Separability of rational relations in $A^* \times \mathbb{N}^m$ by recognizable relations is decidable

Christian Choffrut [1]
http://www.liafa.jussieu.fr/∼cc
Christian.Choffrut@liafa.jussieu.fr

Serge Grigorieff [1]
http://www.liafa.jussieu.fr/∼seg
Serge.Grigorieff@liafa.jussieu.fr

Abstract

Given a direct product of monoids $M = A^* \times \mathbb{N}^m$ where A is finite and $\mathbb{N}$ is the additive monoid of nonnegative integers, the following problem is recursively decidable: given two rational subsests of M, does there exist a recognizable subset which includes one of the subsets and excludes the other.

Keywords: automata, recognizability, separability

1 Introduction

The family of recognizable subsets of a finitely generated monoid M is included in the family of the rational subsets. It thus makes sense to consider the following separability problem: given two rational subsets X and Y of M, decide whether or not there exists a recognizable subset T for which $X \subseteq T$ and $Y \cap T = \emptyset$ holds. The purpose of this work is to answer positively in the case of direct products of free, finitely generated monoids $A_1^* \times A_2^* \times \ldots \times A_{m+1}^*$ where all A_i's, except maybe one, contain at most one element. More formally, identifying the additive monoid of nonnegative integers with the free monoid on a one letter alphabet, we establish the following.

Theorem 1. *Let A be a finite nonempty alphabet. Given two rational subsets R and S of $A^* \times \mathbb{N}^m$, it is decidable whether or not there exists a recognizable subset $T \subseteq A^* \times \mathbb{N}^m$ such that $X \subseteq T$ and $Y \cap T = \emptyset$ hold.*

Many decision problems concerning rational and recognizable subsets of $\mathbb{N}^m$ have been investigated. For most of them, the solution consists of taking advantage of the strong closure properties these two families enjoy.

[1] L.I.A.F.A., Université Paris 7, 2 Pl. Jussieu – 75 251 Paris Cedex – France

E.g., equality of two rational subsets reduces to determining whether or not their symmetric difference is empty, and the symmetric difference happens to be rational. In the present case, such general properties do not help and we have to rely on a new, more algebraic approach. Our proof can be explained relatively simply. First, we reduce the general case of rational subsets of $A^* \times \mathbb{N}^m$ to that of rational subsets of $\mathbb{N}^{2m}$. We show that recognizable separability of rational subsets of $\mathbb{N}^m$ is equivalent — modulo some technical extra condition — to the disjointness of their images modulo some integer q. Finally we show that if such an integer exists, it is bounded by some effectively computable function of the two subsets.

Concerning the relevance of our result, we can argue that there exists a common belief that most decision problems concerning rational subsets of a direct product $A_1^* \times \ldots \times A_m^*$ are undecidable if $m \geq 2$ and at least two of the A_i's have at least 2 elements, but are decidable whenever all alphabets A_i have at most one element, e.g., "are two rational subsets disjoint?", "are two rational subsets equal?", "is a rational subset equal to the full direct product?", "is a rational subset recognizable?", etc..., see Fischer & Rosenberg, 1968 [5] and Ginsburg & Spanier, 1964 [6] respectively. The intermediate case where the product is isomorphic to $A^* \times \mathbb{N}^m$ and A has at least two elements, requires a special treatment, see [9], [8], [12].

The paper is organized as follows. Section 2 recalls basic definitions and poses the problem of separability. Section 3 focuses on specific properties of direct product of (free) monoids. In section 4 a simplification of the problem is given; the general problem can be reduced to that where a unique rational subset in $\mathbb{N}^m$ is given. Section 5 tackles the problem by introducing the notion of ultimate behaviour of a subset and by proving the above theorem.

2 Preliminaries

For the sake of self-containment, we recall basic notions but we refer to standard textbooks for a more detailed exposition, ([1, 2, 14]).

2.1 Rational and recognizable subsets of a monoid

The *rational* operations on subsets of a monoid M are the set theoretical union, the product and the star where these last two operations are defined, for $X, Y \subseteq M$, as $XY = \{xy : x \in X \text{ and } y \in Y\}$ and $X^* = \bigcup_{i \geq 1} X^i$ (which is the submonoid generated by X). The family of rational subsets

of a monoid M, denoted by $\mathrm{Rat}(M)$, is the smallest family containing all finite subsets of M and closed under the rational operations.

The family of *recognizable* subsets of M, denoted by $\mathrm{Rec}(M)$, is the family of subsets X for which there exists a morphism h of M into a finite monoid F such that $X = h^{-1}(h(X))$ holds. Equivalently, there exists a subset $F_0 \subseteq F$ such that $X = h^{-1}(F_0)$. Standard constructions show that $\mathrm{Rec}(M)$ is a Boolean algebra. The following technical result is elementary. It says that all recognizable subsets of a finite collection share a common morphism. Its proof is left to the reader.

Lemma 2. *Given finitely many recognizable subsets $T_1, \ldots, T_n$ of a monoid M, there exists a finite monoid H and a morphism $h : M \to H$ such that $T_i = h^{-1}h(T_i)$ for $i = 1, \ldots, n$.*

2.2 Separable subsets of a monoid

The central notion of our work is the following.

Definition 3. *Two rational subsets R and S of a monoid M are* separable *if there exists a recognizable subset $T \subseteq M$ such that $R \subseteq T$ and $S \cap T = \emptyset$.*

The *separability problem* consists of asking whether or not two given rational subsets of a monoid are separable. Our Theorem states that the problem is recursively decidable for the monoids of the form $A^* \times \mathbb{N}^m$. The following easy observation will be useful. It shows in particular that the relation of being separable is symmetric.

Proposition 4. *Two rational subsets R, S of M are separable if and only if there exists a morphism h of M into a finite monoid such that $h(R)$ and $h(S)$ are disjoint.*

3 Direct products of free monoids

3.1 Rational subsets of $\mathbb{N}^m$

We consider the direct product $\mathbb{N}^m$ of m copies of the set of non-negative integers. An element $u \in \mathbb{N}^m$ is also called a *vector* and its i-th component is denoted by $u[i]$. For $i = 1, \ldots, m$, the i-th canonical vector having all entries equal to 0 except that in position i equal to 1, is denoted by e_i. The projection of $\mathbb{N}^m$ onto the submonoid generated by the vector e_i is denoted by π_i. The sum of two elements $u, v \in \mathbb{N}^m$ is defined componentwise:

$(u+v)[i] = u[i] + v[i]$. With this operation, $\mathbb{N}^m$ is the free commutative monoid on m generators.

As the monoid $\mathbb{N}^m$ is commutative we use the additive notation. In particular, the product of two subsets $X, Y \subseteq \mathbb{N}^m$ is called their sum: $X + Y = \{x + y : x \in X, y \in Y\}$.

Special rational subsets play an important role. A subset X is *linear* if it is of the form $\{a\} + B^* = \{a + t_1 b_1 + \ldots + t_k b_k : t_1, \ldots, t_k \in \mathbb{N}\}$ where a is an element of $\mathbb{N}^m$ and $B = \{b_1, \ldots, b_k\}$ is a finite subset of $\mathbb{N}^m$. Actually, we shall use the less correct but simpler notation $a + B^*$ by identifying the vector with the singleton it represents. A subset is *semilinear* if it is a finite union of linear subsets. Rational subsets of $\mathbb{N}^m$ have simple forms, [3, p. 175].

Proposition 5. *A relation $R \subseteq \mathbb{N}^m$ is rational if and only if it is semilinear.*

The family of rational relations form an effective Boolean algebra [6, Cor.1 p.366]. This is crucial since our decision procedure uses extensively such operations.

Proposition 6. $\mathrm{Rat}(\mathbb{N}^m)$ *is closed under complementation. Furthermore, the union and the complement of two rational subsets can be effectively computed.*

3.2 Recognizability in direct products of monoids

When the monoid is a direct product $M \times N$, the morphism defining a recognizable subset as in paragraph 2.1, splits into two morphisms defined on each component. This is made precise in the following Lemma where, given two mappings $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$, the mapping $f_1 \times f_2 : X_1 \times X_2 \to Y_1 \times Y_2$ is defined as $(f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2))$.

Lemma 7. *Let M, N be monoids and $T \in \mathrm{Rec}(M \times N)$. Then there exist two morphisms $f : M \to H$ and $g : N \to H$ into a finite monoid H such that*

$$T = (f \times g)^{-1}(f \times g)(T)$$

Moreover, if $M = N$ then we may choose $f = g$.

Proof. Let $h : M \times N \to H$ be a morphism into a finite monoid H such that $T = h^{-1}(h(T))$ holds. Define $f : M \to H$ and $g : N \to H$ by $f(x) = h(x, 1)$ and $g(y) = h(1, y)$ and set $K = \{(a, b) \in H \times H : ab \in h(T)\}$. Then we have the sequence of equivalences

$$(x, y) \in T \;\Leftrightarrow\; h(x, y) = h(x, 1)h(1, y) \in h(T) \;\Leftrightarrow\; (f(x), g(y)) \in K$$

Thus, $T = (f \times g)^{-1}(K)$, which yields $T = (f \times g)^{-1}(f \times g)(T)$.
Suppose now that $M = N$. Let $H' = H \times H$ and $f' : M \to H'$ be the morphism such that $f'(x) = (h(x,1), h(1,x))$. Then

$$(x,y) \in T \;\Leftrightarrow\; h(x,y) = h(x,1)h(1,y) \in h(T) \;\Leftrightarrow\; (f'(x), f'(y)) \in K'$$

where $K' = \{((a,b),(c,d)) \in H' \times H' : ad \in h(T)\}$. Thus, as above, we have $T = (f' \times f')^{-1}(K')$, which yields $T = (f' \times f')^{-1}(f' \times f')(T)$. □

With the above Lemma, Proposition 4 can be refined for direct products as follows.

Proposition 8. *Two subsets R, S of $M \times M$ are separable if and only if there exists a morphism $h : M \to H$ into a finite monoid H such that $(h \times h)(R)$ and $(h \times h)(S)$ are disjoint.*

Concerning the monoid $\mathbb{N}^m$, its recognizable subsets can be described very precisely, [1].

Proposition 9. *A subset of $\mathbb{N}^m$ is recognizable if and only if it is a finite union of subsets of the form*

$$\{(a_1 + t_1 b_1, \ldots, a_m + t_m b_m) : t_1, \ldots, t_m \in \mathbb{N}\}$$

where the a_i's and the b_i's are nonnegative integers.

4 Simplifying the input

We reduce the input of the problem to a unique data: separability of two rational subsets over $A^* \times \mathbb{N}^m$ is equivalent to that of a rational subset of $\mathbb{N}^{2m}$ with the fixed rational subset

$$\Delta^{(m)} = \{(x_1, ..., x_m, x_1, ..., x_m) \in \mathbb{N}^{2m} : (x_1, ..., x_m) \in \mathbb{N}^m\} \qquad (1)$$

4.1 Separability: from $A^* \times \mathbb{N}^m$ to $\mathbb{N}^{2m}$

Given $R, S \subseteq A^* \times \mathbb{N}^m$ we set $R^{-1} = \{(x,u) \in \mathbb{N}^m \times A^* : (u,x) \in A^* \times \mathbb{N}^m$ and $R^{-1} \circ S = \{(x,y) : \exists u \in A^*\ ((x,u) \in R^{-1}$ and $(u,y) \in S)\}$. Because rational subsets which are binary relations are closed under composition whenever the common component is a free monoid, [4, §8.1], [2, Thm.IX.4.1.] or [14, Thm.IV.1.5.], the subset $R^{-1} \circ S$ is rational if R and S are.

Theorem 10. *Two rational subsets $R, S \subseteq A^* \times \mathbb{N}^m$ are separable if and only if $R^{-1} \circ S$ (which is rational) and $\Delta^{(m)}$ are.*

Proof. The condition is necessary. We make constant use of Proposition 4. Indeed, let $f : A^* \times \mathbb{N}^m \to F$ be a morphism into a finite monoid F such that $f(R) \cap f(S) = \emptyset$. Define $g : \mathbb{N}^m \times \mathbb{N}^m \to F \times F$ by $g(v, w) = (f(1, v), f(1, w))$ for all $(v, w) \in \mathbb{N}^m \times \mathbb{N}^m$. We claim that $g(R^{-1} \circ S) \cap g(\Delta) = \emptyset$. By way of contradiction, assume there exist $(u, v) \in R$ and $(u, w) \in S$ such that the element (v, w) of $R^{-1} \circ S$ satisfies $g(v, w) \in g(\Delta)$. Then $f(1, v) = f(1, w)$ and therefore $f(u, v) = f(u, 1)f(1, v) = f(u, 1)f(1, w) = f(u, w)$ contradicting $f(R) \cap f(S) = \emptyset$.

The condition is sufficient. Indeed, as observed above, the subset $R^{-1} \circ S$ is rational. Now, assume $R^{-1} \circ S$ is separable from $\Delta^{(m)}$. Using Proposition 8, let $h : \mathbb{N}^m \to H$ be a morphism into a finite monoid such that,

$$h(u) \neq h(v) \text{ for all } (u, v) \in R^{-1} \circ S \tag{2}$$

For each $\alpha \in H$ let $X_\alpha = \pi_1\left((A^* \times h^{-1}(\alpha)) \cap R\right) \subseteq A^*$ where π_1 is the projection onto the first component. This set X_α is rational: $A^* \times h^{-1}(\alpha)$ is recognizable (the direct product of two recognizable subset is a recognizable subset of the direct product, e.g., [1, Thm III. 1. 5]), its intersection with R is rational (in a finitely generated monoid, the intersection of a rational and a recognizable subsets is a rational subset, e.g., [1, Proposition III. 2. 6]) and the image of the result via π_1 is again rational (the image of a rational subset in a morphism is rational, e.g., [1, Corollary III. 2. 3]). Kleene's fundamental Theorem asserts equality $\mathrm{Rat}(A^*) = \mathrm{Rec}(A^*)$. Now, by Lemma 2 there exists a morphism $f : A^* \to F$ into a finite monoid F which recognizes all X_α simultaneously, i.e. for which $X_\alpha = f^{-1}f(X_\alpha)$ holds for all $\alpha \in H$. We claim that $(f \times h)(R) \cap (f \times h)(S) = \emptyset$. If this is not the case, there exist $(x_1, u_1) \in R$ and $(x_2, u_2) \in S$ such that $f(x_1) = f(x_2)$ and $h(u_1) = h(u_2)$ holds. In particular, $x_1 \in X_{h(u_1)}$ and $x_2 \in f^{-1}f(x_1) \subseteq f^{-1}f(X_{h(u_1)}) = X_{h(u_1)}$. Thus, there exists u_1' such that $(x_2, u_1') \in R$ and $h(u_1) = h(u_1')$. Then we have $(u_1', u_2) \in R^{-1} \circ S$ and $h(u_1') = h(u_2)$, a contradiction to (2). □

5 The proof

It is easy to reduce the problem of separating two arbitrary rational subsets of the free commutative monoids to that of separating two linear subsets. We start with this latter problem.

5.1 Modular images and ultimate behavior

The difficulty that we have to overcome is of the same nature as that when studying finitely generated submonoids of the nonnegative integers: the submonoid ultimately exhibits a regularity (i.e., coincides with the subgroup generated in $\mathbb{Z}$) but there is an initial "mess" which is hard, if interesting at all, to describe. It just happens that the ultimate behaviour of a recognizable subset containing a given rational subset and which is a potential candidate for the separation can be described with some precision.

For $q \in \mathbb{N} \setminus \{0\}$,we denote by $\varphi_q : \mathbb{N}^m \to \{0, \ldots, q-1\}^m$ the map defined by $\varphi_q(x) = (y[1], \ldots, y[m])$ with $y[i] = x[i] \mod q$ for $i = 1, \ldots m$. For any subset $R \subseteq \mathbb{N}^m$, we denote by $R_{|q}$ the subset of vectors in R, all components of which are greater than or equal to q.

Lemma 11. *Suppose $T \subseteq \mathbb{N}^m$ is recognizable and $T_{|n}$ is infinite for all n. Then there exists q such that $T_{|q} = \left(\varphi_q(T_{|q}) + qe_1^* + qe_2^* + \ldots qe_m^*\right)_{|q}$.*

Proof. By Proposition 9 we have $T = \bigcup_{j=1,\ldots,p} T_j$ where $T_j = \prod_{i=1,\ldots,m}(a_{j,i} + b_{j,i}^*)$. Let $J \subseteq \{1, \ldots, p\}$ be the subset of indices j for which all $b_{j,i}$'s, $i = 1, \ldots, m$, are strictly positive. The hypothesis on T insures that J is non empty.
Define ℓ as an integer which is greater than all $a_{j,i}$'s, $j = 1, \ldots, p$ and $i = 1, \ldots, m$. We obtain $T_{|\ell} = \left(\bigcup_{j \in J} T_j\right)_{|\ell}$.
Let $q \geq \ell$ be an integer which is a multiple of all $b_{j,i}$'s, $j \in J$, $i = 1, \ldots, m$. Clearly, $T_j = T_j + qe_1^* + \ldots + qe_m^*$ for any $j \in J$. Whence

$$T_{|q} = T_{|q} + qe_1^* + \ldots + qe_m^* \supseteq \left(\varphi_q(T_{|q}) + qe_1^* + \ldots + qe_m^*\right)_{|q}$$

Since the inclusion $T_{|q} \subseteq \varphi_q(T_{|q}) + qe_1^* + \ldots + qe_m^*$ is trivial, the proof of equality $T_{|q} = \left(\varphi_q(T_{|q}) + qe_1^* + qe_2^* + \ldots qe_m^*\right)_{|q}$ is complete. □

Proposition 12. *Let $a \in \mathbb{N}^m$ be a vector and let B be a finite subset of $\mathbb{N}^m$. Suppose that the projections of the linear subset $a + B^*$ on each component are infinite. Then, $(a + B^*)_{|q}$ is infinite and $\varphi_q(a + B^*) = \varphi_q((a + B^*)_{|q})$ for all $q > 0$.*

Proof. Because of the condition on B, for all $i = 1, \ldots, m$ there exists a vector $b_i \in B$ for which the condition $b_i[i] \neq 0$ holds. In particular, $b = b_1 + \ldots + b_m$ has all components greater than 0. If $u \in a + B^*$ then $u + qb$ still belongs to $a + B^*$ and has all components greater than q, hence is in $(a + B^*)_{|q}$. Finally, observe that $\varphi_q(u + qb) = \varphi_q(u)$. □

5.2 Separating two linear subsets

The purpose of this paragraph is to solve the specific case of two linear subsets.

Lemma 13. *Let $R = a + B^*$ and $S = c + D^*$ be linear subsets included in $\mathbb{N}^m$.*
1. Suppose R and S have infinite projections on each component. Then R and S are separable if and only if there exists an integer q such that $\varphi_q(R)$ and $\varphi_q(S)$ are disjoint.
2. More generally let I be the set of indices i for which R has finite projection on the i-th component. Let $\pi'_I : \mathbb{N}^m \to \mathbb{N}^{m-|I|}$ be the projection which erases all components in I and let U be the recognizable set $\{x \in \mathbb{N}^m : x[i] = a[i], i \in I\}$. Then R and S are separable if and only if $\pi'_I(R \cap U)$ and $\pi'_I(S \cap U)$ are separable subsets in $\mathbb{N}^{m-|I|}$.

Proof. If $\varphi_q(R)$ and $\varphi_q(S)$ are disjoint then $\varphi_q^{-1}\varphi_q(R)$ is recognizable and separates R and S. Conversely, assume T is recognizable and separates R and S. Proposition 12 and inclusion $R \subseteq T$ insure that T satisfies the hypothesis in Lemma 11. Thus, for some integer q we have

$$T_{|q} = \left(\varphi_q(T_{|q}) + qe_1^* + \ldots + qe_m^*\right)_{|q} \tag{3}$$

We prove that $\varphi_q(R) \cap \varphi_q(S) = \emptyset$. Assume by contradiction that $u \in S$ is such that $\varphi_q(u) \in \varphi_q(R)$. As in the proof of Proposition 12, the hypothesis on S yields some vector $d \in D^*$ has all components greater than 0. Consider the vector $u + qd$, which still belongs to S and has all components greater than q. Proposition 12 insures that $\varphi_q(R) = \varphi_q(R_{|q})$. Since $R \subseteq T$, we get $\varphi_q(R_{|q}) \subseteq \varphi_q(T_{|q})$. Thus, $\varphi_q(u + qd) = \varphi_q(u) \in \varphi_q(T_{|q})$, so that we have $u+qd \in \varphi_q(T_{|q})+qe_1^*+\ldots+qe_m^*$, hence $u+qd \in \left(\varphi_q(T_{|q}) + qe_1^* + \ldots + qe_m^*\right)_{|q}$. Equality (3) yields $u + qd \in T_{|q}$. Thus, $u + qd$ belongs to S and T, a contradiction. This proves assertion 1. The proof of assertion 2 is routine verification. □

The effectiveness of the previous property relies on the existence of the Smith normal form of integer matrices, cf. [11, Thm 3.8]. Basically, it guarantees that the integer q, if it exists, can be effectively computed.

We recall the definition of the Smith normal form briefly. Let $\mathcal{A}$ be an $m \times n$ integer matrix, $m \geq n$ of rank p. There exists a unimodular (i.e., an integer matrix with determinant equal to ± 1) $m \times m$-matrix $\mathcal{U}$ and a

unimodular $n \times n$-matrix $\mathcal{V}$ such that

$$\mathcal{A}' = \mathcal{U}\mathcal{A}\mathcal{V} = \begin{pmatrix} a_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \\ 0 & 0 & \dots & a_p & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \end{pmatrix} \tag{4}$$

holds, where a_j divides a_{j+1} for $j = 1, \dots, p-1$.

Lemma 14. *Let $\mathcal{A}$ be an $m \times n$ integer matrix $m \geq n$ of rank p and let $\mathcal{A}x = b$ be a linear system of equations. Set $b' = \mathcal{U}b = (b'_j)_{1 \leq i \leq m}$ where $\mathcal{U}$ is the unimodular matrix leading to the Smith normal form* (4)*.*
1. The system has a solution in the finite ring $\mathbb{Z}/q\mathbb{Z}$ if and only if

$$\begin{cases} b'_j \text{ is divisible by } gcd(a_j, q) & \text{for all } j \in \{1, \dots, p\} \\ b'_j \text{ is divisible by } q & \text{for all } j \in \{p+1, \dots, m\} \end{cases} \tag{5}$$

2. There exists q such that the system has no solution in $\mathbb{Z}/q\mathbb{Z}$ if and only if a_j does not divide b'_j for some $j \leq p$ or $b'_j \neq 0$ for some $j \geq p+1$.

Proof. 1. $\mathcal{V}$ is invertible in $\mathbb{Z}$, hence also in $\mathbb{Z}/q\mathbb{Z}$. Thus, the system $\mathcal{A}x = b$ has a solution in $\mathbb{Z}/q\mathbb{Z}$ if and only if so does the system $\mathcal{A}'y = b'$ with $y = \mathcal{V}^{-1}x$. Assertion 1 follows from the fact that the system can be writtten as

$$\begin{cases} a_j \ y_j \equiv b'_j \mod q & \text{for } j = 1, ..., p \\ 0 \ y_j \equiv b'_j \mod q & \text{for } j = p+1, ..., m \end{cases}$$

Whence (5). Concerning assertion 2, the condition is necessary since if $b'_j \neq 0$ holds for some $j \geq p+1$ then any q greater than b'_j will do. The condition is clearly sufficient. □

Theorem 15. *Given two linear subsets $a + B^*$ and $c + D^*$ of $\mathbb{N}^m$, it is decidable in polynomial time whether or not there exists q such that $\varphi_q(a + B^*)$ and $\varphi_q(c + D^*)$ are disjoint.*

Proof. Let $B = \{b_1, ..., b_k\}$ and $D = \{d_1, ..., d_l\}$ and $n = k + l$. Consider the matrix $\mathcal{A} \in \mathbb{Z}^{m \times n}$ with columns $b_1, ..., b_k, -d_1, ..., -d_l$ and the column matrix $b = a - c$. By introducing n variables $x_1, ..., x_k, y_1, ..., y_l$, the condition $\varphi_q(a + B^*) \cap \varphi_q(c + D^*) = \emptyset$ is reduced to the non existence in $\mathbb{Z}/q\mathbb{Z}$ of solutions of the system $\mathcal{A}x = b$. We conclude with assertion 2 of Lemma 14. The complexity claim is a direct consequence of [15]. □

5.3 Proof of Theorem 1

We have all the ingredients to prove our result. The following remark is more or less trivial and its verification is left to the reader. Let $R = \bigcup_{j=1,\ldots,r} R_j$ and $S = \bigcup_{k=1,\ldots,s} S_k$ be finite unions of linear subsets of $\mathbb{N}^m$. Then R and S are separable if and only if R_j and S_k are separable for all pairs (j,k).

Given two rational subsets R and S of $A^* \times \mathbb{N}^m$ defined indifferently by rational expressions or automata, we proceed as follows. We construct an automaton recognizing $R^{-1} \circ S \subseteq \mathbb{N}^{2m}$. Then we convert it into a finite union $V_1 \cup \ldots \cup V_p$ of linear subsets of $\mathbb{N}^{2m}$. At this point we are reduced to checking whether each V_j is separable from $\Delta^{(m)}$ as defined in equality (1). If V_j has infinite projections on all components then assertion 1 of Theorem 15 applies. Otherwise we consider the projection as in assertion 2 of Lemma 13 before applying Theorem 15. □

Ackowledgement The authors wish to thank Antoine Choffrut for pointing out the Smith normal form for integer matrices.

References

[1] J. Berstel. *Transductions and context-free languages*. Teubner, 1979.

[2] S. Eilenberg. *Automata, languages and machines*, volume A. Academic Press, 1974.

[3] S. Eilenberg and M.-P. Schützenbeger. Rational sets in commutative monoids. *J. of Algebra*, 13(2):173–191, 1969.

[4] C. C. Elgot and J. E. Mezei. On Relations Defined by Finite Automata. *IBM J. Res. Develop*, 9:47–68, 1965.

[5] P.C. Fischer and A. Rosenberg. Multitape one-way nonwriting automata. *J. Computer System Sci.*, 2:88–101, 1968.

[6] S. Ginsburg and Spanier. Bounded ALGOL-like languages. *Trans. Amer. Math. Soc.*, 113(1):333–368, 1964.

[7] S. Ginsburg and E.H. Spanier. Semigroups, Presburger formulas, and languages. *Pacific J. Math.*, 16:285–296, 1966.

[8] S. Grigorieff. Modelization of deterministic rational relations. *Theoret. Comput. Sci.*, 281:423–453, 2002.

[9] O. Ibarra. Reversal-bounded multicounter machines and their decision probems. *J. Assoc. Comput. Mach.*, 25(1):116–133, 1978.

[10] O. Ibarra. The unsolvability of the equivalence problem for epsilon-free NGSM's with unary input (output) alphabet and applications. *SIAM Journal of Computing*, 7:524–532, 1978.

[11] N. Jacobson. *Basic Algebra 1.* (Freeman, San Francisco, CA), 1974.

[12] L. Lisovik. Identity problem of regular events over the direct product of free and cyclic semi-groups. *Doklady Akademik Nauk Ukrainian SSR*, (6):410–413, 1979.

[13] V. V. Prasolov. *Problems and Theorem in linear Algebra*, volume 134. American Mathematical Society, 1991.

[14] J. Sakarovitch. *Eléments de théorie des automates.* Vuibert, 2003.

[15] A. Storjohann. Nearly optimal algorithms for computing Smith normal forms of integer matrices. In *ISSAC'96*, pages 267–274. ACM, 1996.