Algoritmuselmélet

NP-teljes problémák

Katona Gyula Y.

Számítástudományi és Információelméleti Tanszék
Budapesti Műszaki és Gazdaságtudományi Egyetem

Karp-redukció

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

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.

Irányított Hamilton-kör probléma (IH)

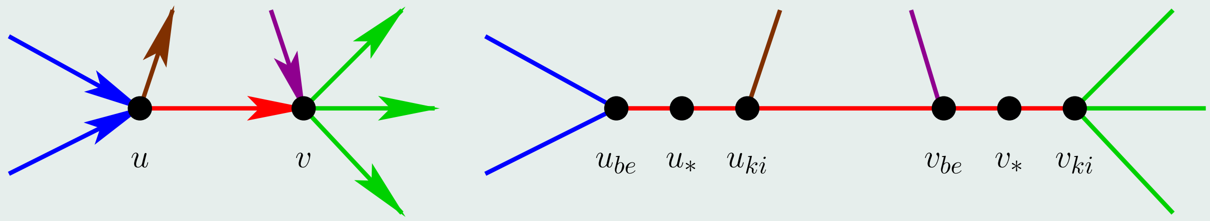
Tétel

$IH \prec H$.

Bizonyítás.

$G = (V, E)$ egy irányított gráf $\to$ $G' = (V', E')$ irányítatlan gráf hogy G' gyorsan megépíthető és G-ben $\exists$ irányított Hamilton-kör $\leftrightarrow$ G'-ben $\exists$ irányítatlan Hamilton-kör.

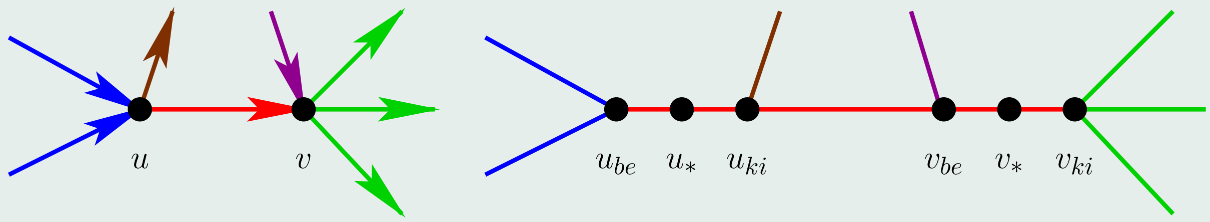
$$V' = \{v_{be}, v_*, v_{ki} \mid v \in V\},$$
$$E' = \{(v_{be}, v_*), (v_*, v_{ki}) \mid v \in V\} \cup \{(u_{ki}, v_{be}) \mid u \to v \in E\}.$$



$v(G) = n, e(G) = e \implies v(G') = 3n, e(G') = 2n + e \implies O(n + e)$ lépésben megkapható.

Bizonyítás.

G-beli F irányított Hamilton-körének megfelel G' egy F' Hamilton-köre.



Az F egy $u \to v$ éle $\longrightarrow$ az F'-ben az $u_* - u_{ki} - v_{be} - v_*$ út.

Ezért $G \in IH \implies G' \in H$

Ha G'-ben van egy $F' \subseteq E'$ Hamilton-kör $\implies$ egy u_*-ból indulva egy u_{ki} felé lépjünk először

$\implies$ csak $u_* - u_{ki} - v_{be} - v_*$ alakú lehet utána $\implies$ ez az út megfelel G-ben egy u -> v élnek. Ezt tovább folytatva Hamilton-kört kapunk G-ben.

Ezért $G' \in H \implies G \in IH$. $\square$

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* $\rightarrow$ *időigénye* $\leq c_1 n^k \implies |f(x)| \leq c_1 n^k$.
Y *felismerő algoritmusával* $c_2 |f(x)|^l$ *időben eldöntjük, hogy* $f(x) \in Y$ *igaz-e.*
$\rightarrow$ *időigénye* $\leq c_2 (c_1 n^k)^l$
$x \in X \Leftrightarrow f(x) \in Y \implies$ *összidő* $O(n^{kl})$ $\surd$

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* $O((|y| + |t|)^l)$:
$O(n^k) + O((|f(x)| + |t|)^l) = O(n^k) + O(|f(x)|^{cl}) = O(n^{kcl})$.

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 $O(n^l)$ időben számolható.
Az $X \prec Z$ függvénye $g(f(x))$ lesz, ami $O((n^k)^l) = O(n^{kl})$ időben számolható. □

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-fomula*
Kérdés: Kielégíthető-e Φ*?*

Tétel (S. A. Cook, L. Levin, 1971)

A SAT *probléma* NP*-teljes.*

Bizonyítás elég bonyolult.

További NP-teljes feladatok

Tétel

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.
$\Longrightarrow$ Ha $X \prec Y$ és $Z \prec X$ teljesül $\forall Z \in \mathrm{NP}$ problémára.
$\Longrightarrow$ $Z \prec Y$ teljesül $\forall Z \in \mathrm{NP}$ problémára.
$\Longrightarrow$ $Y \in \mathrm{NP}$-nehéz.
Mivel $Y \in \mathrm{NP}$ is $\Longrightarrow$ $Y \in \mathrm{NP}$-teljes. $\square$

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

A 3-SZÍN probléma

Tétel

A 3SZÍN *probléma* NP*-teljes.*

Bizonyítás.

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

Maximális méretű független pontrendszer gráfokban

MAXFTLEN

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

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

Tétel

A MAXFTLN *nyelv* NP*-teljes.*

Bizonyítás.

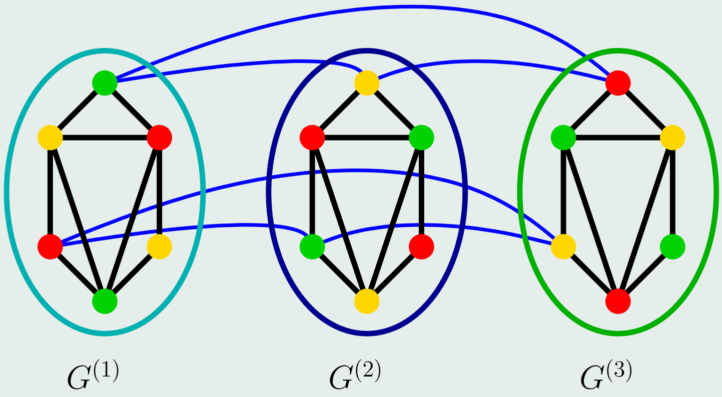
MAXFTLEN $\in$ NP*: tanú egy k-elemű $S \subseteq V(G)$ független csúcshalmaz.* $\checkmark$

Megadunk egy 3SZÍN $\prec$ MAXFTLEN *Karp-redukciót: $G \to (G', k')$*

$$G \in \text{3SZÍN} \Leftrightarrow (G', k') \in \text{MAXFTLEN}$$

Bizonyítás.

G' megadása: Vegyük G három másolatát ($G^{(1)}$, $G^{(2)}$, $G^{(3)}$), minden csúcs három példányát összekötjük.



$|V(G')| = 3|V(G)|$ és
$|E(G')| = 3|V(G)| + 3|E(G)|$,
legyen $k' = |V(G)|$.

Ha G színezhető 3 színnel $\Longrightarrow$ G' is $\Longrightarrow$
a piros pontok halmaza G'-ben független és $|V(G)|$ van belőlük. $\surd$
Ha G'-ben van $|V(G)|$ független, akkor legyen S egy ilyen ponthalmaz G'-ben.
$\Longrightarrow$ Minden G-beli x pontnak pontosan 1 példányát tartalmazza S.
$\Longrightarrow$ Az x pont legyen sárga / piros / zöld, ha ez a példány $G^{(1)}$-ben / $G^{(2)}$-ben / $G^{(3)}$-ban van. $\Longrightarrow$ ez jó színezés G-ben. $\surd$ $\square$

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 *nyelv* 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). $\surd$ $\square$

Részgráf izomorfia probléma

RÉSZGÁFIZO

Bemenet: G, H gráfok.

Kérdés: Van-e G-ben H-val izomorf részgáf?

Tétel

A RÉSZGÁFIZO *nyelv* NP*-teljes.*

Bizonyítás.

RÉSZGÁFIZO $\in \mathrm{NP}$: tanú egy részgáf és annak izomorfiája H-val. $\surd$
Megadunk egy MAXKLIKK $\prec$ RÉSZGÁFIZO Karp-redukciót:
$f(G, k) = (G, K_k)$. $\surd$ $\square$

Ha X NP-nehéz és Y általánosítása X-nek, akkor Y is NP-nehéz.
$\Longrightarrow$ RÉSZGÁFIZO speciális esete a MAXKLIKK-nek $\Longrightarrow$ NP-nehéz.

Hamilton-kör probléma

Tétel

A H *nyelv* NP*-teljes.*

Bizonyítás.

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

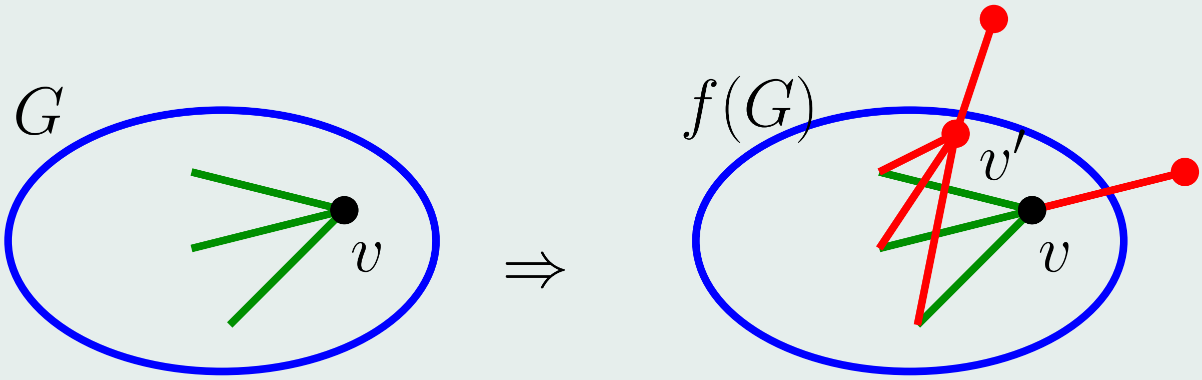
Hamilton-út probléma

Tétel

Az H-ÚT *nyelv* NP*-teljes.*

Bizonyítás.

H-ÚT $\in$ NP, mert egy Hamilton-út tanú. $\surd$
Belátjuk, hogy H $\prec$ H-ÚT.



G-ben akkor és csak akkor van Hamilton-kör, ha $f(G)$-ben van Hamilton-út. $\square$

A Hátizsák feladat

Hátizsák feladat:
Adottak tárgyak $s_1, \ldots, s_m > 0$ súlyai, ezek $v_1, \ldots, v_m > 0$ értékei, valamint a b megengedett maximális összsúly.
Tegyük fel, hogy az s_i, v_i, b számok egészek.
A feladat az, hogy találjunk egy olyan $I \subseteq \{1, .., m\}$ részhalmazt, melyre $\sum_{i \in I} s_i \leq b$, és ugyanakkor $\sum_{i \in I} v_i$ a lehető legnagyobb.
$\Longrightarrow$
HÁT

Bemenet: $s_1, \ldots, s_m$; $v_1 \ldots, v_m$; b; k.
Kérdés: Van-e olyan $I \subseteq \{1, \ldots, m\}$ melyre $\sum_{i \in I} s_i \leq b$ és $\sum_{i \in I} v_i \geq k$?

Lemma

HÁT $\in$ NP

Vegyük azt a speciális esetet, amikor $s_i = v_i$ és $b = k$. $\Longrightarrow$

A Részhalmaz összeg probléma

RH

Bemenet: $(s_1, \ldots, s_m; b)$.
Kérdés: Van-e olyan $I \subseteq \{1, \ldots, m\}$ melyre $\sum_{i \in I} s_i = b$?

Tétel

Az RH *nyelv* NP*-teljes.*

Bizonyítás.

RH $\in \mathrm{NP}$. $\surd$
Belátható, hogy SAT $\prec$ RH.

Speciális eset: Partíció feladat: ahol $b = \frac{1}{2}\sum s_i$.
PARTÍCIÓ

Bemenet: $(s_1, \ldots, s_m)$.
Kérdés: Van-e olyan $I \subseteq \{1, \ldots, m\}$ melyre
$\sum_{i \in I} s_i = \frac{1}{2}\sum_{i=1}^{m} s_i$?

A Partíció probléma

Tétel

A PARTÍCIÓ *probléma* NP*-teljes.*

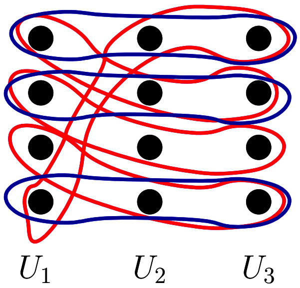
Bizonyítás.

Partíció $\in \mathrm{NP}$. $\surd$
Belátjuk, hogy RH $\prec$*Partíció*, pedig RH általánosabb!
Vegyük az RH egy $x = (s_1, \ldots, s_m; b)$ inputját.
$\Longrightarrow$ Feltehető, hogy $b \leq s = \sum_{i=1}^{m} s_i$.
$f(x) = (s_1, \ldots, s_m, s + 1 - b, b + 1)$.
A számok összege $2s + 2$, az utolsó két szám nem lehet egy partíció ugyanazon osztályában, mert az összegük túl nagy: $s + 2 > \frac{1}{2}(2s + 2)$.

RH-nak megoldása az $R \subset \{s_1, ..., s_m\}$ számhalmaz$\Leftrightarrow$ a megoldáshoz vegyük hozzá $(s + 1 - b)$-t $\Leftrightarrow$ PARTÍCIÓ-nak megoldása az $R \cup \{s + 1 - b\}$ számhalmaz. $\square$

A háromdimenziós házasítás

Párosítási feladat általánosítása: Legyenek U_1, U_2, U_3 azonos méretű véges halmazok $\Longrightarrow |U_i| = t$.
Adott még $U_1 \times U_2 \times U_3$ valamely S részhalmaza $\Longrightarrow (u_1, u_2, u_3)$ alakú hármasok.
Kiválasztható-e S-ből egy *háromdimenziós házasítás*?
$\Longrightarrow$ olyan t-elemű $S' \subseteq S$ részhalmaz, mely minden U_i-beli pontot lefed. (Mivel t-elemű, mindent csak egyszer fedhet le.)



3-DH: olyan U_1, U_2, U_3; $S \subseteq U_1 \times U_2 \times U_3$ rendszerek, melyeknél S-ből kiválasztható egy háromdimenziós házasítás.

A háromdimenziós házasítás

Tétel

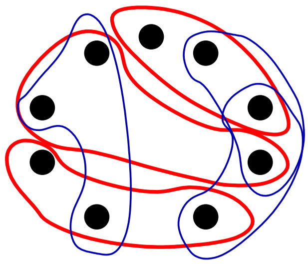
A 3-DH feladat NP*-teljes.*

Bizonyítás.

3-DH $\in$ NP $\surd$
$\exists$ 3-SAT $\prec$ 3-DH $\square$

X3C

Pontos fedés hármasokkal: adott egy U véges halmaz, és U háromelemű részhalmazainak egy $\mathcal{F} = \{X_1, X_2, \ldots, X_k\}$ családja. Eldöntendő, hogy az $\mathcal{F}$-ből kiválaszthatók-e páronként diszjunkt halmazok, melyek együttesen lefedik U-t.
Jelölje X3C azokat az $(U, \mathcal{F})$ párokat, melyekre igen.



Tétel

Az X3C nyelv NP*-teljes.*

Bizonyítás.

X3C $\in \mathrm{NP}$ teljesül: tanú egy pontos fedés.
Megmutatjuk, hogy 3-DH $\prec$ X3C.
X3C általánosabb probléma, mint 3-DH. Ha van algoritmus az általánosra, akkor azzal a speciális is megoldható. $\surd$ $\square$

Ha L NP-nehéz és L' általánosítása L-nek, akkor L' is NP-nehéz.