

# ÜTEMTERV

## Algoritmusok és vizsgálatuk (GEMAK121M, GEMAK234-B)

### és Számításelmélet (GEMAK234B)

#### c. tárgyakhoz

Mérnök informatikus (mesterszak) és Programtervező informatikus (alapszak)  
hallgatók számára

**Óraszám: heti 3+1, (aláírás+kollokvium, 5 kredit)**

2019/20-as tanév I. félév.

- 1-2. hét:** Számítási modellek. A Turing gép fogalma, működése.
- 3. hét:** A RAM-gép. Boole-függvények és logikai hálózatok.
- 4. hét:** Algoritmikus eldönthetőség. Szimuláció fogalma, szimulációs tételek. Gödel-tétel, Church-tézis. Rekurzív és rekurzívan felsorolható nyelvek, rekurzív illetve parciálisan rekurzív függvények. Nevezetes nyelvek (Az R, Re, coR, coRE nyelvosztályok és ezek kapcsolata) és bonyolultságuk.
- 5. hét:** Néhány algoritmikusan eldönthetetlen probléma. Idő és tárkapacitásos-univerzális Turing-gépek fogalma. Idő-tár tétel. A Turing gép időigénye. A Turing kiszámíthatóság, Church-Turing tézis. Polinomiális idejű algoritmusok
- 6. hét:** 1. zárthelyi dolgozat megírása.
- 7. hét:** Nemdeterminisztikus algoritmusok, nemdeterminisztikus Turing gépek, Az NP és a coNP nyelvosztály.
- 8. hét:** Példák NP-beli nyelvekre. A tanú-tétel.
- 9. hét:** Nemdeterminisztikus algoritmusok bonyolultsága.
- 10. hét:** NP-teljesség, Cook-tétel. Néhány NP-teljes probléma, Karp redukció, Cook-Levin tétel.
- 11. hét:** Közelítő és randomizált algoritmusok. Prímtesztelés.
- 12. hét:** 2. zárthelyi dolgozat megírása.
- 13. hét:** Információs bonyolultság. A Kolmogorov bonyolultság és alkalmazásai. Az entrópia.
- 14. hét:** A bonyolultság alkalmazásai. A kriptográfia alapfogalmai, az RSA-kód. Párhuzamos algoritmusok. Párhuzamos bonyolultságelmélet.

**A tárgy lezárásának módja:** aláírás, kollokvium

**Az aláírás feltétele:**

- Az előadások felkészült, rendszeres látogatása.
- A félév során a két zárthelyi dolgozat (6. és 12. héten) legalább elégséges szintű megírása. A zárthelyi dolgozatok megírása mindenki számára kötelező.

A zárthelyi dolgozatok elméleti kérdéseket (tételek, definíciók) illetve számolási feladatokat tartalmazhatnak.

- Ha valamelyik zárthelyi dolgozat nem sikeres, akkor azt az utolsó héten lehet pótolni a megfelelő tananyagrészekből. Ha ez sem sikeres, akkor a későbbiekben az egész féléves anyagból kell pótolni.

A vizsga írásbeli. A félévközi zárthelyi dolgozatok eredménye beleszámít a vizsgajegybe.

Meg nem engedett eszközök használata esetén a vizsga elégtelen és további vizsga abban a vizsgaidőszakban csak szóban, bizottság előtt, a tanszék által megadott időpontban lehetséges.

Miskolc, 2019. szeptember 7.

(Dr. Házy Attila)  
a tárgy jegyzője

**3. Feladat** Készítsen Turing gépet, amely az  $x_1x_2 \dots x_n$  bemenet esetén előállítja az

$$x_nx_nx_{n-1}x_{n-1} \dots x_2x_2x_1x_1$$

kimenetet (6pont)

Miskolci Egyetem

Név:.....

Alkalmazott Matematikai Tanszék

Neptun-kód:.....

Zárthelyi dolgozat ALGORITMUSOK ÉS VIZSGÁLATUK c. tantárgyból  
Mérnök informatikus mesterszak, programtervező informatikus, gazdaságinformatika alapszakos  
hallgatók számára

**1. Feladat** Definiálja a következő fogalmakat: (1-1 pont)

(a) Növekvő rendezés:

(b) A Turing-gép:

(c) Rekurzív függvény:

(d) Rekurzíve felsorolható nyelv:

(e) Turing-gép időigénye:

(f) jól számolható függvény:

**2. Feladat** Fogalmazza meg a következő tételeket: (1-1 pont)

(a) Church-tézis:

(b) Rice Tétele:

(c) Gödel nem-teljességi tétele:

(d) Soroljon fel 3 polinomiális idejű aritmetikai algoritmust:

(e) Idő-hierarchia tétel:

(f) Gyorsítási tétel:

Miskolci Egyetem

Alkalmazott Matematikai Tanszék

Miskolc, .....

Név: .....

Neptun-kód: .....

Zárthelyi dolgozat ALGORITMUSOK ÉS VIZSGÁLATUK (GEMAK121M) c. tantárgyból

**1. Feladat** Definiálja a következő fogalmakat: (1-1 pont)

(a) Nemdeterminisztikus Turing-gép:

(b) Legális számolás:

(c) NP-teljesség:

(d) Fermat feltétel:

(e) gyengén eldöntés (Monte-Carlo):

(f) Informatikusan véletlen sorozat:

**2. Feladat** Fogalmazza meg a következő tételeket: (1-1 pont)

(a) Savitch-tétel:

(b) Cook-tétel:

(c) Kuratowski-tétel:

(d) Adjon 3 példát NP-teljes problémára:

(e) Schwartz-lemmája:

(f) kis Fermat-tétel:

Miskolci Egyetem

Név:.....

Alkalmazott Matematikai Tanszék

Neptun-kód:.....

Zárthelyi dolgozat ALGORITMUSOK ÉS VIZSGÁLATUK c. tantárgyból  
Mérnök informatikus mesterszak, programtervező informatikus, gazdaságinformatika alapszakos  
hallgatók számára

**1. Feladat** Definiálja a következő fogalmakat: (1-1 pont)

(a) Növekvő rendezés:

A növekvő rendezésben minden rövidebb szó megelőz minden hosszabb szót, az azonos hosszúságú szavak pedig lexikografikusan vannak rendezve.

(b) A Turing-gép:

$T = \{k, \Sigma, \Gamma, \alpha, \beta, \gamma\}$ , ahol  $k \geq 1$  egy természetes szám,  $\Sigma$  és  $\Gamma$  véges halmazok,  $*$   $\in \Sigma$   
 $\{\text{START}, \text{STOP}\} \in \Gamma$ , és

$$\alpha : \Gamma \times \Sigma^k \rightarrow \Gamma$$

$$\beta : \Gamma \times \Sigma^k \rightarrow \Sigma$$

$$\gamma : \Gamma \times \Sigma^k \rightarrow \{-1, 0, 1\}^k$$

tetszőleges leképezések. ( $\alpha$  adja meg az új állapotot,  $\beta$  a szalagokra írt jeleket,  $\gamma$  azt, hogy mennyit lép a fej).

(c) Rekurzív függvény:

Egy  $f : \Sigma_0 \rightarrow \Sigma_0$  függvényt kiszámíthatónak vagy rekurzívnak nevezünk, ha van olyan  $T$  Turing-gép (tetszőleges  $k$  számú szalaggal), mely bármely  $x \in \Sigma_0$  bemenettel (vagyis első szalagjára az  $x$  szót, a többire az üres szót írva), véges idő után megáll, és az utolsó szalagjára az  $f(x)$  szó lesz írva.

(d) Rekurzíve felsorolható nyelv:

Az  $\mathcal{L}$  nyelvet rekurzíve fölsorolhatónak nevezzük, ha vagy  $\mathcal{L} = \emptyset$ , vagy van olyan kiszámítható  $f : \Sigma_0 \rightarrow \Sigma_0$  függvény melynek értékkészlete  $\mathcal{L}$ .

(e) Turing-gép időigénye:

A  $T$  Turing-gép időigénye az a  $time_T(n)$  függvény, amely a gép lépésszámának maximumát adja meg  $n$  hosszúságú bemenet esetén.

(f) jól számolható függvény:

Az  $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  függvényt jól számolhatónak nevezzük, ha van olyan Turing-gép, mely  $f(n)$ -et az  $n$  bemeneten  $O(f(n))$  idő alatt kiszámítja.



**2. Feladat** Fogalmazza meg a következő tételeket: (1-1 pont)

(a) Church-tézis:

Minden "számítás" az általa megadott rendszerben formalizálható.

(b) Rice Tétele:

Bármely nem-triviális nyelv-tulajdonságra algoritmikusan eldönthetetlen, hogy egy adott  $\mathcal{L}_T$  nyelvnek megvan-e.

(c) Gödel nem-teljességi tétele:

Minden minimálisan megfelelő elmélet nem-teljes.

(d) Soroljon fel 3 polinomiális idejű aritmetikai algoritmust:

Polinomiálisak az alapvető aritmetikai műveletek: egész számok összeadása, kivonása, szorzása, maradékos osztása. Euklideszi-algoritmus. Moduláris hatványozás.

(e) Idő-hierarchia tétel:

Ha  $f(n)$  teljesen időkonstruálható és  $g(n)(\log g(n)) = o(f(n))$ , akkor van olyan nyelv  $DTIME(f(n))$ -ben mely nem tartozik  $DTIME(g(n))$ -be.

(f) Gyorsítási tétel:

Bármely rekurzív  $g(n)$  függvényhez létezik olyan rekurzív  $\mathcal{L}$  nyelv, hogy minden  $\mathcal{L}$ -et eldöntő  $T$  Turing-géphez létezik olyan  $\mathcal{L}$ -et eldöntő  $S$  Turing-gép, melyre  $g(times_S(n)) < time_T(n)$ .

**3. Feladat** Készítsen Turing gépet, amely az  $x_1x_2 \dots x_n$  ( $x_i \in 0, 1$ ) bemenet esetén előállítja az

$$x_nx_nx_{n-1}x_{n-1} \dots x_2x_2x_1x_1$$

kimenetet (6pont)

Legyen  $k = 2$ ,  $\Sigma = \{0, 1, *\}$  és  $\Gamma = \{START, STOP, VISSZA, MASOL\}$

állapot	jelek	$\alpha$	$\beta$	$\gamma$
<i>START</i>	(0, *)	<i>START</i>	(0, *)	(1, 0)
<i>START</i>	(1, *)	<i>START</i>	(1, *)	(1, 0)
<i>START</i>	(*, *)	<i>VISSZA</i>	(*, *)	(-1, 0)
<i>VISSZA</i>	(0, *)	<i>MASOL</i>	(0, 0)	(0, 1)
<i>VISSZA</i>	(1, *)	<i>MASOL</i>	(1, 1)	(0, 1)
<i>VISSZA</i>	(*, *)	<i>STOP</i>	(*, *)	(0, 0)
<i>MASOL</i>	(0, *)	<i>VISSZA</i>	(0, 0)	(-1, 1)
<i>MASOL</i>	(1, *)	<i>VISSZA</i>	(1, 1)	(-1, 1)

Minden más eset hiba (nem lehetséges).

Miskolci Egyetem

Miskolc, .....

Alkalmazott Matematikai Tanszék

Név: .....

Neptun-kód: .....

Zárthelyi dolgozat ALGORITMUSOK ÉS VIZSGÁLATUK (GEMAK121M, GEMAK234-B) c.  
tantárgyból

**1. Feladat** Definiálja a következő fogalmakat: (1-1 pont)

(a) Nemdeterminisztikus Turing-gép:

Egy nem-determinisztikus Turing-gép egy  $T = \{k, \Sigma, \Gamma, \alpha, \beta, \gamma\}$  rendezett 6-os, ahol  $k \geq 1$  egy természetes szám,  $\Sigma$  és  $\Gamma$  véges halmazok,  $*$   $\in \Sigma$   
 $\{\text{START}, \text{STOP}\} \in \Gamma$ , és

$$\alpha \subseteq \Gamma \times \Sigma^k \times \Gamma$$

$$\beta \subseteq \Gamma \times \Sigma^k \times \Sigma$$

$$\gamma \subseteq \Gamma \times \Sigma^k \times \{-1, 0, 1\}^k$$

tetszőleges relációk.

(b) Legális számolás:

A gép egy legális számolása lépéseknek egy sorozata, ahol minden lépésben (ugyanúgy, mint a determinisztikus Turing gépnél) a vezérlőegység új állapotba megy át, a fejek új jeleket írnak a szalagokra, és legföljebb egyet lépnek jobbra vagy balra. Eközben fenn kell állni a következőknek: ha a vezérlőegység állapota a lépés előtt  $g \in \Gamma$  volt, és a fejek a szalagokról rendre a  $h_1, \dots, h_k \in \Sigma$  jeleket olvasták, akkor az új  $g'$  állapotra, a leírt  $h'_1, \dots, h'_k$  jelekre és a fejek  $\varepsilon_1, \dots, \varepsilon_k \in \{-1, 0, 1\}$  lépéseire teljesül:

$$((g, h_1, \dots, h_k), g') \in \alpha$$

$$((g, h_1, \dots, h_k), (h'_1, \dots, h'_k)) \in \beta$$

$$((g, h_1, \dots, h_k), (\varepsilon_1, \dots, \varepsilon_k)) \in \gamma$$

(c) NP-teljesség:

Egy NP-beli  $\mathcal{L}$  nyelvet NP-teljesnek nevezünk, ha minden NP-beli nyelv polinomiálisan visszavezethető  $\mathcal{L}$ -re.

(d) Fermat feltétel:

Ha - adott  $m$  mellett - egy  $a$  számra  $a^{m-1} - 1$  osztható  $m$ -mel, akkor azt mondjuk, hogy  $a$  kielégíti a Fermat-feltételt.

(e) gyengén eldöntés (Monte-Carlo):

Azt mondjuk, hogy a randomizált Turing-gép gyengén eldönt (vagy Monte-Carlo értelemben eldönt) egy  $\mathcal{L}$  nyelvet, ha minden  $x \in \Sigma^*$  bemenetre legalább  $3/4$  valószínűséggel úgy áll meg, hogy  $x \in \mathcal{L}$  esetén az eredményszalagra 1-et,  $x \notin \mathcal{L}$  esetén az eredményszalagra 0-t ír. (Röviden: legfeljebb  $1/4$  a valószínűsége annak, hogy hibás választ ad.)

(f) Informatikusan véletlen sorozat:

Legyen  $x$  végtelen 0 – 1 sorozat, és jelölje  $x_n$  az első  $n$  eleme által alkotott kezdőszeletét. Az  $x$  sorozatot informatikusan véletlennek nevezzük, ha  $K(x_n)/n \rightarrow 1$  ha  $n \rightarrow \infty$ .

**2. Feladat** Fogalmazza meg a következő tételeket: (1-1 pont)

(a) Savitch-tétel:

Ha  $f(n)$  jól számolható függvény, és  $f(n) \geq \log n$ , akkor minden  $\mathcal{L} \in NSPACE(f(n))$  nyelvhez van olyan  $c > 0$ , hogy  $\mathcal{L} \in DSPACE(cf(n)^2)$ .

(b) Cook-tétel:

A SAT nyelv NP-teljes.

(c) Kuratowski-tétel:

Egy gráf akkor és csak akkor rajzolható síkba, ha nem tartalmaz olyan részgráfot, mely élek felosztásával jön létre a teljes 5-szögből vagy a három-ház-háromkút gráfból.

(d) Adjon 3 példát NP-teljes problémára:

Lefogási feladat, k-Partíció feladat és a Partíció feladat, Gráfok 3 színnel való színezhetősége, A Független ponthalmaz feladat, A Diophantoszi egyenlőlenségrendszer megoldhatósága, A Részletösszeg probléma.

(e) Schwartz-lemmája:

Ha  $f$  nem azonosan 0  $n$ -változós, minden változójában legfeljebb  $k$ -adfokú polinom, és a  $\xi_i$  ( $i = 1, \dots, n$ ) értékek a  $[0, N-1]$  intervallumban egyenletes eloszlás szerint véletlenszerűen és egymástól függetlenül választott egész számok, akkor  $Prob(f(\xi_1, \dots, \xi_n) = 0) \leq \frac{k}{N}$ .

(f) kis Fermat-tétel:

Ha  $m$  prím, akkor minden  $1 \leq a \leq m-1$  természetes számra  $a^{m-1} - 1$  osztható  $m$ -mel.