ALGORITMUSOK ÉS BONYOLULTSÁGELMÉLET

Matematika MSc hallgatók számára

12. Előadás

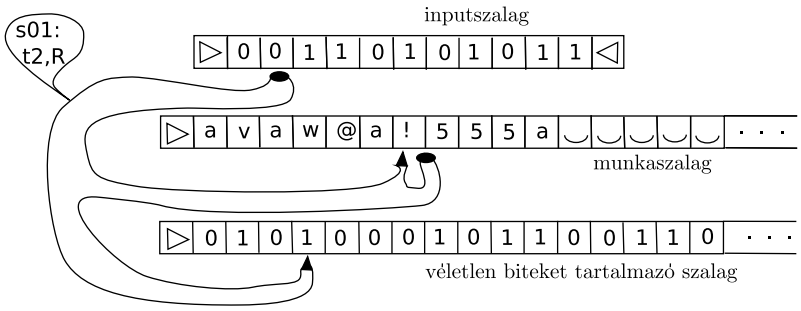
Előadó: Hajnal Péter
Jegyzetelő: Vass Mária

2012. Május 2.

1. Véletlen számokat használó Turing-gépek

A véletlen számokat használó Turing-gépek az input mellett véletlen számokat is használnak. Az ilyen gépeket (nyelvileg kissé helytelenül) szokták véletlen algoritmusoknak/TG-nek is nevezni.

Definíció. A T véletlen számokat használó Turing-gép annyiban különbözik az eldöntő Turing-géptől, hogy az input- és munkaszalag mellett adott egy harmadik szalag, az úgynevezett véletlenszalag, ami ρ „véletlen forrást" tárol. Érdemes feltennünk, hogy ezen a szalagon csak jobbra mozoghat a fej és csak olvashatja az épp aktuális mezőt, továbbá hogy a ρ_i karakterek (a ρ szalagtartalom i-edik karaktere) uniform, független eloszlásúak.



1. ábra.

Ez a Turing-gép modell hasonlít a nem-determinisztikus esethez. Ott is pluszban egy szalag van (neve a nemdeterminisztikus esetben tamúszalag). Az átmeneti függvény az ott látható módon definiálható/ Esetünkben is egy valószínúségszámítási T Turing-gép futása egy ω input és egy ρ véletlen karaktersorozat által meghatározott. Azaz a T-t leíró átmeneti függvény ismeretében

$$(\omega, \rho) \to \kappa_0(\omega, \rho), \kappa_1, \kappa_2, \ldots, \kappa_\ell \to T(\omega, \rho) \in \{ELFOGAD, ELVET\}$$

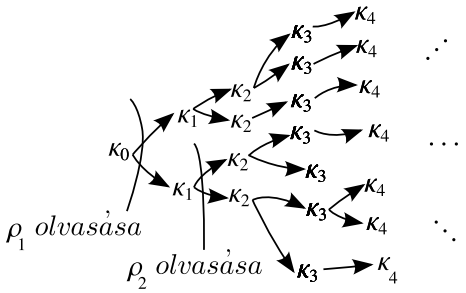
konfigurációsorozat definiálható. Ez a T gép egy futása.

Megjegyzés. A véletlen forrást tartalmazó szalag ábécéje tetszőleges lehet. Gyakori a $\{0, 1\}$ választás, de gondolhatunk nagyobb (persze véges) ábécére is. A $\{0, 1\}$ választás esetén a szalag karaktereire véletlen bitekként hivatkozunk.

A későbbiekben a véletlen TG-ek közül azok érdekelnek, ahol a futási idő korlátozott. Ebben az esetben adott inputnál (pontosabban adott inputméretnél) az

egyik irányban végtlen véletlen számokat tartalmazó szalag tartalmának csak korlátozott részét olvashatjuk el. Adott inputnál az időkorlát miatt el nem érhető véletlen karaktereket „el is felejthetjük”. Így a számítás mögött lévő valószínűségi mező nagyon egyszerű. Például $\Omega = \{0,1\}^{t(n)}$ az uniform eloszlással, azaz a legegyszerűbb kombinatorikus valószínűségi mező.

Ha csak az inputot, ω-t ismerjük, akkor a futás nem meghatározott. A lehetséges futások összessége egy gyökeres fában írható le:



2. ábra.

Egy input esetén a számítás a fa gyökérétől egy levélig vezető úton előforduló konfigurációkat jár be. Ez lesz az inputhoz tartozó számítási út. Ez egy valószínuségi változó, hasonlóan a Galton-deszka tetején bedobott golyó útjához.

A fenti modell leírása nem volt nehéz. DE mit jelent egy nyelv elfogadása/kiszámolása? Több lehetőség is van. Mi kettőt emelünk ki.

Definíció. Egy L nyelvre $L \in \mathcal{BPP}$ (Bounded Error Probabilistic Polinomial time) akkor és csak akkor, ha létezik T véletlen Turing-gép melyre:

i) T polinomidejű ω-ban,

ii) $\omega \in L$ esetén: $\mathbb{P}(T(\omega,\rho) = ELFOGAD) \geq 2/3$,

míg $\omega \notin L$ esetén: $\mathbb{P}(T(\omega,\rho) = ELVET) \geq 2/3$.

Megjegyzés. Az ii)-ben szereplő két feltételt együtt is megfogalmazhatjuk: annak az esélye, hogy T jó értéken áll le, legalább $2/3$ minden inputra. Vagyis a hibázás valószínűsége legfeljebb $1/3$.

A hibázás lehetősége miatt nyelvileg jobban kifejezők a VALÓSZÍNŰLEG-JÓ és VALÓSZÍNŰLEG-ROSSZ elnevezések a két leálló állapotra.

Definíció. Egy L nyelvre $L \in \mathcal{RP}$ akkor és csak akkor, ha létezik T véletlen Turing-gép melyre:

i) T polinomális ω-ban,

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

míg $\omega \notin L$ esetén: $\mathbb{P}(T(\omega,\rho) = ELVET) = 1$.

Megjegyzés. Azaz a hibázás csak az egyik irányban lehetséges. Ha a gépünk ELFOGAD állapottal áll le, akkor biztosan tudjuk, hogy $\omega \in L$. Más esetben 1 valószínűséggel el kellene vetnie T-nek (a kombinatorikus valószínűségi mezőnél ez a biztos esemény).

A két leálló állapot természetes elnevezése: BIZTOS-JÓ≡ELFOGAD és VALÓSZÍNŰLEG-ROSSZ.

A nemdeteminizmushoz hasonlóan az $\mathcal{RP}$ osztály definíciójában egy aszimetria van az elfogadás és elvetés között. Emiatt egy új osztály bevezetése természetes.

Definíció. Egy L nyelvre $L \in \text{co}\mathcal{RP}$ akkor és csak akkor, ha $\overline{L} = \Sigma^* - L \in \mathcal{RP}$.

Vagyis ekvivalens módon:

Definíció. Egy L nyelvre $L \in \text{co}\mathcal{RP}$ akkor és csak akkor, ha létezik T véletlen Turing-gép melyre:

i) T polinomális ω-ban,

ii) $\omega \in L$ esetén: $\mathbb{P}(T(\omega, \rho) = ELFOGAD) = 1$,

míg $\omega \notin L$ esetén: $\mathbb{P}(T(\omega, \rho) = ELVET) \geq 1/2$.

2. Hibajavítás

Ha $\mathcal{BPP}$ definíciójában i) és ii)-nél a 2/3-ot lecseréljük 1/2-re, akkor egy semmitmondó osztályt írnánk le. Minden nyelv beletartozna azzal a triviális algoritmussal, ami beolvassa az első véletlen bitet, és ha ott 1-et lát, akkor ELFOGAD állapottal befejeződne, 0-t látva pedig ELVET állapotba jutna (a véletlenszalagon a $\{0, 1\}$ ábécét feltételezve). Ha a 2/3-ot 1-re felvinnénk, akkor pedig a definíciónk a determinisztikus számolás írná le. Természetes, hogy a valódi definícióban szereplő 2/3 szám az $(1/2, 1)$ intervallumba esik. A konkrét választás azonban esetleges. Ezt írja le a következő két észrevétel.

Észrevétel. Ha $\mathcal{RP}$ definíciójában ii) első feltételénél az 1/2-et $1/p(|\omega|)$-re vagy $1 - 1/2^{p(|\omega|)}$-re cseréljük, akkor $\mathcal{RP}$ definíciója változatlan marad (ahol p polinom).

Ha $\mathcal{RP}$ definíciójában a módosított ii) első sora

$$\omega \in L \text{ esetén: } \mathbb{P}(T(\omega, \rho) = ELFOGAD) \geq 1/p(|\omega|),$$

akkor azt tesszük fel, hogy a hibázás ($\omega \in L$, de a számolás elveti ω-t) valószínűsége lgfeljebb $1 - 1/p(n)$. Az észrevétel a hibázás valószínűsége 1/2 alá vihető (erdeti definíció), sőt $1/2^{q(n)}$ alá vihető a polinom időkorlát megtartása mellett. Azaz az észrevétel egy hibajavító képessége a véletlen algoritmusoknak.

Az észrevétel igazolása, a hibajavító $\widetilde{T}$ algoritmus: Az erdeti T Turing-gépet r-szer ismételjük (új, azaz az előzőektől független véletlen bitek olvasásával), ha valamikor ELFOGAD állapottal történik a futás, akkor leállunk és $\widetilde{T}$ is ELFOGAD állapotú lesz. Azonban, ha mind az r alkalommal ELVET állapottal áll le az ismétlés,

akkor $\widetilde{T}$ is ELVET/VALÓSZÍNŰLEG-ROSSZ állapotú lesz. $\widetilde{T}$ hibázása akkor lehetséges, hogy ha ω input L-beli, azonban minden ismétlés ELVET állapothoz vezet. Azaz mind az r független ismétlés T-nek hibázó futása. Tehát $\omega \in L$ esetén

$$\mathbb{P}(\widetilde{T} \text{ hibázik } \omega\text{-n}) = (\mathbb{P}(T \text{ hibázik }))^r .$$

A leggyengébb feltevés esetén is — ha $\mathbb{P}(T \text{ hibázik }) \leq 1 - 1/p(n)$ — r-et polinomiálisnak kell választanunk ahhoz, hogy az eredeti hibázás r-edik hatványa kívánt méretű legyen.

Észrevétel. Ha $\mathcal{BPP}$ i) és ii)-ben a két 2/3-ot lecseréljük $1/2 + 1/p(|\omega|)$)-ra, vagy a 2/3-ot lecseréljük $1 - 1/2^{p(|\omega|)}$-ra, akkor (mindkét esetben) nem változtatunk a $\mathcal{BPP}$ osztályon.

Az észrevételt ismét megfogalmazhatjuk, mint hibajavítási lehetőséget: Azaz, ha azt követeljük meg, hogy $\omega \in L$ esetén: $\mathbb{P}(T(\omega, \rho) = ELFOGAD) \geq 1/2 + 1/p(|\omega|)$, míg $\omega \notin L$ esetén: $\mathbb{P}(T(\omega, \rho) = ELVET) \geq 1/2 + 1/p(|\omega|)$ — vagyis a hibázás valószínűsége legfeljebb $1/2 - 1/p(|\omega|)$—, akkor a hibázás exponenciálisan kicsivé tehető (a polinom idő megtartása mellett).

Az észrevétel indoklása: Legyen T egy L nyelvet relaxált $\mathcal{BPP}$ módon eldöntő Turing-gép. Azaz a hibázás valószínűsége akár $1/2 - 1/p(|\omega|)$ nagyságú is lehet. Legyen $\widetilde{T}$ az a Turing-gép, amely T-t r-szer (feltesszük, hogy r páratlan, azaz $r = 2s+1$) függetlenül (újabb és újabb véletlen bitek elolvasásával) futtatja. Így r darab eredményt kapunk ($\{ELFOGAD, ELVET\}^r$ egy eleme). Úgynevezett „többségi szavazás" mondja meg, hogy mi lesz $\widetilde{T}$ eredménye. (Azért jó, hogy páratlan sokszor futtatjuk T-t, mert így egyértelműen el tudjuk dönteni, hogy melyikből kimenetelből van több.)

Meg kell becsülnünk a

$$\mathbb{P}(\widetilde{T} \text{ téved } \omega\text{-n})$$

valószínűséget. Legyen ξ_i az a valószínűségi változó, ami az i-edik ismétlés tévedésénél 1, különben 0. $\xi_1, \xi_2, \ldots, \xi_r$ független azonos eloszlású valószínűségi változók.

$$\mathbb{E}\xi_i \leq 1/2 - 1/p(|\omega|) \stackrel{\text{jel}}{=} 1/2 - \epsilon.$$

A „$\widetilde{T}$ téved ω-n" esemény átfogalmazva: „$\xi_1 + \xi_2 + \ldots + \xi_r \geq s + 1$", azaz „$\xi_1 + \xi_2 + \ldots + \xi_r > r/2$". Azaz eseményünk része a következő eseménynek

$$\xi_1 + \xi_2 + \ldots + \xi_r - \mathbb{E}(\xi_1 + \xi_2 + \ldots + \xi_r) > \epsilon r.$$

Speciálisan

$$\mathbb{P}(\widetilde{T} \text{ téved } \omega\text{-n}) \leq \mathbb{P}(\xi_1 + \xi_2 + \ldots + \xi_r - \mathbb{E}(\xi_1 + \xi_2 + \ldots + \xi_r) > \epsilon r).$$

A felső becslésünk standard valószínűségszámítási eredményekkel becsülhető. Például a Chernoff-egyenlőtlenségből kapjuk, hogy

$$\mathbb{P}(\widetilde{T} \text{ téved } \omega\text{-n}) \leq \mathbb{P}(\xi_1 + \xi_2 + \ldots + \xi_r - \mathbb{E}(\xi_1 + \xi_2 + \ldots + \xi_r) > \epsilon r) \leq 2e^{-\epsilon^2 r/3}.$$

Ha $\epsilon = 1/p(|\omega|)$, akkor is r nagyságát polinomiálisnak kell választanunk ahhoz, hogy utóbbi becslésünk exponenciálisan kicsi legyen ($1/2^{q(n)}$).

3. Véletlen TG-ek osztályainak helye korábbi osztályaik között

Már az $\mathcal{RP}$ nyelvosztály definíciójából látszik a

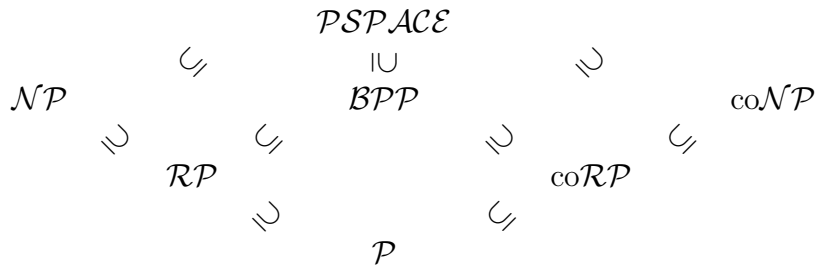
$$\mathcal{P} \subseteq \mathcal{RP} \subseteq \mathcal{NP}$$

tartalmazási lánc: Ha $\mathcal{RP}$ definíciójában, az ii) esetben kikötjük, hogy mindkét esemény valószínűsége pontosan 1, akkor $\mathcal{P}$ definíciójához jutunk, míg ha csak a 0-nál nagyobb voltát tesszük fel, akkor $\mathcal{NP}$-hez jutunk. A $\mathcal{P} \subseteq co\mathcal{RP} \subseteq co\mathcal{NP}$ lánc pedig a komplementálás/negálás tulajdonságából következik. A $\mathcal{BPP}$ nyelvosztály beillesztése az előbbi két észrevétel után nyilvánvaló.

Az előző bekezdés összes osztálya $\mathcal{PSPACE}$-ben van a következő észrevétel miatt:

Tegyük fel, hogy T egy tanú/véletlen szalagos Turing-gép $t(n)$ (polinomiális) időkorláttal. Feltehető, hogy az algoritmusunk plusz szalagjának ábécé-je $\{0,1\}$ és az algoritmus $t(n)$ bitet olvas el. A plusz szalag tartalmára $2^{t(n)}$ lehetőség van. Könnyű leírni egy $\widetilde{T}$ $\mathcal{PSPACE}$-beli gépet, amely megszámolhatja az összes olyan tartalmat, amely T elfogadó futásához vezet. Ezek után ha T egy $\mathcal{BBP}/\mathcal{NP}/\mathrm{co}\mathcal{NP}$-beli nyelvséget igazol, akkor $\widetilde{T}$ módosítható úgy, hogy a T által elfogadott nyelvet fogadja el.

Összefoglalva:



A fenti nyilvánvaló tartalmazásokon túl két továbbit említünk meg.

1. Tétel (Adlemann).

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

Bizonyítás. Legyen $L \in \mathcal{BPP}$. Ekkor (az észrevételeket felhasználva) létezik T véletlen Turing-gép úgy, hogy bármely ω-ra $\mathbb{P}(\text{„}T \text{ hibázik"}) \leq 1/2^q(n)$, ahol $q(n)$ egy általunk választott polinom, n pedig ω hosszát jelenti.

Ekkor jelöljük a rossz ρ-kat az alábbi módon:

$$R_\omega = \{\rho : T(\omega, \rho) \text{ futás eredménye hibás}\}.$$

Ha összegezve az összes ω-ra az „$r \in R_\omega$" események valószínűségét egy 1-nél határozottan kisebb számot kapunk, akkor létezik olyan ρ_0 véletlen szalagtartalom, melyre igaz, hogy egyik R_ω-hoz sem tartozik hozzá, azaz $T(\omega, \rho_0)$ futás bármely ω-ra korrekt. Ez könnyen elérhető, hiszen $|\Sigma|^n$ darab n hosszú input van és „$r \in R_\omega$" valószínűsége $1/2^{n^2}$-nél kisebbé tehető.

A $T(\omega, \rho)$ futás számolását egy polinom méretű hálózattal leírhatjuk/kódolhatjuk. Tudunk olyan hálózatot csinálni, ami veszi az ω és ρ bitkódját és kiszámolja a futás végeredményét, ami 0 esetén ELVET, 1 esetén pedig ELFOGAD. Az (ω, ρ) inputot olvasó hálózat polinom méretű és uniform.

A tételt bizonyító hálózat ugyanez a hálózat lesz, de 0, 1-ek fognak szerepelni azon változók helyén, amelyek a véletlen biteket kódolják. (Így csak az ω inputot kódoló változók lesznek inputkapuk a hálózatban.) A véletlen bitek lerögzítése/behuzalozása úgy történik, hogy a ρ_0 véletleszszalag-tartalmat kódolja.

Az új hálózat már nem uniform, hiszen ρ_0 megtalálására nincs eljárásunk. Egy összeszámolási indoklás alapján tudjuk létét. Másrészt hálózatunk n hoszú inputokon T Turing-gépet számolását végzi el, azaz L-et dönti el. ■

2. Tétel (Gács Péter—Sipser).

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

Bizonyítás. (Lautemann) $\mathcal{BPP}$ zárt a komplementálásra, így elég csak belátnunk, hogy $\Sigma_2\mathcal{P}$-ben benne van. A tétel bizonyítása előtt először definiáljunk két fogalmat és igazoljuk az alábbi lemmát.

Definíció. Legyen $R \subset \Sigma^N$.

Az R halmaz akkor és csak akkor ritka, ha $|R| < 1/N|\Sigma^N|$.

Az R halmaz akkor és csak akkor sűrű, ha $|R| > (1 - 1/N)|\Sigma^N|$.

Fontos észrevennünk, hogy ezen fogalmak NEM egymás komplementerei.

3. Lemma (Főlemma). *Legyen $N > |\Sigma|$ tetszőleges. Ekkor*

i) Ha R ritka, akkor tetszőleges $c_1, \ldots, c_N \in \Sigma^N$ esetén $\cup_i(R + c_i) \subsetneq \Sigma^N$

ii) Ha R sűrű, akkor van olyan $c_1, \ldots, c_N \in \Sigma^N$, hogy $\cup_i(R + c_i) = \Sigma^N$.

A lemma bizonyítása: Az i) állítás triviális, hiszen a $R + c_i$ halmaz elemszáma megegyezik R elemszámával (a c_i hozzáadása olyan, mintha a számegyenesen eltolnám). Így $\cup_{i=1}^N(R + c_i)$-ben kevesebb elem van, mint $|\Sigma^N|$, ugyanis R ritka.

ii) rész bizonyításához valószínűségszámítási módszert használunk. $c_1, \ldots, c_N$ véletlen, uniform eloszlású Σ^N-beli elemek. Elég belátni, hogy

$$\mathbb{P}(\cup_{i=1}^N(R + c_i) = \Sigma^N) > 0.$$

Azaz ha véletlen c_i-ket választok, akkor nem lehetetlen esemény, hogy az eltólt R-ek együtt kiadják Σ^N-et. Az „$\cup_{i=1}^N(R + c_i) = \Sigma^N$” eseményünk egy átírása:

„bármely Σ^N-beli x-re létezik olyan i index, melyre $x \in c_i + R$”,

azaz

„mindegyik $x \in \Sigma^N$-re $(x - R) \cap \{c_1, \ldots, c_N\} \neq \emptyset$”,

azaz

„van olyan $x \in \Sigma^N$, hogy $(x - R) \cap \{c_1, \ldots, c_N\} = \emptyset$” $= \overline{B}$.

Tudjuk, hogy az $x - R$ halmaz mérete legalább $(1 - 1/N)|\Sigma^N|$, mivel R sűrű. Ekkor kapjuk, hogy konkrét $x \in \Sigma^N$ esetén

$$\mathbb{P}((x - R) \cap \{c_i\} = \emptyset) \leq \frac{1}{N},$$

továbbá a c_i-k független választása miatt

$$\mathbb{P}((x-R)\cap\{c_1,\ldots,c_N\}=\emptyset)\leq\left(\frac{1}{N}\right)^N,$$

Jelöljük B_x-szel az x-hez rossz c_i-k halmazát. Kaptuk, hogy B_x valószínűsége kisebb, mint $(1/N)^N$, továbbá felhasználva, hogy x-ekből $|\Sigma|^N$ darab van, kapjuk hogy $\mathbb{P}(\cup B_x)=\mathbb{P}(B)<1$. Ez adja a lemma állítását. ■

A tétel bizonyítása: Legyen $\Sigma=\{0,1,\ldots,|\Sigma|-1\}$, additív $\bmod|\Sigma|$ aritmetikával. Legyen T egy $L\in\mathcal{BPP}$-t bizonyító Turing-gép. Σ^N-beli ω esetén definiáljuk a következő halmazt:

$$J_\omega=\{\omega:\ \text{amelyekkel } T \text{ ELFOGAD állapotba kerül } \omega\text{-n}\}.$$

Ha $\omega\in L$, akkor J_ω sűrű, míg ellenkező esetben, J_ω ritka. A Főlemmát alkalmazva könnyen kapjuk a Tételbeli állítást. $\omega\in L$ akkor és csak akkor, ha léteznek a Főlemmabeli c_i-k úgy, hogy bármely Σ^N-beli x esetén c_i+J_ω lefedi x-et valamely i indexre, azaz kapjuk, hogy c_i-x J_ω-beli, c_i-x véletlen szalagtartalom esetén ELFOGAD-ó futása van a Turing-gépnek.

A tétel bizonyításához már csak azt kell belátnunk, hogy a fenti leírás L egy $\Sigma_2\mathcal{P}$-beli nyelvként való jellemzése. Valóban:

$$\omega\in L\Longleftrightarrow\exists c_1,\ldots,c_N\forall x\text{-re }(T(\omega,c_i-x)=ELFOGAD),$$

ahol a zárójeles kifejezés egy determinisztikus, polinomiális Turing-géppel eldönthető. Így a bizonyítás már teljes. ■