

Вопросы к экзамену по алгоритмам

SPb HSE, 1-й курс ПАДИИ, июнь 2025

Общая информация

- Слайды от Данила: [\[link\]](#)
- Конспекты ПМИ: [\[part1\]](#) [\[part2\]](#) [\[part3\]](#) [\[part4\]](#)
- Практики и куски разборов: [\[wiki\]](#)
- Экзамен: письменный + устный, ≈ 1 час на подготовку билета, ≈ 20 минут на ответ записанного и дополнительных вопросов. Экзамен проходит *без* использования конспекта и других источников.
- *Курсивом* помечено то, что было разобрано на практике.
- (a) темы, обязательные к знанию (без них не получить удовл. оценку)
- (+) факультативные темы (оценка 10) – нужно заботать 6 **любых** темы из 9.

Паросочетания

1. Лемма о доп пути, ЧДП dfs-ом
2. Кун
3. minVC: Vertex Cover
4. maxIS: Independent Set
5. Жадная инициализация. Найдите паросочетания размера $1/2|\Box|$
6. Обнуление пометок. Что, если не обнулять пометки? Как за $\Box(\Box + \Box)$ найти >1 пути?
7. Лемма Холла и Кун
8. Найти паросочетание, которое покрывает вершины из подмножества $\Box$ левой доли.
9. Двудольная клика
10. ?
11. ?

Потоки

12. Задача про 2 рёберно непересекающихся пути на примере графа из рёбер (1-2-3-4) (1-3) (2-4): неверное решение "dfs/bfs + удалить рёбра"; верное решение "разрешать отменять рёбра" за $O(E)$.
13. Аксиоматика потоков в орграфе ($0 \leq f_e \leq c_e$; входящий поток = исходящий поток), которая приводит нас к dfs-у по рёбрам $f < c$ для поиска дополняющего пути.
14. Алгоритмы и теорема Форда-Фалкерсона. Доказательство: вводим разрез, сразу получаем $F(S,T) \leq C(S,T)$, предъявляем поток: $F(S,T) = C(S,T) \Rightarrow \min C = \max F$
15. Scaling (Масштабирование потока, $E^2 \log U$)
16. Эдмондс-Карп (потому что от bfs один шаг к FB)
17. MinCost-k-flow (FB с очередью)
18. Решение задачи о назначениях (взвешенное паросочетание)
19. MinCost-Circulation (Клейн)
20. bonus: Потенциалы (FB $\rightarrow$ Dijkstra)
21. bonus: Техника использования разрезов
22. ?
23. ?

Теория чисел и Гаусс

24. База: Возведение в степень за $\log N$.
25. База: Факторизация за $n^{1/2}$; проверку на простоту за $n^{1/2}$.
26. Проверка на простоту: тест Миллера-Рабина. Числа Кармайкла. Версия для 232 (2 7 61)
27. gcd; Расширенный Евклид (рекурсивная реализация в 3 строки)
28. Обратный по модулю (два способа)
29. Решето Эратосфена за $N \log \log N$
30. Функция Эйлера. Вычисление от N . Вычисление всех $\phi[1..N]$ за $N \log \log N$.
31. Шифрование: закрытый ключ, XOR-шифрование;
32. Шифрование: протокол Диффи-Хеллмана для обмена закрытым ключом.
33. Шифрование: открытый ключ, RSA.
34. Решето за $O(N)$
35. Факторизация рандомом за $n^{1/2}$: тыкаем в рандом, пока $\gcd(x, n) \neq 1$
36. Факторизация за $n^{1/4}$
37. Первообразный корень: угадываем за $\log \log p$; проверяем за $O(\log^2 p)$; нужно предварительно найти факторизацию $p-1$.
38. Дискретное логарифмирование за: $p^{1/2}$ (big-step-baby-step)
39. Решение уравнений вида $x^k = a(p)$ через логарифмирование.
40. Линейная алгебра: метод Гаусса для квадратной A : $\det A \neq 0$ (без случаев)
41. Линейная алгебра: нахождение базиса множества векторов (добавляем в Гаусса строки по одной, вычитаем из новой старые; порядок столбцов не меняем)
42. Линейная алгебра: решение системы $Ax=b$, нахождение аффинного подпространства решений.
43. ?
44. ?

FFT

45. Умножение за n^2 , хранение многочленов. Числа: переносы за $O(n)$.
46. Умножение за $n \log n$: общая схема умножения.
47. Прямое FFT: рекурсивная схема.
48. Числа: $\text{BASE}=104$, $\text{double}=15-16$ знаков $\Rightarrow N \cdot \text{BASE}^2 < 10^{15}$
49. Обратное FFT: обоснование; $\text{reverse}(f+1, f+N)$
50. Ускорение FFT: подсчёт за $O(N)$ всех корней из единицы
51. Использование FFT: разделяй и властвуй для деления
52. Использование FFT: разделяй и властвуй для смены системы счисления
53. ?
54. ?

LP и ILP

55. Линейное программирование: постановка задачи LP, разные формы ($Ax=b/Ax \leq b$, $c > \min/\max$, отсутствие/наличие $c > \dots$)
56. Примеры задач LP: поток, mincost поток
57. Примеры задач LP: SAT, IS, VC (решение должно быть целым $\Rightarrow$ ILP)
58. Примеры задач: Knapsack, Hamopath, мультипродуктовый поток

59. Примеры на LP: Нейрон. Обучение перцептрона.
60. Геометрический смысл (выпуклый многогранник, вершины, bounding-box).
61. Решение $Ax \leq b, x \geq 0$ перебором вершин: выберем $C(n+m, n)$ плоскостей, пустим Гаусса.
62. Симплекс метод (в предположении, что есть начальное решение): общая идея (перебор вершин, только общая идея)
63. Нахождение начальной точки симплексом.
64. Двойственность: построение двойственной задачи, теоремы о двойственности — слабая, сильная (формулировка).
65. Доказательства про двойственность: слабая двойственность.
66. ?
67. ?

Экзотика

68. P и NP. Примеры.
69. Модели вычислений. RAM-w. bfs pf $O(n^2/w)$.
70. Модели вычислений. RAM. bfs за $O(n)$. $P = NP$.
71. Алгоритмы во внешней памяти: сортировка (QuickSort, MergeSort, multimerge — хранить кучу текущих блоков)
72. Параллельные алгоритмы: сортировка (выбрали несколько опорных элементов, относительно каждого разбить массив, сортировать результат разбиения независимо)
73. Приближённые алгоритмы: TSP через MST
74. ?
75. ?

Дополнительные вопросы

- (+) 76. Стабильные паросочетания: существования, алгоритм построения.
- (+) 77. Венгерский алгоритм поиска mincost perfect matching.
- (+) 78. Диниц с масштабированием для поиска потока за $\mathcal{O}(VE \log U)$.
- (+) 79. Mincost поток за полином. Capacity scaling, $\mathcal{O}(Dijkstra \cdot E \log U)$.
- (+) 80. Алгоритм Видемана для решения СЛАУ за $\mathcal{O}(n \cdot \text{notZeroes})$.
- (+) 81. FFT: нерекурсивная реализация; оптимизация числа умножений; преобразование-бабочка (для лучшего доступа к кешу).
- (+) 82. Вычисление значений многочлена в произвольных n точках за $\mathcal{O}(n \log 2n)$.
- (+) 83. Реализация Симплекс метода (на уровне подробности, как Гаусса делали).
- (+) 84. Доказательство того, что $\exists$ NPC задачи. $ВН \in NPC$.