Consider the 5×5 matrix in the right corner of the above matrix, first column which is a special solution to (12). Its other columns consist of a basis for the solution space of the corresponding homogeneous Diophantine equation to (12). Therefore, the general solution of (12) is

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 14 \\ 6 \\ 98 \\ 60 \\ 339 \end{bmatrix} + \begin{bmatrix} -95 & 106 & -1 & -63 \\ 6 & -7 & 0 & 4 \\ -12 & 48 & 28 & 155 \\ 32 & -100 & 47 & -219 \\ 125 & -104 & -13 & -81 \end{bmatrix} q, \quad q \in \mathbb{Z}^4.$$

Note that the size of the components of the above general solution is smaller than that of the equation (12), that is a good property of the algorithm.

Now, again consider the matrix M'. Having applied the basis reduction algorithm to M' and then Euclid's algorithm to its last row, we obtain the matrix

$$\begin{bmatrix} -6 & -11 & 95 & -1 & 10 \\ 9 & 2 & -6 & 0 & -1 \\ 1 & -5 & 12 & 28 & 64 \\ 8 & -26 & -32 & 47 & -21 \\ 67 & -277 & -125 & -13 & 8 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

that gives the following general solution to (12), better than the previous one (specially, for the first column)

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} -6 \\ 9 \\ 1 \\ 8 \\ 67 \end{bmatrix} + \begin{bmatrix} -11 & 95 & -1 & 10 \\ 2 & -6 & 0 & -1 \\ -5 & 12 & 28 & 64 \\ -26 & -32 & 47 & -21 \\ -277 & -125 & -13 & 8 \end{bmatrix} q, \quad q \in \mathbb{Z}^4.$$

In [2] we compared some methods, such as the Euclid, Bradley, Kertzner, Rosser and Morito-Salkin algorithms, from a computational point of view, for solving a linear Diophantine equation and observed that the Rosser algorithm was the best one. These methods are generalizations of the Euclid's algorithm. All of them try to construct a unimodular matrix such that a multiplier of

the first column is a special solution and the other columns contain a basis of the integer solution space for the corresponding homogeneous equation for Diophantine equation.

If we solve (12) by Rosser algorithm, we obtain the following general solution

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} -88 \\ 15 \\ 0 \\ -216 \\ -17 \end{bmatrix} + \begin{bmatrix} 284 & -621 & -346 & -132 \\ -20 & 44 & 24 & 9 \\ 2 & -38 & -17 & -8 \\ 139 & 1446 & 624 & 424 \\ 124 & -321 & -64 & 10 \end{bmatrix} q, \quad q \in \mathbb{Z}^4.$$

Note that our general solution is better than that of Rosser algorithm.

In what follows, we compare the Rosser algorithm (R.A.) and our algorithm (O.A.) from view point of the size of numbers in computed general solution and CPU time (size of an integer number is the number of bits in its binary representation). For this purpose, we solve (1) for $n = 5, 10, 15, 20$, such that the data are chosen in interval $[1, 10^8]$ at random. For each $n = 5, 10, 15, 20$ we solve 30 Diophantine equations and compute:

A: the size of data in (1)
B: the size of the computed special solution
C: the size of the computed basis
T: CPU time.

If we define μ_A, μ_B, μ_C and μ_T as the average of the A, B, C and T, respectively, then we have

	n	5	10	15	20
	μ_A	20.69	20.29	21.43	22.95
O.A.	μ_T	0.056	0.263	0.722	1.434
	μ_B	4.83	2.63	1.63	1.6
	μ_C	6.6	3.61	2.61	2.25
R.A.	μ_T	0.013	0.031	0.073	0.135
	μ_B	6.29	5.39	4.14	4.4
	μ_C	10.11	9.29	8.29	9.45

By observing the above table, we conclude that in all cases our algorithm obtained a better general solution than the Rosser algorithm while its CPU time is larger. Since Rosser algorithm has an advantage over the generalizations of Euclid's algorithm, thus our new method should be better than such methods.

Acknowledgement: The author would like to thank Professor EMILIO SPEDICATO for reading and correcting the final manuscript of this work.

References

[1] T. J. CHON, G. E. COLLINS, *Algorithms for the solution of systems of linear Diophantine equations*, SIAM J. Comp. **11** (1982), 687–708.

[2] H. ESMAEILI, N. MAHDAVI–AMIRI, *Algorithms for Computing the Greatest Common Divisor and Applications to Linear Diophantine Equation* (in Persian), Farhang va Andishe-ye Riyāzi, **21** (2002), 1–25.

[3] E. HLAWKA, J. SCHOIßENGEIER, R. TASCHNER, *Geometric and analytic number theory*, Springer-Verlag, 1991.

[4] A. K. LENSTRA, H. W. LENSTRA, L. LOVĂSZ, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.

[5] M. T. MCCLELLAN, *The exact solution of systems of linear equations with polynomial coefficients*, J. Assoc. Comput. Mach. **20** (1973), 563–588.

[6] G. L. NEMHAUSER, L. WOLSEY, *Integer and combinatorial optimization*, John Wiley and Sons, 1999.

[7] A. SCHRIJVER, *Theory of integer and linear programming*, John Wiley and Sons, 1986.

(Recibido en septiembre de 2005. Aceptado para publicación en abril de 2006)

HAMID ESMAEILI
DEPARTMENT OF MATHEMATICS
BU-ALI SINA UNIVERSITY
HAMEDAN, IRAN
e-mail: esmaeili@basu.ac.ir