

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

БОЛЬШОЕ НАЗВАНИЕ КУРСА
V СЕМЕСТР

Лектор: *Иван Иванович Иванов*

$h \backslash nu$

Автор: *Павел Дуров*
Репозиторий на Github

осень 2022

Содержание

1	Продолжение ДП	2
1.1	Рюкзак с оптимизацией	2
1.1.1	Альтернативный вариант	2
1.2	Динамическое программирование с помощью матриц	2
1.3	Задача	3
1.4	Задача	3
1.5	Задача	4
2	Матрицы Адамара	4
3	Коды, исправляющие ошибки	6

1 Продолжение ДП

1.1 Рюкзак с оптимизацией

→ w предметов

→ w_i - вес

→ c_i - стоимость

Решение мы помним с прошлой лекции, а сейчас займемся оптимизацией памяти:

$dp[i][o]$ зависят только от $dp[i-1][o]$, поэтому нам достаточно хранить не всю таблицу целиком, а всего 2 слоя, с которыми мы работаем.

Итог - память $O(W)$

1.1.1 Альтернативный вариант

Будем действовать от стоимости предметов:

1. Заводим массив $dp[0 \dots n-1][0 \dots C-1]$, где $C = \sum_{i=0}^{n-1} c_i$
2. $dp'[i][b]$ - min суммарный вес предметов, имеющих номера $\leq i$, и общую стоимость b
3. $dp'[i][b] = \min(dp[i-1][b], dp'[i-1][b-c_i] + w_i)$

Это используется, если суммарная стоимость значительно меньше суммарного веса.

1.2 Динамическое программирование с помощью матриц

Попробуем найти $F_n = F_{n-1} + F_{n-2}$ с методом матриц.

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F_{n-1} \\ F_{n-2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F_{n-2} \\ F_{n-3} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \cdot \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}$$

БИНАРНОЕ ВОЗВЕДЕНИЕ МАТРИЦЫ В СТЕПЕНЬ

Проводится так же, как и для натуральных чисел:

$$a^n = \begin{cases} 1, & \text{если } n = 0 \\ \left(a^{\frac{n}{2}}\right)^2, & \text{если } n \text{ четно} \\ a \cdot a^{n-1}, & \text{если } n \text{ нечетно} \end{cases} \quad (1.1)$$

Если две матрицы имеют размеры $k \times k$, то их произведение можно найти за $O(k^3)$

Тогда A^n описанным алгоритмом находится за $O(k^3 \log n)$

Задача $a_n = \lambda a_{n-1} + \mu a_{n-2} + 1$

$$\begin{pmatrix} a_n \\ a_{n-1} \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda & \mu & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ 1 \end{pmatrix}$$

Взяв произведение этих матриц, получим ответ за $O(3^3 \log n)$

Задача Пусть G – невзвешенный ориентированный граф. Найти количество путей длины ровно k из вершины x в вершину y

На ввод дается матрица смежности M , где $m_{ij} = 1 \Leftrightarrow$ есть ребро $i \rightarrow j$, а 0 иначе.

Пусть $dp[v][l]$ – количество путей длины l от x до v .

Тогда $dp[v][l] = \sum_{u \in v: M_{uv}=1} dp[u][l-1]$

$$\begin{pmatrix} dp[1][l] \\ dp[2][l] \\ \vdots \\ dp[v][l] \\ \vdots \\ dp[n][l] \end{pmatrix} = M^T \cdot \begin{pmatrix} dp[1][l-1] \\ dp[2][l-1] \\ \vdots \\ dp[v][l-1] \\ \vdots \\ dp[n][l-1] \end{pmatrix}$$

Комментарий от эксперта:

Пересчет динамики получается домножением столбца $dp[v][i-1]$ на транспонированную матрицу смежности слева

Утверждение 1.1. M^k – количество путей из u в v длины ровно k .

1.3 Задача

Найти количество путей длины $\leq k$ из x в y .

Можно найти ответ из суммы $(M^0 + M^1 + \dots + M^k)_{xy}$, но как ее посчитать быстро?

Введем $f(M, k) = (M^k, M^0 + M^1 + \dots + M^{k-1})$.

1. $k = 0 \rightarrow f(M, k) = (E, E)$
2. $k \neq 2 \rightarrow f(M, k-1) = (M^{k-1}, M^0 + M^1 + \dots + M^{k-2})$, откуда $f(M, k) = f(M, k-1)$, в котором умножили первый элемент на M , предварительно прибавив его ко второму.
3. $k \geq 2$, $f(M, k)$ получается из $f(M, \frac{k}{2})$ умножением первой части, увеличенной на 1, на вторую и возведением первой части в квадрат.

ВТОРОЙ КОММЕНТАРИЙ ОТ ЭКСПЕРТА:

По формуле геометрической прогрессии $\sum_{i=0}^k M^i = (M^{k+1} - E) \cdot (M - E)^{-1}$. Если $M - E$ необратима, подкрутим её коэффициент на 0.00001.

1.4 Задача

Пусть G – граф. Надо проверить, есть ли хотя бы 1 путь из x в y длины ровно k ?

$$d[v][l] = \bigvee_u (dp[u][l-1] \wedge M_{uv})$$

Обозначим $A * B = C$, где $*$ – булево умножение, такое выражение:

$$c_{ij} = \bigvee_k (A_{ik} \wedge B_{kj})$$

Утверждение 1.2. $M_{uv}^{*k} = 1$, если есть путь $u \rightarrow v$, а иначе 0

Такое тоже работает за $O(n^3 \log k)$

1.5 Задача

G - взвешенный граф. Хотим найти \min стоимость пути длины ровно k из x в y .

Пусть $dp[v][l]$ - минимальная стоимость пути $x \rightarrow v$ за l ребер. Тогда его можно найти по формуле $\min(dp[u][l-1] + cost(u, v))$

Обозначим: $A \circ B = C$, где

$$c_{ij} = \min_k (a_{ik} + b_{kj})$$

$$(A \circ B) \circ C = A \circ (B \text{ circ } C)$$

Утверждение 1.3. $M^{\circ k}$ - минимальная стоимость пути из u в v , используя ровно k ребер.

2 Матрицы Адамара

Определение 2.1. Матрицей Адамара называется матрица A , если и только если

$$[A]_{ij} \in \{1, -1\}$$

И ее строки попарно ортогональны (то есть скалярное произведение любых двух строк равно 0)

Пример. 1. $n = 1$ — очев

2. $n = 2$:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

3. $n = 2$:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Замечание. $n \geq 2 \Rightarrow n = 2k$

Доказательство. Очевидно, т.к. если мы перемножим любые две строки, то тогда в скалярном произведении придется сложить нечетное количество ± 1 , тогда эта сумма точно не будет равна 0. \square

Утверждение 2.1. Если у матрицы попарно ортогональны строчки, то и столбцы — тоже

Определение 2.2. Нормальная форма матрицы Адамара: когда $A_1 = A^1 = (1, 1, \dots, 1)$

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm 1 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm 1 & \dots & \pm 1 \end{pmatrix}$$

Замечание. Любую матрицу адамара можно привести к нормальному виду путем домножения строк и столбцов на -1 .

Теорема 2.1. $n > 2 \Rightarrow n = 4k$

Доказательство. Приведем матрицу Адамара к нормальному виду. Теперь переставим столбцы, чтобы вторая строчка была вида

$$(1, \underbrace{1 \dots 1}_{\frac{n}{2}}, \underbrace{-1, -1, \dots -1}_{\frac{n}{2}})$$

А третья строка была вида

$$(1, \underbrace{1 \dots 1}_x, \underbrace{-1, -1, \dots -1}_{\frac{n}{2}-x}, \underbrace{1, 1 \dots 1}_{\frac{n}{2}-x}, \underbrace{-1, -1, \dots -1}_x)$$

Тогда скалярное произведение второй и третьей будет равно

$$x - \left(\frac{n}{2} - x\right) - \left(\frac{n}{2} - x\right) + x = 4x - n = 0$$

Тогда $x=4$

□

Теорема 2.2. (Гипотеза Адамара) Если $n = 4k$, то матрица Адамара существует.

Доказательство. Не доказана

□

Определение 2.3. Кронекеровское произведение матриц $A * B = C \Rightarrow$

$$C = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \in M_{mn \times mn}$$

Утверждение 2.2. Кронекеровское произведение двух матриц Адамара есть матрица Адамара

Доказательство. Скалярное произведение двух строк равняется

$$\sum_{k=1}^n \left(\sum_{s=1}^m a_{ik} a_{jk} b_{i's} b_{j's} \right) = \sum_{k=1}^n a_{ik} a_{jk} \left(\sum_{s=1}^m b_{i's} b_{j's} \right) = (B_{i'}, B_{j'}) \left(\sum_{k=1}^n a_{ik} a_{jk} \right) = (B_{i'}, B_{j'})(A_i, A_j) \neq 0$$

□

Теорема 2.3 (Пэли). Пусть $p = 4k + 3$ — простое число. Тогда \exists матрица Адамара порядка $p + 1$.

Доказательство. Рассмотрим матрицу порядка p , такую, что $A_{ab} = \left(\frac{a-b}{p}\right)$ (символ Лежандра). Тогда произведение любых двух строк i, j равно

$$\sum_{b=1}^p \left(\frac{i-b}{p}\right) \left(\frac{j-b}{p}\right)$$

$c = i - b$.

$$\sum_{c=1}^p \left(\frac{c}{p}\right) \left(\frac{c-i+j}{p}\right)$$

Причем, $c = p \Rightarrow \left(\frac{c}{p}\right) = 0$

$$\sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \left(\frac{c-i+j}{p}\right) = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \left(\frac{c(1+c^{-1}(i-j))}{p}\right) = \sum_{c=1}^{p-1} \left(\frac{1+c^{-1}(i-j)}{p}\right)$$

При этом, $i-j, c^{-1} \not\equiv_p 0 \Rightarrow$ выражение $1+c^{-1}(i-j)$ пробегает все остатки $\bmod p$, кроме 1. Но тогда итоговая сумма равна $0 - \left(\frac{1}{p}\right) = -1$. Тогда рассмотрим такую матрицу:

$$C = \left(\begin{array}{c|ccc} 1 & 1 & \dots & 1 \\ \hline 1 & & & \\ \vdots & & A & \\ 1 & & & \end{array} \right)$$

Где все нули в A заменены на -1 (получится матрица A' , причем замены произойдут только на главной диагонали). Докажем, что она подходит. Заметим, что в матрице A' поровну 1 и -1 . Тогда скалярное произведение с первой строчкой точно будет 0. Возьмем строчки i, j в матрице A' . В их скалярном произведении добавилась $(-1)\left(\frac{i-j}{p}\right) + (-1)\left(\frac{j-i}{p}\right) = 0$. Теперь посчитаем скалярное произведение любых двух строк, к нему просот добавится 1 за счет первого столбца. Тогда это будет матрицей Адамара. \square

Теорема 2.4 (Пэли). Пусть $p = 4k + 1$ — простое число. Тогда \exists матрица Адамара порядка $2(p+1)$.

Теорема 2.5 (б/д). $\forall \varepsilon > 0 \exists n_0 : \forall n > n_0$ на отрезке $[n, (1 + (1 + \varepsilon)n)]$ есть порядок матрицы Адамара

Теорема 2.6 (переформулировка, тоже б/д). $\exists f : f(n) = o(n)$, такая, что на отрезке $[n, n + f(n)]$ есть порядок матрицы Адамара

3 Коды, исправляющие ошибки

Представим ситуацию: разговариваем с бабушкой. Еще мы с ней общаемся азбукой морзе (отправляем ей 0 или 1) и передаем ей сообщения длины n . Известно, что бабушка неправильно услышит не более чем k циферок. Как тогда с ней общаться?

Определение 3.1. Расстояние Хэмминга между словами — количество несовпадающих координат

Тогда нам, по сути, надо расположить непересекающиеся "шары" радиуса k , состоящие из слов. В таком случае мы сможем определить, какое слово мы передали, т.к. оно будет лежать не более, чем в одном шаре.

Определение 3.2. (n, M, d) -код — такой словарь, в котором M слов, каждое из которых имеет длину n и минимальное расстояние между любыми двумя словами равно d .

Теорема 3.1 (Граница Плоткина). Пусть дан (n, M, d) -код, где $2d > n$. Тогда $M \leq \frac{2d}{2d-n}$.

Доказательство неулучшаемости оценки. Рассмотрим матрицу Адамара:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm 1 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm 1 & \dots & \pm 1 \end{pmatrix}$$

И зачеркнем в ней первый столбец. Будем рассматривать строки как слова. Тогда расстояние Хэмминга между ними равно $\frac{n}{2}$ (т.к. скалярное произведение любых двух равно 0). Тогда получили $(n-1, n, \frac{n}{2})$. Но тогда плоткин дает результат $\frac{2^{\frac{n}{2}}}{2^{\frac{n}{2}} - (n-1)} = n$, т.е. мы нашли пример, который точно подходит под оценку. \square