

1. NP-полнота

Определение 1. $VERTEX - COVER = \{(G, R) : \text{в графе } G \exists \text{ вершинное покрытие размером } k\} \in NPC$

$$3 - SAT \leq_p VERTEX - COVER$$

Определение 2. $3-COL = \{G : \text{граф } G \text{ можно раскрасить в 3 цвета}\}$

Определение 3. $SUBSET - SUM = \{(n_1, n_2, \dots, n_k, N) : \exists m \exists i_1, \dots, i_m; n_{i_1} + \dots + n_{i_m} = N\}$

$$3SAT \leq_p SUBSET - SUM$$

Определение 4. $HAMPATH = \{(G, s, t) : \text{в ор. графе } G \exists \text{ гамильтонов путь из } s \text{ в } t\}$

$$UHAMPATH = \{(G, s, t) : \text{в неор.графе } G \exists \text{ путь из } s \text{ в } t\}$$

Определение 5. $CoNP = \{L : \bar{L} \in NP\}$

$$P \subset NP \cap coNP$$

$$\bar{L} \in NP \exists p \exists q \exists M(x \in \bar{L} \Leftrightarrow \exists s |s| = p(|x|), M(x, s) = 1)$$

$$\exists p \exists q \exists M(x \in L \Leftrightarrow \forall s (|s| = p(|x|) \rightarrow M(x, s) = 0))$$

Определение 6. $TAUT = \{\varphi : \varphi - \text{тавтология}\} \in CoNP$

Определение 7. $EXP = \bigcup DTIME(2^n)$

Определение 8. $NEXP = \bigcup NTIME(2^n)$

Теорема 1. $EXP \neq NEXP \Rightarrow P \not\subseteq NP$

Доказательство. Пусть $L \in NEXP, L \in NTIME(2^{n^L})$

$$L_{pad} = \{x01^{2^{|x|^c}} : x \in L\}$$

$$L \in NEXP \Rightarrow L_{pad} \in NP$$

1. Проверить, что вход имеет вид $x01^{2^{|x|^c}}$

2. Проверить, что $x \in L$. На недет. маш. $O(2^{n^c})$ шагов \Rightarrow лин. время от длины входа. $P = NP, L_{pad} \in NP \Rightarrow L \subset EXP$ (приписать) $01^{2^{|x|^c}}$ и применить алгоритм для L_{pad})

Утверждение 1. Если $P = NP$, то $\forall P \in NP \exists$ полиномиальный алгоритм, находящий сертификат для $x \in L$

Доказательство.

1. Док-во для SAT Пусть $\varphi \in SAT, x_1, \dots, x_k$ - пер-ые. $\varphi_0 = \varphi(x_2 \dots x_k) = \varphi(0, x_2 \dots x_k)$ $\varphi_1 = \varphi(1, x_2, \dots x_k)$