Algoritmuselmélet

NP-teljes problémák

Katona Gyula Y.

Számítástudományi és Információelméleti Tanszék
Budapesti Műszaki és Gazdaságtudományi Egyetem

Emlékeztető

Definíció

Egy X eldöntési problémához tartozó L_X nyelv *azoknak a bemeneteknek a halmaza, amelyekre a válasz* IGEN. *A lehetséges bemeneteket (amelyek tehát vagy beletartoznak L_X-be vagy nem),* szavaknak *hívjuk.*

Egy X eldöntési probléma és x bemenet esetén

- $x \in X$ *jelöli, hogy az x bemenetre a válasz* IGEN,
- $x \notin X$ *jelöli, hogy az x bemenetre a válasz* NEM.

Karp-redukció

Mikor nem lényegesen nehezebb egy X probléma egy Y problémánál?
Ha Y felhasználásával meg lehet oldani X-et is.
$\Longrightarrow$ X megoldása visszavezethető az Y probléma megoldására.

Definíció

Legyen X és Y két eldöntési probléma. Az X Karp-redukciója (polinomiális visszavezetése) *az Y problémára egy olyan polinom időben számolható f függvény, amely X minden lehetséges bemenetéhez hozzárendeli Y egy lehetséges bemenetét úgy, hogy*

$$x \in X \Leftrightarrow f(x) \in Y.$$

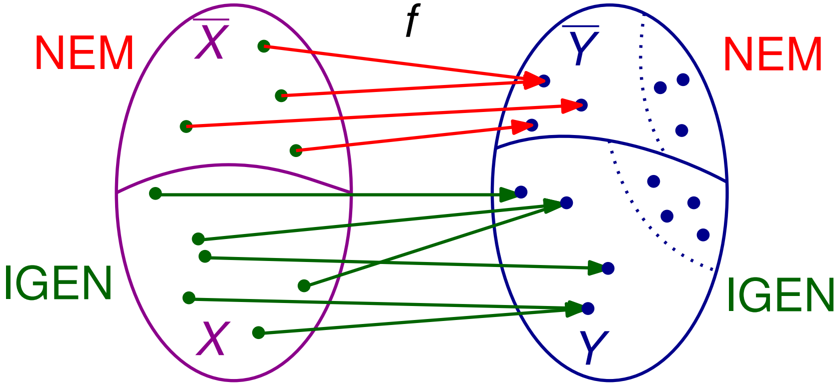
Jelölés: $X \prec Y$, ha X-nek van Karp-redukciója Y-re.

Ha tehát van algoritmusunk Y eldöntésére $\Longrightarrow$ $x \in X$-re kiszámítjuk $f(x)$-et, eldöntjük $f(x) \in Y$? $\Longrightarrow$ tudjuk, hogy $x \in X$ igaz-e. $\surd$

Ha tudnánk, hogy X nehéz, és tudjuk, hogy $X \prec Y$
$\Longrightarrow$ Y is nehéz lenne.

Ha Y könnyű, és X nem lényegesen nehezebb nála, akkor X is könnyű.

Karp-redukció



3SZÍN és 4SZÍN

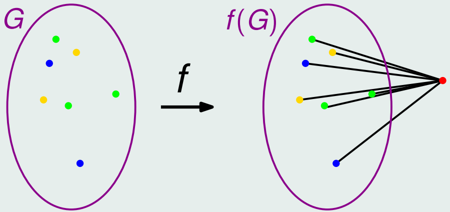
3SZÍN — **Bemenet:** G gráf.
Kérdés: Igaz-e, hogy G színezhető 3 színnel?

4SZÍN — **Bemenet:** G gráf.
Kérdés: Igaz-e, hogy G színezhető 4 színnel?

Állítás

3SZÍN $\prec$ 4SZÍN.

Bizonyítás.



- f polinom időben számolható $\surd$
- G 3 színnel színezhető $\Leftrightarrow$ $f(G)$ 4 színnel színezhető $\surd$

$\square$

A Karp-redukció tulajdonságai

Tétel

1. *Ha $X \prec Y$ és $Y \in \mathrm{P}$, akkor $X \in \mathrm{P}$.*
2. *Ha $X \prec Y$ és $Y \in \mathrm{NP}$ akkor $X \in \mathrm{NP}$.*
3. *Ha $X \prec Y$, akkor $\overline{X} \prec \overline{Y}$*
4. *Ha $X \prec Y$ és $Y \in \mathrm{coNP}$, akkor $X \in \mathrm{coNP}$.*
5. *Ha $X \prec Y$ és $Y \in \mathrm{NP} \cap \mathrm{coNP}$, akkor $X \in \mathrm{NP} \cap \mathrm{coNP}$.*
6. *Ha $X \prec Y$ és $Y \prec Z$, akkor $X \prec Z$.*

Bizonyítás.

Legyen f az X Karp-redukciója Y-re, ahol f $c_1 n^k$ időben számolható. x egy bemenet, melyről szeretnénk eldönteni, hogy $x \in X$ teljesül-e, n az x hossza.

Bizonyítás.

1.: Kiszámítjuk $f(x)$-et $\to$ időigénye $\leq c_1 n^k \implies |f(x)| \leq c_1 n^k$.
Y felismerő algoritmusával $c_2|f(x)|^\ell$ időben eldöntjük, hogy $f(x) \in Y$ igaz-e.
$\to$ időigénye $\leq c_2(c_1 n^k)^\ell$
$x \in X \Leftrightarrow f(x) \in Y \implies$ összidő $O(n^{k\ell})$ $\surd$

2.: Az $f(x) \in Y$ tény egy t tanúja jó $x \in X$ tanújának is, és az Y-hoz tartozó $\mathcal{T}$ tanúsító algoritmus egy kis módosítással jó lesz az X tanúsító algoritmusának is.
$\mathcal{T}'$ az (x, t) bemenetre először kiszámítja $f(x)$-et, majd az $(f(x), t)$ párra alkalmazza $\mathcal{T}$-t.
Ha az eredmény IGEN*, akkor legyen $\mathcal{T}'$ eredménye is* IGEN*, különben pedig* NEM.
$|t| = O(|f(x)|^c) \implies |t| = O(n^{kc})$
$\mathcal{T}'$ lépésszáma, ha $\mathcal{T}$ lépésszáma $O((|y| + |t|)^\ell)$:
$O(n^k) + O((|f(x)| + |t|)^\ell) = O(n^k) + O(|f(x)|^{c\ell}) = O(n^{kc\ell})$.

Bizonyítás.

3.: X-nek egy Karp-redukciója Y-ra egyben egy Karp-redukció $\overline{X}$-ről $\overline{Y}$-re, hiszen $x \in X \iff f(x) \in Y$ ugyanaz, mint $x \notin X \iff f(x) \notin Y$

4.: $\Longleftarrow$ 2.,3.

5.: $\Longleftarrow$ 2.,4.

6.: Legyen f az $X \prec Y$ függvénye, ami $O(n^k)$ időben számolható és g az $Y \prec Z$ függvénye, ami $O(n^\ell)$ időben számolható.
Az $X \prec Z$ függvénye $g(f(x))$ lesz, ami $O((n^k)^\ell) = O(n^{k\ell})$ időben számolható. $\square$

NP-teljes problémák

Definíció

Az X eldöntési probléma NP-nehéz, ha tetszőleges (azaz minden) $X' \in \mathrm{NP}$ probléma esetén létezik $X' \prec X$ Karp-redukció.
Az X eldöntési probléma NP-teljes, ha $X \in \mathrm{NP}$ és X NP-nehéz.

Egy NP-teljes probléma tehát legalább olyan nehéz, mint bármely más NP-beli probléma.
Ha egy ilyen problémáról kiderülne, hogy P-beli (coNP-beli), akkor ugyanez igaz lenne minden NP-beli problémára.

Van-e NP-teljes probléma?

Boole-formulák

Definíció

Az $f : \{0,1\}^n \to \{0,1\}$ *függvényeket n-változós* Boole-függvényeknek *vagy* Boole-formuláknak *hívjuk.*

Tétel

Minden Boole-függvény felírható az $x_1, \ldots, x_n$ *Boole-változók, az* $\wedge, \vee, \neg$ *logikai műveletek és zárójelek segítségével.*

Pl. Boole-formula:

$$\Phi = (x_1 \vee \neg x_2 \vee x_5) \wedge ((\neg x_3 \vee x_2 \vee (x_6 \wedge x_1)) \wedge \neg(x_5 \vee x_6))$$

Boole-formulák

Definíció

Egy Boole-formula kielégíthető, ha lehet úgy értékeket adni a változóinak, hogy a függvény értéke 1 legyen.

Pl. $\Phi(x_1, x_2) = (x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2)$ kielégíthető, mert ha $x_1 = 1$ és $x_2 = 0$, akkor $\Phi(x_1, x_2) = 1$

De pl. $(x_1 \wedge \neg x_1)$ nyilván nem kielégíthető.

Cook–Levin-tétel

Van-e NP-teljes probléma?

Definíció

SAT *probléma:*

Bemenet: Φ *Boole-formula*

Kérdés: Kielégíthető-e Φ*?*

Tétel (S. A. Cook, L. Levin, 1971)

A SAT *probléma* NP*-teljes.*

Bizonyítás elég bonyolult.

NP-teljesség

Kérdés

Miért jó tudni, hogy egy probléma NP-teljes?

Ha valaki ad egy polinomiális algoritmust egy NP-teljes problémára, akkor az megoldja a nagy sejtést.

Tétel

Ha X NP-teljes és $X \in \mathrm{P}$, akkor $\mathrm{P} = \mathrm{NP}$.

Bizonyítás.

X NP-teljes $\implies$ minden $L \in \mathrm{NP}$-re van $L \prec X$ redukció.
Karp-redukció 1. tulajdonság $\implies$ Ha $X \in \mathrm{P}$, akkor $L \in \mathrm{P}$ is teljesül.
Vagyis $\mathrm{NP} \subseteq \mathrm{P}$. Mivel tudjuk azt is, hogy $\mathrm{P} \subseteq \mathrm{NP}$ $\implies$ $\mathrm{P} = \mathrm{NP}$ $\square$

További NP-teljes feladatok

Tétel (Iszonyú Hasznos Tétel - IHT)

Ha az X probléma NP-teljes, $Y \in \mathrm{NP}$ és $X \prec Y$, akkor Y is NP-teljes.

Bizonyítás.

Láttuk, hogy a Karp-redukció tranzitív.
Ha $X \prec Y \implies Z \prec X$ teljesül minden $Z \in \mathrm{NP}$ problémára.
tranzitivitás $\implies Z \prec Y$ teljesül minden $Z \in \mathrm{NP}$ problémára.
$\implies Y \in \mathrm{NP}$-nehéz.
Mivel $Y \in \mathrm{NP}$ is $\implies Y \in \mathrm{NP}$-teljes. □

Nem kell már minden NP-beli problémát az Y-ra redukálni; elég ezt megtenni egyetlen NP-teljes X problémával.

A 3SZÍN probléma

Tétel

A 3SZÍN probléma NP-teljes.

Bizonyítás.

Már láttuk, hogy $\in$ NP*, belátható, hogy* SAT $\prec$ 3SZÍN*.*

Maximális méretű független ponthalmaz gráfokban

MaxFtlen

Bemenet: G gráf, $k \in \mathbb{Z}^+$.

Kérdés: Van-e G-nek k elemű független csúcshalmaza?

Tétel

A MaxFtln probléma NP-teljes.

Maximális méretű klikk

MAXKLIKK

Bemenet: G gráf, $k \in \mathbb{Z}^+$.
Kérdés: Van-e G-ben k pontú teljes részgráf (k-klikk)?

Tétel

A MAXKLIKK probléma NP-teljes.

Bizonyítás.

MAXKLIKK $\in \mathrm{NP}$: tanú egy k-elemű $S \subseteq V(G)$ teljes részgráf. $\surd$
Megadunk egy MAXFTLEN $\prec$ MAXKLIKK Karp-redukciót:
$f(G, k) = (\overline{G}, k)$ (független ponthalmaz a komplementerben teljes gráf). $\surd$ $\square$

Hamilton-kör probléma

H Bemenet: G gráf
Kérdés: Van-e G-ben Hamilton-kör?

Tétel

A H probléma NP-teljes.

Bizonyítás.

Már láttuk, hogy H $\in \mathrm{NP}$. $\surd$
Belátható, hogy SAT $\prec$ H. (bonyolult)

H-ÚT Bemenet: G gráf
Kérdés: Van-e G-ben Hamilton-út?