NP - трудные задачи

≡ Задача поиска (search problem)

$C(I, S)$ - двуместный предикат
I - (instance) условие задачи
S - (solution) решение задачи

По I найти S: $C(I, S)$

≡ Задача разрешения (decision problem)

...

По I проверить $\exists$ ли S: $C(I, S)$

Задача булевой выполнимости (SAT, Satisfiability)

Вход: φ - формула в КНФ

$\varphi(\bar{x}) = (x_1 \vee \neg x_2 \vee x_3 \ldots) \wedge (x_7 \vee x_{13} \vee \neg x_4) \wedge \ldots$

переменная — литерал — клоз/дизъюнкт (clause)

search:
$I = \varphi(\bar{x})$
S - выполняющий набор $\bar{\alpha}$: $\varphi(\bar{\alpha}) = 1$

decision:
Вопрос: $\exists$ ли $\bar{\alpha}$: $\varphi(\bar{\alpha}) = 1$

Лемма

$\exists$ poly time алг. для search SAT $\Leftrightarrow$
$\exists$ poly time алг. для decision SAT

$\Rightarrow$ очевидно

$\Leftarrow$ A:

$A(\varphi) \xrightarrow{1} A(\varphi|_{x_1=1}) \xrightarrow{1} A(\varphi|_{\substack{x_1=1 \\ x_2=0}}) \xrightarrow{1} \ldots$
$\searrow 0$ $\qquad A(\varphi|_{x_1=0,\, x_2=1}) \longrightarrow \ldots$

Если A для decision SAT работает за $poly(|\varphi|)$ =>

A' работает за $|\varphi| \cdot poly(|\varphi|)$ (для search)

Что известно про SAT?

- Не умеем решать быстрее $O(2^n \cdot poly(n))$
- Умеем решать k-SAT за $O(c^n)$, $c \in (1,2)$, $c = c(k)$ $O(2^{\varepsilon n})$ $\varepsilon < 1$
- При $k = 2$ решение за $O(|\varphi|)$
- Хорновские формулы (в # клозе ≤ 1 переменной без отриц.)

NP vs P

≡ P - класс задач поиска: по I можно получить S за время $poly(|I|)$

≡ NP - класс задач поиска: $|S| \leq poly(|I|)$, $C(I,S)$ можно проверить за $poly(|I|)$ ($poly(|I| + |S|)$)

Лемма:

$P \subseteq NP$

Утв: $SAT \in NP$

Сведения

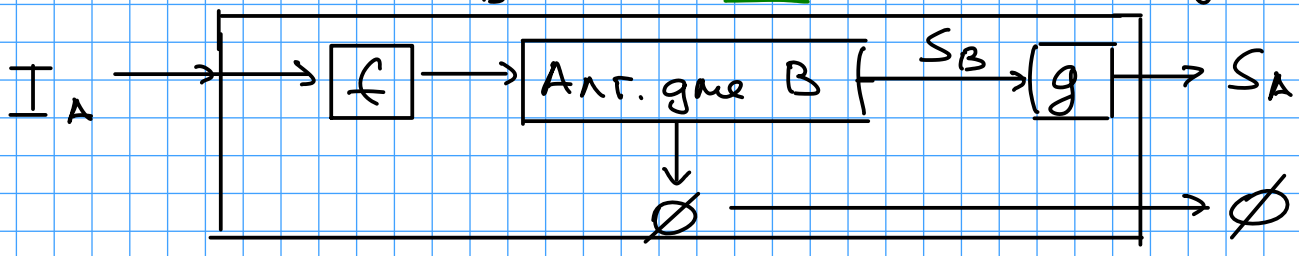
$A \leq B$ – A сводится к B (сводится по Карпу, many-one)

$\exists\ f : \{I_A\} \to \{I_B\}$

$\exists\ g : \{S_B\} \to \{S_A\}$

f, g – полиномиально вычислимые

1. $\forall I_A : [\exists S_A : C_A(I_A, S_A)] \Leftrightarrow [\exists S_B : C_B(f(I_A), S_B)]$
2. $\forall I_A\ \forall S_B\ C_B(f(I_A), S_B) \Rightarrow C_A(I_A, g(S_B))$



Т.е. умея решать B мы научимся решать A.

Утв: $\exists$ polytime алг. для $B \Rightarrow$ $\exists$ polytime алг. для A

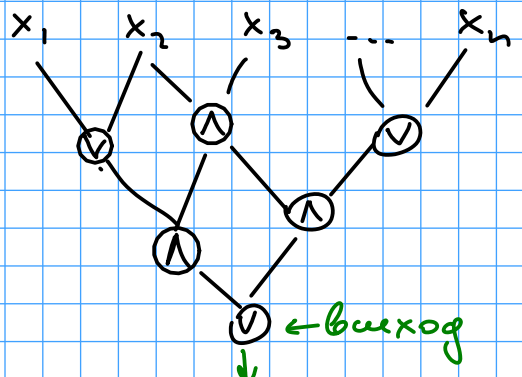
Утв: $A \leq B,\ B \leq C \Rightarrow A \leq C$

Утв: Классы P и NP замкнуты отн. сведений по Карпу

≡ A – NP-трудная задача, если $\forall B \in NP \quad B \leq A$

≡ A – NP-полная, если A – NP-трудная и $A \in NP$ (самая сложная задача в NP)

Circuit SAT



Вход: схема C

Выход: α : $C(\alpha) = 1$

Очевидно: $SAT \leq CircuitSAT$

Th. Кука - Левина

$\forall A \in NP \quad A \le$ Circuit SAT

$A \in NP \Rightarrow \exists$ предикат $C(I, S)$, который можно вычислить за $poly(|I|)$

Т.е. существует "программа" на "компьютере", которая вычисляет C и работает время $poly(|I|) = p(n)$, $n = |I|$

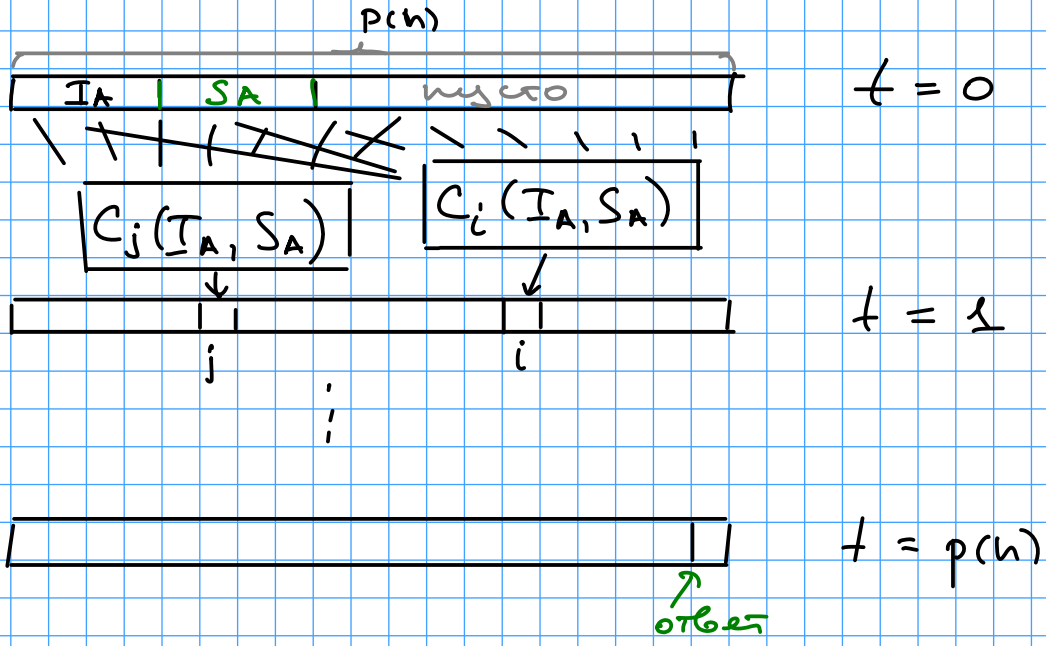
Пусть "компьютер" - это RAM машина

Отметим $f: \{I_A\} \to \{I_{CS}\}$

I_A — условие A, I_{CS} — Circuit SAT

Преобразуем программу для $C(I_A, \cdot)$

в снэпок памяти машины для $C(I_A, \cdot)$ в начальный момент



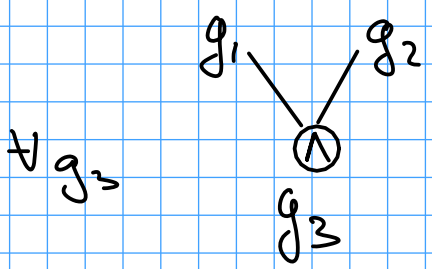
По $C(I_A, \cdot)$ построим схему размера $O(p^2(n))$

□

Следствие:

Circuit SAT – NP-полная задача

Circuit SAT ≤ SAT



$f(g_3) =$

$(\neg g_3 \vee g_1) \wedge (\neg g_3 \vee g_2) \wedge$

$(g_3 \vee \neg g_1 \vee \neg g_2)$

$(g_1 \wedge g_2) \rightarrow g_3$

По схеме получается: $\left(\bigwedge_{g \in C} f(g)\right) \wedge (out)$

Это сведение Circuit SAT к 3SAT

SAT ≤ 3SAT

$(x_1 \vee x_2 \vee x_3 \ .. \vee x_k) \longrightarrow$

$(x_1 \vee x_2 \vee y_1) \wedge (\neg y_1 \vee x_3 \vee y_2) \wedge (\neg y_2 \vee x_4 \vee y_3) \wedge$

$\wedge \ldots \wedge (\neg y_{k-3} \vee x_{k-1} \vee x_k)$

$y_1 \ldots y_{k-3}$ – новые переменные.

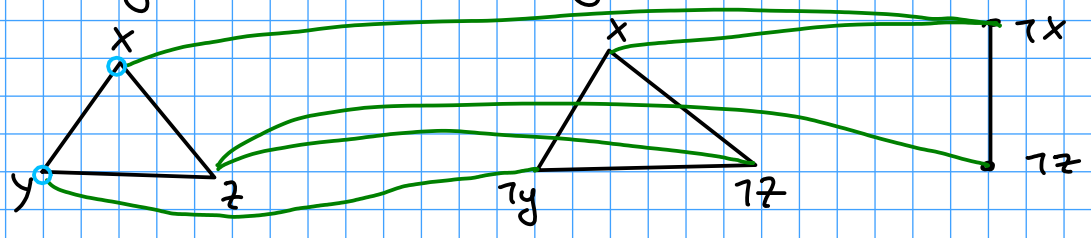
IS (independent set)

Вход: (G, k)

Выход: IS размера k

3SAT ≤ IS

$(x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee \neg z)$

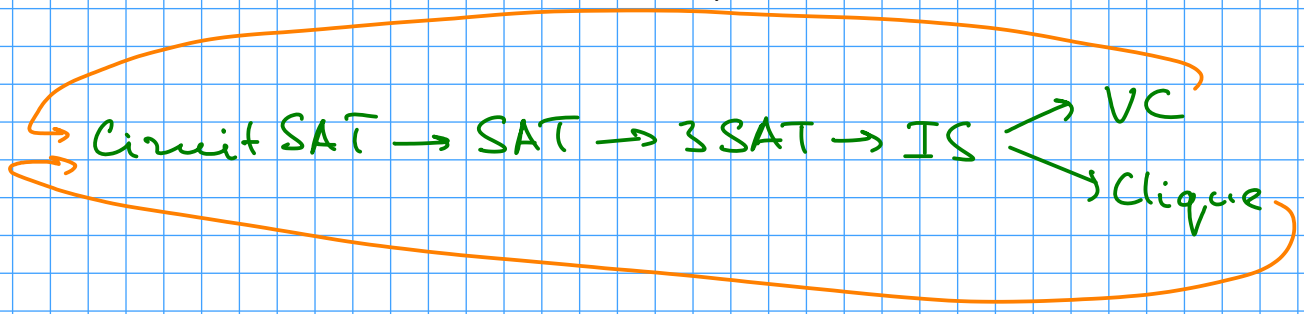


$IS \leq VC$ (вершинное покрытие)

$IS(G, k) \longrightarrow VC(G, |V| - k)$

$IS \leq Clique$

$IS((V, E), k) \longrightarrow Clique((V, \overline{E}), k)$



$P \stackrel{?}{=} NP \Rightarrow 10^6$ $

Другие NP-полные задачи:

- TSP (задача коммивояжёра)

  Эм путь длины $\leq k$
- Hamylton Cycle
- Balanced Cut

$\frac{1}{2}|V| \leq |S| \leq \frac{2}{3}|V|$

- Integer Linear Programming
- Graph Coloring ($G \geq 3$ цвета)
- Longest Path
- Subset Sum

  Множество чисел → подмножество чисел $= k$
- Целочисленный рюкзак
- Set Cover

Замечание:

Многие NP-полные задачи имеют внешних "барьеров" на P (фазовый переход)

Решение NP-трудных задач

1. Эвристики
2. Приближённые алгоритмы

Существуют "сложные задачи" в NP \ NPC

- Factoring

Вход: n Выход p, q: $n = p \cdot q$

- Graph Isomorphism

Вход: (G_1, G_2) Выход: π - перестановка

$\pi(G_1) = G_2$