С. Н. Кяжин, В. М. Фомичев

ОПРЕДЕЛЯЮЩИЕ СВОЙСТВА ПРИМИТИВНЫХ НАБОРОВ НАТУРАЛЬНЫХ ЧИСЕЛ

Введение

Матрица M называется положительной (неотрицательной), если положительны (неотрицательны) все ее элементы, обозначается $M > 0$ ($M \geq 0$). Неотрицательная матрица называется примитивной, если $M^t > 0$ при некотором натуральном t, а наименьшее натуральное γ, при котором $A^\gamma > 0$, называется экспонентом (показателем примитивности) матрицы M, обозначается $\exp M$. Если такое t не существует, то $\exp M = \infty$.

Сильно связный орграф Γ называется примитивным, если примитивна матрица смежности его вершин, т. е. для некоторого натурального m и для любой пары (i,j) в Γ существует путь из i в j длины m. Наименьшее такое m называется экспонентом графа Γ.

Одной из важных задач при изучении перемешивающих свойств преобразований является определение экспонентов перемешивающих матриц и, соответственно, перемешивающих графов [1, 2]. При исследовании экспонентов матриц и графов часто используется эпиморфизм мультипликативного моноида неотрицательных матриц порядка n на моноид n-вершинных орграфов, где умножение орграфов определено как умножение бинарных отношений [3]. Матрица положительна $\Leftrightarrow$ соответствующий граф полный. Отсюда следует, что орграф Γ и его матрица смежности M одновременно примитивны или не примитивны, в случае примитивности экспоненты их равны.

Критерий примитивности орграфа Γ определяется длинами его простых контуров [2] (контур простой, если проходит через любую вершину не более одного раза). Если $C_1,\ldots,C_k$ есть все простые контуры орграфа Γ длин $l_1,\ldots,l_k$ соответственно, то орграф Γ примитивный $\Leftrightarrow$ НОД$(l_1,\ldots,l_k) = 1$.

Набор взаимно простых в совокупности натуральных чисел $A = (a_1,\ldots,a_k)$ называется примитивным, т. е. набор A примитивен $\Leftrightarrow \gcd(a_1,\ldots,a_k) = 1$.

Функция Фробениуса $f(a_1,\ldots,a_k)$ определяется на всех примитивных наборах чисел при $k > 1$ и $a_1 > 1$ как наибольшее натуральное число, не представимое в виде линейной комбинации чисел набора A над множеством N_0, где $N_0 = N \cup \{0\}$, т. е.

$$f(a_1,\ldots,a_k) = \max\{t \in N: t \neq n_1a_1 + \ldots + n_ka_k\}, \quad (1)$$

где $n_1,\ldots,n_k \in N_0$. При $a_1 = 1$ любое число из N_0 представимо в виде линейной комбинации чисел набора A. В этом случае полагают:

$$f(1,a_2,\ldots,a_k) = -1. \quad (2)$$

При $k = 2$ и $\gcd(a_1,a_2) = 1$ формула числа Фробениуса известна:

$$f(a_1,a_2) = a_1a_2 - a_1 - a_2. \quad (3)$$

1. Основные свойства примитивных наборов натуральных чисел

Из определения примитивного набора чисел следуют свойства:

Утверждение 1. Если $A = (a_1,\ldots,a_k)$ — примитивный набор чисел, то примитивен любой набор, полученный из A либо добавлением любого натурального числа, либо при $k > 1$ удалением числа a, кратного одному из остальных чисел набора.

Доказательство. Для $b \in N$ при данных условиях $\gcd(a_1,\ldots,a_k,b) \leq \gcd(a_1,\ldots,a_k) = 1$. Следовательно, $\gcd(a_1,\ldots,a_k,b) = 1$.

Пусть при $k > 1$ какое-то число из примитивного набора A кратно некоторому другому числу, например $a_2 = ra_1$, где $r \in N$. Тогда выполнено:

$$1 = \gcd(a_1,\ldots,a_k) \leq \gcd(\{a_1,\ldots,a_k\}\setminus\{a_2\}) = d \geq 1. \quad (4)$$

Отсюда d делит любое число из множества $\{a_1,\ldots,a_k\}\backslash\{a_2\}$, вместе с тем d делит и a_2, так как $a_2 = ra_1$, значит, d делит $\gcd(a_1,\ldots,a_k)$. Следовательно, $d = 1$, т. е. множество $\{a_1,\ldots,a_k\}\backslash\{a_2\}$ примитивное.

Следствие. Набор A примитивен, если содержит пару взаимно простых чисел.

Набор из N^k назовем приведенным, если в наборе любое число не кратно любому другому числу. Иначе говоря, приведенный набор является антицепью в решетке натуральных делителей числа k_A, обозначаемой $D(k_A)$, где $k_A = \text{НОК}(a_1,\ldots,a_k)$.

Любому примитивному набору A размера $k \geq 1$ однозначно соответствует приведенный набор $\varpi(A)$ размера l, где $1 \leq l \leq k$: если в наборе A число a_j кратно a_i, то набор $\varpi(A)$ не содержит a_j (большее или равное число).

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

Все примитивные наборы длины 2, не содержащие 1, являются тупиковыми, так как при удалении одного из элементов набора остается число, отличное от 1. В соответствии с утверждением 1 примитивный тупиковый набор является приведенным набором.

Примитивный набор A размера $k > 1$ назовем r-примитивным, где $0 \leq r \leq k - 1$, если после удаления из A любого подмножества порядка r примитивность получившегося набора сохраняется. Тупиковый набор 0-примитивен, но не 1-примитивен.

Далее полагаем, что $A = (a_1,\ldots,a_k) \in N^k$ — приведенный набор, где $a_k \leq n$. Пусть 2^A — булеан множества $\{a_1,\ldots,a_k\}$, $P(A,k)$ — множество всех примитивных подмножеств порядка k из 2^A, $P(A) = \bigcup\limits_{1<k<n} P(A,k)$. Заметим, если A — примитивный приведенный набор, то все наборы из $P(A)$ также приведенные.

На множестве $P(A)$ определим отношение частичного порядка: $(b_1,\ldots,b_l) \leq (a_1,\ldots,a_k) \Leftrightarrow l \leq k$ и найдется бесповторная упорядоченная выборка $(i_1,\ldots,i_l)$ из $(1,\ldots,k)$, такая, что $i_1 <\ldots < i_l$ и b_j делит a_{i_j}, $j = 1,\ldots,l$.

Тупиковый набор $B \in P(A)$ назовем минимальным в $P(A)$, если не существует другого набора $B' \in P(A)$, такого, что $B' \leq B$. Для любого набора B из $P(A)$ имеется хотя бы один минимальный тупиковый набор $\theta(B)$, такой, что $\theta(B) \leq B$.

Тупиковый набор $B \in P(A)$ назовем 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 приведенный набор, то $\langle P(A),\leq\rangle$ — верхняя полурешетка, максимальный элемент которой есть A и любой минимальный элемент которой есть тупиковый минимальный набор.

Доказательство. Если наборы $A_1,A_2 \in P(A)$ и имеют размеры соответственно l и r, то их верхняя грань $\sup\{A_1,A_2\}$ определена как набор размера t упорядоченных по возрастанию элементов множества $A_1 \cup A_2$, где $\max\{l,r\} \leq t \leq r + l < n$. В соответствии с утверждением 1 $\sup\{A_1,A_2\}$ также есть примитивный набор из $P(A)$, т. е. $\langle P(A),\leq\rangle$ — верхняя полурешетка.

Утверждения о максимальном элементе и минимальных элементах полурешетки вытекают соответственно из определения множества $P(A)$ и из определения тупикового минимального набора.

Для приведенного набора A рассмотрим наибольший общий делитель как функцию, определенную на 2^A. При $B = \{a_{i_1},\ldots,a_{i_l}\} \in 2^A$ обозначим: $\gcd B = \gcd(a_{i_1},\ldots,a_{i_l})$, если $B \neq \varnothing$ и $\gcd\varnothing = \text{НОК}(a_1,\ldots,a_k)$; $D(A) = \{\gcd B : B \in 2^A\}$. Множество $D(A)$ частично упорядочено по отношению делимости: $\gcd B \leq \gcd B'$ для $B,B' \in 2^A \Leftrightarrow \gcd B$ делит $\gcd B'$.

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

Доказательство. Установим биективность функции $\gcd B: 2^A \to D(A)$, для этого достаточно убедиться в ее инъективности.

Предположим, что функция gcd$B$ не инъективна, т. е. найдутся множества $B_1,B_2 \in 2^A$, $B_1 \neq B_2$, такие, что gcdB_1 = gcdB_2 = d. Заметим, gcd$(B_1 \cup B_2)$ делит d в соответствии с определением функции gcd$B$. Вместе с тем d делит каждое из чисел множества $B_1 \cup B_2$. Значит, gcd$(B_1 \cup B_2) = d$.

Так как $B_1 \neq B_2$, то одно из этих множеств не включено в другое, пусть для определенности $B_2 \backslash B_1 \neq \varnothing$. Обозначим $B_3 = A \backslash (B_1 \cup B_2)$. В соответствии с определением функции gcd$B$ имеем цепь равенств:

$$1 = \gcd A = \gcd(B_1 \cup B_2 \cup B_3) = \gcd(\gcd(B_1 \cup B_2), B_3) = \gcd(d, B_3) = \gcd(\gcd B_1, B_3) = \gcd(B_1 \cup B_3). \quad (5)$$

Следовательно, множество $B_1 \cup B_3$ примитивное, где $B_1 \cup B_3 \subset A$, так как $B_2 \backslash B_1 \neq \varnothing$. Отсюда получаем противоречие с тупиковостью набора A.

В соответствии с определением функции gcd$B$, если $B \subset B'$, то gcdB' делит gcd$B$, значит, биекция $2^A \leftrightarrow D(A)$ антиизотонна.

2. Критерии тупиковости и k-минимальности наборов натуральных чисел

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

Теорема 1. Набор A — примитивный тупиковый $\Leftrightarrow$ $(\mu_1,\ldots,\mu_k)$ — набор попарно взаимно простых чисел, отличных от 1. При этом

$$a_i = c_i \mu_1 \ldots \mu_k / \mu_i, \quad (6)$$

где $(c_1,\ldots,c_k)$ есть 1-примитивный набор натуральных чисел и $\gcd(c_i,\mu_i) = 1$, $i = 1,\ldots,k$.

Доказательство. Пусть набор A — примитивный тупиковый. Если $\mu_i = 1$ при некотором $i \in \{1,\ldots,k\}$, то множество A_i — примитивное, что противоречит тупиковости набора A. Если $\gcd(\mu_i,\mu_j) = d > 1$ при $i \neq j$, то d делит все числа множеств A_i и A_j, значит, d делит все числа набора A, что противоречит примитивности набора A.

Докажем достаточность. Если набор A не примитивный, то $\gcd A = d > 1$. Отсюда d делит μ_i при любом $i = 1,\ldots,k$, значит, числа $\mu_1,\ldots,\mu_k$ не являются попарно взаимно простыми, т. е. имеем противоречие. Если набор A не тупиковый, то $\mu_i = 1$ при некотором $i \in \{1,\ldots,k\}$, что противоречит условию.

По определению чисел $\mu_1,\ldots,\mu_k$ число a_i делится на каждое из чисел множества $\{\mu_1,\ldots,\mu_k\} \backslash \{\mu_i\}$, следовательно, для $i = 1,\ldots,k$ верно (6), где $(c_1,\ldots,c_k) \in N^k$.

Заметим, набор $(c_1,\ldots,c_k)$ — примитивный, иначе набор A не примитивный в силу (6). Если $\gcd(c_i,\mu_i) = d > 1$ при некотором $i \in \{1,\ldots,k\}$, то d делит все числа набора A в соответствии с (6) и с определением чисел $\mu_1,\ldots,\mu_k$, что противоречит примитивности набора A. Следовательно, $\gcd(c_i,\mu_i) = 1$ при любом $i = 1,\ldots,k$. Из (6) и определения чисел $\mu_1,\ldots,\mu_k$ следует также, что

$$\mu_i = \gcd(\{c_1\mu_2\ldots\mu_k,\ldots,c_k\mu_1\ldots\mu_{k-1}\} \backslash \{c_i\mu_1\ldots\mu_k/\mu_i\}). \quad (7)$$

Каждое число множества $\{c_1\mu_2\ldots\mu_k,\ldots,c_k\mu_1\ldots\mu_{k-1}\} \backslash \{c_i\mu_1\ldots\mu_k/\mu_i\}$ делится на μ_i. Тогда из (7) следует, что $\gcd(\{c_1,\ldots,c_k\} \backslash \{c_i\} = 1$, $i = 1,\ldots,k$, значит, $(c_1,\ldots,c_k)$ есть 1-примитивный набор.

Следствие 1. Пусть $B = \{a_{i_1},\ldots,a_{i_l}\} \in 2^A$ и $\overline{B} = A \backslash B$, тогда

$$\gcd B = \gcd\{c_{i_1},\ldots,c_{i_l}\} \cdot \prod_{j \in \overline{B}} \mu_j. \quad (8)$$

Доказательство. Заметим, если $c_1,\ldots,c_k,x_1,\ldots,x_k \in N$, то $\gcd(c_1x_1,\ldots,c_kx_k)$ делится на $\gcd(\{c_1,\ldots,c_k\} \cdot \gcd(x_1,\ldots,x_k)$. Отсюда, положив $x_i = \mu_1\ldots\mu_k/\mu_i$, $i = 1,\ldots,k$, в соответствии с (6) получаем, что gcd$B$ делится на $\gcd\{c_{i_1},\ldots,c_{i_l}\} \cdot \gcd\{x_{i_1},\ldots,x_{i_l}\}$, где из теоремы 1 следует, что $\gcd\{x_{i_1},\ldots,x_{i_l}\} = \prod_{j \in B} \mu_j$.

Без ущерба для общности положим $B = \{a_1,\ldots,a_l\}$, где $1 \leq l \leq k$, и обозначим: $c' = \gcd(c_1,\ldots,c_l)$, $x' = \gcd(x_1,\ldots,x_l)$, в этих условиях множества $C' = \{c_1/c',\ldots,c_l/c'\}$ и $X' = (x_1/x',\ldots,x_l/x')$ — примитивные.

Пусть $\gcd B = d \cdot c' \cdot x'$ при натуральном $d > 1$, тогда $\gcd B' = d$, где $B' = \{a_1/c'x', \ldots, a_l/c'x'\}$. Следовательно, d делит $c_r x_r / c'x'$ при $r = 1,\ldots,l$, отсюда

$$d = d(c_r) \cdot d(x_r), \tag{9}$$

где $d(c_r)$ делит c_r/c' и $d(x_r)$ делит x_r/x'. В силу примитивности множества C' найдется номер $r \in \{1,\ldots,l\}$, такой, что $d(x_r) > 1$. Тогда, учитывая, что $x_i/x' = \mu_1 \ldots \mu_l/\mu_i$, $i = 1,\ldots,l$, и числа $\mu_1 \ldots \mu_l$ попарно взаимно простые, найдется номер $j \in \{1,\ldots,l\}$, такой, что $\gcd(d(x_r),\mu_j) = d_{rj} > 1$, значит, d_{rj} делит d. Заметим, $\gcd(x_j/x',\mu_j) = 1$, значит, $\gcd(x_j/x',d_{rj}) = 1$, отсюда в силу (8) d_{rj} делит $d(c_j)$, поэтому d_{rj} делит c_j/c'.

Вместе с тем в соответствии с теоремой 1 $\gcd(c_j,\mu_j) = 1$, тогда $\gcd(d(c_j),d_{rj}) = 1$. Имеем противоречие. Следовательно, $d = 1$.

Представление целого числа n произведением степеней простых чисел $\rho_1,\ldots,\rho_s$:

$$n = \varepsilon\, p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \tag{10}$$

где $\varepsilon = \pm 1$, $k_i > 0$ — кратность числа ρ_i, $i = 1,\ldots s$, называется каноническим разложением числа n, при этом множество чисел $\{\rho_1,\ldots,\rho_s\}$ называется факторной базой числа n, обозначается: $F(n) = \{\rho_1,\ldots,\rho_s\}$. Факторной базой набора A (обозначается $F(A)$) назовем множество чисел:

$$F(A) = F(a_1) \cup \ldots \cup F(a_k). \tag{11}$$

Докажем критерий k-минимальности тупикового примитивного набора.

Следствие 2. Примитивный тупиковый набор A является k-минимальным $\Leftrightarrow$ $(\mu_1,\ldots,\mu_k)$ — набор простых чисел, $c_i = 1$, $i = 1,\ldots,k$.

Доказательство. Пусть A есть k-минимальный набор и каноническое разложение μ_i при некотором $i \in \{1,\ldots,k\}$ имеет вид: $\mu_i = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$. Рассмотрим набор B, состоящий из чисел $\mu_1,\ldots,\mu_{i-1},\mu_{i+1},\ldots,\mu_k$, $\mu_i' = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s - 1}$. Согласно (6) $B \le A$, причем его длина равна k. Тогда A не является k-минимальным. Если $c_i > 1$ при некотором $i \in \{1,\ldots,k\}$, то существует набор B', которому соответствуют $c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_k$, $c_i' = 1$. Согласно (6) $B' \le A$, что противоречит k-минимальности. Следовательно, $(\mu_1,\ldots,\mu_k)$ — набор простых чисел, и $c_i = 1$, $i = 1,\ldots,k$.

Если набор не является k-минимальным, то существует набор $A' = (a_1',\ldots,a_k')$, такой, что $A' \le A$. Согласно (6) $a_i' = c_i'\mu_1' \ldots \mu_k'/\mu_i'$, $i = 1,\ldots,k$, причем c_i' делит c_i или μ_j' делит μ_j при некотором $i,j \in \{1,\ldots,k\}$. Тогда $c_i > 1$ или μ_j — составное соответственно.

Следствие 3. Факторная база k-минимального тупикового набора есть $\{\mu_1,\ldots,\mu_k\}$.

Примеры k-минимальных тупиковых примитивных наборов:

– 3-минимальные наборы $A = (6,10,15)$, $F(A) = \{2,3,5\}$; $B = (10,14,35)$, $F(B) = \{2,5,7\}$;

– 4-минимальный набор $C = (30,42,70,105)$, $F(C) = \{2,3,5,7\}$.

3. Перечисление примитивных наборов натуральных чисел

Обозначим через PR_m множество всех примитивных наборов, элементы которых не превышают натуральное число m. Построим алгоритм перечисления множества PR_m.

Ограничимся наборами размера m, так как любой набор из PR_m имеет размер не более m. По утверждению 1 любой примитивный набор A можно получить из соответствующего тупикового набора A' добавлением любого числа. По следствию 2 теоремы 1 любой тупиковый набор A' можно получить из соответствующего k-минимального набора A'' умножением элемента набора a_i на отличное от μ_i число, взаимно простое с μ_j, $i \in \{1,\ldots,k\}$, $j = 1,\ldots,i-1,i+1,\ldots,k$. Очевидно, если $A \in PR_m$, то $A' \in PR_m$ и $A'' \in PR_m$.

По следствию 2 теоремы 1 набор размера 2 является 2-минимальным $\Leftrightarrow$ он представляет собой пару простых чисел. Таким образом, задача сводится к перечислению k-минимальных тупиковых примитивных наборов из PR_m размера $k > 2$.

В соответствии с теоремой 1 и ее следствием 2 k-минимальный тупиковый примитивный набор $A = (a_1,\ldots,a_k)$ состоит из чисел $a_i = \mu_1\ldots\mu_k/\mu_i$, где $(\mu_1,\ldots,\mu_k)$ — набор простых чисел. Основываясь на данном свойстве, построим алгоритм перечисления.

Пусть $P(x)$ — множество простых чисел, не больших x. Известно [4], что

$$\varpi(x) = |P(x))| \approx x/\ln x. \quad (12)$$

Искомые наборы $(a_1,\ldots,a_k)$ состоят из произведений простых чисел вида $\mu_1\ldots\mu_k/\mu_i$, где $\mu_1\ldots\mu_k/\mu_i \le m$, $k > 2$. Так как наименьшими простыми числами являются 2 и 3, то

$$\max(\mu_1,\ldots,\mu_k) \le 2m/3. \quad (13)$$

Алгоритм состоит в следующем: для каждой выборки $(\mu_1,\ldots,\mu_k)$ из $P(2m/3)$ размера $k = 3,\ldots,\varpi(2m/3)$, упорядоченной по возрастанию, проверяем условие $\mu_1\ldots\mu_k/\mu_i \le m$. Если условие выполнено, строим набор по правилу: $a_i = \mu_1\ldots\mu_k/\mu_i$, $i = 1,\ldots,k$.

Оценим вычислительную сложность алгоритма в условиях однопроцессорного вычислителя. В качестве элементарной операции рассмотрим построение одной произвольной выборки. Количество выборок размера k равно $C^k_{\pi(2m/3)}$. Тогда общее количество выборок размера $k = 3,\ldots,\varpi(2m/3)$ не превышает $2^{\varpi(2m/3)}$. Вычислительная сложность алгоритма имеет порядок $O(2^{\varpi(2m/3)})$.

Пусть теперь числа $a_1,\ldots,a_k$ не ограничены. Получим нижнюю оценку для наибольшего числа в k-минимальном тупиковом примитивном наборе.

Если набор $(\mu_1,\ldots,\mu_k)$ упорядочен по возрастанию, то

$$\max(a_1,\ldots,a_k) = \mu_1\ldots\mu_k/\mu_1. \quad (14)$$

Известна оценка для n-го простого числа [5]: $\rho_n > n\ln n$. Следовательно,

$$\max(a_1,\ldots,a_k) > k!\cdot\ln 2\cdot\ldots\cdot\ln k. \quad (15)$$

Точные числовые границы для $k = 3,\ldots,8$, посчитанные с помощью (14), приведены в таблице 1.

Таблица 1. Числовые границы для наборов длины k

Размер набора k	**Нижняя граница $\max(a_1,\ldots,a_k)$**
3	15
4	105
5	1155
6	15015
7	255255
8	4849845

Оценки (13) и (15) могут быть уточнены.

СПИСОК ЛИТЕРАТУРЫ:

1. *Фомичев В. М.* Оценки экспонентов примитивных графов. // Прикладная дискретная математика. 2011. № 2 (12). С. 101–112.
2. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
3. *Биркгоф Г.* Теория решеток. М.: Наука, 1984.
4. *Коблиц Н.* Курс теории чисел и криптографии. М.: ТВП, 2001.
5. *Rosser B.* The n-th prime is greater than n*log n. // Proc. London Math. Soc. 1939. Vol. 45. P. 21–44.