

**Feasible Proofs of Matrix Identities
with Csanky's Algorithm**

CSL'05

Michael Soltys

McMaster University, Canada

What is the complexity of the concepts needed to prove theorems of matrix algebra?

For example:

- $AB = I \supset BA = I$
- The Cayley-Hamilton Theorem
(If $p_A(x) = \det(xI - A)$, then $p_A(A) = 0$)
- $\det(AB) = \det(A) \det(B)$
- Linear Independence
($n + 1$ vectors in \mathbb{F}^n must be *linearly dependent*)

Using **Gaussian Elimination** we can prove these principles in **PolyTime**:

$$\mathbf{S}_2^1, \mathbf{V}^1, \mathbf{PV}, \dots$$

with the elements of the underlying field \mathbb{F} properly encoded.

* * *

Aside: if $\mathbf{V}^1 \vdash \exists Y \alpha(X, Y)$, then $f(X) = Y$ is a *polytime* function, and if f is polytime, then there exists an $\alpha(X, Y)$ such that $\underline{\mathbb{N}}^2 \models \alpha(X, f(X))$, and $\mathbf{V}^1 \vdash \exists! Y \alpha(X, Y)$.

\mathbf{NC}^2 algorithms for computing the characteristic polynomial:

1. Berkowitz's algorithm
2. "Newton's Symmetric Polynomials" (Csanky's) algorithm
3. Chistov's algorithm

Can we use them to give \mathbf{NC}^2 proofs of matrix properties?

Berkowitz's algorithm is based on Samuelson's identity:

$$A = \left(\begin{array}{c|c} a & R \\ \hline S & M \end{array} \right)$$

$$p(x) = (x - a)q(x) - R \cdot \text{adj}(xI - M) \cdot S$$

p and q are the char polys of A and M , respectively, and

$$p = C_1 q$$

For example, if A is a 4×4 matrix, then $p = C_1 q$ is given by by:

$$\begin{pmatrix} p_4 \\ p_3 \\ p_2 \\ p_1 \\ p_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -a & 1 & 0 & 0 \\ -RS & -a & 1 & 0 \\ -RMS & -RS & -a & 1 \\ -RM^2S & -RMS & -RS & -a \end{pmatrix} \begin{pmatrix} q_3 \\ q_2 \\ q_1 \\ q_0 \end{pmatrix}$$

Berkowitz's algorithm consists in repeating this for q , etc., and obtaining p as a product of matrices:

$$p = C_1 C_2 \cdots C_n$$

$$\text{BERK}_A(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_0.$$

Csanky's algorithm works as follows:

$s_0 = 1$, and for $1 \leq k \leq n$,

$$s_k = \frac{1}{k} \sum_{i=1}^k (-1)^{i-1} s_{k-i} \operatorname{tr}(A^i)$$

So,

$$s_0 = 1$$

$$s_1 = \operatorname{tr}(A)$$

$$s_2 = \frac{1}{2} (s_1 \operatorname{tr}(A) - s_0 \operatorname{tr}(A^2))$$

$$s_3 = \frac{1}{3} (s_2 \operatorname{tr}(A) - s_1 \operatorname{tr}(A^2) + s_0 \operatorname{tr}(A^3))$$

$$\text{CSANKY}_A(x) = s_0 x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots \pm s_n x^0.$$

LA

- Equality axioms

$$x = x, x = y \supset y = x, \dots$$

- Axioms for indices

$$i + 1 \neq 0, i * (j + 1) = (i * j) + 1, \dots$$

- Field axioms

$$a + (-a) = 0, a * b = b * a, \dots$$

- Axioms for

- $\lambda ij \langle m, n, t \rangle$ operator for constructing matrices

- e.g., $A + B := \lambda ij \langle n, n, e(A, i, j) + e(B, i, j) \rangle$

- $\Sigma A =$ sum of entries in $A = a + \Sigma R + \Sigma S + \Sigma M$

- Rules for logical consequence, induction on open formulas (only bounded index quantification), equality rules.

LA proves ring properties of matrices (e.g., associativity of matrix multiplication), and can state, but *apparently* not prove:

- $AB = I \supset BA = I$
- $[AB = I \wedge AC = I] \supset B = C$
- $AB = I \supset [AC = 0 \supset C = 0]$
- $AB = I \supset A^t B^t = I$
- If a column of A is zero, then for any B , $AB \neq I$

However, **LA** can prove them equivalent.

Open Problem: Show independence of any of the above from **LA**.

LAP

Add matrix powering function P to **LA** with the axioms $P(0, A) = I$ and $P(n + 1, A) = P(n, A) * A$

BERK, CSANKY can be expressed as terms of **LAP**.

Open Problem: Can **LAP** prove the correctness of these algorithms?

QLA

Formulas with matrix quantifiers, and the axioms are all the theorems of **LA**.

Shows the equivalences of:

1. **The Cayley-Hamilton Theorem**

$$(\text{CSANKY}_A(A) = 0)$$

2. $(\exists B \neq 0)[AB = I \vee AB = 0]$

3. **Linear Independence**

$(n + 1$ vectors in \mathbb{F}^n must be linearly dependent)

4. **Weak Linear Independence**

$(n^k$ vectors $(n, k > 1)$ in \mathbb{F}^n must be linearly dependent)

5. **Every matrix has an annihilating polynomial**

Matrix powering can be expressed in **QLA** with $\text{POW}(A, n)$:

$$\exists B[B = \langle B_0 = I, B_1, \dots, B_n \rangle \wedge (\forall i \leq n)(i < n \supset B_{i+1} = B_i * A)]$$

And

$$\mathbf{QLA} \vdash (\exists B \neq 0)[CB = I \vee CB = 0] \supset \text{POW}(A, n)$$

But

$$\mathbf{QLA} \not\vdash \text{POW}(A, n)$$

Therefore **QLA** cannot prove $(\exists B \neq 0)[CB = I \vee CB = 0]$, and so it **cannot** prove linear independence.

QLA $\vdash (\exists B \neq 0)[CB = I \vee CB = 0] \supset \text{POW}(A, n)$

Use the reduction of matrix powering to matrix inverse^a.

Let N be an $n^2 \times n^2$ matrix consisting of $n \times n$ blocks which are all zero except for $n - 1$ copies of A above the diagonal of zero blocks.

Then, $N^n = 0$, and so $(I - N)^{-1} = I + N + N^2 + \dots + N^{n-1} =$

$$\begin{pmatrix} I & A & A^2 & \dots & A^{n-1} \\ 0 & I & A & \dots & A^{n-2} \\ & & & \vdots & \\ & & & & I \end{pmatrix}$$

^aStephen Cook, "A taxonomy of problems with fast parallel algorithms," Information and Computation, Vol. 64, 1985.

Set $C = I - N$.

Show that if $CB = 0$, then $B = 0$.

(By induction on the rows of B , starting at the bottom.)

Using $(\exists B \neq 0)[CB = I \vee CB = 0]$, conclude that there is a B such that $CB = I$.

It remains to show that $B = I + N + N^2 + \dots + N^{n-1}$.

(Again, by induction on the rows of B , starting at the bottom.)

B contains $I, A, A^2, \dots, A^{n-1}$ in its top rows.

POW(A, n) follows.

On the other hand, **QLA** *does not* prove $\text{POW}(A, n)$.

Over the field \mathbb{Z}_2 , **LA** translates into $\mathbf{AC}^0[2]$.

So, the “ B ” in $\text{POW}(A, n)$ could be witnessed with an $\mathbf{AC}^0[2]$ function, *if* $\mathbf{QLA} \vdash \text{POW}(A, n)$.

But that would mean that $\text{DET}(\mathbb{Z}_2) \subseteq \mathbf{AC}^0[2]$ — contradiction.

(Because, “bit counting” is not in $\mathbf{AC}^0[2]^a$, while it is in $\mathbf{L} \subseteq \mathbf{SL} \subseteq \text{DET}(\mathbb{Z}_2)^b$.)

^a $\text{Mod}(3)$ is \mathbf{AC}^0 reducible to MAJORITY, and by the result of Razborov-Smolensky $\mathbf{AC}^0[2]$ does not contain $\text{Mod}(3)$, so it follows that MAJORITY is not in $\mathbf{AC}^0[2]$.

^bE. Grädel, “Capturing Complexity Classes by Fragments of Second Order Logic,” *Theoretical Computer Science*, vol. 101, 1992.

$\exists\mathbf{LA}$

Allows induction over formulas with bounded existential matrix quantifiers.

P is definable in $\exists\mathbf{LA}$

$\exists\mathbf{LA}$ is a **PolyTime** theory

$\exists\mathbf{LA}$ can prove all the principles stated thus far.

Something better: let $\exists\mathbf{PLA}$ be the theory where induction is allowed only over formulas with

bounded existential *permutation* quantifiers

Then, $\exists\mathbf{PLA}$ still proves all these principles.

Conclusion

The Principle of Linear Independence is “all there is” to textbook Linear Algebra — proof complexity confirms this conceptual intuition.

LI cannot be shown trivially, i.e., in a simple theory such as **QLA**.

A host of principles of Linear Algebra are **QLA**-equivalent to LI.

LI can be shown with a PolyTime theory such as **∃LA**.

Open Question: Can LI be shown with an **NC²** theory, for example **LAP**?