DECIDABILITY OF MULTIPLICATIVE MATRIX EQUATIONS

---

joint work with Sebastian Heintze and Armand Noubissie
Combinatorics and Number Theory 14-3 (2025), 251–270

A. Markov (1951): A Turing machine cannot decide if a matrix M belongs to a given semigroup of (6×6)-integer valued matrices (MEMBERSHIP PROBLEM)

K.A. Mihailova (1958): undecidability of membership problem for subgroups of $SL_4(\mathbb{Z})$

M.S. Paterson (1970): undecidability of membership problem for semigroups of (3×3)-integer valued matrices

OPEN PROBLEM: for subsemigroups of $SL_3(\mathbb{Z})$

I. Potapov and P. Semukhin (2017): semigroup membership problem is decidable in $GL_2(\mathbb{Z})$

OPEN PROBLEM: for subgroups of $GL_2(\mathbb{Q})$

KNAPSACK PROBLEM

Given $(n\times n)$-square matrices $A_1, \dots, A_s$ and A, do there exist positive integers $k_1, \dots, k_s$ such that

(1) $$A_1^{k_1} \cdot \ldots \cdot A_s^{k_s} = A.$$

Special case $A = 0$ (zero matrix) ... MORTALITY PROBLEM
Special case $A = I$ (identity) ... IDENTITY PROBLEM

Theorem. (Bell – Halava – Harju – Karhumäki – Potapov (2008))

The (knapsack)-mortality problem is undecidable for integer matrices of large n and s.

Idea of proof: Use formal power series (with coefficients in $\mathbb{Z}$):

$$S = \sum_{w \in A^*} (S,w)\, w \in \mathbb{Z}\langle\langle A \rangle\rangle$$

where $A = \{x_1, \dots, x_k\}$ is a finite alphabet and A^* the free monoid generated by A ("words"); (S,w) denotes the coefficients.

Natural concepts: addition, (Cauchy) product $(ST,w) = \sum_{uv=w} (S,u)(T,v)$, polynomials, external product $(kS,w) = k(S,w)$ for $k \in \mathbb{Z}$, star operation $S^* = \sum_{i \geq 0} S^i$, if the coefficient of the empty word is 0.

The above operations are called rational. A formal power series S is called $\mathbb{Z}$-rational if it is contained in the rational closure of the set of polynomials $\mathbb{Z}\langle A \rangle$.

Schützenberger 1961/62: a) Extension to formal power series over semirings K (e.g. Boolean algebras) instead of $\mathbb{Z}$

b) A formal power series S is recognizable (by a finite automaton or Turing machine) if it can be checked by a Turing machine whether $\exists w \in A^*$ with $(S,w) = 0$

c) S is K-recognizable $\Longleftrightarrow$ S is K-rational.

d) The Hadamard product $S \odot T = \sum_{w \in A^*} (S,w)(T,w)\, w$ of two K-rational power series is K-rational

Hilbert's 10^{th} problem There is no algorithm (Turing machine) solving any polynomial Diophantine equation $P(n_1, \dots, n_k) = 0$ (Matijasevic 1970)

•) Let $P(n_1, \dots, n_k)$ be integer polynomial. Take $A = \{x, y\}$, then $\mathbb{Z}$-rational power series can be constructed with

$$(S, w) = P(n_1, \dots, n_k)^2 \qquad \text{for } w = x^{n_1} y x^{n_2} y \dots y x^{n_k} \in A^*$$

and

$$(S, w) = 1 \qquad \text{for } w \text{ not of this form}$$

Construction is based on Hadamard product.

•) Thus $\exists w$ with $(S, w) = 0 \Leftrightarrow P(n_1, \dots, n_k) = 0$ has solution in natural numbers

•) Extension of construction to finite alphabets $A = \{x_1, \dots, x_k\}$.

•) Constructing matrices $A_1, \dots, A_s$ such that equation (1) with $A = 0$ (mortality problem) reduces to the equation $(S, w) = 0$ with S constructed above. ∎

OPEN PROBLEM : DECIDABILITY FOR SYMMETRIC MATRICES ?

Bell, Potapov and Semukhin (2021): The ABC-problem

$$(2) \qquad A^{k_1} B^{k_2} C^{k_3} = 0$$

for $n \times n$ matrices with entries from an algebraic number field is equivalent to the Skolem problem of order n.

Skolem problem: Is there an algorithm for deciding whether there is a j such that $u_j = 0$ for a linear recurrence sequence $(u_j)_{j=0}^{\infty}$ of order n?

Mignotte, Shorey and Tijdeman (1984): Skolem problem
Vereshchagin (1985)
is decidable for recurrences up to order 3 (over algebraic number fields) and up to $n \leq 4$ for real algebraic number fields.

$\rightsquigarrow$ Baker's effective method

COMMUTING MATRICES

Babai, Beals, Cai, Ivanyos and Luks (1996): The knapsack problem (1) for commuting matrices $A_1, \dots, A_s$ is decidable in polynomial time.

Aim of our work: Establish explicit bounds for the solutions $k_1, \dots, k_s$ to (1) in terms of heights $\mathcal{H}(A_j)$ (multiplicative height of the matrix A_j)

Theorem. Let $A_1, \dots, A_s$ be commuting, diagonizable matrices in $GL_n(\mathbb{K})$ ($\mathbb{K}$ alg. number field) of bounded height $\mathcal{H}(A_j) \ll H$, which satisfy

$$(3) \qquad A_1^{k_1} \cdots A_s^{k_s} = I_n \qquad \text{(identity problem)}$$

with $k_j \neq 0$. Then there exist exponents with $|k_j| \ll (\log H)^R$ $(j=1,\dots,s)$ for a positive integer $R < s$ such that (3) holds.

Tools: •) Commuting diagonizable matrices can be diagonalized with the same invertible transformation

•) Dirichlet's theorem for S-units

Theorem. Let A_1, A_2, A_3 be Heisenberg matrices of bounded height (over algebraic numbers), i.e.

$$A_i = \begin{pmatrix} 1 & a_i & c_i \\ 0 & 1 & b_i \\ 0 & 0 & 1 \end{pmatrix} \qquad (i=1,2,3)$$

and $\mathcal{H}(A_i) \ll H$. If there are non-zero integers k_1, k_2, k_3 satisfying

$$(4) \qquad A_1^{k_1} A_2^{k_2} A_3^{k_3} = I_3 ,$$

then there are exponents with $|k_i| \ll H^{58}$ $(i=1,2,3)$.

Main tool: general Siegel lemma. Let A be an $M \times N$ matrix (over number field $\mathbb{K}$) of rank R. Then there is a solution $\underline{x} \in \mathcal{O}_{\mathbb{K}}^N$ of $A\underline{x} = \underline{0}$ with

$$\mathcal{H}(\underline{x}) \leq |D_{\mathbb{K}/\mathbb{Q}}|^{\frac{1}{2d}} \left(\sqrt{N}\, \mathcal{H}(A)\right)^{\frac{R}{N-R}}$$

Remark.
- either $|k_1|, |k_2|, |k_3| \ll H^2$, or all solutions satisfy $|k_i| \ll H^{58}$.
- in case of only two factors in (4) we obtain the bound $|k_1|, |k_2| \ll H$.

$\rightsquigarrow$ Problems for symmetric matrices
(no semigroup structure)

<u>Theorem.</u> Let A_1, A_2, A_3 be symmetric (2×2) matrices with real algebraic number entries of bounded height $h(A_i) \leq H$.

[Here $h(U)$ denotes the logarithmic height of the set of entries of U ($= A_i$ for $i = 1,2,3$)]. Assume that the equation

$$(5) \qquad A_1^{k_1} A_2^{k_2} = A_3^{k_3}$$

has a solution in non-zero integers k_1, k_2, k_3. Then there is an effectively computable constant C and exponents $k_1, k_2, k_3 \leq C$ such that equation (5) holds.

$\Longrightarrow$ The knapsack-identity problem for 3 symmetric 2×2-matrices over real algebraic number fields is decidable.

<u>Tools:</u> •) diagonalization by orthogonal transformations:

$$T_i = \begin{pmatrix} a_i & b_i \\ -b_i & a_i \end{pmatrix} \quad \text{and} \quad A_i = T_i \begin{pmatrix} \lambda_i & 0 \\ 0 & \mu_i \end{pmatrix} T_i^{-1}$$

•) matrix computations, <u>case studies</u> and reduction two system of 4 equations of the form

$$\begin{array}{l} \lambda_1^{k_1} \lambda_2^{k_2} \\ \lambda_1 \; \mu_2 \\ \mu_1 \; \lambda_2 \\ \mu_1 \; \mu_2 \end{array} \mu_3^{-k_3} - c_1 \left(\frac{\lambda_3}{\mu_3}\right)^{k_3} = c_4$$

a) $\frac{\lambda_3}{\mu_3}$ <u>not a root of unity</u> $\Longrightarrow$ $k_3 \cdot h\left(\frac{\lambda_3}{\mu_3}\right) \leq C'$

Győry (2019)

$$\Longrightarrow k_3 \leq C'' = C''(H, \mathbb{K})$$

$\rightsquigarrow$ number field

- Thus for any of these finitely many values for k_3, the mentioned 4 equations imply that

$$\lambda_1^{k_1}\lambda_2^{k_2},\ \lambda_1^{k_1}\mu_2^{k_2},\ \mu_1^{k_1}\lambda_2^{k_2},\ \mu_1^{k_1}\mu_2^{k_2} \text{ all equal a constant.}$$

- Then apply Dirichlet's S-unit theorem and the following Lemma (Evertse-Győry, 2022):

Let $U \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$ and assume that $Uy = b$ is solvable in $\mathbb{Z}^n$. Then it has a solution $y \in \mathbb{Z}^n$ with

$$h(y) \leq m\,h([U,b]) + \frac{1}{2} m \log m .$$

- The cases when $\frac{\lambda_3}{\mu_3}$ is a root of unity or some of the involved constants $= 0$ are much simpler or can be reduced to a result contained in Mignotte-Shorey-Tijdeman (1984).

$\blacksquare$

$\rightsquigarrow$ A general bound for the number of solutions of matrix equations

Let A_1, A_2 be diagonizable $(\ell\times\ell)$-matrices with algebraic entries and let A_1, A_2 be commuting and their eigenvalues are non-zero and not roots of unity.
Let $\mathbb{K}$ be a number field containing all eigenvalues of A_1 and A_2 denoted by $\gamma_1, \dots, \gamma_\ell$ and $\beta_1, \dots, \beta_\ell$, resp. and let $c>1$ be a real number. Assume there is a place $|\cdot|$ of $\mathbb{K}$ such that $|\beta_i|, |\gamma_i| < 1$ holds for all $i \in \{1, \dots, \ell\}$ and let $\Gamma_{1,i} \cap \Gamma_{2,j} = \{1\}$, where $\Gamma_{1,i}$ and $\Gamma_{2,j}$ denote the groups generated by $\{\gamma_i\}$ and $\{\beta_j\}$, respectively (for all i, j). Fix a polynomial $f(X_1, X_2, Z) = Z^d + a_1 Z^{d-1} + \dots + a_d$,

where $a_i = a_i(X_1, X_2) \in \mathbb{K}[X_1, X_2]$ and $f(0,0,Z)$ has no double root. Let S be the set of places containing the archimedian ones as well as those above the eigenvalues of A_1 and A_2 and those above the roots of $f(0,0,Z)$. Let $\mathcal{D}$ be the set of diagonizable $(\ell\times\ell)$-matrices with algebraic entries which commute with A_1 and A_2 such that its eigenvalues belong to $\mathcal{O}_S$.

Consider the matrix equation

$$(6) \qquad f(A_1^n, A_2^m, Z) = 0 \qquad \text{with} \quad \max(n,m) \leq c \min(n,m)$$

in unknowns $(m,n) \in \mathbb{N}^2$ and $Z \in \mathcal{D}$. Then there exist only finitely many pairs of arithmetic progressions (in n and m) such that any solution (n,m) of (6) belongs to one of them and the eigenvalues of Z belong to the algebra generated by the eigenvalues of A_1 and A_2.

<u>Remark.</u> •) The solutions (n,m) are solutions of certain exponential Diophantine equations.

•) The result can be extended to k commuting diagonizable matrices $A_1, \dots, A_k$

•) 0 can be replaced on the right-hand side of (6) by any matrix B, which commutes with all A_i, provided that the solutions Z commute with B.

<u>Tools:</u> •) Lower bound for polynomials $f \in \mathbb{C}[z]$ of degree $n \geq 2$ with roots $\alpha_1, \dots, \alpha_n$ in terms of Mahler measure $M(f)$ and discriminant $D(f)$:

$$|f(z)| \geq \frac{|D(f)|^{1/2}}{n^{\frac{n-1}{2}}\, 2^{n-1}\, M(f)^{n-2}} \min_i \{|z - \alpha_i|\}$$

(Stewart 1991)

•) Let $\mathbb{K}$ be a number field, S a finite set of places of $\mathbb{K}$ containing the archimedian ones and $\mu \in S$.
Let $N \in \mathbb{N}$, $\varepsilon > 0$, $\sigma > \varepsilon(N+2)$ and $c_0, \dots, c_N \in \overline{\mathbb{K}}^*$.
Then there are only finitely many $(N+1)$-tuples $w = (w_0, \dots, w_N) \in (\mathbb{K}^*)^{N+1}$ such that

(i) $h_S(w_i) + h_S(w_i^{-1}) < \varepsilon h(w_i)$ for $i = 1, \dots, N$

(ii) $|c_0 w_0 + \dots + c_N w_N|_\mu < (H(w_0) H_S(w_0)^{N+1})^{-1} (\prod_{i=0}^{N} H(w_i))^{-\sigma}$

hold and no subsum of the $c_i w_i$ involving $c_0 w_0$ vanishes.

(Corvaja - Zannier (2002) using subspace theorem)
(Here, as usual H_S denotes the S-height and h_S the logarithmic S-height).

$\rightsquigarrow$ Counting results for multiplicatively dependent tuples

$\mathcal{D}_n(\mathbb{Z}, H)$ ... set of diagonizable $(n \times n)$-matrices A with integer entries, $\mathcal{H}(A) \ll H$ and $\det A \neq 0$.

$\mathcal{D}^*_{n,2}(\mathbb{Z}, H)$ ... set of multiplicatively dependent pairs of matrices from $\mathcal{D}_n(\mathbb{Z}, H)$ such that none of the components is a root of I_n.

Katznelson (1993): number of singular matrices with bounded entries $\ll H^{n^2-n} \log H$

$\Rightarrow \# \mathcal{D}_n(\mathbb{Z}, H) \gg H^{n^2}$

$\rightsquigarrow$ symmetric matrices : $\mathcal{S}_n(\mathbb{Z},H) \subseteq \mathcal{D}_n(\mathbb{Z},H)$

both components are symmetric $\mathcal{S}^*_{n,2}(\mathbb{Z},H) \subseteq \mathcal{D}^*_{n,2}(\mathbb{Z},H)$

Eskin-Katznelson (1995): number of singular symmetric matrices with bounded entries $\ll H^{\frac{n^2-n}{2}} \log H$

$\Rightarrow \# \mathcal{S}_n(\mathbb{Z},H) \gg H^{\frac{n^2+n}{2}}$

<u>Theorem</u>. $H^{\frac{n^2+n}{2}} \ll \# \mathcal{S}^*_{n,2}(\mathbb{Z},H) \ll H^{n^2} (\log H)^{2+n}$

<u>Tools:</u> •) refinement of S. Friedland (1972):

Let a_{ij} for $i,j \in \{1,\dots,n\}$ with $i \neq j$ as well as $\lambda_1,\dots,\lambda_n$ be given elements from an algebraically closed field $\mathbb{K}$. Then there exists an $(n\times n)$-matrix over $\mathbb{K}$ with eigenvalues $\lambda_1,\dots,\lambda_n$ and whose (i,j)-~~entry~~ is equal to a_{ij} for $i\neq j$; the number of such matrices is $\leqq n^{n^2}$.

•) general form of Siegel's lemma

$\blacksquare$

<u>Remark</u> This approach extends to algebraic number fields

$\rightsquigarrow$ s-tuples of symmetric and multiplicatively dependent matrices $\mathcal{S}^*_{n,s}(\mathbb{Z}, H)$ (of bounded height $\leq H$)

Theorem (n=2)

$$\left.\begin{array}{ll} s \text{ even} & H^{s+o(1)} \\ s \text{ odd} & H^{s-1} \end{array}\right\} \ll_s \# \mathcal{S}^*_{2,s}(\mathbb{Z}, H) \ll_s H^{2s+o(1)}$$

Tools:
- •) bound for the divisor function $\tau(m) \ll m^{o(1)}$;
- •) ideas from Habegger - Ostafe - Shparlinski (arxiv 2203.03880) for counting

They get much sharper results, also for general $\mathcal{O}_{\mathbb{Z}d}$ in case of arbitrary integer matrices —

However, the case of symmetric matrices is still open, even over $\mathbb{Z}$

$\rightsquigarrow$ extensions to number fields?

! THANK YOU !