Задание на третью неделю.

№1

Пуст дана $3-$CNF формула ϕ. Преобразуем ее следующим образом в Φ:
Сначала из всех дизъюнктов уберем повторяющиеся элементы, т. е. теперь в каждом дизъюнкте все переменные различны. Далее дизъюнкты, в которых 3 переменные оставим без изменения. В которых 2 переменные: $x_1 \vee x_2 \longrightarrow (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \bar{x_3})$. Дизъюнкты с одной переменной: $x_1 \longrightarrow (x_1 \vee x_4 \vee x_3) \wedge (x_1 \vee \bar{x_4} \vee \bar{x_3}) \wedge (x_1 \vee x_4 \vee \bar{x_3})$.
Т. е. i-ый дизъюнкт $d_i(x_1, x_2)$ переходит в $D_i(x_1, x_2, x_3, X_4)$.
Из АЛКТГ очевидно, что если при некоторых переменых x_1, x_2 дизъюнкт $d_i(x_1, x_2) = 1$, то дизъюнкт $D_i(x_1, x_2, x_3, x_4) = 1x_3, x_4$. И наоборот, если при некоторых переменых x_1, x_2 дизъюнкт $d_i(x_1, x_2) = 0$, то дизъюнкт $D_i(x_1, x_2, x_3, x_4) = 0x_3, x_4$. Значит, формула ϕ выполнима (т. е. в ней истинный каждый дизъюнкт) $\iff \Phi$ выполнима. При этом Φ РОВНО-3CNF. Таким образом, при помощи данного полиномиального (длина формулы увеличивается не более чем в 6 раз) преобразования 3CNF сводится к РОВНО-3CNF.

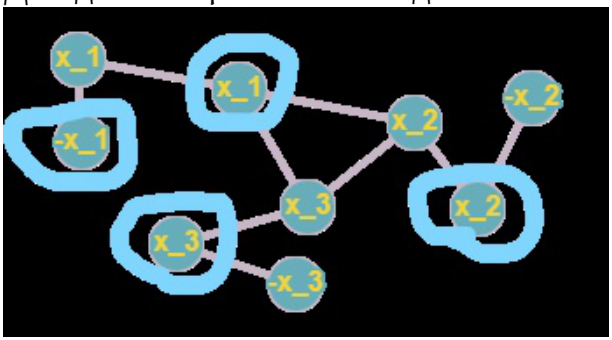
В задачах $3-5$ в начале применим описанный выше алгоритм, чтобы свести 3CNF *к РОВНО–*3CNF*. И работать дальше уже с РОВНО–*3CNF. Для данной λ РОВНО–3CNF: $\lambda(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x_2} \vee x_3) \wedge (x_1 \vee x_2 \vee \bar{x_3}) \wedge (x_1 \vee \bar{x_2} \vee \bar{x_3}) \wedge (\bar{x_1} \vee x_4 \vee x_3) \wedge (\bar{x_1} \vee \bar{x_4} \vee \bar{x_3}) \wedge (\bar{x_1} \vee x_4 \vee \bar{x_3})$.
$\phi = (x_1 \vee x_2 \vee \bar{x_3})$.

№3

35(i) Если у формулы есть выполняющий набор, то в каждом дизъюнкте есть хотя бы одна истинная переменная. Из каждого из m 3-дизъюнкта выберем по одной вершине, соответствующий истинной переменной x_i. Среди выбранных вершин все из разных дизъюнктов, а так же среди них не может быть пары: переменная и ее отрицание, т. к. они не могут одновременно быть истинны (1). Далее для

каждой вершины, уже выбранной в мн-во и соответствующей переменной x_i, добавим в множество вершину, соотв. $\bar{x_i}$ из литеральной пары вершин для переменного x_i Если есть переменные y_i, которым не соответствует ни одна вершина из выбранного множества, то для каждой такой переменной добавим в мн-ве литеральную вершину, соотв. y_i из литеральной пары вершин для y_i. Итого получим $m+n$ вершин, среди которых по одной вершине из каждого дизъюнкта и по одной (это следует из (1)) из каждой литеральной пары. Выберем из получившегося мн-ва две произвольные вершины. Они либо лежат в разнх дизъюнктах, либо в разных литеральных парах, либо одна лежит в паре, а другая в дизъюнкте И тогда они соответствуют двум противоположным переменным (вида x_i и $\bar{x_i}$). Тогда из построения конструкции выбранные вершины графа образуют множество из $m+n$ вершин, никакие две из которого не связаны ребром. Т. е. множество этих вершин покрывает 0 ребер. $\Rightarrow$ Множество из оставшихся вершин покрывает все ребра. Мощность такого множества $3m+2n-(n+m)=2m+n$. $\Rightarrow$ Искомое вершинное покрытие найдено. Из этого следует, что если формула из m дизъюнктов и n переменных выполнима, то в соответствующем ей графе (который можно построить по формуле за полиномиальное время) существует вершинное покрытие мощностью $n+2m$.

Для данного ф это можно сделать так:



Выделенные синим вершины составляют мн-во A. Оставшиеся вершины образуют искомое мн-во вершинного покрытия B из $n+2m=3+2=5$ вершин.

Предположим, что для рассматриваемого графа нашлось вершинное покрытие, множество B, мощностью не более $2m+n$. Рассмотрим дополнение этого мн-ва (в нем не меньше $m+n$ вершин) - мн-во A. Если какие-то две вершины из множества A соединены ребром, то вершины из множества B не покрывают это ребро, а это невозможно, т. к. B вершинное покрытие. Значит, в мн-ве A никакие две вершины

не соединены с друг другом. Из построения из этого следует, что во множестве A все вершины из попарно разных 3-дизъюнктов и литеральных пар, и нету вершины из дизъюнкта и вершины из пары, соответствующих одной переменной. $\Rightarrow$ Мощность мн-ва не больше $m + n$.
Если мощность мн-ва равна $m + n$, из принципа Дирихле во множестве A найдутся вершины из всех 3-дизъюнктов и по одной из каждой пары. Т. к. во множестве при этом не может быть двух вершин из одной литеральной пары, то среди m вершин из A, лежащих в дизъюнктах, нет вершин, соответствующих противоположным переменным. Тогда рассмотрим набор переменных, в котором истинны те и только те литералы, которые соответствуют вершинам множества A, лежащим в дизъюнктах (т. е. те, которые не соединены с вершиной, соотв. противоположной переменной). Это можно сделать из вышесказанного. Полученный набор будет выполнимым, т. к. в каждом из дизъюнктов хотя бы одна переменная истинна. То есть, если в графе G_λ есть вершинное покрытие мощностью не более $2m + n$, то λ выполнима. В случае $36(ii)$ λ невыполнима, а значит в графе G_λ все вершинные покрытия мощностью больше $2m + n$.
Значит, с учетом $35(i)$ полиномиальная (построение графа по форле занимает пол. время) сводимость 3-ВЫПОЛНИМОСТЬ к языку ВЕРШИННОЕ ПОКРЫТИЕ доказана.

№4

$36(i)$ Если у формулы есть выполняющий набор, то в каждом дизъюнкте есть хотя бы одна истинная переменная. Из каждого из m 3-дизъюнкта выберем по одной вершине, соответствующей такой переменной. Среди литералов, соотв. выбранным вершинам, которые все истинны и из разных дизъюнктов, не может быть пары из переменного и его отрицания, т. к. они не могут быть одновременно истинны. Тогда из построения конструкции следует, что все m вершины из этого множества попарно соединены ребрами. Таким образом, клика размером m найдена. Из этого следует, что если формула из m дизъюнктов выполнима, то в соответствующем ей графе (который можно построить по формуле за полиномиальное время) есть клика размером m. Проиллюстрируем на примере данного ϕ:

$\phi = (x_1 \vee x_2 \vee \bar{x_3}), m = 1$. Построенный по описанной конструкции граф:

Выбирая любую вершину из единственного дизъюнкта получаем искомую единичную клику.
Покажем, что если в графе G_λ существует клика мощностью n, то λ, формула с m дизъюнктами, выполнима. Рассмотрим такую клику. Если в ней есть две вершины, соответствующие литералам из одного дизъюнкта или двум противоположным литералам, то между этими вершинами нет ребра (из конструкции), а это невозможно из определения клики. Т. к. мощность клики m, а различных дизъюнктов всего m, то во множестве литералов L, соответствующих вершинам из клики, есть ровно один литерал из каждого дизъюнкта. Тогда, рассмотрим набор переменных, в котором истинны те и только те литералы, которые соответствуют вершинам из множества A. Это можно сделать, т. к. из вышесказанного во мн-ве нету двух противоположных литералов. Полученный набор будет выполнимым, т. к. в каждом из дизъюнктов хотя бы одна переменная истинна. Значит, λ выполнима. В случае $3б(ii)$ λ невыполнима, а значит в графе G_λ все клики мощностью меньше n.
$\Rightarrow$ С учетом $3б(i)$ полиномиальная сводимость языка 3-ВЫПОЛНИМОСТ к языку КЛИКА доказана.

№5

По описанной конструкции построим 2−CNF. Рассмотрим мн-во дизъюнктов L_i, полученное из i-го дизъюнкта$(a_i \vee b_i \vee c_i)$ в форме РОВНО-3CNF. Тогда среди L_i не меньше 3 ложных дизъюнктов: $\bar{a_i} \vee \bar{c_i}, \bar{b_i} \vee \bar{c_i}, \bar{a_i} \vee \bar{d_i}$. При $d_i = 1$ оставшиеся 7 дизъюнктов истинны. Если среди a_i, b_i, c_i только один равен 0, для определенности c_i, то ложны не меньше 3 дизъюнктов: $c_i, \bar{a_i} \vee \bar{d_i}$ и один из $d_i, c_i \vee \bar{d_i}$. При $d_i = 1$ оставшиеся 7 дизъюнктов истинны. Если среди a_i, b_i, c_i, только один равен 1, для определенности a_i, то ложны не меньше трех: b_i, c_i и один из $d_i, \bar{a_i} \vee \bar{d_i}$. При $d_i = 1$, оставшиеся 7 дизъюнктов истинны.

Если $a_i = b_i = c_i = 0$, то ложных дизъюнктов не менее четырех: a_i, b_i, c_i и один из $d_i, c_i \vee \bar{d}_i$. $\Rightarrow$ Значение d_i можно подобрать так, чтобы среди L_i было 7 дизъюнктов $\Longleftrightarrow$ Среди a_i, b_i, c_i есть переменная равная 1 $\Longleftrightarrow$ i-ый дизъюнкт в исходном РОВНО-3CNF истинный. Таким образом, если все k дизъюнкты в РОВНО-3CNF выполнимы (т. е формула выполнима), то в получившейся 2CNF 7k выполненых дизъюнктов. Если хотя бы один из дизъюнктов в РОВНО-3CNF не выполняется (т. е формула невыполнима), то в получившейся 2CNF $\leq 7(k-1)+6 = 7k-1$ выполненых дизъюнктов. Таким образом, при $q = 7$ описанная конструкция полиномиально сводит РОВНО-3CNF к 2CNF.
Проиллюстрируем на примере 37(ii):
Построенная 2CNF:

$$x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge (x_1 \vee \bar{x_2}) \wedge (\bar{x_1} \vee \bar{x_3}) \wedge (\bar{x_2} \vee \bar{x_3}) \wedge (\bar{x_1} \vee \bar{x_4}) \wedge (x_2 \vee \bar{x_4}) \wedge (x_3 \vee \bar{x_4}).$$

Пороговое значение $kq = 7$.
37(ii) Такие наборы переменных были рассмотренны выше. Т. е. например при $x_1 = x_2 = x_3 = x_4 = 1$.

№2

34(i) Построим A_ϕ: $\{x_1, \bar{x_1}\}, \{x_2, \bar{x_2}\}, \{\bar{x_3}, x_3\}$. Протыкающем множеством из $n = 3$ элементов будет, например: $\{x_1, x_2, \bar{x_3}\}$.
Покажем, что если формула выполнима, то A_ϕ имеет протыкающее мн-во мощностью n. Если у формулы есть выполняющий набор, то в каждом дизъюнкте есть хотя бы один истинный элемент (здесь $\bar{x_i}$ тоже считается за элемент). Из каждого из n дизъюнкта выберем по одному такому элементу. Уберем из выбранного мн-ва все дубли, т. е. оставим только попарно разные элементы. Получим мн-во B. Среди выбранных элементов не может быть пары из переменного и его отрицания, т. к. они не могут быть одновременно истинны. Значит никакие два элемента из B не лежат в одном подмн-ве вида $A_i = \{x_i, x_i\}$. Пусть мощность B равна k. Тогда мн-во B пересекает все подмн-ва вида A_c и k из n подмн-в вида A_i. Добавив в мн-во B по одному элементу из $n-k$ еще не перечисленных подмн-в вида A_i получим мн-во B_1, мощностью n, и пересекающее все подмн-ва. Таким образом, если формула выполнима, то A_ϕ имеет протыкающее

мн-во мощностью n.
Покажем, что если A_λ имеет протыкающее мн-во мощностью n, то формула λ выполнима. Т. к. в подмн-ах вида A_i различные элементы, а их всего n, то в протыкающем множестве B мощностью n, должно быть ровно по одному элементу из каждого такого подмножества. Т. е. в B не может быть двух противоположных элементов (x_i и $\bar{x_i}$). Тогда можно взять такой набор из переменных, где истинны те и только те элементы, которые входят в мн-во B. При этом формула будет выполнима, т. к. мн-во B имеет хотя бы один общий элемент с каждым дизъюнктом, а значит в каждом дизъюнкте точно есть истинный элемент. $\Rightarrow$ Если A_λ имеет протыкающее мн-во мощностью n, то формула λ выполнима.
$34(i)$ Данное λ невыполнимо, $n = 2$, значит мощность протыкающего мн-ва больше двух.
Т. к. A_λ имеет протыкающее мн-во мощностью $n \iff$ формула λ выполнима, а построение сводящей конструкции занимает полиномиальное время, то ВЫПОЛНИМОСТЬ сводится к языку ПРОТЫКАЮЩЕЕ МНОЖЕСТВО.

№6

Аналогично задачи 10(Доп) из прошлого задания, где мы использовали сводимость к SAT. Только теперь оракул выдает ответ за полиномиальное время, а это влияет в решении только на степень полиномиальной сложности поиска раскраски.

№8

По теореме о простоте выполнение следующих условий

- $g^{p-1} \equiv 1 \pmod p$
- $\forall$ простого делителя q числа $p - 1 \to g^{(p-1)/q} <> 1 \pmod p$.

$\iff p$ простое число.
Тогда в качестве сертификата $s(p)$ возьмем число g и разложение

$p-1$ на простые множители $p_1, p_2, \ldots, p_m$ (которых $\leq \log_2 p$) и соответствующие им сертификаты (для делителей > 5) $s(p_1), \ldots s(p_n)$. Таким образом, сертификат определен рекурсивно, множество необходиое для сертификата будет пополняться пока не дойдет до известных нам простх чисел. Такой сертификат имеет полиномиальную сложность (можно показть по индукции по кол-во уровней рекурсии). Тогда, алгоритм верификации должен будет проверить, что:

1. $p_1 \ldots p_m = p - 1$, проверяется прямым умножением за полиномиальное время.
2. Возвести число g в степени $g^{p-1}, g^{(p-1)/p_n}, \ldots g^{(p-1)/p_n}$ (т. е. $n+1$ раз возвести в степень $\leq p-1$) и проверить у полученных чисел остатки от деления на p. Это все можно сделать за полиномиальное время.
3. Проверить на простоту числа $p_1, p_2, \ldots, p_n$. С помощью их сертификатов это можно сделать за полиномиальное время.

Приведем сертификат для $p = 3911, g = 13$:

- $3911 : g = 13, 3910 = 2 \cdot 5 \cdot 17 \cdot 23$
  - 2: известное простое
  - 5: известное простое
  - 17: $g = 2, 16 = 2^4$
    - 2: известное простое
  - 23: $g = 2, 22 = 2 \cdot 11$
    - 2: известное простое
    - 11: $g = 2, 10 = 2 \cdot 5$
      - 2: известное простое
      - 5: известное простое

№7

Покажем равновыполнимость:
Если существует набор переменных $x_1, ..., x_n$, то подставив их и зна-

чения $y_1, ..., y_m$, посчитанные по ним (т. е. $y_1 = x_1 \vee x2, \dots$), получим истинную формулу (т. к. первые m дизъюнктов это просто равенства для $y_1, \dots, y_m$ (очевидно выполняемые), преобразованные в КНФ, а последний дизъюнкт $y_m = 1$, т. к. y_m равно значению $CircuitSat$ при этих переменных $x_1, ..., x_n$, а оно истинно). Значит формула выполнима.

И наоборот, если формула, построенная по схеме, истинна при некоторых переменных, то равенства $y_1 = .., \dots, y_n = \dots$ выполняются и y_m истинно. При этом y_m равно значению $CircuitSat$ при этих же переменных $x_1, \dots x_n$. Значит $CircuitSat$ выполнима.

Таким образом, равновыполнимость формулы доказана.