**ALGORITMUSOK ÉS BONYOLULTSÁGELMÉLET**

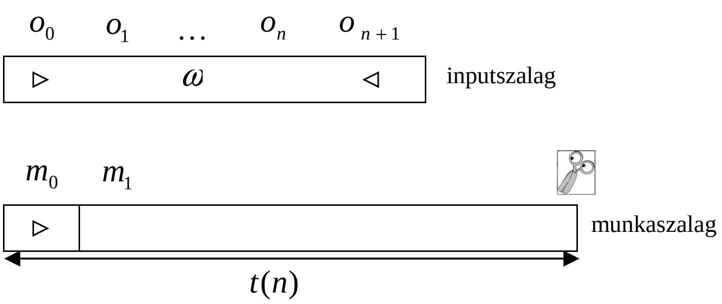
Matematika MSc hallgatók számára

# 6. Előadás

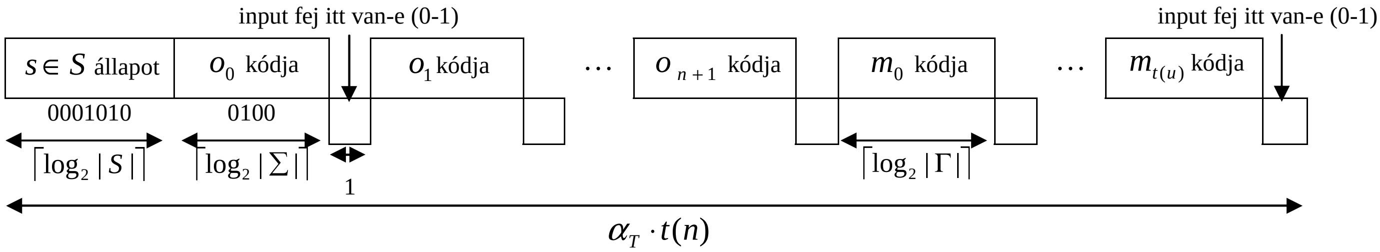
*Előadó: Hajnal Péter*

*Jegyzetelő: Krizsán Lívia* 2010. március 8.

**Definíció.** Legyen $T$ egy Turing-gép, $TIME(\omega;T) \le t(|\omega|)$ és $n = |\omega|$, ahol $t$ szép függvény. Legyen $\kappa$ egy tetszőleges konfigurációja $T$-nek $\omega$-n.

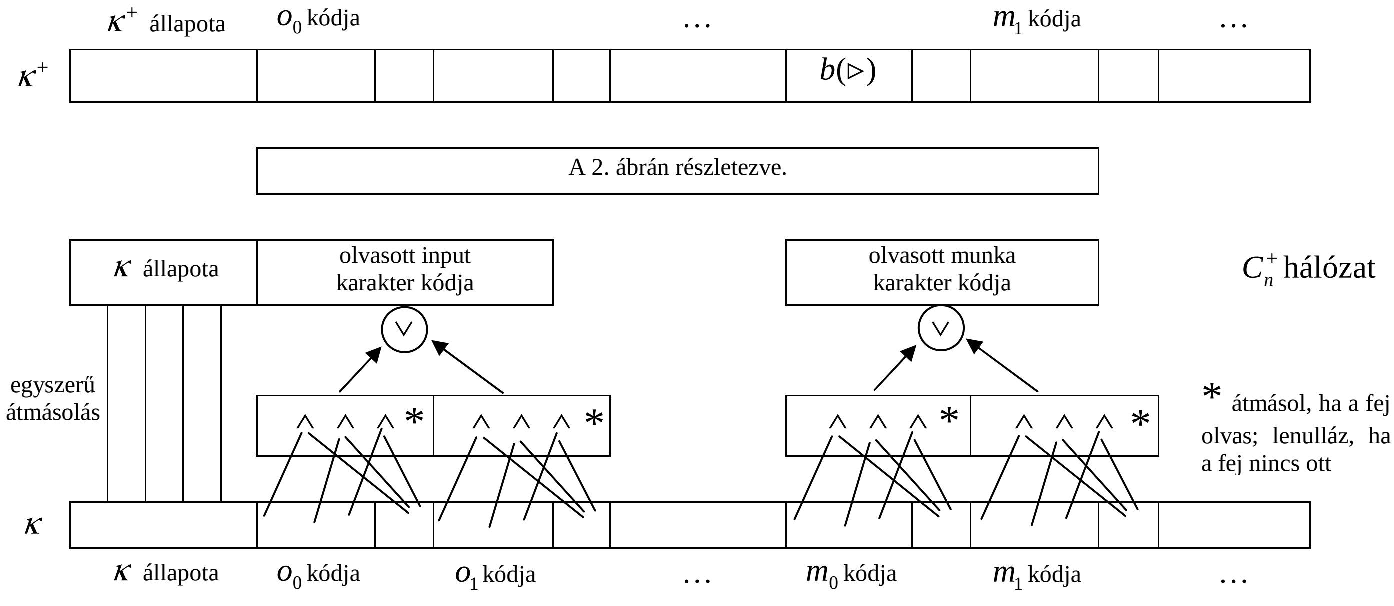



A $\kappa$ konfiguráció $b(\kappa)$-val jelölt *kódolás*a a {0, 1} *ABC*-ben:

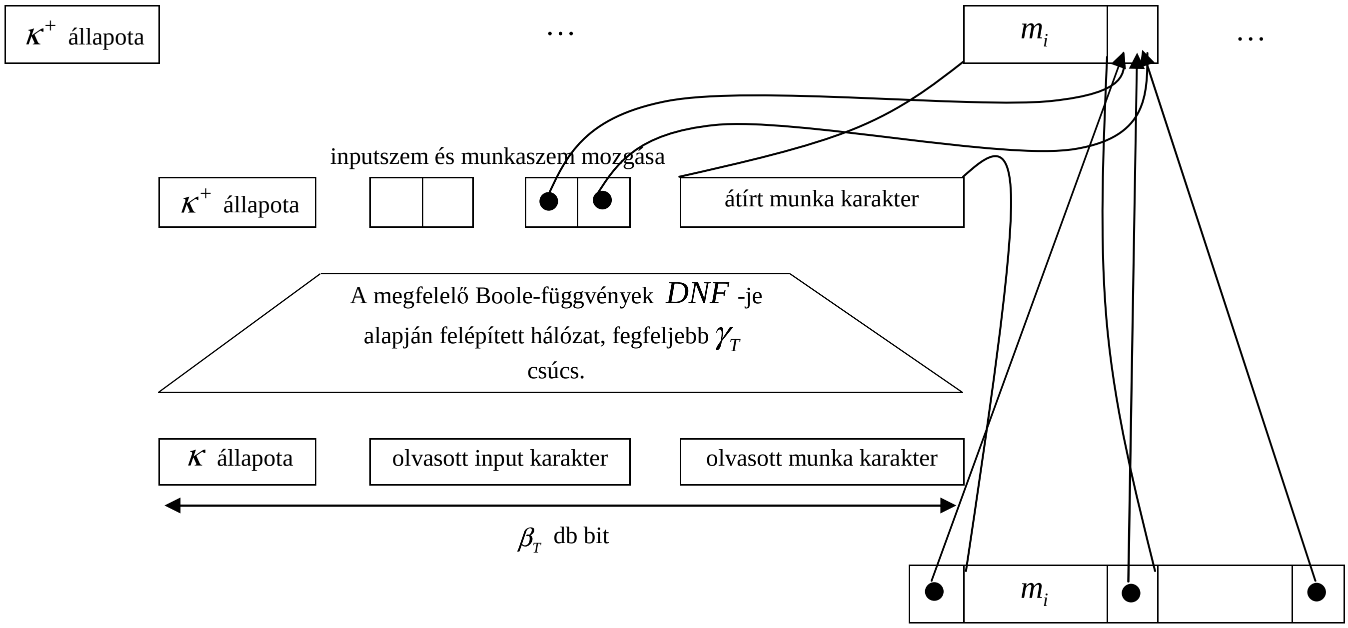



**Megjegyzés.** *START* állapot kódja megállapodás szerint $00\ldots0$, az *ELFOGAD* állapoté pedig $11\ldots1$.

**Emlékeztető.** A $\delta$ átmeneti függvény definiálja egy $\kappa$ konfiguráció $\kappa^+$ rákövetkezőjét. Kódolásunkkal a rákövetkező hozzárendelése egy $\{0,1\}^{\alpha_T f(n)} \to \{0,1\}^{\alpha_T f(n)}$ Boole-függvénnyel írható le: $b(\kappa) \to b(\kappa^+)$. Ez a Boole-függvény az alábbi hálózattal kiszámolható (a hálózatnak az output csúcsai a legfelső szinten vannak):




*1.ábra*

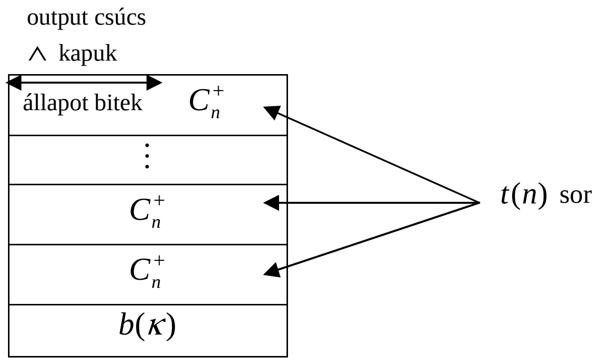



*2.ábra*

A kapott hálózatot jelöljük $C_n^+$-szal.

Ezek után a gép futásának eredményét is kiszámolhatjuk egy hálózattal (az elfogadás az $ELFOGAD \equiv 11\ldots1$ állapotba jutás).

<u>*Definíció*</u>: A fenti jelölésekkel definiáljuk a $C_n$ hálózatot a következőképp:




<u>*Tétel*</u>: *(i)* Legyen $T$ egy Turing-gép, $\omega$ egy $n$ hosszú input, $T(\omega) = \begin{cases} 1 & ha\ T\ ELFOGAD \\ 0 & ha\ T\ ELVET \end{cases}$,

$\kappa_\omega \in \{0,1\}^{\alpha_T f(n)}$, $C_n(\kappa_\omega)$ pedig a fent definiált hálózat által kiszámított bit.

Ekkor $T(\omega) = C_n(\kappa_\omega)$.

*(ii)* Ha $T$ egy polinomiális Turing-gép, akkor létezik olyan kiszámoló $R$ Turing-gép, amely $\omega$ ismeretében kiszámolja $b(\omega)$-t ($\omega$ bináris kódját) és $\lceil C_n \rceil$-t $LOGSPACE$ -ben.

<u>*Következmény*</u>: A HÁLÓZAT-KIÉRTÉKELÉS $P$ -teljes $\prec_L$ redukcióra.

*Bizonyítás*:

*(i)* Láttuk, hogy hálózat-kiértékelés $\in P$.

*(ii)* Legyen $L \in P$. Ekkor létezik olyan $T$ Turing-gép és $\alpha$ természetes szám, hogy $T$ eldönti $L$-et és időigénye $\leq \alpha \cdot n^\alpha$. Figyeljük meg, hogy

$$\omega \xrightarrow{R} b(\omega), \lceil C_n \rceil$$

$L$ -nek egy inputja hálózat-kiértékelés egy inputja

Így a fenti tételben szereplő $R$ Turing-gép és az (i) állításból adódóan $L \prec_L$ HÁLÓZAT-KIÉRTÉKELÉS. □

*Megjegyzés*: $b(\kappa)$, $C_n^+$ és $C_n$ hasonló módon definiálhatók nem-determinisztikus Turing-gépek és konfigurációk esetén is.

<u>Tétel</u> *(nem determinisztikus eset)*:

(i) Ha $T$ egy nem-determinisztikus Turing-gép, $\omega$ egy $n$ hosszú input, $T(\omega,\tau) = \begin{cases} 1 & ha\ T\ ELFOGAD \\ 0 & ha\ T\ NEM-STIMMEL \end{cases}$, $b(\tau) = (t_1, t_2, \ldots, t_{\beta_T n})$ ahol $t_i$-k adott tanúszalag-tartalom esetén vesznek fel $0-1$ értékeket, akkor $T(\omega,\tau) = C_n(\kappa_\omega, b(\tau))$.

(ii) $\left| C_n(\kappa_\omega, t_1, \ldots, t_{\beta_T n}) \right|$ $LOGSPACE$ -ben kiszámolható.

<u>Következmény</u>: $HÁLÓZAT-SAT$ $NP$ -teljes ($\prec_L$ redukcióra, és így $\prec_P$ redukcióra is).

<u>Definíció</u>: Legyen $V = \{x_1, \ldots, x_n\}$ és $\overline{V} = \{\neg x_1, \ldots, \neg x_n\}$. Ekkor az $L = V \cup \overline{V}$ halmaz elemeit *literál*oknak, a $C \subseteq L$ részhalmazokat pedig *klóz*oknak nevezzük.

*Megjegyzés*: Minden $CNF$ formula klózok egy $\{C_i\}_{i \in I}$ halmaza. Egy klózra úgy gondolunk, mint elemeinek/benne levő literáloknak $\vee$-gyal összekapcsolt formulája, míg a $CNF$ klózjainak $\wedge$-sel összekapcsolt formulája.

<u>Definíció</u>: $CNF-SAT$ probléma: Adott egy $\varphi$ $CNF$ formula. Döntsük el, hogy kielégíthető-e.

*Megállapodás*: A $CNF-SAT$ problémát az egyszerűség kedvéért mostantól csak $SAT$ -ként emlegetjük.

<u>Tétel</u>*(Cook, Levin)*: $SAT$ $NP$ -teljes.

*Bizonyítás*:

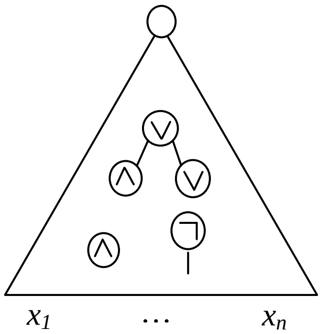
Egy $NP$ -teljességi eredményünk van. Ezt az alábbi séma szerint használhatjuk további $NP$ -teljességi eredmények igazolására:

$SAT \in NP$

$HÁLÓZAT-SAT \prec_P SAT$, továbbá $L \in NP \Rightarrow L \prec_P HÁLÓZAT-SAT$.

$L \in NP \Rightarrow L \prec_P SAT$

Legyen $C$ egy tetszőleges hálózat:




Minden $v \in V$ -hez rendeljünk hozzá egy $y_v$ változót, és írjuk fel a következő Boole-egyenletrendszert:

$$\begin{cases} y_v = x_i, & \text{ha } v\ i\text{-edik input} \\ y_v = y_u \vee y_w, & \text{ha } v\text{-t } u \text{ és } w \text{ vagy-kapuval való összekapcsolásával nyerjük} \\ y_v = y_u \wedge y_w, & \text{ha } v\text{-t } u \text{ és } w \text{ és-kapuval való összekapcsolásával nyerjük} \\ y_v = \neg y_u, & \text{ha } v\text{-t } u \text{ negálásával nyerjük.} \end{cases}$$

Az egyenletek mindegyike átírható egy $CNF$ formula kielégítésre. Csak az utolsó típusú egyenletet részletezzük:

$y_v = \neg y_u \equiv \{y_u, y_v\}$ egy db 0, egy db 1 $\equiv \{y_u, y_v\} \geq$ egy db 0, $\geq$ egy db 1 $\equiv$

$(y_u \vee y_v) \wedge (\neg y_u \vee \neg y_v)$ igaz

Ezt mindegyik egyenletre megtéve és a kapott formulákat $\wedge$-sel összekapcsolva kapjuk:

$$\text{egyenletrendszer megoldhatósága} \equiv \underbrace{\bigwedge \boxed{\begin{array}{c}\text{Minden egyenletre vele}\\ \text{ekvivalens } CNF\\ \text{formula}\end{array}}}_{\text{kielégíthető-e}}$$

$\lceil C \rceil$-hoz hozzárendeltünk egy $\varphi$ $CNF$ formulát. Ez $P$-ben kiszámolható.

$\lceil C \rceil \in HÁLÓZAT - SAT$ akkor és csak akkor teljesül, ha $\varphi \in SAT$. Azaz

$HÁLÓZAT - SAT \prec_P SAT$. □