

11. Előadás

Előadó: Hajnal Péter

Jegyzetelő: Hajnal Péter

2011. április 26.

## 1. Mahaney-tétel bizonyítása

**Emlékeztető.** Mahaney-tétel feltevése  $SAT^* \prec S$ , ahol  $S \subset \Sigma^*$  egy ritka nyelv, azaz alkalmas  $t(x) \in \mathbb{N}[x]$  polinomra  $|S \cap \Sigma^n| \leq t(n)$  minden  $n \in \mathbb{N}$  esetén. Ezen feltevés alapján kell egy polinomiális algoritmust adnunk  $SAT$ -ra.

$SAT^*$ -hoz fel kell idéznünk egy rendezést a  $\{0, 1\}^{\leq n}$  halmazon:  $x, y \in \{0, 1\}^{\leq n}$  esetén  $x \prec y$ , ha  $x$  és  $y$  első eltérő bitje 0 az  $x$ -ben és 1 az  $y$ -ban vagy pedig  $y$  valódi kezdőszelete  $x$ -nek.

Azonos hosszú szavakra megszorítva ez éppen a lexikografikus rendezés.

**Bizonyítás.** Polinom időben megoldjuk a  $SAT$  problémát: Algoritmusunk futása alatt mindig lesz egy polinomiális hosszú  $L_i$  listánk  $\{0, 1\}^i \subset \{0, 1\}^{\leq n}$  elemeiből, azaz  $L_i$  elemeinek hossza mindig ugyanaz az  $i$  lesz (a futás során  $i$  egyesével fog nőni).

$L_0$  az  $\epsilon$  0-hosszú szóból áll.

$L_i = \{\ell_1, \dots, \ell_s\}$ -ből rekurzív módon írjuk fel  $L_{i+1}$ -et. Feltesszük, hogy a fenti indexelés a lexikografikus sorrendet, azaz  $\prec$ -et követi. A rekurzió több listán keresztül jut el a céljához.  $L_i^+$  tartalmazza  $L_i$  elemeinek összes kiterjesztését egy bittel:

$$L_i^+ = \{\ell_1 0, \ell_1 1, \dots, \ell_s 0, \ell_s 1\}$$

Azaz listánk teljes hossza  $2|L_i|$ . Feltesszük, úgy írtuk fel, hogy sorrendje a lexikografikus sorrend.

„Nem hagyhatjuk”, hogy ez a lista mindig megduplázódjon, exponenciálisan nagy legyen.  $L_i^+$  minden elemére végezzük el a Karp-redukciót. Könnyű látni, hogy listánk elején NEM  $S$ -beli elemet kell kapnunk. Egy ponton lesz egy váltás és után a redukció csupa  $S$ -beli elemet ad (ez a rész lehet üres is). Sajnos  $S$  „nehéz” nyelv a váltást „nem látjuk”. Először az azonos sorozatra redukálódott elemek közül csak az elsőt hagyjuk meg. Legyen  $L_i^{+-}$  az így kapott lista.

Ez a lista még lehet hosszú. Azonban azok a bitsorozatok, amik  $S$ -beli karakter-sorozatra redukálódnak már kevesen vannak:  $S$  maga ritka és maradék listánkon már különböző elemekre képez a redukció. A polinomiális redukciót legfeljebb  $n$  hosszú bitsorozatokra futtatjuk így a redukció által kiszámolt output hosszára polinomiális becslést adhatunk. Így az ilyen  $S$ -beli szavak száma legfeljebb  $\bar{q}(n)$ .

A következő lépésben ismét ritkítjuk listánka (most  $L_i^{+-}$ -t). A lexikografikus rendezésben utolsó  $\bar{q}(n)$  elemét hagyjuk csak meg. Az eredmény lesz  $L_{i+1}$ .

A rekurzióval  $L_n$ -et számoljuk ki. Eljárásunk során minden listánk legfeljebb  $2\bar{q}(n)$  hosszú, így az  $L_n$  lista előállításának időigénye polinomiális.

Végül  $L_n$  mindegyik elemére ellenőrizzük kielégíti-e  $\varphi$ -t. Ha bármelyik kielégítő értékadás, akkor elfogadjuk az inputot. Különben elvetjük. Ez a lépés időigénye is polinomiális ( $|L_n| \leq \bar{q}(n)$ ).

Csak az algoritmus helyességét kell ellenőrizni. Egyetlen módon tévedhet: Egy kielégíthető formula esetén  $L_n$  elemi közt nem lesz kielégítő értékadás. A következő állítás  $i = n$  esete ezt zárja ki és így bizonyítja a tételt.

**1. Lemma.** *Tegyük fel, ho  $\varphi$ -nek van kielégítő értékadása. Legyen a rendezésünkben az első ilyen értékadás,  $e$ , továbbá  $i$  hosszú kezdőszelete legyen  $e_i$ . Ekkor  $e_i$  az  $L_i$  listán lesz.*

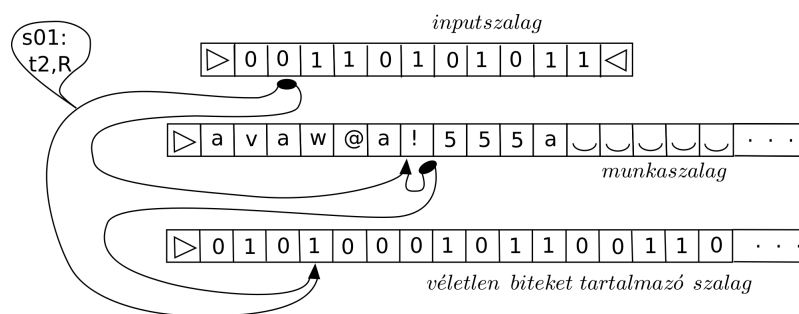
**Lemma bizonyítása.**  $i = 0$  esetén nyilvánvaló az állítás.

Tegyük fel, hogy  $e_i \in L_i$ . Ekkor nyilván  $e_{i+1} \in L_{i+1}$ . Az első ritkítást megelőző redukciókban  $e_{i+1}$  lesz az első elem, ami  $S$ -beli elemre képződik, azaz megmarad.

A második ritkítást úgyválasztottuk, hogy biztos megmaradjon  $L_i^{+-}$  összes olyan eleme, ami  $S$ -beli elemre redukálódik (ezek a listánk hátulsó részében legfeljebb  $\bar{q}(n)$  elem). Így  $e_{i+1}$  ismét megmarad. Kaptuk, hogy  $e_{i+1} \in L_{i+1}$ , ahogy bizonyítani kellett. ■

## 2. Véletlen számokat használó/valószínűségszámítási Turing-gépek

**Definíció.** Egy  $T$  Turing-gépet *véletlen számokat használó* (röviden véletlen) Turing-gépnek nevezünk (eldöntési feladatok esetén), ha az input- és munkaszalag mellett van egy harmadik szalag, egy úgy nevezett *véletlenszalag*, amely véletlen számok egy sorozatát tartalmazza, és az szalaghoz tartozó fej egyetlen műveletre képes: jobbra lépni és olvasni az elé kerülő mezőt. (Általában a véletlenszalag ábécéje  $\Sigma_v = \{0, 1\}$  (ez nem szükségszerű), továbbá a szalag bitjei uniform eloszlásúak.) Az ilyen  $T$  futása az  $\omega \in \Sigma_{input}^n$  inputszalag-tartalomból és  $\rho$  véletlenszalag-tartalomból egyértelműen (determinisztikusan) meghatározható (a kiszámolt értéket/leálló állapotot jelöljük  $T(\omega, \rho)$ -val).



1. ábra.

**Megjegyzés.** Ha csak  $\omega$ -t rögzítjük, akkor a futás már szereteágazó lesz (függ a véletlen biteket tartalmazó szalag tartalmától). A fa, amely a futás lehetőségeit leírja hasonlít a nem-determinizmus esetén látott képhez. Ott a futást egy „zseniális elme” irányította, most a véletlen mozgatja. Adott input esetén a futásra úgy gondolhatunk, mint a „Galton-deszkán” lefutó golyó utjára.

Akár a nem-determinizmusnál most is gondot kell fordítanunk az elfogadás/elvetés definiációjára. Erre több lehetőségünk is van. Mi csak polinomiális időkorlát mellett definiálunk két lehetőséget.

**Definíció.** Egy  $L$  nyelvre  $L \in \mathcal{BPP}$  pontosan akkor, ha létezik polinom idejű véletlen  $T$  Turing-gép, amelyre teljesül a következő két feltétel:

$$(BP_1) \quad \omega \in L \text{ esetén } \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 2/3,$$

$$(BP_2) \quad \omega \notin L \text{ esetén } \mathbb{P}_\rho(T(\omega, \rho) = \text{ELVET}) \geq 2/3.$$

**Megjegyzés.** 1. Tehát annak az esélye, hogy  $T$  jó értéken áll le,  $2/3$  minden  $\omega$ -ra. Egyszerűen megfogalmazva, ha  $L \in \mathcal{BPP}$ , akkor ELFOGAD = „VALÓSZÍNŰLEG-JÓ”, ELVET = „VALÓSZÍNŰLEG-ROSSZ”.

2. A  $\mathcal{BPP}$  nyelvosztály elnevezésében  $\mathcal{B}$  a „bounded error” szóra, a két  $\mathcal{P}$  pedig a „probabilistic” illetve „polynomial” szavakra utal.

**Definíció.** Egy  $L$  nyelvre  $L \in \mathcal{RP}$  pontosan akkor, ha létezik polinom idejű  $T$  Turing-gép, amelyre teljesül a következő két feltétel:

$$(R_1) \quad \omega \in L \text{ esetén } \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 1/2,$$

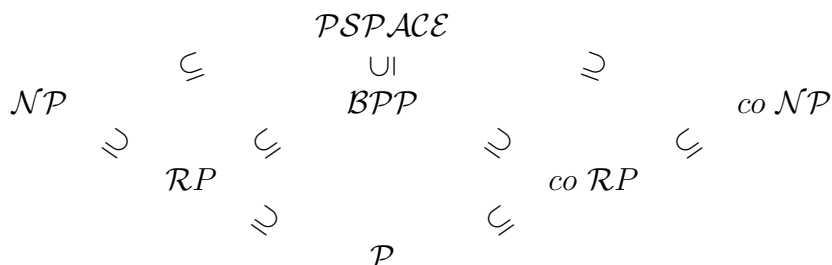
$$(R_2) \quad \omega \notin L \text{ esetén } \mathbb{P}_\rho(T(\omega, \rho) = \text{ELVET}) = 1.$$

**Megjegyzés.** 1. Vagyis ha  $L \in \mathcal{RP}$ , akkor ha  $T(\omega, \rho)$  ELFOGAD, akkor  $\omega \in L$  biztosan teljesül. Így elég ELVET = „VALÓSZÍNŰLEG-ROSSZ” átírást elvégezni, hogy a leálló állapotok kifejezzék az  $\mathcal{RP}$  gépek filozófiáját.

2. A nyelvosztály nevében  $\mathcal{R}$  a „random” szóból származik.

**Megjegyzés.** A  $\mathcal{BPP}$  nyelvosztály definíciójában az elfogadás/elvetés között szimmetria volt. Azt mondhatjuk, hogy  $co \mathcal{BPP} = \mathcal{BPP}$ . Ez nem igaz  $\mathcal{RP}$  esetén. Így természetesen bevezethető a  $co \mathcal{RP}$  nyelvosztály. A részletek kidolgozása nem okozhat problémát a halgató számára.

A következő diagram a bevezetett és néhány ismerős osztály viszonyát foglalja össze.



Már a  $\mathcal{RP}$  osztály definíciójából könnyen látszik, hogy  $\mathcal{P} \subset \mathcal{RP} \subset \mathcal{NP}$  illetve  $\mathcal{P} \subset co \mathcal{RP} \subset co \mathcal{NP}$ . Az első tartalmazási lánc az alábbi megfigyelések eredménye:

Ha az  $(R_1)$ -ben szereplő esemény valószínűségéről azt kötjük ki, hogy pontosan 1 (így  $(R_1)$  és  $(R_2)$  is teljesül) akkor  $\mathcal{P}$  definícióját kapjuk (a véletlenszalag olvasása helyett mindig 0 értéket képzelve). Ha pedig az  $(R_1)$ -ben szereplő esemény valószínűségéről azt kötjük ki, hogy 0-nál szigorúan nagyobb, akkor  $\mathcal{NP}$  definícióját kapjuk

(a véletlenszalagot tanúszalagként elképzelve). A másik tartalmazási lánc pedig a komplementálás/negálás tulajdonságából következik. A  $\mathcal{BPP}$  osztály beillesztése a következő tétel után nyilvánvaló.

Az alábbi tétel alapvető jelentőségű.

**2. Tétel.**  $\mathcal{RP}$  és  $\mathcal{BPP}$  is robusztus a hibázás valószínűségének korlátozását tekintve a következő értelemben:

(i)  $\mathcal{RP}$  definíciója nem változik, ha  $(R_1)$ -et  $(R_1^-)$ -szal vagy  $(R_1^+)$ -szal helyettesítjük, ahol ezek rendre

$$(R_1^-): \omega \in L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 1/p(|\omega|),$$

$$(R_1^+): \omega \in L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 1 - 1/2^{p(|\omega|)},$$

ahol  $p \in \mathbb{N}[x]$  tetszőleges (minden egész helyen pozitív) polinom.

(ii)  $\mathcal{BPP}$  definíciója nem változik, ha  $(BP_k)$ -t  $(BP_k^-)$ -szal vagy  $(BP_k^+)$ -szal helyettesítjük ( $k \in \{1, 2\}$ ), ahol ezek rendre

$$(BP_1^-): \omega \in L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 1/2 + 1/p(|\omega|),$$

$$(BP_2^-): \omega \in L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 1/2 + 1/p(|\omega|),$$

$$(BP_1^+): \omega \notin L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELVET}) \geq 1 - 1/2^{p(|\omega|)},$$

$$(BP_2^+): \omega \notin L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELVET}) \geq 1 - 1/2^{p(|\omega|)}.$$

ahol  $p$  hasonló az előző pontban szereplőhöz.

**Bizonyítás.** (i) legyen  $T$   $\mathcal{P}$  idejű  $L$ -t eldöntő véletlen Turing-gép. A hibázás valószínűségét vizsgáljuk. Legyen  $\omega \in L$  úgy, hogy  $|\omega| = n$ . A hibázás csak  $\omega \in L$  esetén lehetséges. Tegyük fel, hogy egy  $T$  polinomiális algoritmus esetén  $(R_2)$  mellett teljesül, hogy

$$\omega \in L \implies \mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq \kappa.$$

Konstruáljuk meg a  $\tilde{T}$  Turing-gépet úgy, hogy  $T$  futását ismétlje meg  $r$ -szer (mindegyik futásnál a véletlen bitek szalagjának újabb blokkját használva). Ezek a futások független eredményt adnak, mert a véletlenszalag egy-egy futásnál felhasznált bitsorozatai is függetlenek. Egy  $\omega$  inputra  $\tilde{T}$  futása ELFOGAD-dal ér véget, ha valamelyik futás elfogadó.

Könnyen látszik, hogy  $\tilde{T}$  polinomiális idejű, ha  $r$  polinomiális  $|\omega|$ -ban, továbbá teljesül hogy  $\mathbb{P}(\tilde{T} \text{ hibázik}) = (\mathbb{P}(T \text{ hibázik}))^r \geq \kappa^r$ .

Tegyük fel, hogy  $T$  teljesítette  $(R_1^-)$  feltevést.

- Ha az  $r = 1/\kappa = 10p(|\omega|)$ -t választással élünk, akkor következik  $\tilde{T}$  elfogadja ugyanazt a nyelvet az  $(R_1)$  feltétel mellett.
- Ha az  $r = 1/\kappa = 10p^2(|\omega|)$ -t választással élünk, akkor következik  $\tilde{T}$  elfogadja ugyanazt a nyelvet az  $(R_1^+)$  feltétel mellett.

Ebből adódik a bizonyítandó.

(ii) Hasonlóan dolgozunk az (i) ponthoz. Legyen  $T$  egy  $L$  nyelvet  $\mathcal{BPP}$  módon eldöntő Turing-gép, amely legalább  $1/2 + \kappa$  valószínűséggel a korrekt választ adja.  $\tilde{T}$  pedig az a Turing-gép, amit  $T$   $r$ -szeri (most  $r$  páratlan szám) ismételt futtatásával

kapunk úgy, hogy  $\tilde{T}$  eredménye az  $r$  eredményből adódik „többségi szavazással”, vagyis az dönt, hogy ELFOGAD vagy ELVETetés futás volt több.  $r$ -et az input méret polinomjának választhatjuk.

Minden futtatáshoz tartozzon egy 0-1 értékű  $X_i$  valószínűségi változó: 1 érték az ELFOGADÁS-nak felel meg, a 0 érték az ELVETÉS-nek.

$\omega \in L$  esetén  $\mathbb{E}[X_i] \geq 1/2 + \kappa$ . A hibázás eseménye, hogy  $S_r < r/2$ , amit felülről becsül, hogy  $|S_r - r\mathbb{E}[X]| > r\kappa$ .

$\omega \notin L$  esetén  $\mathbb{E}[X_i] \leq 1/2 - \kappa$ , A hibázás eseménye, hogy  $S_r > r/2$ , amit felülről becsül, hogy  $|S_r - r\mathbb{E}[X]| > r\kappa$ .

A bizonyítás befejezéséhez egy valószínűségszámítási tételt idézünk fel (bizonyítása nélkül).

**3. Tétel.** (Chernoff-becslés) Legyenek  $\{X_i\}_{i=1}^r$  független, azonos eloszlású, 0-1 értékű valószínűségi változók ( $\mathbb{P}[X_i = 1] = p$  és így  $\mathbb{P}[X_i = 0] = 1 - p$ ). Legyen  $S_r = X_1 + X_2 + \dots + X_r$  (így  $\mathbb{E}S_r = rp$ ). Ekkor

$$\mathbb{P}[|S_r - rp| \geq \Delta] \leq 2e^{-2\Delta^2/r}.$$

Ebből a bizonyítás vége egyszerűen adódik:

- Ha  $\kappa$  értéke  $\text{BP}_1^-$  szerint adott, akkor  $r$  választásával elérhetjük, hogy  $-\kappa^2 \cdot r < -1/10$  legyen. Azaz  $\tilde{T}$   $\text{BP}_1$  szerint hibázzon.
- Ha  $\kappa$  értéke  $\text{BP}_1$  szerint adott, akkor  $r$  választásával elérhetjük, hogy  $-\kappa^2 \cdot r < -10p(|\omega|)$  legyen. Azaz  $\tilde{T}$   $\text{BP}_1^+$  szerint hibázzon.

$\omega \notin L$  esetén teljesen hasonlóan dolgozhatunk. ■