Алгоритмы и модели вычислений.
Задание 5: сложность вычислений: классы P, NP, co-NP II

Сергей Володин, 272 гр.

задано 2014.03.13

Задача 1

1. Докажем, что HAMPATH $\leqslant_m^p$ UHAMPATH.
HAMPATH $= \{(G,s,t) \big| G -$ ориентированный граф, в G существует гамильтонов путь из s в $t\}$,
UHAMPATH $= \{(G,s,t) \big| G -$ неориентированный граф, в G существует гамильтонов путь из s в $t\}$.
Пусть G — ориентированный граф, s и t — его вершины. $x = (G,s,t)$. Определим $f(x) = (G', s', t')$. Для каждой вершины $v \in V(G)$, кроме s и t, добавим в $V(G')$ три вершины v_i, v_m, v_o. Для s и t добавим s_o и t_i. Соединим $v_i \leftrightarrow v_m$ и $v_m \leftrightarrow v_o$ (стрелкой $\leftrightarrow$ обозначено неориентированное ребро). Для каждого $(u,v) \in E(G)$ добавим $(u_o, v_i) \in E(G')$. G' — получившийся граф, $s' = s_o$, $t' = t_i$.
   (a) Пусть $x = (G,s,t) \in$ HAMPATH. Тогда существует путь $s \to v_1 \to v_2 \to ... \to v_n \to t$. По построению, тогда существует путь $s_o \leftrightarrow v_{1i} \leftrightarrow v_{1m} \leftrightarrow v_{1o} \leftrightarrow ... \leftrightarrow v_{ni} \leftrightarrow v_{nm} \leftrightarrow v_{no} \leftrightarrow t_i$, который является гамильтоновым путем в G' (все вершины по построению: для каждой вершины исходного графа, кроме s и t добавляются 3 в образе, все они посещены. s_o и t_i также посещены. Если есть повтор $v_{i\cdot} = v_{j\cdot}$, то (структура пути в образе) есть повтор $v_{im} = v_{jm}$. Значит, есть повтор в исходном пути — противоречие), поэтому $f(x) \in$ UHAMPATH
   (b) Пусть $f(x) = (G', s_o, t_i) \in$ UHAMPATH. Из вершины с индексом $\cdot_o$ по построению есть ребра только в вершины с индексом $\cdot_i$. Из вершины v_i есть ребро только в v_m, из вершины v_m — только в v_o. Поэтому гамильтонов путь имеет вид $s_o \leftrightarrow v_{1i} \leftrightarrow v_{1m} \leftrightarrow v_{1o} \leftrightarrow ... \leftrightarrow v_{ni} \leftrightarrow v_{nm} \leftrightarrow v_{no} \leftrightarrow t_i$, значит, в исходном графе G есть путь $s \to v_1 \to v_2 \to ... \to v_n \to t$, и он гамильтонов (аналогично: все вершины по построению, повтор означает повтор в другом пути — противоречие), поэтому $x \in$ HAMPATH
   (c) f — вычислима за полиномиальное время (линейное по количеству ребер и вершин время)
2. Поскольку HAMPATH $\in \mathsf{NP}$-c, HAMPATH $\leqslant$ UHAMPATH, UHAMPATH $\in \mathsf{NP}$, то (см. решение 4-го задания, вспомогательные утверждения, 2) UHAMPATH $\in \mathsf{NP}$-c $\blacksquare$

Задача 2

См. (каноническое) 21

Задача 3

Получилось доказать не совсем то, что нужно

1. $\mathcal{C} \supset \mathsf{NP} \cup \text{co-}\mathsf{NP}$.

   (a) Пусть $L \in \mathsf{NP}$. Тогда (семинар) $L \leqslant_m^p \text{SAT} \Leftrightarrow \exists f\colon \Sigma^* \to \Sigma^*\colon \forall x(x \in L \Leftrightarrow f(x) \in \text{SAT})$, f — вычислима за полиномиальное время. Определим M_{SAT}: вычисляем за полиномиальное время (определение сводимости) $f(x)$ (x — вход), спрашиваем оракула $f(x) \overset{?}{\in} \text{SAT}$ за $O(1)$. Ответ — ответ оракула (корректно из определения сводимости). Время работы полиномиально: $T(|x|) = \text{poly}(|x|) + O(1) = \text{poly}(|x|)$.

   (b) Пусть $L \in \text{co-}\mathsf{NP}$. Тогда $\overline{L} \leqslant_m^p \text{SAT} \Leftrightarrow \exists f\colon \Sigma^* \to \Sigma^*\colon \forall x(x \in \overline{L} \Leftrightarrow f(x) \in \text{SAT}) \Leftrightarrow \forall x(x \in L \Leftrightarrow f(x) \notin \text{SAT})$, f — вычислима за полиномиальное время. Определим M_{SAT}: вычисляем за полиномиальное время (определение сводимости) $f(x)$ (x — вход), спрашиваем оракула $f(x) \overset{?}{\in} \text{SAT}$ за $O(1)$. Ответ — <u>противоположный</u> ответу оракула (корректно из определения сводимости). Время работы полиномиально: $T(|x|) = \text{poly}(|x|) + O(1) = \text{poly}(|x|)$.

2. *(Идея обсуждалась с Дарьей Решетовой).* Пусть $L \in \mathcal{C}$. Тогда существует МТ M_{SAT}, вычисляющая $x \overset{?}{\in} L$ за полиномиальное время, и делающая не более одного обращения к оракулу $t \overset{?}{\in} \text{SAT}$. Рассмотрим машину M_{SAT}. Она может обращаться к оракулу, либо не обращаться. Если она обращается к оракулу на входе x, обозначим $n(x) = 1$, иначе $n(x) = 0$. В первом случае до обращения к оракулу $Or(x)$ она вычисляет вход $f(x)$ для него. После обращения (получения $f(x) \overset{?}{\in} L$, 0 либо 1), машина выдает ответ (0 либо 1). Если ответ тот же, обозначим $s(x) = 0$, иначе $s(x) = 1$. В случае, если M_{SAT} не обращается к оракулу, она выдает ответ, вычисляя $a(x) \in \{0, 1\}$. Поэтому ее можно представить следующим псевдокодом:

```
M(x)
{
  if(n(x)) return(Or(f(x)) ^ s(x));
  else return(a(x));
}
```

   Поскольку M_{SAT} полиномиальна, $n(\cdot)$, $s(\cdot)$, $a(\cdot)$ вычислимы за полиномиальное время.
   Обозначим

   (a) $L_a = \{x \big| n(x) = 0 \wedge a(x) = 1\}$,

   (b) $L_0 = \{x \big| n(x) = 1 \wedge s(x) = 0 \wedge Or(f(x)) = 1\}$,

   (c) $L_1 = \{x \big| n(x) = 1 \wedge s(x) = 1 \wedge Or(f(x)) = 0\}$.

   Тогда $L = L_a \cup L_0 \cup L_1$ (все случаи в псевдокоде выше).

   (a) Получаем, что $L_a \in P$ (так как $a(\cdot)$ и $n(\cdot)$ вычислимы за полиномиальное время).

   (b) Докажем, что $L_0 \in \mathsf{NP}$. $Or(f(x)) = 1 \Leftrightarrow f(x) \in \text{SAT}$. Поскольку $\text{SAT} \in \mathsf{NP}$, то $\forall t(t \in \text{SAT} \Leftrightarrow \exists y\colon R_{\text{SAT}}(t, y) = 1)$, R_{SAT} — вычислима за полиномиальное время, $|y| = \text{poly}(|x|)$. Определим $R(x, y) = n(x) \wedge \neg s(x) \wedge R_{\text{SAT}}(f(x), y)$ — вычислима за полиномиальное время.

      i. Пусть $x \in L_0$. Тогда $n(x) = 1$, $s(x) = 0$, и $f(x) \in \text{SAT} \Rightarrow \exists y\colon R_{\text{SAT}}(f(x), y) = 1$. Получаем $x \in L_0 \Rightarrow \exists y\colon R(x, y) = 1$.

      ii. Пусть $x \notin L_0$. Тогда, либо $n(x) = 0$, и тогда для всех $y \hookrightarrow R(x, y) = 0$, аналогично в случае $s(x) = 1$: $\forall y \hookrightarrow R(x, y) = 0$. Если $n(x) = 1$ и $s(x) = 0$, то $f(x) \notin \text{SAT}$, и для всех $y \hookrightarrow R_{\text{SAT}}(x, y) = 0$, откуда $\forall y \hookrightarrow R(x, y) = 0$.

      Итак, $\forall x(x \in L_0 \Leftrightarrow \exists y\colon R(x, y) = 1)$ ■

   (c) Докажем, что $L_1 \in \text{co-}\mathsf{NP}$. Определим $R(x, y) = \neg n(x) \vee \neg s(x) \vee R_{\text{SAT}}(f(x), y)$ — вычислима за полиномиальное время.

      i. Пусть $x \in L_1 \Leftrightarrow x \notin \overline{L_1}$. Тогда $n(x) = 1 \Rightarrow \neg n(x) = 0$, $s(x) = 1 \Rightarrow \neg s(x) = 0$, и $f(x) \notin \text{SAT}$, откуда $\forall y \hookrightarrow R_{\text{SAT}}(f(x), y) = 0$. Получаем $x \notin \overline{L_1} \Rightarrow \forall y \hookrightarrow R(x, y) = 0 \vee 0 \vee 0 = 0$.

      ii. Пусть $x \notin L_1 \Leftrightarrow x \in \overline{L_1}$. Тогда, либо $n(x) = 0$, и тогда для всех $y \hookrightarrow R(x, y) = 1$, аналогично в случае $s(x) = 0$: $\forall y \hookrightarrow R(x, y) = 1$. Если $n(x) = 1$ и $s(x) = 1$, то $f(x) \in \text{SAT}$, и $\exists y\colon R_{\text{SAT}}(x, y) = 1$, откуда $\exists y\colon R(x, y) = 1$

      Итак, $\forall x(x \in \overline{L_1} \Leftrightarrow \exists y\colon R(x, y) = 1)$ ■

   Получаем, что $L = \underbrace{L_a}_{\in \mathsf{P}} \cup \underbrace{L_0}_{\in \mathsf{NP}} \cup \underbrace{L_1}_{\in \text{co-}\mathsf{NP}}$.

   Поскольку $L_a \cup L_0 \in \mathsf{NP}$ (сертификат для слов из L_0 тот же, в предикат добавляется «или ($y = \varepsilon$ и $x \in L_a$)» — вычислимо за полиномиальное время), для краткости запишем $L = L_0 \cup L_1$, где $L_0 \in \mathsf{NP}$, $L_1 \in \text{co-}\mathsf{NP}$.

Итак, $\mathsf{NP} \cup \text{co-}\mathsf{NP} \subset \mathcal{C} \subset \{L \big| L = L_0 \cup L_1\colon L_0 \in \mathsf{NP},\ L_1 \in \text{co-}\mathsf{NP}\}$

(каноническое) Задача 21

ГЦ $= \{G$ — ориентированный граф$|$в G существует гамильтонов цикл$\}$.
ГП $= \{(G, s, t)$ — ориентированный граф, две его вершины$|$в G существует гамильтонов путь из s в $t\}$.

1. Докажем, что ГП $\leqslant_m^p$ ГЦ. Пусть $x = (G, s, t)$ — граф и две его вершины. Определим граф $f(x)$: возьмем G, удалим все ребра между s и t, все ребра в s, все ребра из t. Добавим одно $t \to s$.

   (a) Пусть $x \in$ ГП, то есть, в G есть гамильтонов путь из s в t. Тогда в этом пути нет ребер из t в s (иначе через t или s путь пройдет дважды). Значит, путь будет гамильтоновым и в $f(x)$. Но в $f(x)$ есть ребро $t \to s$, получаем гамильтонов цикл, составленный из пути и одного ребра. Значит, $f(x) \in$ ГЦ

   (b) Пусть $f(x) \in$ ГЦ, то есть, в $f(x)$ есть гамильтонов цикл. В этот цикл входят вершины s и t, так как в него входят все вершины графа. Но из t нет других ребер, кроме как в s (по построению), значит, в цикл входит ребро $t \to s$. Рассмотрим весь путь без этого ребра. Он гамильтонов, так как является гамильтоновым циклом без одного ребра. Этот путь будет также путем в G, так как не содержит ребра $t \to s$, а в G ребер больше (кроме $t \to s$). Также этот путь будет гамильтоновым, так как множества вершин G и $f(x)$ совпадают. Значит, $x \in$ ГП

   (c) Сводимость f в явном виде. $A[i][j]$ — матрица графа G, $B[i][j]$ — матрица графа $f(x)$. $A[i][j] = 1 \Leftrightarrow$ есть ребро из i-й вершины в j-ю. $|V(G)| = n$. Считаем, что s и t — индексы вершин s и t. Алгоритм:

```
for(i = 0; i < n; i++)
  for(j = 0; j < n; j++)
    B[i][j] = A[i][j]; // copying graph f(x) := G

for(i = 0; i < n; i++)
{
  B[i][s] = 0; // removing edges to s
  B[t][i] = 0; // removing edges from t
}

B[t][s] = 1; // adding edge from t to s
```

   Получаем, что f — вычислима за полиномиальное время: $T(G) = O(n^2) + O(n) + O(1) = O(n^2)$. Длина записи графа $l(G) = \Omega(n^2)$ (элементы матрицы $n \times n$), поэтому $T(G) = O(l(G))$, т.е. время вычисления f линейно по длине входа.

2. *(Идея обсуждалась с Игорем Силиным).* Докажем, что ГЦ $\leqslant_m^p$ ГП. Пусть $x = G$ — граф. Фиксируем некоторую его вершину v. «Разделим» ее на две вершины s и t, из s добавим все ребра из v, в t направим все ребра в v. Удалим ребра между s и t. Получим граф G'. Определим $f(x) = (G', s, t)$.

   (a) Пусть $x \in$ ГЦ. Тогда в $x = G$ существует гамильтонов цикл. Он содержит все вершины, в том числе и вершину v: $v \to v_1 \to \ldots \to v_n \to v$. Тогда в графе G' образа $f(x)$ будет путь $s \to v_1 \to \ldots \to v_n \to t$, и он будет гамильтоновым (все вершины по построению, вершины v_i не повторяются, т.к. исходный цикл гамильтонов, если t или s повторяется, то v встречается более 2-х раз в цикле — противоречие), т.е. $f(x) \in$ ГП

   (b) Пусть $f(x) \in$ ГП. Тогда существует гамильтонов путь $s \to \ldots \to t$. Значит, в G есть цикл $v \to \ldots \to v$, и он гамильтонов (в ... все вершины, кроме s и t для образа, значит, там все вершины, кроме v для исходного графа). Получаем $x \in$ ГЦ.

   (c) Сводимость f в явном виде. $A[i][j]$ — матрица графа $x = G$, $B[i][j]$ — матрица графа из $f(x)$. $|V(G)| = n$. Алгоритм:

```
v = n - 1; // any vertex of G
s = v;
t = v + 1; // new vertex

for(i = 0; i < n + 1; i++)
  for(j = 0; j < n + 1; j++)
    B[i][j] = 0;

for(i = 0; i < n; i++)
{
  if(A[v][i] == 1)
    B[s][i] = 1; // (v, i) in E <=> (s, i) in E'
  if(A[i][v] == 1)
    B[i][t] = 1; // (i, v) in E <=> (i, t) in E'
}

for(i = 0; i < n - 1; i++)
  for(j = 0; j < n - 1; j++)
      B[i][j] = A[i][j]; // copying rest of the graph

B[t][s] = 0; // (t, s) not in E'
B[s][t] = 0; // (s, t) not in E'
```

   Получаем, что f — вычислима за полиномиальное время: $T(G) = O(n^2) + O(n) + O(1) = O(n^2)$, аналогично $T(G) = O(l(G))$.

(каноническое) Задача 23

1. $\Psi(x_1, x_2) \stackrel{\text{def}}{=} (\neg x_1 \vee x_2)$. Базовое множество $(n = 2)$ $\{x_1, x_2, \neg x_1, \neg x_2\}$.
   Семейство подмножеств $A_\Psi = \big\{\{x_1, \neg x_1\},\ \{x_2, \neg x_2\},\ \{\neg x_1, x_2\}\big\}$.
   $\measuredangle A \stackrel{\text{def}}{=} \{x_1,\ x_2\}$. Получаем $A \cap \{x_1, \neg x_1\} \ni x_1$, $A \cap \{x_2, \neg x_2\} \ni x_2$, $A \cap \{\neg x_1, x_2\} \ni x_2$.
   Значит, A — протыкающее множество для A_Ψ, и $|A| = 2$.

2. $\chi(x_1, x_2, x_3) \stackrel{\text{def}}{=} (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge \neg x_3$. Семейство подмножеств $(n = 3)$ $A_\chi = \big\{\{x_1, \neg x_1\}, \{x_2, \neg x_2\}, \{x_3, \neg x_3\}, \{x_1, x_2, x_3\}, \{\neg x_1, \neg x_2\}, \{x_1, \neg x_2\}, \{\neg x_1, x_2, x_3\}, \{\neg x_3\}\big\}$. Пусть A — протыкающее множество. Тогда $A \cap \{\neg x_3\} \neq \varnothing \Rightarrow A \ni \neg x_3$. Также $A \cap \{x_1, \neg x_1\} \neq \varnothing$, поэтому A содержит x_1 или $\neg x_1$. Аналогично $x_2 \in A$ или $\neg x_2 \in A$. Получаем, что A содержит не менее трех элементов. Предположим, что их ровно 3. Рассмотрим все возможные 4 случая (или×или раньше по тексту):

   (a) $A = \{x_1, x_2, \neg x_3\}$. Тогда $A \cap \{\neg x_1, \neg x_2\} = \varnothing$ — противоречие.

   (b) $A = \{x_1, \neg x_2, \neg x_3\}$. Тогда $A \cap \{\neg x_1, x_2, x_3\} = \varnothing$ — противоречие.

   (c) $A = \{\neg x_1, x_2, \neg x_3\}$. Тогда $A \cap \{x_1, \neg x_2\} = \varnothing$ — противоречие.

   (d) $A = \{\neg x_1, \neg x_2, \neg x_3\}$. Тогда $A \cap \{x_1, x_2, x_3\} = \varnothing$ — противоречие.

   Получаем, что A содержит более трех элементов ■