Секция «Дискретная математика и математическая кибернетика»

Алгоритм поиска корней односторонних матричных полиномов над простыми конечными полями

Научный руководитель – Макаревич Олег Борисович

Буртыка Филипп Борисович

Выпускник (магистр)

Южный федеральный университет, Институт математики, механики и компьютерных наук им. И.И. Воровича, Ростов-на-Дону, Россия

E-mail: bbfilipp@ya.ru

Унитарный односторонний матричный полином (УОМП) n-го порядка степени d над полем $\mathbb{K}$ – это выражение вида:

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

$\in \mathsf{M}_n(\mathbb{F})[X]\mathrm{F}_i, X \in \mathsf{M}_n(\mathbb{K})$. *Корнем* одностороннего матричного полинома (1) называется такая матрица $\mathbf{S} \in \mathsf{M}_n(\mathbb{K})$, что $\mathcal{F}(\mathbf{S}) = \mathbf{0}$. Каждому одностороннему матричному полиному можно поставить в соответствие λ-матрицу $\mathcal{F}(\lambda)$ [1]. *Латентным корнем (л.к.)* $\mathcal{F}(\lambda)$ называется такое $\lambda_0 \in \mathbb{K}$ что $det(\mathcal{F}(\lambda_0)) = \mathbf{0}$.

В работах [1]-[3] предлагались алгоритмы нахождения корней УОМП для случая, когда полем $\mathbb{F}$ является поле комплексных чисел $\mathbb{C}$. Однако до сих пор не было рассмотрен случай, когда полем $\mathbb{F}$ является какое-то конечное поле. Алгоритмы из [1]-[3] существенно опираются на алгебраическую замкнутость поля $\mathbb{C}$, поэтому их обобщение на конечные поля нетривиально.

В данной работе предлагается алгоритм для поиска корней УОМП для случая, когда полем $\mathbb{F}$ является поле $\mathbb{F}_p$ вычетов по модулю простого числа p.

Основная идея алгоритма заключается в нахождении множества корней S_{ext} в некотором расширении поля $\mathbb{F}_p$, и затем построении на основе множества S_{ext} множества корней в исходном поле.

Дается оценка асимптотической сложности предложенного алгоритма как функции от размеров матриц, степени УОМП и числа p.

Источники и литература

1) Dennis, Jr J. E., Traub J. F., Weber R. P. Algorithms for solvents of matrix polynomials //SIAM Journal on Numerical Analysis. – 1978. – Т. 15. – №. 3. – С. 523-533.

2) Pereira E. On solvents of matrix polynomials //Applied numerical mathematics. – 2003. – Т. 47. – №. 2. – С. 197-208.

3) Wilson R. L. Polynomial equations over matrices //Rutgers University