Definíciók és tételek a beugró vizsgára

(a szóbeli viszgázás jogáért)

Utolsó módosítás: 2008. december 2.

Bevezetés

Számítási problémának nevezünk egy olyan, a matematika nyelvén megfogalmazott kérdést, amire számítógéppel szeretnénk megadni a választ.

Egy problémát a hozzá tartozó konkrét bementettel együtt a **probléma egy példányá**nak nevezzük.

Speciális számítási probléma az **eldöntési probléma**. Ilyenkor a problémával kapcsolatos kérdés egy eldöntendő kérdés, tehát a probléma egy példányára a válasz „igen" vagy „nem" lesz.

Egy $f : A \to B$ függvényt **kiszámíthatóná**k nevezünk, ha létezik olyan algoritmus amely minden $x \in A$ elemre véges sok lépésben kiszámítja az $f(x) \in B$ értéket (tehát f teljesen definiált, azaz totális függvény).

Egy probléma **megoldható**, ha az általa meghatározott függvény kiszámítható.

Ha egy eldöntési probléma megoldható, akkor azt is mondjuk, hogy a probléma **eldönthető**. Egy eldönthető probléma tekinthető úgy is mint egy formális nyelv. A probléma példányait elkódoljuk egy megfelelő ábécé feletti szavakban. Ezek után magát a problémát azonosítjuk azzal a formális nyelvvel, mely azokat a szavakat tartalmazza, melyek a probléma „igen" példányait kódolják, vagyis azokat a példányokat melyekre a problémát eldöntő algoritmus „igen" választ ad.

Legyenek $f, g : N \to R_+$ függvények, ahol N a természetes számok, R_+ pedig a nemnegatív valós számok halmaza. Azt mondjuk, hogy f **legfeljebb olyan gyorsan nő mint** g (jelölése: $f(n) = \mathcal{O}(g(n))$) ha létezik olyan $c > 0$ szám és $n_0 \in N$, hogy $f(n) \leq c \cdot g(n)$ minden $n \geq n_0$ számra. Az $f(n) = \Omega(g(n))$ jelöli azt, hogy $g(n) = \mathcal{O}(f(n))$ teljesül, és $f(n) = \Theta(g(n))$ jelöli azt, hogy $f(n) = \mathcal{O}(g(n))$ és $f(n) = \Omega(g(n))$ is teljesül.

<u>Tétel</u> Minden polinomiális függvény lassabban nő, mint bármely exponenciális függvény, azaz minden $p(n)$ polinomhoz és c pozitív valós számhoz van olyan n_0 egész szám, hogy minden $n \geq n_0$ esetén $p(n) \leq 2^{cn}$.

Az **algoritmus fogalmának egy intuitív** definíciója: Utasítások egy jóldefiniált, véges sorozata, melyeket végrehajtva megoldható egy adott feladat (probléma).

Eszközök, melyek az **algoritmus fogalmának matematikai modelljei**: rekurzív függvények, λ-kalkulus, Turing-gépek, RAM gépek, Post-gépek, Markov-algoritmusok.

<u>Church-Turing tézis</u> A kiszámíthatóság különböző matematikai modelljei mind az effektíven kiszámítható függvények osztályát definiálják.

Formális nyelvi alapismeretek

Legyen Σ egy véges, nem üres halmaz. Σ-t **ábécé**nek, az elemeit pedig **betű**knek nevezzük.

Σ betűinek egy tetszőleges véges (akár üres) sorozatát **Σ-feletti szó**nak nevezzük. Σ^* jelöli az összes Σ-feletti szót, Σ^+ a $\Sigma^* - \{\varepsilon\}$ halmazt, $l(u)$ az $u \in \Sigma^*$ szó hosszát, $l_a(u)$ pedig az u-beli a betűk számát. A 0 hosszú szót **üres szó**nak nevezzük (jele: ε). **Σ-feletti nyelv**en a Σ^* egy részhalmazát értjük.

A kiszámíthatóság elmélet alapjai

A **Turing-gép** egy olyan $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ rendszer, ahol

- Q az állapotok véges, nemüres halmaza,
- $q_0, q_i, q_n \in Q$, q_0 a kezdő-, q_i az elfogadó és q_n az elutasító állapot,
- Σ és Γ ábécék, a bemenő jelek illetve a szalag szimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\Gamma - \Sigma$ tartalmaz egy speciális $\sqcup$ szimbólumot,
- $\delta : (Q - \{q_i, q_n\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ az átmenet függvény.

A Turing-gép működésének fázisait a gép úgynevezett konfigurációival írjuk le. A **Turing-gép konfigurációja** egy uqv szó, ahol $q \in Q$ és $u, v \in \Gamma^*$, $v \neq \varepsilon$. Ez a konfiguráció a gép azon állapotát tükrözi amikor a szalag tartalma uv (uv után szalagon már csak $\sqcup$ van), a gép a q állapotban van, és a gép író-olvasó feje a v első betűjére mutat. A gép **kezdőkonfiguráció**ja egy olyan $q_0u\sqcup$ szó, ahol u csak Σ beli betűket tartalmaz.

Egy Turing-gép **konfigurációátmeneté**t az alábbiak szerint definiáljuk. Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$ és $u, v \in \Gamma^*$. Ha $\delta(q, a) = (r, b, R)$, akkor $uqav \vdash ubrv'$, ahol $v' = v$, ha $v \neq \varepsilon$, különben $v' = \sqcup$. Most tegyük fel azt, hogy $\delta(q, a) = (r, b, L)$. Ebben az esetben ha $u \neq \varepsilon$, akkor $uqav \vdash u'rcbv'$, ahol $c \in \Gamma$ és $u'c = u$, egyébként pedig $uqav \vdash urbv$.

Azt mondjuk, hogy M **véges sok lépésben eljut** a C konfigurációból a C' konfigurációba (jele $C \vdash^* C'$), ha van olyan $n \geq 0$ és $C_1, \ldots, C_n$ konfigurációsorozat, hogy $C_1 = C$, $C' = C_n$ és minden $1 \leq i < n$-re, $C_i \vdash C_{i+1}$.

Ha $q \in \{q_i, q_n\}$, akkor azt mondjuk, hogy az uqv konfiguráció egy **megállási konfiguráció**. $q = q_i$ esetében elfogadó, míg $q = q_n$ esetében elutasító konfigurációról beszélünk.

Az M **által felismert nyelv** (amit $L(M)$-mel jelölünk) azoknak az $u \in \Sigma^*$ szavaknak a halmaza, melyekre igaz, hogy $q_0u\sqcup \vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ szavakra.

Egy $L \in \Sigma^*$ nyelv **Turing-felismerhető**, ha $L = L(M)$ valamely M Turing-gépre. Továbbá, egy $L \subseteq \Sigma^*$ nyelv **eldönthető**, ha létezik olyan M Turing-gép, mely minden bemeneten megállási konfigurációba jut és felismeri az L-et. A Turing-felismerhető nyelveket szokás **rekurzívan felsorolható**nak, az eldönthető nyelveket pedig **rekurzív**nak is nevezni. A rekurzívan felsorolható nyelvek osztályát RE-vel, a rekurzív nyelvek osztályát pedig R-rel jelöljük.

Tekintsünk egy $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ Turing-gépet és annak egy $u \in \Sigma^*$ bemenő szavát. Azt mondjuk, hogy M **futási ideje (időigénye) az** u **szón** n ($n \geq 0$), ha M a $q_0u\sqcup$ kezdőkonfigurációból n lépésben el tud jutni egy megállási konfigurációba. Ha nincs ilyen szám, akkor M futási ideje az u-n végtelen.

Legyen $f : N \rightarrow N$ egy függvény. Azt mondjuk, hogy M **időigénye** $f(n)$ (vagy, hogy M egy $f(n)$ **időkorlátos gép**), ha minden $u \in \Sigma^*$ input szóra, M időigénye az u szón legfeljebb $f(l(u))$.

Legyen $k > 1$. Egy k**-szalagos Turing-gép** egy olyan $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ rendszer, ahol a komponensek a δ kivételével megegyeznek az egyszalagos Turing-gép komponenseivel, δ pedig a következőképpen adódik. $\delta : (Q - \{q_i, q_n\}) \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, R, S\}^k$. Itt az S szimbólum azt az esetet jelöli amikor az író-olvasó fej helyben marad. A többszalagos Turing-gép konfigurációi, a konfigurációátmenetek valamint a felismert illetve elöntött nyelv definíciója az egyszalagos eset értelemszerű általánosításai. A többszalagos Turing-gép modell időigényét is az egyszalagoshoz hasonlóan definiáljuk.

A továbbiakban egy L nyelvet $f(n)$ **időben eldönthető**nek nevezünk, ha eldönthető egy $f(n)$ időkorlátos (akár többszalagos) Turing-géppel.

Tétel Minden k-szalagos, $f(n)$ időkorlátos Turing-géphez van vele ekvivalens egyszalagos, $\mathcal{O}(f(n)^2)$ időkorlátos Turing-gép.

Egy M **nemdeterminisztikus Turing-gép** átmenetfüggvénye $\delta : (Q - \{q_i, q_n\}) \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{L, R\})$ alakú. Tehát M minden konfigurációjából néhány (esetleg nulla) különböző konfigurációba mehet át. Ily módon M számítási sorozatai egy u szón egy fával reprezentálhatók. A fa csúcsa M kezdőkonfigurációja, a szögpontjai pedig M konfigurációi. A fa minden levele megfelel M egy számítási sorozatának az u-n. Végül M akkor fogadja el u-t, ha a fa valamelyik levele elfogadó konfiguráció. Nevezzük ezt a most leírt fát M **nemdeterminisztikus számítási fájá**nak az u-n.

Az M **nemdeterminisztikus Turing-gép által felismert nyelv** a determinisztikus esethez hasonlóan definiálható, a gép által eldöntött nyelv pedig a következőképpen. Azt mondjuk, hogy egy **nemdeterminisztikus Turing-gép eldönt egy** $L \subseteq \Sigma^*$ **nyelvet** ha felismeri, és minden $u \in \Sigma$ szóra M számítási sorozatai végesek és elfogadási vagy elutasítási konfigurációba vezetnek. A nemdeterminisztikus Turing-gép definíciója értelemszerűen kiterjeszthető a többszalagos esetre is.

A nemdeterminisztikus Turing-gép időigényét a következő módon definiáljuk. Legyen $f : N \rightarrow N$ egy függvény és M egy nemdeterminisztikus Turing-gép.

Azt mondjuk, hogy az M **időigénye** $f(n)$, ha egy n hosszú bemeneten nincsenek M-nek n-nél hosszabb számítási sorozatai.

Tétel Minden M $f(n)$ időigényű nemdeterminisztikus Turing-gép ekvivalens egy $2^{\mathcal{O}(f(n))}$ (exponenciális) időigényű determinisztikus Turing-géppel.

Eldönthetetlen problémák

Az $L_{\text{átló}}$ nyelv azon $\{0,1\}$-feletti Turing-gépek bináris kódjait tartalmazza, melyek nem fogadják el önmaguk kódját, mint bemenő szót. Formálisan, $L_{\text{átló}} = \{w_i \mid i \geq 1, w_i \notin L(M_i)\}$, ahol w_i az i-ik szó a $\{0,1\}$-feletti szavak felsorolásában, M_i pedig a w_i bináris szóval elkódolt $\{0,1\}$ ábécé feletti Turing-gép.

Tétel Az $L_{\text{átló}}$ nem rekurzívan felsorolható.

Legyen L egy Σ-feletti tetszőleges nyelv. Az L nyelv **komplementer**ét $\bar{L}$-el jelöljük és az alábbi módon definiáljuk: $\bar{L} = \{w \mid w \in \Sigma^*, w \notin L\}$.

Tétel Ha L egy rekurzív nyelv, akkor a komplementere is rekurzív.

Tétel Legyen L egy nyelv. Ha L és $\bar{L}$ is rekurzívan felsorolható, akkor L rekurzív.

Az L_{u} nyelv azon (M, w) párok halmaza (egy megfelelő bináris szóban elkódolva), ahol M egy $\{0,1\}$ bemenő ábécé feletti Turing-gép, w pedig egy $\{0,1\}$-feletti szó úgy, hogy $w \in L(M)$, azaz M elfogadja w-t. Formálisan, $L_{\text{u}} = \{\langle M, w\rangle \mid w \in L(M)\}$.

Tétel L_{u} rekurzívan felsorolható, de nem rekurzív.

Legyen Σ és Δ két ábécé és f egy Σ^*-ból Δ^*-ba képező függvény. Azt mondjuk, hogy f **kiszámítható**, ha van olyan M Turing-gép, hogy M-et egy $w \in \Sigma^*$ szóval a bemenetén indítva, M úgy áll meg, hogy a szalagján az $f(w)$ szó van.

Legyen $L_1 \in \Sigma^*$ és $L_2 \in \Delta^*$ két nyelv (azaz eldöntési probléma). Azt mondjuk, hogy L_1 **visszavezethető** L_2-re, ha van olyan $f : \Sigma^* \to \Delta^*$ kiszámítható függvény, hogy minden $w \in \Sigma^*$ szóra, $w \in L_2$ akkor és csak akkor teljesül, ha $f(w) \in L_2$ is teljesül.

Tétel Legyen L_1 és L_2 két eldöntési probléma és tegyük fel, hogy L_1 visszavezethető L_2-re. Akkor igazak az alábbi állítások:

1. Ha L_1 eldönthetetlen, akkor L_2 is az (azaz ha $L_1 \notin R$, akkor $L_2 \notin R$).
2. Ha $L_1 \notin RE$, azaz nem rekurzívan felsorolható, akkor $L_2 \notin RE$ szintén teljesül.

A **Turing-gépek megállási problémája**, mint formális nyelv:

$$L_{\text{halt}} = \{\langle M, w\rangle \mid M \text{ megáll a } w \text{ bemeneten}\},$$

azaz L_{halt} azon (M, w) Turing-gép és bemenet párosokat tartalmazza megfelelően elkódolva, hogy az M gép megáll a w bemenetet.

Tétel L_{halt} rekurzívan felsorolható, de nem rekurzív.

Ha $\mathcal{P}$ a rekurzívan felsorolható nyelvek egy halmaza, akkor $\mathcal{P}$-t a **rekurzívan felsorolható nyelvek egy tulajdonságá**nak nevezzük. Továbbá, $\mathcal{P}$ egy **nem triviális tulajdonság**, ha $\mathcal{P} \neq \varnothing$ és $\mathcal{P} \neq RE$. Azt mondjuk, hogy egy $L \in RE$ **nyelv rendelkezik a $\mathcal{P}$ tulajdonsággal**, ha $L \in \mathcal{P}$.

$L_{\mathcal{P}}$ azon Turing-gépek kódjait tartalmazza, melyek $\mathcal{P}$ tulajdonsággal rendelkező nyelveket ismernek fel.

Tétel (Rice tétele) Legyen $\mathcal{P}$ a rekurzívan felsorolható nyelvek egy nem triviális tulajdonsága. Akkor az $L_{\mathcal{P}}$ nyelv eldönthetetlen (azaz $L_{\mathcal{P}} \notin R$).

A **Post Megfelelkezési Probléma (PMP)** a következőképpen definiálható: Adott egy $D = \{\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\}$ dominóhalmaz, ahol $n \geq 1$ és minden $1 \leq i \leq n$-re, u_i és v_i egy Σ-feletti nem üres szó. A kérdés az, hogy van-e D-nek **megoldása**, azaz van-e olyan $i_1, \ldots, i_m \subseteq \{1, \ldots, n\}$ indexsorozat valamely $m \geq 1$-re, melyre teljesül, hogy $u_{i_1} \ldots u_{i_m} = v_{i_1} \ldots v_{i_m}$.

Tétel A Post Megfelelkezési Probléma algoritmikusan eldönthetetlen. Másképpen fogalmazva az

$$L_D = \{\langle D \rangle \mid D \text{ egy olyan dominókészlet aminek van megoldása}\}$$

nyelv nem R-beli.

Tekintsük az alábbi nyelveket (problémákat):

- $TAUT_1 = \{\langle\varphi\rangle \mid \varphi \text{ egy elsőrendű tautológia}\}$,
- $UNSAT_1 = \{\langle\varphi\rangle \mid \varphi \text{ egy kielégíthetetlen elsőrendű formula}\}$,
- $SAT_1 = \{\langle\varphi\rangle \mid \varphi \text{ egy kielégíthető elsőrendű formula}\}$,

Tétel A $TAUT_1$, $UNSAT_1$ és SAT_1 problémák egyike sem eldönthető, azaz $TAUT_1$, $UNSAT_1$, $SAT_1 \notin R$.

Következmény Algoritmikusan eldönthetetlen, hogy elsőrendű formulák egy tetszőleges véges F halmazára illetve egy A elsőrendű formulára teljesül-e, hogy $F \models A$.

Tétel A $TAUT_1$ és az $UNSAT_1$ nyelvek rekurzívan felsorolhatóak. Továbbá, ha F elsőrendű formulák egy tetszőleges véges halmaza, akkor azon A formulák halmaza, melyekre igaz, hogy $F \models A$ szintén rekurzívan felsorolható.

Következmény $SAT_1 \notin RE$, azaz SAT_1 nem rekurzívan felsorolható.

Bevezetés a bonyolultságelméletbe

Legyen $f(n) : N \to N$ egy függvény. Akkor

$$\mathbf{TIME}(f(n)) = \{L \mid L \text{ eldönthető } \mathcal{O}(f(n)) \text{ időigényű Turing-géppel}\}.$$

Továbbá, $\mathbf{P} = \bigcup_{k\geq 1} \mathbf{TIME}(n^k)$. Tehát **P** azon nyelveket tartalmazza, melyek eldönthetőek polinom időkorlátos determinisztikus Turing-géppel.

$$\mathbf{NTIME}(f(n)) = \{L \mid L \text{ eldönthető } \mathcal{O}(f(n)) \text{ időigényű } \textbf{nemdeterminisztikus} \text{ Turing-géppel}\}.$$

Továbbá, $\mathbf{NP} = \bigcup_{k\geq 1} \mathbf{NTIME}(n^k)$. Tehát **NP** azon nyelveket tartalmazza, melyek eldönthetőek polinom időkorlátos nemdeterminisztikus Turing-géppel.

<u>Tétel</u> $\mathbf{P} \subseteq \mathbf{NP}$. Az a sejtés (azaz még nem bizonyított), hogy a fenti tartalmazás valódi.

Legyen Σ és Δ két ábécé és f egy Σ^*-ból Δ^*-ba képező függvény. Azt mondjuk, hogy f **polinom időben kiszámítható**, ha kiszámítható egy polinom időigényű Turing-géppel.

Legyen $L_1 \in \Sigma^*$ és $L_2 \in \Delta^*$ két nyelv. Azt mondjuk, hogy L_1 **polinom időben visszavezethető** L_2**-re** (jele: $L_1 \leq_p L_2$), ha van olyan $f : \Sigma^* \to \Delta^*$ polinom időben kiszámítható függvény, hogy minden $w \in \Sigma^*$ szóra, $w \in L_1$ akkor és csak akkor teljesül, ha $f(w) \in L_2$ is teljesül.

<u>Tétel</u> Legyen L_1 és L_2 két probléma úgy, hogy $L_1 \leq_p L_2$. Ha L_2

1. **P**-beli, akkor L_1 is **P**-beli.
2. **NP**-beli, akkor L_1 is **NP**-beli.

Legyen L egy probléma. Azt mondjuk, hogy L **NP-teljes**, ha

1. **NP**-beli és
2. minden további **NP**-beli probléma polinom időben visszavezethető L-re.

<u>Tétel</u> Legyen L egy **NP**-teljes probléma. Ha $L \in \mathbf{P}$, akkor $\mathbf{P} = \mathbf{NP}$.

<u>Tétel</u> Legyen L_1 egy **NP**-teljes és L_2 egy **NP**-beli probléma. Ha $L_1 \leq_p L_2$ (azaz L_1 polinom időben visszavezethető L_2-re), akkor L_2 is **NP**-teljes.

Literálnak nevezünk egy ítéletváltozót (melynek értéke `igaz` illetve `hamis` lehet) illetve annak negáltját. **Tag**nak nevezzük a literálok diszjunkcióját („vagy” kapcsolatát) és **konjunktív normálformá**nak (knf) a tagok konjunkcióját („és” kapcsolatát). Ezek után a SAT **problémá**t a következőképpen definiáljuk.

SAT=$\{\langle\phi\rangle \mid \phi$ kielégíthető konjunktív normálformában adott logikai formula$\}$

Tehát SAT azon konjunktív normálformákat tartalmazza, egy megfelelő ábécé felett elkódolva, melyek kielégíthetőek.

Tétel (Cook tétele) SAT **NP**-teljes.

Legyen $k \geq 1$. A kSAT problémát a következőképpen definiáljuk. $k\text{SAT} = \{\langle\phi\rangle : \langle\phi\rangle \in \text{SAT}, \phi$ minden tagjában k literál van $\}$.

Tétel 3SAT **NP**-teljes.

A TELJES RÉSZGRÁF, FÜGGETLEN CSÚCSHALMAZ és CSÚCSLEFEDÉS problémákat a következőképpen definiáljuk.

$$\text{TELJES RÉSZGRÁF} = \{\langle G, k\rangle \mid G \text{ véges gráf, } k \geq 1, G\text{-nek létezik } k \text{ csúcsú teljes részgráfja } \}.$$

Tehát a TELJES RÉSZGRÁF azon G és k párokat tartalmazza, megfelelő ábécé feletti szavakban elkódolva, melyekre igaz, hogy G-ben van k csúcsú teljes részgráf, azaz olyan részgráf, melyben bármely két csúcs között van él.

$$\text{FÜGGETLEN CSÚCSHALMAZ} = \{\langle G, k\rangle \mid G \text{ véges gráf, } k \geq 1, G\text{-nek van } k \text{ elemű független csúcshalmaza } \}.$$

Vagyis a FÜGGETLEN CSÚCSHALMAZ azon G és k párokat tartalmazza, melyekre igaz, hogy G-ben van k olyan csúcs, melyek közül egyik sincs összekötve a másikkal.

CSÚCSLEFEDÉS $= \{\langle G, k\rangle \mid G$ véges gráf, $k \geq 1, G$-nek van olyan k elemű csúcshalmaza, mely tartalmazza G minden élének legalább egy végpontját $\}$.

Tétel A TELJES RÉSZGRÁF, FÜGGETLEN CSÚCSHALMAZ és CSÚCSLEFEDÉS problémák **NP**-teljesek.

Tétel Ha $\mathbf{P} \neq \mathbf{NP}$, akkor van olyan $L \in \mathbf{NP}$ nyelv, hogy $L \notin \mathbf{P}$, de L nem is **NP**-teljes.