International Journal of Foundations of Computer Science
© World Scientific Publishing Company

On the Minimal Polynomial of a Matrix*

Thanh Minh Hoang†
Abt. Theoretische Informatik
Universität Ulm, 89069 Ulm, Germany

and

Thomas Thierauf‡
FB Elektronik und Informatik
FH Aalen, 73430 Aalen, Germany

ABSTRACT

We investigate the complexity of the degree and the constant term of the minimal polynomial of a matrix. We show that the degree of the minimal polynomial is computationally equivalent to the matrix rank.
We compare the constant term of the minimal polynomial with the constant term of the characteristic polynomial. The latter is known to be computable in the logspace counting class **GapL**. We show that if this holds for the minimal polynomial as well, then the *exact counting in logspace* class $\mathbf{C_=L}$ is closed under complement. Whether $\mathbf{C_=L}$ is closed under complement is one of the main open problems in this area.
As an application of our techniques we show that the problem of deciding whether a matrix is diagonalizable is complete for $\mathbf{AC^0(C_=L)}$, the $\mathbf{AC^0}$*-closure of* $\mathbf{C_=L}$.

Keywords: Linear Algebra, Minimal Polynomial, Logspace Counting Class.

1. Introduction

Computing the determinant of a matrix is an important topic in mathematics and theoretical computer science which has been studied for many years. With respect to parallel computation, the determinant is in $\mathbf{NC^2}$ [4, 5, 6, 7]. Many problems in linear algebra are closely related to the determinant, and hence, are in $\mathbf{NC^2}$ as well. However, $\mathbf{NC^2}$ does not capture the exact complexity of problems in linear algebra. In particular, the determinant is not known to be $\mathbf{NC^2}$-complete. Our goal is to determine precisely the complexity of such problems.

The initial step in this direction was done by Damm [8], Toda [21], Vinay [23], and Valiant [22] (see [16] for more details on the history). They showed that the determinant of an integer matrix characterizes the complexity class **GapL**, a *logspace counting classes* that can handle integers. Toda [21] showed more problems to be

*This work was supported by the German Research Foundation
†Email: hoang@informatik.uni-ulm.de
‡Email: thierauf@informatik.uni-ulm.de. Part of the work done at the Universität Ulm

GapL-complete, including matrix powering and the inverse of a matrix. There are also graph theoretic problems related to counting the number s-t-paths in a graph [21] (see also [19]).

The verification of **GapL** functions is captured by the class $\mathbf{C_=L}$. A complete problem of this class is the problem of testing singularity, i.e., the problem of testing whether the determinant of a given matrix is zero. More general, Allender, Beals, and Ogihara [2] considered the matrix rank:

- the decision problem whether the rank of A is less than some given number r is $\mathbf{C_=L}$-complete,
- the decision problem whether the rank of A equals some given r, is complete for $\mathbf{C_=L} \wedge \mathbf{coC_=L}$, the class of sets that can be written as the conjunction of sets in $\mathbf{C_=L}$ and in $\mathbf{coC_=L}$,
- the problem of computing the rank is in $\mathbf{AC^0(C_=L)}$, the $\mathbf{AC^0}$-closure of $\mathbf{C_=L}$. The problem of verifying one bit of the rank (at a given position), and the problem of deciding whether two matrices have the same rank are complete for $\mathbf{AC^0(C_=L)}$.

The complexity of the minimal polynomial has been studied before [14](see also [12, 13]). In this paper, we show that the *degree of the minimal polynomial* of a matrix is computationally equivalent to the matrix rank problem, i.e. complete for $\mathbf{AC^0(C_=L)}$. Moreover, in analogy to the results on the rank we show that the decision problem whether

- the degree of the minimal polynomial is less than some given m is $\mathbf{C_=L}$-complete,
- the degree of the minimal polynomial is equal some given m is complete for $\mathbf{C_=L} \wedge \mathbf{coC_=L}$, and
- the degrees of the minimal polynomials of two matrices are equal is complete for $\mathbf{AC^0(C_=L)}$.

We also investigate the complexity of the constant term of the minimal polynomial. The constant term of the characteristic polynomial is **GapL**-complete. We ask whether the constant term of the minimal polynomial can be computed in **GapL**, too. We show that this question is strongly connected with another open problem: *if the constant term of the minimal polynomial can be computed in* **GapL**, *then* $\mathbf{C_=L}$ *is closed under complement*. This connection is a consequence of a hardness result: the problem of deciding whether the constant terms of the minimal polynomials of two matrices are equal is complete for $\mathbf{AC^0(C_=L)}$.

Whether $\mathbf{C_=L}$ is closed under complement is one of the big open questions in this area. Recall that many related classes have this property: **NL** [15, 20], **SL** [17], **PL** (trivially), and nonuniform **UL** [18]. Thus our results on the constant term of the minimal polynomial offers a new point of attack to the open question whether $\mathbf{C_=L}$ is closed under complement.

A final observation is about the diagonalizability of matrices. In [13] it was shown that the diagonalizability problem, which is to decide whether a given matrix is diagonalizable, is hard for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. We show that this class also is an upper bound for the diagonalizability problem. It follows that the diagonalizability problem is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. We extend the result to *simultaneous diagonalizability* where one has to decide whether *all* of k given matrices are diagonalizable by the same diagonalizing matrix.

2. Preliminaries

We assume familiarity with some basic notions of complexity theory and linear algebra. We refer the readers to the papers [2, 3] for more details and properties of the considered complexity classes, and to the textbooks [9, 11, 10] for more background in linear algebra.

2.1. Complexity Classes

For a nondeterministic Turing machine M, we denote the number of accepting and rejecting computation paths on input x by $acc_M(x)$ and by $rej_M(x)$, respectively. The difference of these two quantities is gap_M, i.e., for all x

$$gap_M(x) = acc_M(x) - rej_M(x).$$

The class **GapL** is defined as the set of all functions $gap_M(x)$ such that M is a nondeterministic logspace bounded Turing machine. **GapL** has many closure properties: for example it is closed under addition, subtraction, and multiplication (see [3]). In [1] (Corollary 3.3) it was shown that **GapL** is closed under composition in a very strong sense: if each element of an $n \times n$ matrix A is **GapL**-computable, then the determinant of A is still computable in **GapL**.

On the basis of the class **GapL** we can define $\mathbf{C}_=\mathbf{L}$ (exact counting in logspace) and **PL** (*probabilistic logspace*) as follows

$$\begin{aligned} \mathbf{C}_=\mathbf{L} &= \{S \mid \exists f \in \mathbf{GapL}, \forall x:\ x \in S \iff f(x) = 0\}, \\ \mathbf{PL} &= \{S \mid \exists f \in \mathbf{GapL}, \forall x:\ x \in S \iff f(x) \geq 0\}. \end{aligned}$$

Since it is open whether $\mathbf{C}_=\mathbf{L}$ is closed under complement, it makes sense to consider the *Boolean closure of* $\mathbf{C}_=\mathbf{L}$, i.e., the class of sets that can be expressed as a Boolean combination of sets in $\mathbf{C}_=\mathbf{L}$. For our purposes, it suffices to consider the following two classes:

(i) $\mathbf{coC}_=\mathbf{L}$ is the class of complement sets $\overline{L}$ where $L \in \mathbf{C}_=\mathbf{L}$,

(ii) $\mathbf{C}_=\mathbf{L} \wedge \mathbf{coC}_=\mathbf{L}$ [2] is defined as the class of intersections of sets in $\mathbf{C}_=\mathbf{L}$ with sets in $\mathbf{coC}_=\mathbf{L}$, i.e.,

$$L \in \mathbf{C}_=\mathbf{L} \wedge \mathbf{coC}_=\mathbf{L} \iff \exists L_1 \in \mathbf{C}_=\mathbf{L},\ L_2 \in \mathbf{coC}_=\mathbf{L}:\ \ L = L_1 \cap L_2.$$

For sets S_1 and S_2, we say that S_1 is $\mathbf{AC}^0$-*reducible to* S_2, if there is a logspace uniform circuit family of polynomial size and constant depth that computes S_1 with unbounded fan-in AND- and OR-gates, NOT-gates, and oracle gates for S_2.

Based on the $\mathbf{AC}^0$-reduction we can define the so-called $\mathbf{AC}^0$-*closures* such as $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ or $\mathbf{AC}^0(\mathbf{GapL})$. In particular, we consider the classes $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ and $\mathbf{AC}^0(\mathbf{GapL})$: the sets that are $\mathbf{AC}^0$-reducible to a set in $\mathbf{C}_=\mathbf{L}$, and to a function in $\mathbf{GapL}$, respectively. The known relationships among these classes are as follows

$$\mathbf{C}_=\mathbf{L} \subseteq \mathbf{C}_=\mathbf{L} \wedge \mathbf{coC}_=\mathbf{L} \subseteq \mathbf{AC}^0(\mathbf{C}_=\mathbf{L}) \subseteq \mathbf{PL} \subseteq \mathbf{AC}^0(\mathbf{GapL}) \subseteq \mathbf{TC}^1 \subseteq \mathbf{NC}^2.$$

Furthermore, we say that S_1 is *(logspace many-one) reducible to* S_2, if there is a function $f \in L$ (deterministic logspace) such that for all x we have $x \in S_1 \iff f(x) \in S_2$. In an analogous way one can define $\mathbf{AC}^0$- or $\mathbf{NC}^1$-many-one reductions. Unless otherwise stated, all reductions in this paper are logspace many-one.

2.2. Linear Algebra

Let $A \in \boldsymbol{F}^{n\times n}$ be a matrix over the field $\boldsymbol{F}$. The *characteristic polynomial* of A is the polynomial $\chi_A(x) = \det(xI - A)$. A nonzero polynomial $p(x)$ over $\boldsymbol{F}$ is called an *annihilating polynomial* for A if $p(A) = \mathbf{0}$. The Cayley-Hamilton Theorem states that $\chi_A(x)$ is an annihilating polynomial for A. The characteristic polynomial is a *monic polynomial*: its highest coefficient is one. The *minimal polynomial* of A, denoted by $\mu_A(x)$, is the unique monic annihilating polynomial for A with minimal degree. Note that if A is an integer matrix, then all coefficients of $\chi_A(x)$ and of $\mu_A(x)$ are also integers. We will denote the degree of a polynomial p by $\deg(p)$ and the constant term of p by $\mathrm{ct}(p)$. It is known that $1 \leq \deg(\mu_A(x)) \leq n$.

Two matrices $A, B \in \boldsymbol{F}^{n\times n}$ are called *similar* if there is a nonsingular matrix $P \in \boldsymbol{F}^{n\times n}$ such that $A = PBP^{-1}$. Furthermore, A is called *diagonalizable* if A is similar to a diagonal matrix. The matrices $A_1, \ldots, A_k$ are called *simultaneously diagonalizable* if there is a nonsingular matrix P such that $PA_1P^{-1}, \ldots, PA_kP^{-1}$ are diagonal.

2.3. Problems

We restrict all the matrix problems in the present paper to the problems for integer matrices. The reason for this restriction is that the integer matrix problems are equivalent to the corresponding rational matrix problems under logspace reducibility (see [2] for more details).

By DETERMINANT we denote the problem of computing the determinant of an $n \times n$ matrix A.

By POWERELEMENT we denote the problem of computing the element at position $(1, n)$ of the power A^m, i.e. the element $(A^m)_{1,n}$, for an $n \times n$ matrix A and an integer m.

Both problems POWERELEMENT and DETERMINANT are complete for $\mathbf{GapL}$ [4, 8, 21, 22, 23].

Various decision problems are based on $\mathbf{GapL}$-functions. The *verification* of a $\mathbf{GapL}$-function is captured by the class $\mathbf{C}_=\mathbf{L}$. A $\mathbf{GapL}$-complete function yields a $\mathbf{C}_=\mathbf{L}$-complete verification problem. For example, the problem of verifying whether

the determinant is zero, i.e. testing singularity, is complete for $\mathbf{C}_=\mathbf{L}$. Similarly, the problem of verifying whether the element at position $(1, n)$ of A^m is zero, is complete for $\mathbf{C}_=\mathbf{L}$. We denote the latter problem by PowerElement$_=$. Allender, Beals and Ogihara [2] considered the rank problem of a matrix. They showed that

- Rank $= \{(A, k, b) \mid$ the k-th bit of rank(A) is $b\}$ is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$,
- Rank$_\leq = \{(A, r) \mid \text{rank}(A) \leq r\}$ is complete for $\mathbf{C}_=\mathbf{L}$, and
- Rank$_= = \{(A, r) \mid \text{rank}(A) = r\}$ is complete for $\mathbf{C}_=\mathbf{L} \wedge \mathbf{coC}_=\mathbf{L}$.

With respect to the minimal polynomial, MinPolynomial is the problem of computing the i-th coefficient d_i of $\mu_A(x)$ for given A and i. MinPolynomial is computable in $\mathbf{AC}^0(\mathbf{GapL})$ and is hard for $\mathbf{GapL}$ [13, 14].

The problem DegMinPol is defined as the set of all triples (A, k, b) such that b is the k-th bit of $\deg(\mu_A(x))$, i.e,

$$\text{DegMinPol} = \{(A, k, b) \mid \text{the } k\text{-th bit of } \deg(\mu_A(x)) \text{ is } b\}.$$

There is a number of decision problems related to MinPolynomial and DegMinPol: Let A and B be square matrices and let $m \geq 1$

- EqMinPolynomial is to decide whether $\mu_A(x) = \mu_B(x)$, i.e.,

$$\text{EqMinPolynomial} = \{(A, B) \mid \mu_A(x) = \mu_B(x)\}.$$

- EqCTMinPol is to decide whether $\text{ct}(\mu_A(x)) = \text{ct}(\mu_B(x))$, i.e.,

$$\text{EqCTMinPol} = \{(A, B) \mid \text{ct}(\mu_A(x)) = \text{ct}(\mu_B(x))\}.$$

- EqDegMinPol is to decide whether $\deg(\mu_A(x)) = \deg(\mu_B(x))$, i.e.,

$$\text{EqDegMinPol} = \{(A, B) \mid \deg(\mu_A(x)) = \deg(\mu_B(x))\}.$$

- DegMinPol$_=$ is to decide whether $\deg(\mu_A(x)) = m$, i.e.,

$$\text{DegMinPol}_= = \{(A, m) \mid \deg(\mu_A(x)) = m\}.$$

- DegMinPol$_\leq$ is to decide whether $\deg(\mu_A(x)) \leq m$, i.e.,

$$\text{DegMinPol}_\leq = \{(A, m) \mid \deg(\mu_A(x)) \leq m\}.$$

Furthermore, we denote the set of all diagonalizable matrices by Diagonalizable, and the set of all collections of simultaneously diagonalizable matrices by SimDiagonalizable.

3. The Minimal Polynomial

In this section we investigate the complexity of the degree and the constant term of the minimal polynomial of a matrix. The upper bounds on the complexity of these problems follow easily from the results in our preceding work [13, 14]. The main contributions of the present paper are the lower bounds for these problems. In particular, we want to point out that the degree of the minimal polynomial has exactly the same complexity as the matrix rank, and the constant term of this polynomial is not computable in **GapL** unless $\mathbf{C_=L}$ is closed under complement.

3.1. Upper Bounds

In [13] it was shown that the minimal polynomial of a square matrix can be computed in $\mathbf{AC^0(GapL)}$. The $\mathbf{AC^0(GapL)}$-algorithm was based on the following observation.

Let A be an $n \times n$ matrix. For each i, $0 \leq i \leq n$, define $\boldsymbol{a}_i$ to the n^2-dimensional column vector that is the concatenation of all the n column vectors of A^i. Then the minimal polynomial $\mu_A(x)$ has degree m if and only if the following two properties hold:

(i) $\mu_A(A) = \mathbf{0}$. Equivalently, the vectors $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ are *linearly dependent.*

(ii) For every monic polynomial $p(x)$ having degree $m-1$ it holds that $p(A) \neq \mathbf{0}$. Equivalently, the vectors $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1}$ are *linearly independent.*

Note that in the case when the degree of $\mu_A(x)$ is m each of the vectors $\boldsymbol{a}_m, \ldots, \boldsymbol{a}_n$ can be represented as a linear combination of the linearly independent vectors $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1}$.

Proposition 1 *1)* DegMinPol$_\leq$ *is in* $\mathbf{C_=L}$. DegMinPol$_=$ *is in* $\mathbf{C_=L} \wedge \mathbf{coC_=L}$.
2) EqDegMinPol *and* DegMinPol *are in* $\mathbf{AC^0(C_=L)}$.

Proof. 1) Given (A, m), let the order of A be n. For each $j = 1, \ldots, n$, we define the $n^2 \times j$ matrix C_j and the symmetric $j \times j$ matrices D_j as follows

$$\begin{aligned} C_j &= (\boldsymbol{a}_0\ \boldsymbol{a}_1\ \cdots\ \boldsymbol{a}_{j-1}), \\ D_j &= C_j^T\ C_j. \end{aligned}$$

Observe that all of the matrices $C_m, \ldots, C_n$ and $D_m, \ldots, D_n$ have rank m, where m is the degree of $\mu_A(x)$, i.e.

$$\mathrm{rank}(D_n) = \deg(\mu_A(x)).$$

Let the characteristic polynomial of D_n be

$$\chi_{D_n}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0.$$

Since D_n is symmetric, we have $\mathrm{rank}(D_n) = n - l$, where l is the smallest index such that $c_l \neq 0$. Hence we have

$$\deg(\mu_A(x)) = n - l.$$

Therefore

$$\begin{aligned}\deg(\mu_A(x)) \le m \quad &\Longleftrightarrow \quad c_0 = c_1 = \cdots = c_{n-m} = 0,\\ \deg(\mu_A(x)) = m \quad &\Longleftrightarrow \quad c_0 = c_1 = \cdots = c_{n-m} = 0 \text{ and } c_{n-m+1} \neq 0.\end{aligned}$$

For a given matrix, the coefficients of its characteristic polynomial are computable in **GapL**. Because each element of D_n is computable in **GapL** and because **GapL** is closed under composition [1], each of the coefficients $c_{n-1}, \ldots, c_0$ is computable in **GapL** as well. Moreover, testing whether $c_i = 0$ simultaneously for multiple values of i can be done in $\mathbf{C}_=\mathbf{L}$ since $\mathbf{C}_=\mathbf{L}$ is closed under conjunction [3]. This proves part 1 and 2 of the proposition.

2) Given (A, B), let the orders of A and B be n and p, respectively. (A, B) is in EqDegMinPol if and only if there is an number m in the set $\{1, \ldots, \min\{n, p\}\}$ such that $\deg(\mu_A(x)) = m$ and $\deg(\mu_B(x)) = m$. Therefore EqDegMinPol is in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Let (A, k, b) be an input to DegMinPol and let n be the order of A. A straightforward approach to obtain the upper bound for DegMinPol might be to use the fact that

$$(A, k, b) \in \text{DegMinPol} \iff (D_n, k, b) \in \text{Rank}.$$

However, the elements of D_n seem to require a **GapL**-computation: $D_n = C_n^T C_n$ and the elements of C_n are computable in **GapL**. Therefore we end up in $\mathbf{AC}^0(\mathbf{GapL})$ that way.

Instead, we construct an $\mathbf{AC}^0$-circuit with oracle gates from $\mathbf{C}_=\mathbf{L}$ for DegMinPol: for each number $m \in \{1, \ldots, n\}$ whose k-th bit is b we construct an $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ circuit to decide whether $\deg \mu_A(x) = m$. The final output is the disjunction of these circuits.

□

Proposition 2 EqMinPolynomial *and* EqCTMinPol *are in* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Proof. Let A and B be given matrices. Consider the coefficients of the minimal polynomial of A

$$\mu_A(x) = x^m + d_{m-1}x^{m-1} + \cdots + d_0.$$

By properties (i) and (ii) above, the coefficient vector $\boldsymbol{d}_A = (d_0, d_1, \ldots, d_{m-1})^T$ is the unique solution of the system of linear equations

$$C_m \boldsymbol{x} = -\boldsymbol{a}_m,$$

or, equivalently,

$$C_m^T C_m \boldsymbol{x} = -C_m^T \boldsymbol{a}_m.$$

Hence we get

$$(d_0, d_1, \ldots, d_{m-1})^T = -D_m^{-1} C_m^T \boldsymbol{a}_m. \tag{1}$$

Notice that D_m is nonsingular and each element of D_m^{-1} can be computed in **GapL** because of the closure properties of **GapL** under composition [1]. We can express the coefficient vector $\boldsymbol{d}_B$ of $\mu_B(x)$ analogously as for A in equation (1). It follows that in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ we can compare the coefficient vectors $\boldsymbol{d}_A$ and $\boldsymbol{d}_B$. □

3.2. Lower Bounds

Allender, Beals, and Ogihara [2] showed that RANK$_{\leq}$ is hard for $\mathbf{C}_{=}\mathbf{L}$ and RANK$_{=}$ is hard for $\mathbf{C}_{=}\mathbf{L} \wedge \mathbf{coC}_{=}\mathbf{L}$. We show that the exact parallels of these results hold for DEGMINPOL$_{\leq}$ and DEGMINPOL$_{=}$ by the following theorem.

Theorem 1 *1)* DEGMINPOL$_{\leq}$ *is hard for* $\mathbf{C}_{=}\mathbf{L}$.

2) DEGMINPOL$_{=}$ *is hard for* $\mathbf{C}_{=}\mathbf{L} \wedge \mathbf{coC}_{=}\mathbf{L}$.

Proof. 1) To show the first part of the theorem, we reduce POWERELEMENT$_{=}$ to DEGMINPOL$_{\leq}$.

Let an $n \times n$ matrix A and an integer $m \geq 1$ be given as input to POWERELEMENT$_{=}$. Our task is to decide whether $(A^m)_{1,n} = 0$. In [14] (see also [13]) it was shown how to construct a matrix B (in logspace) such that

$$\mu_B(x) \quad = \quad x^{2m+2} - ax^{m+1}, \text{ where } a = (A^m)_{1,n}.$$

Let C be the companion matrix of the polynomial x^{2m+2}, that is, the $(2m+2) \times (2m+2)$ matrix in which all the elements on the first sub-diagonal are 1 and the rest is all 0. Note that the companion matrix of a polynomial $p(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_1 x + \alpha_0$ is the following $k \times k$ matrix

$$P = \begin{bmatrix} 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ & & \cdots\cdots\cdots\cdots & & \\ 0 & 0 & \cdots & 1 & -\alpha_{k-1} \end{bmatrix},$$

and that $\chi_P(x) = \mu_P(x) = p(x)$ (see [10], Section 3.3). Therefore we have $\chi_C(x) = \mu_C(x) = x^{2m+2}$.

Define the diagonal *block matrix* $D = \begin{bmatrix} B & \mathbf{0} \\ \mathbf{0} & C \end{bmatrix}$. It is known that the minimal polynomial of D is the *least common multiple* (for short: lcm) of the polynomials $\mu_B(x)$ and $\mu_C(x)$ (see [10], Section 3.3, exercise 8). Therefore, we obtain

$$\begin{aligned} \mu_D(x) \quad &= \quad \text{lcm}\{x^{m+1}(x^{m+1} - a), x^{2m+2}\} \\ &= \quad \begin{cases} x^{2m+2}, & \text{for } a = 0, \\ x^{2m+2}(x^{m+1} - a), & \text{for } a \neq 0. \end{cases} \end{aligned}$$

It follows that

$$a = (A^m)_{1,n} = 0 \iff \deg(\mu_D(x)) = 2m + 2.$$

2) To show the second part of the theorem, we reduce an arbitrary language L in $\mathbf{C}_{=}\mathbf{L} \wedge \mathbf{coC}_{=}\mathbf{L}$ to DEGMINPOL$_{=}$. Namely, we compute (in logspace) matrices A_1 and A_2 of order n_1 and n_2, respectively, and integers m and l, $1 \leq m, l$, such that for every w:

$$w \in L \quad \iff \quad (A_1^m)_{1,n_1} = 0 \text{ and } (A_2^l)_{1,n_2} \neq 0.$$

Due to Lemma 1 below we may assume w.l.o.g. that $m > l$.

Let $a_1 = (A_1^m)_{1,n_1}$ and $a_2 = (A_2^l)_{1,n_2}$. As explained in the first part of the proof, (in logspace) we can compute matrices B_1 and B_2 such that

$$\begin{aligned} \mu_{B_1}(x) &= x^{2m+2} - a_1 x^{m+1}, \\ \mu_{B_2}(x) &= x^{2l+2} - a_2 x^{l+1}. \end{aligned}$$

By C we denote again the companion matrix of x^{2m+2}. Define the matrix

$$D = \begin{bmatrix} B_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & B_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & C \end{bmatrix}.$$

Then we get

$$\begin{aligned} \mu_D(x) &= \mathrm{lcm}\{\mu_{B_1}(x),\ \mu_{B_2}(x),\ \mu_C(x)\} \\ &= \mathrm{lcm}\{x^{m+1}(x^{m+1} - a_1),\ x^{l+1}(x^{l+1} - a_2),\ x^{2m+2}\} \\ &= x^{2m+2}\mathrm{lcm}\{x^{m+1} - a_1,\ x^{l+1} - a_2\}. \end{aligned}$$

Since $m > l$, we have

$$\deg(\mu_D(x)) = \begin{cases} 2m + l + 3, & \text{for } a_1 = 0,\ a_2 \neq 0, \\ 3m + 3, & \text{for } a_1 \neq 0,\ a_2 = 0, \\ 2m + 2, & \text{for } a_1 = 0,\ a_2 = 0, \\ 3m + 3 + r, & \text{for } a_1 \neq 0,\ a_2 \neq 0, \text{ where } r > 0. \end{cases}$$

We concluded that for every w

$$\begin{aligned} w \in L &\iff a_1 = 0 \text{ and } a_2 \neq 0 \\ &\iff \deg(\mu_D(x)) = 2m + l + 3. \end{aligned}$$

This completes the proof of the theorem.

□

By Proposition 1 and Theorem 1 we obtain the following corollary.

Corollary 1 *1)* DEGMINPOL$_{\leq}$ *is complete for* $\mathbf{C}_{=}\mathbf{L}$.

2) DEGMINPOL$_{=}$ *is complete for* $\mathbf{C}_{=}\mathbf{L} \wedge \mathbf{coC}_{=}\mathbf{L}$.

The following lemma completes the proof of Theorem 1.

Lemma 1 *Let A be an $n \times n$ matrix and let $m \geq 1$. For any $k \geq 1$ there is a matrix $\widetilde{A}$ of order $p = n(mk+1)$ such that $(A^m)_{1,n} = (\widetilde{A}^{km})_{1,p}$.*

Proof. Define the following $(mk+1) \times (mk+1)$ block matrix $\widetilde{A}$

$$\widetilde{A} = \begin{bmatrix} \mathbf{0} & A & & & & & & & & \\ & \mathbf{0} & I & & & & & & & \\ & & \ddots & \ddots & & & & & & \\ & & & \mathbf{0} & I & & & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \ddots & \ddots & & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & & & \mathbf{0} & A & & \\ & & & & & & & \mathbf{0} & I & \\ & & & & & & & & \ddots & \ddots \\ & & & & & & & & & \mathbf{0} & I \\ & & & & & & & & & & \mathbf{0} \end{bmatrix}.$$

Each block of $\widetilde{A}$ is a matrix of order n. In the first block super-diagonal of $\widetilde{A}$ the pattern of an A followed by $(k-1)$ times I is repeated m times, and the rest is all zero-matrix ($\mathbf{0}$).

An elementary calculation shows that $\widetilde{A}^{mk}$ has A^m as its upper right block at position $(1, mk+1)$, and all other blocks are $\mathbf{0}$

$$\widetilde{A}^{mk} = \begin{bmatrix} \mathbf{0} & \cdots & \mathbf{0} & A^m \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \end{bmatrix}$$

Therefore, we have $(A^m)_{1,n} = (\widetilde{A}^{km})_{1,p}$.

□

Next we show that several decision problems based on the minimal polynomial are hard for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. Let FSLE denote the problem *Feasible Systems of Linear Equations* [2]. An input to FSLE consists of an $m \times n$ matrix A and an m-dimensional integer vector $\boldsymbol{b}$. One has to decide whether the system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ has a rational solution $\boldsymbol{x}$. Allender, Beals, and Ogihara [2] proved that FSLE is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Theorem 2 EqMinPolynomial, EqDegMinPol, DegMinPol, *and* EqCTMinPol *are hard for* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Proof. Let $(A, \boldsymbol{b})$ be an input to FSLE. Define the symmetric $(m+n) \times (m+n)$ matrix

$$B = \begin{bmatrix} \mathbf{0} & A \\ A^T & \mathbf{0} \end{bmatrix}$$

and the vector $\boldsymbol{c} = (\boldsymbol{b}^T, \mathbf{0})^T$ of length $m+n$. Furthermore, define the following two $(m+n+1) \times (m+n+1)$ matrices

$$C = \begin{bmatrix} B & \mathbf{0} \\ \mathbf{0} & 0 \end{bmatrix} \text{ and } D = \begin{bmatrix} B & \boldsymbol{c} \\ \mathbf{0} & 0 \end{bmatrix}.$$

Let $\lambda_1, \ldots, \lambda_k$ be distinct eigenvalues of C. It will be useful later on to observe that

(a) C is a symmetric matrix. Therefore, C is diagonalizable, its elementary divisors have the form $(x-\lambda_i)$, and $\mu_C(x) = (x-\lambda_1)\cdots(x-\lambda_k)$ (see [10], Section 3.3, Theorem 3.3.6 and Corollary 3.3.8).

(b) C and D are singular matrices. They have the same characteristic polynomial: $\chi_C(x) = \chi_D(x) = x\,\chi_B(x)$, and consequently they have the same eigenvalues. It follows that $\deg(\mu_C(x)) \leq \deg(\mu_D(x))$, and the elementary divisors of D have the form $(x-\lambda_i)^{t_i}$, for some $t_i \geq 1$.

We prove the following equivalences

$$
\begin{aligned}
(A, \boldsymbol{b}) \in \text{FSLE} &\iff (B, \boldsymbol{c}) \in \text{FSLE} && (2)\\
&\iff C \text{ is similar to } D && (3)\\
&\iff D \in \textsc{Diagonalizable} && (4)\\
&\iff \mu_C(x) = \mu_D(x) && (5)\\
&\iff \deg(\mu_C(x)) = \deg(\mu_D(x)) && (6)\\
&\iff \deg(\mu_D(x)) \text{ is odd} && (7)\\
&\iff \mathrm{ct}(\mu_{C_\alpha}(x)) = \mathrm{ct}(\mu_{D_\alpha}(x)), && (8)
\end{aligned}
$$

where $C_\alpha = C + \alpha I$ and $D_\alpha = D + \alpha I$ for an appropriate positive integer α to be chosen later.

Equivalences (2), (3), and (4) were shown in [13]. For completeness, we include a proof.

Equivalence (2). The equivalence holds because the system $A^T\boldsymbol{x} = \boldsymbol{0}$ is always feasible.

Equivalence (3). Consider the case where the system $B\boldsymbol{x} = \boldsymbol{c}$ is feasible. Let $\boldsymbol{x}_0$ be a solution of the system. Define the $(m+n+1) \times (m+n+1)$ matrix T by

$$
T = \begin{bmatrix} I & \boldsymbol{x}_0 \\ \boldsymbol{0} & -1 \end{bmatrix}.
$$

It is easy to see that T is nonsingular and that $CT = TD$. Thus, C is similar to D.

Conversely, if the above system is not feasible, then C and D have different ranks. This implies that they can not be similar.

Equivalence (4). By observation (a) from above, matrix C is similar to a diagonal matrix, say C'. If C is similar to D, then D is similar to C' because the similarity relation is transitive. Hence D is diagonalizable.

Conversely, if D is diagonalizable, then D has only linear elementary divisors. By observation (b), C and D have the same eigenvalues. It follows that C and D must have the same system of elementary divisors, i.e., they are similar.

Equivalence (5). If C is similar to D, then clearly $\mu_C(x) = \mu_D(x)$.

Conversely, if $\mu_C(x) = \mu_D(x)$, then $\mu_D(x)$ contains only linear irreducible factors, because $\mu_C(x)$ has this property by observation (a). Therefore D is diagonalizable (see [10], Section 3.3, Corollary 3.3.10).

Equivalence (6). By observation (b) we have $\deg(\mu_C(x)) \leq \deg(\mu_D(x))$. These degrees are *equal* if and only if every root of $\mu_D(x)$ has multiplicity 1. The latter holds if and only if D is diagonalizable.

Equivalence (7). Let the distinct non-zero eigenvalues of the matrix $A^T A$ be $\delta_1, \delta_2, \ldots, \delta_l$ (they are all positive). Then the distinct eigenvalues of C are as follows

$$-\sqrt{\delta_l}\,, -\sqrt{\delta_{l-1}}\,, \ldots, -\sqrt{\delta_1}\,, 0\,, \sqrt{\delta_1}\,, \ldots, \sqrt{\delta_{l-1}}\,, \sqrt{\delta_l}$$

(see [11], Chapter 3). Note that C is a singular matrix. Thus, the number of distinct eigenvalues of C is $2l+1$. This implies that $k = \deg(\mu_C(x)) = 2l+1$ is always odd.

To prove the claim, we show that

$$\deg(\mu_D(x)) \in \{\deg(\mu_C(x)),\ \deg(\mu_C(x)) + 1\}.$$

Since $\deg(\mu_C(x)) \leq \deg(\mu_D(x))$ by observation (b), it suffices to show that $\deg(\mu_D(x)) \leq \deg(\mu_C(x)) + 1$.

We consider powers of C and D

$$C^i = \begin{bmatrix} B^i & \mathbf{0} \\ \mathbf{0} & 0 \end{bmatrix}, \qquad D^i = \begin{bmatrix} B^i & B^{i-1}\boldsymbol{c} \\ \mathbf{0} & 0 \end{bmatrix}. \tag{9}$$

Let the minimal polynomial of C be

$$\mu_C(x) = x^k + d_{k-1}x^{k-1} + \cdots + d_1 x + d_0.$$

Since $\mu_C(C) = \mathbf{0}$, we can write C^k as

$$C^k = -(d_{k-1}C^{k-1} + \cdots + d_1 C + d_0 I).$$

By equation (9) for C^i this yields

$$B^k = -\sum_{i=0}^{k-1} d_i B^i.$$

By equation (9) for D^i we get

$$\begin{aligned} D^{k+1} &= \begin{bmatrix} B^{k+1} & B^k\boldsymbol{c} \\ \mathbf{0} & 0 \end{bmatrix} \\ &= \begin{bmatrix} -\sum_{i=0}^{k-1} d_i B^{i+1} & -\sum_{i=0}^{k-1} d_i B^i \boldsymbol{c} \\ \mathbf{0} & 0 \end{bmatrix} \\ &= -\sum_{i=0}^{k-1} d_i D^{i+1}. \end{aligned} \tag{10}$$

Define the polynomial

$$p(x) = x\mu_C(x) = x^{k+1} + d_{k-1}x^k + \cdots + d_1x^2 + d_0x.$$

Equation (10) implies that $p(D) = \mathbf{0}$. By definition of the minimal polynomial, we must have

$$\deg(\mu_D(x)) \leq \deg(p) = k + 1.$$

We conclude that $\deg(\mu_D(x))$ must be either k or $k + 1$.

Equivalence (8). Observe that, for any α, equivalences (2) to (6) still hold when we replace C_α and D_α for C and D, respectively. In particular we have

$$\mu_C(x) = \mu_D(x) \Longrightarrow \mathrm{ct}(\mu_{C_\alpha}(x)) = \mathrm{ct}(\mu_{D_\alpha}(x)).$$

It remains to select an appropriate value for α such that the converse implication holds.

Fix any α. Since the distinct eigenvalues of C are $\lambda_1, \ \ldots, \ \lambda_k$, the distinct eigenvalues of C_α are $\lambda_1 + \alpha, \ \ldots, \ \lambda_k + \alpha$.

Since C_α is symmetric and since C_α and D_α still have the same eigenvalues, we can write

$$\begin{aligned} \mu_{C_\alpha}(x) &= \prod_{i=1}^{k}(x - (\lambda_i + \alpha)), \text{ and} \\ \mu_{D_\alpha}(x) &= \prod_{i=1}^{k}(x - (\lambda_i + \alpha))^{t_i}, \end{aligned}$$

where $t_i \geq 1$ for $i = 1, 2, \ldots, k$.

It suffices to choose α such that $\lambda_i + \alpha > 1$ for all i. If $\mu_{C_\alpha}(x)$ and $\mu_{D_\alpha}(x)$ have the same constant term for such an α, then they must be equal. Define

$$\alpha = \|C\| + 2,$$

where $\|C\|$ is the *maximum column sum matrix norm* of $C = (c_{i,j})$ which is defined as follows

$$\|C\| = \max_{1 \leq j \leq m+n+1} \sum_{i=1}^{m+n+1} |c_{i,j}|$$

(see [10], Section 5.6).

The *spectral radius* of C, denoted by $\rho(C)$, is as follows

$$\rho(C) = \max_{1 \leq i \leq k} |\lambda_i|.$$

It is known that $\rho(C) \leq \|C\|$ (see [10], Section 5.6). Therefore, $\lambda_i + \alpha > 1$, for $i = 1, 2, \ldots, k$. Note that α can be computed in logspace. This completes the proof of the theorem.

□

By Proposition 1 and 2, and by Theorem 2 we get the following corollary.

Corollary 2 EQMINPOLYNOMIAL, EQDEGMINPOL, DEGMINPOL, *and* EQCTMINPOL *are complete for* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

In Section 3.1, it was shown that, given A, one can compute a matrix B in **GapL** such that $\deg(\mu_A(x)) = \mathrm{rank}(B)$. On the other hand, we don't know whether there is a converse reduction, i.e. given A, compute B such that $\mathrm{rank}(A) = \deg(\mu_B(x))$. Note that Corollary 2 provides such a reduction only for the bitwise versions of these functions, namely DEGMINPOL and RANK.

Recall that the constant term of the characteristic polynomial $\chi_A(x)$ is $(-1)^n \det(A)$. This term is computable in **GapL**. Now assume for a moment, that the constant term of the minimal polynomial is in **GapL** as well. It follows that EQCTMINPOL is in $\mathbf{C}_=\mathbf{L}$, because this is asking whether the difference of two constant terms (a **GapL**-function) is zero. By Theorem 2, it follows that $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L}) = \mathbf{C}_=\mathbf{L}$.

Corollary 3 *If the constant term of the minimal polynomial of a matrix is computable in* **GapL**, *then* $\mathbf{C}_=\mathbf{L}$ *is closed under complement.*

We can considerably weaken the assumption in Corollary 3: it suffices to have a certain *addition property* of the constant term of the minimal polynomial. Namely, given matrices A and B, suppose there is a matrix C such that each element of C is computable in **GapL**, and

$$\mathrm{ct}(\mu_C(x)) = \mathrm{ct}(\mu_A(x)) - \mathrm{ct}(\mu_B(x)).$$

Then we have $(A, B) \in$ EQCTMINPOL if and only if $\mathrm{ct}(\mu_C(x)) = 0$. The latter is equivalent to $\det(C) = 0$. Since the the determinant of C is a **GapL**-function ([1], Corollary 3.3), we conclude that $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ collapses to $\mathbf{C}_=\mathbf{L}$.

Corollary 4 *If the constant term of the minimal polynomial has the above addition property, then* $\mathbf{C}_=\mathbf{L}$ *is closed under complement.*

4. Diagonalizability

In [12] it was shown that the problem of deciding whether two matrices are similar is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. Related to the similarity problem is the diagonalizability problem. DIAGONALIZABLE is hard for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ by Theorem 2 and is contained in $\mathbf{AC}^0(\mathbf{GapL})$ [13]. In this section we show that DIAGONALIZABLE and SIMDIAGONALIZABLE are complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Theorem 3 DIAGONALIZABLE *is complete for* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Proof. It remains to prove that DIAGONALIZABLE is in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

In Section 3.1, it was shown how to construct a matrix D_n, for a given $n \times n$ matrix A, such that $\deg(\mu_A(x)) = \mathrm{rank}(D_n)$. Matrix A is diagonalizable if and only if its minimal polynomial contains only linear irreducible factors. The latter is equivalent to the condition that the degree of $\mu_A(x)$ is equal the number of distinct eigenvalues of the matrix A.

Let l be the number of distinct eigenvalues of A. Another way to characterize l is by means of the *Hankel matrix* H_A associated with A. More precisely, the Hankel

matrix $H_A = (h_{i,j})$ is defined as a symmetric $n \times n$ matrix whose elements are defined as follows

$$h_{i,j} = \text{trace}(A^{i+j-2}), \text{ for } i,j = 1,\ldots,n,$$

where trace(X) is the sum of all elements on the diagonal of the matrix X. It is well known that $l = \text{rank}(H_A)$ (see [9], Chapter XV, Theorem 6).

In summary, we have

$$\begin{aligned} A \text{ is diagonalizable} &\iff \deg(\mu_A(x)) = \#\text{ of distinct eigenvalues of } A \\ &\iff \text{rank}(D_n) = \text{rank}(H_A). \end{aligned} \tag{11}$$

Since each element of D_n and H_A can be computed in **GapL**, the condition in equivalence (11) can be tested in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. Hence, DIAGONALIZABLE is in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

□

Finally, we consider the problem SIMDIAGONALIZABLE. The problem is to decide, given k $n \times n$ matrices $A_1,\ldots,A_k$, whether there exists a nonsingular matrix S such that SA_iS^{-1} are diagonal, for all i, $1 \le i \le k$.

In the case when all matrices A_i are already diagonalizable these matrices are simultaneously diagonalizable if and only if they are pairwise commutable, i.e., $A_i\ A_j = A_j\ A_i$ for all i,j, $1 \le i,j \le k$ (see [10], Section 1.3). This can be checked in $\mathbf{NC}^1$. Therefore, the main part is to test whether $A_i \in$ DIAGONALIZABLE, for all i, $1 \le i \le k$. By Theorem 3 we get the following corollary.

Corollary 5 SIMDIAGONALIZABLE *is complete for* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

5. Summary

In the following table we summarize the complexities of the problems considered in the paper.

Problem	complete for
DEGMINPOL$_\le$	$\mathbf{C}_=\mathbf{L}$
DEGMINPOL$_=$	$\mathbf{C}_=\mathbf{L} \wedge \mathbf{coC}_=\mathbf{L}$
DEGMINPOL	$\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$
EQDEGMINPOL	$\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$
EQMINPOLYNOMIAL	$\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$
EQCTMINPOL	$\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$
DIAGONALIZABLE	$\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$
SIMDIAGONALIZABLE	$\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$

Acknowledgments

We thank Meena Mahajan for many interesting discussions and helpful comments on an earlier version of the paper. The comments of the anonymous referees helped to improve the presentation of the paper.

References

1. E. Allender, V Arvind, and M. Mahajan. Arithmetic complexity, Kleene closure, and formal power series. Technical Report *ECCC*, TR99-008, 1999.
2. E. Allender, R. Beals, and M. Ogihara. The complexity of matrix rank and feasible systems of linear equations. *Computational Complexity*, 8:99 –126, 1999.
3. E. Allender and M. Ogihara. Relationship among PL, #L, and the determinant. *RAIRO-Theoretical Informatics and Applications*, 30:1 –21, 1996.
4. S. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18:147–150, 1984.
5. A. Borodin, J. Von zur Gathen, and J. Hopcroft. Fast parallel matrix and GCD computations. *Information and Control*, 52:241–256, 1982.
6. A. L. Chistov. Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. *Foundations of Computation Theory (FCT)*, 5, 1985.
7. L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5:618–623, 1976.
8. C. Damm. DET = $L^{(\#L)}$. Technical Report Informatik-Preprint 8, Fachbereich Informatik der Humboldt-Universität zu Berlin, 1991.
9. F. Gantmacher. *The Theory of Matrices*, volume 1 and 2. AMS Chelsea Publishing, 1977.
10. R. Horn and C. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.
11. R. Horn and C. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1991.
12. T. M. Hoang and T. Thierauf. The complexity of verifying the characteristic polynomial and testing similarity. In *15th IEEE Conference on Computational Complexity (CCC)*, pages 87–95. IEEE Computer Society Press, 2000.
13. T. M. Hoang and T. Thierauf. The complexity of the minimal polynomial. In *26th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, Lecture Notes in Computer Science 2136, pages 408–420. Springer-Verlag, 2001.
14. T. M. Hoang and T. Thierauf. The complexity of the characteristic and the minimal polynomial. *Theoretical Computer Science*, 295:205–222, 2003.
15. N. Immerman. Nondeterministic space is closed under complement. *SIAM Journal on Computing*, 17:935–938, 1988.
16. M. Mahajan and V Vinay. Determinant: Combinatorics, algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, 1997(5), 1997.
17. N. Nisan and A. Ta-Shma. Symmetric logspace is closed under complement. *Chicago Journal of Theoretical Computer Science*, 1995(Article 1), 1995.
18. K. Reinhardt and E. Allender. Making nondeterminism unambiguous. *SIAM Journal on Computing*, 29:1118–1131, 2000.
19. M. Santha and S. Tan. Verifying the determinant in parallel. *Computational*

Complexity, 7:128–151, 1998.

20. R. Szelepcsényi. The method of forced enumeration for nondeterministic automata. *Acta Informatica*, 26(3):279–284, 1988.
21. S. Toda. Counting problems computationally equivalent to the determinant. Technical Report CSIM 91-07, Dept. of Computer Science and Information Mathematics, University of Electro-Communications, Chofu-shi, Tokyo 182, Japan, 1991.
22. L. Valiant. Why is boolean complexity theory difficult. In M.S. Paterson, editor, *Boolean Function Complexity*, London Mathematical Society Lecture Notes Series 169. Cambridge University Press, 1992.
23. V Vinay. Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits. In *6th IEEE Conference on Structure in Complexity Theory*, pages 270–284, 1991.