

XI. Előadás (2020. Május. 07.)

(A) Eldönthetőséggel kapcsolatos definíciók

Legyen U egy univerzúm és $P \subseteq U$ egy nemüres részhalmaza.

(1) Azt mondjuk hogy P halmaz *eldönthető*, ha létezik egy olyan algoritmus (utasításokból álló véges lista), ami bármely $u \in U$ elemről véges lépésben eldönti hogy P -hez tartozik-e vagy sem.

Példák: A definícióból következően minden véges halmaz eldönthető. Az is világos, hogy egy eldönthető halmaz elemszáma legfeljebb megszámlálhatóan végtelen lehet, mert egy véges halmaz elemeiből képezhető összes véges hosszúságú sorozatok száma megszámlálhatóan végtelen számosságú. Ezért az ennél nagyobb számosságú halmazok biztosan nem eldönthető halmazok. Pl. $\mathbb{R}$, a valós számok halmaza kontinuum számosságú, így nem eldönthető.

(2) A $\mathcal{P}$ tulajdonság *eldönthető*, ha a $P = \{x \in U \mid x \text{ } \mathcal{P} \text{ tulajdonságú}\}$ halmaz eldönthető.

Pl. Az „ n szám prímszám” tulajdonság eldönthető, mert a prímszámok halmaza eldönthető.

(3) A Π probléma *eldönthető*, ha véges számú $\mathcal{P}_1, \dots, \mathcal{P}_n$ eldönthető tulajdonság ellenőrzését jelenti a megoldása.

Pl. Az hogy egy f igazságfüggvény Scheffer függvény-e, annak ellenőrzését jelenti, hogy f nem 0-örző, nem 1-örző, nem monoton, nem lineáris és nem önduális-e. Mivel mindegyik tulajdonság eldönthető, az hogy f Scheffer függvény-e egy eldönthető probléma.

K. Gödel konstruált olyan $P(n)$, $n \in \mathbb{N}$ predikátumot amely esetén az a kérdés hogy $P(n)$ mely természetes számokra igaz (és melyekre nem) nem eldönthető.

Megjegyzés 1. Legyen most P egy legfeljebb megszámlálhatóan végtelen számosságú halmaz - ismert tény hogy akkor P elemeit egy $\Sigma = \{0, 1\}$ ábécé szavaival kódolhatjuk (azaz kölcsönösen egyértelműen megfeleltethetjük egy $P^* \subseteq \Sigma^*$ szóhalmaz elemeinek.) Vegyük észre, hogy múlt órán tanultak értelmében P pontosan akkor eldönthető halmaz, ha P^* egy rekurzív nyelv.

Állítás 1. A következő kijelentések egyenértékűek:

- (i) A P halmaz eldönthető;
- (ii) Van olyan $\chi_{P^*} : \Sigma^* \rightarrow \{0, 1\}$ kiszámítható függvény, hogy $\chi_{P^*}(w) = 1$, ha $w \in P^*$ és $\chi_{P^*}(w) = 0$, ha $w \notin P^*$;
- (iii) P^* egy rekurzív nyelv;
- (iv) Van olyan ciklusmentes M Turing gép amire $\mathcal{L}(M) = P^*$.

Bizonyítás: Az előbbi megjegyzés alapján (i) $\Leftrightarrow$ (iii). A (iii) $\Leftrightarrow$ (iv) ekvivalenciát a múlt órán mutattuk meg.

(iii) $\Rightarrow$ (ii). Ha $P^* \subseteq \Sigma^*$ rekurzív nyelv, akkor egy tetszőleges $w \in \Sigma^*$ szó esetén a $w \in P^*$ hozzátartozás véges lépésben eldönthető, így a χ_{P^*} karakterisztikus függvény értéke véges lépésben kiszámítható (lévén ez csak 0 vagy 1 lehet).
(ii) $\Rightarrow$ (iii). Ha χ_{P^*} kiszámítható függvény, értékét minden $w \in \Sigma^*$ esetén véges lépésben meg lehet határozni. Ha ez 1, akkor $w \in P^*$; tehát a $w \in P^*$ hozzátartozás is véges lépésben eldönthető, így $P^* \subseteq \Sigma^*$ egy rekurzív nyelv. $\square$

Következmény 1. Egy Π probléma akkor és csak akkor eldönthető, ha Π -nek egyértelműen megfeleltethető egy $L_\Pi \subseteq \Sigma^*$ nyelv, továbbá egy M ciklusmentes Turing gép (ami tehát minden szóra megáll) amire $\mathcal{L}(M) = L_\Pi$.

Bizonyítás: A fenti állítás azonnal következik az eldönthető probléma definíciójából, a Megjegyzés 1.-ből és az Állítás 1.(iv)-ből. $\square$

A Formális Nyelvek tárgya eldönthetetlen problémái.

Az első ilyen probléma A. Turing nevezetes eredménye által vált ismertté:

Állítás 2. Nincs olyan algoritmus ami egy tetszőleges TM gép és egy tetszőlegesen választott $w \in \Sigma^*$ szó esetén eldöntené hogy a TM gép a w szó beolvasása után véges lépésben megáll-e vagy sem.

Állítás 3. (i) Eldönthetetlen az a kérdés hogy egy tetszőleges rekurzívan felsorolható nyelv

(a) üres-e;

(b) véges-e;

(c) környezetfüggetlen-e?

(ii) Eldönthetetlen az a kérdés hogy egy tetszőleges $G = (V, T, P, S)$ k. független nyelvtan kétértelmű-e vagy sem.

Megjegyzés 2. Fontos hogy egy probléma „eldönthetőségét” helyesen értelmezzük. Például az Állítás 3(ii) nem azt jelenti hogy egy konkrét G k. független nyelvtan (L k. független nyelv) esetén eldönthető-e a kétértelműség, hanem azt, hogy nem létezik olyan *univerzális* algoritmus, ami a kérdést minden G környezetfüggetlen nyelvtan esetén egységesen eldöntené.

(B) A Turing gép kódolása

Az alább ismertetett eljárást fel fogjuk használni Turing nevezetes eredményének az ismertetésénél.

Tekintsük az alábbi standard Turing gépet:

$\mathcal{M} = (Q, \{0, 1\}, \{0, 1, B\}, \delta, q_1, B, \{q_f\})$, ahol $Q = \{q_1, q_2, \dots, q_n\}$, $F = \{q_f\} \subseteq Q$, $\mathcal{L}(\mathcal{M}) \subseteq (0 + 1)^*$

Minden állapothoz, betűhöz és B -hez is egy bináris szót rendelünk:

A q_i állapotnak 0^i -t feleltetünk meg.

$$X_j := \begin{cases} 0 & \text{ha } X_j = 0 \\ 00 & \text{ha } X_j = 1 \\ 000 & \text{ha } X_j = B \end{cases} \text{ - így a } (q_i, X_j) \text{ párnak } 0^i 10^j \text{ felel meg.}$$

A δ tranzíciós függvény hatását a köv. képpen kódolhatjuk:

L - szimbóluma: 0;

R - szimbóluma: 00.

Ha az utasítás $\delta((q_i, X_j) = (q_k, X_l, D)$ alakú, ahol $D = \begin{cases} L \\ \text{vagy} \\ R \end{cases}$;

akkor ezt így kódoljuk: $0^i 10^j 10^k 10^l 10^m$, ahol $l \in \{1, 2, 3\}$ és $m \in \{1, 2\}$,

Tehát a kód 5 részből áll és 4 elválasztó jelet, vagyis 4 drb. 1-est tartalmaz.

Például tekintsük az köv. utasítást: $\delta((q_1, 1) = (q_2, B, L)$

Ezt így kódoljuk (unáris kódot használva):

0100100100010

A TM gép egy teljes bináris kódja:

111kód₁11kód₂11...11kód_n111 - jelsorozat.

Itt a kódokat mindig az 11 csoport választja el, 111 jelzi hogy kódsor kezdődik, illetve hogy véget ért a kódsor.

Azt hogy az $(\mathcal{M}, w)$ pár eredménye a $w' \in (0+1)^*$ bináris szó, így jelölhetjük:

111kód₁11kód₂11...11kód_n111BBw bin.szóBBw'bin.szó

A bináris szavakat (a TM gép bináris kódját is beleértve) 2-es számrendszerebeli szavakká alakítva tehát egy $m, n : k$ számhármast kapunk, amit úgy tekinthetünk hogy a k szám az m és n függvénye. $(T\mathcal{M}(m, n) = k)$.

(C) Turing nevezetes eredménye

Legyen $\Sigma = \{0, 1\}$ és $\Gamma = \{0, 1, B\}$ rögzített. A kérdés az, hogy eldönthető-e algoritmussal az a probléma hogy egy tetszőlegesen választott standard TM gép és $w \in \Sigma^*$ szó esetén a TM gép akceptálja-e a w szót vagy sem. (Más megfogalmazásban: Van-e olyan „univerzális” algoritmust ami minden TM gép és minden $w \in \Sigma^*$ szó esetén eldönti ezt a kérdést?)

A válasz Turing nevezetes eredménye - ami az Állítás 2.-ben is szerepel - hogy ilyen algoritmus nincs. Más megfogalmazásban ez azt jelenti hogy nincs olyan U „univerzális TM gép” amivel egy tetszőleges TM gép adatait (kódját) és egy tetszőleges $w \in \Sigma^*$ szót beolvasva, U pontosan akkor áll meg, ha a TM gép akceptálja w -t.

Turing tulajdonképpen azt igazolta, hogy ilyen univerzális U turing gép nem létezik.

(D) Turing eredményének bizonyításvázlata

Tegyük fel hogy van ilyen U gép - ez azt jelenti, hogy van olyan U standard Turing gép aminek az input szalagjára egy tetszőleges $\mathcal{M}$ TM gép unáris kódját és a w bináris szót írva, U pontosan akkor áll meg ha $\mathcal{M}$ akceptálja a w szót.

A TM gépek előbb vázolt kódolásából kiindulva készítettünk egy táblázatot, ahol az n számnak megfelelő TM gép az m számnak megfelelő w szó hatására a szalagra egy olyan w szót ír, aminek a kettes számrendszerbeli értéke k . (Tehát $TM(n, m) = k$). Mivel egyes számoknak nem fognak TM gépek megfelelni, így egyes sorok üresen maradnak (lásd 1.Ábra) -ezt úgy tudjuk kiküszöbölni, hogy a TM gépeknek megfelelő számokat egy $i_1, i_2, \dots, i_k$ sorozatban helyezzük el és a sorokban lévő számok helyét a Turing gépeket most csak a $k = 1, 2, 3, \dots$ sorszámmukkal címkézzük meg. Így kapjuk a 2. Táblázatot (2 Ábra). Jól látható, hogy az első táblázatban bizonyos kockák üresen maradtak, a neki megfelelő 2. Táblázatba oda kérdőjeleket írtunk. Ez azt jelenti, hogy bizonyos szavak esetén nem tudjuk előre hogy a w szó hatására a sorhoz rendelt Turing gép megáll-e, vagy végtelen ciklusba kerül.

Ha az Univerzális U Turing gép létezik, akkor a segítségével ezt az utóbbi kérdést mindig el tudjuk dönteni, - így most ezekbe a kockákba -1 -et írunk ha TM gép végtelen ciklusba kerül, ellenkező esetben pedig a megállás után kapott w' bin. szó 2-es számrendszerbeli értékét. Ily módon minden kockába egy egész szám került (lásd 3. Ábra).

Így tehát egy $H(k, m)$ kétváltozós függvényt kapunk, amit a 3. Ábrán látható táblázat add meg. Értelmezzük most a $H^*(k, m) = H(k, m) + 1$ függvényt. Mivel ennek minden értéke most már egy nemnegatív egész szám, $H^*(k, m)$ nem más mint egy algoritmussal megadható - azaz rekurzív **egész** függvény. Definiáljuk most a $\Lambda(m) = H^*(m, m) = H(m, m) + 1$ egyváltozós függvényt. Mivel ez a függvény is rekurzív egész függvény, a tanultak alapján meg kell egyezzen egy alkalmasan megválasztott (standard) TM géphez tartozó egész függvénnyel. De ez a gép egy kell legyen a táblázatban felsorolt Turing gépek között, a neki megfelelő függvény pedig a táblázat egy megfelelő sorában kell megtalálható legyen. Ez viszont biztosan lehetetlen, mert a táblázat sorai a $H(-, m)$ alakú függvényeket tartalmazzák és ezek mindegyike legalább egy helyen különbözik a $\Lambda(m) = H(m, m) + 1$ függvénytől! Tehát ilyen függvény a táblázat egyik sorában sem szerepelhet. Így hát ellentmondásra jutottunk, ami azt jelenti, hogy a feltevésünk hibás: nem létezhet univerzális TM gép. $\square$