

# Újelvű számítások az informatikában

---

Gazdag Zsolt

SZTE

## A kurzus vázlata

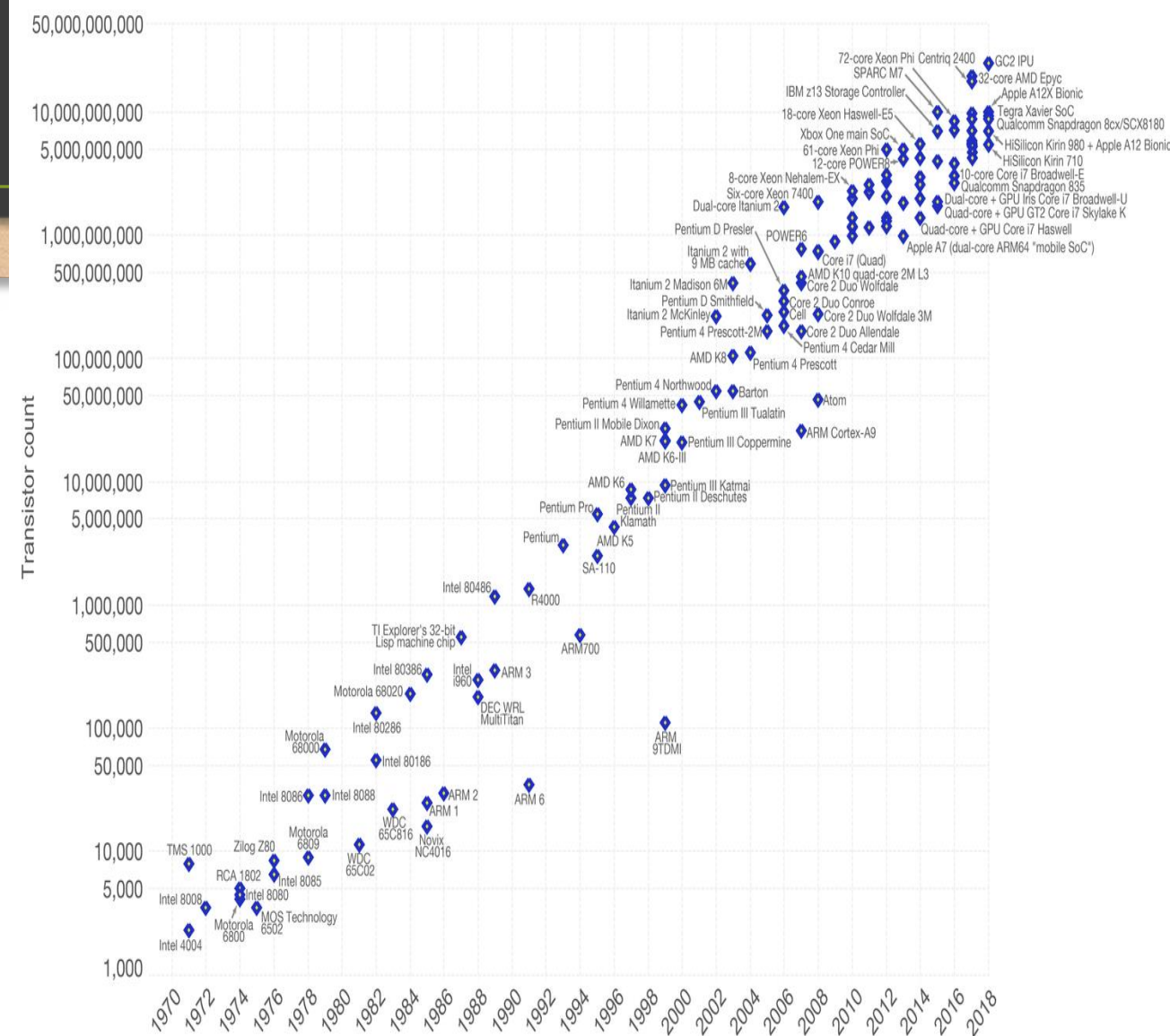
- Motiváció
- Klasszikus bonyolultságelmélet
- L-rendszerek
- Membrán számítások
- DNA számítások
- Kvantum számítások

# Miért érdekesek az új elví számítási modellek?

- **Moore-törvény:** A Neumann elven alapuló számítógépek számítási kapacitása kb. 2 évenként megduplázódik (a legolcsóbb elérhető komponenseket figyelembe véve is)
- A tranzisztorok mérete lassan eléri az atomi szintet – itt már a kvantumfizika szabályai érvényesülnek

## Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.



Data source: Wikipedia ([https://en.wikipedia.org/wiki/Transistor\\_count](https://en.wikipedia.org/wiki/Transistor_count))

The data visualization is available at OurWorldInData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

# Miért érdekesek az új elvű számítási modellek?

- Vannak nehezen megoldható problémák
  - A futási idő, rossz esetben, a bemenet méretével exponenciálisan arányosan növekszik:  
pl. Klikk, Sat, Utazóügynök/Hamilton út, Prímfelbontás
- Általában: az **NP-teljes** és ezeknél bonyolultabb problémák megoldása már nehéz
  - Később látni fogjuk, hogy mit értünk NP-teljes probléma alatt
- Miért nem segít a Moore-törvény?
- A megduplázódott számítási kapacitás csak annyit segít, hogy **eggyel nagyobb** méretű bemenetet tudunk kezelni ugyanannyi idő alatt
- Az NP-teljes problémák hatékonyan megoldhatók **nemdeterminisztikus Turing-gépekkel**
- A nemdeterminisztikus Turing-gép **nem realiztikus** számítási modell!

# Miért érdekesek az új elvű számítási modellek?

- A **természetben** megfigyelhetők olyan folyamatok, melyekkel valamilyen szinten **modellezhető** a nemdeterminisztikus Turing-gép számítási ereje
- Ezeket a folyamatok vizsgálata, modellezése a **természet-motiválta számítások** témakörébe tartozik
- Ide tartoznak az előadáson vizsgált modellek is: **membrán számítás, DNS számítás, kvantum számítás**
- A membránszámítás és a DNS számítás **formális nyelvi eszközökkel** modellezi a természetben lezajló folyamatokat

# A klasszikus bonyolultságelmélet

- Amiről ebben a részben szó lesz:
  - Formális nyelvi alapfogalmak
  - Zérusrendű logika
  - A Turing-gép
  - Klasszikus bonyolultság-elméleti osztályok
    - P, NP, NP-teljes, PSPACE, L, NL

# Formális nyelvek

- $\Sigma$  **ábécé**: véges, nemüres halmaz, pl.  $\Sigma = \{0,1\}$
- $\Sigma$ -**feletti szó**:  $\Sigma$ -beli betűk véges (akár 0 hosszú) sorozata, pl.: 00101
- $\Sigma^*$ : Az összes  $\Sigma$ -feletti szó halmaza
- $\varepsilon$ : **üres szó**,  $\varepsilon \in \Sigma^*$
- $|u|$ :  **$u$  hossza**,  $|u|_a$ :  $u$ -beli  $a$ -betűk száma
- $\Sigma$ -**feletti formális nyelv**:  $L \subseteq \Sigma^*$ , pl.:
  - $L_1 = \{00,11\}$ ,
  - $L_2 = \{u \in \{0,1\}^* \mid |u|_0 \text{ páros}\}$ ,
  - $L_3 = \{0^n 1^n \mid n \geq 0\}$ ,
  - $L_4 = \{u \in \{0,1\}^* \mid |u|_0 = |u|_1\}$ ,
  - $L_5 = \{u \in \{0,1\}^* \mid u\text{-ban nem szerepel a } 00 \text{ és az } 11 \text{ részszo}\}$

# Reguláris nyelvek

- **Műveletek** nyelveken:
  - **halmazelméleti:** komplementer, unió, metszet
  - **reguláris:**
    - unió
    - konkatenáció:  $L_1 \cdot L_2 = \{uv \mid u \in L_1, v \in L_2\}$
    - iteráció:  $L^* = \{u_1 \dots u_n \mid n \geq 0, u_1, \dots, u_n \in L\}$
- **Reguláris nyelvek:** egy betűből álló nyelvek + üres nyelv + a reguláris művelek (véges sokszor).
- Pl. a következő nyelvek regulárisak (a kapcsos zárójelet elhagyjuk):
  - $L_1 = \{00, 11\} \Rightarrow 00 \cup 11$
  - $L_2 = \{u \in \{0,1\}^* \mid |u|_0 \text{ páros}\} \Rightarrow 1^*(01^*01^*)^*$
  - $L_5 = \{u \in \{0,1\}^* \mid u\text{-ban nem szerepel a } 00 \text{ és az } 11 \text{ részszó}\} \Rightarrow (0 \cup \emptyset^*)(10)^*(1 \cup \emptyset^*)$

# Környezetfüggetlen nyelvtanok

- A környezetfüggetlen (röviden: CF) nyelvtan
  - egy  $G = (N, \Sigma, P, S)$  rendszer, ahol
    - $N$  a nemterminálisok,  $\Sigma$  pedig a terminálisok ábécéje ( $N \cap \Sigma = \emptyset$ );  $S$  a kezdő nemterminális;
    - $P$  pedig  $A \rightarrow w$  alakú átírási szabályok véges halmaza, ahol
      - $A$ : nemterminális,  $w$  pedig egy mondatforma, azaz egy tetszőleges  $(N \cup \Sigma)^*$ -beli szó
  - Ha  $\alpha, \beta$  mondatformák, akkor  $\alpha \Rightarrow_G \beta$  jelöli azt, hogy  $G$  egy lépésben levezeti  $\beta$ -t az  $\alpha$ -ból a következőképpen:
    - keres  $\alpha$ -ban egy  $A$  nemterminálist és  $P$ -ben egy  $A \rightarrow w$  szabályt, és
    - kicseréli  $\alpha$ -ban ezt az  $A$ -t  $w$ -re
  - Azt mondjuk, hogy  $G$  levezeti a  $\beta$ -t az  $\alpha$ -ból ( $\alpha, \beta$  mondatformák) ha  $\beta$  megkapható  $\alpha$ -ból az egy lépéses levezetés véges sokszori alkalmazásával

# Környezetfüggetlen nyelvtanok

- A  $G$  által **generált nyelv**: az összes olyan csak terminálisokból álló szó, amit  $G$  le tud vezetni az  $S$ -ből kiindulva
- **Példa**: Legyen  $G$  az a CF nyelvtan, melynek
  - nemterminálisai:  $S$  (így a kezdő nemterminális is  $S$ ),
  - terminálisai  $a, b$ ,
  - szabályai pedig  $S \rightarrow aSb, S \rightarrow \varepsilon$
  - Az  $a^3b^3$  szó levezetése  $S$ -ből:  $S \Rightarrow aSb \Rightarrow aaSbb \Rightarrow aaaSbbb \Rightarrow a^3b^3$
  - A generált nyelv: azon szavak halmaza, melyekben ugyanannyi  $a$  betű van, mint  $b$

# Chomsky hierarchia

- A **Chomsky-hierarchia** nyelvosztályai:
  - **Reguláris (REG) nyelvek**
    - Modellek: reguláris kifejezések, véges automaták, jobblinéáris nyelvtanok
    - Felhasználás: egyszerű gépek modellezése (kimenettel: protokollok megadása), mintaillesztés, lexikális elemzés
  - **Környezetfüggetlen (CF) nyelvek**
    - Modellek: környezetfüggetlen nyelvtanok, veremautomaták
    - Felhasználás: programozási nyelvek szintaxisa (attribútumokkal szemantika is), XML (DTD)
  - **Környezetfüggő (CS) nyelvek**
    - Modellek: környezetfüggő nyelvtanok, lineárisan korlátos Turing-gép
    - Felhasználás: gyakorlatilag minden hétköznapi probléma legfeljebb ilyen bonyolultságú
  - **Rekurzívan felsorolható (RE) nyelvek**
    - Modellek: általános nyelvtanok, Turing-gép
    - Felhasználás: elméleti szempontból fontosak (több nyelv mint eszköz)
- **Hierarchia:**  $REG \subset CF \subset CS \subset RE$

# Zérusrendű logika - Szintaxis

- **Ítéletváltozók:**  $Var = \{p, q, r, \dots\}$  (megszámlálhatóan végtelen halmaz)
- (Zérusrendű) **formulák**
  - Az ítéletváltozók
  - Ha  $F$  formula, akkor  $\neg F$  is az
  - Ha  $F$  és  $G$  formula, akkor  $(F \wedge G)$ ,  $(F \vee G)$  és  $(F \rightarrow G)$  is azok
  - Más formula nincs
- **Példa:**  $F = \neg(p \vee q) \rightarrow p$

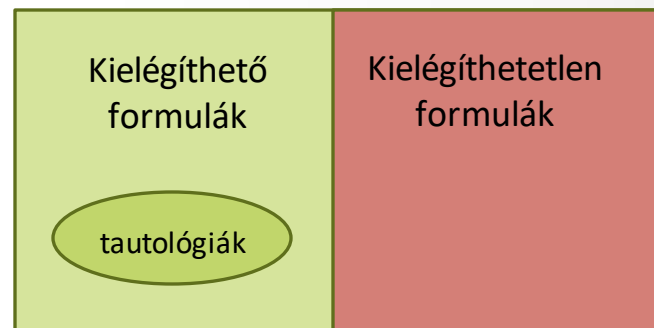
- **Szemantika:**

	$p$	$q$	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$
$I_1$	0	0	1	0	0	1
$I_2$	0	1	1	0	1	1
$I_3$	1	0	0	0	1	0
$I_4$	1	1	0	1	1	1

	$p$	$q$	$\neg(p \vee q)$	$\neg(p \vee q) \rightarrow p$
$I_1$	0	0	1	0
$I_2$	0	1	0	1
$I_3$	1	0	0	1
$I_4$	1	1	0	1

# Zérusrendű logika - Szemantika

- **Interpretáció:**  $I: Var \rightarrow \{0,1\}$ 
  - pl.:  $I(p) = 1, I(q) = 0$
- $I$  kiterjeszthető formulákra
  - pl.  $I(\neg(p \vee q) \rightarrow p) = 1$
- $I$  **kielégíti**  $F$ -et:  $I(F) = 1$
- **Szemantikus tulajdonságok:**
  - $F$  **kielégíthető**: van olyan  $I$ , ami kielégíti  $F$ -et
  - $F$  **kielégíthetetlen**, ha nem kielégíthető
  - $F$  **tautológia**, ha minden  $I$  kielégíti  $F$ -et
  - **Megjegyzés:**  $F$  tautológia  $\Leftrightarrow \neg F$  kielégíthetetlen
  - $F$  és  $G$  **ekvivalensek** ( $F \equiv G$ ) ha minden interpretációban ugyanaz az értékük



# Zérusrendű logika – Logikai következmény

- Logikai **következmény**
  - $\Sigma$  tetszőleges formulahalmaz,  $F$  formula
    - $\Sigma \models F$  : minden interpretáció ami kielégíti az összes  $\Sigma$ -beli formulát kielégíti  $F$ -et is
  - Példa:  $\{p \rightarrow q, q \rightarrow r\} \models p \rightarrow r$
- **Megjegyzés:**  $\Sigma \models F \Leftrightarrow \Sigma \cup \{\neg F\}$  kielégíthetetlen
- A szemantikus tulajdonságok **eldönthetők**:
  - igazságtábla, szemantikus fa, rezolúció
- A logikával kapcsolatos problémák általában **visszavezethetők** szemantikus tulajdonságok eldöntésére

# Zérusrendű logika – Konjunktív normálforma

- **Literál:** Ítéletváltozó vagy tagadott ítéletváltozó
- **Klóz:** véges sok literál  $\vee$ -kapcsolata
- **Konjunktív normálforma** (KNF): véges sok klóz  $\wedge$ -kapcsolata
- **Példa:**  $p \wedge (q \vee \neg p) \wedge \neg q$  egy KNF
- **Tétel:** minden  $F$ -hez megadható ekvivalens  $G$  KNF
  - **Bizonyítás:** Használjuk az alábbi ekvivalenciákat:
    - $F \rightarrow G \equiv \neg F \vee G$
    - De Morgan:  $\neg(F \vee G) \equiv \neg F \wedge \neg G$ ,  $\neg(F \wedge G) \equiv \neg F \vee \neg G$
    - Disztributivitás:  $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$  és  $(G \wedge H) \vee F \equiv (G \vee F) \wedge (H \vee F)$

# KNF-ek kielégíthetősége

- **Megjegyzés:** egy  $F$  KNF kielégíthető  $\Leftrightarrow$  van olyan interpretáció, ami minden  $F$ -beli klózt kielégít
- **SAT probléma:**
  - Adott:  $F$  KNF
  - Kérdés: kielégíthető-e  $F$ ?
- A **SAT megoldása:**
  - Egy  $F$  KNF legyen mostantól klózok halmaza, egy klóz pedig literálok halmaza
  - Egy  $\Sigma$  klózhalmazra, legyen
    - $\Sigma|_{p=1}$  az a klózhalmaz, amit úgy kapunk  $\Sigma$ -ból, hogy elhagyjuk belőle a  $p$ -t tartalmazó klózokat és a maradék klózokból a  $\neg p$ -t
    - $\Sigma|_{p=0}$  az a klózhalmaz, amit úgy kapunk  $\Sigma$ -ból, hogy elhagyjuk belőle a  $\neg p$ -t tartalmazó klózokat és a maradék klózokból a  $p$ -t

# KNF-ek kielégíthetősége

- Jelölje  $\square$  az **üres klózt**, azaz azt a klózt amiben nincs egy literál sem

- $\square$  kielégíthetetlen!

- Legyen  $\Sigma$  egy klózhalmaz

- Az alábbi  $A(\Sigma)$   $\Sigma$  kielégíthetőségét dönti el:

- function**  $A(\Sigma)$

- if  $\square \in \Sigma$  then return hamis

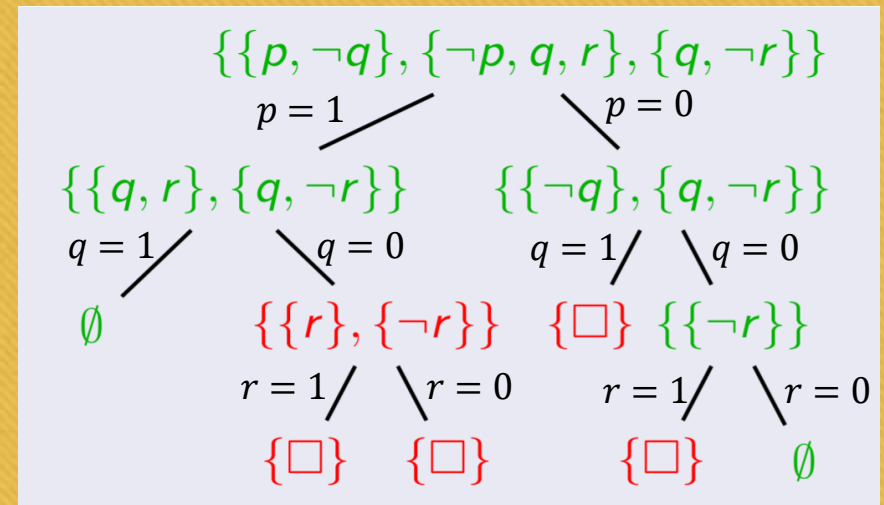
- if  $\Sigma = \emptyset$  then return igaz

- Legyen  $p$  egy változó

- return  $A(\Sigma|_{p=1}) \vee A(\Sigma|_{p=0})$

- $A(\Sigma)$  akkor és csak akkor ad vissza igaz-at ha  $\Sigma$  kielégíthető

Példa:



# A QBF probléma

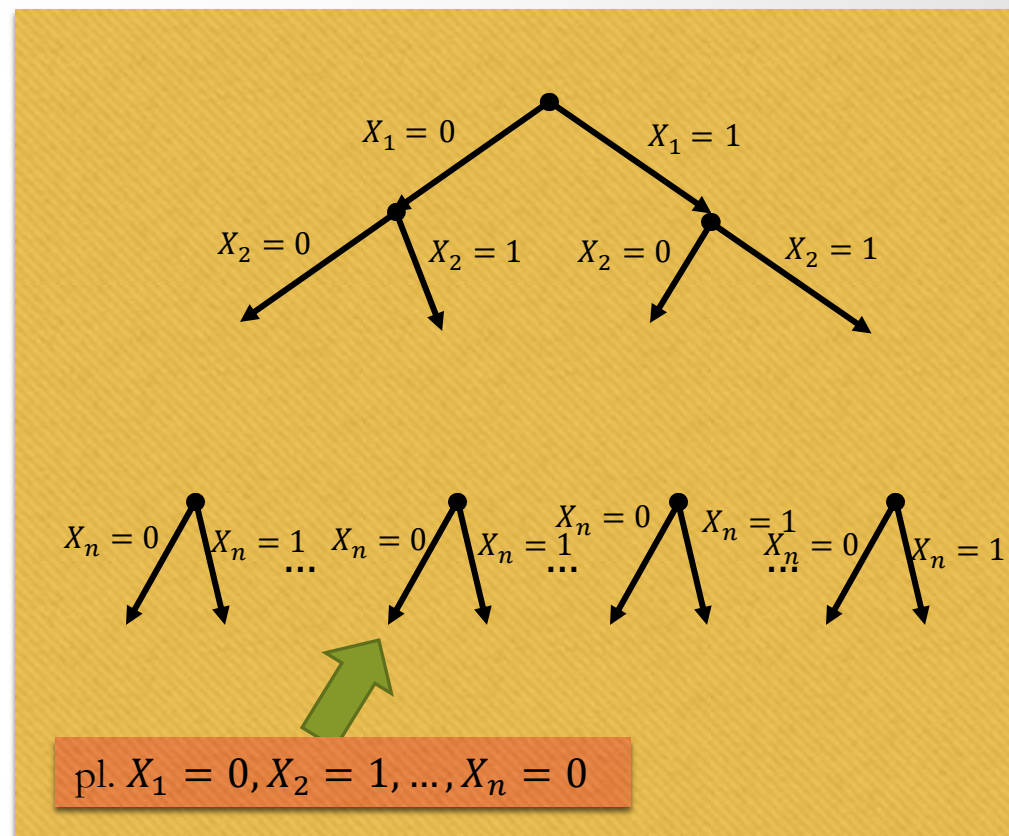
- Egy  $X_1, X_2, \dots, X_n$  ( $n$  egy pozitív páratlan szám) ítéletváltozók feletti **teljesen kvantifikált Boole formula** (QBF) a következő alakú:
  - $\varphi = \exists X_1 \forall X_2 \exists X_3 \dots \forall X_{n-1} \exists X_n F$ , ahol  $F$  egy a fenti változók feletti KNF
- Azt mondjuk, hogy  **$\varphi$  igaz**, ha a következő teljesül:
  - létezik  $X_1$  olyan értéke, hogy
  - akárhogy választom meg  $X_2$  értékét,
  - létezik  $X_3$  olyan értéke, hogy
  - ...
  - létezik  $X_n$  olyan értéke, hogy  $F$  igaz.

Példa:

$\exists X \forall Y \exists Z ((X \vee Y) \wedge (Y \vee Z) \wedge (\neg Y \vee \neg Z))$  igaz

# A QBF probléma megoldása

- Legyen  $\varphi = \exists X_1 \forall X_2 \exists X_3 \dots \forall X_{n-1} \exists X_n F$  egy QBF
- Hogyan lehet eldönteni, hogy  $\varphi$  igaz-e?
- Írjunk fel egy teljes  $T_\varphi$  bináris fát:
  - a gyökér van legfelül, ez a 0-ik szint
  - $n + 1$  szint van
  - az  $i$ -ik szintről az  $i + 1$ -re vezető élek ( $0 \leq i < n$ ) az  $X_i$  igazságértékelései
  - a leveleken ( $n + 1$ -ik szint) egy-egy interpretáció van



# A QBF probléma megoldása

- Címkezzük  $T_\varphi$  csúcsait a következőképpen:
  - a levelek címkéje legyen *igaz* vagy *hamis* annak megfelelően, hogy a megfelelő interpretáció kielégíti-e  $F$ -et
  - legyen  $i < n$  és tegyük fel, hogy az  $i$ -nél nagyobb sorszámú szinten lévő csúcsokat már címkéztük
  - legyen  $\alpha$  egy  $i$ -ik szinten lévő csúcs
    - ha  $i$  páros, akkor  $\alpha$  címkéje pontosan akkor *igaz* ha  $\alpha$  **valamelyik** gyermekének címkéje *igaz*
    - ha  $i$  páratlan, akkor  $\alpha$  címkéje pontosan akkor *igaz* ha  $\alpha$  **mindegyik** gyermekének címkéje *igaz*
- $\varphi$  akkor és csak akkor igaz ha  $T_\varphi$  gyökerének címkéje igaz

Példa:

$$\varphi = \exists X \forall Y \exists Z ((X \vee Y) \wedge (Y \vee Z) \wedge (\neg Y \vee \neg Z))$$

