Модел. и анализ информ. систем. Т. **21**, № **2** (2014) 39–49

УДК 512.643.8

Быстрое умножение матрицы с большим мультипликативным порядком на вектор над конечным полем

Иванов Д. М.

Ярославский государственный университет им. П. Г. Демидова
150000 Россия, г. Ярославль, ул. Советская, 14

e-mail: dmitrii347@gmail.com

получена 3 февраля 2014

Ключевые слова: умножение матрицы на вектор, рекуррентные последовательности

Рассмотрим линейную рекуррентную последовательность векторов $\{\vec{v}_k\}_{k\geq 0}$ длины n с элементами из $\mathbb{F}_q$, для которой верно соотношение

$$\forall k \in \mathbb{N} \quad \vec{v}_{k+1} = Y\vec{v}_k,$$

где Y — это $n \times n$-матрица из $GL_n(q)$. Период этой последовательности будет равен мультипликативному порядку матрицы Y, максимально возможным значением которого будет $q^n - 1$ [3, с. 363].

В статье решается задача построения матрицы Y с большим мультипликативным порядком, которая позволяла бы вычислять элементы последовательности за меньшее количество арифметических операций, чем стандартное умножение матрицы на вектор, и при этом порождала бы последовательности с большим периодом.

Главное утверждение статьи звучит следующим образом. Пусть $n = st$, $1 < s, t < n$. Тогда существуют $s \times s$-матрицы $A_1, A_2, \ldots, A_s$ и $t \times t$-матрицы $B_1, B_2, \ldots, B_s$ над полем $\mathbb{F}_q$ такие, что матрица $Y = \sum_{i=1}^{s} A_i \otimes B_i$ из $GL_n(q)$ имеет мультипликативный порядок $\frac{q^n-1}{(s,q^t-1)}$.

1. Введение

Рассмотрим линейную рекуррентную последовательность $\{u_k\}_{k\geq 0}$ элементов из поля $\mathbb{F}_q$, которая удовлетворяет соотношению

$$\forall k \in \mathbb{N}_0 \quad u_{k+n} = a_0u_k + a_1u_{k+1} + \cdots + a_{n-1}u_{k+n-1}.$$

Будем обозначать через $\vec{u}_{k+n} = (u_k, u_{k+1}, \ldots, u_{k+n-1})^T$ вектор длины n, составленный из последовательных элементов $\{u_k\}_{k\geq 0}$. $n \times n$-матрицу следующего вида:

$$A = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{n-1} \end{pmatrix}$$

называют **сопровождающей матрицей рекуррентной последовательности**, она обладает следующим свойством:

$$A\vec{u}_{k+n} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{n-1} \end{pmatrix} \begin{pmatrix} u_k \\ u_{k+1} \\ \vdots \\ u_{k+n-1} \end{pmatrix} = \begin{pmatrix} u_{k+1} \\ u_{k+2} \\ \vdots \\ u_{k+n} \end{pmatrix} = \vec{u}_{k+n+1},$$

то есть умножение A на $\vec{u}_{k+n}$ даёт нам только один следующий элемент последовательности $\{u_k\}_{k\geq 0}$. Если мы возведём матрицу A в степень n, то умножение A^n на $\vec{u}_{k+n}$ будет давать $\vec{u}_{k+2n}$, то есть сразу n следующих элементов последовательности. Период $\{u_k\}_{k\geq 0}$ будет равен мультипликативному порядку матрицы A (далее обозначается как $o(A)$), поэтому чем больше $o(A)$, тем лучше для некоторых приложений. Максимально возможным значением для $o(A)$ является $q^n - 1$ [3, с. 363].

Рассмотрим теперь другую рекуррентную последовательность $\{v_k\}_{k\geq 0}$ элементов из конечного поля $\mathbb{F}_q$, задаваемую следующим образом для всех k из $\mathbb{N}$:

$$\begin{cases} v_{(k+1)n-n} = y_{1,1}v_{kn-n} + y_{1,2}v_{kn-n+1} + \cdots + y_{1,n}v_{kn-1} \\ \cdots \\ v_{(k+1)n-2} = y_{n-1,1}v_{kn-n} + y_{n-1,2}v_{kn-n+1} + \cdots + y_{n-1,n}v_{kn-1} \\ v_{(k+1)n-1} = y_{n,1}v_{kn-n} + y_{n,2}v_{kn-n+1} + \cdots + y_{n,n}v_{kn-1} \end{cases}$$

где $y_{i,j} \in \mathbb{F}_q$. Если обозначить через $\vec{v}_k$ вектор $(v_{kn-n}, v_{kn-n+1}, \ldots, v_{kn-1})^T$, то будет верно утверждение

$$Y\vec{v}_k = \begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n-1,1} & y_{n-1,2} & \cdots & y_{n-1,n} \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n} \end{pmatrix} \begin{pmatrix} v_{kn-n} \\ v_{kn-n+1} \\ \vdots \\ v_{kn-1} \end{pmatrix} = \begin{pmatrix} v_{(k+1)n-n} \\ v_{(k+1)n-n+1} \\ \vdots \\ v_{(k+1)n-1} \end{pmatrix} = \vec{v}_{k+1}.$$

Поэтому можно смотреть на $\{\vec{v}_k\}$ как на рекуррентную последовательность векторов длины n с соотношением

$$\forall k \in \mathbb{N} \quad \vec{v}_{k+1} = Y\vec{v}_k,$$

где Y — это $n \times n$-матрица из $GL_n(q)$. Период этой последовательности будет равен $o(Y)$ для любого ненулевого начального вектора $\vec{v}_1$. Используя стандартное умножение матрицы на вектор, получим, что вычисление каждого следующего элемента последовательности будет требовать $n(n-1)$ сложений и n^2 умножений.

В статье решается задача построения матрицы Y с большим мультипликативным порядком, которая позволяла бы вычислять элементы последовательности за меньшее количество арифметических операций, чем стандартное умножение матрицы на вектор, и при этом порождала бы последовательности с большим периодом.

2. Предварительные замечания и обозначения

Через I_n будем обозначать единичную $n \times n$-матрицу, а через $o(A)$ — мультипликативный порядок $n \times n$-матрицы A, то есть наименьшее целое m такое, что $A^m = I_n$.

Как обычно (n, m) — это наибольший общий делитель для целых n и m. Группу обратимых $n \times n$-матриц над конечным полем из q элементов $\mathbb{F}_q$ относительно операции умножения будем обозначать как $GL_n(q)$, а её подгруппу из матриц с определителем равным 1 как $SL_n(q)$.

Если A — $m \times n$-матрица, а B — $p \times q$-матрица, то через $A \otimes B$ будем обозначать их произведение Кронекера, то есть $mp \times nq$-матрицу вида

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}.$$

Произведение Кронекера обладает следующими свойствами:

1. $(A \otimes B)(C \otimes D) = AC \otimes BD$.
2. Пусть $AXB^T = C$, где A, X, B^T, C — это матрицы подходящих размеров, а B^T — транспонированная матрица B, тогда $(A \otimes B)\vec{X}^T = \vec{C}^T$, в данном случае стрелки означают, что к матрицам X и C был применён оператор векторизации. Этот оператор, выписывая строки матрицы одну за другой, преобразует её в вектор-строку, транспонировав которую можно получить вектор-столбец.

Выражение вида $a := b + c$, как и в некоторых языках программирования, означает, что переменной a присвоили значение $b + c$.

3. Основная теорема

Для доказательства основной теоремы потребуются следующие вспомогательные леммы.

Лемма 1. *В группе $SL_s(q^t)$ существует элемент порядка $\frac{q^{st}-1}{q^t-1}$.*

Доказательство. Рассмотрим группу $GL_s(q^t)$, в ней существует элемент A с максимальным порядком равным $q^{st} - 1$. Пусть $\det(A) = \lambda \in \mathbb{F}_{q^t}$, тогда определитель элемента $B = A^{q^t-1}$ будет равен

$$\det(B) = \det(A^{q^t-1}) = \det(A)^{q^t-1} = \lambda^{q^t-1} = 1.$$

Следовательно, $B \in SL_s(q^t)$. Элемент B будет искомым, так как его мультипликативный порядок равен $\frac{q^{st}-1}{q^t-1}$. □

Лемма 2. *Пусть $f, s \in \mathbb{N}$, тогда $(\frac{f^s-1}{f-1}, f-1) = (s, f-1)$.*

Доказательство. Пусть r делит $f - 1$, то есть $f \equiv 1 \mod r$, тогда

$$\begin{aligned} \frac{f^s-1}{f-1} &= 1 + f + \cdots + f^{s-1} \\ &\equiv \underbrace{1 + 1 + \cdots + 1}_{s} \mod r \end{aligned}$$

Пусть $d = (\frac{f^s-1}{f-1}, f-1)$, тогда верно, что d делит $f-1$, следовательно, $\frac{f^s-1}{f-1} \equiv s \mod d$. Вместе с тем $\frac{f^s-1}{f-1} \equiv 0 \mod d$, что даст нам $s \equiv 0 \mod d$, то есть d делит s. Отсюда будет следовать, что

$$d|(s, f-1). \tag{1}$$

Обратно, пусть $d' = (s, f-1)$, тогда верно, что d' делит $f-1$, следовательно, $\frac{f^s-1}{f-1} \equiv s \mod d'$. Вместе с тем $s \equiv 0 \mod d'$, что даст нам $\frac{f^s-1}{f-1} \equiv 0 \mod d'$, то есть d' делит $\frac{f^s-1}{f-1}$. Отсюда будет следовать, что

$$d'| \left(\frac{f^s-1}{f-1}, f-1 \right). \tag{2}$$

Вместе утверждения (1) и (2) означают $(\frac{f^s-1}{f-1}, f-1) = (s, f-1)$. □

Лемма 3. *Пусть $C = (c_{mn})$ — это $st \times st$-матрица, тогда существуют $s \times s$-матрицы A_i и $t \times t$-матрицы B_i такие, что $C = \sum_{i=1}^{s^2t^2} A_i \otimes B_i$.*

Доказательство. Будем смотреть на матрицу C как на s^2 клеток размера $t \times t$. Каждый элемент C можно записать как c_{ijkl}, где ij — индекс клетки, kl — индекс элемента в клетке.

Обозначим через E_{ijkl} $st \times st$-матрицу, у которой элемент с индексом $ijkl$ равен единице, все остальные — нулю. Тогда $E_{ijkl} = E_{ij}^{(1)} \otimes E_{kl}^{(2)}$, где

$$E_{ij}^{(1)} = \begin{matrix} \\ i \end{matrix} \begin{matrix} \begin{matrix} \quad j \end{matrix} \\ \begin{pmatrix} 0 & \vdots & 0 \\ \cdots & 1 & \cdots \\ 0 & \vdots & 0 \end{pmatrix} \end{matrix}, \quad E_{kl}^{(2)} = \begin{matrix} \\ k \end{matrix} \begin{matrix} \begin{matrix} \quad l \end{matrix} \\ \begin{pmatrix} 0 & \vdots & 0 \\ \cdots & 1 & \cdots \\ 0 & \vdots & 0 \end{pmatrix} \end{matrix}.$$

Так как $C = \sum_{i,j,k,l} c_{ijkl} E_{ijkl}$, то доказано существование представления. □

Теорема 1 (Основная)**.** *Пусть $n = st$, $1 < s, t < n$. Тогда существуют $s \times s$-матрицы $A_1, A_2, \ldots, A_s$ и $t \times t$-матрицы $B_1, B_2, \ldots, B_s$ над полем $\mathbb{F}_q$ такие, что матрица $Y = \sum_{i=1}^{s} A_i \otimes B_i$ из группы $GL_n(q)$ имеет мультипликативный порядок $\frac{q^n-1}{(s,q^t-1)}$.*

Как показано в лемме 3, любую $st \times st$-матрицу C можно представить в виде $C = \sum_{i=1}^{s^2t^2} A_i \otimes B_i$, где A_i и B_i — это $s \times s$ и $t \times t$-матрицы соответственно. Поэтому ценность теоремы будет в том, что для представления матрицы Y с большим мультипликативным порядком будет достаточно не более s слагаемых.

Доказательство. Для доказательства нам будет нужна вспомогательная матрица

$$Y' = (A \otimes B)(I_{st} + \sum_{i=1}^{s-1} C_i \otimes D_i).$$

Здесь A — это нижнетреугольная $s \times s$-матрица из $GL_s(q)$ вида

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_1 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \alpha_{s-1} & 1 \end{pmatrix},$$

а $t \times t$-матрица B равна единичной I_t.

C_i — это $s \times s$-матрица вида

$$C_i = \begin{pmatrix} 0 & \cdots & 1 & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix},$$

где 1 расположена в $i+1$-ом столбце первой строки.

$t \times t$-матрицы D_i берутся из линейной оболочки циклической группы $\langle R \rangle$, где матрица $R \in GL_t(q)$ имеет мультипликативный порядок $q^t - 1$. По следствию из леммы Шура и теоремы Веддербёрна [1, 6] линейная оболочка группы $\langle R \rangle$ является полем, изоморфным $\mathbb{F}_{q^t}$, поэтому каждая матрица D_i будет соответствовать какому-то элементу $\beta_i \in \mathbb{F}_{q^t}$.

Напомню, что характеристический многочлен $p(x) = p_0 + p_1 x + \cdots + p_{t-1}x^{t-1} + x^t$ матрицы R будет иметь степень t. По теореме Гамильтона-Кэли получим

$$p(R) = p_0 I_t + p_1 R + \cdots + p_{t-1}R^{t-1} + R^t = 0.$$

Отсюда можно выразить R^t через линейную комбинацию меньших степеней. Поэтому при построении линейной оболочки можно ограничиться степенями R от 0 до $t-1$, то есть

$$\mathbb{F}_{q^t} \cong \{\gamma_0 I_t + \gamma_1 R + \gamma_2 R^2 + \cdots + \gamma_{t-1}R^{t-1} \mid \gamma_i \in \mathbb{F}_q\}.$$

Из вышесказанного следует, что так как I_t и $\alpha_i I_t$ являются элементами линейной оболочки группы $\langle R \rangle$, они также соответствуют каким-то элементам поля $\mathbb{F}_{q^t}$. Очевидно, что I_t — это единица из $\mathbb{F}_{q^t}$, а $\alpha_i I_t$ для краткости будем обозначать через α_i, то есть теперь $\alpha_i \in \mathbb{F}_{q^t}$. Поэтому на матрицу

$$A \otimes B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_1 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \alpha_{s-1} & 1 \end{pmatrix}$$

и на матрицы

$$\sum_{i=1}^{s-1} C_i \otimes D_i = \begin{pmatrix} 0 & \beta_1 & \beta_2 & \cdots & \beta_{s-1} \\ 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

можно смотреть как на $s \times s$-матрицы над полем $\mathbb{F}_{q^t}$.

Более того, так как определители $A \otimes B$ и $I_{st} + \sum_{i=1}^{s-1} C_i \otimes D_i$ равны единице, их можно считать элементами $SL_s(q^t)$. Поэтому их произведение

$$Y' = (A \otimes B)(I_{st} + \sum_{i=1}^{s-1} C_i \otimes D_i) = \begin{pmatrix} 1 & \beta_1 & \beta_2 & \cdots & \beta_{s-1} \\ \alpha_1 & \alpha_1\beta_1 + 1 & \alpha_1\beta_2 & \cdots & \alpha_1\beta_{s-1} \\ 0 & \alpha_2 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_{s-1} & 1 \end{pmatrix}$$

также будет из $SL_s(q^t)$. Характеристическим многочленом матрицы Y' будет:

$$\det(\lambda I_s - Y') = \det \begin{pmatrix} \lambda-1 & -\beta_1 & -\beta_2 & \cdots & -\beta_{s-1} \\ -\alpha_1 & \lambda-\alpha_1\beta_1-1 & -\alpha_1\beta_2 & \cdots & -\alpha_1\beta_{s-1} \\ 0 & -\alpha_2 & \lambda-1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -\alpha_{s-1} & \lambda-1 \end{pmatrix}$$

$$= \det \begin{pmatrix} \lambda-1 & -\beta_1 & -\beta_2 & \cdots & -\beta_{s-1} \\ -\lambda\alpha_1 & \lambda-1 & 0 & \cdots & 0 \\ 0 & -\alpha_2 & \lambda-1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -\alpha_{s-1} & \lambda-1 \end{pmatrix} = 0.$$

Здесь используется то, что если умножить первую строку матрицы $\lambda I_s - Y'$ на α_1 и вычесть её из второй строки, то получится матрица с тем же определителем.

Разложив определитель по первой строке получим

$$(\lambda-1)^s - \lambda\sum_{i=1}^{s-1}(\lambda-1)^{s-i-1}\gamma_i = 0,$$

где

$$\gamma_i = \alpha_1 \cdots \alpha_i\beta_i.$$

Докажем индукцией по s, что, раскрыв скобки и сгруппировав коэффициенты при соответствующих степенях λ, мы получим

$$\lambda^s + \sum_{i=1}^{s-1}(g_i - \gamma_i)\lambda^{s-i} + (-1)^s = 0, \tag{3}$$

где

$$g_i = \sum_{j=0}^{i-1} e_{ij}\gamma_j, \quad \gamma_0 = 1 \tag{4}$$

при этом $e_{ij} \in \mathbb{F}_{q^t}$ возникают из биномиальных коэффициентов.

Пусть M_s обозначает $s \times s$-матрицу вида

$$\begin{pmatrix} \lambda-1 & -\beta_1 & -\beta_2 & \cdots & -\beta_{s-1} \\ -\lambda\alpha_1 & \lambda-1 & 0 & \cdots & 0 \\ 0 & -\alpha_2 & \lambda-1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -\alpha_{s-1} & \lambda-1 \end{pmatrix}.$$

База индукции:

$$\det M_2 = \det \begin{pmatrix} \lambda-1 & -\beta_1 \\ -\lambda\alpha_1 & \lambda-1 \end{pmatrix} = \lambda^2 + (-2-\alpha_1\beta_1)\lambda + 1.$$

Шаг индукции: пусть формула (3) верна для M_s, докажем, что она будет также верна для M_{s+1}. Для этого разложим определитель матрицы

$$M_{s+1} = \begin{pmatrix} \lambda-1 & -\beta_1 & -\beta_2 & \cdots & -\beta_s \\ -\lambda\alpha_1 & \lambda-1 & 0 & \cdots & 0 \\ 0 & -\alpha_2 & \lambda-1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & -\alpha_s & \lambda-1 \end{pmatrix}$$

по последнему столбцу

$$\begin{aligned}
\det M_{s+1} &= (\lambda-1)\det M_s - \gamma_s\lambda \\
&= (\lambda-1)\left(\lambda^s + \sum_{i=1}^{s-1}(g_i-\gamma_i)\lambda^{s-i} + (-1)^s\right) - \gamma_s\lambda \\
&= \lambda^{s+1} + \sum_{i=1}^{s-1}(g_i-\gamma_i)\lambda^{s-i+1} + (-1)^s\lambda - \lambda^s - \sum_{i=1}^{s-1}(g_i-\gamma_i)\lambda^{s-i} + (-1)^{s+1} - \gamma_s\lambda \\
&= \lambda^{s+1} + (g_1-\gamma_1)\lambda^s + \sum_{i=2}^{s-1}(g_i-\gamma_i)\lambda^{s-i+1} + (-1)^s\lambda - \\
&\quad - \lambda^s - \sum_{i=1}^{s-2}(g_i-\gamma_i)\lambda^{s-i} - (g_{s-1}-\gamma_{s-1})\lambda + (-1)^{s+1} - \gamma_s\lambda \\
&= \lambda^{s+1} + (g_1-\gamma_1)\lambda^s + \sum_{i=2}^{s-1}(g_i-\gamma_i)\lambda^{s-i+1} + (-1)^s\lambda - \\
&\quad - \lambda^s - \sum_{i=2}^{s-1}(g_{i-1}-\gamma_{i-1})\lambda^{s-i+1} - (g_{s-1}-\gamma_{s-1})\lambda + (-1)^{s+1} - \gamma_s\lambda \\
&= \lambda^{s+1} + (g_1-1-\gamma_1)\lambda^s + \sum_{i=2}^{s-1}\left(g_i - g_{i-1} + \gamma_{i-1} - \gamma_i\right)\lambda^{s-i+1} + \\
&\quad + \left((-1)^s - g_{s-1} + \gamma_{s-1} - \gamma_s\right)\lambda + (-1)^{s+1}
\end{aligned}$$

Если теперь обозначить

$$\begin{aligned}
g'_1 &= g_1 - 1 \\
g'_i &= g_i - g_{i-1} + \gamma_{i-1} \text{ для всех } i \in \{2,3,\ldots,s-1\} \\
g'_s &= (-1)^s - g_{s-1} + \gamma_{s-1},
\end{aligned}$$

то получим формулу (3).

Пусть θ — элемент поля $\mathbb{F}_{q^{st}}$, имеющий порядок $\frac{(q^{st}-1)}{(q^t-1)}$. По лемме 1 в группе $SL_s(q^t)$ существует элемент Z с таким порядком, причём характеристический многочлен $\chi_Z(\lambda) = \lambda^s + \sum_{i=1}^{s-1} d_i\lambda^{s-i} + (-1)^s$ матрицы Z имеет своим корнем θ, и все коэффициенты d_i этого многочлена лежат в поле $\mathbb{F}_{q^t}$.

Система уравнений $g_i - \alpha_1\alpha_2\ldots\alpha_i\beta_i = d_i$, где $i = 1,2,\ldots,s-1$ имеет треугольную матрицу и потому разрешима относительно $\beta_1,\beta_2,\ldots,\beta_{s-1}$ при любой правой части, когда $\alpha_1\alpha_2\ldots\alpha_{s-1} \neq 0$. Например, можно взять $\alpha_1 = \alpha_2 = \cdots = \alpha_{s-1} = 1$.

Отсюда следует, что матрица Y' имеет мультипликативный порядок равный $(q^{st}-1)/(q^t-1)$ при соответствующим образом выбранных элементах $\beta_1, \beta_2, \ldots, \beta_{s-1}$. Напомню, что

$$Y' = (A \otimes I_t)(I_{st} + C_1 \otimes D_1 + \cdots + C_{s-1} \otimes D_{s-1}),$$

где D_i выбраны из линейной оболочки группы $\langle R \rangle$ и соответствуют элементам $\beta_i \in \mathbb{F}_{q^t}$. Легко увидеть, что матрицы D_i будут перестановочны с R. Отсюда следует, что $I_s \otimes R$ перестановочна с $A \otimes I_t$ и с любой из матриц $C_i \otimes D_i$. Поэтому матрица

$$\begin{aligned} Y &:= (I_s \otimes R)Y' \\ &= (I_s \otimes R)(A \otimes I_t)(I_{st} + \sum_{i=1}^{s-1} C_i \otimes D_i) \\ &= (A \otimes R)(I_{st} + \sum_{i=1}^{s-1} C_i \otimes D_i) \end{aligned}$$

имеет мультипликативный порядок

$$o(Y) = \frac{o(Y')o(R)}{(o(Y'), o(R))} = \frac{q^{st}-1}{(\frac{q^{st}-1}{q^t-1}, q^t-1)} = \frac{q^n-1}{(s, q^t-1)},$$

где последнее равенство получено с помощью леммы 2. □

Доказанная выше теорема ничего не говорит о том, как построить матрицу Y с мультипликативным порядком $\frac{q^n-1}{(s,q^t-1)}$, она лишь говорит нам, что такая матрица существует. Для практических целей этого может оказаться достаточно, потому что мы можем выбирать случайным образом матрицы $\{D_i\}$ (причем чем больше будет среди них нулевых матриц, тем меньше будет нужно арифметических операций для умножения Y на вектор) до тех пор, пока не сконструируем матрицу с нужным мультипликативным порядком. Один раз найдя такую матрицу, мы можем использовать её для построения множества рекуррентных последовательностей.

Замечу, что в одном часто встречающемся на практике случае, когда числа $q = 2^{q'}$ и $n = 2^{n'}$ являются степенями двойки (поэтому $s = 2^{s'}$ и $t = 2^{t'}$), мы получим, что существует матрица с мультипликативным порядком

$$\frac{q^n-1}{(s, q^t-1)} = \frac{q^n-1}{(2^{s'}, 2^{q't}-1)} = q^n - 1,$$

то есть будет достигнут максимально возможный порядок для элемента $GL_n(q)$.

В конце нужно отметить, что если в условии теоремы 1 поменять местами переменные s и t, то, сделав соответствующие замены в доказательстве, мы снова получим верное утверждение. То есть если для нас выгоднее искать матрицу Y как элемент группы $GL_t(q^s)$, а не $GL_s(q^t)$, то мы можем так делать.

4. Вычисление элементов рекуррентной последовательности

Теперь рассмотрим вопрос, как помогает структура матрицы из теоремы 1 при вычислении элементов рекуррентной последовательности, и посчитаем, сколько для этого потребуется сложений и умножений. Пусть m_k и m_{k+1} — это $s \times t$-матрицы, полученные из векторов $\vec{v}_k$ и $\vec{v}_{k+1}$ длины st соответственно. Тогда из

$$\vec{v}_{k+1} = \left(\sum_{i=1}^{s} A_i \otimes B_i\right)\vec{v}_k = (A \otimes R)\left(I_{st} + \sum_{i=1}^{s-1} C_i \otimes D_i\right)\vec{v}_k$$

и 2 свойства произведения Кронекера будет следовать, что

$$m_{k+1} = A(m_k + \sum_{i=1}^{s-1} C_i m_k D_i^T)R^T, \tag{5}$$

то есть элементы векторной рекуррентной последовательности $\{\vec{v}_k\}_{k\geq 0}$ можно вычислять по формуле (5), предварительно преобразовав векторы в матрицы.

Вычисление $C_i m_k$ сводится к выделению в матрице m_k $(i+1)$-ой строки и размещению её на первое место, все же остальные строки в матрице $C_i m_k$ будут нулевыми, поэтому данный шаг не требует ни сложений, ни умножений.

Для получения $C_i m_k D_i^T$ необходимо единственную ненулевую строку матрицы $C_i m_k$ умножить справа на D_i^T, что потребует $t(t-1)$ сложений и t^2 умножений. Обозначим через r число ненулевых матриц D_i. Эмпирически было установлено, что это число может быть значительно меньше s. Таким образом, для вычисления $m' := m_k + \sum_{i=1}^{s-1} C_i m_k D_i^T$ потребуется $st + rt(t-1)$ сложений и rt^2 умножений.

Напомню, что $s \times s$-матрица A имеет вид

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_1 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \alpha_{s-1} & 1 \end{pmatrix},$$

поэтому вычисление $m'' := Am'$ будет требовать $(s-1)t$ сложений и не будет требовать умножений, если мы возьмём $\alpha_1 = \cdots = \alpha_{s-1} = 1$.

Чтобы узнать, сколько нужно операций для вычисления $m''R^T$, рассмотрим, как строится матрица R с мультипликативным порядком $q^t - 1$. Для этого нам нужен примитивный многочлен степени t с коэффициентами из поля $\mathbb{F}_q$

$$p(x) = p_0 + p_1 x + \cdots + p_{t-1}x^{t-1} + x^t \ \in \mathbb{F}_q[x].$$

Напомню, что **примитивным** называют минимальный многочлен, корнем которого будет образующий мультипликативной группы поля $\mathbb{F}_q$. В свою очередь **минимальным многочленом** алгебраического элемента называют многочлен, которому кратны все многочлены, корнем которых является данный элемент.

Если выписать коэффициенты $p(x)$ в матрицу следующим образом:

$$\begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ -p_0 & -p_1 & \cdots & -p_{t-1} \end{pmatrix},$$

то получим **сопровождающую матрицу** унитарного многочлена, мультипликативный порядок которой равен $q^t - 1$. Её мы и возьмём в качестве R. Поэтому вычисление $m''R^T$ будет требовать $s(t-1)$ сложений и st умножений.

Таким образом, общее количество арифметических операций, необходимых для умножения матрицы на вектор, равно $rt^2 + 3st - (r+1)t - s$ сложений и $rt^2 + st$ умножений или, используя симметричность s и t, $r's^2 + 3ts - (r'+1)s - t$ сложений и $r's^2 + ts$ умножений.

В наихудшем случае, когда r равно s (соответственно r' равно t), получим, что для умножения матрицы на вектор требуется всего $st^2 + 2st - s - t$ сложений и $st^2 + st$ умножений (соответственно $ts^2 + 2ts - t - s$ сложений и $ts^2 + ts$ умножений), что всё равно будет лучше, чем стандартный алгоритм, который требует $s^2t^2 - st$ сложений и s^2t^2 умножений. Замечу, что либо s, либо t будет меньше, чем $\sqrt{n}$, из этого можно получить асимптотическую оценку $O(n^{3/2})$ для числа умножений и сложений.

Кроме того, описанная схема даёт возможность проводить некоторые вычисления параллельно, а именно для каждого i можно вычислять $C_i m_k D_i^T$ в отдельном потоке. Использование параллельных вычислений дополнительно сократит время, необходимое для нахождения следующего элемента последовательности.

5. Благодарности

Хочу выразить глубокую благодарность своему научному руководителю Льву Сергеевичу Казарину за идею и помощь в написании этой статьи.

Список литературы

1. *Супруненко Д. А., Тышкевич Р. И.* Перестановочные матрицы // Наука и Техника. 1966. [*Suprunenko D. A., Tyshkevich R. I.* Perestanovochnye matritsy // Nauka i Tekhnika. 1966 (in Russian)].

2. *Винберг Э. Б.* Курс алгебры. М.: Издательство МЦНМО. 2011 [*Vinberg E. B.* Kurs algebry. M.: Izdatelstvo MTsNMO, 2011 (in Russian)].

3. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. М.: Мир, 1976. (English transl.: *Birkhoff G., Bartee T.* Modern applied algebra. McGraw-Hill Companies, 1970.)

Fast Multiplication of a Matrix with Large Multiplicative Order by a Vector Over a Finite Field

Ivanov D. M.

P.G. Demidov Yaroslavl State University,
Sovetskaya str., 14, Yaroslavl, 150000, Russia

Keywords: matrix-vector multiplication, recurrent sequences

Consider a linear recurrent sequence of vectors $\{\vec{v}_k\}_{k\geq 0}$ of length n over $\mathbb{F}_q$ that satisfies the relation

$$\forall k \in \mathbb{N} \quad \vec{v}_{k+1} = Y\vec{v}_k,$$

where Y is an $n \times n$-matrix from $GL_n(q)$. The period of this sequence equals the multiplicative order of the matrix Y, whose maximum is $q^n - 1$ [3, p. 363].

The paper solves a problem of constructing a matrix Y with large multiplicative order that requires less arithmetic operations than standard matrix-vector multiplication to compute elements of this recurrent sequence and that generates a sequence with large period.

The main assertion of the paper is the following. Let $n = st,\ 1 < s, t < n$, then there exist $s \times s$-matrices $A_1, A_2, \ldots, A_s$ and $t \times t$-matrices $B_1, B_2, \ldots, B_s$ over the field $\mathbb{F}_q$ such that a matrix $Y = \sum_{i=1}^{s} A_i \otimes B_i$ from $GL_n(q)$ has the multiplicative order equal to $\frac{q^n-1}{(s,q^t-1)}$.

Сведения об авторах:
Иванов Дмитрий Михайлович,
Ярославский государственный университет им. П.Г. Демидова,
аспирант