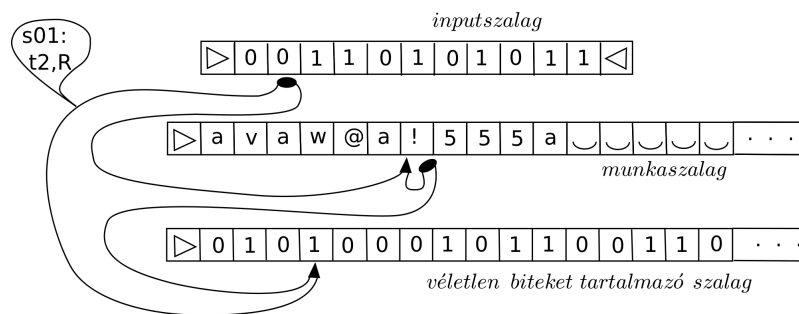


1. Véletlen számokat használó/valószínűségszámítási Turing-gépek

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 ρ véletlenszalag-tartalomból egyértelműen (determinisztikusan) meghatározható (a kiszámolt értéket/leálló állapotot jelöljük $T(\omega, \rho)$ -val).



1. ábra.

Megjegyzés. Ha csak ω -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 útjára.

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:

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

(BP₂) $\omega \notin L$ 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 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 „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:

(R₁) $\omega \in L$ esetén $\mathbb{P}_\rho(T(\omega, \rho) = \text{ELFOGAD}) \geq 1/2$,

(R₂) $\omega \notin L$ 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 $\text{co } \mathcal{BPP} = \mathcal{BPP}$. Ez nem igaz \mathcal{RP} esetén. Így természetesen bevezethető a $\text{co } \mathcal{RP}$ nyelvosztály. A részletek kidolgozása nem okozhat problémát a halgatónak 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 $\mathcal{P} \subset \text{co } \mathcal{RP} \subset \text{co } \mathcal{NP}$. Az első tartalmazási lánc az alábbi megfigyelések eredménye:

Ha az (R₁)-ben szereplő esemény valószínűségéről azt kötjük ki, hogy pontosan 1 (így (R₁) és (R₂) is teljesül) akkor \mathcal{P} definícióját kapjuk (a véletlenszalag olvasása helyett mindig 0 értéket képzelve). Ha pedig az (R₁)-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.

1. 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 ω 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 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 $\mathbb{E}[X_i] \geq 1/2 + \kappa$. 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 valószínűségi számítási tételt idézünk fel (bizonyítása nélkül).

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 $S_r = X_1 + X_2 + \dots + X_r$ (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 κ értéke BP_1^- szerint adott, akkor r (polinomiális) választásával elérhetjük, hogy $-\kappa^2 \cdot r < -1/10$ legyen. Azaz \tilde{T} BP_1 szerint hibázzon.
- Ha κ értéke BP_1 szerint adott, akkor r (polinomiális) választásával elérhetjük, hogy $-\kappa^2 \cdot r < -10p(|\omega|)$ legyen. Azaz \tilde{T} BP_1^+ szerint hibázzon.

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

2. Véletlen algoritmusok logaritmikus tárral

Az \mathcal{L} osztályt eddig jól körüljártuk. Egyik első megjegyzésünk az volt, ha egy L nyelvet eldöntünk logaritmikus tár felhasználásával, akkor algoritmusunk szükség-szerűen polinomiális.

A véletlen „komponens” minden probléma nélkül „hozzáadható” a logaritmikus tárhoz. Ekkor azonban a következő „jelenséget” tapasztaljuk. Az eddigi polinom idő (automatikus garancia) megszűnik.

Ezt a következő géppel világítjuk meg. A gép egy óra lesz. Szükségszerűen CSÖRÖG állapotban áll meg. Az inputból kiolvassuk n hosszát és a munkaszalagon egy $\log n$ hosszú számlálót jelölünk ki, 0 kezdőértékkel. Majd el kezdjük olvasni a véletlen szalagot. A látott 1-eseket számoljuk. Azaz, ha 1-est látunk, akkor a számlálót növeljük eggyel. Ha 0-t látunk, akkor a számlálót lenullázzuk. Ha a számláló betelik (csupa 1-es lesz a kijelölt területen), akkor a CSÖRÖG állapotba jutunk.

Azaz a gép akkor ráll le/CSÖRÖG állapotba jut, ha $2^{\log n} = n^{\mathcal{O}(1)}$ darab 1-est, egy blokkban egymás után „tapasztal” a véletlen szalagon. Nyilván „erre hosszú ideig kell várni”.

3. Lemma. A fenti gép logaritmikus tárat használ. A CSÖRÖG állapotba jutáshoz szükséges lépések számának várható értéke exponenciális.

Az analízis egyszerű/alap valószínűségi számítási eszközökkel adódik.

A fenti „óra” lehetőséget ad a véletlen bitekre alapuló hosszú idő kijelölésére. Ez néha „csalásnak” tekinthető.

Definíció. Legyen \mathcal{RL} azon nyelvek osztálya, amit véletlen biteket használó logaritmikus tárú géppel el tudunk dönteni.

Legyen $\mathcal{RL}^{\text{poly}}$ azon nyelvek osztálya, amit véletlen biteket használó logaritmikus tárú, polinomiális idejű géppel el tudunk dönteni.

★

Végül megemlítünk egy véletlen és logaritmikusan tárat használó algoritmust. A kérdés, amit megoldunk egy fontos probléma. A jól ismert \mathcal{NL} -teljes irányított elérhetőség irányítatlan változata:

Definíció. Az ELÉRHETŐSÉG a következő probléma:

Input: G gráf, $s, t \in V(G)$, Output: $\exists? st$ út G -ben.

Azaz ELÉRHETŐSÉG a következő nyelv:

$$\{(G, s, t) : \text{van } st \text{ út } G\text{-ben}\}$$

A probléma irányított változata is fontos:

Definíció. Amennyiben gráfunk irányított és irányított st út létezését teszteljük $\overrightarrow{\text{ELÉRHETŐSÉG}}$ problémáról/nyelvről beszélünk.

Nyilvánvaló, hogy ELÉRHETŐSÉG, $\overrightarrow{\text{ELÉRHETŐSÉG}}$ \mathcal{NL} -beli nyelv, azaz nem-determinisztikus logaritmikusan tárral megoldható. Tudjuk, hogy ELÉRHETŐSÉG, $\overrightarrow{\text{ELÉRHETŐSÉG}}$ $\mathcal{SPACE}(\log^2)$ -beli nyelv, azaz log-négyzet tárban determinisztikusan megoldható (Savitch-tétel). Ennél több $\overrightarrow{\text{ELÉRHETŐSÉG}}$ nyelvről nem is nagyon ismert. Minden előrelépés hatalmas áttörés lenne, hiszen a teljes \mathcal{NL} nyelvosztályról tudnánk meg valami lényegeset.

Az ELÉRHETŐSÉG esetén azonban további eredmények ismertek.

4. Tétel (Aleliunas–Karp–Lipton–Lovász–Rackoff, 1979). *Létezik olyan ELÉRHETŐSÉG-et kiszámító véletlen algoritmus, amely*

(i) *polinomiális és LOGSPACE-ben megvalósítható,*

(ii) $(G, s, t) \in \text{ELÉRHETŐSÉG}$ esetén $\mathbb{P}(\text{ELFOGAD eredmény } (G, s, t)\text{-n}) > \frac{1}{2}$.

Továbbá $(G, s, t) \notin \text{ELÉRHETŐSÉG}$ esetén $\mathbb{P}(\text{ELVET eredmény } (G, s, t)\text{-n}) = 0$.

A tételt az alábbi, viszonylag egyszerű algoritmus igazolja:

5. Algoritmus. *(Aleliunas–Karp–Lipton–Lovász–Rackoff)*

Véletlen sétát végzünk s -ből kiindulva $10 \cdot n^3$ lépésen keresztül.

Minden lépés után tetszeljük t elérését:

ha elérjük: BIZTOS-JÓ

ha nem érjük el: séta folytatása

Ha ELFOGAD állapot lérése nélkül ért véget a séta (letelik az időnk), akkor VALÓSZÍNŰLEG-ROSSZ állapottal állunk le.

Az algoritmus analízise sem nehéz, ha a Markov-láncok elméletének alapjait ismerjük. Az analízist elhagyjuk.

A tétel tömören összefoglalva $\text{ELÉRHETŐSÉG} \in \mathcal{RL}^{\text{poly}}$.

★ ★ ★

A véletlen szerepe kiküszöbölhető. Ez a „derandomizáció” egy hosszú kutatás (majd 30 évvel a véletlen algoritmus után) koronája. Csak megemlítjük a végső tételt.

6. Tétel (Reingold, 2008). $\text{ELÉRHETŐSÉG} \in \mathcal{L}$.