

# **Bonyolultságelmélet jegyzet**

Készítették Grolmusz Vince előadásai alapján a 2025/25. évi hallgatók

(Nem hivatalos lektorátlan verzió)

2025. ősz

# Contents

1	Kommunikációs játékok .....	3
2	NP-n túl .....	9
2.1	Polinomialis hierarchia .....	9
2.2	PSPACE teljesség .....	12

# 1 Kommunikációs játékok

Ennek a fejezetnek a nagy része (majdnem minden) a számítástudomány jegyzetből lett átemelve.

Ezt a fejezetet újra kell olvasni és megnevezni mekkora az átfedés a számítástudományon elhangzottak és a bonyolultságon elhangzottak között. A fő tettek megtalálhatók bizonyításokkal: Teglalapp fedés, Mehlhorn–Schmidt, AUY

Cél: van két játékos, akik bármit ki tudnak számolni gyorsan, de egymás között nehezen kommunikálnak.

## Definíció 1.1

## Kommunikációs játék

Adott  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  és  $x, y \in \{0, 1\}^n$ . A ismeri  $x$ -et, de  $y$ -t nem, B ismeri  $y$ -t, de  $x$ -et nem. Ki akarják számolni  $f(x, y)$ -t. A költség az A és B között (bármely irányban) kommunikált bitek száma.

Akkor tekintjük  $f(x, y)$ -t kiszámoltnak, ha az egyik játékos ismeri  $f(x, y)$ -t, és a másik játékos tudja, hogy az egyik tudja.

## Definíció 1.2

## Protokoll költsége

A  $P$  protokoll mellett  $f$  költsége a legrosszabb  $(x, y)$  input páron  $\kappa_P(f)$ .

## Megjegyzés

Megkövetelhetnénk, hogy mindketten tudják  $f(x, y)$ -t, ez 1 bit különbséget jelentene csak legfeljebb.

## Definíció 1.3

## Protokoll

A közös számolási módszer szabályait, hogy mikor ki, és milyen bitet küld protokollnak nevezzük. (Ez az algoritmus megfelelője több játékos esetén.)

## Példa

Legyen  $f$  tetszőleges, ekkor A elküldheti  $x$ -et B-nek, aki „ingyen” kiszámolja  $f(x, y)$ -t. Ennek a költsége  $n$ .

## Példa

## ID-függvény

Legyen

$$\text{ID}(x, y) = \begin{cases} 1, & \text{ha } x = y \\ 0, & \text{ha } x \neq y \end{cases}$$

Ekkor a fenti  $P$  protokollal  $\kappa_P(\text{ID}) = n$  teljesül.

## Definíció 1.4

## Kommunikációs bonyolultság

$\kappa(f)$  a  $\kappa_P(f)$ -ek minimuma az összes  $f$ -et kiszámoló  $P$  protokollon.

### Tétel 1.5

$$\kappa(\text{ID}) = n.$$

Ennek a bizonyításához kell a következő definíció és tétel.

### Definíció 1.6

### Kommunikációs mátrix

Az  $f$  kommunikációs mátrixa az az  $M_f \in \{0, 1\}^{2^n \times 2^n}$ , amelynek sorai  $x$ -szel, oszlopai  $y$ -nal vannak indexelve, és az  $x$ -hez tartozó sor  $y$ -hoz tartozó oszlopában  $f(x, y)$  szerepel.

### Megjegyzés

A továbbiakban a log mindig a 2-es alapú logaritmust jelenti.

### Tétel 1.7

### Mehlhorn–Schmidt

$\kappa(f) \geq \log r(M_f)$ , ahol  $r(M_f)$  az  $M_f$  mátrix rangját jelöli.

**Proof:** Legyen  $P$  egy adott protokoll. Tegyük fel, hogy A kezd. Ekkor A kommunikál egy bitet. Ez rögzített  $P$  protokoll mellett bizonyos  $x$ -ekre 0, bizonyos  $x$ -ekre 1. Ezzel az  $M_f$  mátrixot két részre bontja: az egyik részben azon sorok vannak, amelyekre 0-t mond, a másikon azok, amelyekre 1-et. Ezek közül az egyik sorrangja  $\geq \frac{1}{2} r(M_f)$ .

Ezt ismételjük addig, amíg A lép. Amikor B lép, akkor ugyanez elismételhető oszloprangra, de egy mátrix sor- és oszloprangja megegyezik. Ha  $x$  és  $y$  olyan, hogy minden lépésnél a nagyobb rangú részmátrixot adják meg, akkor  $k$  lépés után a részmátrix rangja  $\geq 2^{-k} r(M_f)$ .

Tegyük fel, hogy a  $k$ . lépésben vége van a játéknak. Ekkor szimmetriaokokból feltehető, hogy A tudja  $f(x, y)$ -t, és B tudja, hogy A tudja. Mivel A tudja  $f(x, y)$ -t, az így kapott részmátrix minden sora homogén, azaz vagy csupa 0-t, vagy csupa 1-et tartalmaz. Ha pedig egy sor nem homogén, akkor A nem tudhatja biztosan  $f(x, y)$ -t. Hasonlóan, az, hogy B tudja biztosan  $f(x, y)$ -t, az azzal ekvivalens, hogy a kapott részmátrix minden oszlopa homogén.

Mivel homogén részmátrix rangja 1, az előbbi egyenlőtlenség szerint  $1 \geq 2^{-k} r(M_f)$ , azaz  $2^k \geq r(M_f)$  fog teljesülni minden olyan  $(x, y)$  párra, amelyeket  $P$   $k$  lépésben számol ki.  $\square$

### Következmény 1.8

Innen könnyen kijön, hogy  $\kappa(\text{ID}) = n$ , ugyanis  $M_{\text{ID}} = I_{2^n}$ , és  $r(I_{2^n}) = 2^n$ , tehát  $n \leq \kappa(\text{ID})$  a Mehlhorn–Schmidt-tétel miatt. Másrészt láttuk, hogy  $\kappa(f) \leq n$  minden  $f$ -re, így  $\kappa(\text{ID}) = n$ .

### Megjegyzés

Felső becslés nem ismeretes  $\kappa(f)$ -re. Lovász és Suchs nevéhez fűződő sejtés szerint  $\exists c > 0$  :  $\kappa(f) \leq \log^c(r(M_f))$ . Tudjuk, hogy  $c > 2$  kell hogy teljesüljön. Ismert továbbá, hogy  $\kappa(f) \leq r(M_f)$ .

### Következmény 1.9

$\text{DISJ}(x, y) = \chi_{\{x \cdot y = 0\}}$ , a halmazdiszjunktsági feladat. Akkor erre is  $\kappa(\text{DISJ}) = n$ .

**Proof of Következmény:** Elemszám szerint rendezve az  $n$  elemű halmaz részhalmazait a sorokban, és a komplementereiket az oszlopokban

$$M_{\text{DISJ}} = \begin{bmatrix} 1 & * & * & \dots \\ 0 & 1 & * & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

felsőháromszög alakú, vagyis  $\kappa(\text{DISJ}) = n$

□

### Definíció 1.10

### Nemdeterminisztikus kommunikációs bonyolultság

Alíz ismeri  $x$ -et, Bob ismeri  $y$ -t, E.T. ismeri mindkettőt, és  $f$ -et is. Utóbbi meg akarja győzni a játékosokat, hogy tudja. Ezt egy bizonyítással teszi, amit függetlenül A-nak, és B-nek is el kell fogadnia. Egy fix E.T. által az  $(x, y)$  párra adott bizonyítás hossza, amikor azt akarja bizonyítani, hogy  $f(x, y) = 1$  legyen  $\kappa_1^{\text{E.T.}}(f(x, y))$ . Legyen továbbá

$$\kappa_1^{\text{E.T.}}(f) := \max_{\{x, y: f(x, y) = 1\}} \kappa_1^{\text{E.T.}}(f(x, y)),$$

végül

$$\kappa_1(f) = \min_{\text{E.T.}} \kappa_1^{\text{E.T.}}(f)$$

a legjobb E.T. által a legrosszabb esetben adott bizonyítás hossza. Hasonlóan definiáljuk a  $\kappa_0(f)$ -et is.

### Megjegyzés

$\max \kappa_0(f), \kappa_1(f) \leq \kappa(f)$  teljesül, hiszen reprodukálhatja az adott esetben a protokoll által megszabott kommunikációját

### Példa

Ha  $x \neq y$ , akkor az  $(i, x_i = 0)$  pár (ahol  $y_i = 1$ ) megadása  $\log(n) + 1$  bit hosszú, és bizonyítja, hogy az ID feladat nem teljesül. Egyenlőségre nem látszik kapásból hasonló jó bizonyítás.

### Tétel 1.11

### Az ND kommunikációs bonyolultság jellemzése fedő téglalapokkal

$\kappa_1(f)$  az a legkisebb  $t$  szám, hogy  $M_f$  egyesei lefedhetők  $2^t$  darab csupa 1-es részmátrixsal

### Megjegyzés

$M_f$ -et már ismerjük, a kommunikációs mátrix. A tételben részmátrix alatt az oszlopok, és sorok egy-egy részhalmazait kiválasztva, a metszetekből álló részt értjük. Figyelem, ez nem feltétlenül egy összefüggő téglalap!

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

-ben az első és utolsó sor, és oszlopok által meghatározott rész is egy ilyen csupa egyes részmátrix.

### Következmény 1.12

Láttuk, hogy  $M_{ID} = I_{2^n}$ , ezt pedig csak úgy fedhetjük le csupa 1-es téglalapokkal, ha külön-külön kiválasztjuk az átlóelemeket. Következik, hogy  $\kappa_1(ID) = n$ .

**Proof of Az ND kommunikációs bonyolultság jellemzése fedő téglalapokkal:**

$(\kappa_1(f) \leq t)$

Tekintsük a fedő téglalapokat. Alíznek van egy sora, Bobnak egy oszlopa. A protokollban megállapodnak a  $2^t$  darab fedőmátrix egy sorrendjében. E.T. bizonyítása az lesz, hogy hanyadik rész mátrixban van az  $(x, y)$  metszet, ez  $t$  bittel kódolható, leellenőrzik, hogy benne van-e az adatuk, és mivel ez csupa egyesből áll, így szükségszerűen  $f(x, y) = 1$ . %feltesszük, hogy E.T. nem hazudik?

$(\kappa_1(f) \geq t)$

Legyen

$H_\alpha = \{(x, y) : A\text{-nál } x, B\text{-nél } y \text{ van, és } \alpha \text{ üzenetet hallják, akkor elfogadják a bizonyítást}\}.$

Ha  $(x_1, y_1), (x_2, y_2) \in H_\alpha$ , akkor  $(x_1, y_2), (x_2, y_1) \in H_\alpha$ , hiszen az  $\alpha$  bizonyítást Alíz elfogadta  $(x_1, y_1)$ -re, az ő nézőpontjából semmi nem különbözteti meg a szituációt attól, mintha  $(x_1, y_2)$  lenne a felállítás, ezt pedig Bob is elfogadja, hiszen számára  $(x_1, y_2)$ , és  $(x_2, y_2)$  ugyanolyan, és ez utóbbit elfogadta  $\alpha$ -ra. Következik, hogy minden  $\alpha$ -ra  $H_\alpha$  megfelel egy rész mátrixnak. Ha E.T. legfeljebb  $t$  bitből bizonyítani tudja, hogy  $f(x, y) = 1$ , ez szolgáltat lazanyát és  $2^t$  darab csupa egyes rész mátrixot. □

Randomizálva azonban gyorsan is lehet a következő Simon és Rabin nevéhez fűződő protokollal. A generál egy véletlen  $p$  prímet  $\in \{1, \dots, n^2\}$  (ahol  $\log x, \log y \leq n$ ), és elküldi az  $(x \bmod p, p)$  üzenetet, B pedig leellenőrzi, hogy  $x \equiv y \bmod p$  teljesül-e, és ezt mondjuk százszor megismétlik.

Ha egyszer is az teljesül, hogy inkongruensek, akkor az eredeti számok sem lehetnek egyenlőek, ha mindig kongruensek, és mégsem egyenlőek, akkor százszor teljesült az, hogy  $p | x - y \neq 0$ .

$A \leq 2^n$  számoknak legfeljebb  $n$  darab prímosztója lehet, és  $n^2$ -ig nagyjából  $\pi(n^2) \sim \frac{n^2}{2 \log(n)}$  darab prím van. Annak a valószínűsége, hogy egyszer teljesül a kongruencia

$$\mathbb{P}(p | x - y) \leq \frac{n}{\frac{n^2}{2 \log(n)}} = \frac{2 \log n}{n} \rightarrow 0.$$

Egy kommunikáció  $4 \log n$  bitet küld, ergo összesen  $400 \log n$  bitnyi kommunikáció történik.

**Nem (teljesen) triviális protokollok:**

### Példa

Tekintsünk egy fagráfot, aminek van két részfája. Kérdés, hogy az  $n$  csúcsú  $T$  fa  $T_1, T_2$  részfájának van-e közös csúcsa. Alíz kapja  $T_1$ -et, Bob  $T_2$ -t értelemszerűen, és mindketten ismerik  $T$ -t. Ez eldönthető lenne a DISJ játék speciális eseteként, de adunk egy okosabb protokollt.

Alíz megmondja  $T_1$  egy tetszőleges  $v$  csúcsát (ez ugye  $\log n$  bit kommunikáció). Majd Bob kiszámolja  $T_2$ -ben a  $v$ -hez legközelebbi  $w$  csúcsot, mivel fában egyértelmű út van két csúcs között, ez értelmes. Ezt visszaküldi Alíznek, ellenőrzi, hogy  $w \in T_1$ , ha igen, ez metszetbeli, és készen vagyunk, ha nem, akkor azt mondja, hogy a két fa diszjunkt. Ugyanis, ha a legközelebbi  $w$  pont nem része a fának, de egy további  $u$  pont része lenne  $T_1$ -nek, az  $uw$  szakasz  $T_2$ -ben van, az  $uw$  szakasz pedig  $T_1$ -ben, vagyis  $u$  közelebb van  $v$ -hez, mint  $w$ .

### Példa

Most Alíz és Bob két részgráfot kap egy  $G$  gráfból úgy, hogy  $G_A$  független csúcsokból áll,  $G_B$  pedig egy teljes részgráf. Kérdés, hogy van-e metszet?

Világos, hogy ha van, legfeljebb 1 pontból állhat.

1. Alíz megnézi, hogy van-e legalább  $\frac{n}{2}$  fokú  $v$  csúcs a gráfjában, ha igen, akkor  $(1, v)$ -t küldi el, ha nem, 0-t.
2. Bob megnézi, hogy van-e  $< \frac{n}{2}$  fokú  $w$  csúcs  $G_B$ -ben, ha igen,  $(1, w)$ -t küld, ha nincs, 0-t.

Ezek után Bob tudja, hogy  $G_A$   $v$ -ből, és a nem-szomszédaiából áll, ez legfeljebb  $\frac{n}{2}$  csúcsból áll, és iteratíven folytathatjuk ezt az eljárást amíg lehet. Ha Bob talál egy kis fokszámú  $w$  csúcsot, akkor az ő gráfjának a többi csúcsa ennek a szomszédai közül kerül ki, és ismét rekurzíven folytatható az eljárás. Mi történik, ha mindketten 0-t küldenek? Alíz gráfjában minden csúcs kisebb mint  $\frac{n}{2}$  fokú,  $G_B$ -ben pedig minden csúcs legalább  $\frac{n}{2}$  fokú, ez a két feltétel kizárja egymást, így a két gráf diszjunkt. Addig ismételtetik a fenti lépést, amíg nem mondanak mindketten nullát. Egy lépés  $\log n + 1$  bit, és  $\log n$  lépésben persze kimerítik a gráfot, vagyis  $O(\log^2 n)$  bitre van összesen szükség.

### Tétel 1.13

Aho–Ullman–Yanakakis

Minden  $f$ -re

$$\kappa(f) \leq (2 + \kappa_0(f))(2 + \kappa_1(f)).$$

### Lemma 1.14

Ha  $M$  egy  $0 - 1$  mátrix,  $H$  egy azonosan nulla részmátrixa,  $H$  sorai alkossák az  $A$ , oszlopai a  $B$  mátrixot, ekkor  $\rho(A) + \rho(B) \leq \rho(M)$ , ahol  $\rho(M)$  a sor/oszloppermutációval képezhető legnagyobb négyzetes felsőháromszög részmátrix méretét jelölli, aminek a főátlója csupa 1-ből áll.

**Proof of Lemma:** A lemma azon múlik, hogy  $A$  és  $B$ -t külön-külön mozgathatjuk, a csupa nulla metszet nem fog változni, és a másik mátrixhoz nem nyúltunk hozzá, diszjunkt sorokból/oszlopokból áll. Egy permutációval megfelelő helyre visszük  $A$ -ban a maximális  $U_A$  felsőháromszög mátrixot, ezt  $B$ -ben is elvégezve ( $U_B$ ) kapunk egy  $\begin{bmatrix} U_B & \\ 0 & U_A \end{bmatrix}$  felsőháromszöget  $M$ -ben.

$$\left[ \begin{array}{c|c|c} & \begin{array}{c} \bar{B}_1 \\ \bar{B}_2 \end{array} & \\ \hline \begin{array}{c} A_1 \\ A_1 \end{array} & 0 & A_2 \\ \hline & \begin{array}{c} \bar{B}_2 \\ \bar{B}_2 \end{array} & \end{array} \right] \rightarrow \left[ \begin{array}{c|c|c|c|c} & \begin{array}{c} \bar{B}_1 \\ \bar{B}_1 \end{array} & \begin{array}{c} \bar{B}_1 \\ U_B \end{array} & & \\ \hline \begin{array}{c} A_1 \\ A_1 \end{array} & 0 & 0 & U_A & A_2 \\ \hline & \begin{array}{c} \bar{B}_2 \\ \bar{B}_2 \end{array} & \begin{array}{c} \bar{B}_2 \\ \bar{B}_2 \end{array} & \begin{array}{c} A_2 \\ A_2 \end{array} & \begin{array}{c} A_2 \\ A_2 \end{array} \end{array} \right]$$

□

**Proof of Aho–Ullman–Yanakakis:** Világos, hogy  $\rho(M_f) \leq r(M_f)$ , és  $\log \rho(M_f) \leq \kappa_1(f)$  teljesülnek, mert egy csupa 1 főátlójú felsőháromszög mátrix teljes rangú, illetve ref{NDKB jell} miatt.

Indukcióval belátjuk, hogy  $\kappa(f) \leq (2 + \log \rho(M_f))(2 + \kappa_0(f))$ . Ha  $\rho(M_f) = 1$ , akkor nem is kell kommunikálni, mert egy ilyen mátrixban vagy csak egyesek állnak, vagy pontosan egy sorában vagy oszlopában vannak egyesek. Az általános lépésben tekintsük a kommunikációs mátrix nullásainak a fedését  $2^{\kappa_0(f)}$  darab csupa nulla részmatrixszal. Alíz megnézi, hogy fed-e az ő  $x$  inputjának egy részét olyan csupa 0 részmatrix, hogy a hozzá tartozó sorokból alkotott  $A$  mátrixra  $\rho(A) \leq \frac{\rho(M_f)}{2}$ , ha igen, akkor elküldi az  $(1, \text{a csupa nulla részmatrix sorszáma})$  üzenetet, ez legfeljebb  $1 + \kappa_0(f)$  bit kommunikáció, ha nincs ilyen részmatrix, akkor 0-t küld. Bob hasonlóan megnézi, hogy van-e az  $y$ -jához olyan fedő csupa 0 mátrix, amely oszlopaihoz tartozó  $B$  mátrixra  $\rho(B) \leq \frac{\rho(M_f)}{2}$ , ha igen  $(1, \text{a fedő mátrix sorszáma})$ , ha nincs ilyen, akkor pedig 0-t küld.

Mi történik, ha mindketten 0-t küldenek?

Akkor  $f(x, y) = 1$ , hiszen ha 0 lenne, akkor a metszetüket lefedné egy csupa 0 részmatrix, de az eddigi kommunikáció szerint az ezen fedőmatrixhoz tartozó sorok, és oszlopok  $\rho$  értékei összesen többet adnak, mint  $\rho(M_f)$ , ellentmondásban a lemmánkkal. □

### Definíció 1.15

- $f \in \text{P}^{\text{CC}}$ , ha  $\exists c > 0 : \kappa(f) \leq \log^c n$ .
- $f \in \text{NP}^{\text{CC}}$ , ha  $\exists c > 0 : \kappa_1(f) \leq \log^c n$ .
- $f \in \text{co-NP}^{\text{CC}}$ , ha  $\exists c > 0 : \kappa_0(f) \leq \log^c n$ .

### Kommunikációs bonyolultságok

A fenti tétel következményeként adódik, hogy  $\text{P}^{\text{CC}} = \text{NP}^{\text{CC}} \cap \text{co-NP}^{\text{CC}}$ .

Láttuk továbbá, hogy  $\text{NP}^{\text{CC}} \neq \text{co-NP}^{\text{CC}}$ , mert ID benne van a jobb oldalon, de a balban nincs.

$\text{P}^{\text{CC}} \neq \text{co-NP}^{\text{CC}}$  szintén az ID miatt (így  $\text{P}^{\text{CC}} \neq \text{NP}^{\text{CC}}$  is teljesül).



## 2 NP-n túl

### 2.1 Polinomialis hierarchia

#### Definíció 2.1

#### Polinomiális reláció

Azt mondjuk, hogy  $P(x, y_1, y_2, \dots, y_l)$  egy polinomiális reláció, ha  $\exists i$  úgy, hogy  $\forall i : |y_i| \leq |x|^c$  és  $P(x, y_1, \dots, y_i)$  kiszámolható  $|x|$ -ben polinomimális időben.

#### Definíció 2.2

#### $\Sigma_i$

Tetszőleges  $L$  nyelvre  $L \in \Sigma_i \Leftrightarrow \exists P(x, y_1, \dots, y_i)$  polinomiális reláció úgy, hogy  $x \in L \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \dots Q y_i$  úgy, hogy  $P(x, y_1, y_2, \dots, y_i)$  teljesül. Ahol  $Q$  a következőképpen van definiálva:

$$Q = \begin{cases} \forall & \text{ha } i \text{ paros} \\ \exists & \text{ha } i \text{ páratlan} \end{cases}$$

#### Definíció 2.3

#### $\Pi_i$

Tetszőleges  $L$  nyelvre  $L \in \Pi_i \Leftrightarrow \exists P(x, y_1, \dots, y_i)$  polinomialis reláció úgy, hogy  $x \in L \Leftrightarrow \forall y_1 \exists y_2 \forall y_3 \dots \tilde{Q} y_i$  úgy, hogy  $P(x, y_1, y_2, \dots, y_i)$  teljesül. Ahol  $\tilde{Q}$  a következőképpen van definiálva:

$$\tilde{Q} = \begin{cases} \forall & \text{ha } i \text{ páratlan} \\ \exists & \text{ha } i \text{ paros} \end{cases}$$

#### Példa

Pár nevezetes bonyolultsági osztály amit már ismerünk:

1.  $\text{NP} = \Sigma_1$
2.  $\text{co-NP} = \Pi_1$
3.  $\text{P} = \Sigma_0 = \Pi_0$

#### Megjegyzés

1. Minden  $i$ -re  $\Sigma_i \subseteq \Sigma_{i+1}$ . Valasszuk úgy a polinomialis relációt hogy az utolsó változótól ne függjön.
2. Minden  $i$ -re  $\Pi_i \subseteq \Pi_{i+1}$ . Valasszuk úgy a polinomialis relációt hogy az első változótól ne függjön.
3. Minden  $i$ -re  $\Pi_i \subseteq \Sigma_{i+1}$ .
4. Minden  $i$ -re  $\Sigma_i \subseteq \Pi_{i+1}$ .

Ezen osztályokat a következő hierarchiával tudjuk vizuálisan jellemezni.

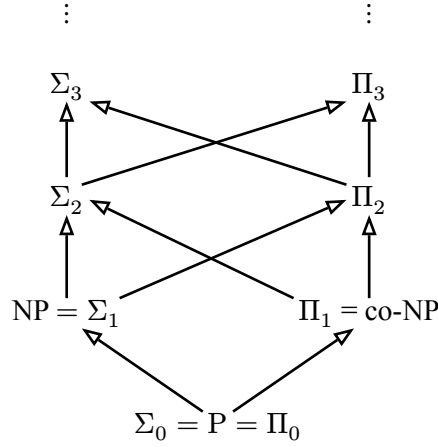


Figure 1: Polinomiális hierarchia vizualizáció

#### Definíció 2.4

#### Polinomialis Hierarchia

$$PH = \bigcup_{i=1}^{\infty} \Sigma_i = \bigcup_{i=1}^{\infty} \Pi_i$$

#### Definíció 2.5

$$\text{INDEPENDENT} := \{(G, m) : \alpha(G) \geq m\}$$

azaz, azon  $G$  grafok és  $m$  számok parosai, melyekre  $G$  függetlenségi száma nagyobb mint  $m$ .

#### Definíció 2.6

$$\text{EXACT\_INDEPENDENT} := \{(G, m) : \alpha(G) = m\}$$

azaz, azon  $G$  grafok és  $m$  számok parosai, melyekre  $G$  függetlenségi száma nagyobb pont  $m$ .

#### Állítás 2.7

$$\text{EXACT\_INDEPENDENT} \in \Sigma_2$$

**Proof:**  $\exists H \subseteq V(G)$  független csucshalmmaz és  $|H| = m$

$\forall H' \subseteq V(G)$  csucshalmazra, ahol  $|H| = m + 1$  mar  $H'$  összefuggo. □

#### Megjegyzés

A letezést ( $\exists$ ) és a mindent ( $\forall$ ) nem kell polinomialis időben számolni, csak a  $H$ -t és  $H'$ -t kell polinomialis időben ellenőrizni.

#### Tétel 2.8

Ha  $\exists i \geq 1$  amire  $\Sigma_i = \Pi_i$ , akkor  $\Sigma_{i+1} = \Pi_{i+1}$ , amiből tovább következik, hogy  $PH = \Sigma_i = \Pi_i$ . Azt mondjuk, hogy a polinomialis hierarchia *összeomlik* az  $i$ -edik szintre.

**Proof:** Mivel tudjuk, hogy  $\Sigma_i \subseteq \Sigma_{i+1}$ , ezért elég azt belátnunk, hogy  $\Sigma_{i+1} \subseteq \Sigma_i$  és ezzel belátjuk, hogy  $\Sigma_i = \Sigma_{i+1}$ . Hasonló módon be tudjuk látni hogy  $\Pi_i = \Pi_{i+1}$ .

Legyen  $L \in \Sigma_{i+1}$  tetszőleges nyelv, bizonyítsuk be hogy  $L \in \Sigma_i$ . Mivel  $L \in \Sigma_{i+1}$ , ezért letezik egy  $P$  polinomialis relacio, melyre

$$x \in L \Leftrightarrow \exists y_1 \forall y_2 \exists \dots Q y_{i+1} P(x, y_1, \dots, y_i).$$

Tovabba, letezik egy  $L' \in \Pi_i$  nyelv, melyre

$$x \in L \Leftrightarrow \exists y_1 : (x, y_1) \in L'.$$

Figyelem, itt csak annyi történt hogy beillesztettük egy extra  $y_1$  változót a letezés ( $\exists$ ) kvantorral a  $P$  definicio ele, így kaptunk egy definiciot  $\Sigma_{i+1}$ -re.

Mivel  $\Sigma_i = \Pi_i$ , ezért  $L' \in \Sigma_i$ , tehát letezik egy polinomialis relacio  $S$  úgy, hogy

$$x \in L \Leftrightarrow \exists y_1 \exists y_2 \forall \dots Q y_{i+1} S(x, y_1, \dots, y_i).$$

Csoportosíthatjuk  $y_1$ -et és  $y_2$ -t.

$$x \in L \Leftrightarrow \exists (y_1, y_2) \forall \dots Q y_{i+1} S(x, (y_1, y_2), \dots, y_i).$$

A jobboldalon  $i$  darab kvantor van és pont abban a sorrendben mint ahogy kell lenniük  $\Sigma_i$  definiciojához. Tehát beláttuk, hogy ha  $L \in \Sigma_{i+1}$  akkor  $L \in \Sigma_i$ . □

### Tétel 2.9

Savitch

Ha  $f(n) \geq n$ , akkor

$$\text{NSPACE}(f(n)) \subseteq \text{DSPACE}(f^2(n))$$

**Proof:** Legyen  $L \in \text{NSPACE}(f(n))$  egy tetszőlegese nyelv, a célunk megmutatni, hogy  $L$  felismerhető egy determinisztikus Turing-géppel  $f^2(n)$  tárban.

Figyeljük meg, hogy aha egy Turing-gép  $t$  tárat használ futása alatt, akkor legfeljebb  $O(2^{c \cdot t})$  különböző konfigurációba kerülhet.

Tudjuk, hogy van egy nemdeterminisztikus Turing-gép mely felismeri az  $L$  nyelvet, tehát a konfigurációs gráfban van út a kezdőállapotból a reprezentáns elfogadó állapotok csúcsába. Mivel legfeljebb  $2^{c \cdot f(n)}$  konfiguráció van, ezért egy elfogadó út hossza legfeljebb  $2^{c \cdot f(n)}$ .

Ha tudunk mutatni egy determinisztikus Turing-gépet ami el tudja dönteni egy gráfban, hogy adott  $s$  és  $t$  csúcsok között van-e út  $O(\log^2 n)$  tárban, akkor a konfigurációs gráfra alkalmazva  $O(f^2(n))$  méretű tárat használó eljárást adnánk  $L$  felismerésére.

Megmutatjuk, hogy  $O(\log^2 n)$  tárban el tudjuk dönteni, hogy  $s$  és  $t$  között megy-e út egy adott  $G$  gráfban. Legyen  $\text{st-conn}(k, s, t)$  az algoritmus ami eldönti, hogy legfeljebb  $k$  hosszú út van-e  $s$  és  $t$  között. Nyilván ha van olyan  $u \in V(G)$  csúcs mely  $s$ -ből elérhető legfeljebb  $k/2$  hosszú úton és  $u$ -ból  $t$  elérhető legfeljebb  $k/2$  hosszú úton, akkor  $s$ -ből  $t$  is elérhető legfeljebb  $k$  hosszú úton.

Tehát a következőképpen néz ki a rekurzió:

$$\begin{cases} \text{st-conn}(0, s, t) = \begin{pmatrix} s \stackrel{?}{=} t \end{pmatrix} \\ \text{st-conn}(1, s, t) = (st) \stackrel{?}{\in} E(G) \\ \text{st-conn}(k, s, t) = \exists u \in V(G) : \text{st-conn}(k/2, s, u) \wedge \text{st-conn}(k/2, u, t). \end{cases}$$

Látszik, hogy a rekurzió mélysége  $O(\log n)$  és mindegyik rekurzív hívásban csak a függvény argumentumait kell tárolnunk amiket bitekben  $O(\log n)$  tárban meg tudjuk oldani. Tehát az st-conn algoritmus  $O(\log^2 n)$  tárban működik, és ezzel készen is vagyunk, mivel

$$(\log(2^{c \cdot f(n)}))^2 = (c \cdot f(n) \cdot \log 2)^2 = c^2 \cdot f^2(n) = O(f^2(n)).$$

□

### Következmény 2.10

$$\text{NPSpace} = \text{PSPACE}$$

**Proof:** Polinom négyzete polinom.

□

## 2.2 PSPACE teljesség

### Definíció 2.11

### PSPACE teljesség

Azt mondjuk, hogy  $L$  PSPACE teljes, ha  $L \in \text{PSPACE}$  és  $\forall L' \in \text{PSPACE}$  nyelvre  $L' \leq L$ . Tehát  $L'$  visszavezethető  $L$ -re polinomiális időben.

### Definíció 2.12

### tqbf – Totally Quantified Boolean Formula

Azt mondjuk, hogy  $\varphi$  egy teljesen kvantifikált Boole-formula, ha olyan alaba írható, hogy

$$\varphi = Q_1 x_1 Q_2 x_2 \dots Q_l x_l f(x_1, x_2, \dots, x_l),$$

ahol  $Q_i \in \{\forall, \exists\}$  és  $x_i$  Boole változók és  $f(x_1, \dots, x_l)$  egy konjunktív normál formula (CNF).

### Példa

$$\varphi = \forall x \exists y \exists z ((x \vee z) \wedge y)$$

Ez a formula igaz.

### Megjegyzés

Egy tqbf vagy igaz vagy hamis. Nem olyan mint egy CNF ahol az a kérdés hogy van-e helyes behelyettesítése, hanem magát a kvantálás megválaszolja, hogy a formula igaz vagy hamis.

### Definíció 2.13

### TQBF – True Quantified Boolean Formula

$$\text{TQBF} := \{\varphi, \text{ ahol } \varphi \text{ egy tqbf és } \varphi = \text{true}\}.$$

Azaz TQBF az igaz teljesen kvantifikált Boole formulák nyelve.

### Tétel 2.14

A TQBF nyelv PSPACE teljes.

**Proof:**

1. TQBF  $\in$  PSPACE

Végezzünk teljes indukciót a kvantorok számára. Ha  $(n - 1)$  kvantoros tqbf ellenőrzését el tudjuk végezni  $\text{poly}(n)$  tárban, akkor  $n$  kvantoros tqbf ellenőrzésénél csak 1-el több bitet kell tárolnom a kvantor típusára és meg  $x_n$  értékét.

## 2. $\forall L \in \text{PSPACE} : L \propto \text{TQBF}$

Röviden megemlítjük, hogy ebben az esetben nem tudjuk azt a trükköt eljátszani amivel bizonyítottuk, hogy  $\text{SAT} \in \text{NPC}$ , mert a Turing-gép összes szabályos lépését leíró formula hossza már bőven nem polinomiális lesz. Ez a trükk azért működött a SAT feladatnál, mert ott polinomiális időben kellett ellenőriznünk, itt viszont a tárnak kell polinomiálisnak lennie.

Az ötlet, hogy újra felhasználjuk az st-conn feladatot. Ha fel tudjuk írni az st-conn feladatot mint egy polinomiálisan méretű tqbf a kezdő csúcsra és az elfogadó csúcsok reprezentására a konfiguráció gráfra, akkor készen lennénk. Mivel bármilyen polinomiális tárban felismerhető nyelvet át tudunk írni polinomiális időben egy polinomiálisan hosszú tqnf-re.

Nézzük mit ad a köztes csúcs trükk amit már használtunk a Savitch tétel bizonyításában:

$$\text{st-conn}(k, s, t) \Leftrightarrow \exists u \in V : \text{st-conn}(k/2, s, u) \wedge \text{st-conn}(k/2, u, t).$$

A probléma ezzel a felírással, hogy bár feleztük a  $k$  paramétert, de a formula hossza nő, tehát összességében nem értünk el érdembeli javulást.

A trükk az, hogy kihasználjuk az univerzális kvantort ( $\forall$ ), hogy ne kelljen dupláznunk a formula méretét:

$$\text{st-conn}(k, s, t) \Leftrightarrow \exists u \in V \forall (x, y) \in \{(s, u), (u, t)\} : \text{st-conn}(k/2, x, y).$$

Ha az  $L$  nyelvet  $t$  tárban felismerte egy Turing-gép, akkor legfeljebb  $2^{c \cdot t}$  konfigurációja van. Tehát a konfigurációs gráfnak legfeljebb  $2^{c \cdot t}$  csúcsa van. Mivel a jobboldali formula mérete polinomiális és  $k$  értékét mindig felezzük, ezért a végső formula mérete polinomiális lesz.

□

### Definíció 2.15

### Generalized Geography játék

Legyen  $(G, u)$  egy rendezett pár, ahol  $G$  egy irányított gráf és  $u \in V(G)$  a gráf egy adott csúcsa. A játékot Alíz és Bob játssza a következő szabályok alapján:

- Alíz kezd az  $u$  csúcsból.
- Alíz és Bob felváltva lépnek.
- A jelenlegi csúcsból csak belőle kifelé menő élrel keresztül szabad lépni a következő csúcsba.
- Már látogatott csúcsba tilos lépni.
- Ha a soron következő játékosnak már nincs szabályos lépése, akkor az ellenfél nyer.

### Megjegyzés

Ez a játék az általánosítása az ország-város játéknak, ahol felváltva sorolunk városokat azzal a megkötéssel, hogy a következő város azzal a betűvel kezdődhet amivel az előző végződött és az veszít aki már nem tud várost mondani.

### Definíció 2.16

### Generalized Geography osztály

$$\text{GG} = \{(G, u) : \text{Alíznek van nyerő stratégiája } u\text{-ból indulva}\}.$$

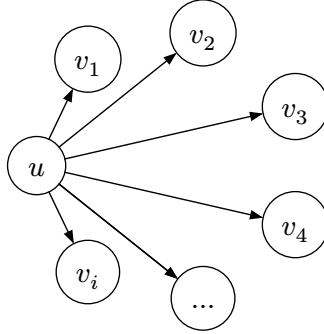
### Tétel 2.17

A GG nyelv PSPACE teljes.

**Proof:**

#### 1. $GG \in PSPACE$

Végezzünk teljes indukciót a leghosszabb út hosszára. Ha polinomiális térben el tudjuk dönteni, hogy Bob-nak nincsen stratégiája legfeljebb  $(n - 1)$  hosszú útra, akkor tudjuk, hogy Alíz-nak van nyerő stratégiája.



Nézzük meg  $u$ -nak az összes ki-szomszédokra, hogy Bob-nak nincs nyerő stratégiája. Mivel minden szomszédra polinomiális térben eldönthetjük, és a tárat újra tudjuk használni, ezért az egész feladatot el tudjuk dönteni polinomiális térben.

#### 2. $TQBF \propto GG$

Tehát a bizonyítás ezen részén azt kell belátnunk, hogy ha kapunk egy teljesen kvantifikált Boole-formulát, akkor arra tudunk adni egy irányított gráfot, amiben pontosan akkor van nyerő stratégiája Alíz-nak, ha a tqnf igaz. Legyen például a tqnf a következő:

$$\varphi = Q_1 x_1 Q_2 x_2 \dots Q_l x_l f(x_1, x_2, \dots, x_l).$$

Az irányított gráfot két részből foglunk felépíteni: kvantifikált értékadások (bal), és ellenőrzés (jobb). Az értékadás részben mindegyik  $x_i$  változóra létrehozunk egy kétirányú elágazást, ahol a balra vezető út azt jelenti, hogy  $x_i$  igaz, míg a jobbra vezető út azt, hogy  $x_i$  hamis.

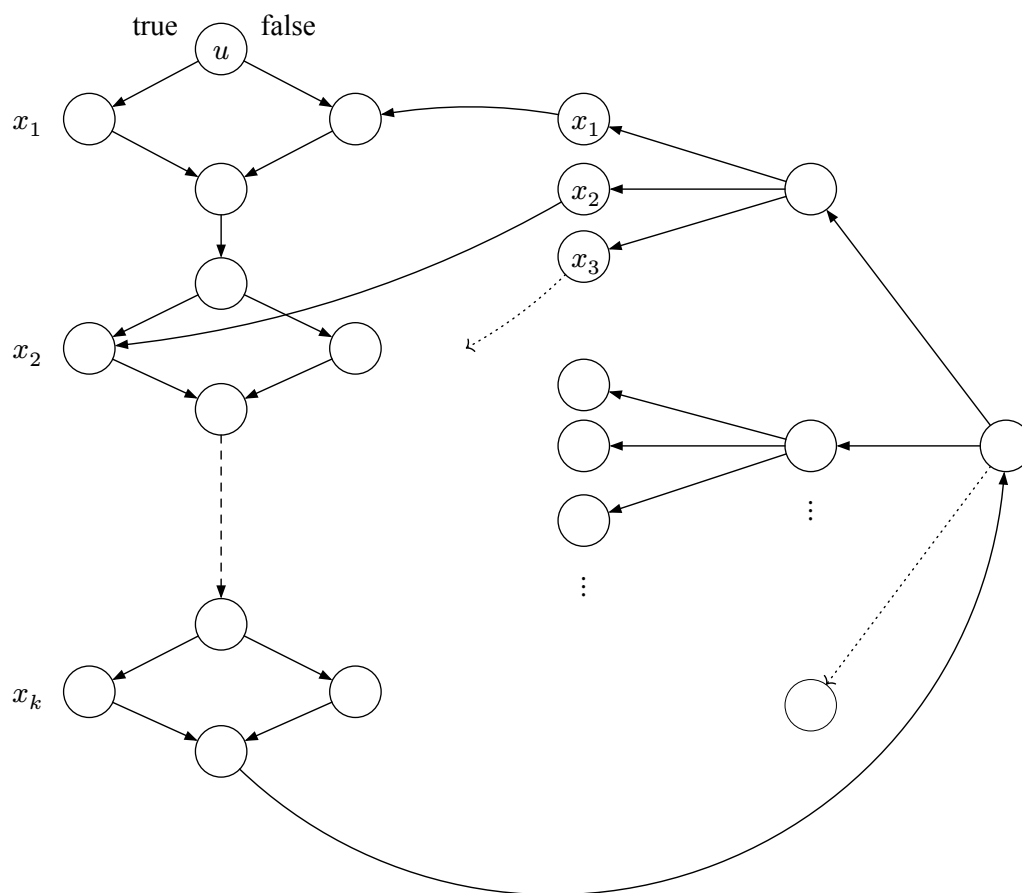
Az értékadásokat az alapján írjuk le, hogy éppen hogyan vannak kvantifikálva. Ha létezési kvantort ( $\exists$ ) látunk, akkor Alízt kényszerítjük lépésre, ha univerzális kvantort ( $\forall$ ), akkor Bobot kényszerítjük lépésre. Ha nem pontosan felváltva szerepelnek a kvantorok, akkor adunk az ellenfélnek egy triviális lépést ahol nincs választása csak előre menni.

Például, ha egymás után van  $\forall x_i$  és  $\forall x_{i+1}$ , akkor egymás után kéne lépni kettőt Bobnak, de ezt a szabályok nem engedik. Ezért azt csináljuk hogy Bob lép egyet, azután beszárnunk egy választás nélküli direkt élt a következő választási lehetőséghez, ezzel kényszerítve Alízt és visszaadva Bobnak a lépés lehetőségét.

A második részben, ahol ellenőrizzük a formulát, úgy írjuk fel a gráfot hogy a gyűjtő csúcsba lépést Bobra kényszerítjük, így Alíz jön soron. Alíz rámutat egy blokk-ra ahol ő tudja hogy minden változó hamis. Így Bob bármelyik változót választja a blokkból az hamis lesz. Azt hogy egy változó hamis úgy mutatjuk meg, hogy miután Bob kiválasztotta, adunk Alíz-nak egy ingyen lépést és utána bekötjük a gráf első felébe oda ahol választottuk  $x_i$  értékét. Ha  $x_i$  tagadása szerepel a blokkban akkor abba a csúcsba kötjük be ami azt reprezentálja, hogy  $x_i$  hamis, különbe abba ami azt hogy  $x_i$  igaz.

Mostmár könnyű meggondolni, hogy ebben az irányított gráfban az, hogy Alíznak van nyerő stratégiája az ekvivalens azzal, hogy a tqnf igaz. Mivel az hogy Alíznak van nyerő stratégiája pont azt jelenti hogy amikor Alíz nyer akkor létezik ( $\exists$ ) olyan lépés, hogy Bob bármit lép ( $\forall$ ) még úgy is Alíz fog nyerni.

A következő ábra talán jobban elmagyarázza az érvelést.



□