Звёздочка №5

Автор: Батраков Ю.А. ФПМИ МФТИ, группа Б05-911.

Постановка задачи

Предложите метод перемножения двух матриц размера n x n над Z_2 за $o(n^3)$ (о-малое!). Используйте метод четырёх русских.

Решение

Переформулировка

Итак, у нас есть две матрицы (пусть A и B) вообще говоря, не обязательно квадратные, элементы которых либо 0, либо 1. Необходимо перемножить их методом "четырёх русских" асимптотически быстрее, чем за $O(n^3)$.

Алгоритм

Предобработка

Выберем какое-то натуральное число k, пока не важно какое, но именно это число в будущем и улучшит асимптотику.

Теперь рассмотрим все возможные комбинации 0 и 1 длины k и назовём его $M = (Z_2)^k$ (будем строить M упорядоченным по возрастанию). Очевидно, таких комбинаций $|M| = 2^k$ штук.

Составим для M "таблицу умножения". То есть определим скалярное произведение по модулю 2 для каждого элемента на каждый элемент из M. Получится матрица $\Gamma = 2^k \times 2^k$, т.е. на 4^k элементов. Отметим также, что вычисление скалярного произведения будет производится за длину кортежа, т.е. за k.

Запрос

I) Возьмём любую матрицу, из поступивших в запросе, например, A (размерности $m \times n$). Разделим каждую её строку на вектора размера k (в конце может остаться меньше чем k элементов, в таком случае доопределим их нулями справа в конце, это не изменит скалярного произведения). Для каждого вектора найдём его номер в M. Получим матрицу A′ размеров $m \times \lceil \frac{n}{k} \rceil$.

II) Возьмём другую матрицу из запроса, соотвественно, B (размерности $n \times p$). Аналогично первой матрице разделим её столбцы на битовые вектора и получим матрицу B' размеров $\lceil \frac{n}{k} \rceil \times p$.

III) Перемножим A' и B' стандартным матричным умножением. Это можно сделать так как для любого любого элемента M определено произведение на любой другой элемент из M по матрице Γ (произведение двух элементов считается за $O(1)$ так как известны их номера в M). Полученный результат и будет произведением исходных матриц.

Корректность

Для удобства обозначений, примем $C = A \times B$, $C' = A' \times B'$. Докажем, что $C = C'$.

Во-первых, заметим, что размерность C совпадает с размерностью C'. Тогда остаётся установить поэлементное равенство.

Во-вторых, рассмотрим элемент матрицы C: $c_{ij} = \sum_{d=1}^{n} a_{id} * b_{dj}$, т.е. скалярное произведение i-ой строки A на j-ый столбец B и соотвествующий элемент матрицы C': $c'_{ij} = \sum_{d=1}^{\lceil \frac{n}{k} \rceil} a'_{id} * b'_{dj}$, т.е. скалярное произведение i-ой строки A' на j-ый столбец B'. Но из того, как мы определяли A' и B' следует, что $a'_{id} * b'_{dj}$ равно скалярному произведению отрезков $[a_{k*i,d}, a_{k*(i+1)-1,d}]$ и $[b_{d,k*j}, b_{d,k*(j+1)-1}]$, т.е. $\sum_{t=1}^{k} a_{k*i+t,d} * b_{d,k*j+t}$ (возможно с учётом нулей, которые добавлялись в конце строки у A и столбца у B. Так как фиктивные элементы отмечались нулями, то они не дадут никакого вклада в сумму). Поэтому вторая сумма просто преобразуется к $\sum_{d=1}^{\lceil \frac{n}{k} \rceil} \sum_{t=1}^{k} a_{k*i+t,d} * b_{d,k*j+t} = \sum_{d=1}^{n} a_{id} * b_{dj} = c_{ij}$.

Следовательно, размерности матриц C и C' совпадают, и матрицы совпадают поэлементно, значит $C = C'$. Ч.Т.Д.

Асимптотика

Именно здесь на сцену выходит k.

Оценим асимптотику предобработки. Необходимо посчитать 4^k скалярных произведений, каждое из которых вычислятся за k операций. Таким образом предобработка требудет $\theta(4^k * k)$ операций. Отметим также, что если k не больше длины машинного слова, то предобработку можно ускорить засчёт побитовых операций.

Немного лирики. Поиск номера нужного нам кортежа в M можно делать за $\theta(k)$ операций! Всё очень просто, мы по сути будем осущствлять бинарный поиск по M. Таким образом так как бинарный поиск работает за логарифм от длины последовательности, т.е. в нашем случае за $\theta(log(4^k)) = \theta(k)$.

Преобразование из A в A' требует в каждой строке для каждого отрезка длины k (которых $\lceil \frac{n}{k} \rceil$) найти его номер в M, поэтому занимает $\theta(m * \frac{n}{k} * k) = \theta(m * n)$ операций, а преобразование из B в B' соответственно $\theta(n * p)$.

Финальное произведение матриц A' и B' считается как обычное произведение матриц за $\theta(m * \frac{n}{k} * p)$.

Тогда итоговая асимптотика предобработки и запроса составляет:
$(\theta(4^k * k), \theta(m * n) + \theta(n * p) + \theta(m * \frac{n}{k} * p)) = (\theta(4^k * k), \theta(m * \frac{n}{k} * p))$. И выбирая $k = log(n)$, имеем предобработку за $\theta(n * log(n))$, а запрос за $\theta(\frac{m*n*p}{log(n)})$. Тогда даже запрос "с нуля", т. е. без заранее выполненой предобработки работает за $\theta(\frac{m*n*p}{log(n)}) = o(m * n * p)$.