Foundations of Complexity Theory

Lecture 6: Complete Problems II

November 25, 2026

Next Dates

Lecture (Wed 1:15pm)
Nov 25th Lecture 6: Complete problems II
Dec 2nd (dies academicus)
9th Lecture 7: NP-complete problems
16th Lecture 8: Complete problems III
23rd
30th

Lecture (Wed 1:15pm)
Jan 6th Lecture 9: Boolean circuits I
13th Lecture 10: Boolean circuits II
20th Lecture 11: Razborov's theorem I
27th
Feb 3rd Lecture 12: Razborov's theorem II

Overview

Contents

1. Basic complexity classes & their relations
2. Reductions & complete problems
3. Boolean circuits & Razborov's theorem
4. Randomization & interactive proof systems
5. Polynomial primality test

Complete Problems for **P**

$G = (N, \Sigma, S, P)$ ... Context-free grammar

Deciding nonemptiness

Is $L(G) \neq \emptyset$?

Complete Problems for **P**

$G = (N, \Sigma, S, P)$ . . . Context-free grammar

Deciding nonemptiness

Is $L(G) \neq \emptyset$?

Solution

1. Let $M \leftarrow \emptyset$ (all nonterminals unmarked)

Complete Problems for **P**

$G = (N, \Sigma, S, P)$ ... Context-free grammar

Deciding nonemptiness

Is $L(G) \neq \emptyset$?

Solution

1. Let $M \leftarrow \emptyset$ (all nonterminals unmarked)
2. Return yes if $S \in M$ (language nonempty if start nonterminal reached)

Complete Problems for P

$G = (N, \Sigma, S, P)$ ... Context-free grammar

Deciding nonemptiness

Is $L(G) \neq \emptyset$?

Solution

1. Let $M \leftarrow \emptyset$ (all nonterminals unmarked)
2. Return yes if $S \in M$ (language nonempty if start nonterminal reached)
3. $M' \leftarrow \{n \in N \mid \exists (n \to w) \in P : w \in (\Sigma \cup M)^*\}$
   (for all productions $n \to w$ with all nonterminals of w marked, mark n)

Complete Problems for P

$G = (N, \Sigma, S, P)$ ... Context-free grammar

Deciding nonemptiness

Is $L(G) \neq \emptyset$?

Solution

1. Let $M \leftarrow \emptyset$ (all nonterminals unmarked)
2. Return yes if $S \in M$ (language nonempty if start nonterminal reached)
3. $M' \leftarrow \{n \in N \mid \exists (n \to w) \in P : w \in (\Sigma \cup M)^*\}$
   (for all productions $n \to w$ with all nonterminals of w marked, mark n)
4. If $M \subsetneq M'$, then $M \leftarrow M'$ and back to step 2
   (if additional states were marked, then back to step 2)

Complete Problems for P

$G = (N, \Sigma, S, P)$ ... Context-free grammar

Deciding nonemptiness

Is $L(G) \neq \emptyset$?

Solution

1. Let $M \leftarrow \emptyset$ (all nonterminals unmarked)
2. Return yes if $S \in M$ (language nonempty if start nonterminal reached)
3. $M' \leftarrow \{n \in N \mid \exists (n \to w) \in P : w \in (\Sigma \cup M)^*\}$
   (for all productions $n \to w$ with all nonterminals of w marked, mark n)
4. If $M \subsetneq M'$, then $M \leftarrow M'$ and back to step 2
   (if additional states were marked, then back to step 2)
5. Return no

Complete Problems for **P**

Emptiness test for CFG

- Nonterminals $\{A, B, C, D, E, F, G, H\}$ with start nonterminal D
- Terminals $\Sigma = \{a, b\}$

$$G \to a \mid GG \mid EG \mid BG \mid DG$$
$$H \to \varepsilon \mid HH \mid HC \mid HB \mid HD$$
$$B \to b$$
$$D \to BB \mid DB \mid BD \mid DD$$
$$E \to GE \mid EE \mid BE \mid DE \mid GB \mid GD \mid EB \mid ED$$
$$C \to CH \mid CB \mid CC \mid CD \mid BH \mid DH \mid BC \mid DC$$
$$F \to GF \mid EF \mid BF \mid DF \mid GC \mid EC \mid GH \mid EH \mid FH \mid FB \mid FC \mid FD$$

Complete Problems for **P**

Emptiness test for CFG

- Nonterminals $\{A, B, C, D, E, F, G, H\}$ with start nonterminal D
- Terminals $\Sigma = \{a, b\}$

$$G \to a \mid GG \mid EG \mid BG \mid DG$$
$$H \to \varepsilon \mid HH \mid HC \mid HB \mid HD$$
$$B \to b$$
$$D \to BB \mid DB \mid BD \mid DD$$
$$E \to GE \mid EE \mid BE \mid DE \mid GB \mid GD \mid EB \mid ED$$
$$C \to CH \mid CB \mid CC \mid CD \mid BH \mid DH \mid BC \mid DC$$
$$F \to GF \mid EF \mid BF \mid DF \mid GC \mid EC \mid GH \mid EH \mid FH \mid FB \mid FC \mid FD$$

Complete Problems for **P**

Emptiness test for CFG

- Nonterminals $\{A, B, C, D, E, F, G, H\}$ with start nonterminal D
- Terminals $\Sigma = \{a, b\}$

$$G \to a \mid GG \mid EG \mid BG \mid DG$$
$$H \to \varepsilon \mid HH \mid HC \mid HB \mid HD$$
$$B \to b$$
$$D \to BB \mid DB \mid BD \mid DD$$
$$E \to GE \mid EE \mid BE \mid DE \mid GB \mid GD \mid EB \mid ED$$
$$C \to CH \mid CB \mid CC \mid CD \mid BH \mid DH \mid BC \mid DC$$
$$F \to GF \mid EF \mid BF \mid DF \mid GC \mid EC \mid GH \mid EH \mid FH \mid FB \mid FC \mid FD$$

Complete Problems for **P**

Emptiness test for CFG

- Nonterminals $\{A, B, C, D, E, F, G, H\}$ with start nonterminal D
- Terminals $\Sigma = \{a, b\}$

$$G \to a \mid GG \mid EG \mid BG \mid DG$$
$$H \to \varepsilon \mid HH \mid HC \mid HB \mid HD$$
$$B \to b$$
$$D \to BB \mid DB \mid BD \mid DD$$
$$E \to GE \mid EE \mid BE \mid DE \mid GB \mid GD \mid EB \mid ED$$
$$C \to CH \mid CB \mid CC \mid CD \mid BH \mid DH \mid BC \mid DC$$
$$F \to GF \mid EF \mid BF \mid DF \mid GC \mid EC \mid GH \mid EH \mid FH \mid FB \mid FC \mid FD$$

Complete Problems for **P**

Emptiness test for CFG

- Nonterminals $\{A, B, C, D, E, F, G, H\}$ with start nonterminal D
- Terminals $\Sigma = \{a, b\}$

$$G \to a \mid GG \mid EG \mid BG \mid DG$$
$$H \to \varepsilon \mid HH \mid HC \mid HB \mid HD$$
$$B \to b$$
$$D \to BB \mid DB \mid BD \mid DD$$
$$E \to GE \mid EE \mid BE \mid DE \mid GB \mid GD \mid EB \mid ED$$
$$C \to CH \mid CB \mid CC \mid CD \mid BH \mid DH \mid BC \mid DC$$
$$F \to GF \mid EF \mid BF \mid DF \mid GC \mid EC \mid GH \mid EH \mid FH \mid FB \mid FC \mid FD$$

Nonterminal D marked $\to$ nonempty language (e.g. $D \Rightarrow BB \Rightarrow^2 bb$)

Complete Problems for **P**

$L_{\mathrm{CFE}} = \{\mathrm{bin}(G) \mid G \text{ context-free grammar}, L(G) \neq \emptyset\}$

§6.1 Theorem (L_{CFE} is **P-complete)**

Nonemptiness problem L_{CFE} of context-free grammars is **P**-complete

Complete Problems for **P**

$L_{\mathrm{CFE}} = \{\mathrm{bin}(G) \mid G \text{ context-free grammar}, L(G) \neq \emptyset\}$

§6.1 Theorem (L_{CFE} is P-complete)

Nonemptiness problem L_{CFE} of context-free grammars is **P**-complete

Proof (1/4)

It should be known that $L_{\mathrm{CFE}} \in \mathbf{P}$. Let $L \in \mathbf{P}$ and $M = (Q, \Sigma, \Gamma, \Sigma', \delta, \square, q_0, q_+, q_-)$ be p-time-bounded deterministic TM for polynomial p with $L(M) = L$. Additionally, let $w = w_1 \cdots w_n \in \Sigma^*$ input. Wlog. suppose that M is 1-TM that copies input onto working tape and only works on working tape afterwards.

Complete Problems for **P**

$L_{\mathrm{CFE}} = \{\mathrm{bin}(G) \mid G \text{ context-free grammar}, L(G) \neq \emptyset\}$

§6.1 Theorem (L_{CFE} is P-complete)

Nonemptiness problem L_{CFE} of context-free grammars is **P**-complete

Proof (1/4)

It should be known that $L_{\mathrm{CFE}} \in \mathbf{P}$. Let $L \in \mathbf{P}$ and $M = (Q, \Sigma, \Gamma, \Sigma', \delta, \square, q_0, q_+, q_-)$ be p-time-bounded deterministic TM for polynomial p with $L(M) = L$. Additionally, let $w = w_1 \cdots w_n \in \Sigma^*$ input. Wlog. suppose that M is 1-TM that copies input onto working tape and only works on working tape afterwards. We mark current working tape position with state and consider alphabet $\Omega = \Gamma \cup (Q \times \Gamma)$. Configurations are then given by

$$K = \{\square\xi(q,\gamma)\zeta\square \mid q \in Q, \gamma \in \Gamma, \xi, \zeta \in \Gamma^*, |\xi\zeta| = 2p(n+2)\}$$

Complete Problems for **P**

Proof (2/4)

Initial configuration is $\kappa_0 = \Box^{p(n+2)+1}(q_0, w_1)w_2 \cdots w_n\Box^{p(n+2)-n+2}$.

Complete Problems for P

Proof (2/4)

Initial configuration is $\kappa_0 = \square^{p(n+2)+1}(q_0, w_1)w_2 \cdots w_n\square^{p(n+2)-n+2}$. Since M is deterministic and all changes are local, there exists function $s\colon \Omega^3 \to \Omega$ such that for all $\kappa, \kappa' \in \square\Omega^*\square$ with $|\kappa| = |\kappa'|$

1. $\kappa, \kappa' \in K$ and $\kappa \Rightarrow_M \kappa'$ iff
2. $\kappa \in K$ and $s(\kappa[i-1], \kappa[i], \kappa[i+1]) = \kappa'[i]$ for all $i \in \mathbb{Z}$ with $|i| \leq p(n+2)$

Complete Problems for P

Proof (2/4)

Initial configuration is $\kappa_0 = \square^{p(n+2)+1}(q_0, w_1)w_2 \cdots w_n\square^{p(n+2)-n+2}$. Since M is deterministic and all changes are local, there exists function $s\colon \Omega^3 \to \Omega$ such that for all $\kappa, \kappa' \in \square\Omega^*\square$ with $|\kappa| = |\kappa'|$

1. $\kappa, \kappa' \in K$ and $\kappa \Rightarrow_M \kappa'$ iff
2. $\kappa \in K$ and $s(\kappa[i-1], \kappa[i], \kappa[i+1]) = \kappa'[i]$ for all $i \in \mathbb{Z}$ with $|i| \leq p(n+2)$

We construct context-free grammar $G_w = (N, \emptyset, S, P)$ such that

- $N = \{S\} \cup \{\langle a, t, i\rangle \in \Omega \times \mathbb{N} \times \mathbb{Z} \mid t \leq p(n+2),\ |i| \leq p(n+2)+1\}$

Complete Problems for P

Proof (2/4)

Initial configuration is $\kappa_0 = \square^{p(n+2)+1}(q_0, w_1)w_2 \cdots w_n\square^{p(n+2)-n+2}$. Since M is deterministic and all changes are local, there exists function $s\colon \Omega^3 \to \Omega$ such that for all $\kappa, \kappa' \in \square\Omega^*\square$ with $|\kappa| = |\kappa'|$

1. $\kappa, \kappa' \in K$ and $\kappa \Rightarrow_M \kappa'$ iff
2. $\kappa \in K$ and $s(\kappa[i-1], \kappa[i], \kappa[i+1]) = \kappa'[i]$ for all $i \in \mathbb{Z}$ with $|i| \leq p(n+2)$

We construct context-free grammar $G_w = (N, \emptyset, S, P)$ such that

- $N = \{S\} \cup \{\langle a, t, i\rangle \in \Omega \times \mathbb{N} \times \mathbb{Z} \mid t \leq p(n+2),\ |i| \leq p(n+2)+1\}$
- and the following productions
  - $S \to \langle (q_+, \gamma), t, i\rangle$ for all $\gamma \in \Gamma$, $t \leq p(n+2)$ and $|i| \leq p(n+2)+1$
    (Generation of accepting configuration after t steps)

Complete Problems for P

Proof (2/4)

Initial configuration is $\kappa_0 = \square^{p(n+2)+1}(q_0, w_1)w_2 \cdots w_n\square^{p(n+2)-n+2}$. Since M is deterministic and all changes are local, there exists function $s\colon \Omega^3 \to \Omega$ such that for all $\kappa, \kappa' \in \square\Omega^*\square$ with $|\kappa| = |\kappa'|$

1. $\kappa, \kappa' \in K$ and $\kappa \Rightarrow_M \kappa'$ iff
2. $\kappa \in K$ and $s(\kappa[i-1], \kappa[i], \kappa[i+1]) = \kappa'[i]$ for all $i \in \mathbb{Z}$ with $|i| \leq p(n+2)$

We construct context-free grammar $G_w = (N, \emptyset, S, P)$ such that

- $N = \{S\} \cup \{\langle a, t, i\rangle \in \Omega \times \mathbb{N} \times \mathbb{Z} \mid t \leq p(n+2),\ |i| \leq p(n+2)+1\}$
- and the following productions
  - $S \to \langle (q_+, \gamma), t, i\rangle$ for all $\gamma \in \Gamma$, $t \leq p(n+2)$ and $|i| \leq p(n+2)+1$
    (Generation of accepting configuration after t steps)
  - $\langle s(a,b,c), t+1, i\rangle \to \langle a, t, i-1\rangle \langle b, t, i\rangle \langle c, t, i+1\rangle$ for all $a, b, c \in \Omega$, $t \leq p(n+2)-1$ and $|i| \leq p(n+2)$
    (Extension to previous configuration)

Complete Problems for **P**

Proof (3/4)

The following productions terminate the derivation

- $\langle \square, 0, i \rangle \to \varepsilon$ and $\langle \square, t, p(n+2)+1 \rangle \to \varepsilon$ and $\langle \square, t, -(p(n+2)+1) \rangle \to \varepsilon$
  for all $t \leq p(n+2)$ and $i \in [-p(n+2), p(n+2)] \setminus [0, n-1]$
  (Erase blanks)
- $\langle (q_0, w_1), 0, 0 \rangle \to \varepsilon$ and $\langle w_{i+1}, 0, i \rangle \to \varepsilon$ for all $1 \leq i \leq n-1$
  (Erase initial configuration)

Complete Problems for P

Proof (3/4)

The following productions terminate the derivation

- $\langle \square, 0, i \rangle \to \varepsilon$ and $\langle \square, t, p(n+2)+1 \rangle \to \varepsilon$ and $\langle \square, t, -(p(n+2)+1) \rangle \to \varepsilon$ for all $t \leq p(n+2)$ and $i \in [-p(n+2), p(n+2)] \setminus [0, n-1]$ (Erase blanks)
- $\langle (q_0, w_1), 0, 0 \rangle \to \varepsilon$ and $\langle w_{i+1}, 0, i \rangle \to \varepsilon$ for all $1 \leq i \leq n-1$ (Erase initial configuration)

We can construct this grammar in logarithmic space. It remains to show that $L(G_w) \neq \emptyset$ iff $w \in L$. Let $\kappa_0 \Rightarrow_M \cdots \Rightarrow_M \kappa_m$ the single computation on input w.

Complete Problems for P

Proof (3/4)

The following productions terminate the derivation

- $\langle \square, 0, i \rangle \to \varepsilon$ and $\langle \square, t, p(n+2)+1 \rangle \to \varepsilon$ and $\langle \square, t, -(p(n+2)+1) \rangle \to \varepsilon$ for all $t \leq p(n+2)$ and $i \in [-p(n+2), p(n+2)] \setminus [0, n-1]$ (Erase blanks)
- $\langle (q_0, w_1), 0, 0 \rangle \to \varepsilon$ and $\langle w_{i+1}, 0, i \rangle \to \varepsilon$ for all $1 \leq i \leq n-1$ (Erase initial configuration)

We can construct this grammar in logarithmic space. It remains to show that $L(G_w) \neq \emptyset$ iff $w \in L$. Let $\kappa_0 \Rightarrow_M \cdots \Rightarrow_M \kappa_m$ the single computation on input w. We show that for all $t \leq m$ and $i \in \mathbb{Z}$ with $|i| \leq p(n+2)+1$

$$\langle a, t, i \rangle \Rightarrow_{G_w}^* \varepsilon \qquad \text{iff} \qquad \kappa_t[i] = a$$

Complete Problems for P

Proof (3/4)

The following productions terminate the derivation

- $\langle \square, 0, i \rangle \to \varepsilon$ and $\langle \square, t, p(n+2)+1 \rangle \to \varepsilon$ and $\langle \square, t, -(p(n+2)+1) \rangle \to \varepsilon$ for all $t \leq p(n+2)$ and $i \in [-p(n+2), p(n+2)] \setminus [0, n-1]$ (Erase blanks)
- $\langle (q_0, w_1), 0, 0 \rangle \to \varepsilon$ and $\langle w_{i+1}, 0, i \rangle \to \varepsilon$ for all $1 \leq i \leq n-1$ (Erase initial configuration)

We can construct this grammar in logarithmic space. It remains to show that $L(G_w) \neq \emptyset$ iff $w \in L$. Let $\kappa_0 \Rightarrow_M \cdots \Rightarrow_M \kappa_m$ the single computation on input w. We show that for all $t \leq m$ and $i \in \mathbb{Z}$ with $|i| \leq p(n+2)+1$

$$\langle a, t, i \rangle \Rightarrow_{G_w}^* \varepsilon \qquad \text{iff} \qquad \kappa_t[i] = a$$

Let $\kappa_t[i] = a$. For $t = 0$ or $|i| > p(n+2)$ the statement trivially holds.

Complete Problems for **P**

Proof (4/4)

Let $t > 0$ and $|i| \leq p(n)$. Then $\kappa_t[i] = s(\kappa_{t-1}[i-1], \kappa_{t-1}[i], \kappa_{t-1}[i+1])$. By induction hypothesis $\langle \kappa_{t-1}[\ell], t-1, \ell \rangle \Rightarrow^*_{G_w} \varepsilon$ for $\ell \in \{i-1, i, i+1\}$.

Complete Problems for **P**

Proof (4/4)

Let $t > 0$ and $|i| \leq p(n)$. Then $\kappa_t[i] = s(\kappa_{t-1}[i-1], \kappa_{t-1}[i], \kappa_{t-1}[i+1])$. By induction hypothesis $\langle \kappa_{t-1}[\ell], t-1, \ell \rangle \Rightarrow^*_{G_w} \varepsilon$ for $\ell \in \{i-1, i, i+1\}$. Thus $\langle \kappa_t[i], t, i \rangle \Rightarrow^*_{G_w} \varepsilon$ utilizing the production

$$\langle \kappa_t[i], t, i \rangle \to \langle \kappa_{t-1}[i-1], t-1, i-1 \rangle \langle \kappa_{t-1}[i], t-1, i \rangle \langle \kappa_{t-1}[i+1], t-1, i+1 \rangle$$

Complete Problems for **P**

Proof (4/4)

Let $t > 0$ and $|i| \leq p(n)$. Then $\kappa_t[i] = s(\kappa_{t-1}[i-1], \kappa_{t-1}[i], \kappa_{t-1}[i+1])$. By induction hypothesis $\langle \kappa_{t-1}[\ell], t-1, \ell \rangle \Rightarrow^*_{G_w} \varepsilon$ for $\ell \in \{i-1, i, i+1\}$. Thus $\langle \kappa_t[i], t, i \rangle \Rightarrow^*_{G_w} \varepsilon$ utilizing the production

$$\langle \kappa_t[i], t, i \rangle \to \langle \kappa_{t-1}[i-1], t-1, i-1 \rangle \langle \kappa_{t-1}[i], t-1, i \rangle \langle \kappa_{t-1}[i+1], t-1, i+1 \rangle$$

Let $\langle a, t, i \rangle \Rightarrow^*_{G_w} \varepsilon$. The cases $t = 0$ or $|i| > p(n+2)$ are again trivial. Let $t > 0$ and $|i| \leq p(n+2)$. There exists production

$$\langle a, t, i \rangle \to \langle b, t-1, i-1 \rangle \langle c, t-1, i \rangle \langle d, t-1, i+1 \rangle \in P$$

and by induction hypothesis $\kappa_{t-1}[i-1] = b$, $\kappa_{t-1}[i] = c$ and $\kappa_{t-1}[i+1] = d$.

Complete Problems for P

Proof (4/4)

Let $t > 0$ and $|i| \leq p(n)$. Then $\kappa_t[i] = s(\kappa_{t-1}[i-1], \kappa_{t-1}[i], \kappa_{t-1}[i+1])$. By induction hypothesis $\langle \kappa_{t-1}[\ell], t-1, \ell \rangle \Rightarrow^*_{G_w} \varepsilon$ for $\ell \in \{i-1, i, i+1\}$. Thus $\langle \kappa_t[i], t, i \rangle \Rightarrow^*_{G_w} \varepsilon$ utilizing the production

$$\langle \kappa_t[i], t, i \rangle \to \langle \kappa_{t-1}[i-1], t-1, i-1 \rangle \langle \kappa_{t-1}[i], t-1, i \rangle \langle \kappa_{t-1}[i+1], t-1, i+1 \rangle$$

Let $\langle a, t, i \rangle \Rightarrow^*_{G_w} \varepsilon$. The cases $t = 0$ or $|i| > p(n+2)$ are again trivial. Let $t > 0$ and $|i| \leq p(n+2)$. There exists production

$$\langle a, t, i \rangle \to \langle b, t-1, i-1 \rangle \langle c, t-1, i \rangle \langle d, t-1, i+1 \rangle \in P$$

and by induction hypothesis $\kappa_{t-1}[i-1] = b$, $\kappa_{t-1}[i] = c$ and $\kappa_{t-1}[i+1] = d$. Hence

$$\kappa_t[i] = s(\kappa_{t-1}[i-1], \kappa_{t-1}[i], \kappa_{t-1}[i+1]) = s(b, c, d) = a$$

With this auxiliary result the main statement is easy to prove. □

Complete Problems for **P**

Illustration: Consider derivation of det. TM

$$\square\square(q_0, a)b\square\square \Rightarrow_M \square\square b(q_0, b)\square\square \Rightarrow_M \square\square ba(q_0, \square)\square \Rightarrow_M \square\square b(q_+, a)\square\square$$

Complete Problems for **P**

Illustration: Consider derivation of det. TM

$$\Box\Box(q_0, a)b\Box\Box \Rightarrow_M \Box\Box b(q_0, b)\Box\Box \Rightarrow_M \Box\Box ba(q_0, \Box)\Box \Rightarrow_M \Box\Box b(q_+, a)\Box\Box$$

Corresponding derivation of context-free grammar G is

$$S \Rightarrow_G \langle (q_+, a), 3, 1\rangle \Rightarrow_G \langle b, 2, 0\rangle \langle a, 2, 1\rangle \langle (q_0, \Box), 2, 2\rangle$$

Complete Problems for **P**

Illustration: Consider derivation of det. TM

$$\Box\Box(q_0, a)b\Box\Box \Rightarrow_M \Box\Box b(q_0, b)\Box\Box \Rightarrow_M \Box\Box ba(q_0, \Box)\Box \Rightarrow_M \Box\Box b(q_+, a)\Box\Box$$

Corresponding derivation of context-free grammar G is

$$\begin{aligned} S &\Rightarrow_G \langle (q_+, a), 3, 1\rangle \Rightarrow_G \langle b, 2, 0\rangle \langle a, 2, 1\rangle \langle (q_0, \Box), 2, 2\rangle \\ &\Rightarrow_G^3 \langle \Box, 1, -1\rangle \langle b, 1, 0\rangle \langle (q_0, b), 1, 1\rangle \\ &\quad \langle b, 1, 0\rangle \langle (q_0, b), 1, 1\rangle \langle \Box, 1, 2\rangle \\ &\quad \langle (q_0, b), 1, 1\rangle \langle \Box, 1, 2\rangle \langle \Box, 1, 3\rangle \end{aligned}$$

Complete Problems for **P**

Illustration: Consider derivation of det. TM

$$\Box\Box(q_0, a)b\Box\Box \Rightarrow_M \Box\Box b(q_0, b)\Box\Box \Rightarrow_M \Box\Box ba(q_0, \Box)\Box \Rightarrow_M \Box\Box b(q_+, a)\Box\Box$$

Corresponding derivation of context-free grammar G is

$$\begin{aligned}
S &\Rightarrow_G \langle (q_+, a), 3, 1\rangle \Rightarrow_G \langle b, 2, 0\rangle \langle a, 2, 1\rangle \langle (q_0, \Box), 2, 2\rangle \\
&\Rightarrow_G^3 \langle \Box, 1, -1\rangle \langle b, 1, 0\rangle \langle (q_0, b), 1, 1\rangle \\
&\qquad \langle b, 1, 0\rangle \langle (q_0, b), 1, 1\rangle \langle \Box, 1, 2\rangle \\
&\qquad \langle (q_0, b), 1, 1\rangle \langle \Box, 1, 2\rangle \langle \Box, 1, 3\rangle \\
&\Rightarrow_G^8 \langle \Box,0,-2\rangle \langle \Box,0,-1\rangle \langle (q_0,a),0,0\rangle \langle \Box,0,-1\rangle \langle (q_0,a),0,0\rangle \langle b,0,1\rangle \langle (q_0,a),0,0\rangle \langle b,0,1\rangle \langle \Box,0,2\rangle \\
&\qquad \langle \Box,0,-1\rangle \langle (q_0,a),0,0\rangle \langle b,0,1\rangle \langle (q_0,a),0,0\rangle \langle b,0,1\rangle \langle \Box,0,2\rangle \langle b,0,1\rangle \langle \Box,0,2\rangle \langle \Box,0,3\rangle \\
&\qquad \langle (q_0,a),0,0\rangle \langle b,0,1\rangle \langle \Box,0,2\rangle \langle b,0,1\rangle \langle \Box,0,2\rangle \langle \Box,0,3\rangle \langle \Box,1,3\rangle
\end{aligned}$$

Complete Problems for **P**

Illustration: Consider derivation of det. TM

$$\Box\Box(q_0,a)b\Box\Box \Rightarrow_M \Box\Box b(q_0,b)\Box\Box \Rightarrow_M \Box\Box ba(q_0,\Box)\Box \Rightarrow_M \Box\Box b(q_+,a)\Box\Box$$

Corresponding derivation of context-free grammar G is

$$\begin{aligned}
S &\Rightarrow_G \langle (q_+,a),3,1\rangle \Rightarrow_G \langle b,2,0\rangle\langle a,2,1\rangle\langle (q_0,\Box),2,2\rangle \\
&\Rightarrow_G^3 \langle \Box,1,-1\rangle\langle b,1,0\rangle\langle (q_0,b),1,1\rangle \\
&\qquad \langle b,1,0\rangle\langle (q_0,b),1,1\rangle\langle \Box,1,2\rangle \\
&\qquad \langle (q_0,b),1,1\rangle\langle \Box,1,2\rangle\langle \Box,1,3\rangle \\
&\Rightarrow_G^8 \langle \Box,0,-2\rangle\langle \Box,0,-1\rangle\langle (q_0,a),0,0\rangle\langle \Box,0,-1\rangle\langle (q_0,a),0,0\rangle\langle b,0,1\rangle\langle (q_0,a),0,0\rangle\langle b,0,1\rangle\langle \Box,0,2\rangle \\
&\qquad \langle \Box,0,-1\rangle\langle (q_0,a),0,0\rangle\langle b,0,1\rangle\langle (q_0,a),0,0\rangle\langle b,0,1\rangle\langle \Box,0,2\rangle\langle b,0,1\rangle\langle \Box,0,2\rangle\langle \Box,0,3\rangle \\
&\qquad \langle (q_0,a),0,0\rangle\langle b,0,1\rangle\langle \Box,0,2\rangle\langle b,0,1\rangle\langle \Box,0,2\rangle\langle \Box,0,3\rangle\langle \Box,1,3\rangle \\
&\Rightarrow_G^{25} \varepsilon
\end{aligned}$$

Complete Problems for **P**

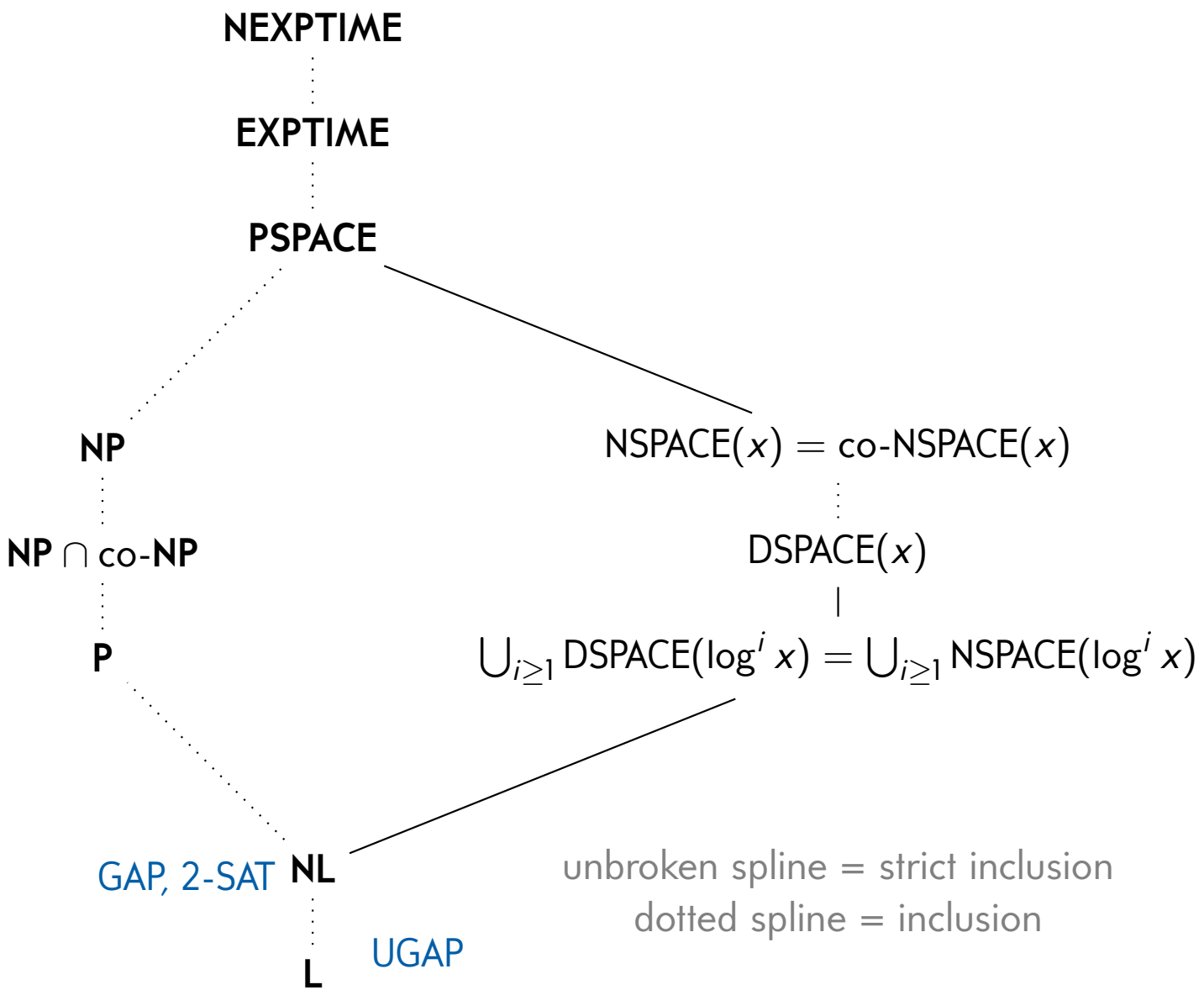
Notes

- No “simple” characterization via logic available
- (Completeness relevant due to log-space reductions)

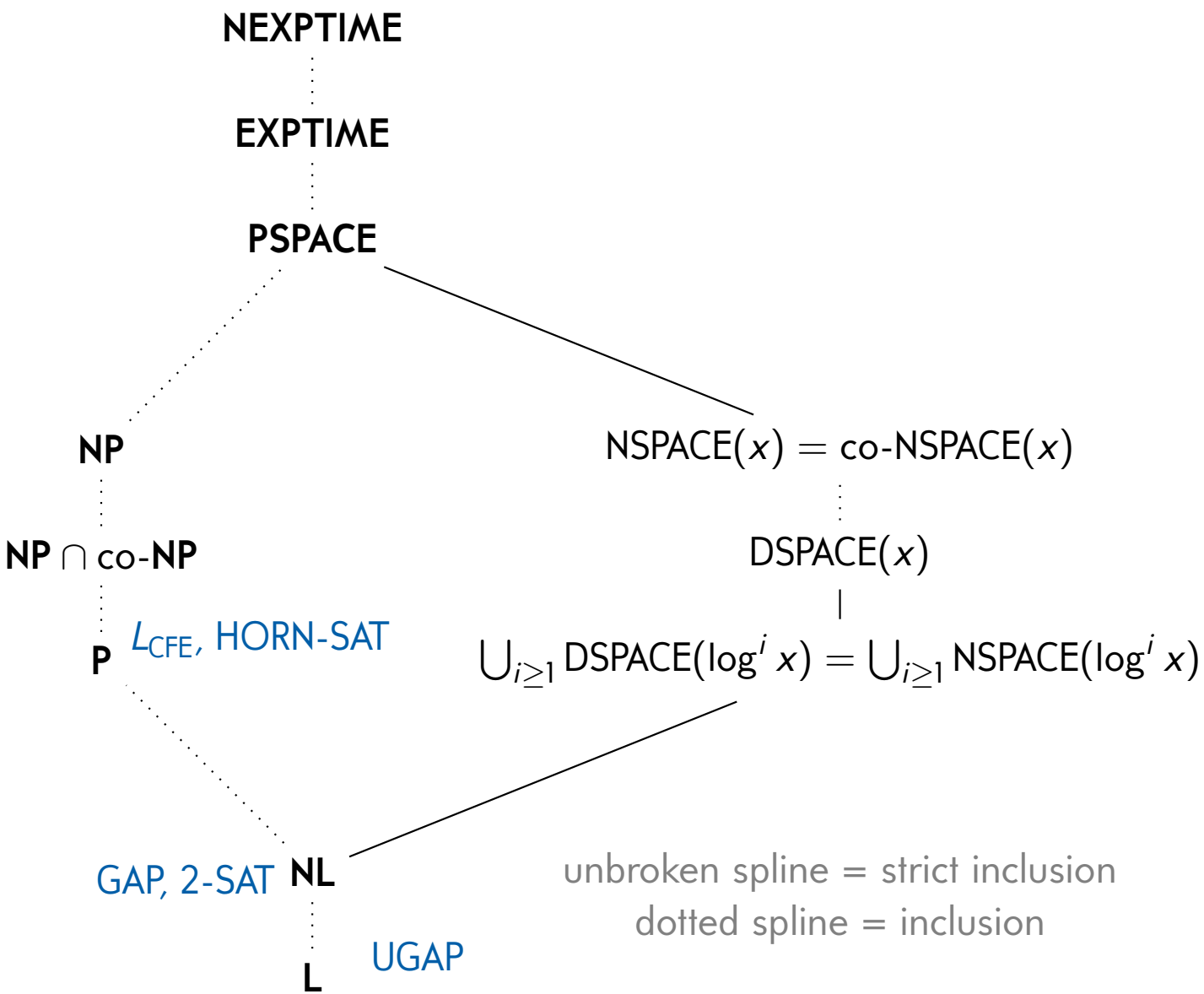
Additional complete problem

- Satisfiability of Horn formulas (HORN-SAT)

Complextiy Classes



Complextiy Classes



Class NP ∩ co-NP

§6.2 Theorem (Fermat's little theorem)

Nonnegative integer $n \in \mathbb{N}$ is prime iff
exists nonnegative integer $x \in \mathbb{N}$ such that $x \leq n-1$

- $x^{n-1} \equiv 1 \bmod n$ and
- $x^i \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, n-2\}$

Pierre de Fermat (* 1607; † 1665)

- French mathematician & lawyer
- Famous number theorist of 17th century
- Produced statements of theorems
  first proof of little theorem provided by Euler



Class **NP** ∩ **co-NP**

$$\text{PRIM} = \{w \in 1\{0,1\}^* \mid w \text{ is binary encoding of prime}\}$$

(PRIM ∈ **P** is known)

§6.3 Theorem

PRIM ∈ **NP** ∩ **co-NP**

Class NP ∩ co-NP

$$\text{PRIM} = \{w \in 1\{0,1\}^* \mid w \text{ is binary encoding of prime}\}$$

(PRIM ∈ **P** is known)

§6.3 Theorem

PRIM ∈ **NP** ∩ **co-NP**

Proof (1/5)

We first prove PRIM ∈ **co-NP**; i.e. $\overline{\text{PRIM}} \in$ **NP**. On input $w \in \{0,1\}^*$ we first check whether $w \in 0\{0,1\}^*$ and accept in this case. Otherwise guess $u, v \in 1\{0,1\}^+$ with $|u| \leq |w| \geq |v|$ and check in polynomial time whether $u \cdot v = w$ (multiplication of binary numbers). If so, then we accept (obviously w represents non-prime). Otherwise we reject.

Proof (2/5)

It remains to prove PRIM ∈ **NP**. We consider the following nondeterministic primality algorithm with input n

1. Accept if $n \in \{2, 3\}$

Proof (2/5)

It remains to prove PRIM $\in$ **NP**. We consider the following nondeterministic primality algorithm with input n

1. Accept if $n \in \{2, 3\}$
2. Guess $2 \leq k \leq \log n$ and $2 \leq p_i \leq n-1$ for all $1 \leq i \leq k$
3. Check whether $\prod_{i=1}^{k} p_i = n-1$ (otherwise reject)

Proof (2/5)

It remains to prove PRIM $\in$ **NP**. We consider the following nondeterministic primality algorithm with input n

1. Accept if $n \in \{2, 3\}$
2. Guess $2 \leq k \leq \log n$ and $2 \leq p_i \leq n-1$ for all $1 \leq i \leq k$
3. Check whether $\prod_{i=1}^{k} p_i = n-1$ (otherwise reject)
4. Check recursively whether p_i prime for all $i \in \{1, \ldots, k\}$

Proof (2/5)

It remains to prove PRIM $\in$ **NP**. We consider the following nondeterministic primality algorithm with input n

1. Accept if $n \in \{2, 3\}$
2. Guess $2 \leq k \leq \log n$ and $2 \leq p_i \leq n-1$ for all $1 \leq i \leq k$
3. Check whether $\prod_{i=1}^{k} p_i = n-1$ (otherwise reject)
4. Check recursively whether p_i prime for all $i \in \{1, \ldots, k\}$
5. Guess $z \in \mathbb{N}$ with $z \leq n-1$ and check whether $z^{n-1} \equiv 1 \bmod n$

Proof (2/5)

It remains to prove PRIM $\in$ **NP**. We consider the following nondeterministic primality algorithm with input n

1. Accept if $n \in \{2, 3\}$
2. Guess $2 \leq k \leq \log n$ and $2 \leq p_i \leq n-1$ for all $1 \leq i \leq k$
3. Check whether $\prod_{i=1}^{k} p_i = n-1$ (otherwise reject)
4. Check recursively whether p_i prime for all $i \in \{1, \ldots, k\}$
5. Guess $z \in \mathbb{N}$ with $z \leq n-1$ and check whether $z^{n-1} \equiv 1 \bmod n$
6. Check whether $z^{\frac{n-1}{p_i}} \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, k\}$

Proof (2/5)

It remains to prove PRIM $\in$ **NP**. We consider the following nondeterministic primality algorithm with input n

1. Accept if $n \in \{2, 3\}$
2. Guess $2 \leq k \leq \log n$ and $2 \leq p_i \leq n-1$ for all $1 \leq i \leq k$
3. Check whether $\prod_{i=1}^{k} p_i = n-1$ (otherwise reject)
4. Check recursively whether p_i prime for all $i \in \{1, \ldots, k\}$
5. Guess $z \in \mathbb{N}$ with $z \leq n-1$ and check whether $z^{n-1} \equiv 1 \bmod n$
6. Check whether $z^{\frac{n-1}{p_i}} \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, k\}$

It is unclear if this runs in polynomial time. We first settle correctness.
If n is prime, then by Fermat's little theorem (§6.2) we can guess prime decomposition of $n-1$ in 2 and guess z in 5 such that the tests succeed.

Proof (3/5)

Now we prove that those tests can only succeed for primes.
Let $n > 3$ and $p_1, \ldots, p_k \in \mathbb{N}$ prime decomposition of $n - 1$.
Additionally, let z be the value guessed in step 5; i.e. $z^{n-1} \equiv 1 \bmod n$.

Proof (3/5)

Now we prove that those tests can only succeed for primes.
Let $n > 3$ and $p_1, \ldots, p_k \in \mathbb{N}$ prime decomposition of $n - 1$.
Additionally, let z be the value guessed in step 5; i.e. $z^{n-1} \equiv 1 \bmod n$.
We show that $z^i \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, n-2\}$,
which proves primality of n by Fermat's little theorem (§6.2).

Proof (3/5)

Now we prove that those tests can only succeed for primes.
Let $n > 3$ and $p_1, \ldots, p_k \in \mathbb{N}$ prime decomposition of $n-1$.
Additionally, let z be the value guessed in step 5; i.e. $z^{n-1} \equiv 1 \bmod n$.
We show that $z^i \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, n-2\}$,
which proves primality of n by Fermat's little theorem (§6.2).
For contradiction assume $i \in \{1, \ldots, n-2\}$ such that $z^i \equiv 1 \bmod n$.
Let m be the greatest common divisor of $n-1$ and i, which yields $a, b \in \mathbb{Z}$
such that $m = a \cdot (n-1) + b \cdot i$ (extended Euclidian algorithm).

Proof (3/5)

Now we prove that those tests can only succeed for primes.
Let $n > 3$ and $p_1, \ldots, p_k \in \mathbb{N}$ prime decomposition of $n-1$.
Additionally, let z be the value guessed in step 5; i.e. $z^{n-1} \equiv 1 \bmod n$.
We show that $z^i \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, n-2\}$,
which proves primality of n by Fermat's little theorem (§6.2).
For contradiction assume $i \in \{1, \ldots, n-2\}$ such that $z^i \equiv 1 \bmod n$.
Let m be the greatest common divisor of $n-1$ and i, which yields $a, b \in \mathbb{Z}$
such that $m = a \cdot (n-1) + b \cdot i$ (extended Euclidian algorithm).

$$z^m = z^{a\cdot(n-1)+b\cdot i} = (z^{n-1})^a \cdot (z^i)^b \equiv 1 \bmod n$$

Proof (3/5)

Now we prove that those tests can only succeed for primes.
Let $n > 3$ and $p_1, \ldots, p_k \in \mathbb{N}$ prime decomposition of $n-1$.
Additionally, let z be the value guessed in step 5; i.e. $z^{n-1} \equiv 1 \bmod n$.
We show that $z^i \not\equiv 1 \bmod n$ for all $i \in \{1, \ldots, n-2\}$,
which proves primality of n by Fermat's little theorem (§6.2).
For contradiction assume $i \in \{1, \ldots, n-2\}$ such that $z^i \equiv 1 \bmod n$.
Let m be the greatest common divisor of $n-1$ and i, which yields $a, b \in \mathbb{Z}$
such that $m = a \cdot (n-1) + b \cdot i$ (extended Euclidian algorithm).

$$z^m = z^{a\cdot(n-1)+b\cdot i} = (z^{n-1})^a \cdot (z^i)^b \equiv 1 \bmod n$$

Since $i \leq n-2$ we have $m < n-1$ and thus m is strict divisor of $n-1$.
Thus there exists $i' \in \{1, \ldots, k\}$ such that m is divisor of $n' = \frac{n-1}{p_{i'}}$.
However, this yields $z^{n'} = (z^m)^\ell \equiv 1 \bmod n$ contradicting 6.

Proof (4/5)

It remains to show that algorithm runs in polynomial time. Successful run can be represented as non-unary branching tree. Leaves represent calls that accept in step 1 and inner nodes represent complete runs from 1 to 6.

Proof (4/5)

It remains to show that algorithm runs in polynomial time. Successful run can be represented as non-unary branching tree. Leaves represent calls that accept in step 1 and inner nodes represent complete runs from 1 to 6. This tree has at most $2 \cdot \lfloor \log n \rfloor - 1$ nodes. For $n \in \{2, 3\}$ we have $2 \cdot \lfloor \log 2 \rfloor - 1 = 2 \cdot \lfloor \log 3 \rfloor - 1 = 1$. Otherwise prime decomposition $p_1, \ldots, p_k$ of $n - 1$ exists and tree contains trees of $p_1, \ldots, p_k$ together with root node.

$$1 + \sum_{i=1}^{k} \left(2 \cdot \lfloor \log p_i \rfloor - 1 \right) \leq 2 \cdot \left\lfloor \log \left(\prod_{i=1}^{k} p_i \right) \right\rfloor - (k - 1) \leq 2 \cdot \lfloor \log n \rfloor - 1$$

Proof (5/5)

We modify algorithm such that (non-unary branching) tree with at most $2 \cdot \lfloor \log n \rfloor - 1$ nodes is guessed. At each node e of tree we guess integer $p_e \leq n$ such that we guess 2 or 3 at each leaf.

Proof (5/5)

We modify algorithm such that (non-unary branching) tree with at most $2 \cdot \lfloor \log n \rfloor - 1$ nodes is guessed. At each node e of tree we guess integer $p_e \leq n$ such that we guess 2 or 3 at each leaf. For every inner node e with integer p_e we additionally guess $z_e \leq p_e - 1$ such that $z_e^{p_e - 1} \equiv 1 \bmod p_e$.
We now check whether tree is valid:

- $p_e - 1 = \prod_{i=1}^{\ell} p_{e_i}$ for every node e with children $e_1, \ldots, e_\ell$

Proof (5/5)

We modify algorithm such that (non-unary branching) tree with at most $2 \cdot \lfloor \log n \rfloor - 1$ nodes is guessed. At each node e of tree we guess integer $p_e \leq n$ such that we guess 2 or 3 at each leaf. For every inner node e with integer p_e we additionally guess $z_e \leq p_e - 1$ such that $z_e^{p_e - 1} \equiv 1 \bmod p_e$. We now check whether tree is valid:

- $p_e - 1 = \prod_{i=1}^{\ell} p_{e_i}$ for every node e with children $e_1, \ldots, e_\ell$
- $z_e^{\frac{p_e - 1}{p_{e'}}} \not\equiv 1 \bmod p_e$ for every node e and child e'

Proof (5/5)

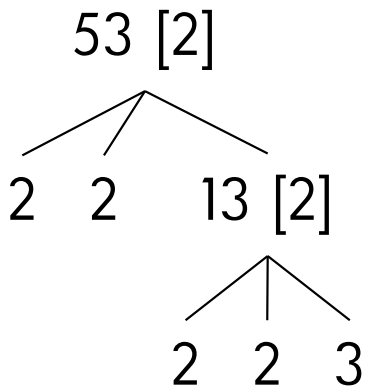
We modify algorithm such that (non-unary branching) tree with at most $2 \cdot \lfloor \log n \rfloor - 1$ nodes is guessed. At each node e of tree we guess integer $p_e \leq n$ such that we guess 2 or 3 at each leaf. For every inner node e with integer p_e we additionally guess $z_e \leq p_e - 1$ such that $z_e^{p_e - 1} \equiv 1 \bmod p_e$. We now check whether tree is valid:

- $p_e - 1 = \prod_{i=1}^{\ell} p_{e_i}$ for every node e with children $e_1, \ldots, e_\ell$
- $z_e^{\frac{p_e - 1}{p_{e'}}} \not\equiv 1 \bmod p_e$ for every node e and child e'

Powers computed in polynomial time by iterated squaring (→ exercise). □

Class NP ∩ co-NP

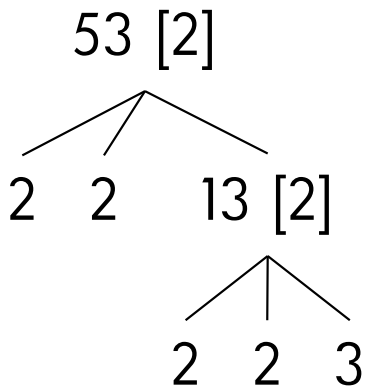
Illustration for $n = 53$



Tree has $7 \leq 2 \cdot \lfloor \log 52 \rfloor - 1 = 2 \cdot 5 - 1 = 9$ nodes

Class NP ∩ co-NP

Illustration for $n = 53$



Tree has $7 \leq 2 \cdot \lfloor \log 52 \rfloor - 1 = 2 \cdot 5 - 1 = 9$ nodes

Additionally

- $2 \cdot 2 \cdot 13 = 52 = 53 - 1$ and $2 \cdot 2 \cdot 3 = 12 = 13 - 1$
- $2^{12} = 4,096 = 315 \cdot 13 + 1 \equiv 1 \bmod 13$ and
  $2^{52} = 4,503,599,627,370,496 \equiv 1 \bmod 53$
- $2^{12/2} = 2^6 = 64 \equiv 12 \bmod 13$ and $2^{12/3} = 2^4 = 16 \equiv 3 \bmod 13$
- $2^{52/2} = 2^{26} = 67,108,864 \equiv 52 \bmod 53$ and
  $2^{52/13} = 2^4 = 16 \equiv 16 \bmod 53$

Complete Problems for **NP**

Notes

- Function $f(n) = n^i$ is log-space computable for all $n, i \in \mathbb{N}$
- Thus $L \preceq_{\mathsf{L}} \mathrm{Pad}_f^{\#}(L)$ via reduction $w \mapsto w\#^{|w|^i - |w|}$
  (see exercise)

Complete Problems for **NP**

§6.4 Theorem

If there are **NP**-complete problems,
then there also exist **NP**-complete problems in $\mathrm{NTIME}(x)$

Proof

Let $L \subseteq \Sigma^*$ be **NP**-complete problem. Since $L \in \mathbf{NP}$ there exists constant $i \in \mathbb{N}$ such that $L \in \mathrm{NTIME}(f\,;g)$ with $f, g\colon \mathbb{N} \to \mathbb{N}$ given by $f(n) = n^i$ and $g(n) = n$ for all $n \in \mathbb{N}$.

Complete Problems for **NP**

§6.4 Theorem

If there are **NP**-complete problems,
then there also exist **NP**-complete problems in $\mathrm{NTIME}(x)$

Proof

Let $L \subseteq \Sigma^*$ be **NP**-complete problem. Since $L \in \mathbf{NP}$ there exists constant $i \in \mathbb{N}$ such that $L \in \mathrm{NTIME}(f\,;g)$ with $f, g\colon \mathbb{N} \to \mathbb{N}$ given by $f(n) = n^i$ and $g(n) = n$ for all $n \in \mathbb{N}$. Translation theorem §4.4 yields $\mathrm{Pad}_f^{\#}(L) \in \mathrm{NTIME}(x)$ for $\# \notin \Sigma$.

Complete Problems for **NP**

§6.4 Theorem

If there are **NP**-complete problems,
then there also exist **NP**-complete problems in $\mathrm{NTIME}(x)$

Proof

Let $L \subseteq \Sigma^*$ be **NP**-complete problem. Since $L \in \mathbf{NP}$ there exists constant $i \in \mathbb{N}$ such that $L \in \mathrm{NTIME}(f\,;g)$ with $f, g\colon \mathbb{N} \to \mathbb{N}$ given by $f(n) = n^i$ and $g(n) = n$ for all $n \in \mathbb{N}$. Translation theorem §4.4 yields $\mathrm{Pad}_f^{\#}(L) \in \mathrm{NTIME}(x)$ for $\# \notin \Sigma$. Let $L' \in \mathbf{NP}$ another problem. Then

$$L' \prec_{\mathsf{L}} L \prec_{\mathsf{L}} \mathrm{Pad}_f^{\#}(L)$$ (see previous note)

Complete Problems for **NP**

§6.4 Theorem

If there are **NP**-complete problems,
then there also exist **NP**-complete problems in $\mathrm{NTIME}(x)$

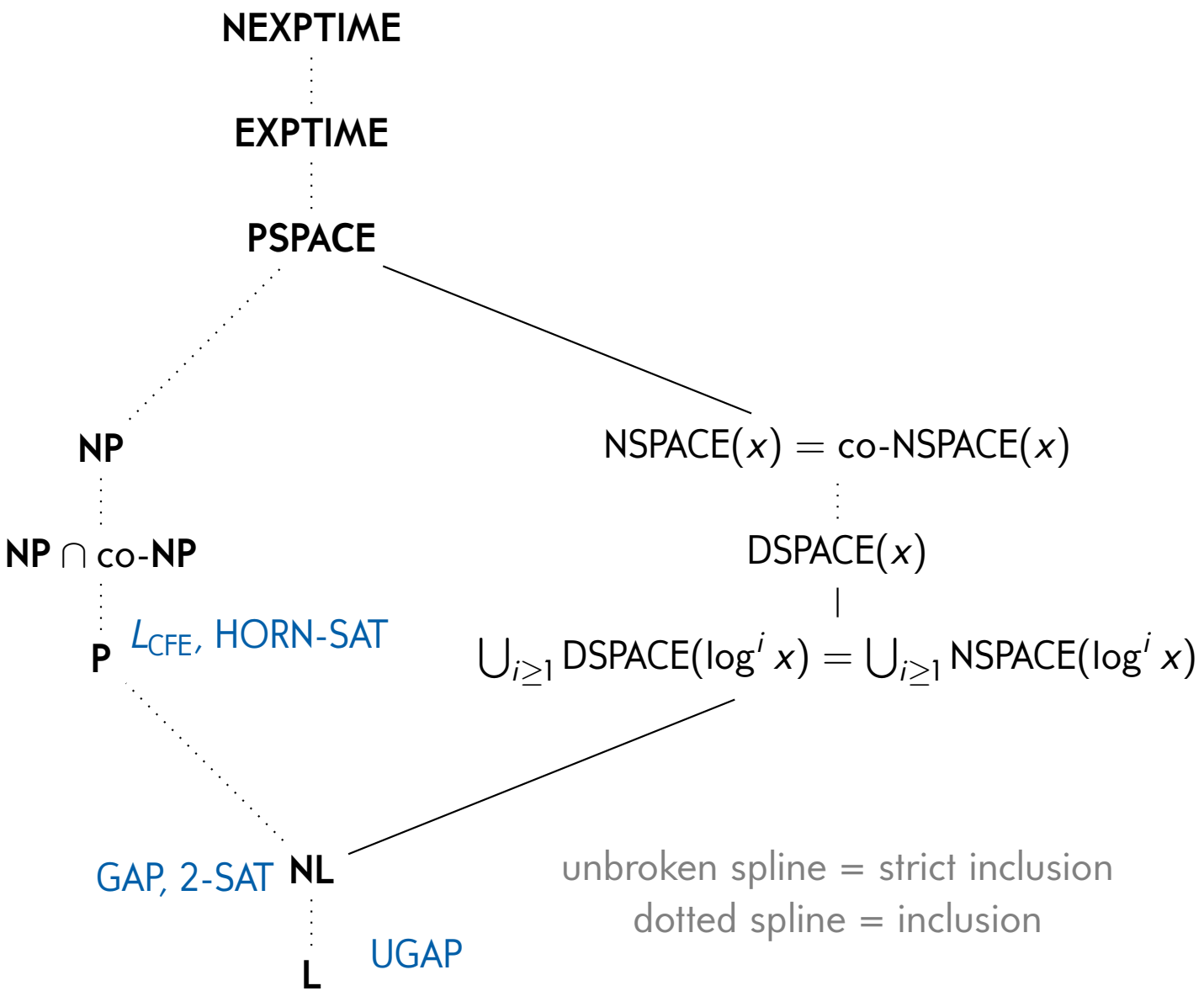
Proof

Let $L \subseteq \Sigma^*$ be **NP**-complete problem. Since $L \in \mathbf{NP}$ there exists constant $i \in \mathbb{N}$ such that $L \in \mathrm{NTIME}(f\,;g)$ with $f, g\colon \mathbb{N} \to \mathbb{N}$ given by $f(n) = n^i$ and $g(n) = n$ for all $n \in \mathbb{N}$. Translation theorem §4.4 yields $\mathrm{Pad}_f^{\#}(L) \in \mathrm{NTIME}(x)$ for $\# \notin \Sigma$. Let $L' \in \mathbf{NP}$ another problem. Then

$$L' \prec_{\mathbf{L}} L \prec_{\mathbf{L}} \mathrm{Pad}_f^{\#}(L) \qquad \text{(see previous note)}$$

By transitivity (§5.4) also $L' \prec_{\mathbf{L}} \mathrm{Pad}_f^{\#}(L)$ and $\mathrm{Pad}_f^{\#}(L)$ is **NP**-complete. □

Complexity Classes



Summary

- Complete problems for **P** (L_{CFE})
- Primality testing in **NP** ∩ **co-NP**
- Linear **NP**-complete problems exist

Sixth exercise sheet available on my website