Matrix Equations and Hilbert's Tenth Problem

Article *in* International Journal of Algebra and Computation · December 2008

DOI: 10.1142/S0218196708004925 · Source: OAI

5 authors, including:

Paul C. Bell
Liverpool John Moores University
39 PUBLICATIONS **265** CITATIONS
SEE PROFILE

Vesa Halava
University of Turku
92 PUBLICATIONS **597** CITATIONS
SEE PROFILE

Tero Harju
University of Turku
276 PUBLICATIONS **2,578** CITATIONS
SEE PROFILE

Igor Potapov
University of Liverpool
140 PUBLICATIONS **708** CITATIONS
SEE PROFILE

Paul Bell | Vesa Halava | Tero Harju | Juhani Karhumäki | Igor Potapov

Matrix Equations and Hilbert's Tenth Problem

Turku Centre *for* Computer Science

TUCS Technical Report
No 840, September 2007

Matrix Equations and Hilbert's Tenth Problem

Paul Bell
TUCS-Turku Centre for Computer Science,
Department of Mathematics, University of Turku,
FIN-20014, Turku, Finland
paubel@utu.fi

Vesa Halava
TUCS-Turku Centre for Computer Science,
Department of Mathematics, University of Turku,
FIN-20014, Turku, Finland
vehalava@utu.fi

Tero Harju
TUCS-Turku Centre for Computer Science,
Department of Mathematics, University of Turku,
FIN-20014, Turku, Finland
harju@utu.fi

Juhani Karhumäki
TUCS-Turku Centre for Computer Science,
Department of Mathematics, University of Turku,
FIN-20014, Turku, Finland
karhumak@utu.fi

Igor Potapov
Department of Computer Science,
The University of Liverpool, L69-3BX, UK
igor@csc.liv.ac.uk

TUCS Technical Report

No 840, September 2007

Abstract

We show a reduction of Hilbert's tenth problem to the solvability of the matrix equation $A_1^{i_1} A_2^{i_2} \cdots A_k^{i_k} = Z$ over non-commuting integral matrices, where Z is the zero matrix, thus proving that the solvability of the equation is undecidable. This is in contrast to the case whereby the matrix semigroup is commutative in which the solvability of the same equation was shown to be decidable in general.

The restricted problem where $k = 2$ for commutative matrices is known as the "A-B-C Problem" and we show that this problem is decidable even for a pair of *non-commutative* matrices over an algebraic number field.

Keywords: Hilbert's tenth problem, Diophantine equations, Matrix equations, Undecidability, Formal power series.

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Introduction

Matrices and matrix semigroups play a fundamental and central role in many diverse fields of mathematics and computer science. There has been a great deal of interest by researchers on computational problems for finitely generated matrix semigroups and many natural decision questions on them are in fact undecidable.

One such problem which was studied is the mortality problem. We are given a finite set of matrices, G, forming a semigroup S, and must determine whether the zero matrix (the matrix with all zero elements) is present in the semigroup. This problem was shown to be undecidable by M. Paterson in 1970 for 3-dimensional integer matrix semigroups, [17], and remains undecidable even when there are only 7 matrices in the generator of the semigroup [9].

The membership problem for a *scalar matrix* (A matrix with a scalar k on all leading diagonal elements and 0 elsewhere) was recently shown to be undecidable for 4-dimensional integral matrices, see [4]. We also mention that the freeness problem for 3-dimensional integral matrix semigroups is undecidable, see [13]. In fact, the problem remains undecidable even when the matrices are upper triangular, see [8].

What can be said of decidable cases in the area however? There are far fewer cases where decision problems are known to be decidable. It was shown that the "orbit problem" (Given a matrix $M \in \mathbb{Q}^{n\times n}$ and vectors $u, v \in \mathbb{Q}^n$, does there exist any $k \geq 0$ such that $M^k u = v$?) is decidable, even in polynomial time, see [12]. Furthermore, it was shown that for a semigroup generated by row-monomial rational matrices (each row of a matrix contains exactly one nonzero element), the membership is decidable for any dimension, see [14]. Some criteria for semigroup freeness in two-dimensional upper triangular matrices was also shown in [8].

Another decidable case which was shown was that for a *commutative* rational matrix semigroup in any dimension, where the membership problem was shown to be decidable in polynomial time, see [1]. In this problem, we are given a (finite) set of matrices $G = \{M_1, M_2, \ldots, M_t\} \subseteq \mathbb{Q}^{n\times n}$ where each matrix in G commutes with each other, and a fixed matrix M. The problem can be stated as: does there exist natural numbers $j_1, j_2, \ldots, j_t$ such that:

$$M_1^{j_1} M_2^{j_2} \cdots M_t^{j_t} = M?$$

In this paper we shall examine a related problem where we consider the above equation for non-commutative integral matrices. We show that given the k matrices $A_1, A_2, \ldots, A_k \subseteq \mathbb{Z}^{n\times n}$, determining whether there exists natural numbers $i_1, i_2, \ldots, i_k$ such that:

$$A_1^{i_1} A_2^{i_2} \cdots A_k^{i_k} = Z,$$

where Z is the zero matrix, is undecidable. We do not use a reduction of Post's correspondence problem, as is standard for undecidability proofs, we instead use

the undecidability of Hilbert's tenth problem and properties of formal power series to show the undecidability.

Given three *commutative* matrices A, B, C the problem of determining the solvability of the equation $A^i B^j = C$ for arbitrary $i, j \geq 0$ is known as the "A-B-C Problem" and was shown to be decidable in [7] (obviously this is a subcase of the more general decidability result of [1] but it was considered prior to this result and formulated after the results of [12]). We show that the "A-B-C Problem" is decidable even for non-commutative matrices A, B, C over an algebraic number field.

2 Preliminaries

2.1 Matrices and Words

Let A be a finite set of *letters* called an *alphabet*. A word w is a finite sequence of letters from A and the set of all words over A is denoted A^*. The *empty word* is denoted by ε. For two words $u = u_1 u_2 \cdots u_i$ and $v = v_1 v_2 \cdots v_j$, where $u, v \in A^*$, the concatenation of u and v is denoted by $u \cdot v$ such that $u \cdot v = u_1 u_2 \cdots u_i v_1 v_2 \cdots v_j$. By abuse of notation, we also refer to concatenation via juxtaposition, i.e., $u \cdot v = uv$. A subset L of A^* is called a *language*.

As usual, for a matrix M, we denote by M^T the transpose of matrix M. For an arbitrary semiring K, let vec be a function, vec : $K^{n \times n} \mapsto K^{n^2}$, such that vec takes an $n \times n$ matrix and creates a n^2 dimensional column vector by stacking the columns of the matrix on top of each other starting with the first, i.e., for a matrix $M \in K^{n \times n}$, then:

$$\text{vec}(M) = (M_{[1,1]}, \ldots, M_{[n,1]}, M_{[1,2]}, \ldots, M_{[n,2]}, \ldots, M_{[1,n]}, \ldots, M_{[n,n]})^T \in K^{n^2}$$

Let $A, B, C, X \in K^{n \times n}$, then it is well known that the equation $AXB = C$ (for unknown X), can be rewritten:

$$(B^T \otimes A)\text{vec}(X) = \text{vec}(C), \tag{1}$$

where $\otimes$ denotes the *Kronecker product*, see [5].

We shall also need the *mixed product property* of Kronecker products, namely that for given matrices $A, B, C, D \in K^{n \times n}$ it holds that:

$$(A \otimes B)(C \otimes D) = (AC \otimes BD) \in K^{n^2 \times n^2}. \tag{2}$$

2.2 Formal Power Series

We use the definitions and terminology as in [6]. Here, and throughout, let K be a semiring and A a finite alphabet generating a free monoid denoted by A^*. A formal power series, S, is defined to be a function:

$$S : A^* \mapsto K,$$

and the image of a word $w \in A^*$ under S is denoted (S, w) and is called the coefficient of w in S. The set of formal power series over A with coefficients in K is denoted by $K\langle\langle A\rangle\rangle$. If there are only finitely many coefficients of a formal power series which are nonzero, then it is called a *polynomial*. The set of polynomials over A with coefficients in K is denoted by $K\langle A\rangle$. We can also use a standard notation for a formal power series $S \in K\langle\langle A\rangle\rangle$ by writing:

$$S = \sum_{w \in A^*} (S, w)w.$$

Given two power series S and T, we can define their *sum* by:

$$(S + T, w) = (S, w) + (T, w),$$

for each word $w \in A^*$. We may also define the *product* of S and T by:

$$(ST, w) = \sum_{uv=w} (S, u)(T, v),$$

where $u, v, w \in A^*$ and clearly the summation is finite for each word w. Two external operations of K on $K\langle\langle A\rangle\rangle$ are given by:

$$(kS, w) = k(S, w), \quad (Sk, w) = (S, w)k,$$

for each $w \in A^*$ where $k \in K$ (note that K is not required to have commutative multiplication in general).

A formal power series, S, is called *proper* if $(S, \varepsilon) = 0$, i.e., the coefficient of the empty word in S is 0. For a proper formal power series S, we may define the *star operation*:

$$S^* = \sum_{i \geq 0} S^i.$$

The rational operations in $K\langle\langle A\rangle\rangle$ are the sum, product, star operation and the two external products. A subset of $K\langle\langle A\rangle\rangle$ is *rationally closed* if it is closed under the rational operations. The smallest subset of $K\langle\langle A\rangle\rangle$ containing a subset E, is called the rational closure of E. A formal power series S is called K*-rational* if it is contained within the rational closure of $K\langle A\rangle$ (the set of polynomials).

If L is any language over an alphabet A, then its *characteristic series* (which we denote by char(L)), is the formal power series $S \in K\langle\langle A\rangle\rangle$:

$$S = \text{char}(L) = \sum_{w \in L} w,$$

i.e., it is the series S such that $(S, w) = 1$ if $w \in L$ and 0 if $w \notin L$.

We may also define the *Hadamard product* of two series $S, T \in K\langle\langle A\rangle\rangle$ by:

$$S \odot T = \sum_{w \in A^*} (S, w)(T, w)w.$$

It was shown by Schützenberger that the Hadamard product of two K-rational formal power series is also K-rational [20].

Furthermore, a formal power series $S \in K\langle\langle A \rangle\rangle$ is called *recognizable* if there exists an integer $n \geq 1$, two vectors $\rho, \tau \in K^n$ and a monoid homomorphism

$$\mu : A^* \mapsto K^{n \times n},$$

such that for all words $w \in A^*$,

$$(S, w) = \rho^T \mu(w) \tau.$$

If such elements exist, then (ρ, μ, τ) is called a *linear representation* of the formal power series S.

The following fundamental theorem was originally shown by Kleene for formal power series with boolean coefficients and later extended by Schützenberger to arbitrary semirings:

Theorem 1 (Schützenberger, 1961 [19])**.** *A formal power series is rational if and only if it is recognizable.*

For details of this proof, see also [6] or [18].

3 Hilbert's Tenth Problem

In 1900, David Hilbert presented a lecture entitled "Mathematische Probleme" in which he posed 23 related open problems for the new millennium. The tenth problem, which is the only decision problem of the list, concerns the solvability of Diophantine equations and can be stated:

Hilbert's Tenth Problem. *Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

The problem remained open for 70 years until a "negative solution" to the problem was shown (In other words, it was shown to be undecidable, although the notion of algorithmic unsolvability was not known at the time) in 1970 by Y. Matiyasevich building upon earlier work of many mathematicians, including M. Davis, H. Putman and J. Robinson. For more details of the history of the problem as well as the full proof of the undecidability of this theorem, see [15]. Note that we may, without loss of generality, restrict the problem to that whereby the solution is over natural numbers rather than rational integers, see [15, p.6].

It is well known that we may reduce Hilbert's tenth problem to a problem in formal power series, namely the problem of determining for a $\mathbb{Z}$-rational formal power series $S \in \mathbb{Z}\langle\langle A \rangle\rangle$, whether there exists any word $w \in A^*$ such that $(S, w) = 0$. We shall now show this reduction, see also [18].

Let $P(n_1, n_2, \ldots, n_k)$ be an integer polynomial with k variables (the variables take natural number values). We shall show a construction of a $\mathbb{Z}$-rational formal power series S over the monoid $A = \{x, y\}$ with coefficients in the natural numbers, such that for any word of the form $w = x^{n_1}yx^{n_2}y\cdots yx^{n_k} \in A^*$, where $n_i \geq 0$ for each $1 \leq i \leq k$, it holds that $(S, w) = P(n_1, n_2, \ldots, n_k)^2$ and for any word, u, not of this form, $(S, u) = 1$. Thus, it follows that there exists some word $w \in A^*$ such that $(S, w) = 0$ if and only if the polynomial P has a solution in natural numbers. Due to the undecidability of the latter problem, the problem on formal power series is also therefore undecidable.

We shall now give the details of the construction as in [18, p.73]. For each index $1 \leq j \leq k$, define:

$$R_j = \left(\sum_{n_1,\ldots,n_{j-1}\geq 0} x^{n_1}yx^{n_2}y\cdots yx^{n_{j-1}}y\right)\left(\sum_{n_j\geq 0} n_j x^{n_j}\right)\left(\sum_{n_{j+1},\ldots,n_k\geq 0} yx^{n_{j+1}}y\cdots yx^{n_k}\right),$$

and it is not difficult to show that each series R_j is $\mathbb{N}$-rational. Furthermore, by examining the product we see that:

$$(R_j, x^{n_1}yx^{n_2}y\cdots yx^{n_k}) = n_j.$$

It can now be seen that the series $R \in \mathbb{Z}\langle\langle A\rangle\rangle$ with the required property can be constructed using the Hadamard product, addition and subtraction of the series $R_1, R_2, \ldots, R_k$. However, we may note that any word w not of the form $x^{n_1}yx^{n_2}y\cdots yx^{n_k}$ will have the property that $(R, w) = 0$. Thus, we finally take the series:

$$S = R \odot R + \text{char}((x^*y)^{k-1}x^*)^C,$$

where the superscript C denotes the complement. This formal power series is clearly still $\mathbb{Z}$-rational and note that $R \odot R$ ensures that each element is positive or 0. Thus S contains a zero for some word if and only if that word is an encoding of a correct solution to the given Diophantine equation as required.

4 Undecidable Matrix Equations

We shall now show a construction which will allow us to obtain the undecidability of solving a specific type of matrix equation. As above, we shall encode a Diophantine equation within an $\mathbb{Z}$-rational formal power series, but use a different underlying monoid. We shall then convert the series to a linear representation (which is guaranteed to exist due to Theorem 1) and using this representation, we shall obtain the undecidability of determining if the matrix equation has a solution.

Theorem 2. *Given integral matrices $A_{n_0}, A_{n_1}, \ldots, A_{n_{k+1}}$ of dimension $n \times n$, it is algorithmically undecidable to determine whether there exists a solution to the equation:*

$$A_{n_0}^{i_0}A_{n_1}^{i_1}\cdots A_{n_{k+1}}^{i_{k+1}} = Z,$$

where Z denotes the zero matrix and $i_0, i_1, \ldots, i_{k+1} \in \mathbb{N}$ are variables.

Proof. Let $P(n_1, n_2, \ldots, n_k)$ denote a polynomial with integer coefficients and let $A = \{x_1, x_2, \ldots, x_k\}$ be an alphabet. Our first step shall be to construct a $\mathbb{Z}$-rational formal power series[1], $S \in \mathbb{N}\langle\langle A \rangle\rangle$, such that for any word of the form $w = x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \in A^*$, it holds that $(S, w) = P(n_1, n_2, \ldots, n_k)^2$ and for any word u not of this form, we have $(S, u) = 1$.

The initial construction is similar to that used in Section 3. Instead of encoding the argument of the polynomial within a binary alphabet however, we use a separate letter for each variable in the encoding. Thus, for each index $1 \leq j \leq k$, we define:

$$R_j = \left(\sum_{n_1,\ldots,n_{j-1} \geq 0} x_1^{n_1} x_2^{n_2} \cdots x_{j-1}^{n_{j-1}} \right) \left(\sum_{n_j \geq 0} n_j x_j^{n_j} \right) \left(\sum_{n_{j+1},\ldots,n_k \geq 0} x_{j+1}^{n_{j+1}} \cdots x_k^{n_k} \right),$$

and as previously, we see that each series R_j is $\mathbb{N}$-rational. We now have the required property that:

$$(R_j, x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}) = n_j.$$

We can thus create a rational formal power series $R \in \mathbb{Z}\langle\langle A \rangle\rangle$ using the Hadamard product, addition and subtraction of the series $R_1, R_2, \ldots, R_k$ in a straightforward manner. To complete the encoding, we must make words not of the correct form have nonzero coefficients, thus we define the series:

$$S = R \odot R + \text{char}(x_1^* x_2^* \cdots x_k^*)^C,$$

where again, char(L) denotes the characteristic series of the language L and the superscript C denotes the complement of the series. Thus S has the property that if any word $w \in A^*$ is such that $(S, w) = 0$, then w is of the form $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ where $n_1, n_2, \ldots, n_k \in \mathbb{N}$, and it holds that $P(n_1, n_2, \ldots, n_k) = 0$. Since it is undecidable if P has any such solution in natural numbers, determining whether S has a zero coefficient for any word $w \in A^*$ is undecidable.

Now, using Theorem 1, there exists an integer $n \geq 1$, two column vectors $\rho, \tau \in \mathbb{Z}^n$ and a monoid morphism $\mu : A^* \mapsto \mathbb{Z}^{n \times n}$ such that for any word $w \in A^*$:

$$(S, w) = \rho^T \mu(w) \tau,$$

and (ρ, μ, τ) is called a linear representation of the $\mathbb{Z}$-rational series S.

We shall not discuss how to convert between rational formal power series and linear representations, see [18] for details. Suffice it to say that in such a conversion, we may assume that ρ is of the form $(1, 0, \ldots, 0)^T$ and τ is of the form $((S, \varepsilon), 0, \ldots, 0, 1)^T$ where ε denotes the empty word. We can also see for a non-empty word, $w \in A^+$ that $\rho^T \mu(w) \tau = \mu(w)_{[1,n]}$, i.e., the value (S, w) is given in the top right element of $\mu(w)$.

[1]The series S is $\mathbb{Z}$-rational but the coeffi cients are natural numbers.

Let $\Gamma = \{\mu(x_1), \mu(x_2), \ldots, \mu(x_k)\} \subseteq \mathbb{Z}^{n\times n}$ and ζ be the semigroup generated by Γ, then we obtain an undecidable scalar reachability problem, with the vectors ρ, τ and scalar 0. As the final step, we shall show how to obtain the matrix equation given in the theorem.

First note that (S, ε) is only present in the τ vector for the case when we have a word of 0 length, otherwise, due to the construction in [18], it will be multiplied by 0 for any non-empty word (since the left most column of $\mu(w)$ has all zero elements for all $w \in A^+$). Since we may check if $(S, \varepsilon) = 0$ independently, we may ignore this value and take the vector $\tau = (0, 0, \ldots, 1)^T$. Let us now define two new matrices:

$$X_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad X_{k+1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{Z}^{n\times n},$$

i.e., X_{k+1} has all zeros except elements $[1, 1]$ and $[n, n]$ which are 1. Note that X_0 and X_{k+1} are both idempotent, thus $X_0^2 = X_0$ and $X_{k+1}^2 = X_{k+1}$. Consider now the equation:

$$X_0^{i_0} X_1^{i_1} \cdots X_k^{i_k} X_{k+1}^{i_{k+1}} = Z, \tag{3}$$

where Z is the zero matrix of dimension n. Since X_0 and X_{k+1} are idempotent, the powers i_0 and i_{k+1} are irrelevant unless they equal 0. If i_0 or i_{k+1} equals 0, then the corresponding matrix equals the identity matrix. We can clearly see below however that the result holds even if either of these matrices equals the identity matrix (in fact we will get more nonzero elements).

Note that for any matrix $M \in \mathbb{Z}^{n\times n}$:

$$X_0 M X_{k+1} = \begin{pmatrix} M_{[1,1]} & \cdots & 0 & M_{[1,n]} \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix},$$

and that $\rho^T M \tau = M_{[1,n]}$. In the construction of [18], each matrix in the image of μ, has a zero first column, thus in an equation of the form $X_0^{i_0} X_1^{i_1} \cdots X_k^{i_k} X_{k+1}^{i_{k+1}}$, the top left element equals 1 if and only if $i_1 = i_2 = \cdots = i_k = 0$ (all central powers are zero corresponding to the empty word and giving the identity matrix), and we discount this case since we may check (S, ε) separately as mentioned. Assume then that the top left element equals 0. Thus, Equation (3) holds if and only if $M_{[1,n]} = \rho^T M \tau = 0$, if and only if $P(n_1, n_2, \ldots, n_k) = 0$. Since determining if $P(n_1, n_2, \ldots, n_k) = 0$ is undecidable, the solvability of Equation (3) for variables $i_0, i_1, \ldots, i_{k+1} \in \mathbb{N}$ is also undecidable as required. □

We can note that the solvability of Equation (3) is decidable (even in polynomial time) when all matrices are commutative, see [1].

5 Decidable Cases

We shall now consider decidable cases, in contrast to the results of the last section. We show that the "A-B-C Problem" is decidable in polynomial time even for non-commuting matrices A, B, C.

Let us state the following theorem from [1] which will be useful in this section:

Theorem 3. *[1, Theorem 1.4] Let $M_1, M_2, \ldots, M_h, N_1, N_2, \ldots, N_k \subseteq \mathbb{F}^{n\times n}$ and $P, Q \subseteq \mathbb{F}^{n\times l}$ be commuting matrices (where $\mathbb{F}$ is an algebraic number field), it is decidable in polynomial time whether there exists any solutions to:*

$$\left(\prod_{i=1}^{h} M_i^{x_i}\right) P = \left(\prod_{j=1}^{k} N_j^{y_j}\right) Q, \tag{4}$$

where $x_1, \ldots, x_h, y_1, \ldots, y_k$ are non-negative integers. If such a set of solutions exists, it can be found in polynomial time.

Note that from this theorem it holds that we may decide whether the intersection of two commutative semigroups S_1, S_2 generated by $\{M_1, M_2, \ldots, M_h\}$ and $\{N_1, N_2, \ldots, N_k\}$ respectively are empty by setting $P = Q = I$ where I is the identity matrix (although we need to remove the trivial solution where all exponents equal zero which is easy to do by increasing the dimension of all matrices by 1 or removing the trivial solution from those considered by Lenstra's algorithm in [1]). The same problem for non-commuting matrices was shown to be undecidable by A. Markov in 1947, [16]. The undecidability bounds were improved in the recent papers [10] and [3].

We shall now use Theorem 3 to show that the A-B-C problem is decidable for non-commutative matrices over an algebraic number field in any dimension.

Theorem 4. *Given three matrices $A, B, C \in \mathbb{F}^{n\times n}$ (where $\mathbb{F}$ is an algebraic number field), it is decidable if there exists any $i, j \geq 0$ such that:*

$$A^i B^j = C.$$

Proof. Note that the matrix product $A^i B^j = C$ can be rewritten

$$((B^T)^j \otimes A^i)\text{vec}(I_n) = \text{vec}(C)$$

where I_n is the n-dimensional identity by applying Equation (1) from Section 2.1.

Iteratively applying the mixed product property of Kronecker products, Equation (2), we see that:

$$((B^T)^j \otimes A^i) = ((B^T)^j \otimes I)(I \otimes A^i) = (B^T \otimes I)^j (I \otimes A)^i,$$

and note that matrices $(B^T \otimes I)$ and $(I \otimes A)$ commute. Thus the problem becomes: "Does there exist an $i, j \geq 0$ such that:

$$(B^T \otimes I)^j (I \otimes A)^i \text{vec}(I_n) = \text{vec}(C)$$

is satisfied?". Since the matrices are now commutative, this is an instance of Equation (4) where $h = 2$, $k = 1$, $M_1 = (B^T \otimes I)$, $M_2 = (I \otimes A)$, $N_1 = I$, $P = \text{vec}(I_n)$ and $Q = \text{vec}(C)$ and by Theorem 3, this problem is decidable. □

We shall now show a relation of the above result to Skolem's problem (also called Pisot's problem), which we shall soon define after some preliminary definitions. A sequence of integers $(u_i)_{i=0}^{\infty}$ is called a linear recurrent sequence if it satisfies the recurrence $u_n = u_{n-1}r_{k-1} + u_{n-2}r_{k-2} + \cdots + u_{n-k}r_0$, where r_i are fixed integers called the *recurrence coefficients*. The first k values, $u_0, u_1, \cdots, u_{k-1}$ are called the *initial conditions* of the sequence.

Skolem's Problem. *Given the initial conditions and recurrence coefficients of a linear recurrent sequence, $(u_i)_{i=0}^{\infty}$, determine whether there exists an integer $i \geq 0$ such that $u_i = 0$.*

The decidability status of Skolem's problem is a long standing open problem. It was recently shown to be decidable for linear recurrences of depth 5, see [11]. The following theorem concerning the *mortality problem* [2] was recently proven:

Theorem 5 ([2])**.** *Skolem's Problem with depth k recurrences can be reduced to the Mortality Problem for a semigroup generated by a pair of k-dimensional integral matrices.*

Utilizing this result and Theorem 4, we obtain the following corollary.

Corollary 6. *There exist integral matrices $P, X, Z \in \mathbb{Z}^{k\times k}$ (where Z is the zero matrix) such that determining if $PX^i = Z$ or $X^iP = Z$ are solvable for some $i \geq 0$, is decidable, but determining if $PX^iP = Z$ has a solution is equivalent to Skolem's problem.*

Proof. In the proof of Theorem 5, we have two integral matrices, $P, X \in \mathbb{Z}^{k\times k}$ such that P has a 1 in the top left element and 0 everywhere else. It follows from the proof that we can therefore state Skolem's problem as, "Given matrices P, X, does there exist an $i \geq 0$ such that $PX^iP = Z$ where Z is the zero matrix?". This proves that the decidability of Skolem's problem can be reduced to the solvability of the equation $PX^iP = Z$.

For the decidable cases, note that P is idempotent, thus $P^2 = P$, from which it follows that $PX^j = P^iX^j$ for any $i > 0$ and we know from Theorem 4 that determining if there exists any $i, j \geq 0$ such that $P^iX^j = Z$ is decidable in polynomial time (if $i = 0$, $P^iX^j = X^j$ which equals Z for some j iff X is nilpotent which is easily checked). An almost identical argument holds for the solvability of $X^iP = Z$, and thus the corollary holds. □

[2] Given a matrix semigroup, determine whether the zero matrix belongs to the semigroup.

References

[1] L. Babai, R. Beals, J. Cai, G. Ivanyos, E. Luks, *Multiplicative Equations over Commuting Matrices*, Proc. 7th ACM-SIAM Sypm. on Discrete Algorithms (SODA '96), 1996.

[2] P. Bell, *Computational Problems in Matrix Semigroups*, Ph. D. Thesis, The University of Liverpool, 2007.

[3] P. Bell, *A Note on the Emptiness of Semigroup Intersections*, Fundamenta Informaticae, 79:1-4, 2007.

[4] P. Bell, I. Potapov, *On the Membership of Invertible Diagonal and Scalar Matrices*, Theoretical Computer Science, 372:37-45, 2007.

[5] D. Bernstein, *Matrix Mathematics*, Princeton University Press, 2005.

[6] J. Berstel, C. Reutenauer, *Rational Series and Their Languages*, Springer-Verlag, 1988.

[7] J. Cai, R. Lipton, Y. Zalcstein, *The Complexity of the Membership Problem for* 2*-Generated Commutative Semigroups of Rational Matrices*, Proc. of Foundations of Computer Science (FOCS 94), 35, 1994.

[8] J. Cassaigne, T. Harju, J. Karhumäki, *On the Undecidability of Freeness of Matrix Semigroups*, Internat. J. Algebra Comput., 9(3-4):295-305, 1999.

[9] V. Halava, T. Harju, M. Hirvensalo, *Undecidability Bounds for Integer Matrices using Claus Instances*, Internat. J. of Foundations of Comp. Sci., Vol. 18, Num. 5, 2007.

[10] V. Halava, T. Harju, *On Markov's Undecidability Theorem for Integer Matrices*, Semigroup Forum, (to appear), 2007.

[11] V. Halava, T. Harju, M. Hirvensalo, J. Karhumäki, *Skolem's Problem - On the Border between Decidability and Undecidability*, TUCS Technical Report, Num. 683, 2005.

[12] R. Kannan, R. Lipton, *Polynomial-Time Algorithm for the Orbit Problem*, Journal of ACM, Vol. 33, Num. 4, 808-821, 1986.

[13] D. Klarner, J. Birget, W. Satterfield, *On the Undecidability of the Freeness of Integer Matrix Semigroups*, Internat. J. Algebra Comput. 1, Num. 2, 223-226, 1991.

[14] A. Lisitsa, I. Potapov, *Membership and Reachability Problems for Row-Monomial Transformations*, Mathematical Foundations of Computer Science (MFCS '04), LNCS 3135, 623-634, 2004.

[15] Y. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, Cambridge, London, 1993.

[16] A. Markov, *On Certain Insoluable Problems Concerning Matrices*, Doklady Akad. Nauk SSSR, 57:539-542, 1947.

[17] M. Paterson, *Unsolvability in* $3x3$ *Matrices*, Studies in Applied Mathematics, 49:105-107, 1970.

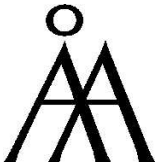
[18] A. Salomaa, M. Soittola, *Automata-Theoretic Aspects of Formal Power Series*, Springer-Verlag, 1978.

[19] M. P. Schützenberger, *On the Definition of a Family of Automata*, Information and Control, 4:245-270, 1961.

[20] M. P. Schützenberger, *On a Theorem of R. Jungen*, Proc. Amer. Math. Soc., 13:885-890, ISSN 0002-9939, 1962.

Lemminkäisenkatu 14 A, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics



Åbo Akademi University
- Department of Computer Science
- Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration
- Institute of Information Systems Sciences

ISBN 978-952-12-1949-8
ISSN 1239-1891