МАТЕМАТИКА

УДК 512.542

МАКСИМАЛЬНЫЙ ПОРЯДОК ЭЛЕМЕНТА И ЭКСПОНЕНТА ГРУППЫ ОБРАТИМЫХ МАТРИЦ НАД КОНЕЧНЫМ ПОЛЕМ

А. А. Шевченко

Пусть $k = \mathbb{F}_q$ — конечное поле из q элементов, $\operatorname{char} k = p$, $q = p^r$. Группа обратимых матриц $\mathrm{GL}(n, \mathbb{F}_q)$ с коэффициентами из k имеет конечный порядок. В работе найден максимальный порядок элемента и экспонента этой группы. Максимальный порядок элемента группы равен $q^n - 1$. Экспонента группы равна $p^{\lceil \log_p n \rceil} \cdot \mathrm{НОК}(q^n - 1, q^{n-1} - 1, \ldots, q - 1)$.

§1. Оценка порядка элемента группы $\mathrm{GL}(n, \mathbb{F}_q)$

Пусть $A \in \mathrm{GL}(n, \mathbb{F}_q)$, J — жорданова форма A, тогда существует матрица $T \in \mathrm{GL}(n, \mathbb{F}_q)$ такая, что $J = T^{-1} \cdot A \cdot T$, следовательно, порядки матриц J и A совпадают и можно перейти к изучению жордановых форм матриц, что сильно упрощает задачу. Жорданова форма матрицы имеет блочно-диагональный вид, каждый блок — это жорданова клетка, а значит, достаточно изучить натуральную степень жордановой клетки. Как известно, (i, j)-й элемент r-й степени жордановой клетки

$$J = \begin{pmatrix} \alpha & 1 & 0 & \ldots & 0 \\ 0 & \alpha & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & \alpha \end{pmatrix}$$

при $i < j$ равен $C_r^{j-i} \cdot \alpha^{r-j+i}$.

В нашем случае матрица J обратима, следовательно, $\alpha \neq 0$. Из приведенной выше формулы можно заметить, что для того, чтобы жорданова клетка в какой-то степени дала единичную матрицу, достаточно, чтобы C_r^k стали равны нулю для всех k от 1 до $r - 1$, а C_r^r вышел за границы рассматриваемой матрицы, и степень делилась на порядок мультипликативной группы поля $\mathbb{F}_q$. Из первого условия следует, что $p \mid C_r^k$ для всех k от 1 до $r - 1$, такое возможно, если $n = p^d$, причем d необходимо выбрать так, чтобы C_r^r вышел за границы рассматриваемой клетки, отсюда $d = \lceil \log_p n \rceil$. Получаем верхнюю оценку для порядка J:

$$\operatorname{ord} J \leqslant p^{\lceil \log_p n \rceil}(q - 1).$$

Теперь пусть обратимая матрица A состоит из нескольких жордановых клеток $J_1, J_2, \ldots, J_n$, их размеры равны, соответственно, $t_1, t_2, \ldots, t_n$, собственные числа, соответствующие им, имеют вид $\alpha_1, \alpha_2, \ldots, \alpha_n$, их порядки равны, соответственно, $q_1, q_2, \ldots, q_n$. Тогда порядок матрицы не превосходит

$$\operatorname{ord} A \leqslant p^{\lceil \log_p(\max_{i=1,\ldots,n} t_i) \rceil} q_1 q_2 \ldots q_n.$$

Теорема 1. *Пусть* $A \in \mathrm{GL}(n, \mathbb{F}_q)$, *тогда* $\operatorname{ord} A \leqslant q^n - 1$.

Шевченко Александр Александрович (olavforever@mail.ru), *студент 4 курса механико-математического факультета Самарского государственного университета, 443011, Россия, г. Самара, ул. Академика Павлова, 1.*

Доказательство. Пусть $f(x)$ — характеристический многочлен матрицы A. В кольце $\mathbb{F}_q[x]$ он однозначно разлагается на неприводимые множители:

$$f = f_1^{l_1}(x)\, f_2^{l_2}(x)\, \ldots\, f_k^{l_k}(x).$$

Обозначим степени многочленов из разложения через $t_1, t_2, \ldots, t_k$ соответственно. Тогда порядок матрицы равен

$$n = t_1 l_1 + t_2 l_2 + \ldots + t_k l_k.$$

Утверждается, что порядки корней f_i в алгебраическом замыкании поля $\mathbb{F}_q$ не превосходят $q^{t_i} - 1$. Действительно, в поле $\mathbb{F}_q[x]/(f_i(x))$ многочлен f_i разлагается на линейные множители, а порядок мультипликативной группы этого поля равен $q^{t_i} - 1$. Без ограничения общности предположим, что все t_i различны. Отсюда получаем, что порядок матрицы не превосходит

$$p^{\lceil \log_p(\max_{i=1,\ldots,k} l_i)\rceil} \prod_{i=1}^{n} (q^{t_i} - 1).$$

Осталось показать, что

$$p^{\lceil \log_p(\max_{i=1,\ldots,k} l_i)\rceil} \prod_{i=1}^{n} (q^{t_i} - 1) \leqslant q^n - 1.$$

Применим очевидную оценку

$$p^{\lceil \log_p(\max_{i=1,\ldots,k} l_i)\rceil} (q^{\sum t_i} - 1) \leqslant q^n - 1.$$

Пусть $q = p^t$ и $\max_{i=1,\ldots,k} l_i = l_j$, получим

$$p^{\lceil \log_p\ l_j\rceil} (p^{t\sum t_i} - 1) \leqslant p^{tn} - 1.$$

Остается показать, что

$$p^{\lceil \log_p\ l_j\rceil + t\sum t_i} - 1 \leqslant p^{tn} - 1,$$

что равносильно

$$\lceil \log_p\ l_j\rceil + t\sum t_i \leqslant tn;$$

другими словами,

$$\lceil \log_p\ l_j\rceil + t\sum t_i \leqslant t(t_1 l_1 + \ldots + t_k l_k).$$

Применяя простые преобразования, получаем, что

$$\lceil \log_p\ l_j\rceil \leqslant t((t_1 - 1)l_1 + \ldots + (t_k - 1)l_k).$$

Последнее неравенство следует из того очевидного факта, что

$$\lceil \log_p\ l_j\rceil \leqslant t(t_j - 1)l_j.$$

Теорема доказана. □

§2. Построение элемента максимального порядка и экспонента группы $\mathrm{GL}(n, \mathbb{F}_q)$

Для того, чтобы построить элемент максимального (по оценке из Теоремы 1) порядка, необходимо использовать фробениусову нормальную форму матрицы [2]. По определению, это матрица вида

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix},$$

где a_i — любые числа. Её характеристический многочлен имеет вид

$$f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_0.$$

Далее приводится алгоритм построения элемента максимального порядка.

1. Необходимо найти $p(\lambda)$ — унитарный примитивный многочлен степени n над полем $\mathbb{F}_q$), он найдётся, так как существует примитивный многочлен произвольной степени [1].

2. По коэффициентам полученного многочлена

$$p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_0$$

нужно восстановить матрицу

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix},$$

характеристический многочлен которой имеет вид

$$f(\lambda) = p(\lambda).$$

Рассмотрим факторкольцо $\mathbb{F}_q[\lambda]/p(\lambda)$, которое из-за неприводимости $p(\lambda)$ является полем; в нём будут лежать все корни многочлена $p(\lambda)$, пусть это числа $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q[\lambda]/p(\lambda)$. Соответствующая жорданова клетка в этом случае имеет вид

$$\begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix}.$$

Чтобы матрица в какой-то степени дала единичную, нужно, чтобы все корни в этой степени давали единицу. Поскольку все они степени одного элемента, значит, степень кратна порядку группы, то есть степень делится на $q^n - 1$. С другой стороны, этот элемент — образующая мультипликативной группы поля, а значит, его порядок равен $q^n - 1$. Полученная матрица и будет иметь порядок $q^n - 1$.

Покажем теперь, что экспонента группы $\mathrm{GL}(n, \mathbb{F}_q)$ равна

$$p^{\lceil \log_p n \rceil} \cdot \mathrm{HOK}(q^n - 1, q^{n-1} - 1, \ldots, q - 1).$$

Сначала докажем, что $\exp(\mathrm{GL}(n, \mathbb{F}_q))$ не меньше, чем

$$p^{\lceil \log_p n \rceil} \cdot \mathrm{HOK}(q^n - 1, q^{n-1} - 1, \ldots, q - 1).$$

Это следует из того, что для каждого множителя можно построить матрицу такого порядка. Допустим, необходимо построить матрицу порядка $q^i - 1$, тогда возьмём матрицу максимального порядка $A \in \mathrm{GL}(i, \mathbb{F}_q)$ и поместим её в верхний левый угол матрицы $n \times n$, на остальных местах на диагонали которой стоят единицы, а остальные недиагональные элементы равны нулю. Матрицу порядка $p^{\lceil \log_p n \rceil}(q-1)$ можно построить, взяв диагональную матрицу, на главной диагонали которой стоит образующая группы $\mathbb{F}_q^*$.

Теперь осталось только заметить, что $\exp(\mathrm{GL}(n, \mathbb{F}_q))$ не больше, чем

$$p^{\lceil \log_p n \rceil} \cdot \mathrm{HOK}(q^n - 1, q^{n-1} - 1, \ldots, q - 1).$$

Действительно, из доказательства Теоремы 1 видно, что каждая матрица имеет порядок, который делит данное выражение.

Литература

1. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. М.: Мир, 1975. 746 с.

2. Прасолов В. В. Задачи и теоремы линейной алгебры. М.: Наука, 1996. 304 с.

Статья поступила в редакцию 15.10.2012 г.