

5. Előadás: Redukciók*Előadó: Hajnal Péter*

2015. tavasz

1. Nehézség, relatív nehézség

A korábbiakban több nyelvosztályt bevezettünk ($\mathcal{L}, \mathcal{P}, \mathcal{D}, \mathcal{EXPT}$). Láttunk több példát központi matematikai problémákra (HAMILTON, \overrightarrow{st} -ELÉRHETŐSÉG, SZÓ-PROBLÉMA, FAKTORIZÁCIÓ, ...). Központi kérdés, hogy az egyes problémákat elhelyezzük a bevezetett hierarchiában. Cél egy fontos probléma minél pontosabb helyének/bonyolultságának meghatározása.

A „hely” meghatározása két feladatból áll.

- (1) Egy L nyelv/probléma bonyolultságának felső becslése (azaz annak bizonyítása, hogy $L \in \mathcal{C}_1$) egy algoritmus megadását kívánja, majd az algoritmus analízisét, ami mutatja, hogy a \mathcal{C}_1 osztályhoz tartozást igazol. Ilyen típusú eredmények (amelyek jóval a számítógépek megjelenése előtt felismerhetők a matematika történetben) alkotják az algoritmuselmélet kiindulópontját.
- (2) Egy L nyelv/probléma bonyolultságának alsó becslése (azaz annak bizonyítása, hogy $L \notin \mathcal{C}_2$) jóval összetettebb. Azt kívánja, hogy rámutassunk egy elméleti nehézségre ami megakadályozza, hogy hatékony algoritmussal megoldhassunk egy feladatot, legyünk bármilyen okosak, legyenek bármilyen zseniális ötletünk.

Az (1) feladatot intenzíven vizsgálják, sok új algoritmus, algoritmuselméleti technika születik nap mint nap. A (2) feladat jóval nehezebb, szinte azt mondhatjuk semilyen eredmény sem született ebben az irányban. Két fontos „támadási irányt” említünk meg:

- (a) A Turing-gép általános modelljét helyettesítsük egy egyszerűbb számítási modellel (ami így várhatóan nem univerzális számítási fogalom) és próbáljunk ott alsó becsléseket bizonyítani. Például a SORTING (n szám nagyság szerinti sorbarendezése) problémánál csak két input szám összehasonlítása és az eredmény szerinti szétágazás alapján dolgozzon eljárásunk. A megkötés természetes. A legtöbb algoritmus ilyen. Belátható, hogy legalább $n \log n$ összehasonlítás szükséges az $otuput$ kiszámításához.
- (b) Ne (abszolút) nehézséget vizsgáljunk, hanem relatívet. Tehát célünk csak annak igazolása, hogy egy probléma legalább olyan nehéz mint egy másik.

Az utóbbi út nagyon gyümölcsözőnek bizonyult. Erről lesz szó ebben az előadásban.

2. Problémák redukciói

Egy L nyelv/probléma ω inputja lényegében egy kérdés: ω hozzátartozik L -hez? A redukció egy olyan hozzárendelés/számolás, ami a kérdés megválaszolása helyett egy új kérdést számol ki: „Leírok egy $\tilde{\omega}$ új inputot és megkérdezem, hogy egy új \tilde{L} nyelvhez tartozik-e. Ha valaki megmondja a választ, akkor én meg tudom mondani az eredeti kérdésre a választ. Sőt az ugyanaz lesz mint az én kérdésemre.” A gondolat furcsa, de fontos. Lássuk a formalizmust:

Definíció. Legyen $L, \hat{L} \subset \Sigma^*$ két nyelv és \mathcal{C} egy bonyolultsági osztály. L redukálható \hat{L} -ra \mathcal{C} -ben, jelben: $L \preceq_{\mathcal{C}} \hat{L}$, ha létezik R kiszámítható Turing-gép, hogy

- (i) R egy \mathcal{C} komplexitású gép/eljárás,
- (ii) $\omega \in L$ pontosan akkor, ha $\tilde{\omega} \in \hat{L}$, ahol $\tilde{\omega}$ az ω -ból R által kiszámolt jelsorozat.

A bevezetett reláció olvasata: L redukálható \hat{L} -re \mathcal{C} -ben. Az L -ben rejlő kérdés visszavezethető az \hat{L} -ben rejlő kérdésre. Jelentése: Az \hat{L} nyelv eldöntési feladata „legalább olyan nehéz”, mint az L -é „modulo \mathcal{C} ”.

Más redukció fogalmak is léteznek. A fenti definíció Karp munkásságában rejlik és általában Karp-redukcióként hivatkozzák. Ha szükség van ennek hangsúlyozására, akkor a $\preceq_{\mathcal{C}}^{\text{Karp}}$ jelölést használjuk. Ebben a kurzusban legtöbbször ilyen redukciót látunk. Legtöbbször le is hagyjuk a felső indexet.

2.1. Egyszerű példák

Legyen

$$\begin{aligned} \text{KLIKK} &= \{[G, k] : G\text{-ben van } k \text{ elemű klikk}\} \\ \text{FÜGGETLEN-CSÚCSHALMAZ} &= \{[G, k] : G\text{-ben van } k \text{ elemű független} \\ &\quad \text{csúcshalmaz}\} \\ \text{LEFOGÁS} &= \{[G, k] : G \text{ lefogható } k \text{ csúccsal}\} \end{aligned}$$

Az alábbi redukciók lényege jól ismert a BSc-s Kombinatorika tárgyból.

Példa. $\text{KLIKK} \preceq_{\mathcal{P}} \text{FÜGGETLEN-CSÚCSHALMAZ}$.

A redukció rendkívül egyszerű: Adott egy $\omega = [G, k]$ inputja a KLIKK problémának. Ekkor G kódjából kiszámoljuk a komplementerét (annak kódját). $\tilde{\omega}$ a $[\bar{G}, k]$ karaktersorozat lesz. A korábbi gráfelméleti tanulmányainkból az új „kérdés” ekvivalens az eredetivel. $\tilde{\omega}$ kiszámításának bonyolultsága nyilván polinomiális (igazából logaritmikus tárban megoldható).

Példa. $\text{FÜGGETLEN-CSÚCSHALMAZ} \preceq_{\mathcal{P}} \text{LEFOGÁS}$.

A redukció rendkívül egyszerű: Adott egy $\omega = [G, k]$ inputja a FÜGGETLEN-CSÚCSHALMAZ problémának. Ekkor G és k kódjából kiszámoljuk $|V(G)| - k$ értéket. $\tilde{\omega}$ a $[G, |V(G)| - k]$ karaktersorozat lesz. A korábbi gráfelméleti tanulmányainkból az új „kérdés” ekvivalens az eredetivel. $\tilde{\omega}$ kiszámításának bonyolultsága nyilván polinomiális (igazából logaritmikus tárban megoldható).

Példa. LEFOGÁS \preceq_P KLIKK.

A redukció rendkívül egyszerű: Adott egy $\omega = [G, k]$ inputja a LEFOGÁS problémának. Ekkor G és k kódjából kiszámoljuk a komplementerét és $|V(G)| - k$ -t. $\tilde{\omega}$ a $[G, |V(G)| - k]$ karaktersorozat lesz. A korábbi gráfelméleti tanulmányainkból az új „kérdés” ekvivalens az eredetivel. $\tilde{\omega}$ kiszámításának bonyolultsága nyilván polinomiális (igazából logaritmikus tárban megoldható).

Megjegyezzük, hogy se a KLIKK, se a LEFOGÁS, se a FÜGGETLEN-CSÚCS-HALMAZ nyelvre nem ismert hatékony algoritmus. Ha bármelyikre lenne, akkor az a másik problémára is jelentős kihatással lenne.

A teljesség kedvéért megemlítünk egy másik fajta redukciót. Ezt Turing nevéhez fűzik.

2.2. Turing-redukció

Definíció. Legyen $L, \hat{L} \subseteq \Sigma^*$ két nyelv és \mathcal{C} egy bonyolultsági osztály.

$L \preceq_{\mathcal{C}}^{\text{Turing}} \hat{L}$ pontosan akkor, ha megadható R eldöntő Turing-gép, amelyre

- (i) L -et dönti el és R egy L_2 -orákulumos gép.
- (ii) R bonyolultsága \mathcal{C} -beli.

(i)-ben szerepel egy eddig ismeretlen fogalom, amit tisztáznunk kell.

Definíció. Legyen $O \subset \Sigma^*$ egy nyelv. R egy O -orákulumos gép, ha van egy extra kérdés/orákulum-szalagja. Erre csak írhat a gép (nincs szem a szalag felett, a kéz csak jobbra mozogva írhat). Az írott karakterek $\Sigma \cup \{?\}$ elemei, azaz az O nyelv ábécéjének elemei és egy speciális ‘?’ jel. A kérdésszalagra a ? jel feírása egy kérdés feltételét jelenti. Az előző kérdőjel (vagy szalag-kezdő jel) és közte lévő Σ^* -beli karaktersorozatról kérdezi meg a gép/algoritmus, hogy az orákulum O nyelvéhez tartozik-e. Az állapothalmaz

$$\{\text{ORÁKULUM-IGEN, ORÁKULUM-NEM}\} \times S_0$$

alakú. Az átmeneti függvény a következő konfigurációnak az állapotában csak a második komponensre hat. Az első komponens csak akkor változik, ha az algoritmus kérdést tesz fel az orákulumhoz. A változást a kérdés karaktersorozat O -hoz való viszonyától függ természetes módon. Azaz a kérdés ára 1 időegység és 0 tár. Ezek után a futás (a kiinduló konfigurációból generált konfigurációsorozat), a kiszámított nyelv értelemszerűen definiálható.

A Karp-redukció nagyon speciális Turing-redukció: Szokásos számolás után egyetlen kérdés hangozhat el az \hat{L} nyelvhez tartozásról. A kérdésre adott válasz egyben a kiszámított bit is.

A Turing-redukció nyilván sokkal erősebb fogalom. Az \hat{L} -ra úgy gondolhatunk, mint egy megíratlan szubrutin. A redukció lényege, hogy ha a \hat{L} szubrutint valaki hatékonyan leírja, akkor L hatékonyan eldönthető (feltéve, hogy R hozzájárulása (ami \mathcal{C} bonyolultságú) is hatékonynak tekinthető). Mi nem kívánjuk a a szubrutin megvalósítását, „meghívását” és az eredmény megkapását egyetlen lépésnek számoljuk.

2.3. Redukálhatóság tulajdonságai

Végül megemlítünk egy fontos tulajdonságát a redukciónak.

1. Lemma. (i) $\preceq_{\mathcal{P}}$ tranzitív.

(ii) $\preceq_{\mathcal{L}}$ tranzitív.

(iii) Legyen $s(n) \geq \log n$ szép tárfüggvény. Ha $L_1 \preceq_{\mathcal{SPACE}(\mathcal{O}(s(n)))} L_2$ és $L_2 \preceq_{\mathcal{L}} L_3$, akkor $L_1 \preceq_{\mathcal{SPACE}(\mathcal{O}(s(n)))} L_3$

Bizonyítás. (i) Tegyük fel, hogy $L_1 \preceq_{\mathcal{P}} L_2$ és $L_2 \preceq_{\mathcal{P}} L_3$. Továbbá R_1 és R_2 kettő, a két redukciónak igazoló algoritmus. Speciálisan R_1 és R_2 is polinomiális. Legyen p_1 és p_2 két polinom, ami R_1 és R_2 időkorlátját adják. p_2 -ről feltehetjük, hogy monoton növvő.

Egy ω inputon futtassuk R_1 -et, ami $\tilde{\omega}$ karaktersorozatot számolja ki. Majd R_2 -t futtassuk $\tilde{\omega}$ -n, ami $\tilde{\tilde{\omega}}$ kiszámításához vezet. Az így kapott Turing-gép legyen R . Belátjuk, hogy R a $L_1 \preceq_{\mathcal{P}} L_3$ redukciónak igazolója.

$\omega \in L_1$ akkor és csak akkor teljesül, ha $\tilde{\omega} \in L_2$. Ami akkor és csak akkor teljesül, ha $\tilde{\tilde{\omega}} \in L_3$ ban,

Be kell még látni, hogy R polinomiális. ω inputon R időigénye $p_1(|\omega|) + p_2(|\tilde{\omega}|)$. $\tilde{\omega}$ -t egy p_1 időkorlátú gép számolja ki ω -ból, így $|\tilde{\omega}| \leq p_1(\omega)$. Így ω -n a futási idejére a következő felső becslés adódik

$$p_1(|\omega|) + p_2(|\tilde{\omega}|) \leq p_1(|\omega|) + p_2(p_1(|\omega|)).$$

Ez egy polinomiális felső becslés.

(ii) Tegyük fel, hogy $L_1 \preceq_{\mathcal{L}} L_2$ és $L_2 \preceq_{\mathcal{L}} L_3$. Továbbá R_1 és R_2 kettő, a két redukciónak igazoló algoritmus. Speciálisan R_1 és R_2 is logaritmikus tárigenyű.

A két redukciónak az előző módon rakunk össze egy R algoritmust: Egy ω inputon futtassuk R_1 -et, ami $\tilde{\omega}$ karaktersorozatot számolja ki. Majd R_2 -t futtassuk $\tilde{\omega}$ -n, ami $\tilde{\tilde{\omega}}$ kiszámításához vezet.

Az így kapott algoritmus NEM jó. A közbülsőnek kiszámolt $\tilde{\omega}$ -ra a munkaszalagon an szükség. Ez várhatóan nem fér el logaritmikus tárban. Ennek ellenére ezen R algoritmus futása legyen a fejünkben. Az igazi \tilde{R} redukciónak felismerjük R futásának töredékeit.

\tilde{R} munkaszalagjai megfelelnek R_1 munkaszalagjainak plusz R_2 munkaszalagjainak. Lesz két plusz szalagunk a korábbi szalag helyett, ami R_1 output- és a vele közös R_2 inputszalagja volt. A plusz két szalag közül az első R_1 output szalagjának egy pozíciójának indexét (a szalag feletti kéz pozícióját) tartalmazza, míg másik szalag tartalma R_2 inputszalagján egy pozíció indexe (a szalag feletti szem pozíciója).

\tilde{R} az R_2 szimulációját végzi az $\tilde{\omega}$ inputszalag tartalom nélkül. Minden olvasási feladatnál meg kell dolgoznunk. Ekkor tudjuk, hogy az R_1 által kiszámolt karaktersorozat hanyadik karakterére vagyunk kíváncsiak. El kezdjük R_1 szimulálását. A szimuláció során a kiszámolt karaktereket nem írjuk le, csupán az output-kéz pozícióját tároljuk. Ha R_1 ír, akkor az új pozíciót összeasonlítjuk az olvasni kívánt pozícióval. Ha megegyezik a két pozíció, akkor a le nem írt karaktert kiolvassuk az állapotból és az R_1 -szimulációt leállítjuk, folytatjuk az R_2 -szimulációt. Ha a két pozíció különbözik, akkor az R_1 -szimulációt folytatjuk.

(iii) Az előző bizonyítás ötletei most is működnek. ■

A fenti bizonyítás egy kis módosítása az alábbi lemmához vezet.

2. Lemma.

(i) $L \preceq_{\mathcal{P}} \widehat{L}$ és $\widehat{L} \in \mathcal{P}$, akkor $L \in \mathcal{P}$.

(ii) $L \preceq_{\mathcal{L}} \widehat{L}$ és $\widehat{L} \in \mathcal{L}$, akkor $L \in \mathcal{L}$.

Bizonyítás. Tekintsünk egy A Turing-gépet, amely az L -ről \widehat{L} -ra történő redukciót végzi, valamint \widehat{A} -ot, amely a \widehat{L} nyelvhez tartozási feladatot dönti el \mathcal{P} -ben. Legyen adott az ω input.

Ekkor végezzük el a

$$\omega \rightarrow A(\omega) \in \Sigma^{p(n)} \rightarrow \widehat{A}(A(\omega)) \in \{\text{ELFOGAD}, \text{ELVET}\}$$

számolást. Az első időigényét az n inputméretben egy p polinom korlátozza. A leghosszabb input, amit kiszámolhatunk $\Sigma^{p(n)}$ -ba esik. A második lépés időigényét az inputméretben egy q polinom korlátozza. Az összidő $(p + q \circ p)(n)$, ami n egy polinomiális függvénye.

A két algoritmus együttese a Karp-redukció fogalma alapján éppen az L nyelvet dönti el, vagyis L is eldönthető polinom időben.

(ii) Az (i) rész és az előző lemma ötletei alapján nyilvánvaló. ■

2.4. Egy további példa

Példa. Legyen L egy tetszőleges \mathcal{NL} -beli nyelv. Ekkor

$$L \preceq_{\mathcal{L}} \overrightarrow{st}\text{-ELÉRHETŐSÉG}.$$

A példához tartozó igazolás tulajdonképpen már elhangzott korábban. Korábban elhangzottakat foglal össze az alábbi tétel:

3. Tétel. Legyen $L \in_T \mathcal{NL}$. Feltehető, hogy a tartalmazást igazoló Turing-gépnek adott hosszúságú inputokon kétféle leálló konfigurációja van (így elfogadó futások ugyanabban a konfigurációban érnek véget).

$\omega \in \Sigma^*$ -hoz rendelhető a T logaritmikusan táru Turing-gép redukált konfigurációinak (irányított) $\overrightarrow{G} = \overrightarrow{G}_{T,\omega}$ gráfja. Ebben ott van v_0 a kiinduló konfigurációnak megfelelő csúcs és v_+ az elfogadó konfigurációnak megfelelő csúcs. Ez a hozzárendelés olyan, hogy

(i) $\omega \in L$ akkor és csak akkor, ha $[\overrightarrow{G}_{\omega,T}, v_0, v_+] \in \overrightarrow{st}\text{-ELÉRHETŐSÉG}$.

(ii) A hozzárendelés kiszámítható és tárigénye $\mathcal{O}(\log(n))$.

A tételből következik a példa korrektsége. Ez a példa jóval általánosabb mint a korábbi példa. Hogy ezt lássuk nézzük meg néhány következményt.

4. Következmény. Ha $\overrightarrow{st}\text{-ELÉRHETŐSÉG} \in \mathcal{P}$, akkor $\mathcal{NL} \subset \mathcal{P}$.

A feltétel igaz, ez egyszerűen adódik például az algoritmuselméleti előadásokon megismert gráf-bejárás algoritmusok leírásából és elemzéséből. A fenti következmény a $\mathcal{NL} \subset \mathcal{P}$ tartalmazásra adott korábbi bizonyításunk újratárgyalása.

5. Következmény. Ha $\overrightarrow{st}\text{-ELÉRHETŐSÉG} \in \mathcal{L}$, akkor $\mathcal{NL} = \mathcal{L}$.

A konklúzió igazából $\mathcal{NL} \subset \mathcal{L}$ (a másik irányú tartalmazás nyilvánvaló). Itt a feltétel igazsága nem ismert, sőt sokan úgy hiszik nem is igaz. Ennek egy indoka lehet, hogy két bonyolultságosztály váratlan egybeesését vonná magával.

3. Teljesség

A fenti okoskodás nagyon fontos. A gondolatmenet lényege, hogy a példa alapján \vec{st} -ELÉRHETŐSÉG az egész \mathcal{NL} nyelvosztály nehézségét magában foglalja. Ez vezet el egy általánosabb fogalom megalkotásához:

Definíció. \widehat{L} nyelv teljes a \mathcal{C} osztályban az \mathcal{R} bonyolultságú rekurzióra, ha:

- (i) $\widehat{L} \in \mathcal{C}$,
- (ii) minden $L \in \mathcal{C}$ esetén $L \preceq_{\mathcal{R}} \widehat{L}$.

Négy speciális esetet kiemelünk.

Definíció. Az \widehat{L} nyelv \mathcal{NP} -teljes ha teljes \mathcal{NP} -ben a \mathcal{P} redukcióra. Azaz \widehat{L} nyelv \mathcal{NP} -teljes, ha

- (i) $\widehat{L} \in \mathcal{NP}$,
- (ii) minden $L \in \mathcal{NP}$ esetén $L \preceq_{\mathcal{P}} \widehat{L}$.

A fenti megállapodás egy alternatívája a $\preceq_{\mathcal{L}}$ redukcióval való dolgozás. Ez a szigorúbb értelmezés is igaz lesz a legtöbb későbbi \mathcal{NP} -teljességet igazoló redukciókra. Mi azonban csak a redukciók könnyebben ellenőrizhető polinom időbeliségét követeljük meg.

Definíció. Az L nyelv \mathcal{NL} -teljes, ha teljes \mathcal{NL} -ben az \mathcal{L} -beli redukcióra nézve.

Definíció. Az L nyelv \mathcal{P} -teljes, ha teljes \mathcal{P} -ben az \mathcal{L} -beli redukcióra nézve.

Definíció. Az L nyelv \mathcal{PSPACE} -teljes, ha teljes \mathcal{PSPACE} -ben a \mathcal{P} -beli redukcióra nézve.

Definíció. \widehat{L} nehéz a \mathcal{C} osztályra \mathcal{R} bonyolultságú redukcióval, ha minden $L \in \mathcal{C}$ esetén $L \preceq_{\mathcal{R}} \widehat{L}$.

Azaz a nehézség a teljesség fogalma az (i) feltétel nélkül. Azaz nem követeljük meg az osztályhoz tartozást csak az osztály elemeinek visszavezethetőségét rá. Gyakran kiszámíthatósági feladatokra is mondják, ha \mathcal{C} -nehéz, ha van olyan redukciós algoritmus, amely által kiszámolt $\tilde{\omega}$ karaktersorozatra a feladat olyan értéket ad, amiből ω nyelvhez tartozása könnyen látható.

A következő tétel az új fogalmak segítségével tömören fogalmazza meg egy korábbi eredményeinket.

6. Tétel. \vec{st} -ELÉRHETŐSÉG \mathcal{NL} -teljes.

A redukciók vizsgálatánál láttuk az \mathcal{NL} -nehézséget. Még korábban láttuk az \mathcal{NL} -hez tartozást.

A tétel alapján az \vec{st} -ELÉRHETŐSÉG-ről szerzett tudásunk egész \mathcal{NL} -re kihat. Erre már láttunk egy példát: \vec{st} -ELÉRHETŐSÉG $\in \mathcal{P}$. Ez alapján adódott, hogy $\mathcal{NL} \subset \mathcal{P}$.

Savitch algoritmus a tárral spórol. Az \vec{st} -ELÉRHETŐSÉG-et \log^2 tárban oldja meg. Egyből adódik a következő tétel:

7. Tétel.

$$\mathcal{NL} \subset \mathcal{SPACE}(\log^2 n).$$

Tetszőleges $\mathcal{NSPACE}(s(n))$ -beli probléma visszavezethető egy \vec{st} -ELÉRHETŐSÉG problémára, ami $\mathcal{O}(s^2(n))$ tárban megoldható. Tehát

8. Tétel.

$$\mathcal{NSPACE}(s(n)) \subset \mathcal{SPACE}(\mathcal{O}(s^2(n))).$$

Speciálisan kapjuk a $\mathcal{PSAPCE} \subset \mathcal{NPSAPCE}$ tartalmazás fordítottját. Azaz

9. Tétel. $\mathcal{PSAPCE} = \mathcal{NPSAPCE}$.

Tudjuk, hogy a determinisztikus osztályok zártak a komplementálásra. Speciálisan kapjuk a következőt:

10. Tétel. $\mathcal{NPSAPCE}$ zárt a komplementálásra.

Egy még „absztraktabb” tétel a következő:

11. Következmény ⁺. *Legyen S szép tárfüggvények egy osztálya, ami zárt a négyzetre emelésre. Ekkor $\mathcal{NPSPACE}(\cup_{s \in S} s(n)) = \mathcal{PSPACE}(\cup_{s \in S} s(n))$.*

Speciálisan $\mathcal{NPSPACE}(\cup_{s \in S} s(n))$ zárt a komplementálásra, azaz

$$\mathcal{NPSPACE}(\cup_{s \in S} s(n)) = \text{co}\mathcal{NPSPACE}(\cup_{s \in S} s(n)).$$

Így egy másik speciális eset: $\mathcal{EXSPACE} = \mathcal{NEXSPACE}$.