

Построим группу S_n в формате минимальных слов по алгоритму из [1]. В итоге максимальная длина минимальных слов группы S_n является решением задачи.

Ниже в таблице приведены решения для $n = 2, 3, \dots, 12$, полученные при помощи компьютерных вычислений.

n	2	3	4	5	6	7	8	9	10	11	12
d	1	2	4	6	9	12	16	20	25	30	36

Аналогичные задачи встречаются на практике, например при проектировании компьютерных вычислительных сетей [2]. Сеть процессоров может быть представлена как неориентированный граф, в котором процессоры являются вершинами, а две вершины графа соединены ребром, если имеется прямое соединение между соответствующими процессорами. С одной стороны, желательно, чтобы между процессорами было как можно меньше соединений, а с другой — обмен данными между процессорами предпочтительно производить с наименьшим числом посредников. Очевидно, эти два критерия противоречат друг другу. На теоретико-групповом языке диаметр графа вычислительной сети равен максимальной длине минимальных слов соответствующей графу группы.

ЛИТЕРАТУРА

1. Кузнецов А. А., Антамошкин А. Н., Шлёпкин А. К. Моделирование периодических групп // Системы управления и информационные технологии. 2008. № 2. С. 4–8.
2. Halt D., Eick B., and O'Brien E. Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005.

УДК 519.6

СТРУКТУРНЫЕ СВОЙСТВА ПРИМИТИВНЫХ НАБОРОВ НАТУРАЛЬНЫХ ЧИСЕЛ

С. Н. Кяжин, В. М. Фомичев

При исследовании перемешивающих свойств композиции преобразований конечно-го множества возникает задача распознавания примитивности квадратной неотрицательной матрицы M и определения её экспонента $[1, 2]$, то есть наименьшего натурального числа γ , при котором $M^\gamma > 0$.

При изучении указанных свойств матрица $M = (m_{ij})$ обладает ровно теми же свойствами, что и её носитель, то есть матрица $\nu(M) = (\nu m_{ij})$, где

$$\nu m_{ij} = \begin{cases} 1, & \text{если } m_{ij} > 0, \\ 0, & \text{если } m_{ij} = 0. \end{cases}$$

Вместо матрицы M можно равносильным образом исследовать примитивность и экспонент орграфа Γ , матрица смежности вершин которого совпадает с $\nu(M)$. Заметим, что множество 0,1-матриц порядка n образует полугруппу G_n относительно операции $*$, где $A * B = \nu(AB)$.

Критерий примитивности орграфа определяется длинами его простых контуров [1]. Если $C_1, \dots, C_k$ — все простые контуры орграфа Γ длин $l_1, \dots, l_k$ соответственно, то орграф Γ примитивный, если и только если наибольший общий делитель $\gcd(l_1, \dots, l_k) = 1$. Таким образом, один из способов распознавания примитивности

орграфа Γ состоит в определении длин $l_1, \dots, l_k$ всех его простых циклов и в проверке примитивности набора чисел $(l_1, \dots, l_k)$, где набор натуральных чисел примитивен, если и только если эти числа взаимно просты.

Распознавание примитивности набора чисел $(l_1, \dots, l_k)$ можно выполнить, применив $k - 1$ раз алгоритм Евклида к элементам набора. Альтернативный подход состоит в использовании заранее составленной таблицы примитивных наборов при ограничении на числа $l_1, \dots, l_k$.

Работа посвящена исследованию свойств примитивных наборов чисел и задаче построения таблицы примитивных наборов при ограничении на числа $l_1, \dots, l_k$.

Утверждение 1. Если A — примитивный набор чисел, то примитивен любой набор, полученный из A добавлением любого натурального числа или (при $|A| > 1$) удалением числа a , кратного одному из остальных чисел набора.

Определение 1. Примитивный набор A размера $k \geq 1$ называется тупиковым, если $A = (1)$ или при $k > 1$ удаление из набора любого элемента нарушает его примитивность.

Определение 2. Примитивный набор A размера $k > 1$ называется r -примитивным, где $0 \leq r \leq k - 1$, если после удаления из A любого подмножества порядка r примитивность получившегося набора сохраняется.

Рассмотрим набор натуральных чисел $A = (a_1, \dots, a_k)$, где каждое из чисел набора не превышает m . Пусть 2^A — булеан множества $\{a_1, \dots, a_k\}$, $P(A, r)$ — множество всех примитивных наборов порядка r из 2^A , $P(A) = \bigcup_{r \leq k} P(A, r)$. На множестве $P(A)$ определим отношение частичного порядка: $(b_1, \dots, b_l) \leq (a_1, \dots, a_r)$, если и только если $l \leq r$ и найдется неповторная упорядоченная выборка $(i_1, \dots, i_l)$ из $(1, \dots, r)$, такая, что $i_1 < \dots < i_l$ и b_j делит a_{i_j} для всех $j = 1, \dots, l$.

Определение 3. Тупиковый набор $B \in P(A)$ называется минимальным в $P(A)$, если не существует другого набора $B' \in P(A)$, такого, что $B' \leq B$, и r -минимальным в $P(A)$, если не существует другого набора $B' \in P(A)$ длины r , такого, что $B' \leq B$.

Утверждение 2. Если A — примитивный набор, то $\langle P(A), \leq \rangle$ — верхняя полурешётка, в которой максимальный элемент есть A и любой минимальный элемент есть тупиковый минимальный набор.

Для набора A рассмотрим наибольший общий делитель как функцию, определённую на 2^A . При $B = \{a_{i_1}, \dots, a_{i_l}\} \in 2^A$ обозначим $\gcd(B) = \gcd(a_{i_1}, \dots, a_{i_l})$, если $B \neq \emptyset$, и $\gcd(\emptyset) = \text{lcm}(a_1, \dots, a_k)$, где $\gcd(a_{i_1}, \dots, a_{i_l})$ и $\text{lcm}(a_{i_1}, \dots, a_{i_l})$ — наибольший общий делитель и наименьшее общее кратное чисел $a_{i_1}, \dots, a_{i_l}$ соответственно; $D(A) = \{\gcd(B) : B \in 2^A\}$. Множество $D(A)$ частично упорядочено по отношению делимости: $\gcd(B) \leq \gcd(B')$ для $B, B' \in 2^A$, если и только если $\gcd(B)$ делит $\gcd(B')$.

Утверждение 3. Если A — примитивный тупиковый набор, то $D(A)$ — решётка, антиизоморфная решётке 2^A .

Обозначим через A_i коатомы решётки 2^A и через μ_i — атомы решётки $D(A)$: $A_i = \{a_1, \dots, a_k\} \setminus \{a_i\}$, $\mu_i = \gcd(A_i)$, $i = 1, \dots, k$.

Теорема 1. Набор A — примитивный тупиковый, если и только если $(\mu_1, \dots, \mu_k)$ — набор попарно взаимно простых чисел, отличных от 1. При этом $a_i = (c_i \mu_1 \dots \mu_k) / \mu_i$, где $(c_1, \dots, c_k)$ есть 1-примитивный набор натуральных чисел и $\gcd(c_i, \mu_i) = 1$ для $i = 1, \dots, k$.

Следствие 1. Прimitивный тупиковый набор A является k -минимальным, если и только если $(\mu_1, \dots, \mu_k)$ — набор простых чисел и $c_i = 1$ для $i = 1, \dots, k$.

По утверждению 1 любой примитивный набор A можно получить из соответствующего тупикового набора A' добавлением любого числа. По следствию 1 любой тупиковый набор A' можно получить из соответствующего k -минимального набора A'' умножением элемента набора a_i на число, взаимно простое с $\mu_i, i \in \{1, \dots, k\}$.

Алгоритм перечисления множества всех k -минимальных примитивных наборов, состоящих из чисел, не превышающих m , состоит в следующем. В соответствии с теоремой 1 и следствием 1 k -минимальный тупиковый примитивный набор $A = (a_1, \dots, a_k)$ состоит из чисел $a_i = (\mu_1 \cdot \dots \cdot \mu_k) / \mu_i$, где $(\mu_1, \dots, \mu_k)$ — набор различных простых чисел. Тогда если $\mu_1 < \dots < \mu_k$, то достаточно перечислить все наборы $(\mu_1, \dots, \mu_k)$ со свойством $\mu_2 \cdot \dots \cdot \mu_k \leq m$.

В качестве μ_k перебираем все простые числа в пределах, указанных неравенством

$$p_s \leq \mu_s \leq \left(\frac{m}{3\Psi_{s-1}} \right)^{\frac{1}{k-s+1}}, \quad (1)$$

где $\Psi_i = p_3 \cdot \dots \cdot p_i$; p_n — n -е простое число. При $3 \leq s < k$ и каждом фиксированном наборе чисел $(\mu_{s+1}, \dots, \mu_k)$ в качестве μ_s перебираем все простые числа в пределах, указанных в (1). При каждом фиксированном наборе чисел $(\mu_3, \dots, \mu_k)$ перебираем все простые числа μ_1 и μ_2 , где $2 \leq \mu_1 < \mu_2 < m^{\frac{1}{k-1}}$.

Оценена вычислительная сложность алгоритма, измеренная числом построенных наборов различных простых чисел $(\mu_1, \dots, \mu_k)$. Количество таковых не превышает $O\left(m^{\ln k} \left(\ln^2 m \cdot \prod_{j=2}^{k-1} \Psi_j\right)^{-1}\right)$. При $k > 2$ для оценки величин Ψ_k можно использовать

оценку [3]: $p_k > k \ln k$. Тогда $\Psi_k > \frac{k!}{2} \prod_{j=3}^k \ln j$.

Значения Ψ_k для $k = 3, \dots, 8$ приведены в таблице.

k	3	4	5	6	7	8
Ψ_k	5	35	385	5005	85085	1616615

Данная таблица показывает, что при ограничении $a_1, \dots, a_k \leq m$ число k -минимальных примитивных наборов быстро убывает с ростом k .

Рассмотренные свойства и алгоритм составления таблицы примитивных наборов могут быть использованы для изучения перемешивающих свойств преобразований, в частности для вычисления экспонентов перемешивающих матриц и соответствующих графов. Алгоритмические вопросы построения простых циклов в графе и вычисления экспонента орграфа рассмотрены более детально в [4].

ЛИТЕРАТУРА

1. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
2. Фомичёв В. М. Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010.
3. Rosser B. The n -th prime is greater than $n \log n$ // Proc. London Math. Soc. 1939. V. 45. P. 21–44.
4. Кяжсин С. Н., Фомичев В. М. О примитивных наборах натуральных чисел // Прикладная дискретная математика. 2012. № 2. С. 5–14.