ALGORITMUSOK ÉS BONYOLULTSÁGELMÉLET

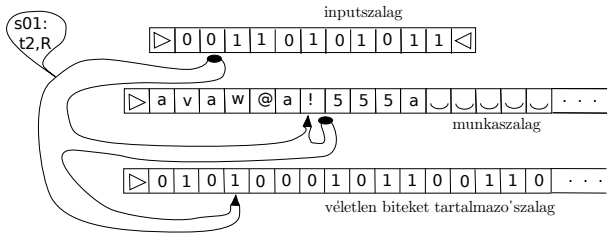
Matematika MSc hallgatók számára

10. Előadás

Előadó: Hajnal Péter
Jegyzetelő: Udvari Balázs 2010. április 19.

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 ún. *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) és a szalag bitjei uniform eloszlásúak.) Az ilyen T futása az $\omega \in \Sigma^n_{input}$ inputszalag-tartalomból és ρ véletlenszalag-tartalomból egyértelműen (determinisztikusan) meghatározható (a kiszámolt értéket/leálló állapotot jeloljük $T(\omega,\rho)$-val).



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$_1$) $\omega \in L$ esetén $\mathbb{P}_\rho\big(T(\omega,\rho) = \text{ ELFOGAD}\big) \geq 2/3$,

(BP$_2$) $\omega \notin L$ esetén $\mathbb{P}_\rho\big(T(\omega,\rho) = \text{ ELVET}\big) \geq 2/3$.

Megjegyzés.

1. Tehát annak az esélye, hogy T jó értéken áll le, $2/3$ minden ω-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 „polinomial” 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:

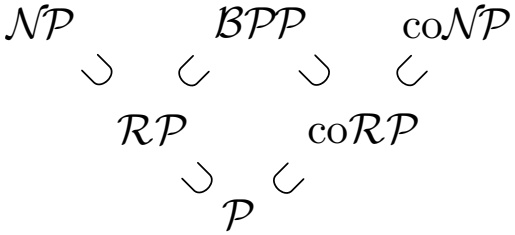
(R$_1$) $\omega \in L$ esetén $\mathbb{P}_\rho\big(T(\omega,\rho) = \text{ ELFOGAD}\big) \geq 1/2$,

(R$_2$) $\omega \notin L$ esetén $\mathbb{P}_\rho\big(T(\omega,\rho) = \text{ ELVET}\big) = 1$.

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.

A következő diagram a bevezetett és néhány ismerős osztály viszonyát fogalalja 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 valószínűségről 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.

1. Tétel. *$\mathcal{RP}$ és $\mathcal{BPP}$ is robosztus 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

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

ahol $p \in \mathbb{N}[x]$ tetszőleges megfelelő (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

$$(BP_1^-)\text{: } \omega \in L \Longrightarrow \mathbb{P}_\rho\big(T(\omega,\rho) = ELFOGAD\big) \geq 1/2 + 1/p(|\omega|),$$
$$(BP_2^-)\text{: } \omega \in L \Longrightarrow \mathbb{P}_\rho\big(T(\omega,\rho) = ELFOGAD\big) \geq 1/2 + 1/p(|\omega|),$$
$$(BP_1^+)\text{: } \omega \notin L \Longrightarrow \mathbb{P}_\rho\big(T(\omega,\rho) = ELVET\big) \geq 1 - 1/2^{p(|\omega|)},$$
$$(BP_2^+)\text{: } \omega \notin L \Longrightarrow \mathbb{P}_\rho\big(T(\omega,\rho) = ELVET\big) \geq 1 - 1/2^{p(|\omega|)}.$$

ahol p hasonló az előző pontban szereplőhöz.

A bizonyítás előtt megemlítünk egy valószínűségszámítási tételt

2. 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 $S_r = X_1 + X_2 + \ldots + X_r$ (így $\mathbb{E}S_r = rp$). Ekkor*

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

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 valószínűsége az eredeti (R_1)-et tartalmazó definíció szerint $\frac{1}{2}$, ha (R_1^-)-t használjuk, akkor $1 - \frac{1}{p(n)}$ és (R_1^+)-t használva $\frac{1}{2^{p(n)}}$.

Konstruáljuk meg a $\widetilde{T}$ Turing-gépet úgy, hogy T futását ismételje meg r-szer. (Ezek a futások független eredményt adnak, mert a véletlenszalag egy-egy futásnál felhasznált bitsorozatai is függetlenek.) Egy ω inputra $\widetilde{T}$ futása ELFOGAD-dal ér véget, ha valamelyik futás elfogadó.

Könnyen látszik, hogy $\widetilde{T}$ polinomiális idejű, ha r polinomiális $|\omega|$-ban, továbbá teljesül hogy $\mathbb{P}(\widetilde{T}\text{ hibázik}) = \big(\mathbb{P}(T\text{ hibázik})\big)^r$. Ha r-t $n = |\omega|$ polinomjának választjuk, akkor (R_1) feltevéséből T-re következik (R_1^+) $\widetilde{T}$-re. Hasonlóan, ha (R_1^-)-et tesszük fel T-re, akkor R_1-et $\widetilde{T}$-re.

(ii) Hasonlóan dolgozunk az *(i)* ponthoz. Legyen T egy L nyelvet $\mathcal{BPP}$ módon eldöntő Turing-gép, $\widetilde{T}$ pedig az a Turing-gép, amit T r-szeri (most r páratlan szám) ismételt futtatásával kapunk úgy, hogy $\widetilde{T}$ eredménye az r eredményből adódik „többségi szavazással", vagyis az dönt, hogy ELFOGAD vagy ELVET 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 $\mathbb{E}[X_i] \geq 1/2 + h$, ahol h attól függ, hogy BP_1, BP_1^+, BP_1^- feltételek melyikével dolgozunk. A hibázás eseménye, hogy $S_r < r/2$, amit felülről becsül, hogy $|S_r - r\mathbb{E}[X]| > hr$. A Chernoff-becslés szerint ez kisebb mint $2e^{-h^2 \cdot r}$.

- Ha h értéke BP_1^- szerint adott, akkor r választásával elérhetjük, hogy $-h^2 \cdot r < -1/10$ legyen. Azaz $\widetilde{T}$ BP_1 szerint hibázzon.
- Ha h értéke BP_1 szerint adott, akkor r választásával elérhetjük, hogy $-h^2 \cdot r < -10p(|\omega|)$ legyen. Azaz $\widetilde{T}$ BP_1^+ szerint hibázzon.

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

$\mathcal{BPP}$ helye korábbi osztályaink között

A címmel kapcsolatban két tételt említünk meg,

3. Tétel (Adlemann).

$$\mathcal{BPP} \subseteq \mathcal{P}^{\textit{nem-uniform}}.$$

Bizonyítás. Legyen $L \in \mathcal{BPP}$. Ekkor az előző tételt használva létezik T polinom idejű véletlen Turing-gép, aminek minden ω inputra a hibázás valószínűsége legfeljebb $\frac{1}{2^{\alpha n}}$.

Tehát létezik olyan ρ véletlenszalag-tartalom, hogy az ezzel végrehajtott futás nem hibázik semelyik ω-ra sem hibázik: jelölje ugyanis R_ω az $\{\rho : T$ hibázik ω-n ρ-val$\}$. Ekkor $\mathbb{P}\big(\cup R_\omega\big) \leq |\Sigma^n| \frac{1}{2^{\alpha n}} < 1$, vagyis az előző megállapítás valóban igaz.

Tekintsük T-t. A számolása folyamatát egy polinom méretű hálózattal szimulálhatjuk, amelynek az inputbitjei ω és ρ kódja.

A fenti univerzálisan jó ρ-t bitjeit lerögzítve/behuzalozva egy hálózatot kapunk, ami csak ω kódjaiból kiszámolja az L-hez tartozást kódoló bitet (a hálózatméret nem változik a huzalozástól, azaz polinomiális). Az ω, ρ-t olvasó hálózat uniform módon konstruálható, az uniformitást a ρ nemkonstruktív mivoltja rontja el. ■

4. Tétel (Gács Péter-Sipser).

$$\mathcal{BPP} \subseteq \Sigma_2\mathcal{P} \cap \Pi_2\mathcal{P}.$$

Bizonyítás. (Lautemann) Mivel $\Pi_2\mathcal{P} = co\Sigma_2\mathcal{P}$, elég megmutatni, hogy $\mathcal{BPP} \subseteq \Sigma_2\mathcal{P}$.

Legyen $\Sigma = \mathbb{Z}_{|\Sigma|} = \{0, 1, \ldots, |\Sigma| - 1\}$ additív mod $|\Sigma|$-aritmetikával.

Definiáljuk a következő fogalmakat: $S \subseteq \Sigma^N$ halmaz akkor és csak akkor *sűrű*, ha $|S| \geq 1 - \frac{1}{N}|\Sigma^N|$, továbbá egy $R \subseteq \Sigma^N$ halmaz akkor és csak akkor *ritka*, ha $|R| < \frac{1}{N}|\Sigma^N|$, azaz $\overline{R}$ sűrű.

Először igazoljuk az alábbi lemmát.

5. Lemma. *(i) Ha R ritka, akkor minden $c_1, \ldots, c_N \in \Sigma^N$-re $\cup_{i=1}^N (c_i + R) \subsetneq \Sigma^N$,*

(ii) Ha S sűrű, akkor létezik olyan $c_1, \ldots, c_N \in \Sigma^N$, hogy $\cup_{i=1}^N (c_i + S) = \Sigma^N$.

A lemma bizonyítása. Az első állítás triviális, hiszen $\cup_{i=1}^N (c_i + R)$-ben kevesebb, mint $N\frac{1}{N}|\Sigma^N| = |\Sigma^N|$ elem van R ritkasága miatt.

A második rész bizonyításához valószínűségszámítási módszert használunk.

Elég belátni, hogy

$$\mathbb{P}\big(r_1, \ldots, r_N \in \Sigma^N : \cup(r_i + S) = \Sigma^N\big) > 0$$

ahol $r_1, \ldots, r_N$ független, uniform eloszlású elemek/vektorok (hiszen $Sigma^N$ egy vektortér). Az eseményt átírva a bizonyítandó

$$\mathbb{P}\Big(\bigwedge_{x \in \Sigma^N} (r_1, \ldots, r_N \in \Sigma^N : \exists i : x \in r_i + S) > 0$$

Az $x \in r_i + S$ feltétel ekvivalens $r_i \in x - S$-sel. $x - S$ elemszáma egyenlő $|S|$-sel, amit becsülhetünk $|S| \geq (1 - \frac{1}{N})|\Sigma^N|$ módon.

Jelölje a fenti és-sel összekapcsolt eseményeket E_x. Ekkor $\mathbb{P}(\overline{E_x}) \leq \frac{1}{N^N}$, így $\mathbb{P}(\overline{\wedge E_x}) = \mathbb{P}(\vee \overline{E_x}) \leq |\Sigma^N|\frac{1}{N^N} < 1$, így a komplementer esemény valószínűsége valóban pozitív és ezzel a lemmát beláttuk.

Most visszatérhetünk a tétel bizonyításához. Legyen T egy $L \in \mathcal{BPP}$-t bizonyító Turing-gép, aminek a hibázási valószínűsége kevesebb, mint $\frac{1}{2^n}$. Legyen $t(n) \in \mathbb{N}$ a futásnak egy polinomiális időkorlátja.

Legyen $S_\omega = \{\rho : T(\omega, \rho) = \text{ELFOGAD}\}$. Jelölje N a futás során elolvasott véletlen bitek számát, ez $t(n)$-nel felülről becsülhető. Vegyük észre, hogy ha $\omega \notin L$,

akkor a hibázás valószínűsége $\frac{|S_\omega|}{|\Sigma^N|} < \frac{1}{2^n} < \frac{1}{N}$, vagyis S_ω ritka. Hasonlóan, ha $\omega \in L$, akkor a nem hibázás valószínűsége $\frac{|S_\omega|}{|\Sigma^N|} > 1 - \frac{1}{2^n} > 1 - \frac{1}{N}$, vagyis S_ω sűrű.

Tehát $\omega \in L$ akkor és csak akkor teljesül, ha S_ω sűrű/nem ritka, ami a lemma alapján ekvivalens a következővel

$$\exists (c_1, \ldots, c_N) \in \Sigma^{N \times N}, \text{ hogy } \forall l \in \Sigma^N\text{-re } l - c_i \in \Sigma_\omega \text{ valamely } i\text{-re.}$$

Az, hogy $l - c_i \in \Sigma_\omega$, ellenőrizhető $\mathcal{P}$-ben. Már csak azt kell észrevenni, hogy az utóbbi bekezdés tartalma L egy $\Sigma_2\mathcal{P}$-beli nyelvként való jellemzése, így a bizonyítás teljes. ■