Секция «Математическая логика, алгебра и теория чисел»

О количестве неразрешимых односторонних унитарных булевых матричных полиномов

Буртыка Филипп Борисович

Аспирант

Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Ростов-на-Дону, Россия

E-mail: bbfilipp@ya.ru

Обозначим как $\mathcal{B}_n$ множество булевых матриц размера $n \times n$. Односторонний (правый) унитарный булев матричный полином степени d от переменной $X \in \mathcal{B}_n$ – это выражение вида

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

где $\mathbf{F}_i \in \mathcal{B}_n$ – коэффициенты. Корень $\mathcal{F}(X)$ – матрица $\mathbf{K} \in \mathcal{B}_n$ такая, что $\mathcal{F}(\mathbf{K}) = \mathbf{0}$, где $\mathbf{0} \in \mathcal{B}_n$ – нулевая матрица. Если $\mathcal{F}(X)$ не имеет корней, то будем называть его *неразрешимым.*

Обозначим множество выражений вида (1) как $UR\mathcal{B}_n(X)$. Пусть $\mathcal{F}_1(X) = \sum_{i=0}^{d_1} \mathbf{F}_{1,i} \cdot X^i$, $\mathcal{F}_2(X) = \sum_{i=0}^{d_2} \mathbf{F}_{2,i} \cdot X^i \in UR\mathcal{B}_n(X)$. На множестве $UR\mathcal{B}_n(X)$ введем операцию умножения: $\mathcal{F}_1(X) \cdot \mathcal{F}_2(X) = \sum_{i=0}^{d_1+d_2} \mathbf{F}_{*,i} \cdot X^i$,
где $\mathbf{F}_{*,i} = \sum_{j+k=i} \mathbf{F}_{1,j} \cdot \mathbf{F}_{2,k}$. Вместе с этой операцией множество $UR\mathcal{B}_n(X)$ образует некоммутативный моноид. Данная операция будет использоваться для доказательства нижней оценки на количество неразрешимых полиномов заданной степени из $UR\mathcal{B}_2(X)$.
Как известно, для скалярного случая есть оценка количества неразрешимых полиномов над $\mathbb{F}_q$ [4] степени d, которая имеет вид $O(q^d)$.

Лемма 1. *Пусть $\mathcal{F}_1(X), \mathcal{F}_2(X) \in UR\mathcal{B}_n(X)$ имеют корни $\mathbf{K}_{\mathcal{F}_1}$ и $\mathbf{K}_{\mathcal{F}_2}$,(т.е. $\mathcal{F}_1(\mathbf{K}_{\mathcal{F}_1}) = \mathbf{0}$ и $\mathcal{F}_2(\mathbf{K}_{\mathcal{F}_2}) = \mathbf{0}$). Тогда для $\mathcal{F}_*(X) = \mathcal{F}_1(X) \cdot \mathcal{F}_2(X)$ обязательно $\mathcal{F}_*(\mathbf{K}_{\mathcal{F}_2}) = \mathbf{0}$, но в общем случае $\mathcal{F}_*(\mathbf{K}_{\mathcal{F}_1}) \neq \mathbf{0}$.*

Лемма 2. *Пусть $\mathcal{F}_1(X), \mathcal{F}_2(X) \in UR\mathcal{B}_2(X)$ неразрешимы. В общем случае $\mathcal{F}_*(X) = \mathcal{F}_1(X) \cdot \mathcal{F}_2(X)$ может оказаться разрешимым.*

Определение 1. $\mathcal{F}(X) \in UR\mathcal{B}_2(X)$ будем называть *строго неразрешимыми*, если для $\forall t \in \mathbb{N}$ полином $(\mathcal{F}(X))^t$ неразрешим.

Лемма 3. *Полиномы* $X^2+\begin{pmatrix}1&1\\1&0\end{pmatrix}\cdot X+\begin{pmatrix}1&1\\1&0\end{pmatrix}$, $X^2+\begin{pmatrix}1&1\\1&0\end{pmatrix}\cdot X+\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $X^2+X+\begin{pmatrix}1&1\\1&0\end{pmatrix}$, $X^2+X+\begin{pmatrix}0&1\\1&1\end{pmatrix}$, $X^2+\begin{pmatrix}0&1\\1&1\end{pmatrix}\cdot X+\begin{pmatrix}0&1\\1&1\end{pmatrix}$, $X^2+\begin{pmatrix}0&1\\1&1\end{pmatrix}\cdot X+\begin{pmatrix}0&1\\1&1\end{pmatrix}$ *строго неразрешимы.*

Лемма 4. *Пусть $\mathcal{F}_1(X), \mathcal{F}_2(X) \in UR\mathcal{B}_2(X)$ – строго неразрешимы, все матрицы-коэффициент их обратимы и $deg(\mathcal{F}_1(X)) = 2$. Тогда произведение $\mathcal{F}_1(X) \cdot \mathcal{F}_2(X)$ – строго неразрешим.*

На основании этих лемм получена следующая теорема, дающая нижнюю оценку числа неразрешимых односторонних матричных полиномов для размерности матриц $n = 2$.

Теорема 1. *Количество неразрешимых унитарных односторонних булевых матричных полиномов степени d при $n = 2$ не менее $6^{d/2}$.*

Источники и литература

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

2) Dennis ,Jr J. E. et al, Algorithms for solvents of matrix polynomials //SIAM Journal on Numerical Analysis. – 1978. – Т. 15. – №. 3. – С. 523-533.

3) Буртыка,Ф.,Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов //Известия Южного федерального университета. Технические науки. – 2014. – №. 8.

4) Lidl,R. et al, Finite fields. – Cambridge university press, 1997. – Т. 20.

Слова благодарности

Работа поддержана грантом РФФИ 16-37-00125 мол-а