

SPb HSE, ПАДИИ, 1 курс, весна 2024/25
Практика по алгоритмам #29

Гаусс
12 мая

Собрано 15 мая 2025 г. в 15:41

Содержание

1. Гаусс	1
2. Разбор задач практики	3
3. Домашнее задание	5
3.1. Обязательная часть	5
3.2. Дополнительная часть	5

Гаусс

1. Первообразный корень

Мы обсудили, как найти первообразный корень простого n . А если n не простое?

2. Квадратный корень по модулю

За сколько уже сейчас вы умеете решать уравнение $x^2 = a \bmod p$?

3. Точка в параллелепипеде

Даны d -мерная точка и d -мерный параллелепипед.
Проверить, лежит ли точка в параллелепипеде.

4. Найти расстояние от точки до подпространства

Дана d -мерная точка и набор из k d -мерных векторов – базис линейного подпространства.
Найти расстояние от точка до подпространства.

5. Выбор базиса минимального веса

Дан набор векторов с весами, вектора образуют линейное пространство. Выбрать из данных векторов базис этого пространства минимального веса. За сколько работает решение?

6. Найти рекуррентность

Вы знаете, что последовательность $1, 1, 2, 3, 5, 8, 13, \dots$ образована линейным рекуррентным соотношением с коэффициентами $1, 1$: $a_i = a_{i-1} + a_{i-2}$. Решим обратную задачу: дана последовательность длины n , найти минимальное k и k коэффициентов, задающие данную последовательность, как линейную рекуррентность.

$\mathcal{O}(n^3 \log n)$, $\mathcal{O}(n^3)$, $\mathcal{O}(nk + k^3 \log k)$.

7. Вероятность выжить

а) Дан грид с дырками. Вы начинаете в $(1, 1)$, за ход переходите с вероятностью $\frac{1}{2}$ вправо, с $\text{Pr} = \frac{1}{2}$ вверх. Если пытаетесь выйти за пределы поля, остаётесь на месте. Если попадаете в дырку, умираете. С какой вероятностью вы дойдёте до клетки (n, m) живым?

б) $p_{\text{right}} = \frac{1}{3}, p_{\text{left}} = \frac{1}{6}, p_{\text{up}} = \frac{1}{3}, p_{\text{down}} = \frac{1}{6}$.

То есть, граф теперь содержит циклы и вообще непонятно, сходится ли процесс.
С какой вероятностью мы в какой-то момент живым доползём до (n, m) ?

8. Онлайн

Вам дана матрица A , на вас онлайн сыпятся запросы y_i . Нужно находить x : $Ax = y_i$.

9. (*) Матричная игра

Игра на матрице. Первый выбирает строку, второй столбец. Делают они это независимо, не зная, что делает соперник. Выигрыш первого игрока – число в матрице. Первый его максимизирует, второй минимизирует. Вероятностная стратегия для первого: выбрать такие вероятности для строк $p_1, \dots, p_m$, чтобы математическое ожидание выигрыша не зависит от хода второго игрока. Найти любой такой вектор p . Не нужно максимизировать выигрыш.

10. (*) Минимальное квадратичное

Дана точка b и вектора $a_1, \dots, a_n$. Выразить вектор $b = \sum a_i x_i: \sum x_i^2 \rightarrow \min$.

11. (*) Задача про XOR

Даны n чисел от 0 до $2^n - 1$. Выбирается случайное подмножество A этих n чисел. Найдите за $2^{n/2} \cdot \text{poly}(n)$ матожидание величины $\text{popcount}(\text{XOR}(A))^2$.

Подсказка: ответ для $\{a_1, a_2\}$ равен ответу для $\{a_1, a_2 \hat{+} a_1\}$

12. (*) Я теряю корни

На лекции научились по данным p, a, b искать $x: x^a = b \bmod p$ (p простое).

Найти не один, а все такие x (заодно можно заметить, что на лекции был маленький обман).

Разбор задач практики

1. Первообразный корень

Всё то же самое, только вместо $n - 1$ используем $\varphi(n)$.

Напомним из алгебры, что первообразный корень есть только у чисел вида $2, 4, p^k, 2p^k$.

2. Квадратный корень по модулю

Логарифмируем $a = g^i$, ищем x в виде $x = g^k$, получаем $g^{2k} = g^i \pmod p \Rightarrow 2k = i \pmod{p-1}$.

3. Точка в параллелепипеде

Сдвинем один из углов параллелепипеда в точку 0. Стороны параллелепипеда, исходящие из точки 0, – вектора, образующие базис пространства. Разложим нашу точку в базисе. Точка внутри iff все координаты от 0 до 1.

4. Найти расстояние от точки до подпространства

Пусть искомая точка – b . Пусть $v = Ax: |Ax - b| = \min$. Есть два решения:

а) Сделаем базис ортогональным. Вычтем из b проекции на все базисные вектора. Останется нормаль к пространству $b - v$.

б) v – точка в подпространстве. Ищем такую точку v , что $v - b$ перпендикулярно всему пространству $\Leftrightarrow$ скалярные произведения со всеми векторами A равны нулю. Получаем $A^t(Ax - b) = 0 \Leftrightarrow x = (A^t A)^{-1} A^t b$.

5. Выбор базиса минимального веса

Будем добавлять вектора в порядке увеличения веса. Добавление работает за $\mathcal{O}(nk)$, где k – размер базиса, n – размерность пространства, если всего векторов m , получили $\mathcal{O}(nmk)$.

Почему эта жадность верна?

Пусть $w_1 \leq w_2 \leq \dots \leq w_n$ – веса векторов, $a_1 < a_2 < \dots < a_k$ – индексы в нашем ответе, $b_1 < b_2 < \dots < b_k$ – индексы в таком оптимальном ответе, что $\text{LCP}(a, b) = \max$. Рассмотрим $\min i: a_i \neq b_i$. Странно, если $a_i > b_i$, мы могли добавить вектор b_i в базис. Возьмём линейно-независимый набор $\{a_1, a_2, \dots, a_i\}$ и будем добавлять в него вектора из $\{b_i\}$.

Успешно добавятся все вектора кроме одного... А вес не добавленного не менее w_{a_i} .

Мы получили набор $c: (w(c) < w(b)) \vee (w(c) = w(b) \wedge \text{LCP}(a, c) > \text{LCP}(a, b))$. Противоречие.

6. Найти рекуррентность

Предполагаем, что $k \leq \frac{n}{2}$. Записываем систему $a_n = a_{n-1}x_1 + a_{n-2}x_2, \dots, a_{n-1} = a_{n-2}x_1 + a_{n-3}x_2 + \dots, a_{\frac{n}{2}+1} = \dots$. В каждой правой части $\frac{n}{2}$ x -ов. Минимальное k равно рангу матрицы (без док-ва). Если мы знаем, что $k \leq m$, то записав систему $m \leq m$, мы можем найти m коэффициентов линейной рекуррентности длины m .

Решение за $\mathcal{O}(n^3 \log n)$: бинпоиск по k , внутри Гаусс.

Решение за $\mathcal{O}(n^3)$: считаем ранг Гауссом (нашли k), затем запускаем ещё одного Гаусса (нашли коэффициенты).

Решение за $\mathcal{O}(nk + k^3 \log k)$: инкрементальный бинпоиск по k ($k = 1, 2, 4, \dots$).

Решение за $\mathcal{O}(nk + k^3)$: после того, как нашли правую границу бинпоиска, считаем ранг.

7. Вероятность выжить

x_{ij} – вероятность выжить, начиная из клетки i, j .

а) Динамика, т.к. граф ациклический.

б) Граф с циклами, но x_{ij} линейно выражается через соседей, поэтому решаем систему уравнений. Гаусс приемлем, но даст дикую погрешность, а вот метод итераций содержит только положительные коэффициенты, поэтому отработает без погрешности.

Система: $x_{i,j} = \frac{1}{3}x_{i,j+1} + \frac{1}{6}x_{i,j-1} + \frac{1}{3}x_{i+1,j} + \frac{1}{6}x_{i-1,j}$, $x_{n,m} = 1$. Метод итераций: изначально все остальные $x_{i,j} = 0$, делаем переход $x \rightarrow A \cdot x$, чтобы ускорить $x \rightarrow A^{2^k} \cdot x$. Погрешности у метода итераций нет, так как все числа >0 (погрешность образуется при вычитании).

P.S. Матожидания числа ходов обсуждать не нужно, это будет в дз.

8. Онлайн

Для $\det A \neq 0$: находим за n^3 LU-разложение $A = LU$. Ответ на запрос за $\mathcal{O}(n^2)$: $x = L^{-1}U^{-1}y_i$

Для произвольной системы, можно сделать обычного итеративного Гаусса, который для каждой строки таскает ещё и вектор коэффициентов, как строка выражается из исходных (длина $\leq \min(n, m)$). Важно запомнить не только строки базиса, но и не базисные, т.к. каждая задаёт условие вида $\sum_j y_{ij} = 0$, которое предстоит проверять для y_i .

9. (*) Матричная игра

Пусть второй игрок выберет j -й столбец, тогда матожидание выигрыша равно

$E_j = p_1 a_{1j} + p_2 a_{2j} + \dots + p_n a_{nj} = t$. Записываем уравнения $E_1 = E_2 = \dots = t$, где неизвестные $p_1, p_2, \dots, p_n, t$. Добавляем уравнение $\sum p_i = 1$.

10. (*) Задача про ХОР

Подсказка: ответ для $\{a_1, a_2\}$ равен ответу для $\{a_1, a_2 \hat{a}_1\}$. n n -битных чисел задают матрицу $n \times n$. Приведём её Гауссом к виду диагональ + прямоугольник треша (свободные переменные) + нулевые строки. Пусть ранг матрицы (длина диагонали) равен k . Заметим, что есть решение за 2^k и есть решение динамикой по строкам за $2^{n-k}k^2$. Получаем $2^{\min(k, n-k)} \text{Poly}(n) \leq 2^{n/2} \text{Poly}(n)$. Динамика: добавляем k строк по одной, важно, сколько мы выбрали единиц и какие значения у $n-k$ свободных переменных.

11. (*) Минимальное квадратичное

Найдём какое-нибудь решение $Ax_0 = b$. Искомое решение $x^* = x_0 - x$, где $Ax = 0$. Множество решений $Ax = 0$ – линейное подпространство. Теперь задача такая: найти в этом пространстве вектор x ближайший к x_0 . См. задачу про расстояние до подпространства.

12. (*) Я теряю корни

Ищем первообразный g . Логарифмируем b по g : $b = g^c$. Ищем x в форме $x = g^y$.

$$x^a = b \bmod p \Leftrightarrow (g^y)^a = g^c \bmod p \Leftrightarrow ya = c \bmod (p-1)$$

Если $c_1 = \gcd(c, p-1)$ не делится на $a_1 = \gcd(a, p-1)$, решений нет. Иначе решения есть.

$$c \neq 0 \Rightarrow y = \frac{c}{a_1} \cdot \left(\frac{a}{a_1}\right)^{-1} \bmod \frac{p-1}{a_1} \Rightarrow y = \frac{c}{a_1} \cdot \left(\frac{a}{a_1}\right)^{-1} + z \frac{p-1}{a_1} \bmod (p-1), 0 \leq z < a_1 \text{ (} a_1 \text{ решений)}.$$

Можно подумать, что $c = 0$ и $a = 0$ – отдельные случаи, но $\gcd(0, p-1) = p-1$ и по общей формуле всё правильно: $c = 0 \Rightarrow$ решаем $x^a = 1$. Если $a = 0$, x любое, иначе $y = 0 \Rightarrow x = 1$.

Домашнее задание

3.1. Обязательная часть

1. (2) Matrix decomposition

Дана матрица A размера $n \times m$. Найти такое представление $A = BC$, что B имеет размер $n \times k$ и k минимально. Подсказка: думайте про A , как про пространство строк.

2. (3) Матожидание времени путешествия

Дана полоска из n клеток. Изначально мы в первой. Каждый ход выбирается случайное x из множества

- a) (1) $\{0, 1, 2, \dots, k\}$
- b) (2) $\{-\frac{k}{2}, \dots, -2, -1, 0, 1, 2, \dots, k\}$

И мы ходим $i \rightarrow \max(1, \min(i + x, n))$. Найти матожидание числа ходов до клетки n . Чем быстрее, тем лучше.

3.2. Дополнительная часть

1. (2) Пересечение сфер

Даны k n -мерных сфер. Найти все точки пересечения, или сказать, что их бесконечно много.

2. (2) Разбиение графа на две доли

Дан неориентированный граф. Нужно разбить его вершины на две доли так, чтобы после удаления рёбер между долями, степени всех вершин были чётны.