ТЕСТ 1. 20.03.2017

ВАРИАНТ 1

1	2	3	4	5	6	7	8	9	10	11	12	$\sum$

Фамилия, имя студента Группа

Фамилия преподавателя, ведущего семинары

1. Решение каждой задачи должно быть обосновано, ответы без обоснования не принимаются и не оцениваются.

2. В некоторых задачах помимо решения требуется дать краткий ответ "да" или "нет" – это указано в условии после числа баллов за задачу.

2. Можно без доказательства использовать факт **NP**–полноты задач, разобранных на лекциях, на семинарах и описанных в каноническом задании по курсу

Задача 1. (3 балла)

Дана программа

```
for bound ← 1, bound ≤ n do
    bound ← bound * 2
    for i ← 0, i < bound do
        i ← i + 1
        for j ← 0, j < n do j ← j + 2
            печать ("алгоритм")
        end for
        for j ← 1, j < n do
            j ← j * 2
            печать ("алгоритм")
        end for
    end for
end for
```

Пусть $g(n)$ обозначает число слов "алгоритм", которые напечатает программа. Найдите θ–асимптотику $g(n)$.

◇

Задача 2. (2 балла)
Даны массив различных положительных чисел $a[1 \dots n]$ и натуральное число $k < n/2$. *Обозначим* A^k *— k-й наименьший элемент массива* $a[1 \dots n]$. Предложите как можно более быстрый алгоритм, который находит сумму элементов массива больших, чем $\dfrac{A_k}{2}$, и меньших, чем $2A_{n-k}$. Считайте, что все арифметические операции выполняются за $O(1)$.

Задача 3. (3 балла)
Постройте NP сертификат простоты числа 2621. Простыми считайте **только числа** 2 **и** 3**,** 5.

Известно, что $2^{2620} \pmod{2621} = 1$; $2^{1310} \pmod{2621} \neq 1$; $2^{655} \pmod{2621} \neq 1$, а у числа 131 первообразный корень < 10.

Замечание. Ссылки на полиномиальный алгоритм проверки простоты не допускаются.

◇

Задача 4. (2 балла) Да Нет
Пусть $L \in$ **co–NP**. Верно ли, что любой язык $N \subset L$, не равный L и не равный пустому языку, принадлежит **co–NP**?

Задача 5. (2 балла) Утверждение верно Утверждение ложно
Язык EUCLID состоит из троек натуральных чисел (a, b, c), таких что Н.О.Д$(a, b) = c$. Язык NOHAMPATH состоит из кодировок графов, в которых нет гамильтонова цикла.

Докажите или опровергните, что если язык NOHAMPATH полиномиально сводится к языку EUCLID, то $\mathbf{NP} = \mathbf{co}$–$\mathbf{NP}$.

◇

Задача 6. (5 баллов)
Боб решил воспользоваться RSA. Для этого он взял числа 91 и 37 и составил из них модуль $91 \cdot 37$. Но Боб не заметил, что число 91 не простое, и вычислил публичный ключ как обратный остаток к своему закрытому ключу по модулю $90 \cdot 36$. Бобу пришло сообщение 6. Какое сообщение было зашифровано, если закрытый ключ Боба 463?

Задача 7. (5 баллов) Утверждение верно Утверждение ложно
Пусть существует полиномиальный алгоритм, разрешающий язык нигде не выполнимых КНФ. (то есть определяющий по стандартному описанию КНФ, верно ли, что нет ни одного набора переменных, на которых она принимает значение True). Докажите или опровергните, что тогда существует полиномиальный алгоритм, который, получив на вход граф, выдаёт одно из его максимальных по размеру независимых подмножеств вершин.

◇

Задача 8. (8 баллов)
Даны n горизонтальных отрезков, лежащих на оси Ox и заданных массивом координат своих концов $[a_i, b_i]$. Отрезки можно сдвигать вправо и влево вдоль оси Ox. Необходимо с помощью сдвигов сделать так, чтобы пересечение всех отрезков стало непустым. Предложите $O(n \log n)$ алгоритм, который находит требуемый набор сдвигов минимальной суммарной длины. Считайте, что все арифметические операции с координатами выполняются за $O(1)$.

Квадратичный алгоритм оценивается из двух баллов.

Задача 9. (3 балла) Да Нет
Определим для любого языка $L \subseteq \Sigma^*$ язык его *надслов* $supw(L) = \{u = wsv \,|\, w, v \in \Sigma^*, s \in L\}$

Верно ли, что класс $\mathbf{P}$ замкнут относительно надслов, т. е. верна ли импликация: если $L \subseteq \mathbf{P}$, то и $supw(L) \subseteq \mathbf{P}$?

◇

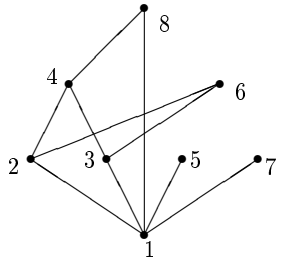
Задача 10. (6 баллов) Да Нет

Определим граф G_n на множестве натуральных чисел чисел $\{1, 2 \ldots, n\}$. в котором вершины — числа, и две вершины соединены тогда и только тогда, когда одно их них делится нацело на другое.

Верно ли, что язык $L = \{(G_n, k)\}$, состоящий из кодировок графов G_n, имеющих клику размера k является **NP**–полным?

Если ответ положительный, то приведите доказательство. Если ответ отрицательный, то приведите полиномиальный алгоритм, решающий эту задачу.

Считайте, что арифметические операции выполняются за $O(1)$. Ниже изображен граф G_8



Задача 11. (6 баллов) Да Нет

Определим для любого языка $L \subseteq \Sigma^*$ язык его подслов $subw(L) = \{u \,|\, \exists w, v \in \Sigma^* : wuv \in L\}$

Верно ли, что класс $\mathbf{P}$ замкнут относительно подслов, т. е. верна импликация: если $L \subseteq \mathbf{P}$, то и $subw(L) \subseteq \mathbf{P}$?

◇

Задача 12. (4 балла) Да Нет

Будем говорить, что граф G содержит (n, k)–**конфигурацию**, если в нём есть k вершинно-непересекающихся клик из n вершин каждая, причём для каждой пары n-клик есть ребро, концы которого принадлежат каждой из клик пары.

Будет ли **NP**–полным язык $\mathrm{GAR} = \{(G, n, k) \mid n, k \geq 100,\ G$ содержит (n, k)–сад$\}$?

ТЕСТ 1. 20.03.2017 ◇ ◇

ВАРИАНТ 2

1	2	3	4	5	6	7	8	9	10	11	12	$\sum$

Фамилия, имя студента Группа

Фамилия преподавателя, ведущего семинары

1. Решение каждой задачи должно быть обосновано, ответы без обоснования не принимаются и не оцениваются.

2. В некоторых задачах помимо решения требуется дать краткий ответ “да” или “нет” – это указано в условии после числа баллов за задачу.

2. Можно без доказательства использовать факт **NP**–полноты задач, разобранных на лекциях, на семинарах и описанных в каноническом задании по курсу

Задача 1. (3 балла) Дана программа

```
for bound ← 1, bound * bound < n do
    bound ← bound + 1
    for i ← 0, i < bound do
        i ← i + 1
        for j ← 0, j < i do
            j ← j + 2
            печать (“алгоритм”)
        end for
        for j ← 1, j < n do
            j ← j * 2
            печать (“алгоритм”)
        end for
    end for
end for
```

Пусть $g(n)$ обозначает число слов “алгоритм”, которые напечатает программа. Найдите Θ–асимптотику $g(n)$.

Задача 2. (2 балла)
Даны массив различных положительных чисел $a[1 \dots n]$ и натуральное число $k < n/2$. *Обозначим* A^k *— k-й наименьший элемент массива* $a[1 \dots n]$.

Предложите линейный алгоритм, который находит количество элементов массива, больших чем $A^2_{(k)}$ и меньших чем $\lfloor \sqrt{A_{(n-k)}} \rfloor$. Считайте, что все арифметические операции и извлечение корня выполняются за $O(1)$.

Задача 3. (3 балла)
Постройте NP сертификат простоты числа 2221. Простыми считайте **только числа** 2 **и** 3.
Известно, что $2^{2220} \pmod{2221} = 1$; $2^{1105} \pmod{2221} \neq 1$; $2^{740} \pmod{2221} \neq 1$; $2^{444} \pmod{2221} \neq 1$.
Замечание. Ссылки на полиномиальный алгоритм проверки простоты не допускаются.

◇ ◇

Задача 4. (2 балла) Да Нет
Пусть язык L принадлежит классу **co–NP**. Возможно ли, что L сводится полиномиальной m–сводимостью (по Карпу) к некоторому конечному языку?

Задача 5. (2 балла) Импликация верна Импликация не верна
Язык ПРОТЫКАЮЩЕЕ МНОЖЕСТВО состоит из кодировок семейств конечных множеств $\{A_1, \ldots, A_m\}$ и натурального числа k, таких что существует множество мощности k, пересекающее *каждое* $A_i, i = 1, \ldots, m$.

Докажите или опровергните, что если язык ПРОТЫКАЮЩЕЕ МНОЖЕСТВО принадлежит **co–NP**, то **NP** = **co–NP**.

Задача 6. (5 баллов)
Боб решил воспользоваться RSA. Для этого он взял числа 133 и 37 и составил из них модуль $133 \cdot 37$. Но Боб не заметил, что число 133 не простое, и вычислил публичный ключ как обратный остаток к своему закрытому ключу по модулю $132 \cdot 36$. Бобу пришло сообщение 31. Какое сообщение было зашифровано, если закрытый ключ Боба 679?

◇ ◇

Задача 7. (5 баллов) Существует Не существует
Пусть построен полиномиальный алгоритм, который умеет находить размер максимальной клики в графе.

Докажите или опровергните, что тогда существует полиномиальный алгоритм, который, получив на вход ДНФ (дизъюнктивную нормальную форму), проверяет ее тавтологичность, т. е. что при всех значениях переменных она истинна.

Задача 8. (8 баллов)
Даны n горизонтальных отрезков, лежащих на оси Ox и заданных массивом координат своих концов $[a_i, b_i]$. Отрезки можно сдвигать вправо и влево вдоль оси Ox. Необходимо с помощью сдвигов сделать так, чтобы пересечение всех отрезков стало непустым. Предложите $O(n \log n)$ алгоритм, который находит требуемый набор сдвигов минимальной суммарной длины. Считайте, что все арифметические операции с координатами выполняются за $O(1)$.

Квадратичный алгоритм оценивается в четверть баллов задачи.

Задача 9. (3 балла) Да Нет

Определим для любого языка $L \subseteq \Sigma^*$ язык его *надслов* $supw(L) = \{u = wsv \mid w, v \in \Sigma^*, s \in L\}$.

Верно ли, что класс **NP** замкнут относительно надслов, т. е. верна ли импликация: если $L \subseteq \mathbf{NP}$, то и $supw(L) \subseteq \mathbf{NP}$?

◇ ◇

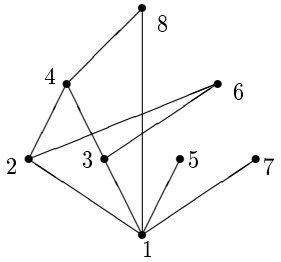
Задача 10. (6 баллов) Да Нет

Определим граф G_n на множестве натуральных чисел чисел $\{1, 2 \ldots, n\}$. в котором вершины — числа, и две вершины соединены тогда и только тогда, когда одно их них делится нацело на другое.

Верно ли, что язык $L = \{(G_n, k)\}$, состоящий из кодировок графов G_n, имеющих независимое множество вершин размера k, является **NP**–полным?

Если ответ положительный, то приведите доказательство. Если ответ отрицательный, то приведите полиномиальный алгоритм, решающий эту задачу.

Считайте, что арифметические операции выполняются за $O(1)$. Ниже изображен граф G_8



Задача 11. (4 балла) Да Нет
Пусть $G = (V, E)$ — это граф с $|V| = n$ вершинами, которые окрашены в k цветов, причем k делит n. Является ли язык НАМРАТН_k, состоящий из описаний k–окрашенных графов, $k \geq 100$, которые содержат k-периодический гамильтонов путь (т. е. цвета вершин при обходе по циклу повторяются с периодом k) **NP**–полным?

◇ ◇

Задача 12. (6 баллов) Да Нет

Определим для любого языка $L \subseteq \Sigma^*$ язык его подслов $subw(L) = \{u \,|\, \exists w, v \in \Sigma^* : wuv \in L\}$

Верно ли, что класс $\mathbf{P}$ замкнут относительно подслов, т. е. верна импликация: если $L \subseteq \mathbf{P}$, то и $subw(L) \subseteq \mathbf{P}$?