A simple, polynomial-time algorithm for the matrix torsion problem

François Nicolas

September 8, 2009

Abstract

The Matrix Torsion Problem (MTP) is: given a square matrix $M$ with rational entries, decide whether two distinct powers of $M$ are equal. It has been shown by Cassaigne and the author that the MTP reduces to the Matrix Power Problem (MPP) in polynomial time [1]: given two square matrices $A$ and $B$ with rational entries, the MTP is to decide whether $B$ is a power of $A$. Since the MPP is decidable in polynomial time [3], it is also the case of the MTP. However, the algorithm for MPP is highly non-trivial. The aim of this note is to present a simple, direct, polynomial-time algorithm for the MTP.

1 Introduction

As usual $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{C}$ denote the semiring of non-negative integers, the field of rational numbers and the field of complex numbers, respectively.

Definition 1 (Torsion). Let $M$ be a square matrix over $\mathbb{C}$. We say that $M$ is torsion if it satisfies the following three equivalent assertions.

(i). There exist $p, q \in \mathbb{N}$ such that $p \neq q$ and $M^p = M^q$.

(ii). The multiplicative semigroup $\{M, M^2, M^3, M^4, \ldots\}$ has finite cardinality.

(iii). The sequence $(M, M^2, M^3, M^4, \ldots)$ is eventually periodic.

The aim of this note is to present a polynomial-time algorithm for the following decision problem:

Definition 2. The Matrix Torsion Problem (MTP) is: given as input a square matrix $M$ over $\mathbb{Q}$, decide whether $M$ is torsion.

For every square matrix $M$ over $\mathbb{Q}$, the size of $M$ is defined as the order of $M$ plus the sum of the lengths of the binary encodings over all entries of $M$. 

1
Previous work. The Matrix Power Problem (MPP) is: given two square matrices $A$ and $B$ over $\mathbb{Q}$ decide whether there exists $n \in \mathbb{N}$ such that such that $A^n = B$. Kannan and Lipton showed that the MPP is decidable in polynomial time \cite{3}. It is rather easy to prove that the MPP is decidable in polynomial time by reduction to the MPP (see Section 4). However, the original algorithm for the MPP is highly non-trivial. Hence, a simple, direct algorithm is still interesting.

2 Generalities

Throughout this paper, $z$ denotes an indeterminate. The next result is well-known and plays a crucial role in the paper.

Proposition 1 (Multiple root elimination). For every polynomial $\nu(z)$ over $\mathbb{C}$, the polynomial

$$\pi(z) := \frac{\nu(z)}{\gcd(\nu'(z), \nu(z))}$$

satisfies the following two properties:

- $\nu(z)$ and $\pi(z)$ have the same complex roots, and
- $\pi(z)$ has no multiple roots.

The set of all positive integers is denoted $\mathbb{N}^*$.

For every $n \in \mathbb{N}^*$, the $n$th cyclotomic polynomial is denoted $\gamma_n(z)$: $\gamma_n(z) = \prod(z - u)$ where the product is over all primitive $n$th roots of unity $u \in \mathbb{C}$. It is well-known that $\gamma_n(z)$ is a monic integer polynomial and that the following three properties hold \cite{4}:

Property 1. For every $m \in \mathbb{N}^*$, $z^m - 1 = \prod_{n \in D_m} \gamma_n(z)$, where $D_m$ denotes the set of all positive divisors of $m$.

Property 2. For every $n \in \mathbb{N}^*$, $\gamma_n(z)$ is irreducible over $\mathbb{Q}$.

Euler’s totient function is denoted $\phi$: for every $n \in \mathbb{N}^*$, $\phi(n)$ equals the number of $k \in \{1, 2, \ldots, n\}$ such that $\gcd(k, n) = 1$.

Property 3. For every $n \in \mathbb{N}^*$, $\gamma_n(z)$ is of degree $\phi(n)$.

The next lower bound for Euler’s totient function is far from optimal. However, it is sufficient for our purpose.

Proposition 2. For every $n \in \mathbb{N}^*$, $\phi(n)$ is greater than or equal to $\sqrt{n/2}$.

A proof of Proposition 2 can be found in appendix. Noteworthy is that $\frac{\phi(n) \ln \ln n}{n}$ converges to a positive, finite limit as $n$ tends to $\infty$. \cite{2}.
3 The new algorithm

Definition 3. For every \( n \in \mathbb{N}^* \), let \( \pi_n(z) := \prod_{j=1}^{n} \gamma_j(z) \).

To prove that the MTP is decidable in polynomial time, we prove that

- a \( d \)-by-\( d \) matrix over \( \mathbb{Q} \) is torsion if and only if it annihilates \( z^d \pi_{2d^2}(z) \), and that
- \( z^d \pi_{2d^2}(z) \) is computable from \( d \) in poly(\( d \)) time.

Proposition 3. Let \( d, n \in \mathbb{N}^* \) be such that for every integer \( m \) greater than \( n \), \( \phi(m) \) is greater than \( d \). For every \( d \)-by-\( d \) matrix \( M \) over \( \mathbb{Q} \) the following three assertions are equivalent.

(i). \( M \) is torsion.

(ii). \( M \) annihilates \( z^d \pi_n(z) \).

(iii). \( M \) satisfies \( M^{n!+d} = M^d \).

Proof. The implication \((iii) \implies (i)\) is clear. Moreover, it follows from Property [1] that \( \pi_n(z) \) divides \( z^{n!} - 1 \), and thus \( z^d \pi_n(z) \) divides \( z^{n!+d} - z^d \). Therefore, \((ii) \implies (iii)\) holds. Let us now show \((i) \implies (ii)\).

Assume that \( M \) is torsion. Let \( p, q \in \mathbb{N} \) be such that \( p < q \) and \( M^p = M^q \). Let \( \mu(z) \) denote the minimal polynomial of \( M \) over \( \mathbb{Q} \). Since \( M^q - M^p \) is a zero matrix, \( \mu(z) \) divides \( z^q - z^p \). By Property [1] \( z^q - z^p \) can be factorized in the form \( z^q - z^p = z^p \prod_{j \in D_{q-p}} \gamma_j(z) \); by Property [2] all factors are irreducible over \( \mathbb{Q} \). Hence, \( \mu(z) \) can be written in the form \( \mu(z) = z^k \prod_{j \in J} \gamma_j(z) \) for some integer \( k \) satisfying \( 0 \leq k \leq p \) and some \( J \subseteq D_{q-p} \). Besides, the Cayley-Hamilton theorem implies that \( \mu(z) \) divides the characteristic polynomial of \( M \) which is of degree \( d \). Therefore, \( d \) is not smaller than the degree of \( \mu(z) \). Since the degree of \( \mu(z) \) equals \( k + \sum_{j \in J} \phi(j) \) by Property [3] we have \( k \leq d \) and \( \max J \leq n \). Hence, \( \mu(z) \) divides \( z^d \pi_n(z) \).

Combining Propositions [2] and [3] we obtain that for every \( d \in \mathbb{N}^* \), a \( d \)-by-\( d \) matrix over \( \mathbb{Q} \) is torsion if and only if it annihilates the polynomial \( z^d \pi_{2d^2}(z) \). To conclude the paper, it remains to explain how to compute \( \pi_n(z) \) in poly(\( n \)) time from any \( n \in \mathbb{N}^* \) taken as input. The idea is to rely on Proposition [1]

Definition 4. For every \( n \in \mathbb{N}^* \), let \( \nu_n(z) := \prod_{j=1}^{n} (z^j - 1) \).

Let \( n \in \mathbb{N}^* \). Clearly, \( \nu_n(z) \) is computable in poly(\( n \)) time. Moreover, it follows from Property [1] that

\[
\nu_n(z) = \prod_{j=1}^{n} (\gamma_j(z))^{\lceil n/j \rceil},
\]
and thus \( \nu_n(z) \) and \( \pi_n(z) \) have the same roots. Since \( \pi_n(z) \) has no multiple roots, Proposition 1 yields a way to compute \( \pi_n(z) \) from \( \nu_n(z) \) in polynomial time:

**Proposition 4.** For every \( n \in \mathbb{N}^* \), \( \pi_n(z) := \frac{\nu_n(z)}{\gcd(\nu_n'(z), \nu_n(z))} \).

4 Comments

The failure of the naive approach. Combining Propositions 2 and 3, we obtain:

**Corollary 1** (Mandel and Simon [5, Lemma 4.1]). Let \( d \in \mathbb{N} \). Every \( d \)-by-\( d \) torsion matrix \( M \) over \( \mathbb{Q} \) satisfies \( M^{(2d^2)!+d} = M^d \).

It follows from Proposition 1 that the MTP is decidable. However, such an approach does not yield a polynomial-time algorithm for the MTP:

**Proposition 5.** Let \( t : \mathbb{N} \to \mathbb{N} \) be a function such that for each \( d \in \mathbb{N}^* \), every \( d \)-by-\( d \) torsion matrix \( M \) over \( \mathbb{Q} \) satisfies \( M^{t(d)+d} = M^d \). Then, \( t \) has exponential growth.

**Proof.** For every \( n \in \mathbb{N}^* \), let \( \ell(n) \) denote the least common multiple of all positive integers less than or equal to \( n \): \( \ell(3) = 6, \ell(4) = 12, \ell(5) = \ell(6) = 60, \) etc. It is well-known that \( \ell \) has exponential growth: for every \( n \in \mathbb{N}^* \), \( \ell(2n) \geq \ell(n) \geq 2^n \).

For every \( d \)-by-\( d \) non-singular matrix \( M \) over \( \mathbb{Q} \), \( M^{t(d)} \) is the identity matrix. Besides, for every integer \( k \) with \( 1 \leq k \leq d \), there exists a \( d \)-by-\( d \) permutation matrix that generates a cyclic group of order \( k \), and thus \( k \) divides \( t(d) \). It follows that \( \ell(d) \) divides \( t(d) \).

Reducing the MTP to the MPP. For the sake of completeness, let us describe the reduction from the MTP to the MPP. Let \( d \in \mathbb{N}^* \) and let \( M \) be a \( d \)-by-\( d \) matrix over \( \mathbb{Q} \). Let \( N_2 := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \), \( A := \begin{bmatrix} M^d & O \\ O & N_2 \end{bmatrix} \), \( O_2 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \) and \( B := \begin{bmatrix} M^d & O \\ O & O_2 \end{bmatrix} \) where \( O \) denotes both the \( d \)-by-two zero matrix and its transpose. It is clear that \( A \) and \( B \) are two \( (d+2) \)-by-\( (d+2) \) matrices over \( \mathbb{Q} \). Moreover, there exists \( n \in \mathbb{N} \) such that \( A^n = B \) if and only if \( M \) is torsion.

5 Open question

Let \( d \in \mathbb{N}^* \). It follows from Corollary 1 that for every \( d \)-by-\( d \) torsion matrix \( M \) over \( \mathbb{Q} \), the sequence \( (M^d, M^{d+1}, M^{d+2}, M^{d+3}, \ldots) \) is (purely) periodic with period at most \( (2d^2)! \). Hence, the maximum cardinality of \( \{M^d, M^{d+1}, M^{d+2}, M^{d+3}, \ldots\} \), over all \( d \)-by-\( d \) torsion matrices \( M \) over \( \mathbb{Q} \), is well-defined. To our knowledge, its asymptotic behavior as \( d \) goes to infinity is unknown.
References

[1] J. Cassaigne and F. Nicolas. On the decidability of semigroup freeness. Submitted, 2008.

[2] G. H. Hardy and E. M. Wright. An introduction to the theory of numbers. Oxford, at the Clarendon Press, fourth edition, 1979.

[3] R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. Journal of the Association for Computing Machinery, 33(4):808–821, 1986.

[4] S. Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, revised third edition, 2002.

[5] A. Mandel and I. Simon. On finite semigroups of matrices. Theoretical Computer Science, 5(2):101–111, 1977.

Proof of Proposition 2

The following two properties of Euler’s totient function are well-known.

Property 4. For every prime number $p$ and every $v \in \mathbb{N}^*$, $\phi(p^v) = p^v - 1 - (p-1)$.  

Proof. For every integer $k$, $\gcd(k, p^v)$ is distinct from one if and only if $p$ divides $k$. From that we deduce the equality

$$\left\{ k \in \{1, 2, \ldots, p^v\} : \gcd(k, p^v) \neq 1 \right\} = \left\{ pq : q \in \{1, 2, \ldots, p^{v-1}\} \right\}.$$  

Besides, it is easy to see that the left-hand side of Equation (1) has cardinality $p^v - \phi(p^v)$ while its right-hand side has cardinality $p^v - 1$.

Property 5. For every $m, n \in \mathbb{N}^*$, $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m, n) = 1$.

Property 5 is consequence of the Chinese remainder theorem. It states that $\phi$ is multiplicative.

Lemma 1. For every real number $x \geq 3$, $\sqrt{x}$ is less than $x - 1$.

Proof. The two roots of the quadratic polynomial $z^2 - z - 1$ are $\frac{1 + \sqrt{5}}{2} \approx 1.618$ and $\frac{1 - \sqrt{5}}{2} \approx -0.618$; they are both smaller than $\sqrt{3} \approx 1.732$. Therefore, $y^2 - y - 1$ is positive for every real number $y \geq \sqrt{3}$. Since for every real number $x \geq 3$, $\sqrt{x}$ is not less than $\sqrt{3}$, $(x - 1) - \sqrt{x} = (\sqrt{x})^2 - \sqrt{x} - 1$ is positive.

Lemma 2. Let $p$ and $v$ be two integers with $p \geq 2$ and $v \geq 1$. Inequality $p^{v/2} \leq p^{v-1}(p-1)$ holds if and only if $(p, v) \neq (2, 1)$. 

5
Proof. If \((p, v) = (2, 1)\) then \(p^{v/2} = \sqrt{2}\) is greater than \(1 = p^{v-1}(p-1)\). If \(v \geq 2\) then \(v/2 \leq v-1\), and thus \(p^{v/2} \leq p^{v-1}(p-1)\) follows. If \(v = 1\) and \(p \geq 3\) then \(p^{v/2} = \sqrt{p}\) is less than \(p-1 = p^{v-1}(p-1)\) according to Lemma 1.

**Lemma 3.** Let \(n \in \mathbb{N}^*\). If \(n\) is odd or if four divides \(n\) then \(\phi(n)\) is greater than or equal to \(\sqrt{n}\).

**Proof.** It is clear that \(\phi(1) = 1 = \sqrt{1}\). Let \(n\) be an integer greater than one. Write \(n\) in the form

\[
n = \prod_{i=1}^{r} p_i^{v_i}
\]

where \(r, v_1, v_2, \ldots, v_r\) are positive integers and where \(p_1, p_2, \ldots, p_r\) are pairwise distinct prime numbers. Properties 4 and 5 yield:

\[
\phi(n) = \prod_{i=1}^{r} \phi(p_i^{v_i}) = \prod_{i=1}^{r} p_i^{v_i-1}(p_i - 1).
\]

Assume either that \(n\) is odd or that four divides \(n\). Then, for each index \(i\) with \(1 \leq i \leq r\), \((p_i, v_i)\) is distinct from \((2, 1)\) and thus inequality \(p_i^{v_i/2} \leq p_i^{v_i-1}(p_i - 1)\) holds. From that we deduce

\[
\phi(n) \geq \prod_{i=1}^{r} p_i^{v_i/2} = \sqrt{n}.
\]

**Proof of Proposition 2.** If \(n\) is odd or if four divides \(n\) then Lemma 3 ensures \(\phi(n) \geq \sqrt{n} \geq \sqrt{n}/2\). Conversely, assume that \(n\) is even and that four does not divide \(n\): there exists an odd integer \(n'\) such that \(n = 2n'\). We have

- \(\phi(n) = \phi(2)\phi(n') = \phi(n')\) according to Property 5 and
- \(\phi(n') \geq \sqrt{n'} = \sqrt{n'/2}\) by Lemma 3.

From that we deduce \(\phi(n) \geq \sqrt{n'/2}\).