Számításelmélet

Számításelmélet

- **Oktató:** Gazdag Zsolt
- **Elérhetőség:** Déli, 2-708, gazdagzs@inf.elte.hu
- **Web:** people.inf.elte.hu/gazdagzs
- **Ajánlott irodalom:**
  - Jegyzet a weben,
  - Papdimitriou: Számítási bonyolultság
  - Sipser: Introduction to the Theory of Computation

Kiszámíthatóság elmélet – Történeti áttekintés

- **1900: Hilbert 23 problémája**
  - Pl. 10-es: keressük meg egy tetszőleges egész együtthatós többváltozós egyenlet gyökeit
    - Pl. bemenet: $3xy - 2x^2 + 2z + 4 = 0$, kimenet: $x = 0, y = 0, z = -2$
- **1920-as évek: Hilbert programja**
  - Célja a matematika összes elméletének axiomatizálása egy végesen reprezentálható axiómarendszerrel
    - **A program része:** egy olyan **Mindent Megoldó Algoritmus** megadása ami a matematika tetszőleges állításáról eldönti, hogy az igaz vagy hamis

Kiszámíthatóság elmélet – Történeti áttekintés

- **1929, Gödel:** Az elsőrendű kalkulus teljes (minden tautológia levezethető egy megfelelő axiómarendszerből)
- **1931, Gödel első nemteljességi tétele**
  - Egy olyan effektíven kiszámítható elmélet ami tartalmazza az elemi aritmetikát nem lehet egyszerre helyes és teljes
  - **Egy *T* elmélet *G* Gödel mondata:** *G egy olyan állítás ami nem bizonyítható T-ben*
  - **Következmény:** Hilbert programja megvalósíthatalan
- **1930-as évek:** különböző algoritmus modellek bevezetése
  - Gödel: rekurzív függvények
  - Church, Kleene, Rosser: λ kalkulus
  - Turing: Turing-gép

Kiszámíthatóság elmélet – Történeti áttekintés

- **Az Mindent Megoldó Algoritmus létezésének cáfolása**
  - 1936, Church: Két λ-kalkulusbeli kifejezés ekvivalenciája eldönthetetlen
  - 1936, Turing: A Turing-gépek megállási problémája eldönthetetlen
- ***Church-Turing-tézis**: a kiszámíthatóság különböző matematikai modelljei mind az effektíven kiszámítható függvények osztályát definiálják*
- **Megjegyzés**: A 10-es probléma algoritmikusan eldönthetetlen (1970, Matiyasevich)

Alan M. Turing, 1912-1954

- Felsőfokú tanulmányok:
  - 1931-34, King's College
  - 1936-38, Princeton (témavezető: A. Church)
  - 1938-39, Cambridge
- Főbb eredmények:
  - Számításelmélet, logika:
    - On Computable Numbers, with an Application to the Entscheidungsproblem
    - Systems of Logic Based on Ordinals (PhD tézis)
  - Kriptográfia:
    - Enigma feltörése (Turing Bomba)
  - Mesterséges intelligencia
    - Turing-teszt, sakk program,…

Kiszámíthatóság elmélet – Alapfogalmak

- **Kiszámítási probléma:** olyan matematikailag precízen megfogalmazott probléma, amit algoritmikusan szeretnénk megoldani
  - Pl. Hilbert 10-es problémája
- Egy **hétköznapi problémához**, megfelelő absztrakcióval, általában megadható ekvivalens kiszámítási probléma
  - Pl. Utazó ügynök → Súlyozott Hamilton kör
  - Hordók pakolása a teherautóra → Körpakolás

Kiszámíthatóság elmélet – Alapfogalmak

- **Eldöntési probléma:** Egy I bemenetre a válasz $igen$ vagy nem (I pozitív vagy negatív bemenet)
  - **Pl. SAT probléma:**
    - Bemenet: φ zérusrendű KNF
    - Kérdés: Kielégíthető-e φ?
- **Egy P probléma reprezentálható** egy

$$f_P: A \to B$$ függvénnyel

bemenetek válaszok (megfelelően elkódolva)

- **Megjegyzés:** Ha P eldöntési probléma, akkor pl. $B = \{0,1\}$ v. $B = \{igen, nem\}$

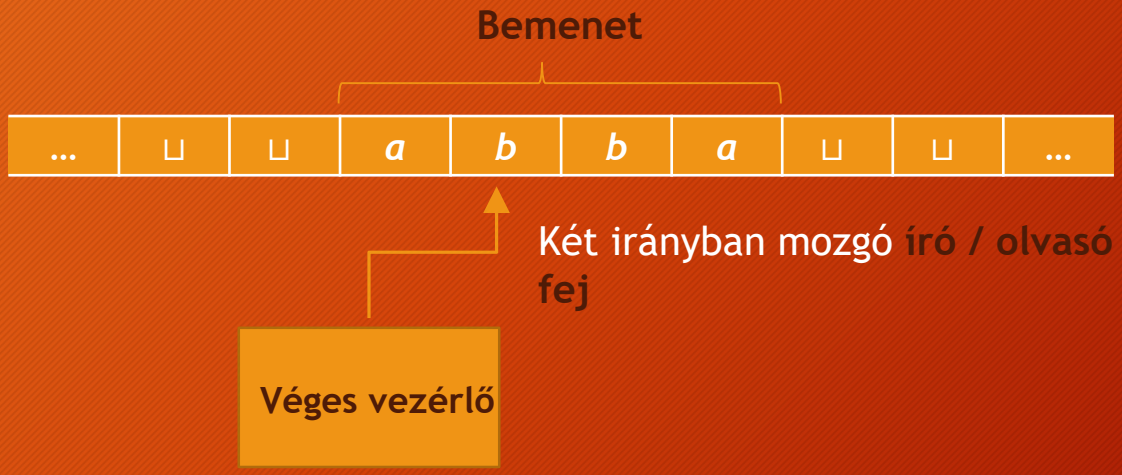
Kiszámíthatóság elmélet – Alapfogalmak

- **P megoldható**, ha **f_P kiszámítható**, azaz minden $I \in A$ esetén $f(I)$ algoritmikusan kiszámítható
- Ha P egy megoldható eldöntési probléma, akkor P **eldönthető**
  - Pl. SAT eldönthető (Hogyan?)
- Egy P eldöntési probléma megfeleltethető egy

  $$L_P := \{\langle I \rangle \mid I \text{ a } P \text{ pozitív bemenete}\}$$ formális nyelvnek
  - Pl. L_{SAT} $(vagy\ SAT) := \{\langle \varphi \rangle \mid \varphi\ kielégíthető\}$
- **Jelölés:** Tetsz. D objektumra $\langle D \rangle$ **jelöli a D elkódolását** egy megfelelő ábécé felett

A Turing gép

- Egy **algoritmus modell** formális nyelvek eldöntésére

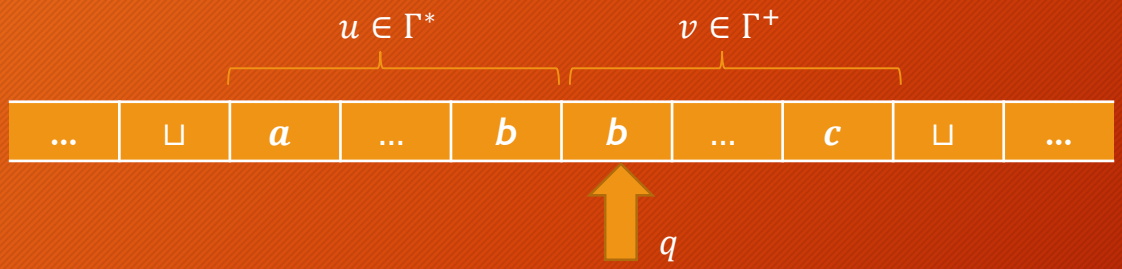


A Turing gép

- **Formálisan:** $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$, ahol
  - Q az **állapotok** véges, nem üres halmaza, q_0: kezdő-, q_i: elfogadó, q_n: elutasító állapot
  - Σ a **bemenő jelek** ábécéje
  - Γ a **szalagszimbólumok** ábécéje
    ($\Sigma \subset \Gamma$, $\sqcup \in \Gamma - \Sigma$, $\sqcup$: **üres szimbólum**)
  - $\delta: (Q - \{q_i, q_n\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ az **átmeneti függvény**
  - **Megjegyzés:** A gyakorlatban az S - helybenmaradás jelet is használjuk

A Turing gép

- **Konfiguráció:** uqv a következőképpen definiálva



- Egy uqv konfiguráció
  - **Kezdőkonfiguráció**, ha $v \in \Sigma^*, q = q_0$ és $u = \varepsilon$ (illetve $v =$⊔, ha $u = \varepsilon$);
  - **Elfogadó konfiguráció**, ha $q = q_i$
  - **Elutasító konfiguráció**, ha $q = q_n$
- Az elfogadó és elutasító konfigurációkat **megállási konfigurációknak** is nevezzük

A Turing gép

- **Összes konfiguráció:** C_M
- **Konfiguráció átmenet:** $\vdash \subseteq C_M \times C_M$
  - Legyen $C_1, C_2 \in C_M$, $C_1 \vdash C_2$ ha az alábbiak egyike teljesül
    - $C_1 = uqav, C_2 = ubpv'$ és $\delta(q,a) = (p,b,R)$ ahol $a,b \in \Gamma, u,v \in \Gamma^*, v' = v$, ha $v \neq \varepsilon$ és $v' = \sqcup$ egyébként
    - $C_1 = ucqav, C_2 = upcbv$ és $\delta(q,a) = (p,b,L)$, ahol $a,b,c \in \Gamma, u,v \in \Gamma^*$

A Turing gép

- **Többlépéses konfiguráció átmenet:** $\vdash^* \subseteq C_M \times C_M$
  - Legyen $C, C' \in C_M$, $C \vdash^* C'$ ha az alábbiak teljesülnek
    - $\exists C_1, \dots, C_n\ (n \geq 1)$: $C_1 = C, C_n = C'$ és
    - $\forall 1 \leq i < n: C_i \vdash C_{i+1}$
  - **Megjegyzés:** $\vdash^*$ a $\vdash$ reflexív, tranzitív lezártja
- **Az M által felismert nyelv:**
  $L(M) := \{u \in \Sigma^* \mid q_0 u \sqcup \vdash^* v q_i v', v, v' \in \Gamma^*, v' \neq \varepsilon\}$
- **Feladat:** Adjunk Turing-gépet, ami az $L = \{uu^{-1} \mid u \in \{a, b\}^*\}$ nyelvet ismeri fel

A Turing gép

- Egy L nyelv **Turing-felismerhető**, ha van olyan M Turing gép, hogy $L = L(M)$. Ha M minden bemeneten meg is áll, akkor L **eldönthető**
- **Megjegyzés:**
  - A Turing-felismerhető nyelveket nevezzük még **rekurzívan felsorolható**, **parciálisan rekurzív** vagy **félig eldönthető** nyelveknek; ezen nyelvek osztályát RE-vel jelöljük
  - Az eldönthető nyelveket nevezzük még **rekurzív** nyelveknek is; ezen nyelvek osztályát R-rel jelöljük
  - Triviálisan $\boldsymbol{R \subseteq RE}$; később megmutatjuk, hogy ez a tartalmazás valódi

A Turing gép

- **Egy M Turing-gép időigénye** $f(n)$ $(f\colon \mathbb{N} \to \mathbb{N})$, ha minden n hosszú bemeneten M legfeljebb $f(n)$ lépésben megáll
- **Feladat:** Mi az előbb megadott Turin-gép időigénye?
- **Megjegyzés:** nem kell a pontos időigényt megadni
- **A nagy O jelölés:**

Legyen $f, g\colon \mathbb{N} \to \mathbb{R}^+$. Az f **legfeljebb olyan gyorsan nő mint a** g (jele: $f = O(g)$), ha $\exists n_0 \in \mathbb{N}, c > 0\colon \forall n \geq n_0$:

$$f(n) \leq c \cdot g(n)$$