1. Модели вычислений. Машины Тьюринга

Классическая машина Тьюринга:
Σ - входной алфавит, $\Gamma \subset \Sigma$ - ленточный алфавит.
$\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R, N\}$ - программа.
q_1 - начальное состояние, q_a, q_r - принимающее и отвергающее состояния.

Варианты машин:

1. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$
2. Лента, бесконечная лишь с одной стороны
3. Уменьшение алфавита Σ
4. Многоленточные машины $\delta : Q \times \Gamma^k \to Q \times \Gamma^k \times \{L, R, N\}^k$

Тезис Черча-Тьюринга
Любой алгоритм можно реализовать на МТ.
Усиленный:
Любую вычислительную систему можно смоделировать на МТ с не более чем полиномиальным временем.
Конфигурация - набор $AqaB$, где q - текущее состояние, a - текущий символ, A - слово слева от a, B - слово справа.
Кроме AaB на ленте только пробелы
Протокол - последовательность конфигураций в процессе работы.
Универсальная МТ: $U(p, x) = M_p(x)$
Язык $L \subset \{0, 1\}^*$

Класс P $= \cup_{k=1}^{\infty} DTIME(n^k)$, $L \in DTIME(t(n))$, если $\exists$ МТ M:

1. Если $x \in L$, то $M(x) = 1$
2. Если $x \notin L$, то $M(x) = 0$
3. $\forall x \exists c$, если $|x| = n$, то $M(x)$ работает $\leq ct(n)$ шагов.

Класс NP: $L \in NP$, если $\exists$ алгоритм $V(..)$:

1. $x \in L \to \exists s : |s| \leq p(|x|), V(x, s) = 1$
2. $x \notin L \to \forall s : |s| \leq p(|x|), V(x, s) = 0$
3. $\forall x \forall s |s| \leq p(|x|), V$ работает не более чем за $q|x|$ шагов.

Th.$P \subset NP$
Док-во:$V(x, s) = M(x)$

2. Недетерминированные МТ

Может быть несколько команд с одной и той же Л.И.$\delta : Q \times \Gamma \Rightarrow Q \times \Gamma \times \{L, R, N\}$
Если несколько вариантов, вычисления разделяются на ветви.
Если на хотя бы на одной ветви q_a - ответ 1.
Если везде q_r - ответ 0.
Если есть бесконечная ветвь - ответа нет.

NTIME(t(n)) - класс языков L: $\exists$ НМТ M:

1. $x \in L \to M(x) = 1$
2. $X \notin L \to M(x) = 0$

3. $\exists c \forall x$ любая ветвь $M(x)$ работает не более чем за $ct(|x|)$ шагов.

Класс NP $= \cup_{k=1}^{\infty} NTIME(n^k)$

$$P = \cup_{k=1}^{\infty} DTIME(n^k)$$

$$NP = \cup_{k=1}^{\infty} NTIME(n^k)$$

$$EXP = \cup_{k=1}^{\infty} DTIME(\chi^{n^k})$$

Теорема 1. $NP \subset EXP$

2.1. Сводимость

Определение 1. L - полиномиально сводится (по Карпу) к языку M, если $\exists$ полиномиальная вычислимая функция: $x \in L \Leftrightarrow f(x) \in M, f : \{0,1\}^* \to \{0,1\}^*$

Утверждение 1.

1. $L \leq_p M, M \in P \Rightarrow L \in P$
2. $L \leq_p M, M \leq_p \Rightarrow L \leq_p N$
3. $L \leq_p M, M \in NP \Rightarrow L \in NP$

Определение 2. Язык M является NP-hard, если $\forall L \in NP \to L \leq_p M$

Определение 3. Язык M является NP-complete, если он NP-hard и $M \in NP$

Утверждение 2. L - NP-hard, $Lle_p M \Rightarrow M - NP - hard$
L - NP-complete, $L \leq_p M, M \in NP \Rightarrow M - NP - complete$

Определение 4. TMSAT $= \{(\alpha, x, 1^n, 1^k) : \exists u \in \{0,1\}^n : M_\alpha(x,u) = 1; M_\alpha(x,u)$ работает k шагов $\}$.

Теорема 2. *TMSAT - NP-полный язык.*

Доказательство.

1. TMSAT $\in NP$
   u - сертификат. Проверка: запустить $M_\alpha(x,u)$ на k шагов.
2. TMSAT - NP-complete.
   $L \in NP \Rightarrow L \leq_p TMSAT$
   $L \in NP \Rightarrow \exists p \exists V \exists q x \in L \Leftrightarrow \exists s \in \{0,1\}^{p(|x|) V(x,s)=1}$ и $V(x,s)$ работает $\leq q(|x| + |s|)$ шагов.
   $f(x) = (\lfloor V \rfloor, x, 1^{p(|x|)}, 1^{q(|x|+p(|x|))})$, $\lfloor V \rfloor$ - программа V.

$\square$

Определение 5. SAT $= \{\varphi | \varphi$ - выполнимая булева формула $\}$.

$$SAT \in NP$$

Определение 6. 3-SAT $= \{\varphi | \varphi$ - выполнимая 3-КНФ $\}$,
3-КНФ: $(q_{11} \vee q_{12} \vee q_{13}) \wedge (q_{21} \vee q_{22} \vee q_{23}) \wedge \ldots \wedge (q_{n1} \vee q_{n2} \vee q_{n3})$, q_{ij} - литерал, т.е. переменная или отрицание переменной.

Утверждение 3. $SAT \leq 3 - SAT$

Доказательство.

1. $SAT \leq CNF - SAT$
   $\varphi \to$ КНФ
   (a) Раскрыть импликации $a \to b \sim \neg a \vee b$
   (b) Пронести внутрь отрицания $\neg(a \wedge b) \sim \neg a \vee \neg b$
   (c) Вынести наружу коньюнкции $(a \wedge b) \vee c \sim (a \vee c) \wedge (b \vee c)$
2. $CNF - SAT \leq_p 3 - SAT (a \vee b \vee c \vee d \vee e) \sim (a \vee b \vee x) \wedge (\neg x \vee c \vee y) \wedge (\neg y \vee d \vee e)$

□

Теорема 3. *[Кука-Левина] SAT - NP-complete*

Доказательство.
Пусть $L \in NP$. Тогда $\exists p, q, V : x \in L \Leftrightarrow \exists s \in \{0,1\}^{p(|x|)} V(x,s) = 1$ и работает $\leq q(|x| + p(|x|))$ шагов. $\Leftrightarrow$ Существует протокол конечного размера $(q(|x| + p(|x|)) + 1 \times q(|x| + p(|x|)) + 1))$ определенного вида (*) $\Leftrightarrow$ выполнима формула $\varphi = \varphi(x)$.

$\Phi = \varphi_{protocol} \& \varphi_{start} \& \varphi_{move} \varphi_{end}$ $x_{i,j,a} = 1 \Leftrightarrow$ в клетке (i,j) стоит символ a,
$0 \leq i \leq q(|x| + p(|x|)), 0 \leq j \leq q(|x| + p(|x|)), a \in \Gamma \cup Q$

$$\phi_{protocol} = \bigwedge_{i,j} (\sum_{a} x_{i,j,a} = 1) \wedge \bigwedge_{i} (\sum_{i,q \in Q} x_{i,j,q} = 1)$$

$$\phi_{start} = x_{0,0,q_1} \wedge x_{0,1,a_1} \wedge x_{0,2,a_2} \wedge \ldots \wedge x_{0,|x|,a} \wedge x_{0,|x|+1,\#}$$

$$\wedge \bigwedge_{j=|x|+2}^{|x|+p(|x|)+1} (\bigvee_{b \in \Sigma} x_{a,j,b}) \wedge \bigwedge_{j=\ldots} x_{0,j,\#}$$

$$\varphi_{end} = \bigvee_{j=0}^{N} x_{N,j,q_a}$$

$$\varphi_{move} = \bigwedge_{i=0}^{N-1} \bigwedge_{j=0}^{N-2} \bigvee_{a_1 \ldots a_6 - dopustimoeokoshko} (x_{i,j,a_1} \wedge x_{i,j+1,a_2} \wedge \ldots \wedge x_{i+1,j+2,a_6})$$

□

3. NP-полнота

Определение 7. $VERTEX - COVER = \{(G,R) :$ в графе $G \exists$ вершинное покрытие размером $k\} \in NPC$

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

Определение 8. 3-COL $= \{G :$граф G можно раскрасить в 3 цвета $\}$

Определение 9. $SUBSET - SUM = \{(n_1, n_2, \ldots, n_k, N) : \exists m \exists i_1, \ldots, i_m; n_i + \ldots + n_{i_m} = N\}$

$3SAT \leq_p SUBSET - SUM$

Определение 10. $HAMPATH = \{(G,s,t) :$ в ор. графе $G \exists$ гамильтонов путь из s в $t\}$

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

Определение 11. $CoNP = \{L : \overline{L} \in NP\}$

$P \subset NP \cap coNP$

$$\overline{L} \in NP \exists p \exists q \exists M(x \in \overline{L} \Leftrightarrow \exists s|s| = p(|x|), M(x, s) = 1)$$
$$\exists p \exists q \exists M(x \in L \Leftrightarrow \forall s(|s| = p(|x|) \to M(x, s) = 0))$$

Определение 12. $TAUT = \{\varphi : \varphi$ - тавтология $\} \in CoNP$

Определение 13. $EXP = \bigcup DTIME(2^n)$

Определение 14. $NEXP = \bigcup NTIME(2^n)$

Теорема 4. $EXP \neq NEXP \Rightarrow P \not= NP$

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 4. 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. $\varphi_0 = \varphi_0(x_2 \dots x_k) = \varphi(0, x_2 \dots x_k)$ $\varphi_1 = \varphi(1, x_2, \dots x_k)$
2. Сводимость в теор. Кука-Левина сохран. это св-во.