ДИАГОНАЛИЗУЕМЫЕ КОРНИ МАТРИЧНЫХ ПОЛИНОМОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Ф.Б. Буртыка

Южный федеральный университет, Большая Садовая 105/42, 344006 Ростов-на-Дону, Россия
bbfilipp@ya.ru

Рассмотрим матричные полиномы следующего вида:

$$\mathcal{F}(X) = \mathbf{F}_d \cdot X^d + \mathbf{F}_{d-1} \cdot X^{d-1} + \cdots + \mathbf{F}_2 \cdot X^2 + \mathbf{F}_1 \cdot X + \mathbf{F}_0 \in \mathbb{Z}_p^{N \times N}[X], \quad (1)$$

где $\mathbf{F}_i \in \mathbb{Z}_p^{N \times N}$ – коэффициенты и $X \in \mathbb{Z}_p^{N \times N}$ – переменная, являющиеся матрицами, состоящими из элементов кольца вычетов $\mathbb{Z}_p$ по модулю простого числа p, $p > 2$. Корнем (1) называется матрица $\mathbf{S} \in \mathbb{Z}_p^{N \times N}$ такая, что $\mathcal{F}(\mathbf{S}) = \mathbf{0}$, где $\mathbf{0} \in \mathbb{Z}_p^{N \times N}$ – нулевая матрица. Нахождение корней матричных полиномов $\in \mathbb{Z}_p^{N \times N}[X]$ имеет приложения в криптографии, например, анализ криптостойкости ПГШ на матричных полиномах [1-3] или отыскание периодов полилинейных рекуррентных регистров сдвига [4].

Для поиска корней (1) можно, к примеру, *свести его к системе скалярных алгебраических уравнений* над $\mathbb{Z}_p$. Данный метод был рассмотрен в [5] на примере матричных полиномов над $\mathbb{Z}_2$, однако он является неэффективным, так как система скалярных уравнений имеет большие размеры и является труднорешаемой.

Другой метод поиска корней (1) основан на работе с *полиномиальными матрицами*. С его помощью можно найти все корни, являющиеся диагонализируемыми матрицами. Данный метод был рассмотрен в [6,7] для матричных полиномов над полем комплексных чисел $\mathbb{C}$. В данной работе рассматривается вопрос о его переносимости на случай $\mathbb{Z}_p$. Напомним некоторые необходимые определения из [6].

Определение 1. Диагонализируемыми корнями (1) называются корни $\mathbf{S} \in \mathbb{Z}_p^{N \times N}$, представимые в виде $\mathbf{S} = \mathbf{V} \cdot \mathbf{D} \cdot \mathbf{V}^{-1}$, где $\mathbf{V} \in \mathbb{Z}_p^{N \times N}$ – обратимая матрица, $\mathbf{D} \in \mathbb{Z}_p^{N \times N}$ – диагональная матрица.

Определение 2. Полиномиальной матрицей, соответствующей матричному полиному (1), называется $\mathcal{F}(x) = \mathbf{F}_d \cdot x^d + \mathbf{F}_{d-1} \cdot x^{d-1} + \cdots + \mathbf{F}_2 \cdot x^2 + \mathbf{F}_1 \cdot x + \mathbf{F}_0 \in \mathbb{Z}_p^{N \times N}[x]$, где $\mathbf{F}_i \in \mathbb{Z}_p^{N \times N}$ – коэффициенты, $x \in \mathbb{Z}_p$ – скалярная переменная (т.е. в полиномиальной матрице элемент с индексами i, j – это полином, коэффициенты которого взяты из i, j-х элементов матриц-коэффициентов матричного полинома при соответствующих степенях).

Определение 3. Латентным корнем $\mathcal{F}(x) \in \mathbb{Z}_p^{N \times N}[x]$ называется такое $\lambda \in \mathbb{Z}_p$, что $det(\mathcal{F}(\lambda)) = 0$, где $d(x) = det(\mathcal{F}(x)) \in \mathbb{Z}_p[x]$ – скалярный полином степени $d \cdot N$.

Определение 4. Латентным вектором, соответствующим латентному корню $\lambda \in \mathbb{Z}_p$ полиномиальной матрицы $\mathcal{F}(x)$, называется вектор $\vec{v} \in Ker(\mathcal{F}(\lambda))$.

Теорема 1. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N \times N}[x]$ имеет латентные корни $\lambda_1, ..., \lambda_N \in \mathbb{Z}_p$, такие что для $\forall \lambda_i, i \in \overline{1, N}$ существуют латентные векторы $\vec{v_i} \in \mathbb{Z}_p^N$, образующие линейно независимую систему векторов $\{\vec{v}_1, ..., \vec{v}_N\}$. Тогда*

$$\mathbf{S} = \mathbf{V} \cdot diag(\lambda_1, ..., \lambda_N) \cdot \mathbf{V}^{-1} \in \mathbb{Z}_p^{N \times N} \quad (2)$$

является корнем матричного полинома $\mathcal{F}(X) \in \mathbb{Z}_p^{N \times N}[X]$, где $\mathbf{V} \in \mathbb{Z}_p^{N \times N}$ — матрица, i -й столбец которой равен $\vec{v}_i$, $diag(\lambda_1, ..., \lambda_N)$ – диагональная матрица со значениями λ_i на диагонали.

Теорема 1 была доказана в [6] для поля комплексных чисел $\mathbb{C}$. Однако легко проверить, что она выполняется и для $\mathbb{Z}_p$. Действительно, она просто следует из того, что все собственные числа и векторы любого корня $\mathbf{S} \in \mathbb{Z}_p^{N \times N}$ полинома $\mathcal{F}(X) \in \mathbb{Z}_p^{N \times N}[X]$ являются латентными корнями и векторами соответственно для $\mathcal{F}(x)$.

Данная теорема дает алгоритм поиска всех диагонализируемых корней $\mathcal{F}(X)$. Сначала необходимо найти все корни $\lambda_1, ..., \lambda_t$ скалярного полинома $det(\mathcal{F}(x)) \in \mathbb{Z}_p[x]$, затем для $\forall i \in \overline{1,t}$ вычисляется $Ker(\mathcal{F}(\lambda_i))$. Из векторов $\in Ker(\mathcal{F}(\lambda_i))$ и λ_i строятся различные комбинации в соответствии с формулой (2) и получаются, соответственно, различные корни (1).

Рассмотрим вопрос о количестве диагонализируемых корней.

Теорема 2. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ с $deg(\mathcal{F}) = d$ имеет t латентных корней $\lambda_1, ..., \lambda_t$ таких, что $\lambda_i \neq \lambda_j$ для $i \neq j$, $N \leq t \leq N \cdot d$. И пусть $\forall \lambda_i$ соответствует одномерное подпространство латентных векторов $V_i = Lin\{\vec{v}_i\}$. Тогда количество диагонализируемых корней $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$ не превосходит $C_{d\cdot N}^N$.*

Теорема 3. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ с $deg(\mathcal{F}) = d$ имеет латентные корни $\lambda_1, ..., \lambda_{d\cdot N}$ такие, что $\lambda_i \neq \lambda_j$ для $i \neq j$. И пусть $\forall \lambda_i$ соответствует одномерное подпространство латентных векторов $V_i = Lin\{\vec{v}_i\}$ таких, что любой набор векторов $\{\vec{v}_{i_1}, ..., \vec{v}_{i_N}\}$ является линейно независимым. Тогда все корни $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$ являются диагонализируемыми, и их количество $= C_{d\cdot N}^N$. Других корней (1) не имеет.*

Матричные полиномы $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$, для которых выполнено условие из теоремы 3, – это, так называемые, *полиномы общего положения* [7]. Они имеют *только* диагонализируемые решения. Матричные полиномы же, не находящиеся в случае общего положения, могут иметь недиагонализируемые решения, которые необходимо искать отдельно.

Отметим, что в [6-7] утверждения теорем 2 и 3 обосновывались для случая поля $\mathbb{C}$. В данной работе установлено, что они также справедливы и для $\mathbb{Z}_p$.

Установлена также следующая теорема.

Теорема 4. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ имеет латентные корни $\lambda_1, ..., \lambda_N$, где $\lambda_i \neq \lambda_j$. И пусть $\exists \lambda_j$ с k-мерным подпространством латентных векторов $\mathtt{V}_j = Lin\{\vec{v}_{j,1}, ..., \vec{v}_{j,k}\}$. А остальным $\lambda_i, i \neq j$ пусть соответствуют одномерные подпространства латентных векторов $\mathtt{V}_i = Lin\{\vec{v}_i\}$. И пусть выполняется $\mathtt{V}_j \cap Lin\{\vec{v}_1, ..., \vec{v}_{j-1}, \vec{v}_{j+1}..., \vec{v}_N\} = \emptyset$. Тогда количество диагонализируемых корней (1) $< p^k - k \cdot (p-1)$.*

Заметим, что в случае поля $\mathbb{C}$ матричный полином, удовлетворяющий условиям теоремы 4, будет иметь бесконечное число корней.

Работа выполнена при финансовой поддержке гранта РФФИ №15-07-00597 А.

Литература

1. Буртыка Ф. Б. *Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов.* // Известия Южного федерального университета. Технические науки, 2014. Т. 157. № 8. С. 107–122.

2. Burtyka Ph. B., Makarevich O. B. *Symmetric fully homomorphic encryption using decidable matrix equations.* // Proceedings of the 7th International Conference on Security of Information and Networks, ACM, 2014. P. 186–197.

3. Буртыка Ф. Б. *Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов.* // Труды Института системного программирования РАН. 2014. Т. 26. № 5. С. 99-115.

4. Гольтваница М. А., Зайцев С. Н., Нечаев А. А. *Скрученные линейные рекурренты максимального периода над кольцами Галуа* //Фундаментальная и прикладная математика. 2012. Т. 17. № 3. С. 5–23.

5. Буртыка Ф. Б. *О сложности нахождения корней булевых матричных полиномов* // Математическое моделирование. 2015. Т. 27.

6. Dennis, Jr J. E., Traub J. F., Weber R. P. *The algebraic theory of matrix polynomials* //SIAM Journal on Numerical Analysis. 1976. Т. 13. № 6. С. 831–845.

7. Гельфанд С. И. *О числе решений квадратного уравнения* // Общематематический семинар Глобус. Выпуск 1. НМУ. МЦНМО. 2004. С. 124–133.