# On the Minimal Polynomial of a Matrix [⋆]

Thanh Minh Hoang and Thomas Thierauf

Abt. Theoretische Informatik
Universität Ulm
89069 Ulm, Germany
{hoang,thierauf}@informatik.uni-ulm.de

**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 behaves as 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 this holds also for the minimal polynomial if and only if the *logspace exact counting class* $\mathbf{C_{=}L}$ is closed under complement. The latter condition is one of the main open problems in this area.
As an application of our techniques we show that the problem to decide whether a matrix is diagonalizable is complete for $\mathbf{AC}^0(\mathbf{C_{=}L})$, the $\mathbf{AC}^0$-*closure of* $\mathbf{C_{=}L}$.

## 1 Introduction

A rule of thumb says that *Linear Algebra is in* $\mathbf{NC}^2$. However, if we look more closely, we see that this is a very rough statement. In particular, we are not able to show that the various problems in Linear Algebra are equivalent under, say, logspace many-one reductions.

It seems to be more appropriate to express the complexity of problems in Linear Algebra in terms of *logspace counting classes*. The initial step in this direction was done by Damm [Dam91], Toda [Tod91], Vinay [Vin91], and Valiant [Val92]. They showed that the determinant of an integer matrix characterizes the complexity class **GapL** (see [MV97] for more details on the history). Toda [Tod91] showed more problems to be complete for **GapL**, 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.

The verification of **GapL** functions is captured by the class $\mathbf{C_{=}L}$. An example of a complete problem is to decide whether an integer matrix $A$ is singular, i.e., whether $\det(A) = 0$. More general, the decision problem, whether the rank of $A$ is less than some given number $k$, is complete for $\mathbf{C_{=}L}$. The problem whether the rank of $A$ *equals* $k$ can be expressed as the conjunction of problems in $\mathbf{C_{=}L}$ and in $\mathbf{coC_{=}L}$, a class that we denote by $\mathbf{C_{=}L} \wedge \mathbf{coC_{=}L}$. The problem to determine the rank of a matrix is captured by the $\mathbf{AC}^0$-closure of $\mathbf{C_{=}L}$, which we denote

[⋆] This work was supported by the Deutsche Forschungsgemeinschaft

by $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. Finally, the problem to decide whether two matrices have the same rank is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. The results on the rank were shown by Allender, Beals, and Ogihara [ABO99].

The complexity of the minimal polynomial has been studied before [HT02](see also [HT00,HT01]). In this paper, we show that there is a strong relationship between the *degree of the minimal polynomial* of a matrix and the matrix rank problem. Namely, the problems to decide whether the degree of the minimal polynomial is less than $k$ or equal $k$, for some given $k$, are complete for $\mathbf{C}_=\mathbf{L}$ and $\mathbf{C}_=\mathbf{L} \wedge \mathbf{coC}_=\mathbf{L}$, respectively. To decide whether the degrees of the minimal polynomials of two matrices are equal is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

We also investigate the complexity of the constant term of the minimal polynomial. The constant term of the characteristic polynomial is **GapL**-complete. By analogy, 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: *the constant term of the minimal polynomial can be computed in* **GapL** *if and only if* $\mathbf{C}_=\mathbf{L}$ *is closed under complement*. This connection is a consequence of a hardness result: to decide whether the constant terms of the minimal polynomials of two matrices are equal is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

Whether $\mathbf{C}_=\mathbf{L}$ is closed under complement is one of the big open questions in this area. Recall that many related classes have this property: **NL** [Imm88,Sze88], **SL** [NTS95], **PL** (trivially), and nonuniform **UL** [RA00]. Thus our results on the constant term of the minimal polynomial might offer some new points to attack this problem.

A final observation is about the diagonalizability of matrices. In [HT01] it is shown that this decision is hard for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. We show that this class also is an upper bound for this problem. It follows that diagonalizability 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 [ABO99,AO96] for more details and properties of the considered complexity classes, and to the textbooks [Gan77,HJ91,HJ85] for more background in linear algebra.

*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 function class **GapL** is defined as the class 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 [AO96]). In [AAM99] (Corollary 3.3) it is shown that **GapL** is closed under composition in a very strong sense: if each entry of an $n \times n$ matrix $A$ is **GapL**-computable, then the determinant of $A$ is still computable in **GapL**.

A set $S$ is in $\mathbf{C_=L}$, if there exists a function $f \in \mathbf{GapL}$ such that for all $x$ we have $x \in S \iff f(x) = 0$. Since it is open whether $\mathbf{C_=L}$ is closed under complement, it makes sense to consider the *Boolean closure of* $\mathbf{C_=L}$, i.e., the class of sets that can be expressed as a Boolean combination of sets in $\mathbf{C_=L}$. For our purposes, it suffices to consider the following two classes: a) $\mathbf{coC_=L}$ is the class of complement sets $\overline{L}$ where $L \in \mathbf{C_=L}$, b) $\mathbf{C_=L} \wedge \mathbf{coC_=L}$ [ABO99] is defined as the class of intersections of sets in $\mathbf{C_=L}$ with sets in $\mathbf{coC_=L}$, i.e.,

$$L \in \mathbf{C_=L} \wedge \mathbf{coC_=L} \iff \exists L_1 \in \mathbf{C_=L},\ L_2 \in \mathbf{coC_=L} : \quad L = L_1 \cap L_2.$$

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 $S_2$. In particular, we consider the classes $\mathbf{AC}^0(\mathbf{C_=L})$ and $\mathbf{AC}^0(\mathbf{GapL})$: the sets that are $\mathbf{AC}^0$-reducible to a set in $\mathbf{C_=L}$, respectively a function in **GapL**. The known relationships among these classes are as follows:

$$\mathbf{C_=L} \subseteq \mathbf{C_=L} \wedge \mathbf{coC_=L} \subseteq \mathbf{AC}^0(\mathbf{C_=L}) \subseteq \mathbf{AC}^0(\mathbf{GapL}) \subseteq \mathbf{TC}^1 \subseteq \mathbf{NC}^2.$$

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.

*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 integer. Let's denote the degree of a polynomial $p$ by $\deg(p)$. Then we have $1 \leq \deg(\mu_A(x)) = m \leq n$.

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.

*Problems.* Unless otherwise stated the domain for the algebraic problems are the integers. By Determinant we denote the problem to compute the determinant of a given $n \times n$ matrix $A$. In PowerElement there is additionally given an integer $m$ and have to compute $(A^m)_{1,n}$, the element of $A^m$ at position $(1, n)$. Both PowerElement and Determinant are complete for **GapL** [Ber84,Dam91,Tod91,Val92,Vin91].

Various decision problems are based on **GapL**-functions. The *verification* of a **GapL**-function is captured by the class $\mathbf{C_=L}$. A **GapL**-complete function yields a $\mathbf{C_=L}$-complete verification problem. For example, to verify whether the determinant is zero, i.e., testing singularity, is complete for $\mathbf{C_=L}$. Similarly, to verify whether $A^m$ at position $(1, n)$ is zero, is complete for $\mathbf{C_=L}$. The latter problem we denote by PowerElement$_=$.

With respect to the minimal polynomial, MinPolynomial is the problem to compute 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 **GapL** [HT01,HT02]. With respect to the degree of the minimal polynomial, DegMinPol is the set of all triple $(A, k, b)$, where $b$ is the $k$-th bit of $\deg(\mu_A(x))$.

There is a bunch of decision problems related to MinPolynomial and DegMinPol: Given two matrices $A$ and $B$, and $k \geq 1$,

- EqMinPolynomial is to decide whether $\mu_A(x) = \mu_B(x)$,
- EqCTMinPol is to decide whether the minimal polynomials of $A$ and $B$ have the same constant term,
- EqDegMinPol is to decide whether the minimal polynomials of $A$ and $B$ have the same degree,
- DegMinPol$_=$ is to decide whether $\deg(\mu_A(x)) = k$,
- DegMinPol$_\leq$ is to decide whether $\deg(\mu_A(x)) \leq k$.

Finally, the set of all diagonalizable matrices is denoted by Diagonalizable. The set of all simultaneously diagonalizable matrices is denoted 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 predecessor paper [HT01,HT02]. The main contributions here are the lower bounds for these problems. In particular, we want to point out that the degree of the minimal polynomial has essentially the same complexity as the matrix rank.

### 3.1 Upper Bounds

In [HT01] it is shown that the minimal polynomial of a matrix $A$ can be computed in $\mathbf{AC}^0(\mathbf{GapL})$. The algorithm was based on the following observation. Define $\boldsymbol{a}_i = \mathit{vec}(A^i)$, where $\mathit{vec}(A^i)$ is the vector of length $n^2$ that is obtained by putting the columns of $A^i$ below each other, for $i = 0, 1, 2, \ldots, n$. Then the minimal polynomial $\mu_A(x)$ with degree $m$ is characterized by the following two properties:

(i) $\mu_A(A) = \mathbf{0}$. Equivalently we can say that $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ are *linearly dependent*, and

(ii) for every monic polynomial $p(x)$ with degree $m-1$, we have $p(A) \neq \mathbf{0}$. Equivalently we can say that $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1}$ are *linearly independent.*

Note that $\boldsymbol{a}_m, \ldots, \boldsymbol{a}_n$ linearly depend on $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{m-1}$ in this case. Define the $n^2 \times j$ matrices $C_j$ and the symmetric $j \times j$ matrices $D_j$ as

$$C_j = (\boldsymbol{a}_0 \; \boldsymbol{a}_1 \; \cdots \; \boldsymbol{a}_{j-1}), \; D_j = C_j^T \; C_j, \;\; \text{for } j = 1, \ldots, n.$$

Then $C_m, \ldots, C_n$ and $D_m, \ldots, D_n$ all have the same rank $m$, which is precisely the degree of $\mu_A(x)$. Hence we have $\deg(\mu_A(x)) = \operatorname{rank}(D_n)$.

Let $\chi_{D_n}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$. Since $D_n$ is symmetric, we have $\operatorname{rank}(D_n) = n - l$, where $l$ is the smallest index such that $c_l \neq 0$. Because **GapL** is closed under composition [AAM99], each of the coefficients $c_{n-1}, \ldots, c_0$ is computable in **GapL**. Therefore, in $\mathbf{C_{=}L}$ we can test whether one or several of the $c_i$'s are zero (note that $\mathbf{C_{=}L}$ is closed under conjunction). In particular, we get a method to verify the degree of the minimal polynomial.

**Proposition 3.1.** *1.* DegMinPol$_{\leq}$ *is in* $\mathbf{C_{=}L}$.
*2.* DegMinPol$_{=}$ *is in* $\mathbf{C_{=}L} \wedge \mathbf{coC_{=}L}$*,*
*3.* DegMinPol*,* EqDegMinPol *are in* $\mathbf{AC}^0(\mathbf{C_{=}L})$*,*

Part 1 and 2 of the proposition follow directly from the discussion above. The problems in part 3 can be solved with some extra $\mathbf{AC}^0$-circuitry.

Next, we consider the coefficients of $\mu_A(x) = x^m + d_{m-1}x^{m-1} + \cdots + d_0$. The vector $(d_0, d_1, \ldots, d_{m-1})^T$ is the unique solution of the system of linear equations $C_m \boldsymbol{x} = -\boldsymbol{a}_m$. 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 $D_m$ nonsingular for $m = \deg(\mu_A(x))$, and each element of $D_m^{-1}$ can be computed in **GapL** [AAM99].

Let $B$ be another matrix and we want to know whether $A$ and $B$ have the same minimal polynomial, or, whether their minimal polynomials have the same constant term. We can express the coefficients of $\mu_B(x)$ analogously as for $A$ in equation (1). It follows that we can compare the coefficients in $\mathbf{AC}^0(\mathbf{C_{=}L})$.

**Proposition 3.2.** EqMinPolynomial *and* EqCTMinPol *are in* $\mathbf{AC}^0(\mathbf{C_{=}L})$.

### 3.2 Lower Bounds

Allender, Beals, and Ogihara [ABO99] showed that the decision problem *Feasible Systems of Linear Equations*, FSLE for short, is complete for $\mathbf{AC}^0(\mathbf{C_{=}L})$. More precisely, an input for FSLE are an $m \times n$ matrix $A$ and a vector $\boldsymbol{b}$ of length $m$ over the integers. One has to decide whether the system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ has a rational solution. We use FSLE as reference problem to show the hardness results.

**Theorem 3.3.** EqDegMinPol, EqMinPolynomial, *and* EqCTMinPol *are hard for* $\mathbf{AC}^0(\mathbf{C_=L})$.

*Proof.* Let $A$ and $\boldsymbol{b}$ be an input for FSLE. Define the symmetric matrix $B = \begin{pmatrix} \mathbf{0} & A \\ A^T & \mathbf{0} \end{pmatrix}$ and vector $\boldsymbol{c} = (\boldsymbol{b}^T, \mathbf{0})^T$ of length $m+n$. We prove that

$$
\begin{aligned}
(A, \boldsymbol{b}) \in \text{FSLE} & \iff (B, \boldsymbol{c}) \in \text{FSLE} & (2)\\
& \iff C = \begin{pmatrix} B & \mathbf{0} \\ 0 \cdots 0 & 0 \end{pmatrix} \text{ is similar to } D = \begin{pmatrix} B & \boldsymbol{c} \\ 0 \cdots 0 & 0 \end{pmatrix} & (3)\\
& \iff D \in \textsc{Diagonalizable} & (4)\\
& \iff \mu_C(x) = \mu_D(x) & (5)\\
& \iff \deg(\mu_C(x)) = \deg(\mu_D(x)) & (6)\\
& \iff \operatorname{ct}(\mu_{C_\alpha}(x)) = \operatorname{ct}(\mu_{D_\alpha}(x)), & (7)
\end{aligned}
$$

where $\operatorname{ct}(\mu_M(x))$ denotes the constant term of $\mu_M(x)$, and $C_\alpha = C + \alpha I$ and $D_\alpha = D + \alpha I$ for an appropriate positive integer $\alpha$ to be chosen later.

Equivalences (2), (3), and (4) were shown in [HT01]. For completeness, we include a proof.

*Equivalence (2).* Note that the system $A^T x = \mathbf{0}$ is always feasible.

*Equivalence (3).* Let $x_0$ be a solution of the system $B\boldsymbol{x} = \boldsymbol{c}$. Define the nonsingular matrix $T = \begin{pmatrix} I & x_0 \\ \mathbf{0} & -1 \end{pmatrix}$. It is easy to check that $CT = TD$, therefore $C$ is similar to $D$. Conversely, if the above system is not feasible, then $C$ and $D$ have different ranks and can therefore not be similar.

*Equivalence (4).* Observe that matrix $C$ is symmetric. Therefore, $C$ is always diagonalizable, i.e., $C$ is similar to a diagonal matrix, say $C'$. Now, if $C$ is similar to $D$, then $D$ is similar to $C'$ as well, because the similarity relation is transitive. Hence $D$ is diagonalizable as well. Conversely, if $D$ is diagonalizable, then $D$ has only elementary divisors of the form $(x - \gamma_i)$ where $\gamma_i$ is any of its eigenvalues. Since $C$ is diagonalizable, its elementary divisors are also linear. Note furthermore that $C$ and $D$ have the same characteristic polynomial. Therefore, they must have the same system of elementary divisors, i.e., they are similar.

*Equivalence (5).* If $C$ is similar to $D$, then it is clearly that $\mu_C(x) = \mu_D(x)$. Conversely, if $\mu_C(x) = \mu_D(x)$, then $\mu_D(x)$ contains only linear irreducible factors, because $\mu_C(x)$ has this property (since $C$ is symmetric matrix). Therefore $D$ is diagonalizable.

*Equivalence (6).* Recall that $\deg(\mu_C(x))$ is exactly the number of all distinct eigenvalues of $C$. Since $C$ and $D$ have the same characteristic polynomial, they have the same eigenvalues, and therefore $\deg(\mu_C(x)) \leq \deg(\mu_D(x))$. These degrees are *equal* iff every root of $\mu_D(x)$ has multiplicity 1. The latter holds iff $D$ is diagonalizable.

*Equivalence (7).* Observe that equivalences (2) to (6) still hold when we replace $C_\alpha$ and $D_\alpha$ for $C$ and $D$, respectively, for any $\alpha$. For an appropriate choice of $\alpha$ we show: if the constant terms of $\mu_{C_\alpha}(x)$ and $\mu_{D_\alpha}(x)$ are equal, then these polynomials are equal.

Fix any $\alpha$. Let $\lambda_1, \ \ldots, \ \lambda_k$ be the distinct eigenvalues of $C$. Then the distinct eigenvalues of $C_\alpha$ are $\lambda_1 + \alpha, \ \ldots, \ \lambda_k + \alpha$. Since $C_\alpha$ is symmetric and since $C_\alpha$ and $D_\alpha$ have the same eigenvalues, we can write

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

where $t_i \geq 1$ for $i = 1, 2, \ldots, k$. In order to prove that $\mu_{C_\alpha}(x) = \mu_{D_\alpha}(x)$, we have to show that all $t_i = 1$, for an appropriate $\alpha$.

Note that the constant terms of these polynomials are the product of the eigenvalues (in the case of $D_\alpha$, with multiplicities $t_i$ each). Hence it suffices to choose $\alpha$ such that all eigenvalues of $C_\alpha$ are greater than 1. This is done as follows. By $\rho(C)$ we denote the *spectral radius* of $C$, i.e. $\rho(C) = \max_{1 \leq i \leq k} |\lambda_i|$. The *maximum column sum matrix norm* of $C = (c_{i,j})$ is defined as

$$||C|| = \max_{1 \leq j \leq 2n+1} \sum_{i=1}^{2n+1} |c_{i,j}|.$$

It is well known that $\rho(C) \leq ||C||$. Therefore, if we choose (in logspace) $\alpha = ||C|| + 2$, then we have $\lambda_i + \alpha > 1$, for $i = 1, 2, \ldots, k$.

□

**Corollary 3.4.** EqDegMinPol, EqMinPolynomial, *and* EqCTMinPol *are complete for* $\mathbf{AC}^0(\mathbf{C_{=}L})$.

Recall that the constant term of the characteristic polynomial can be computed 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 $\mathbf{C_{=}L}$, because this is asking whether the difference of two constant terms (a **GapL**-function) is zero. By Corollary 3.4, it follows that $\mathbf{AC}^0(\mathbf{C_{=}L}) = \mathbf{C_{=}L}$. This argument is a proof of the following corollary:

**Corollary 3.5.** *If the constant term of the minimal polynomial of a matrix is computable in* **GapL**, *then* $\mathbf{C_{=}L}$ *is closed under complement.*

**Theorem 3.6.** *1.* DegMinPol$_{\leq}$ *is hard for* $\mathbf{C_{=}L}$, *and*
*2.* DegMinPol$_{=}$ *is hard for* $\mathbf{C_{=}L} \wedge \mathbf{coC_{=}L}$.

*Proof.* 1) To show the first claim, we reduce PowerElement$_{=}$ to DegMinPol$_{\leq}$. Let $A$ be a $n \times n$ matrix and $m \geq 1$ be an input for PowerElement$_{=}$. One has to decide whether $(A^m)_{1,n} = 0$. In [HT02] (see also [HT01]) it is shown how to construct a matrix $B$ in logspace such that

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

Let $C$ be the companion matrix of the polynomial $x^{2m+2}$, that is, a $(2m+2) \times (2m+2)$ matrix, where all the elements on the first sub-diagonal are 1 and all the other elements are 0. Then we have $\chi_C(x) = \mu_C(x) = x^{2m+2}$.

Define $D = \begin{pmatrix} B & \mathbf{0} \\ \mathbf{0} & C \end{pmatrix}$. It is known that the minimal polynomial of $D$ is the *least common multiple* (for short: lcm) of the polynomials $\mu_B(x)$ and $\mu_C(x)$. Therefore we have

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

It follows that $(A^m)_{1,n} = 0 \Longleftrightarrow \deg(\mu_D(x)) = 2m + 2$.

2) To show the second claim, we reduce an arbitrary language $L \in \mathbf{C_=L} \wedge \mathbf{coC_=L}$ to DegMinPol$_=$. Namely, we compute (in logspace) matrices $A_1$ and $A_2$ of order $n_1$ and $n_2$, respectively, and integers $1 \leq m, l \leq n$ such that for all $w$

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

We show in Lemma 3.7 below that 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, 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 $x^{2m+2}$. For the diagonal block matrix $D = \begin{pmatrix} B_1 & & \\ & B_2 & \\ & & C \end{pmatrix}$, we get (for $m > l$)

$$\begin{aligned} \mu_D(x) &= \operatorname{lcm}\{\mu_{B_1}(x),\ \mu_{B_2}(x),\ \mu_C(x)\} \\ &= \operatorname{lcm}\{x^{m+1}(x^{m+1} - a_1),\ x^{l+1}(x^{l+1} - a_2),\ x^{2m+2}\} \\ &= \begin{cases} 2m + l + 3, & \text{for } a_1 = 0,\ a_2 \neq 0, \\ 3m + 3, & \text{for } a_1 \neq 0,\ a_2 = 0, \\ 2m + 2, & \text{for } a_1 = 0,\ a_2 = 0, \\ 3m + 3 + r, & \text{for } a_1 \neq 0,\ a_2 \neq 0, \text{ where } r > 0. \end{cases} \end{aligned}$$

In summary, we have
$w \in L \Longleftrightarrow a_1 = 0$ and $a_2 \neq 0 \Longleftrightarrow \deg(\mu_D(x)) = 2m + l + 3$.

□

The following lemma completes the proof of Theorem 3.6

**Lemma 3.7.** *Let $A$ be an $n \times n$ matrix and $m \geq 1$. 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* $\widetilde{A}$

$$\left(\begin{array}{ccccccccccc}
\mathbf{0} & A &&&&&&&&& \\
& \mathbf{0} & I &&&&&&&& \\
&& \ddots & \ddots &&&&&&& \\
&&& \mathbf{0} & I &&&&&& \\ \hline
&&&& \mathbf{0} & A &&&&& \\
&&&&& \mathbf{0} & I &&&& \\
&&&&&& \ddots & \ddots &&& \\
&&&&&&& \mathbf{0} & I && \\ \hline
&&&&&&&& \ddots & \ddots & \\
&&&&&&&&& \mathbf{0} & I \\ \hline
&&&&&&&&&& \mathbf{0}
\end{array}\right)$$

Each block of $\widetilde{A}$ is a matrix of order $n$. All blocks are zero except for the ones on the first block super-diagonal. Here we start with $A$ followed by $(k-1)$-times $I$. This pattern occurs $m$-times in total.

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

□

## 4 Diagonalizability

In [HT00] it is shown that the decision whether two matrices are similar is complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. It is well known that Diagonalizable is hard for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$ (see Theorem 3.3) and is contained in $\mathbf{AC}^0(\mathbf{GapL})$ [HT01]. In this section we show that Diagonalizable and SimDiagonalizable are complete for $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

**Theorem 4.1.** Diagonalizable *is complete for* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

*Proof.* It remains to prove that Diagonalizable is in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. Given matrix $A$. In Section 3.1 we shown how to construct a matrix $C_n$ such that $\deg(\mu_A(x)) = \operatorname{rank}(C_n)$.

Matrix $A$ is diagonalizable iff its minimal polynomial contains only linear irreducible factors. This is the case iff $\deg(\mu_A(x))$ equals the number of distinct eigenvalues of $A$. The latter number can be determined as the rank of the *Hankel matrix* $H_A$ associated with $A$ (see Chapter XV. in [Gan77]). Therefore, we have

$$\begin{aligned} A \text{ is diagonalizable } &\iff \deg(\mu_A(x)) = \#\text{ of distinct eigenvalues of } A \\ &\iff \operatorname{rank}(C_n) = \operatorname{rank}(H_A). \end{aligned} \qquad (8)$$

Since each element of $C_n$ and $H_A$ can be computed in **GapL**, equation (8) can be checked in $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$. □

We consider the problem SimDiagonalizable. Given matrices $A_1, \ldots, A_k$ of order $n$ and $k \geq 1$. We have to test whether there is a nonsingular matrix $S$ such that $SA_iS^{-1}$ are diagonal, for all $1 \leq i \leq k$. If all matrices $A_i$ are diagonalizable then they are simultaneously diagonalizable iff they are pairwise commutable, i.e. $A_i\ A_j = A_j\ A_i$ for all $i, j$. The latter test can be done in $\mathbf{NC}^1$. Therefore the main part is to test whether $A_i \in$ Diagonalizable, for all $i$. By Theorem 4.1 we get the following:

**Corollary 4.2.** SimDiagonalizable *is complete for* $\mathbf{AC}^0(\mathbf{C}_=\mathbf{L})$.

## References

[AAM99] E. Allender, V Arvind, and M. Mahajan. Arithmetic complexity, Kleene closure, and formal power series, 1999.

[ABO99] E. Allender, R. Beals, and M. Ogihara. The complexity of matrix rank and feasible systems of linear equations. *Computational Complexity*, 8:99–126, 1999.

[AO96] E. Allender and M. Ogihara. Relationship among PL, #L, and the determinant. *RAIRO-Theoretical Informatics and Applications*, 30:1–21, 1996.

[Ber84] S. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18:147–150, 1984.

[Dam91] C. Damm. DET $= \mathrm{L}^{(\#L)}$. Technical Report Informatik-Preprint 8, Fachbereich Informatik der Humboldt Universitaet zu Berlin, 1991.

[Gan77] F. Gantmacher. *The Theory of Matrices*, volume 1 and 2. AMS Chelsea Publishing, 1977.

[HJ85] R. Horn and C. Johnson. *Matrix Analysis.* Cambridge University Press, 1985.

[HJ91] R. Horn and C. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, 1991.

[HT00] 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.

[HT01] T. M. Hoang and T. Thierauf. The complexity of the minimal polynomial. In *26th International Symposium, MFCS 2001*, pages 408–420. Springer, 2001.

[HT02] T. M. Hoang and T. Thierauf. The complexity of the characteristic and the minimal polynomial. Invited paper to the special issue in *Theoretical Computer Science* of the 26th MFCS conference 2001, to appear, 2002.

[Imm88] N. Immerman. Nondeterministic space is closed under complement. *SIAM Journal on Computing*, 17:935–938, 1988.

[MV97] M. Mahajan and V Vinay. Determinant: Combinatorics algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, 5, 1997.

[NTS95] N. Nisan and A. Ta-Shma. Symmetric logspace is closed under complement. *Chicago Journal of Theoretical Computer Science*, 1995.

[RA00] K. Reinhardt and E. Allender. Making nondeterminism unambiguous. *SIAM Journal on Computing*, 29:1118–1131, 2000.

[Sze88] R. Szelepcsényi. The method of forced enumeration for nondeterministic automata. *Acta Informatica*, 26(3):279–284, 1988.

[Tod91] 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.

[Val92] 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.

[Vin91] V Vinay. Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits. In *6th IEEE Conference on Structure in Complexity Theory*, pages 270–284, 1991.