Второй курс, осенний семестр 2021/22
Практика по алгоритмам #11

Линейная алгебра

29 ноября

Собрано 30 ноября 2021 г. в 15:49

Содержание

Линейная алгебра

1. **Разложение вектора в базисе**
   a) Базис – произвольный набор линейно независимых векторов.
   b) Базис – столбцы треугольной матрицы.
   c) Ортогональный базис.

2. **Точка в параллелепипеде**

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

3. **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.

   a) Ортогонализацией базиса.
   b) Методом Гаусса.
   c) `(*)` Решая $|Ax - b| \to \min$

4. **Выбор базиса минимального веса**

   Дан набор векторов с весами, вектора образуют линейное пространство. Выбрать из данных векторов базис этого пространства минимального веса.

5. **Найти рекуррентность**

   Вы знаете, что последовательность $1, 1, 2, 3, 5, 8, 13, \ldots$ 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.

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

6. **Минимальное квадратичное**

   Дана точка b и вектора $a_1, \ldots, a_n$. Выразить вектор $b = \sum a_i x_i \colon \sum x_i^2 \to \min$.

7. **Вероятность выжить**
   a) Дан грид с дырками. Вы начинаете в $(1, 1)$ за ход переходите с вероятностью $\frac{1}{2}$ вправо, с вероятностью $\frac{1}{2}$ вверх. Если пытаетесь выйти за пределы поля, ничего не происходит. Если попадаете в дырку, умираете. С какой вероятностью вы дойдёте до клетки (n, m) живым?
   b) $p_{right} = \frac{1}{3}, p_{left} = \frac{1}{6}, p_{up} = \frac{1}{3}, p_{down} = \frac{1}{6}$. То есть граф теперь содержит циклы и вообще непонятно, сходится ли процесс.

8. **(*) 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 $p_1, \ldots, p_m$, чтобы математическое ожидание выигрыша не зависит от хода второго игрока. Найти любой такой вектор p. Не нужно максимизировать выигрыш.

9. **(*) Задача про XOR**

Даны n чисел от 0 до $2^n - 1$. Выбирается случайное подмножество A этих n чисел.
Найдите за $2^{n/2} \cdot poly(n)$ матожидание величины $\texttt{popcount}(\texttt{XOR}(A))^2$.
Подсказка: ответ для $\{a_1, a_2\}$ равен ответу для $\{a_1, a_2 \hat{} a_1\}$

Разбор задач практики

1. **RSA**
   a) Пусть $n = pq$, известно $\varphi(n) \Rightarrow \varphi(n) = n - p - q + 1 \Rightarrow p + q = -(\varphi(n) - n - 1) \Rightarrow x^2 + (\varphi(n) - n - 1)x + n = 0$ имеет корни p, q.
   b) Нам дали $c = m^e \bmod n$. Загадаем случайное число r.
   Дадим оракулу $r^e c \bmod n = (rm)^e \bmod n$, с вероятностью 0.01 он расшифрует.

2. **Разложение вектора в базисе**
   Раскладываем столбец b в базисе A (столбцы матрицы A – вектора базиса).
   a) Базис – произвольный набор линейно независимых векторов.
   Придётся за $\mathcal{O}(n^3)$ Гауссом решить систему $Ax = b$.
   b) Базис – трапецевиная матрица.
   Тогда метод Гаусса уже не нужен, достаточно восстановить x за $\mathcal{O}(n^2)$.
   c) Ортогональный базис. a_i – базисный вектор. Тогда $x_i = \frac{\langle b, a_i \rangle}{\langle a_i, a_i \rangle}$. $\mathcal{O}(n^2)$.
   Если базис ещё и ортонормированный, $|a_i| = 1$, то $x_i = \langle b, a_i \rangle$.

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 точка – b. Пусть $v = Ax \colon |Ax - b| = \min$
   a) Сделаем базис ортогональным. Вычтем из b проекции на все базисные вектора. Останется нормаль к пространству $b - v$.
   b) v – точка в подпространстве. Ищем такую точку v, что $v - b$ перпендикулярно всему пространству $\Leftrightarrow$ скалярные произведения со всеми векторами A равны нулю. Получаем $A^t(Ax - b) = 0 \Leftrightarrow x = (A^t A)^{-1} A^t b$.
   c) $|Ax - b| \to \min \Leftrightarrow (Ax - b)^2 \to \min$. Дифференцируем, приравниваем производную к нулю, получаем такое же уравнение, как в предыдущем пункте.

5. **Выбор базиса минимального веса**
   Будем добавлять вектора в порядке увеличения веса. Почему эта жадность верна?

   Пусть $w_1 \leqslant w_2 \leqslant \ldots \leqslant w_n$ – веса векторов, $a_1 < a_2 < \cdots < a_k$ – индексы в нашем ответе, $b_1 < b_2 < \cdots < b_k$ – индексы в таком оптимальном ответе, что $\texttt{LCP}(a, b) = \max$. Рассмотрим $\min i \colon a_i \neq b_i$. Странно, если $a_i > b_i$, мы могли добавить вектор b_i в базис. Возьмём линейно-независимый набор $\{a_1, a_2 \ldots, a_i\}$ 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 $c \colon (w(c) < w(b)) \vee (w(c) = w(b) \wedge \texttt{LCP}(a, c) > \texttt{LCP}(a, b))$. Противоречие.

6. **Найти реккурентность**
   Предполагаем, что $k \leqslant \frac{n}{2}$. Записываем систему $a_n = a_{n-1}x_1 + a_{n-2}x_2 \ldots, a_{n-1} = a_{n-2}x_1 +$

$a_{n-3}x_2+\ldots, a_{\frac{n}{2}+1} = \ldots$. В каждой правой части $\frac{n}{2}$ x-ов. Минимальное k равно рангу матрицы (без док-ва). Если мы знаем, что $k \leqslant m$, то записав систему $m \leqslant m$, мы можем найти m коэффициентов линейной реккурентности 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), запускаем ещё одного Гаусс (нашли коэффициенты).

7. **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.

8. **Вероятность выжить**
x_{ij} – вероятность выжить, начиная из клетки i, j.
а) Динамика, т.к. граф ацикличен.
б) Граф с циклами, но x_{ij} линейно выражается через соседей, поэтому Гаусс.

9. **(*) Матричная игра**
Пусть второй игрок выберет j-й столбец, тогда матожидание выигрыша равно $E_j = p_1a_{1j} + p_2a_{2j} + \cdots + p_na_{nj} = t$. Записываем уравнения $E_1 = E_2 = \cdots = t$, где неизвестные $p_1, p_2, \ldots, p_n, t$. Добавляем уравнение $\sum p_i = 1$.

10. **(*) Задача про XOR**
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 + нулевые строки. Пусть ранг матрицы (длина диагонали) равен k. Заметим, что есть решение за 2^k и есть решение динамикой по строкам с $2^{n-k}k^2$ состояниями. Получаем $2^{\min(k,n-k)}Poly(n) \leqslant 2^{n/2}Poly(n)$.

Домашнее задание

3.1. Обязательная часть

1. **(2+2) Винни-Пух и мёд**

   У Винни Пуха есть бесконечные запасы из k видов горшочков мёда. Каждый вид горшочков требует сколько-то дней от Пуха, чтобы съесть весь мёд из одного горшочка.

   Пух уже провёл серию экспериментов: брал несколько горшочков, записывал день недели, когда начал эксперимент, съедал весь мёд, записывал день недели, когда эксперимент закончился. По понятным причинам Пух очень любит экспериментировать.

   А Кролик не любит мёд, но любит предсказывать будущее. Помогите Кролику, зная результаты k экспериментов, сказать, можно ли однозначно сказать результат следующего. Оцените время работы алгоритма.

   a) **(2)** Винни берёт произвольные множества горшков.
   b) **(2)** Винни всегда берёт горшки не более чем двух разных типов.

2. **(3) 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.*

3. **(2) Расстояние в n-мерном пространстве**

   Даны m точек в n-мерном пространстве и k линейно независимых векторов, задающих подпространство. За $\mathcal{O}(kn(k+m))$ найти для каждой точки расстояние до подпространства.

4. **(3) Оптимальное представление точек**

   Даны $m \geqslant n$ n-мерных векторов, порождающих всё n-мерное пространство. Даны k запросов: выразить точку в виде линейной комбинации, минимизируя сумму квадратов коэффициентов. Ответить на все запросы за $\mathcal{O}((m+k)n^2)$.

5. **(4) Матожидание времени путешествия**

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

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

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

3.2. Дополнительная часть

1. **(3) Гаусс на многочленах**

   Дана квадратная матрица A из $n \times n$ элементов $\mathbb{R}[x]$. k — максимальная из степеней многочленов в матрице.

   a) **(1)** Найти её определитель за $\mathcal{O}(c^n \cdot \text{poly}(k))$.
   b) **(2)** В предположении, что матрица не вырожденная, решите систему уравнений $Ax = b$.
   c) **(+1)** Найти её определитель за полином.

2. **(4) 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.

3. **(3) Пересечение сфер**

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

4. **(3) Матожидание пути**

   Дан грид со стенками и **дырками**, мы идём из $(1, 1)$ в (n, m).
   В каждый момент времени вероятности сдвинуться вправо и вверх равны $\frac{1}{3}$, а влево и вниз $\frac{1}{6}$.
   При попытки идти в стенку ничего не происходит. При попытки идти в дырку мы умираем.
   Грид таков, что мы или свалимся в дырку, или дойдём до конца.
   Пусть мы дошли до конца, не упав в дырку. Какая средняя длина пути была пройдена?

5. **(4) Максимальный равномерный поток**

   Поток называется равномерным, если для любых двух вершин a и b любые два пути из a в b, по которым течёт поток, имеют одинаковую длину (количество рёбер). Найдите в неорграфе максимальный равномерный поток.