Лекция 10

Подготовил Коврижных Алексей, КН-301

23.11.15

Теория алгоритмов 2015

Язык задачи

Определение

$R = \{(x, y)\}$ - *задача поиска.*
$L(R) = \{x | \exists y : (x, y) \in R\}$ - *язык для задачи* R *(условия, для которых есть решения)*

Исследуем взаимосвязь задачи поиска с их языками.

Утверждение

$R_1 \underset{l}{\to} R_2 \Rightarrow L(R_1) \underset{c}{\to} L(R_2)$

Доказательство

$R_1 \underset{l}{\to} R_2 \Rightarrow \exists f, g : (x, g(y)) \in R_1 \Leftrightarrow (f(x), y) \in R_2$
Нужно доказать, что $f(x) \in L(R_2) \Leftrightarrow x \in L(R_1)$
Пусть $f(x) \in L(R_2) \Leftrightarrow \exists y : (f(x), y) \in R_2 \Leftrightarrow (x, g(y)) \in R_1 \Leftrightarrow x \in L(R_1)$

Следствие

$R \in FNP\text{-}C \Rightarrow L(R) \in NP\text{-}C$

Утверждение

$\forall FNP\text{-}CR \underset{p}{\rightarrow} L(R)$

Доказательство

$R \underset{l}{\rightarrow} F\text{-}SAT \underset{p}{\rightarrow} SAT \underset{k}{\rightarrow} L(R)$

Сведение по Левину корректно, т.к. $F\text{-}SAT$ FNP-полна, сведение по Куку было доказано на прошлой лекции, сведение по Карпу корректно, т.к. L(R) - NP-полна. Теперь докажем, что все три сведения эквивалентны сведению по Куку.

Доказательство

Построим ДМТ (из определения сводимости по Куку) решающую задачу R.
Алгоритм:
1) По x построить $F \in F\text{-}SAT$
2) Запустить алгоритм сведения по Куку $F\text{-}SAT \underset{p}{\to} SAT$ (см. предыдущую лекцию). Каждый раз, когда алгоритм вызывает оракул от формулы Z, заменяем Z на $Z' \in L(R)$ с помощью преобразования (3) (по Карпу) и вызываем оракул $L(R)$.

Классы дополнений языков

Определение

$L \in CoNP \Leftrightarrow \overline{L} \in NP$

Определение

$L \in CoNP \Leftrightarrow \exists M_L \forall w \notin L \exists c : M_L(w, c) = 1$

Очевидно, что $\forall L : L \underset{p}{\to} \overline{L}$.

Утверждение

$L \in NP\text{-}C \Rightarrow \overline{L} \in CoNP\text{-}C$

Для доказательства рассмотрим другое утверждение.

Утверждение

$L_1 \underset{k}{\to} L_2 \Rightarrow \overline{L_1} \underset{k}{\to} L_2$

Доказательство

$L_1 \underset{k}{\to} L_2 \Rightarrow \exists f : w \in L_1 \Leftrightarrow f(w) \in L_2 \Rightarrow w \notin L_1 \Leftrightarrow f(w) \notin L_2 \Rightarrow w \in \overline{L_1} \Leftrightarrow f(w) \in \overline{L_2}$

Докажем еще один простой факт:

Утверждение

$P \subseteq NP \cap CoNP$

Доказательство

$$L \in P \Leftrightarrow \exists M\text{-ДМТ}\ \forall w \ \ \begin{array}{l} M(w) = 0 \Leftrightarrow w \notin L \\ M(w) = 1 \Leftrightarrow w \in L \end{array}$$

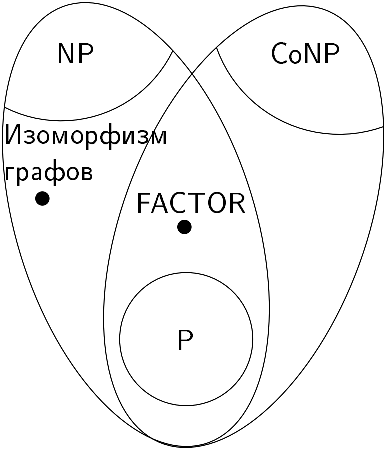
Данное определение симметрично относительно отрицания, то есть $L \in P \Leftrightarrow \overline{L} \in P$, *следовательно* $P = CoP$.

Тогда $\forall L : L \in P \Rightarrow \overline{L} \in P \Rightarrow \overline{L} \in NP \Rightarrow L \in CoNP$

Итак,

1. $P \subseteq NP$
2. $P \subseteq CoNP$

Отсюда следует, что $P \subseteq NP \cap CoNP$.



Определение

FACTOR - задача факторизации. По заданным n, m определить, есть ли у числа n простой делитель, больший чем m.

Теорема

$FACTOR \in NP \cap CoNP$

Доказательство

Возьмем сертификат $C = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_l^{k_l} = n$ *(разложение числа на простые делители). По нему можно быстро (полиномиально) убедиться как в том, что у числа есть простые делители больше* m*, так и в обратном.*

Замечание

Существует полиномиальный алгоритм проверки на простоту - тест Агравала-Каяла-Саксены.

Полиномиальная иерархия классов

- P - M-ДМТ, работающая за полином. $M(w) \in \{0, 1\}$
- NP - $\exists ?x : M(w, x) = 1$
- $CoNP$ - правда ли, что $\forall x M(w, x) = 1$
- FNP - найди $x : M(w, x) = 1$
- $\Sigma^2 P$ - $\exists ?x \forall y M(w, x, y) = 1$
- $\prod^2 P$ - правда ли, что $\forall x \forall y M(w, x, y) = 1$
- $F\Sigma^2 P$ - найди $x : \forall y M(w, x, y) = 1$ (пример: Задача коммивояжёра)