СЛОЖНОСТЬ НАХОЖДЕНИЯ КОРНЕЙ БУЛЕВЫХ МАТРИЧНЫХ ПОЛИНОМОВ

Ф.Б.Буртыка

Южный федеральный университет,
Институт компьютерных технологий и информационной безопасности

27 августа 2014 г.

Содержание

Матричные уравнения и матричные полиномы специального вида

$$\mathbf{F}_n \cdot X^n + \mathbf{F}_{n-1} \cdot X^{n-1} + \cdots + \mathbf{F}_2 \cdot X^2 + \mathbf{F}_1 \cdot X + \mathbf{F}_0,$$

$$\mathbf{F}_i = \begin{pmatrix} (f_i)_{11} & (f_i)_{12} & \cdots & (f_i)_{1N} \\ (f_i)_{21} & (f_i)_{22} & \cdots & (f_i)_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ (f_i)_{N1} & (f_i)_{N2} & \cdots & (f_i)_{NN} \end{pmatrix}, \; X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1N} \\ x_{21} & x_{22} & \cdots & x_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N1} & x_{N2} & \cdots & x_{NN} \end{pmatrix}$$

Пример с матрицами 2×2

$$\begin{pmatrix} (f_2)_{00} & (f_2)_{01} \\ (f_2)_{10} & (f_2)_{11} \end{pmatrix} \cdot X^2 + \begin{pmatrix} (f_1)_{00} & (f_1)_{01} \\ (f_1)_{10} & (f_1)_{11} \end{pmatrix} \cdot X + \begin{pmatrix} (f_0)_{00} & (f_0)_{01} \\ (f_0)_{10} & (f_0)_{11} \end{pmatrix} = \mathbf{0}$$

$$X = \begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix}$$

Приложения

- Криптоанализ ПГШ. Взлом криптографической схемы полностью гомоморфного шифрования на основе матричных полиномов эквивалентен решению системы матричных алгебраических уравнений.
- Построения моделей и анализ поведения дискретных динамических систем.
- Проверка интегрируемости систем.
- Моделирование электронных схем.

Способы явного выражения корней матричного полинома

1. Теорема Виета для матричных полиномов (Д. Б. Фукс и А.С. Шварц, 1994).
2. Сведение к матрице, элементы которой – полиномы (Б. З. Шаваровский, 2007)

Сколько решений у квадратного уравнения?

$$a \cdot x^2 + b \cdot x + c = 0$$

Если все элементы – квадратные матрицы, то от нуля до $C^n_{2 \cdot n}$, где n – размер матриц

Корни булевых матричных полиномов

Простейший пример неприводимого матричного полинома –

$$X^2 - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Соответствующее матричное уравнение

$$X^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

не имеет решений, поскольку на роль X подходит только матрица, имеющая только нулевые собственные значения (если квадрат матрицы имеет только нулевые собственные значения, то и она сама имеет только нулевые собственные значения), т.е. идемпотентная матрица, но квадрат любой идемпотентной 2×2 матрицы равен нулевой матрице.

Квадратичное уравнение без линейного члена

Рассмотрим простейшее квадратное булево матричное уравнение вида

$$X^2 = \begin{pmatrix} c_0 & c_1 \\ c_2 & c_3 \end{pmatrix}$$

Каковы его решения при разных константах?

Квадратичное уравнение без линейного члена

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}^2=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}0&1\\0&0\end{pmatrix}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix},\ \begin{pmatrix}0&1\\0&1\end{pmatrix}^2=\begin{pmatrix}0&1\\0&1\end{pmatrix}$$
$$\begin{pmatrix}1&0\\1&0\end{pmatrix}^2=\begin{pmatrix}1&0\\1&0\end{pmatrix},\ \begin{pmatrix}0&0\\1&1\end{pmatrix}^2=\begin{pmatrix}0&0\\1&1\end{pmatrix},\ \begin{pmatrix}1&1\\0&0\end{pmatrix}^2=\begin{pmatrix}1&1\\0&0\end{pmatrix}$$
$$\begin{pmatrix}1&1\\0&1\end{pmatrix}^2=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}1&1\\1&0\end{pmatrix}^2=\begin{pmatrix}0&1\\1&1\end{pmatrix},\ \begin{pmatrix}0&1\\1&1\end{pmatrix}^2=\begin{pmatrix}1&1\\1&0\end{pmatrix}$$
$$\begin{pmatrix}0&0\\0&1\end{pmatrix}^2=\begin{pmatrix}0&0\\0&1\end{pmatrix},\ \begin{pmatrix}1&0\\0&1\end{pmatrix}^2=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}1&0\\1&1\end{pmatrix}^2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$
$$\begin{pmatrix}1&1\\1&1\end{pmatrix}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix},\ \begin{pmatrix}1&0\\0&0\end{pmatrix}^2=\begin{pmatrix}1&0\\0&0\end{pmatrix},\ \begin{pmatrix}0&0\\1&0\end{pmatrix}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

Элементы степеней матрицы X

Рассмотрим матрицу $X = \{x_{i,j}\}_{i,j=1}^{N}$, её умножение саму на себя дает

$$X^2 = \{\sum_{k_1=1}^{N} (x_{i,k_1} \cdot x_{k_1,j})\}_{i,j=1}^{N},$$

$$X^3 = \{\sum_{k_1=1}^{N} x_{i,k_1} \sum_{k_2=1}^{N} (x_{k_1,k_2} \cdot x_{k_2,j})\}_{i,j=1}^{N}$$

...

$$X^n = \{\sum_{k_1=1}^{N} x_{i,k_1} \sum_{k_2=1}^{N} x_{k_1,k_2} \cdot \ldots \cdot \sum_{k_{n-1}=1}^{N} (x_{k_{n-2},k_{n-1}} \cdot x_{k_{n-1},j})\}_{i,j=1}^{N},$$

где $x_{i,j} \in \mathbb{Z}_p$.

Сведение к системе булевых алгебраических уравнений

Обозначим элементы неизвестной матрицы X в степени n через

$$(X^n)_{ij} = \sum_{k_1,\ldots,k_{n-1}} x_{i,k_1} \cdot x_{k_1,k_2} \cdot \ldots \cdot x_{k_{n-2},k_{n-1}} \cdot x_{k_{n-1},j} \ ,$$

где $k_i = 1, ..., N$, а через $F_t = \{(f_t)_{i,j}\}_{i,j=1}^{N}$, $(f_t)_{i,j} \in \mathbb{Z}_p$ обозначим коэффициенты матричного полинома.
Покоординатно получим систему полиномов следующего вида:

$$\sum_{n=1}^{d} \sum_{k=0}^{N} (f_n)_{i,k} \cdot (X^n)_{kj} + (f_0)_{i,j} \equiv 0 \pmod{p}$$

для каждого $i, j = 1, ..., N$. Таким образом, количество уравнений в этой системе – N^2 при общем числе различных мономов более чем $1 + N + N^2 + ... + N^{n-1}$.

Пример

$$\begin{pmatrix} (f_2)_{00} & (f_2)_{01} \\ (f_2)_{10} & (f_2)_{11} \end{pmatrix} \cdot X^2 + \begin{pmatrix} (f_1)_{00} & (f_1)_{01} \\ (f_1)_{10} & (f_1)_{11} \end{pmatrix} \cdot X + \begin{pmatrix} (f_0)_{00} & (f_0)_{01} \\ (f_0)_{10} & (f_0)_{11} \end{pmatrix},$$

где

$$X = \begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix},$$

$$X^2 = \begin{pmatrix} x_{00}x_{00} + x_{01}x_{10} & x_{00}x_{01} + x_{01}x_{11} \\ x_{10}x_{00} + x_{11}x_{10} & x_{10}x_{01} + x_{11}x_{11} \end{pmatrix}$$

Пример

$$\begin{cases} (f_2)_{00}(x_{00}x_{00} + x_{01}x_{10}) + (f_2)_{01}(x_{10}x_{00} + x_{11}x_{10}) + \\ \qquad + (f_1)_{00} \cdot x_{00} + (f_1)_{01} \cdot x_{10} + (f_0)_{00} = 0 \\ \\ (f_2)_{10}(x_{00}x_{00} + x_{01}x_{10}) + (f_2)_{11}(x_{10}x_{00} + x_{11}x_{10}) + \\ \qquad + (f_1)_{10} \cdot x_{00} + (f_1)_{11} \cdot x_{10} + (f_0)_{10} = 0 \\ \\ (f_2)_{00}(x_{00}x_{01} + x_{01}x_{11}) + (f_2)_{01}(x_{10}x_{01} + x_{11}x_{11}) + \\ \qquad + (f_1)_{00} \cdot x_{01} + (f_1)_{01} \cdot x_{11} + (f_0)_{01} = 0 \\ \\ (f_2)_{10}(x_{00}x_{01} + x_{01}x_{11}) + (f_2)_{11}(x_{10}x_{01} + x_{11}x_{11}) + \\ \qquad + (f_1)_{10} \cdot x_{01} + (f_1)_{11} \cdot x_{11} + (f_0)_{11} = 0 \end{cases}$$

Матричное уравнение первой степени

Нахождению корней приведённого матричного полинома первой степени (для матриц 2×2)

$$X + \begin{pmatrix} c_0 & c_1 \\ c_2 & c_3 \end{pmatrix} = \mathbf{0}$$

соответствует нахождению решений полинома Жегалкина

$$(x_0 \oplus c_0) \vee (x_1 \oplus c_1) \vee (x_2 \oplus c_2) \vee (x_3 \oplus c_3) = 0$$

пользуясь формулой $A \vee B = A \oplus B \oplus A \cdot B$ получим

$$x_0x_1x_2x_3 + x_0x_1x_2(1+c_3) + x_0x_1x_3(1+c_2) + x_0x_2x_3(1+c_1) + x_1x_2x_3(1+c_0) +$$

$$+ x_0x_1(c_2c_3 + c_2 + c_3 + 1) + x_2x_3(c_0c_1 + c_1 + c_0 + 1) + x_1x_3(1+c_0)(1+c_2) +$$

$$+ x_0x_2(1 + c_3) + x_1x_2(1 + c_0)(1 + c_3) + x_1(1 + c_0)(c_2c_3 + c_2 + c_3) +$$

$$+ x_2(1 + c_3)(c_0c_1 + c_0 + c_1) + (c_0c_1 + c_0 + c_1)(c_2c_3 + c_2 + c_3) = 0$$

Матричное уравнение второй степени

Нахождение корней приведённого матричного полинома второй степени

$$X^2 + \begin{pmatrix} c_4 & c_5 \\ c_6 & c_7 \end{pmatrix} \cdot X + \begin{pmatrix} c_0 & c_1 \\ c_2 & c_3 \end{pmatrix} = \mathbf{0}$$

соответствует нахождению решений полинома Жегалкина

$$(x_0 + x_1x_2 + c_4x_0 + c_5x_2 + c_0) \vee (x_0x_1 + x_1x_3 + c_4x_1 + c_5x_3 + c_1) \vee$$

$$\vee (x_2x_0 + x_3x_2 + c_6x_0 + c_7x_2 + c_2) \vee (x_1x_2 + x_3 + c_6x_1 + c_7x_3) = 0$$

Эксперименты по сложности нахождения корней с помощью базисов Грёбнера (SINGULAR)

Таблица: Время работы алгоритмов в зависимости от размерности матриц N и степени матричного полинома deg

	$N = 4$	$N = 5$	$N = 6$
deg=3	4 мин	>48 часов	>8 дней
deg=4	8 ч	-	-
deg=5	33 ч	-	-

Заключение

Была поставлена задача определения корней булева матричного полинома. Был предложен универсальный способ – сведение к системе булевых алгебраических уравнений и к задаче «ВЫПОЛНИМОСТЬ». Было исследовано, какое может быть количество корней у булева матричного полинома. Для оценки практической сложности нахождения корней булева матричного полинома были проведены эксперименты, свидетельствующие о том, что в общем случае вычислительная сложность задачи сравнима с задачей факторизации или дискретного логарифмирования в конечных полях.