Bulletin of the Iranian Mathematical Society
Vol. 27, No. 1, pp 1-18 (2001)

GENERATING THE INTEGER NULL SPACE AND CONDITIONS FOR DETERMINATION OF AN INTEGER BASIS USING THE ABS ALGORITHMS

H. Esmaeili, N. Mahdavi-Amiri and E. Spedicato

*Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran

**Department of Mathematics, Statistics and Computer Science, University of Bergamo, Bergamo, Italy

Abstract: We have presented a method, based on the **ABS** class of algorithms, for solving the linear systems of Diophantine equations. The method provides the general solution of the system by computing an integer solution along with an integer matrix (generally rank deficient), named as the Abaffian, the integer row combinations of which generate the integer null space of the coefficient matrix. Here we show that, in general, one can not expect that any full set of linearly independent rows of the Abaffian form an integer basis for the integer null space. We determine the necessary and sufficient conditions under which a full rank Abaffian would serve as an integer basis.

[0] *2000 MSC:* 15A03, 15A06, 65F05, 65F30

[0] *Keywords:* ABS algorithms, Diophantine equation, Integer null space.

1. Introduction

Suppose $\mathbb{Z}$ represents all integers. Consider the Diophantine linear system of equations

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

where $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$, and $m \leq n$. By solving the system (1), firstly we mean the determination of the existence of the solution. Secondly, if the system has a solution , then we mean the computation of an integer solution $\bar{x}$ and an integer matrix H so that the rows of H, not necessarily independent, generate the integer null space of A. That is,

$$Integer\ Null(A) = Integer\ Range(H^T).$$

Having this, the integer solutions for (1) are determined by

$$x = \bar{x} + H^T y,$$

for integer vectors y. If the dimension of null space of A is r, and

$$H = [h_1, \ldots, h_i, \ldots, h_r]^T,$$

with h_i's being linearly independent, then H^T is said to be an integer basis matrix for the integer null space of A.

Several methods, based on computing the Hermite normal form, have been introduced before ([3,5]). Recently, **ABS** methods have been used extensively for solving general linear systems. In [7], we have presented a method, based on the **ABS** class of algorithms, for solving the system (1). These methods produce an integer solution $\bar{x}$, if it exists, and an integer matrix, named Abaffian, whose integer row combinations span the integer null space of the coefficient matrix A; hence the general integer solution of the system is readily at hand.

Section 2 explains the class of **ABS** methods and provides some of its properties. In section 3, we briefly discuss our algorithm for solving the Diophantine equations (1). In this section, we then show that, in general, one can not expect that any full set of linearly independent rows of the Abaffian matrix form a basis for the integer null space of the coefficient matrix. In section 4, we present necessary and sufficient conditions on the Abaffian for the existence and hence the determination of an integer basis.

2. ABS Algorithms

ABS methods have been developed by Abaffy, Broyden and Spedicato [1]. Consider the system of linear equations

$$Ax = b, \tag{2}$$

where $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ and $rank(A) = m$. Let $A = (a_1, \ldots, a_m)^T$, $a_i \in \mathbb{R}^n$, $i = 1, \ldots, m$ and $b = (b_1, \ldots, b_m)^T$. Also let $A_i = (a_1, \ldots, a_i)$ and $b^{(i)} = (b_1, \ldots, b_i)^T$.

Assume $x_1 \in \mathbb{R}^n$ arbitrary and $H_1 \in \mathbb{R}^{n \times n}$, Spedicato's parameter, arbitrary and nonsingular. Note that for any $x \in \mathbb{R}^n$ we can write $x = x_1 + H_1^T q$ for some $q \in \mathbb{R}^n$.

The **ABS** class of methods are of the direct iteration types of methods for computing the general solution of (2). In the beginning of the ith iteration, $i \geq 1$, the general solution of the first $i-1$ equation is at hand. We realize that if x_i is a solution for the first $i-1$ equations and if $H_i \in \mathbb{R}^{n \times n}$, with $rank(H_i) = n - i + 1$, is so that the columns of H_i^T span the null space of A_{i-1}^T, then

$$x = x_i + H_i^T q,$$

with arbitrary $q \in \mathbb{R}^n$, forms the general solution of the first $i-1$ equations. That is, with

$$H_i A_{i-1} = 0,$$

we have

$$A_{i-1}^T x = b^{(i-1)}.$$

Now, since $rank(H_i) = n - i + 1$ and H_i^T is a spanning matrix for $null(A_{i-1}^T)$, by assumption (one that is trivially valid for $i = 1$), then if we let

$$p_i = H_i^T z_i,$$

with arbitrary $z_i \in \mathbb{R}^n$, Broyden's parameter, then $A_{i-1}^T p_i = 0$ and

$$x(\alpha) = x_i - \alpha p_i,$$

for any scalar α, solves the first $i-1$ equations. We can set $\alpha = \alpha_i$ so that $x_{i+1} = x(\alpha_i)$ solves the ith equation as well. If we let

$$\alpha_i = \frac{a_i^T x_i - b_i}{a_i^T p_i},$$

with assumption $a_i^T p_i \neq 0$, then

$$x_{i+1} = x_i - \alpha_i p_i$$

is a solution for the first i equations. Now, to complete the **ABS** step, H_i must be updated to H_{i+1} so that $H_{i+1} A_i = 0$. It will suffice to let

$$H_{i+1} = H_i - u_i v_i^T \tag{3}$$

and select u_i, v_i so that $H_{i+1} a_j = 0$, $j = 1, \ldots, i$. The updating formula (3) for H_i is a rank-one correction to H_i. The matrix H_i is generally known as the Abaffian. The **ABS** methods usually use $u_i = H_i a_i$ and $v_i = H_i^T w_i / w_i^T H_i a_i$, where w_i, Abaffy's parameter, is an arbitrary vector satisfying

$$w_i^T H_i a_i \neq 0.$$

Thus, the updating formula can be written as below:

$$H_{i+1} = H_i - \frac{H_i a_i w_i^T H_i}{w_i^T H_i a_i}.$$

We can now give the general steps of an **ABS** algorithm [1,2]. In the algorithm below, r_{i+1} denotes the rank of A_i and hence the rank of H_{i+1} equals $n - r_{i+1}$.

ABS Algorithm for Solving General Linear Systems

(1) Choose $x_1 \in \mathbb{R}^n$, arbitrary, and $H_1 \in \mathbb{R}^{n \times n}$, arbitrary and nonsingular. Let $i = 1$, $r_1 = 0$.

(2) Compute $t_i = a_i^T x_i - b_i$ and $s_i = H_i a_i$.

(3) *If* ($s_i = 0$ and $t_i = 0$) *then* let $x_{i+1} = x_i$, $H_{i+1} = H_i$, $r_{i+1} = r_i$ and *go to* step (7) (the ith equation is redundant). *If* ($s_i = 0$ and $t_i \neq 0$) *then* Stop (the ith equation and hence the system is incompatible).

(4) $\{s_i \neq 0\}$ Compute the search direction $p_i = H_i^T z_i$, where $z_i \in \mathbb{R}^n$ is an arbitrary vector satisfying $z_i^T H_i a_i = z_i^T s_i \neq 0$. Compute

$$\alpha_i = t_i / a_i^T p_i$$

and let

$$x_{i+1} = x_i - \alpha_i p_i.$$

(5) $\{$Updating $H_i\}$ Update H_i to H_{i+1} by

$$H_{i+1} = H_i - \frac{H_i a_i w_i^T H_i}{w_i^T H_i a_i}$$

where $w_i \in \mathbb{R}^n$ is an arbitrary vector satisfying $w_i^T s_i \neq 0$.

(6) Let $r_{i+1} = r_i + 1$.

(7) *If* $i = m$ *then* Stop (x_{m+1} is a solution) *else* let $i = i + 1$ and *go to* step (2).

We note that after the completion of the algorithm, the general solution of (2), if compatible, is written as $x = x_{m+1} + H_{m+1}^T q$, where $q \in \mathbb{R}^n$ is arbitrary.

Below, we list certain properties of the **ABS** methods [2]. For simplicity, we assume $rank(A_i) = i$.

- $H_i a_i \neq 0$ if and only if a_i is linearly independent of $a_1, \ldots, a_{i-1}$.
- Every row of H_{i+1} corresponding to a nonzero component of w_i is linearly dependent on other rows.
- The direction searches $p_1, \ldots, p_i$ are linearly independent.

- If $L_i = A_i^T P_i$, where $P_i = (p_1, \ldots, p_i)$, then L_i is a nonsingular lower triangular matrix.
- The set of directions $p_1, \ldots, p_i$ together with independent columns of H_{i+1}^T form a basis for $\mathbb{R}^n$.
- The matrix $W_i = (w_1, \ldots, w_i)$ has full column rank and $Null(H_{i+1}^T) = Range(W_i)$, while $Null(H_{i+1}) = Range(A_i)$.
- If rows $j_1, \ldots, j_i$ of W_i are linearly independent then the same rows of H_{i+1} are linearly dependent and vice versa. Specially, each row of H_{i+1} corresponding to a nonzero element of w_i is dependent.
- If $s_i \neq 0$, then $rank(H_{i+1}) = rank(H_i) - 1$.
- The updating formula H_i can be written as:

$$H_{i+1} = H_1 - H_1 A_i (W_i^T H_1 A_i)^{-1} W_i^T H_1,$$

where $W_i^T H_1 A_i$ is strongly nonsingular (the determinants of all of its main principal submatrices are nonzero).

3. Solving Linear Diophantine Equations

Consider the linear Diophantine system of equations

$$Ax = b, \quad x \in \mathbb{Z}^n \tag{4}$$

where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$. The following results indicate how to choose H_1, z_i and w_i within the **ABS** algorithms to obtain the integer solution of (4); see [7]. Assume δ_i to be the greatest common divisor (gcd) of the components of $H_i a_i$.

Theorem 1. *Let A be full rank and suppose that the Diophantine system* (4) *is solvable. Consider the sequence of Abaffians generated by the basic ABS algorithm with the following parameter choices:*

(a) H_1 is unimodular (an integer matrix whose inverse is also integer with the modules of its determinant equal to 1).

(b) *For* $i = 1, \ldots, m$, *the integer vector* w_i *is such that* $w_i^T H_i a_i = \delta_i$, $\delta_i = gcd(H_i a_i)$.

Then the following properties are true:

(c) *The sequence of Abaffians generated by the algorithm is well-defined and consists of integer matrices.*

(d) *If* x_{i+1} *is a special integer solution of the first* i *equations, then any integer solution* x *of the first* i *equations can be written in the form* $x = x_{i+1} + H_{i+1}^T q$ *for some integer vector* q.

Theorem 2. *Let* A *be full rank and consider the sequence of matrices* H_i *generated by the basic ABS algorithm with parameter choices as in* Theorem 1. *Let the initial point* x_1 *in the basic ABS algorithm be an arbitrary integer vector and let* z_i *be chosen such that* $z_i^T H_i a_i = gcd(H_i a_i)$. *Then system* (4) *has integer solutions if and only if* $gcd(H_i a_i)$ *divides* $a_i^T x_i - b_i$ *for* $i = 1, \ldots, m$.

Note: The computation of δ_i and solving for an integer y in $s_i^T y = \delta_i$, where $s_i = H_i a_i$, can be achieved by Rosser's algorithm [9,10].

It follows from the above theorems that if there exists a solution for the system (4), then $x = x_{m+1} + H_{m+1}^T q$, with arbitrary $q \in Z^n$, forms the general solution of (4). We continue by an analysis showing that, in general, any $n-m$ independent columns of H_{m+1}^T would not be an integer basis for the integer null space of the matrix A. For simplicity, let $x_1 = 0$, $\bar{x} = x_{m+1}$, $H = H_{m+1}$ and assume $rank(A) = m$. Let $\bar{H} \in \mathbb{Z}^{(n-m)\times m}$ be a matrix composed of any set of $n-m$ linearly independent rows of H. We show that, in general, it can not be expected that

$$x = \bar{x} + \bar{H}^T y, \quad y \in \mathbb{Z}^{n-m}, \tag{5}$$

provide all the integer solutions for (4).

Let $P = (p_1, \ldots, p_m)$ be the matrix of search directions obtained from the application of an **ABS** algorithm in solving the system (4). Let $K = (P, \bar{H}^T)$. We know that the matrix K is nonsingular and

$$AK = A(P, \bar{H}^T) = (AP, A\bar{H}^T) = (L, 0),$$

where L is lower triangular and nonsingular. The next theorem states conditions under which $x = \bar{x} + \bar{H}^T y$, $y \in \mathbb{Z}^{n-m}$, forms the general solution of (4). We note that since $x_1 = 0$ then we can write $\bar{x} = Pq$ for some vector q. Hence we have $b = A\bar{x} = APq = Lq$. Since L is nonsingular then $q = L^{-1}b$ and $\bar{x} = PL^{-1}b$.

Theorem 3. *The expression $x = \bar{x} + \bar{H}^T y$ is the general solution for the Diophantine system* (4) *when the matrix $K = (P, \bar{H}^T)$ is unimodular.*

Proof: The vector $x = \bar{x} + \bar{H}^T y$ for any integer vector y is integer. For such x we have $Ax = b$, since $A\bar{H}^T = 0$. Now suppose $x \in \mathbb{Z}^n$ satisfies $Ax = b$. Let $K^{-1}x = u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$. Since K is unimodular then u in an integer vector with $u_1 \in \mathbb{Z}^m$ and $u_2 \in \mathbb{Z}^{n-m}$. Now, we can write

$$b = Ax = AKK^{-1}x = AKu = (L, 0)\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = Lu_1, \quad u_1 = L^{-1}b.$$

Hence

$$x = Ku = (P, \bar{H}^T)\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = Pu_1 + \bar{H}^T u_2 = PL^{-1}b + \bar{H}^T u_2 = \bar{x} + \bar{H}^T u_2. \square$$

Note: Using the geometry of numbers, the converse of the above theorem is also established (see [4]).

Consider the single Diophantine equation $a^T x = 0$, $x \in \mathbb{Z}^n$. Assume H_1 is unimodular. Let $\delta = gcd(s)$, where $s = H_1 a$, and assume z is so that $s^T z = \delta$. We know from Rosser's algorithm that the first component of s has the largest magnitude in s and is nonzero, since $s \neq 0$. Thus $\| s \|_\infty = |s^T e_1| \neq 0$, where e_1 is the first column of the identity matrix. Suppose $p = H_1^T z$ is the search direction of the **ABS** method for solving $a^T x = 0$, and w is an integer vector so that $w^T e_1 \neq 0$ and $s^T w = \delta$. Then, from the **ABS** properties, the first row of H_2 is dependent and we can define $\bar{H}$ to represent the independent rows of H_2 by

$$\bar{H} = E\left(H_1 - \frac{H_1 a w^T H_1}{w^T H_1 a}\right) = E\left(I - \frac{s w^T}{\delta}\right) H_1,$$

where E is the identity matrix with its first row deleted. From Theorem 3, the vector $x = \bar{H}^T y$, where y is an arbitrary integer vector, is the general solution for $a^T x = 0$, $x \in \mathbb{Z}^n$, when $M = (p, \bar{H}^T)$ is unimodular. Since H_1 is unimodular, then

$$M = (p, \bar{H}^T) = \left(H_1^T z, H_1^T \left(I - \frac{ws^T}{\delta} \right) E^T \right) = H_1^T \left(z, \left(I - \frac{ws^T}{\delta} \right) E^T \right)$$

is unimodular if and only if the matrix

$$\left(z, \left(I - \frac{ws^T}{\delta} \right) E^T \right)$$

is unimodular. Let

$$K = (z, B),$$

where

$$B = \left(I - \frac{ws^T}{\delta} \right) E^T.$$

We note that K is nonsingular. We shall make use of the determinant of K in subsequent discussions. Note the following lemma.

Lemma 1. *If $K = (z, B)$, where $B = (I - ws^T/\delta)E^T$ and E is obtained from the identity matrix with its first row deleted, then* $\det K = w^T e_1$.

Proof: The matrix $K = (z, B)$ is a rank one correction to the matrix $\bar{K} = I - ws^T/\delta = (\bar{K} e_1, B)$, since

$$K = \bar{K} + (z - \bar{K} e_1) e_1^T.$$

Note that

$$\begin{aligned} K &= I - e_1 e_1^T - \frac{ws^T}{\delta} + \frac{e_1^T s}{\delta} w e_1^T + z e_1^T \\ &= K_1 + (z - e_1) e_1^T, \end{aligned}$$

where

$$K_1 = I + wv^T,$$

and

$$v^T = \frac{1}{\delta}[(e_1^T s)e_1^T - s^T].$$

Hence

$$det\, K_1 = 1 + v^T w = \frac{(e_1^T s)(e_1^T w)}{\delta} \neq 0.$$

Thus K_1 is always properly defined and always nonsingular and we may write $K = K_1 K_2$, where

$$K_2 = I + K_1^{-1}(z - e_1)e_1^T.$$

Therefore

$$det\, K_2 = 1 + e_1^T K_1^{-1}(z - e_1).$$

Now, expanding K_1^{-1} by the Sherman-Morrison-Woodbury formula [8] gives $det\, K_2 = \delta/(e_1^T s)$. Since $det\, K = det K_1\, det\, K_2$, the result follows. □

Therefore, K and hence M are unimodular if and only if the integer vector w satisfies $w^T e_1 = 1$ and $w^T s = \delta$, conditions not expected to hold in general. Egervary's method [6] is a special **ABS** method with the selections $H_1 = I$, $x_1 = 0$ and $w = z$. Since the Diophantine system $s^T z = \delta$, $z^T e_1 = 1$, lacks integer solutions in general, then Egervary's claim that any set of independent columns of H^T provides an integer basis for the general integer solutions is refuted. The next example validates this statement.

Example 1. If we use Egervary's method for solving the homogeneous Diophantine equation

$$a^T x = 0 \quad , \quad a^T = (1, 1, 1), \tag{6}$$

with $z = (2, 2, -3)^T$, we obtain:

$$H = H_2^T = I - za^T = \begin{bmatrix} -1 & -2 & -2 \\ -2 & -1 & -2 \\ 3 & 3 & 4 \end{bmatrix}.$$

There are three possible choices for $\bar{H}^T$.

(a) $\bar{H}^T = (H_2^T e_1\,,\, H_2^T e_2)$. The vector $\bar{x} = (-2, 1, 1)^T$ satisfies (6). The only solution for $\bar{H}^T t = \bar{x}$ is $t = (-4/3, 5/3)^T$.

(b) $\bar{H}^T = (H_2^T e_1\,,\, H_2^T e_3)$. The vector $\bar{x} = (-2, 1, 1)^T$ satisfies (6). The only solution for $\bar{H}^T t = \bar{x}$ is $t = (-3, 5/2)^T$.

(c) $\bar{H}^T = (H_2^T e_2\,,\, H_2^T e_3)$. The vector $\bar{x} = (-3, 2, 1)^T$ satisfies (6). The only solution for $\bar{H}^T t = \bar{x}$ is $t = (5, -7/2)^T$.

We see that in all the possible three cases there is at least one integer solution $\bar{x}$ for (6) not being generated by an integer combinations of columns of $\bar{H}^T$.

Note: For the homogeneous Diophantine system (case $b = 0$ in (4)), Egervary [6] presented a method being now a special version of the **ABS** algorithms with $H_1 = I$, $x_1 = 0$, $z_i = w_i$ for all i. We realize that the general solution in this case is written as $x = H_{m+1}^T y$, where $y \in \mathbb{Z}^n$ is arbitrary. Egervary believed that with r being the rank of A, any set of $n - r$ independent columns of H_{m+1}^T would form an integer basis for the integer solutions of the system. The results given above clearly invalidates this belief (see also [7]).

In the next section, we introduce the necessary and sufficient conditions for producing an integer basis from the Abaffian matrix. There, we return to Example 1 again and show how to determine an integer basis using these conditions.

4. The Necessary and Sufficient Conditions

Assume $rank(A) = m$. We now determine conditions under which one can eliminate m columns of H_{m+1}^T and obtain an integer basis, composed of $n - m$ linearly independent columns, for $Null(A) \cap \mathbb{Z}^n$. For convenience, let $H = H_{m+1}$. Let $W = (w_1, \ldots, w_m) \in \mathbb{Z}^{n \times m}$ be the matrix with Abaffian parameters as its columns. We know that $rank(W) = m$. According to **ABS** properties, the rows of H corresponding to m linearly independent rows of W are linearly dependent. Since $rank(H) = n - m$

then, without loss of generality, we can write $H = \begin{pmatrix} \bar{H} \\ U\bar{H} \end{pmatrix}$, where $\bar{H} \in \mathbb{Z}^{(n-m)\times n}$ corresponds to the $n-m$ linearly independent rows of H and $U \in \mathbb{R}^{m\times(n-m)}$. We can now let $W^T = (V^T, T^T)$, where $T \in \mathbb{Z}^{m\times m}$ is nonsingular. Since

$$0 = H^T W = \bar{H}^T V + \bar{H}^T U^T T$$

then $\bar{H}^T U^T = -\bar{H}^T V T^{-1}$ and whereof

$$U^T = -VT^{-1}.$$

We emphasize that U is not necessarily an integer matrix. Fix an arbitrary vector $y \in Null(A) \cap \mathbb{Z}^n$. The full column rank system

$$\bar{H}^T t = y \tag{7}$$

has a unique solution. The following lemma gives the correspondence between t, the unique solution of (7), and the solutions of the system

$$H^T x = y. \tag{8}$$

Lemma 2. *x is a solution of* (8) *if and only if we have*

$$x = \begin{pmatrix} t \\ 0 \end{pmatrix} + \begin{pmatrix} -U^T \\ I_m \end{pmatrix} q,$$

with t being the unique solution of (7) *and $q \in \mathbb{R}^m$.*

Proof: Let $x = \begin{pmatrix} x_{n-m} \\ x_m \end{pmatrix}$ be a solution of (8). Then

$$y = H^T x = \bar{H}^T x_{n-m} + \bar{H}^T U^T x_m = \bar{H}^T (x_{n-m} + U^T x_m).$$

Since (7) has a unique solution then $t = x_{n-m} + U^T x_m$ and hence

$$x = \begin{pmatrix} t \\ 0 \end{pmatrix} + \begin{pmatrix} -U^T \\ I_m \end{pmatrix} x_m.$$

Conversely, let t be the unique solution of (7) and $q \in \mathbb{R}^m$. Consider

$$x = \begin{pmatrix} t \\ 0 \end{pmatrix} + \begin{pmatrix} -U^T \\ I_m \end{pmatrix} q.$$

We have

$$H^T x = \bar{H}^T t - \bar{H}^T U^T q + \bar{H}^T U^T q = \bar{H}^T t = y.$$

Therefor, x is a solution of (8). $\Box$

We saw before that for any $y \in Null(A) \cap \mathbb{Z}^n$, the integer vector $x = H_1^{-T} y$ solves (8). Let $H_1^{-1} = (H_{11}^T, H_{21}^T)$. H_1 being unimodular, both H_{11} and H_{21} are integer matrices. Applying Lemma 2, for some $q \in \mathbb{R}^m$ and t, the unique solution of (7), we must have:

$$x = H_1^{-T} y = \begin{pmatrix} H_{11} \\ H_{21} \end{pmatrix} y = \begin{pmatrix} t \\ 0 \end{pmatrix} + \begin{pmatrix} -U^T \\ I_m \end{pmatrix} q.$$

Hence we have:

$$\begin{aligned} H_{11} y &= t - U^T q \\ H_{21} y &= q. \end{aligned}$$

Now, for $x = H_1^{-T} y$ since y is an integer vector then both q and $t - U^T q$ must be integer vectors. Therefore, to have t integer it would suffice that $\bar{H}^T$ be constructed from H^T in such a way that the corresponding matrix U be integer (or can be reduced to an integer matrix). On the other hand, we realize that no column of $\bar{H}^T$ should have a common divisor other than one (that is, the greatest common divisor for every column should be one), since the system $\bar{H}^T t = y$ will have noninteger solutions, otherwise. Having this in mind, we consider reducing the matrix $H^T = (\bar{H}^T, \bar{H}^T U^T)$ accordingly. To make the columns of $\bar{H}^T$ be relatively prime, we multiply H^T by D on the right, where D is a diagonal matrix as below

$$D = \begin{pmatrix} \bar{D} & 0 \\ 0 & I_m \end{pmatrix},$$

with $\bar{D}_{ii} = 1/gcd(H^T e_i)$. Therefore, we have

$$\tilde{H}^T = H^T D = (\hat{H}^T, \hat{H}^T \hat{U}^T),$$

where

$$\hat{H}^T = \bar{H}^T \bar{D}, \quad \hat{U}^T = \bar{D}^{-1} U^T.$$

Now, let $adj(T)$ be the classical adjoint of T (that is, $T^{-1} = adj(T)/det\,T$). Since $U^T = -VT^{-1}$, we can write

$$\hat{U}^T = -\bar{D}^{-1} V T^{-1} = -\bar{D}^{-1} V\, adj(T)/det\,T.$$

The following theorem states the necessary and sufficient conditions for the solution of the system $\hat{H}^T t = \bar{H}^T \bar{D} t = y$ to be integer.

Theorem 4. *Let $y \in Null(A) \cap \mathbb{Z}^n$ be arbitrary. The solution $\hat{t}$ for the full column rank system $\hat{H}^T t = y$ is an integer vector if and only if $det\,T \mid \bar{D}^{-1} V\, adj(T)$. ($a|b$ means a divided by b is an integer.)*

Proof: We saw that $x = H_1^{-T} y \in \mathbb{Z}^n$, for any $y \in Null(A) \cap \mathbb{Z}^n$, satisfies $H^T x = y$. Thus, for $\tilde{x} = D^{-1} H_1^{-T} y \in \mathbb{Z}^n$ we have $\tilde{H}^T \tilde{x} = y$. Let $\tilde{x} = (\tilde{x}_{n-m}^T, \tilde{x}_m^T)^T$ and suppose that $det\,T | \bar{D}^{-1} V\, adj(T)$. Then $\hat{U}$ is an integer matrix and

$$\tilde{x} = \begin{pmatrix} \tilde{x}_{n-m} \\ \tilde{x}_m \end{pmatrix} = D^{-1} H_1^{-T} y = \begin{pmatrix} \bar{D}^{-1} & 0 \\ 0 & I_m \end{pmatrix} \begin{pmatrix} H_{11} y \\ H_{21} y \end{pmatrix} = \begin{pmatrix} \bar{D}^{-1} H_{11} y \\ H_{21} y \end{pmatrix}.$$

Thus, the vector

$$\hat{t} = \tilde{x}_{n-m} + \hat{U}^T \tilde{x}_m = \bar{D}^{-1} H_{11} y + \bar{D}^{-1} U^T H_{21} y = \bar{D}^{-1} (H_{11} y + U^T H_{21} y)$$

is integer and

$$\begin{aligned} \hat{H}^T \hat{t} &= \bar{H}^T \bar{D} \bar{D}^{-1} (H_{11} y + U^T H_{21} y) = \bar{H}^T (I_{n-m}, U^T) \begin{pmatrix} H_{11} y \\ H_{21} y \end{pmatrix} \\ &= (\bar{H}^T, \bar{H}^T U^T) H_1^{-T} y = H^T x = y. \end{aligned}$$

Conversely, suppose that for any $y \in Null(A) \cap \mathbb{Z}^n$, the solution $\hat{t}$ for $\hat{H}^T t = y$ be integer. Applying Lemma 2, the integer solutions for $\tilde{H}^T x = y$ can be written as

$$\tilde{x} = \begin{pmatrix} \hat{t} \\ 0 \end{pmatrix} + \begin{pmatrix} -\hat{U}^T \\ I_m \end{pmatrix} q,$$

where $q \in \mathbb{Z}^m$. Since $\tilde{H}^T \tilde{x} = y$, then

$$\begin{aligned}\hat{t} &= \tilde{x}_{n-m} + \hat{U}^T \tilde{x}_m = \bar{D}^{-1} H_{11} y + \bar{D}^{-1} U^T H_{21} y \\ &= (\bar{D}^{-1}, \bar{D}^{-1} U^T) \begin{pmatrix} H_{11} y \\ H_{21} y \end{pmatrix} = (\bar{D}^{-1}, \bar{D}^{-1} U^T) H_1^{-T} y.\end{aligned}$$

Note that, for any $y \in Null(A) \cap \mathbb{Z}^n$, $H_1^{-T} y$, $\hat{t}$ and D^{-1} are integers. Therefore, $\bar{D}^{-1} U^T$ must also be an integer matrix because the rows of H_{21} are relatively prime. From $\bar{D}^{-1} U^T = -\bar{D}^{-1} V adj(T)/det T$, it follows that $det\ T |\ \bar{D}^{-1} V adj(T)$. $\square$

We now return to case (b) in Example 1. We have,

$$\bar{H}^T = \begin{bmatrix} -1 & -2 \\ -2 & -2 \\ 3 & 4 \end{bmatrix}, \quad W = \begin{pmatrix} 2 \\ 2 \\ -3 \end{pmatrix}, \quad T = (2),$$

$$V = \begin{pmatrix} 2 \\ -3 \end{pmatrix}, \quad U = \frac{-1}{2}(2, -3), \quad \bar{D} = \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}.$$

We see that

$$\hat{H}^T = \begin{bmatrix} -1 & -1 \\ -2 & -1 \\ 3 & 2 \end{bmatrix},$$

and

$$\hat{U} = (-1, 3),$$

an integer vector now. The solution for $\hat{H}^T t = y$, with $y = (-2, 1, 1)^T$, is the integer vector $\hat{t} = (-3, 5)^T$. On the other hand, any $y \in Null(a^T) \cap \mathbb{Z}^3$ can be written as $y = (-\alpha - \beta, \alpha, \beta)^T$, where α and β are arbitrary integers. For any such y, the solution for $\hat{H}^T t = y$ is given by $\hat{t} = (-2\alpha - \beta, 3\alpha + 2\beta)^T$. Therefore, in this case, we have

$$\{x \in \mathbb{Z}^3 \mid a^T x = 0\} = \{\hat{H}^T q \mid q \in \mathbb{Z}^2\}.$$

Similar developments for case (c) will also result in an integer basis for $Null(a^T) \cap \mathbb{Z}^3$. At the same time, we note that no integer basis can be obtained from the matrix in case (a). Therefore, we observe that an integer basis can not necessarily be obtained from any set of linearly independent columns of H^T.

Determining an Integer Basis

Considering the **ABS** properties, instead of deleting the m dependent columns of H^T all at the same time, deletions can be made in steps. From the **ABS** properties, at the end of the i-th iteration, an independent column of H_{i+1}^T can be identified and subsequently deleted. We know that any column of H_{i+1}^T corresponding to a nonzero component of w_i is linearly dependent on the other columns. Let $w_i = (w_{1i}, \ldots, w_{ni})^T$ and suppose $w_{ki} \neq 0$, for some k, $1 \leq k \leq n$. Then $T = w_{ki}$, $V = (w_{1i}, \ldots, w_{k-1,i}, w_{k+1,i}, \ldots, w_{ni})^T$ and $U^T = -V/w_{ki}$. We can now state the following rule for the deletion of a dependent column of H_{i+1}^T at the end of the i-th iteration.

Deletion Rule For a Dependent Column

Let $\delta_j = gcd(H_{i+1}^T e_j)$ for all j. Delete the k-th column of H_{i+1}^T, where $w_i^T e_k \neq 0$ and $w_i^T e_k | \delta_j w_i^T e_j$ for all j.

We note that one can not expect the satisfaction of the above conditions in all cases. Thus, the **ABS** approach may signal the failure by recognizing that an integer basis may not be obtained. Nevertheless, the columns of H^T span $Null(A) \cap \mathbb{Z}^n$ and, as such, the general integer solutions may be obtained using H. The following example illustrates the point.

Example 2. Consider the Diophantine system below:

$$a^T x = 0 \quad , \quad a^T = (1, 3, -2). \tag{9}$$

With the choice $z = (2, 3, 5)^T$, we have:

$$H^T = I - za^T = \begin{bmatrix} -1 & -6 & 4 \\ -3 & -8 & 6 \\ -5 & -15 & 11 \end{bmatrix}.$$

We see that every column of H^T is relatively prime. Consider the system $\bar{H}^T t = y$, where $y = (-1, 1, 1)^T$ is a solution of (9).

(a) By selecting $\bar{H}^T = (H^T e_1, H^T e_2)$, we have $t = (-7/5, 2/5)^T$.

(b) By selecting $\bar{H}^T = (H^T e_1, H^T e_3)$, we have $t = (-5/3, -2/3)^T$.

(c) By selecting $\bar{H}^T = (H^T e_2, H^T e_3)$, we have $t = (5/2, 7/2)^T$.

We see that in all the possible three cases there is at least one integer solution for (9) not being generated by an integer combinations of columns of $\bar{H}^T$.

5. Conclusions

We saw how an integer Abaffian (not necessarily full rank) matrix is obtained by use of the **ABS** methods for solving a linear Diophantine system of equations. The integer combinations of the rows of the Abaffian span the integer null space of the coefficient matrix. We proved that, in general, it can not be expected that the resulting Abaffian would contain an integer basis for this integer null space. Finally, we specified the necessary and sufficient conditions under which the Abaffian would present an integer basis.

Acknowledgements. *The work of the first two authors has been supported by the Research Council of Sharif University of Technology. The authors are grateful to the referees for their constructive comments, specially to one anonymous referee who provided a more concise proof of* Lemma 1.

References

[1] J. Abaffy, C.G. Broyden, E. Spedicato, A class of direct methods for linear equations, *Numer. Math.*, 45 (1984) 361-376.

[2] J. Abaffy, E. Spedicato, *ABS Projection Algorithms: Mathematical Techniques for Linear and Nonlinear Equations*, Ellis Horwood, Chichester, 1989.

[3] G.H. Bradly, Algorithms for Hermite and Smith normal matrices and linear Diophantine equations, *Math. Comp.*, 25 (1971) 897-907.

[4] J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, Berlin, 1959.

[5] T.J. Chou, E.E. Collins, Algorithms for the solution of systems of linear Diophantine equations, *SIAM J. Comp.*, 11 (1982) 786-708.

[6] E. Egervary, On rank-diminishing operations and their applications to the solution of linear equations, *ZAMP*, 9 (1960) 376-386.

[7] H. Esmaeili, N. Mahdavi-Amiri, E. Spedicato, A class of ABS algorithms for Diophantine linear systems, to appear in *Numericshe Mathematik*.

[8] G.H. Golub, C.F. Van Loan, *Matrix Computations*, Johns Hopkins University Press, 1989.

[9] S. Morito, H.M. Salkin, Using the Blankinship algorithm to find the general solution of a linear Diophantine equation, *Acta Inf.*, 13 (1980) 379-382.

[10] J.B. Rosser, A note on the linear Diophantine equation, *Amer. Math. Monthly*, 48 (1941) 662-666.

تول د ف پوچ صح ح و شر لازم و کاف بر تع ن ک پ ه صح ح بر س س روشه ABS

ر ساس رده روشها ABS روشی ر حل دستگاه معادلات د وفانتی خطی ر ه کرده م. ن روش جو عمومی دستگاه ر ا جاد ک جو صح ح ر دستگاه و ک ماتر س صح ح رت ه ناقص ماتر س افی که ترک ها صح ح سطرها ش ف ا پوچ صح ح ماتر س ر ر تول د می‌کنند دست می‌دهد. در ن مقاله تد نشان می‌ده م که در حالت کلی نمی‌تو ن نت ار د شت که هر مجموعه کامل مستقل خطی ز سطرها ماتر س افی ک پا ه صح ح ر ف ا پوچ صح ح ماتر س ر تشک ل دهد. شر طی لازم وکافی ر تع ن می‌کن م که تحت نها می‌تو ن ز سطرها ماتر س افی ک ماتر س پا ه صح ح ر ف ا پوچ صح ح تشک ل د د.