Что такое проблема P vs NP?

Занятие 3. Полиномиальные верификаторы. NP-полные задачи
Определения и задачи

Верификатором для языка A называется такой алгоритм V, что $A = \{w : V$ принимает пару $\langle w, c\rangle$ для некоторого слова $c\}$. При этом слово c называется доказательством или сертификатом принадлежности слова w языку A. Верификатор полиномиальный, если время его работы на входе $\langle w, c\rangle$ есть $O(n^k)$ для некоторого k, где n — длина слова w. Заметим, что длина сертификата для полиномиального верификатора тоже есть полином от слова языка (за полиномиальное время машина может пройти только по полиномиальному количеству клеток ленты).

1. Докажите, что язык лежит в классе NP тогда и только тогда, когда у него есть полиномиальный верификатор.

2. Про все языки из класса NP, встречавшиеся в предыдущих листках, докажите их принадлежность NP с помощью альтернативного определения из задачи 1.

Символы $\wedge$, $\vee$, $\neg$ обозначают логическое И, ИЛИ и НЕ соответственно (вместо $\neg$ используют также черту сверху $^{-}$). С помощью этих операций из переменных, принимающих значения ИСТИНА и ЛОЖЬ, можно составлять формулы. Например, $(\bar{x} \wedge y) \vee (x \wedge \bar{x})$ или $(z \vee \bar{y}) \wedge (x \vee z \vee \bar{y}) \wedge y$. Формула называется выполнимой, если существует такой набор присвоений переменным значений ИСТИНА и ЛОЖЬ, так что значение формулы становится ИСТИНА. $SAT = \{\langle\phi\rangle : \phi$ — выполнимая формула$\}$, $kSAT = \{\langle\phi\rangle : \phi$ — формула, являющаяся логическим И скобок, каждая из которых есть логическое ИЛИ k переменных или их отрицаний$\}$.

3. Докажите, что SAT и $kSAT$ для любого k лежат в NP.

4. Докажите, что $2SAT$ лежит в P.

Функция $f\colon \Sigma^* \to \Sigma^*$ полиномиально вычислима, если существует такая машина Тьюринга, работающая за полиномиальное время, которая, получив на вход слово w, завершает работу со словом $f(w)$ на ленте. Мы говорим, что язык $A \subseteq \Sigma^*$ полиномиально сводится к языку $B \subseteq \Sigma^*$ и пишем $A \leqslant_P B$, если существует такая полиномиально вычислимая функция $f\colon \Sigma^* \to \Sigma^*$, называемая сводимостью, что $w \in A \Leftrightarrow f(w) \in B$.

5. **а)** Докажите, что если $A \leqslant_P B$ и $B \in \mathrm{P}$, то $A \in \mathrm{P}$. **б)** Докажите, что если $A \leqslant_P B$ и $B \in \mathrm{NP}$, то $A \in \mathrm{NP}$. **в)** Докажите, что если $A \leqslant_P B$ и $B \leqslant_P C$, то $A \leqslant_P C$.

6. Докажите следующие сводимости: **а)** $3SAT \leqslant_P SAT$; **б)** $SAT \leqslant_P 3SAT$; **в)** $3SAT \leqslant_P CLIQUE$; **г)** $3SAT \leqslant_P HAMPATH$ (определения $CLIQUE$ и $HAMPATH$ см. в предыдущем листке).

Язык A называется NP-полным, если $A \in \mathrm{NP}$ и для любого $B \in \mathrm{NP}$ выполнено $B \leqslant_P A$.

7. Докажите, что если какой-то NP-полный язык лежит в P, то P = NP.

8. **а)** Докажите, что SAT NP-полный. **б)** Докажите, что $HAMPATH$ NP-полный.

9. Докажите, что если A является NP-полным, язык B лежит в NP и $A \leqslant_P B$, то B является NP-полным.

10. Предположим, P $\neq$ NP. Докажите тогда, что в NP существуют языки, которые не лежат в P, но и не являются NP-полными.