Computer simulation of algorithms for solving the Unilateral Matrix Polynomial Problem: average-case complexity estimation

F. B. Burtyka[1] (Rostov-on-Don, Southern Federal University)
bbfilipp@yandex.ru

Unilateral (monic) matrix polynomial (UMP) of n-th order is an expression of the form

$$\mathcal{F}(X) = X^d + \mathbf{F}_{d-1} \cdot X^{d-1} + \cdots + \mathbf{F}_2 \cdot X^2 + \mathbf{F}_1 \cdot X + \mathbf{F}_0,$$

where $\mathbf{F}_i, i = 0, ..., d-1$ («coefficients») and X («variable») are $n \times n$ matrices.

In this work, the entries of all matrixes are from the arbitrary fixed prime finite field $\mathbb{F}_p$.

The solvent of $\mathcal{F}(X)$ is an $n \times n$ matrix $\mathbf{S}$, such that $\mathcal{F}(\mathbf{S}) = \mathbf{0}$, where $\mathbf{0}$ is zero n-th order matrix.

The (Decisional) Unilateral Matrix Polynomial Problem (DUMP Problem) is given UMP $\mathcal{F}(X)$ to decide whether it has at least one solvent.

The work studies three algorithms for finding solvents: two λ-matrix based and exhaustive search one.

The computational experiments investigated the behavior of the algorithms for samples of the problem with matrix dimensions 2..8, degrees 2..10 and basic fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$, and $\mathbb{F}_7$. In all cases we estimated the exact number of atomic operations needed to decide the sample of the problem.

The studies show that the number of atomic steps needed to solve the samples of the problem was exponential from matrix dimension and from the degree in average. This potentially makes the DUMP problem interesting for computer security because it's potentially hardness for quantum computers.

[1]The work is supported by Russian Ministry of Education and Science according to the project No. 2.6264.2017/8.9