ACTA ARITHMETICA
163.3 (2014)

Solving linear systems of equations over integers with Gröbner bases

by

Amir Hashemi (Isfahan and Tehran)

1. Introduction. Let $\mathbf{A} = [a_{ij}]$ be an $m \times n$ matrix with integer entries, and $\mathbf{b}$ an $m \times 1$ column matrix with integer entries. The main contribution of this paper is to solve the system $\mathbf{A}\mathbf{x} = \mathbf{b}$ over integers, i.e. to determine whether there exists an $n \times 1$ matrix $\mathbf{x}$ with integer entries satisfying this equality, and in the affirmative case, to find the general integer solution of the system. This problem appears often in modelling and it has been widely studied in the literature. Furthermore, it is central in discrete optimization and linear algebra, and has many applications in mathematics and engineering.

The system $\mathbf{A}\mathbf{x} = \mathbf{b}$ is a called a *linear Diophantine system* (after the Greek mathematician Diophantus of Alexandria) and in its simplest nontrivial form may be considered as the equation $ax + by = c$. Solving this equation over integers has its origin in the works of the French mathematician Bézout (1730–1783) who showed that this equation has a solution if and only if c is a multiple of the greatest common divisor of a and b. In this paper (for brevity), we refer to a linear Diophantine system as an LDS.

One common and simple way to solve an LDS over integers is to use *integer* linear algebra or more precisely *linear integer programming* [10, 12, 15]. For this purpose, we need a weak definition of row-echelon form of matrices over integers which is employed in the following theorem.

Theorem 1.1 ([10]). *To solve the* LDS $\mathbf{A}\mathbf{x} = \mathbf{b}$ *over integers by unimodular row operations, one can reduce* $[\mathbf{A}^t|\mathbf{I}]$ *to* $[\mathbf{R}|\mathbf{T}]$ *where* $\mathbf{R}$ *is in reduced echelon form. Then the system* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *has integer solutions if and only if the system* $\mathbf{R}^t\mathbf{y} = \mathbf{b}$ *has integer solutions for* $\mathbf{y}$*, and all solutions of* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *are of the form* $\mathbf{x} = \mathbf{T}^t\mathbf{y}$.

2010 *Mathematics Subject Classification*: Primary 13P10; Secondary 11D04.
Key words and phrases: linear Diophantine systems, polynomial ideals, monomial ordering, Gröbner bases.

DOI: 10.4064/aa163-3-5

Solving an LDS over natural numbers (which has interesting applications in integer programming) can be tackled by applying *Gröbner bases*, an important algorithmic object in computational algebraic geometry. The notion of Gröbner bases was introduced and an algorithm for its construction was designed in 1965 by Buchberger in his Ph.D. thesis [3] (for an English translation, see [4]). Later on, he discovered [6] two criteria for detecting some useless reductions that made the Gröbner bases method a practical tool to solve a wide class of problems in polynomial ideal theory (like ideal membership, equality of ideals and solving polynomial systems) and in many other research areas of science and engineering (like integer programming, computer graphics, digital signal processing and robotics). We refer to [1, 2, 5, 7] for more details on the theory of Gröbner bases and its applications.

The connection between Gröbner bases and solving an LDS over *naturals* was first established by Conti and Traverso [9]. Urbaniak et al. [14] modified Buchberger's algorithm for computing a Gröbner basis of the toric ideal associated to an LDS to solve it over naturals. For more details on this subject the reader is referred to Section 2 as well as [13] and [1, p. 107]. Further, we refer to [8] for an application of Gröbner bases to study the number of positive solutions to systems of generalized Pell equations. However, in all these references, the authors have considered only the natural solutions of an LDS, and not the integer solutions. In this paper, we consider the general integer solutions of an LDS, and we present a nontrivial application of Gröbner bases to solve an LDS over integers.

It should be noted that while, in general, solving an LDS over naturals is an NP-complete problem, such a system can be solved over integers in polynomial time through the Hermite normal form (see [11] for more details). However, it is worth investigating the theoretical algorithms (even with bad worst-case complexity) which may be applicable for special classes of problems.

The paper is organized as follows. In Section 2, we review the results due to Conti and Traverso on solving an LDS over naturals. Section 3 is devoted to a new application of Gröbner bases to solving an LDS over integers. We conclude the paper with some examples.

2. Gröbner bases and integer programming. In this section, we recall some definitions and basic results related to Gröbner bases and their application to solving integer programming problems. The results of this section are taken from [1].

Let $\mathcal{R} = \Bbbk[x_1, \ldots, x_n]$ be a polynomial ring where $\Bbbk$ is an arbitrary field. Let $\mathcal{I} = \langle f_1, \ldots, f_k \rangle$ be the ideal of $\mathcal{R}$ generated by the polynomials $f_1, \ldots, f_k$. Also let $f \in \mathcal{R}$ and let $\prec$ be a monomial ordering on the monomials in $x_1, \ldots, x_n$. The *leading monomial* of f is the greatest monomial (with respect to $\prec$) appearing in f; we denote it by $\mathrm{LM}(f)$. The *leading coefficient* of f, denoted by $\mathrm{LC}(f)$, is the coefficient of $\mathrm{LM}(f)$. The *leading term* of f is $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f)$. The *leading term ideal* of $\mathcal{I}$ is defined to be $\mathrm{LT}(\mathcal{I}) = \langle \mathrm{LT}(f) \mid f \in \mathcal{I}\rangle$. A finite set $G = \{g_1, \ldots, g_k\} \subset \mathcal{I}$ is called a *Gröbner basis* of $\mathcal{I}$ with respect to $\prec$ if $\mathrm{LT}(\mathcal{I}) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_k)\rangle$. For more details, we refer to [2, pp. 213–214].

Let $a_{ij}, b_i \in \mathbb{N}$ with $i = 1, \ldots, m$ and $j = 1, \ldots, n$. We look for a solution $(\sigma_1, \ldots, \sigma_n) \in \mathbb{N}^n$ of the system

$$(*) \quad \begin{cases} a_{11}\sigma_1 \ + \cdots + a_{1n}\sigma_n = b_1, \\ \qquad\qquad \vdots \\ a_{m1}\sigma_1 + \cdots + a_{mn}\sigma_n = b_m. \end{cases}$$

To solve this system, we transform it into an equivalent problem in a polynomial ring; then we will solve the new problem by means of Gröbner bases techniques. To do so, let us define the $\mathbb{k}$-algebra homomorphism

$$\phi : \mathbb{k}[y_1, \ldots, y_n] \to \mathbb{k}[x_1, \ldots, x_m]$$

so that $\phi(y_i) = x_1^{a_{1i}} \cdots x_m^{a_{mi}}$ for each i. The next proposition provides an algorithmic method of solving the above system (see [1, p. 106]).

Proposition 2.1. *The system* $(*)$ *has a natural solution iff* $x_1^{b_1} \cdots x_m^{b_m}$ *is the image under* ϕ *of a monomial in* $\mathbb{k}[y_1, \ldots, y_n]$. *Moreover, if* $x_1^{b_1} \cdots x_m^{b_m}$ *is equal to* $\phi(y_1^{\sigma_1} \cdots y_n^{\sigma_n})$, *then* $(\sigma_1, \ldots, \sigma_n)$ *is a solution of the system.*

In order to determine whether $x_1^{b_1} \cdots x_m^{b_m}$ is in the image of ϕ, we compute a Gröbner basis G of the ideal $\mathcal{I} = \langle y_1 - x_1^{a_{11}} \cdots x_m^{a_{m1}}, \ldots, y_n - x_1^{a_{1n}} \cdots x_m^{a_{mn}}\rangle$ with respect to the lexicographical monomial ordering with $y_i \prec x_j$ for all i, j. Let h be the remainder of $x_1^{b_1} \cdots x_m^{b_m}$ modulo G. If there exists $(\sigma_1, \ldots, \sigma_n) \in \mathbb{N}^n$ so that $h = y_1^{\sigma_1} \cdots y_n^{\sigma_n}$, then $(\sigma_1, \ldots, \sigma_n)$ is a solution of the system, and the system has no natural solution otherwise.

We now consider the case where the a_{ij}'s and b_i's may be negative integers. In this case, we introduce a new variable w, and we consider the ideal $\mathcal{J} = \langle x_1 \cdots x_m w - 1\rangle$. For any exponent $(a_{1i}, \ldots, a_{mi}) \in \mathbb{Z}^m$ with some negative components, we shall write it as $(a_{1i}, \ldots, a_{mi}) = (a'_{1i}, \ldots, a'_{mi}) + \alpha_i(-1, \ldots, -1)$ where $(a'_{1i}, \ldots, a'_{mi}) \in \mathbb{N}^m$ and $\alpha \in \mathbb{N}$. Thus, for each i, we have $x_1^{a_{1i}} \cdots x_m^{a_{mi}} + \mathcal{J} = x_1^{a'_{1i}} \cdots x_m^{a'_{mi}} w^{\alpha_i} + \mathcal{J}$. We consider the polynomial map

$$\psi : \mathbb{k}[y_1, \ldots, y_n] \to \mathbb{k}[x_1, \ldots, x_m, w]/\mathcal{J}$$

given by $\psi(y_i) = x_1^{a'_{1i}} \cdots x_m^{a'_{mi}} w^{\alpha_i} + \mathcal{J}$ for each i. Further, we write $x_1^{b_1} \cdots x_m^{b_m} + \mathcal{J} = x_1^{b'_1} \cdots x_m^{b'_m} w^{\beta} + \mathcal{J}$. The next proposition generalizes Proposition 2.1 to the case where the a_{ij}'s and b_i's are not all naturals (see [1, p. 109]).

Proposition 2.2. *With the above notations, the system* $(*)$ *has a natural solution iff* $x_1^{b'_1}\cdots x_m^{b'_m}w^\beta+\mathcal{J}$ *is the image under* ψ *of a monomial in* $\Bbbk[y_1,\ldots,y_n]$. *Moreover, if* $x_1^{b'_1}\cdots x_m^{b'_m}w^\beta+\mathcal{J}=\psi(y_1^{\sigma_1}\cdots y_n^{\sigma_n})$, *then* $(\sigma_1,\ldots,\sigma_n)$ *is a solution of the system.*

To decide whether $x_1^{b'_1}\cdots x_m^{b'_m}w^\beta+\mathcal{J}$ is in the image of ψ, we employ the method mentioned above. To this end, we must replace $x_1^{b_1}\cdots x_m^{b_m}$ by $x_1^{b'_1}\cdots x_m^{b'_m}w^\beta$, the ideal $\mathcal{I}$ by

$$\mathcal{I}=\langle y_1-x_1^{a'_{11}}\cdots x_m^{a'_{m1}}w^{\alpha_1},\ldots,y_n-x_1^{a'_{1n}}\cdots x_m^{a'_{mn}}w^{\alpha_n},x_1\cdots x_mw-1\rangle,$$

and the monomial ordering by the lexicographical monomial ordering $y_i\prec w\prec x_j$ for all i,j. For examples illustrating these methods, we refer to [1, pp. 107–110].

3. Main results. In this section, we state our main results on non-trivial applications of Gröbner bases techniques to finding the general integer solution of an LDS.

Let us again consider the system $(*)$. We assume first $a_{ij},b_i\in\mathbb{N}$ for $i=1,\ldots,m$ and $j=1,\ldots,n$. We introduce the new variable z and we let $\mathcal{I}=\langle y_1-x_1^{a_{11}}\cdots x_m^{a_{m1}},\ldots,y_n-x_1^{a_{1n}}\cdots x_m^{a_{mn}},y_1\cdots y_nz-1\rangle$. Furthermore, let G be a Gröbner basis of $\mathcal{I}$ with respect to the lexicographical monomial ordering with $z\prec y_i\prec x_j$ for all i,j. The next theorem may be considered as a generalization of Proposition 2.1 to integer solutions of an LDS.

Main Theorem 3.1. *In the above notations, the system* $(*)$ *has an integer solution iff the remainder of* $x_1^{b_1}\cdots x_m^{b_m}$ *modulo* G *only involves* y_i*'s and* z. *Moreover, if the remainder is* $y_1^{\alpha_1}\cdots y_n^{\alpha_n}z^\alpha$, *then* $(\alpha_1-\alpha,\ldots,\alpha_n-\alpha)$ *is a solution of the system.*

Proof. Assume that $(*)$ has a solution $(c_1,\ldots,c_n)$ in $\mathbb{Z}^n$. Also, without loss of generality, assume that there exists i so that $c_1,\ldots,c_i\in\mathbb{N}$ and $c_{i+1},\ldots,c_n\in\mathbb{Z}_{<0}$. We now consider the new system

$$\begin{cases} a_{11}\sigma_1+\cdots+a_{1i}\sigma_i=b_1-a_{1,i+1}c_{i+1}-\cdots-a_{1n}c_n,\\ \qquad\vdots\\ a_{m1}\sigma_1+\cdots+a_{mi}\sigma_i=b_m-a_{m,i+1}c_{i+1}-\cdots-a_{mn}c_n.\end{cases}$$

The above system with the unknowns $(\sigma_1,\ldots,\sigma_i)$ has a natural solution $(c_1,\ldots,c_i)$. From Proposition 2.1 we conclude that

$$x_1^{b_1-a_{1,i+1}c_{i+1}-\cdots-a_{1n}c_n}\cdots x_m^{b_m-a_{m,i+1}c_{i+1}-\cdots-a_{mn}c_n}-y_1^{c_1}\cdots y_i^{c_i}\in\mathcal{J}$$

with $\mathcal{J}=\langle y_1-x_1^{a_{11}}\cdots x_m^{a_{m1}},\ldots,y_i-x_1^{a_{1i}}\cdots x_m^{a_{mi}}\rangle$. Note that $\mathcal{J}\subset\mathcal{I}$. Since

$y_j - x_1^{a_{1j}} \cdots x_m^{a_{mj}} \in \mathcal{I}$ for $j = i+1, \ldots, n$, we deduce that

$$x_1^{b_1-a_{1,i+1}c_{i+1}-\cdots-a_{1n}c_n} \cdots x_m^{b_m-a_{m,i+1}c_{i+1}-\cdots-a_{mn}c_n} - x_1^{b_1} \cdots x_m^{b_m} y_{i+1}^{-c_{i+1}} \cdots y_n^{-c_n} \in \mathcal{I}.$$

We set $A = x_1^{b_1} \cdots x_m^{b_m} y_{i+1}^{-c_{i+1}} \cdots y_n^{-c_n} - y_1^{c_1} \cdots y_i^{c_i}$. It then follows that $A \in \mathcal{I}$. On the other hand, we have $y_1 \cdots y_n z - 1 \in \mathcal{I}$, which yields $(y_1 \cdots y_n z)^{-c_{i+1}} - 1 \in \mathcal{I}$. Therefore, multiplying A by $y_1^{-c_{i+1}} \cdots y_i^{-c_{i+1}} y_{i+2}^{-c_{i+1}} \cdots y_n^{-c_{i+1}} z^{-c_{i+1}}$, we obtain

$$x_1^{b_1} \cdots x_m^{b_m} y_{i+2}^{-c_{i+2}} \cdots y_n^{-c_n} - y_1^{c_1-c_{i+1}} \cdots y_i^{c_i-c_{i+1}} y_{i+2}^{-c_{i+1}} \cdots y_n^{-c_{i+1}} z^{-c_{i+1}} \in \mathcal{I}.$$

An induction argument will then show that there exist natural numbers $\alpha_1, \ldots, \alpha_n, \alpha$ such that $x_1^{b_1} \cdots x_m^{b_m} - y_1^{\alpha_1} \cdots y_n^{\alpha_n} z^{\alpha} \in \mathcal{I}$. Hence the remainder of $x_1^{b_1} \cdots x_m^{b_m}$ modulo G only involves y_i's and z.

Conversely, suppose that the remainder of $x_1^{b_1} \cdots x_m^{b_m}$ modulo G only involves y_i's and z, say it equals $y_1^{\alpha_1} \cdots y_n^{\alpha_n} z^{\alpha}$. We shall prove that then $(\alpha_1 - \alpha, \ldots, \alpha_n - \alpha)$ is a solution of the system $(*)$. If we multiply $x_1^{b_1} \cdots x_m^{b_m} - y_1^{\alpha_1} \cdots y_n^{\alpha_n} z^{\alpha}$ by $y_1^{\alpha} \cdots y_n^{\alpha}$, and replace y_i by $x_1^{a_{1i}} \cdots x_m^{a_{mi}}$ for each i, we get

$$b_j + a_{j1}\alpha + \cdots a_{jn}\alpha = a_{j1}\alpha_1 + \cdots a_{jn}\alpha_n$$

for each j. This shows $(\alpha_1 - \alpha, \ldots, \alpha_n - \alpha)$ is a solution of the system. ■

Proposition 3.2. *In the above setting, suppose that, in addition, G is a head-reduced Gröbner basis. Then the system $(*)$ has a unique integer solution iff $G \cap K[y_1, \ldots, y_n, z]$ has only one element.*

Proof. Assume first that $(*)$ has a unique solution $\Lambda \in \mathbb{Z}^n$, but $G \cap K[y_1, \ldots, y_n, z]$ has at least two elements. We know that $y_1 \cdots y_n z - 1 \in G$. Therefore, according to the defined monomial ordering, there exists an integer i such that the other element of this intersection is of the form $p = y_i^{\alpha_i} \cdots y_n^{\alpha_n} z^{\alpha} - y_i^{\beta_i} \cdots y_n^{\beta_n} z^{\beta}$ with $\alpha_j, \alpha, \beta_j, \beta \in \mathbb{N}$ and $\alpha_i > \beta_i$. On the other hand, we have $(y_1 \cdots y_n z)^t - 1 \in \mathcal{I}$ for $t \in \{\alpha, \beta\}$. Hence, by multiplying p by $(y_1 \cdots y_n)^{\alpha+\beta}$ we conclude that

$$y_1^{\beta} \cdots y_{i-1}^{\beta} y_i^{\alpha_i+\beta} \cdots y_n^{\alpha_n+\beta} - y_1^{\alpha} \cdots y_{i-1}^{\alpha} y_i^{\beta_i+\alpha} \cdots y_n^{\beta_n+\alpha} \in \mathcal{I},$$

and thus

$$a_{\ell 1}(\beta-\alpha)+\cdots+a_{\ell,i-1}(\beta-\alpha)+a_{\ell i}(\alpha_i+\beta-\alpha-\beta_i)+\cdots+a_{\ell n}(\alpha_n+\beta-\alpha-\beta_n) = 0$$

for each ℓ. Furthermore, we can observe that the vector

$$\Lambda' = (\beta - \alpha, \ldots, \beta - \alpha, \alpha_i + \beta - \alpha - \beta_i, \ldots, \alpha_n + \beta - \alpha - \beta_n)$$

is not zero. This implies that $\Lambda + \Lambda'$ is a solution of the system and $\Lambda + \Lambda' \neq \Lambda$, which contradicts our assumption.

Conversely, assume that $G \cap K[y_1, \ldots, y_n, z]$ has only one element $y_1 \cdots y_n z - 1$, but the system has two solutions $(\alpha_1 - \alpha, \ldots, \alpha_n - \alpha)$ and $(\beta_1 - \beta, \ldots, \beta_n - \beta)$ with $\alpha_i, \alpha, \beta_i, \beta \in \mathbb{N}$. Then $x_1^{b_1} \cdots x_m^{b_m} - y_1^{\alpha_1} \cdots y_n^{\alpha_n} z^{\alpha}$

and $x_1^{b_1}\cdots x_m^{b_m} - y_1^{\beta_1}\cdots y_n^{\beta_n}z^{\beta}$ belong to $\mathcal{I}$. Therefore, the polynomial $q = y_1^{\alpha_1}\cdots y_n^{\alpha_n}z^{\alpha} - y_1^{\beta_1}\cdots y_n^{\beta_n}z^{\beta}$ belongs to $\mathcal{I}$. If $\alpha_1 = \beta_1 = 0$, then there is no $g \in G$ such that $\mathrm{LT}(g) \,|\, \mathrm{LT}(q)$, which is a contradiction. Otherwise, we multiply q by $(y_2\cdots y_n z)^{\alpha_1+\beta_1}$, and this eliminates y_1 from q. Hence, there is no $g \in G$ whose leading term divides the leading term of this new polynomial, and this completes the proof. ■

In the examples below, we apply this theorem to compute the general integer solutions of two LDSs.

Example 3.3. Let us calculate the general integer solution of

$$\begin{cases} 12\sigma_1 + 7\sigma_2 + \ 9\sigma_3 \qquad\quad = 12, \\ \qquad\quad 5\sigma_2 + \ 8\sigma_3 \ + 10\sigma_4 = 0, \\ 15\sigma_1 \qquad\ + 21\sigma_3 + 69\sigma_4 = 3. \end{cases}$$

Let $\mathcal{I} = \langle y_1 - x_1^{12}x_3^{15}, y_2 - x_1^{7}x_2^{5}, y_3 - x_1^{9}x_2^{8}x_3^{21}, y_4 - x_2^{10}x_3^{69}, y_1y_2y_3y_4z - 1\rangle$. Using the function `Basis` of the package `Groebner` of `Maple12`, we compute a Gröbner basis B for $\mathcal{I}$ with respect to the lexicographical ordering with $z \prec y_4 \prec \cdots \prec y_1 \prec x_4 \prec \cdots \prec x_1$. The normal form of $x_1^{12}x_3^{3}$ with respect to B is $z^{336}y_1^{293}y_3^{656}y_4^{248}$, which can be computed by using the function `NormalForm`. From Theorem 3.1, we can conclude that

$$(293, 0, 656, 248) - (336, 336, 336, 336) = (-43, -336, 320, -88)$$

is a solution of the system. The computation of the Gröbner basis took 214.3 seconds and it used 4294.6 Mbytes of memory (the calculations in this paper were conducted on a personal computer with 2.7GHz, Intel(R) Core(TM) i7-2620M, 8 GB RAM and 32 bits under the Windows operating system).

Now we wish to compute the general solution of the system. We note that the polynomial $p = y_2^{1581}y_4^{238} - z^{237}y_3^{1967}$ belongs to B. Since $y_1y_2y_3y_4z - 1$ is in $\mathcal{I}$, multiplying p by $(y_1y_3y_4z)^{1581}(y_1y_2y_3z)^{238}$, we will deduce that $z^{2056}y_1^{1819}y_2^{238}y_3^{3786}y_4^{1581} - 1 \in \mathcal{I}$. Then we can write $(1819, 238, 3786, 1581) - (2056, 2056, 2056, 2056) = (-237, -1818, 1730, -475)$, and therefore for each equation $a_{i1}\sigma_1 + a_{i2}\sigma_2 + a_{i3}\sigma_3 + a_{i4}\sigma_4 = b_i$ of the given system, we have $-237a_{i1} - 1818a_{i2} + 1730a_{i3} - 475a_{i4} = 0$. This implies that

$$\begin{aligned}(-43, -336, 320, -88) &+ k(-237, -1818, 1730, -475)\\ &= (-237k - 43, -1818k - 336, 1730k + 320, -475k - 88)\end{aligned}$$

is the general solution of the system where k is an arbitrary integer. Finally, we apply Proposition 2.1. For this, we must consider the ideal generated by the generators of $\mathcal{I}$ except $y_1y_2y_3y_4z - 1$. Let B be its Gröbner basis (its computation took 4 seconds and used 77.6 Mbytes of memory). Then the normal form of $x_1^{12}x_3^{3}$ with respect to B is $x_1^{12}x_3^{3}$. Thus, according to Proposition 2.1, the system has no natural solution.

Example 3.4. Let us consider the following LDS:

$$\begin{cases} \sigma_1 + \sigma_2 + 2\sigma_4 + \sigma_5 + \sigma_6 = 12 \\ \sigma_1 + 2\sigma_2 + \sigma_3 + 3\sigma_4 + 2\sigma_5 = 0 \\ 3\sigma_3 + \sigma_4 + 2\sigma_5 = 2 \\ \sigma_2 + 2\sigma_3 + \sigma_4 + \sigma_5 + \sigma_6 = 6 \\ \sigma_1 + \sigma_2 + \sigma_3 + \sigma_4 = 61 \\ \sigma_2 + 3\sigma_3 + \sigma_5 + \sigma_6 = 44. \end{cases}$$

We set

$$\mathcal{I} = \langle y_1 - x_1x_2x_5, y_2 - x_1x_2^2x_4x_5x_6, y_3 - x_2x_3^3x_4^2x_5x_6^3, \\ y_4 - x_1^2x_2^3x_3x_4x_5, y_5 - x_1x_2^2x_3^2x_4x_6, y_6 - x_1x_4x_6, y_1 \cdots y_6z - 1\rangle.$$

We denote by B a Gröbner basis for $\mathcal{I}$ with respect to the lexicographical ordering with $z \prec y_6 \prec \cdots \prec y_1 \prec x_6 \prec \cdots \prec x_1$. The normal form of $x_1^{12}x_3^2x_4^6x_5^{61}x_6^{44}$ with respect to B is $z^{22}y_1^{82}y_2^{29}y_3^{38}y_5^{10}y_6^{23}$. From Theorem 3.1, we conclude that

$$(82, 29, 38, 0, 10, 23) - (22, 22, 22, 22, 22, 22) = (60, 7, 16, -22, -12, 1)$$

is a solution of the system. We computed the Gröbner basis in 292.1 seconds, and using 12508.6 Mbytes of memory. It is worth noting that since the only element of B involving y_i's and z is $y_1 \cdots y_6z - 1$, the system has no other integer solution (Proposition 3.2).

Now we employ Proposition 2.1. So, we consider the ideal

$$\mathcal{I} = \langle y_1 - x_1x_2x_5, y_2 - x_1x_2^2x_4x_5x_6, y_3 - x_2x_3^3x_4^2x_5x_6^3, \\ y_4 - x_1^2x_2^3x_3x_4x_5, y_5 - x_1x_2^2x_3^2x_4x_6, y_6 - x_1x_4x_6\rangle.$$

Let B be its Gröbner basis (its computation took 7.4 seconds and used 146.2 Mbytes of memory). The normal form of the polynomial $x_1^{12}x_3^2x_4^4x_5^{61}x_6^{44}$ with respect to B is $x_1^6x_3^2x_5^{61}x_6^{38}y_6^6$. Thus, according to Proposition 2.1, the system has no natural solution.

We now consider the system $(*)$ in which the a_{ij}'s and b_i's may be negative integers, and state the analogue of Proposition 2.2. For this purpose, assume that $a_{ij}, b_i \in \mathbb{Z}$. Thus, we can write $(a_{1i}, \ldots, a_{mi}) = (a'_{1i}, \ldots, a'_{mi}) + \alpha_i(-1, \ldots, -1)$ where $a'_{ij}, \alpha_i \in \mathbb{N}$. Suppose that $(b_1, \ldots, b_m) = (b'_1, \ldots, b'_m) + \beta(-1, \ldots, -1)$ with $b'_i, \beta \in \mathbb{N}$. Furthermore, we let

$$\mathcal{I} = \langle y_1 - x_1^{a'_{11}} \cdots x_m^{a'_{m1}} w^{\alpha_1}, \ldots, y_n - x_1^{a'_{1n}} \cdots x_m^{a'_{mn}} w^{\alpha_n}, y_1 \cdots y_nz - 1, x_1 \cdots x_mw - 1\rangle$$

and G be a Gröbner basis of $\mathcal{I}$ with respect to the lexicographical monomial ordering with $z \prec y_i \prec w \prec x_j$ for all i, j.

Main Theorem 3.5. *In the above notations, the system $(*)$ has an integer solution iff the remainder of $x_1^{b'_1} \cdots x_m^{b'_m} w^{\beta}$ modulo G only involves y_i's* *and z. Moreover, if the remainder is $y_1^{\gamma_1}\cdots y_n^{\gamma_n}z^{\gamma}$, then $(\gamma_1-\gamma,\ldots,\gamma_n-\gamma)$ is a solution of the system.*

Proof. Suppose that $(*)$ has a solution $(c_1,\ldots,c_n)\in\mathbb{Z}^n$. We may assume that there exists i such that $c_1,\ldots,c_i\in\mathbb{N}$ and $c_{i+1},\ldots,c_n\in\mathbb{Z}_{<0}$. As in the proof of Theorem 3.1, consider the new system

$$\begin{cases} a_{11}\sigma_1 \ + \cdots + \ a_{1i}\sigma_i = b_1 - a_{1,i+1}c_{i+1} - \cdots - a_{1n}c_n, \\ \qquad\qquad \vdots \\ a_{m1}\sigma_1 + \cdots + a_{mi}\sigma_i = b_m - a_{m,i+1}c_{i+1} - \cdots - a_{mn}c_n. \end{cases}$$

The above system with the unknowns $(\sigma_1,\ldots,\sigma_i)$ has a natural solution $(c_1,\ldots,c_i)$. Then we can write

$$(b_j-a_{j,i+1}c_{i+1}-\cdots-a_{jn}c_n)_{j=1}^m = (b_1',\ldots,b_m')-c_{i+1}(a_{1,i+1}',\ldots,a_{m,i+1}')-\cdots \\ -c_n(a_{1n}',\ldots,a_{mn}')+(\beta-c_{i+1}\alpha_{i+1}-\cdots-c_n\alpha_n).(-1,\ldots,-1).$$

From Proposition 2.2, we see that the polynomial

$$x_1^{b_1'}\cdots x_m^{b_m'}(x_1^{a_{1,i+1}'}\cdots x_m^{a_{m,i+1}'})^{-c_{i+1}}\cdots(x_1^{a_{1n}'}\cdots x_m^{a_{mn}'})^{-c_n}w^{\beta-c_{i+1}\alpha_{i+1}-\cdots-c_n\alpha_n} \\ -y_1^{c_1}\cdots y_i^{c_i}$$

belongs to the ideal

$$J=\langle y_1-x_1^{a_{11}'}\cdots x_m^{a_{m1}'}w^{\alpha_1},\ldots,y_n-x_1^{a_{1n}'}\cdots x_m^{a_{mn}'}w^{\alpha_n},x_1\cdots x_mw-1\rangle.$$

Note that $\mathcal{J}\subset\mathcal{I}$. It follows that

$$p=x_1^{b_1'}\cdots x_m^{b_m'}w^{\beta}y_{i+1}^{-c_{i+1}}\cdots y_n^{-c_n}-y_1^{c_1}\cdots y_i^{c_i}\in\mathcal{I}.$$

From $y_1\cdots y_nz-1\in\mathcal{I}$ we conclude that $(y_1\cdots y_nz)^{-c_{i+1}}-1\in\mathcal{I}$. If we multiply p by $y_1^{-c_{i+1}}\cdots y_i^{-c_{i+1}}y_{i+2}^{-c_{i+1}}\cdots y_n^{-c_{i+1}}z^{-c_{i+1}}$, then we shall have

$$x_1^{b_1'}\cdots x_m^{b_m'}w^{\beta}y_{i+2}^{-c_{i+2}}\cdots y_n^{-c_n}-y_1^{c_1-c_{i+1}}\cdots y_i^{c_i-c_{i+1}}y_{i+2}^{-c_{i+1}}\cdots y_n^{-c_{i+1}}z^{-c_{i+1}}\in\mathcal{I},$$

and consequently there exist $\gamma_1,\ldots,\gamma_n,\gamma\in\mathbb{N}$ such that $x_1^{b_1'}\cdots x_m^{b_m'}w^{\beta}-y_1^{\gamma_1}\cdots y_n^{\gamma_n}z^{\gamma}\in\mathcal{I}$. For the converse, see the proof of Theorem 3.1. ∎

Remark 3.6. It is worth commenting that Proposition 3.2 remains true in the case $a_{ij},b_i\in\mathbb{Z}$ if we replace G by the Gröbner basis introduced above for this case.

Example 3.7. Let us consider the following LDS:

$$\begin{cases} \sigma_1 \ \ - 2\sigma_2 + 5\sigma_3 = -47, \\ 3\sigma_1 \ + 7\sigma_2 - \ \sigma_3 \ = 12, \\ -4\sigma_1 + \ \sigma_2 \ - 2\sigma_3 = -7. \end{cases}$$

Letting $\mathcal{I}=\langle y_1-x_1^5x_2^7w^4,y_2-x_2^9x_3^3w^2,y_3-x_1^7x_2w^2,y_1y_2y_3z-1,x_1x_2x_3w-1\rangle$, we compute a Gröbner basis B with respect to the lexicographical ordering with $z \prec y_3 \prec y_2 \prec y_1 \prec w \prec x_3 \prec x_2 \prec x_1$. On the other hand, we can write $(-47, 12, -7)$ as $(0, 59, 40) + 47(-1, -1, -1)$. The normal form of $x_2^{59}x_3^{40}w^{47}$ with respect to B is equal to $z^{12}y_1^{19}y_2^{9}$, and this yields the integer solution $(7, -3, -12)$. The computation of the Gröbner basis took 4.3 seconds, and it needed 77 Mbytes of memory. Further, we observe that the only element of B involving y_i's and z is $y_1 \cdots y_6 z - 1$, thus the system has only one integer solution (Proposition 3.2). If we remove the polynomial $y_1y_2y_3z - 1$ from $\mathcal{I}$, the normal form of $x_2^{59}x_3^{40}w^{47}$ with respect to the Gröbner basis of this new ideal is $x_3^{31}y_1y_2^{7}y_3w^{39}$, which means that system has no natural solution (see Proposition 2.2). This computation took 0.1 seconds, and it used 2 Mbytes of memory.

Acknowledgements. The author would like to thank an anonymous reviewer for helpful comments on the earlier draft of this paper. This research was in part supported by a grant from IPM (No. 92550420).

References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Amer. Math. Soc., 1994.

[2] T. Becker and V. Weispfenning, *Gröbner Bases: a Computational Approach to Commutative Algebra*, Springer, 1993.

[3] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*, PhD thesis, Univ. Innsbruck, 1965.

[4] B. Buchberger, *An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal*, J. Symbolic Comput., Special Issue on Logic, Mathematics, and Computer Science: Interactions 41 (2006), 475–511.

[5] B. Buchberger, *An algorithmic criterion for the solvability of algebraic systems of equations*, Aequationes Math. 3 (1970), 374–383 (in German); English transl. in [7], 535–545.

[6] B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner bases*, in: Symbolic and Algebraic Computation (EUROSAM'79, Marseille, 1979). Lecture Notes in Comput. Sci. 72, Springer, Berlin, 1979, 3–21.

[7] B. Buchberger and F. Winkler (eds.), *Gröbner Bases and Applications* (Linz, 1998), London Math. Soc. Lecture Note Ser. 251, Cambridge Univ. Press, Cambridge, 1998.

[8] M. Cipu, *Gröbner Bases and Diophantine Analysis*, J. Symbolic Comput. 43 (2008), 681–687.

[9] P. Conti and C. Traverso, *Buchberger algorithm and integer programming*, in: Lecture Notes in Comput. Sci. 539, Springer, 1991, 130–139.

[10] W. J. Gilbert and A. Pathria, *Linear Diophantine Equations*, http://www.math.uwaterloo.ca/~wgilbert/Research/, 1990.

[11] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Computing 8 (1979), 499–507.

[12] F. Lazebnik, *On systems of linear diophantine equations*, Math. Mag. 69 (1996), 261–266.

[13] R. R. Thomas, *A geometric Buchberger algorithm for integer programming*, Math. Oper. Res. 20 (1995), 864–884.

[14] R. Urbaniak, R. Weismantel and G. M. Ziegler, *A variant of the Buchberger algorithm for integer programming*, SIAM J. Discrete Math. 10 (1997), 96–108.

[15] B. L. van der Waerden, *Algebra, Vol. II*, Ungar, New York, 1970.

Amir Hashemi
Department of Mathematical Sciences
Isfahan University of Technology
Isfahan, 84156-83111, Iran
and
School of Mathematics
Institute for Research in Fundamental Sciences (IPM)
Tehran, 19395-5746, Iran
E-mail: Amir.Hashemi@cc.iut.ac.ir

Received on 25.7.2013
and in revised form on 20.10.2013 (7532)