Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

II СЕМЕСТР

Лектор: *Райгородский*

h\nu

Автор: *Киселев Николай*
Репозиторий на Github

весна 2025

Содержание

«««< HEAD

1 Динамическое программирование (окончание)

1.1 ДП с помощью масок

Пусть $U = \{0, 1, \dots, n-1\}$ $A \subset U$

Тогда будем записывать A как массив длины n, где $i \in A \leftrightarrow a_i = 1$. Такое представление называется *маской множества*

Как проверить входит ли x в A?

```
bit(mask, pos) {
  return (mask » pos) & 1; }
```

Как брать пересечения и объединения?

$A \cap B$	$A \cup B$
$mask_A \| \| mask_B$	$mask_A \& mask_B$

1.1.1 Задача 1

Пусть даны a_{ij} - стоимость выполнения j-го задания i-ым работников. Найти минимальную стоимость выполнения всех заданий.

Решение:

Пусть $dp[i][mask]$ - минимальная стоимость распределить первых i работников, чтобы они выполнили множество заданий маски.

$$dp[i][mask] = min_{b \in mask}(a_{ib} + dp[i-1][\underbrace{mask|b}_{mask+(1<<b)}])$$

Асимптотика: $O(2^n n^2)$

1.1.2 Задача 2

Максимальная клика в графе за $O(2^{\frac{n}{2}})$

Определение 1.1. Клика $C \subset V$ такова, что для любых ее двух вершин есть ребро между ними.

Решим пока задачу за $O(2^k)$, где k - количество вершин

Обозначим за $neighbour(v)$ маску соседей v

Тогда $clique(mask) = true \leftrightarrow clique(mask|v) = true, mask|v \subset neighbour(v)$

Осталось только придумать, как из маски за $O(1)$ выкидывать ее вершину.

Сделаем это предпосчетом для каждой маски за $O(2^k)$, записывая последовательно ее старший бит.

1.1.3 Задача 3

Найти максимальную клику в маске.
Решение:

1. Если clique(mask) == true, то subclique(mask) = |mask|
2. Возьмем максимальное значение из:
   (a) subclique(mask | v) - не берем v
   (b) 1 + subclique(mask & neighbour(v)) - берем v

Такое тоже работает за $O(2^k)$
Теперь мы готовы решить основную задачу...

Шаг 1 Разобьем граф на 2 половинки, где будем искать клики. Пусть $corr[mask]$ - множество вершин правой доли, которые соединены со всеми вершинами mask.

Шаг 2 Хотим добавить их к mask, чтобы получилась клика. Единственное требование - все выбранные вершины $corr[mask]$ должны быть кликой –> А это ведь Задача 3!!!

То есть ответ будет состоять из $max(|mask| + subclique(mask))$, где mask - клика из левой части. Осталось понять, как считать $corr[mask]$

Шаг 0 $corr[mask] = corr[mask|v]\ \&\ neighbour(v)$

1.2 ДП по профилю

1.2.1 Задача 1

Пусть есть доска $n \times m$, сколько существует способов покрыть ее доминошками.
$dp[j][mask]$ - количество способов полностью покрыть j столбцов, т. ч. mask - множество строк, где лежат "торчащие"доминошки.
"Торчащие"доминошки - те, что расположены в j и $j + 1$ столбцах.

1. База: $dp[0][0] = 1, dp[0][\neq 0] = 0$
2. Переход: Обозначим за old_mask маску на $j - 1$ столбце. Переберем по всевозможным old_mask.
3. Заметим, что, зафиксировав mask и old_mask, картинка полностью заполняется. Добавляем $dp[i - 1][old]$ к $dp[j][mask]$, если
   (a) old $\cap$ mask = 0
   (b) В old $\cup$ mask все блоки из нулей-четной длины

Получаем асимптотику $O(4^n m)$, но можно подправить на $O(3^n m)$, если не рассматривать случаи $old \cap mask = 1$ в каком-то бите.

1.3 Изломанный профиль

Считаем, что профиль - теперь часть доски, покрытая доминошками по предположению.

Комментарий: Раньше профиль получался из целых столбцов, а теперь нет

=======

2 ОТА

Эту часть конспекта для вас затеха: Иван Бирюков

Теорема 2.1.

1) $\forall n > 1$ $\exists!$ его представление в виде

$$n = p_1 p_2 \dots p_s$$

Комментарий: $p_1, p_2, \dots, p_s$ - простые числа, единственность с точностью до порядка множителей

2) p_i - i-ое простое число Тогда $\forall n$ $\exists!$ $(\alpha_1, \alpha_2, \dots, \alpha_n)$:

$$n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$$

Следствие. $\nu_p(n)$ - max степень вхождения p в $n \Longrightarrow n \not\vdots p^{\nu_p(n)+1}$

Сейчас мы приведем несколько доказательств этой теоремы

2.1 Первое доказательство (не было доведено)

Доказательство. Найдем существование разложения по индукции по n:

База: $n = 2$. Переход: $n = ab \to \left(p_{a_1}^{\alpha_{a_1}} p_{a_2}^{\alpha_{a_2}} \dots p_{a_s}^{\alpha_{a_s}}\right) \cdot \left(p_{b_1}^{\alpha_{b_1}} p_{b_2}^{\alpha_{b_2}} \dots p_{b_k}^{\alpha_{b_k}}\right)$ или n - простое

Осталось понять единственность.

Пойдем от противного: пусть $\exists$ min $n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_k$

Для простоты упорядочим простые числа в обоих разложениях.

Если $p_1 = q_1$, то у числа $\frac{n}{p_1}$ есть 2 разложения. Значит, $p_1 \neq q_1 \to n \geqslant p_1 p_2 \geqslant p_1^2$

Аналогично получается $n \geqslant q_1^2 \to n \geqslant max(p_1^2, q_1^2) \geqslant q_1(p_1 + 2) > q_1 p_1 + 1$

Рассмотрим число $x = n - p_1 q_1$. Оно меньше n и больше 1, а тогда у него есть единственное разложение на простые сомножители $\tau_1, \tau_2, \dots, \tau_m$:

$x = p_1(p_2 \dots p_s - q_1) = q_1(q_2 \dots q_k - p_1) = \tau_1 \dots \tau_m$, в наборе $\tau : \tau_1 \leqslant \dots \leqslant p_1 \leqslant q_1 \leqslant \tau_m$ □

2.2 Второе доказательство

Лемма 2.1 (Евклида)**.** *p - простое. Тогда $mn \vdots p \to m \vdots p$ или $n \vdots p$*

Лемма 2.2 (Евклида 2.0)**.** *$(m, k) = 1, mn \vdots k \to n \vdots k$*

$2 \Longrightarrow 1$:. $k = p, m \not\vdots p \to (m, p) = 1 \to n \vdots k$ □

Доказательство. Докажем единственность по лемме Евклида:

$n = p_1 \underbrace{\ldots p_s}_{m} = q_1 \ldots q_l$

По лемме Евклида $p_1 = q_1$ или $m \vdots q_1$. Повторяя процедуру, получим, что $p_i = q_1$, сократим на него и повторим алгоритм. □

Докажем теперь лемму Евклида 2.0

Доказательство. По линейному представлению НОДа $\exists x\ \exists y:\ mx+ky=1$

$$mx+ny=1 \to \underbrace{mn}_{\vdots k}x+\underbrace{k}_{\vdots k}ny=n \to n\vdots k$$

□

Доказательство этой же леммы через идеалы:

Определение 2.1. I - идеал в $\mathbb{Z}$, если:

1. $\forall a, b\ \in I : a+b=I$
2. $\forall a\ \in I\ \forall b\ \in \mathbb{Z} : ab \in I$

Доказательство. Зафиксируем m и определим $I_m = \{a \mid ma \vdots p\} \to n$, p *лежат в идеале*

Лемма 2.3. *Пусть d - минимальное положительное число в I*
Тогда $I = \{cd \mid c \in \mathbb{Z}\}$

Следует из деления элемента с остатком □

А тогда $d=1$ или $d=p$. Во втором случае $n\vdots p$, в первом - $m \ldots p$
»»»> 574fc0c2d8f10f22df24bae7ee15b18ccf992e4e