Тест 3 по АМВ

Вариант 1

Фамилия И.О., группа: _____

1	2	3	4	5	6	7	8	9	10	11	Σ	оценка

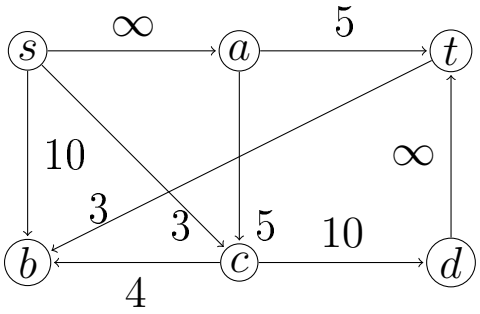
Тест closed book, no device. Решение любой задачи без обоснования не засчитывается. Использование алгоритма из курса считается обоснованием. Если в задаче есть поля «ДА», «НЕТ», то ответ должен быть обведён, иначе задача не проверяется. Все задачи оцениваются в 2 балла.

1. Пусть для положительной функции $f(n)$ известно, что $f(n) = (3 + o(1))^n + \Theta(n^{100})$. Верно ли в общем случае, что $\log f(n) = \Theta(n)$? ДА НЕТ

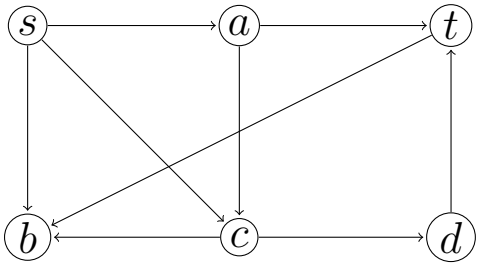
2. Вычислить $10^{26^{329}} \bmod 14$.

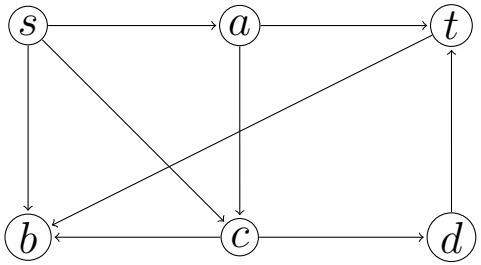
3. RSA. Пусть модуль $N = 187$, открытый ключ $e = 23$. Вам пришло зашифрованное сообщение $x = 2$. Расшифруйте его.

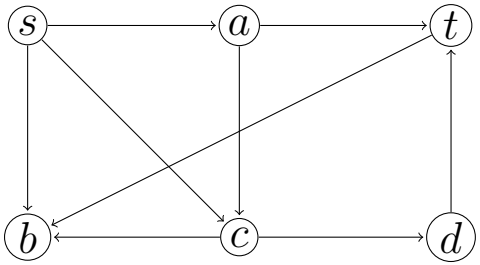
4.

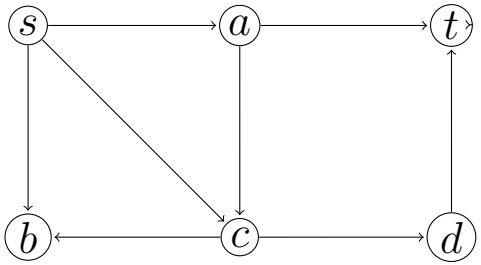


Найти максимальный поток $s \to t$ и минимальный разрез в потковой сети. Вы должны привести последовательность увеличивающих путей и остаточных графов для каждого шага построения. Начальный поток нулевой.

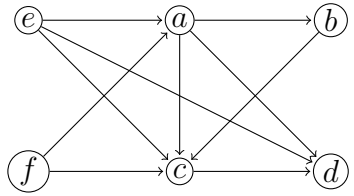








5.



Продемонстрировать работу алгоритма топологической сортировки.

◇

6. Дан массив длины n, состоящий из различных целых чисел. Известно, что в массиве есть ровно одна инверсия (пара (i, j) называется инверсией A, если $i < j$ и $A[i] > A[j]$). Верно ли, что всякий алгоритм сортировки такого массива работает за $\Omega(n \log n)$? ДА НЕТ

7. Дан связный взвешенный неориентированный граф, у которого $|E| = |V| = n$. Верно ли, что можно найти минимальное остовное дерево этого графа за линейное по n время? ДА НЕТ

◇

8. Лежит ли следующая задача в классе NPC? Заданы графы $G = (V_1, E_1), H = (V_2, E_2)$. Верно ли что в G существует подграф, изоморфный H, т.е. существует инъективное отображение $f\colon V_2 \to V_1$ такое, что если ребро $\{u, v\} \in E_2$, то ребро $\{f(u), f(v)\} \in E_1$. ДА НЕТ

9. Найти Θ–асимптотику $T(n) = T(\frac{n}{6}) + T(\frac{7n}{9}) + 2n$, считайте, что $T(n) = 1$ для $n \leqslant 3$.

◇

10. Пусть $f(x) = x$, $g(x) = x$. Студент перемножает эти многочлены с помощью ДПФ. Сперва он находит массивы коэффициентов для этих многочленов $F = [0, 1]$, $G = [0, 1]$, затем производит ДПФ этих массивов и получает $F^* = [1, -1]$, $G^* = [1, -1]$, затем поэлементно перемножает массивы, и получает $H^* = [1, 1]$, наконец, он проводит обратное преобразование, получает $H = [1, 0]$ и заключает, что $h(x) = f(x) \cdot g(x) = 1$.

1) Найдите ошибку в вычислениях студента.

2) Проведите правильные вычисления, т.е, перемножьте f и g с помощью ДПФ.

◇

11. Является ли следующий язык NP–полным? Язык состоит из описаний КНФ, для которых существует набор значений переменных, обращающий в истину все дизъюнкты, кроме, быть может, одного. ДА НЕТ

Тест 3 по АМВ

Вариант 2

Фамилия И.О., группа: _____

1	2	3	4	5	6	7	8	9	10	11	Σ	оценка

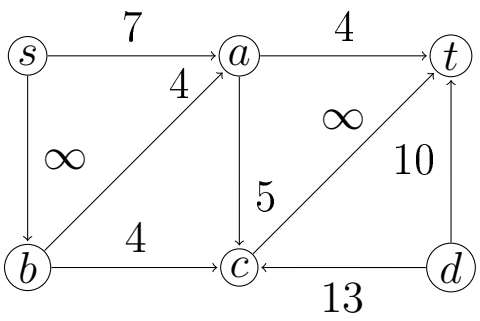
Тест closed book, no device. Решение любой задачи без обоснования не засчитывается. Использование алгоритма из курса считается обоснованием. Если в задаче есть поля «ДА», «НЕТ», то ответ должен быть обведён, иначе задача не проверяется. Все задачи оцениваются в 2 балла.

1. Пусть для положительной функции $f(n)$ известно, что $f(n) = n^{3+o(1)} + \Theta(1.01^n)$. Верно ли в общем случае, что $\log f(n) = \Theta(n)$? ДА НЕТ

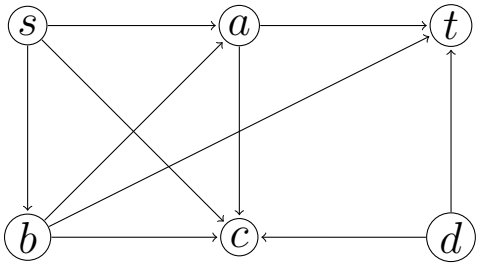
2. Вычислить $6^{36^{216}} \bmod 22$.

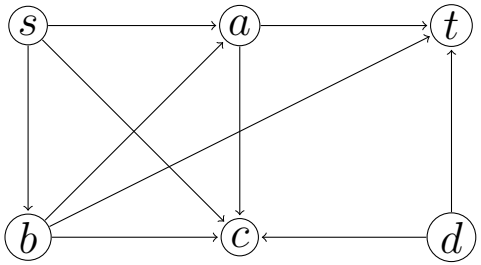
3. RSA. Пусть модуль $N = 161$, открытый ключ $e = 19$. Вам пришло зашифрованное сообщение $x = 2$. Расшифруйте его.

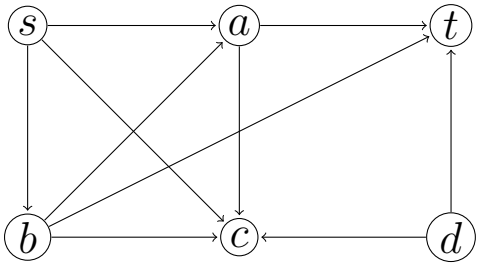
4.

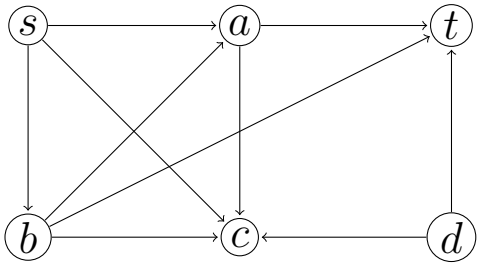


Найти максимальный поток $s \to t$ и минимальный разрез в потоковой сети. Вы должны привести последовательность увеличивающих путей и остаточных графов для каждого шага построения. Начальный поток нулевой.

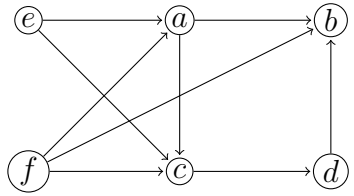








5.



Продемонстрировать работу алгоритма топологической сортировки.

◇ ◇

6. Дан массив длины n, каждый элемент массива есть натуральное число, не превосходящее 10. Верно ли, что всякий алгоритм сортировки такого массива работает за $\Omega(n \log n)$? ДА НЕТ

7. В неориентированном связном взвешенном графе есть цикл, в этом цикле строго наименьшее по весу ребро есть e. Верно ли, что e принадлежит каждому минимальному остовному дереву графа? ДА НЕТ

◇ ◇

8. Лежит ли следующая задача в классе NPC? Задан взвешенный граф $G = (V, E)$ и натуральное число k. Верно ли что в G существует минимальное остовное дерево, степень всех вершин в котором не более k? ДА НЕТ

9. Найти Θ–асимптотику $T(n) = T(\frac{n}{7}) + T(\frac{5n}{6}) + 4n$, считайте, что $T(n) = 1$ для $n \leqslant 3$.

10. Пусть $f(x) = -x$, $g(x) = x$. Студент перемножает эти многочлены с помощью ДПФ. Сперва он находит массивы коэффициентов для этих многочленов $F = [0, -1]$, $G = [0, 1]$, затем производит ДПФ этих массивов и получает $F^* = [-1, 1]$, $G^* = [1, -1]$, затем поэлементно перемножает массивы, и получает $H^* = [-1, -1]$, наконец, он проводит обратное преобразование, получает $H = [-1, 0]$ и заключает, что $h(x) = f(x) \cdot g(x) = -1$.

1) Найдите ошибку в вычислениях студента.

2) Проведите правильные вычисления, т.е, перемножьте f и g с помощью ДПФ.

11. Является ли следующий язык NP–полным? Язык состоит из описаний КНФ, для которых существует набор значений переменных, обращающий в истину ровно один дизъюнкт. ДА НЕТ