# Chapter 5: The Witness Reduction Technique

Joseph Cloud, Ashley Wilson, Mengqi Zhang

April 19 & 24, 2023

**Definition 8.2** (**#P**) **#P** is the set of all functions  $f: \{0, 1\}^* \to \mathbb{N}$  such that there is a NPTM M such that for all  $x \in \{0, 1\}^*$ ,

f(x) = number of accepting branches in M's computation graph on x

**Definition 8.2** (**#P**) **#P** is the set of all functions  $f: \{0, 1\}^* \to \mathbb{N}$  such that there is a NPTM M such that for all  $x \in \{0, 1\}^*$ ,

f(x) = number of accepting branches in M's computation graph on x

Proper Subtraction  $(\Theta)$   $a \ominus b = \max(\{0, a - b\})$ 

**Definition 8.2** (**#P**) **#P** is the set of all functions  $f: \{0, 1\}^* \to \mathbb{N}$  such that there is a NPTM M such that for all  $x \in \{0, 1\}^*$ ,

f(x) = number of accepting branches in M's computation graph on x

Proper Subtraction  $(\Theta)$   $a \ominus b = \max(\{0, a - b\})$ 

Let  $\sigma$  be an operation from  $\mathbb{N} \times \mathbb{N}$  to  $\mathbb{N}$  and let  $\mathcal{F}$  be a class of functions from  $\mathbb{N}$  to  $\mathbb{N}$ . We say that  $\mathcal{F}$  is closed under (the operation)  $\sigma$  if

$$(\forall f_1 \in \mathcal{F})(\forall f_2 \in \mathcal{F})[h_{f_1,f_2} \in \mathcal{F}]$$

where  $h_{f_1,f_2}(n) = \sigma [f_1(n), f_2(n)]$ 



#### Other #P Closures

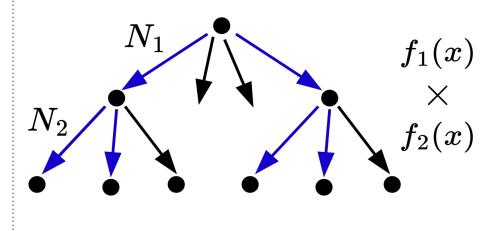
Example: #P is closed under addition Example: #P is closed under multiplication

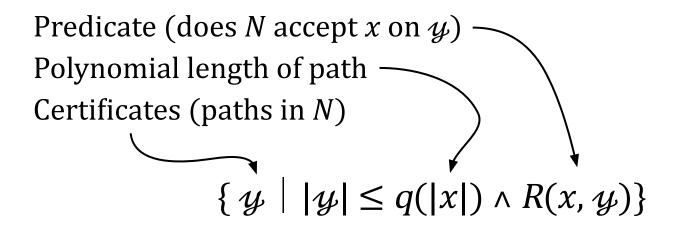




#### Other #P Closures

Example: #P is closed under addition Example: #P is closed under multiplication





#### **Definition of UP**

A language L is in **UP** if there is a polynomial-time predicate R and a polynomial q such that for all x,

$$||\{y \mid |y| \le q(|x|) \land R(x,y)\}|| = \begin{cases} 0 \text{ if } x \notin L \\ 1 \text{ if } x \in L \end{cases}$$

#### **Definition of PP**

A language L is in **PP** if there exists a polynomial q and a polynomial-time predicate R such that for all x,

$$||\{y \mid |y| = q(|x|) \land R(x,y)\}|| = \begin{cases} <2^{q(|x|)-1} & \text{if } x \notin L \\ \ge 2^{q(|x|)-1} & \text{if } x \in L \end{cases}$$

#### **Definition of** $\bigoplus$ **P**

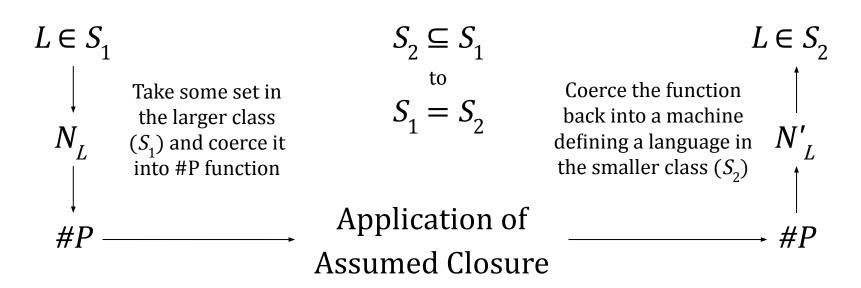
A language L is in  $\bigoplus \mathbf{P}$  if there exists a polynomial q and a polynomial-time predicate R such that for all x,

$$||\{y \mid |y| \le q(|x|) \land R(x,y)\}|| = \begin{cases} even & \text{if } x \notin L \\ odd & \text{if } x \in L \end{cases}$$

#### Witness Reduction Technique

- Witness?
- Adding is easy, removing is difficult
- Consequences of the possibility of removing witnesses
- Complexity class collapse
- Idea of the technique

#### Witness Reduction Technique



Find a collapse that characterizes the closure

Operator 'completeness' for #P

- 1. **#P** is closed under proper subtraction.
- 2. #P is closed under every polynomial-time computable operation
- 3.  $\mathbf{UP} = \mathbf{PP}$

- #P is closed under proper subtraction.
   #P is closed under every polynomial-time computable operation
  - 3. IJP = PP

- #P is closed under proper subtraction.
   #P is closed under every polynomial-time computable operation
   UP = PP

**Theorem 5.6** The following statements are equivalent

- #P is closed under proper subtraction.
   #P is closed under every polynomial-time computable operation
   UP = PP

- 1. Closed ( $\#P, \ominus$ )

2. Closed (#P,op) | (op is any arbitrary polynomial-time computable operation)

3. UP = PP

$$Closed(\#P, \ominus) \rightarrow UP = PP$$

$$Closed(\#P, \bigcirc) \rightarrow PP \subseteq UP \land UP \subseteq PP$$

 $\mathbf{UP} \subseteq \mathbf{PP}$  by direct proof

#### **UP** $\subseteq$ **PP** by direct proof

- 1. Let *L* be a UP language and let *N* be the NPTM that accepts *L*
- 2. Let N' be a NPTM with the same depth, q(|x|), as N and accepts on all paths but one
- 3. Let  $N_{pp}$  be a NPTM that chooses between simulating N and N'

Computation Paths :  $2^{q(|x|)+1}$ 

Accepting Paths :  $2^{q(|x|)}$  ( $N: 1, N': 2^{q(|x|)} - 1$ )

$$Closed(\#P, \ominus) \rightarrow UP = PP$$

$$Closed(\#P, \bigcirc) \rightarrow PP \subseteq UP \land UP \subseteq PP$$

 $\mathbf{UP} \subseteq \mathbf{PP}$  by direct proof

$$Closed(\#P, \ominus) \rightarrow PP \subseteq UP$$

$$Closed(\#P, \ominus) \rightarrow PP \subseteq CoNP \land CoNP \subseteq UP$$

 $Closed(\#P, \bigcirc) \rightarrow PP \subseteq CoNP$ 

 $L \in PP$ 

$$L = \{ x \mid ||\{ y \mid |y| = q(|x|) \land R(x, y)\}|| \ge 2^{q(|x|) - 1} \}$$

Let q'(|x|) = q(|x|) + 1 and for  $b \in \{0, 1\}$ , R'(x, yb) = R(x, y) and, for all  $n, q(n) \ge 1$  (avoid q(|x|) = 0)

$$Closed(\#P, \bigcirc) \rightarrow PP \subseteq CoNP$$

Let N be an NPTM that on input x guesses each y such that |y| = q(|x|) then tests R(x, y)

The **#P** function *f* defined by this NPTM has that

$$x \in L \to f(x) \ge 2^{q(|x|)-1}$$
$$x \notin L \to f(x) < 2^{q(|x|)-1}$$

$$Closed(\#P, \bigcirc) \rightarrow PP \subseteq CoNP$$

$$g(x) = 2^{q(|x|)-1} - 1$$
 is a #**P** function

By assumption of closure under proper subtraction

$$h(x) = f(x) \ominus g(x)$$

is a #**P** function, and by substituting yields

$$h(x) \ge 1$$
 if  $x \in L$ 

$$h(x) = 0$$
 if  $x \notin L$  Clearly **NP**, but ...

$$Closed(\#P, \ominus) \rightarrow PP \subseteq CoNP$$

There exists a NPTM N for which  $\hbar$  computes the number of accepting paths

The values of h are such that N is an NP machine, so the arbitrary **PP** language is in **NP** 

It follows that  $PP \subseteq NP$ 

$$PP = CoPP \rightarrow PP \subseteq CoNP$$

$$Closed(\#P, \ominus) \rightarrow CoNP \subseteq UP$$

Let *L* be an arbitrary Co**NP** language

There exists a NPTM N that accepts  $\overline{L}$ 

*N* defines a #**P** function *f* such that

$$x \in L \to f(x) = 0$$

$$x \notin L \rightarrow f(x) \ge 1$$

$$Closed(\#P, \ominus) \rightarrow CoNP \subseteq UP$$

The constant function g(x) = 1 is a #**P** function

By assumption of closure under proper subtraction

$$h(x) = g(x) \ominus f(x)$$

is a #**P** function, and by substituting yields

$$h(x) = 1$$
 if  $x \in L$ 

$$h(x) = 0$$
 if  $x \notin L$ 

h corresponds to a **UP** machine

- **#P** is closed under proper subtraction.
- 2. #P is closed under every polynomial-time computable operation 3. UP = PP

$$\mathbf{UP} = \mathbf{PP} \rightarrow \mathbf{Closed}(\#\mathbf{P}, op)$$

- 1. Let *op* be an arbitrary polynomial-time computable operation
- 2. Let f and g be arbitrary  $\#\mathbf{P}$  functions

$$B_f = \{ \langle x, n \rangle \mid f(x) \ge n \} \in \mathbf{PP}$$

$$B_g = \{ \langle x, n \rangle \mid g(x) \ge n \} \in \mathbf{PP}$$

$$\mathbf{UP} = \mathbf{PP} \rightarrow \mathbf{Closed}(\#\mathbf{P}, op)$$

- 1. Let *op* be an arbitrary polynomial-time computable operation
- 2. Let f and g be arbitrary  $\#\mathbf{P}$  functions

$$B_f = \{ \langle x, n \rangle \mid f(x) \ge n \} \in \mathbf{PP}$$

$$B_g = \{ \langle x, n \rangle \mid g(x) \ge n \} \in \mathbf{PP}$$

$$\begin{array}{cccc} V &= \{ \ \langle x, n_1, n_2 \rangle \ | \ \langle x, n_1 \rangle \in B_f \wedge \langle x, n_1 + 1 \rangle \not \in B_f \wedge \\ & \langle x, n_2 \rangle \in B_g \wedge \langle x, n_2 + 1 \rangle \not \in B_g \} \end{array}$$

$$\mathbf{UP} = \mathbf{PP} \rightarrow \mathbf{Closed}(\#\mathbf{P}, op)$$

V gives precise values of f(x) and g(x) by testing adjacent ns to find transition points in  $B_f$  and  $B_g$ 

V4-truth-table reduces to the language  $B_f \oplus B_g$ 

 $\bigoplus$  denotes disjoin Union:  $Y \bigoplus Z = \{0x \mid x \in Y\} \cup \{1x \mid x \in Z\}$ 

$$\mathbf{UP} = \mathbf{PP} \rightarrow \mathbf{Closed}(\#\mathbf{P}, op)$$

V gives precise values of f(x) and g(x) by testing adjacent ns to find transition points in  $B_f$  and  $B_g$ 

**Corollary 9.17** PP is closed under polynomial time bounded-truth-table reductions and disjoint union  $\rightarrow V \in \mathbf{PP}$ 

 $V \in \mathbf{UP}$  by assumption that  $\mathbf{UP} = \mathbf{PP}$ 

$$\mathbf{UP} = \mathbf{PP} \rightarrow \mathbf{Closed}(\#\mathbf{P}, op)$$

f and g are  $\#\mathbf{P}$  functions, so for some polynomial q and for all x  $\max\{f(x), g(x)\} \le 2^{q(|x|)}$ 

#### Consider the **NP** machine *N* that on input *x*

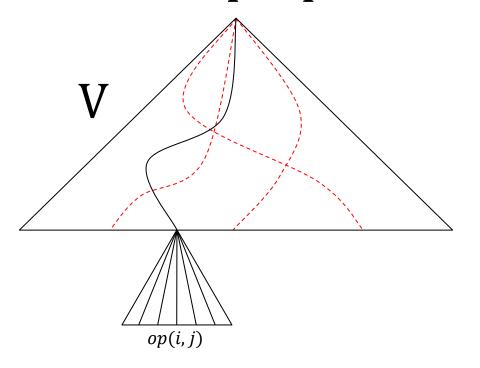
- 1. Nondeterministically choose an integer i,  $0 \le i \le 2^{q(|x|)}$
- 2. Nondeterministically choose an integer j,  $0 \le j \le 2^{q(|x|)}$
- 3. Guesses a computation path of V on input  $\langle x, i, j \rangle$ . If the path rejects, reject. Otherwise, nondeterministically guess an integer k,  $1 \le k \le op(i, j)$  and accept.

$$\mathbf{UP} = \mathbf{PP} \rightarrow \mathbf{Closed}(\#\mathbf{P}, op)$$

For all  $i \neq f(x)$  and  $j \neq g(x)$ ,  $V(\langle x, i, j \rangle)$  rejects

For the correct i and j, N(x) accepts along precisely op(i, j) paths

The #**P** function defined by this machine is h(x) = op(f(x), g(x))



# How Significant is the Collapse?

**Theorem 5.7** The following statements are equivalent

- 1. UP = PP
- 2.  $\mathbf{UP} = \mathbf{NP} = \mathbf{CoNP} = \mathbf{PH} = \bigoplus \mathbf{P} = \mathbf{PP} \cup \mathbf{PP^{PP}} \cup ...$

**Theorem 5.7** The following statements are equivalent

- 1. UP = PP
- 2.  $\mathbf{UP} = \mathbf{NP} = \mathbf{CoNP} = \mathbf{PH} = \bigoplus \mathbf{P} = \mathbf{PP} = \mathbf{PP} \cup \mathbf{PP^{PP}} \cup ...$

Prove each of the above in sequence

$$\mathbf{UP} = \mathbf{NP} = \mathbf{CoNP} = \mathbf{PH} = \mathbf{PP} = \mathbf{PP} \cup \mathbf{PP^{PP}} \cup \dots$$

#### $NP \subseteq PP$

- 1. Let  $L \in \mathbf{NP}$  and let N be the NPTM that accepts L
- 2. Let N' be a NPTM with the same depth, q(|x|), as N and accepts on all paths but one
- 3. Let  $N_{PP}$  be a NPTM that chooses between simulating N and N'

Computation Paths:  $2^{q(|x|)+1}$ 

Accepting Paths :  $\geq 2^{q(|x|)}$  (N :  $\geq 1$ , N' :  $2^{q(|x|)} - 1$ )

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$
  
 $UP \subseteq NP \subseteq PP$ ,  $UP = PP \rightarrow UP = NP$ 

- 1. Let  $L \in \mathbf{NP}$  and let N be the NPTM that accepts L
- 2. Let N' be a NPTM with the same depth, q(|x|), as N and accepts on all paths but one
- 3. Let  $N_{PP}$  be a NPTM that chooses between simulating N and N'

Computation Paths :  $2^{q(|x|)+1}$ Accepting Paths :  $\geq 2^{q(|x|)}$  (N :  $\geq 1$ , N' :  $2^{q(|x|)} - 1$ )

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$

$$PP = CoPP$$

- 1. Let  $L \in \mathbf{PP}$  and let N be the NPTM that accepts L
- 2. Let N' be equivalent to N, but ensuring the rightmost path rejects
- 3. Let  $N_{C_0PP}$  a NPTM that takes N' and expands down one level

For the rightmost leaf node of N', one child accepts and one rejects For accepting leaf nodes of N', both children reject For rejecting leaf nodes of N', both children accept

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$

$$PP = CoPP$$

- 1. Let  $L \in \mathbf{PP}$  and let N be the NPTM that accepts L
- 2. Let N' be equivalent to N, but ensuring the rightmost path rejects
- 3. Let y be the number of accepting paths in N'
- 4. Let h 1 be the depth of N

Rejecting Paths: 2y + 1

Accepting Paths :  $2^{h+1} - 2y - 1$ 

$$\mathbf{UP} = \mathbf{NP} = \mathbf{CoNP} = \mathbf{PH} = \mathbf{PP} = \mathbf{PP} \cup \mathbf{PP^{PP}} \cup \dots$$

$$PP = CoPP$$

- 1. Let  $L \in \mathbf{PP}$  and let N be the NPTM that accepts L
- 2. Let N' be equivalent to N, but ensuring the rightmost path rejects
- 3. Let y be the number of accepting paths in N'
- 4. Let h 1 be the depth of N

$$PP = CoPP$$
,  $NP = PP \rightarrow NP = CoNP$ 

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$

$$NP = CoNP \rightarrow NP^{NP \cap CoNP} = NP^{NP} = NP \rightarrow PH = NP$$

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$

$$P^{NP} \subseteq PH$$
,  $NP = UP \rightarrow P^{UP} \subseteq PH$ ,  $UP = PH \rightarrow P^{UP} = UP$ 

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$

$$P^{NP} \subseteq PH$$
,  $NP = UP \rightarrow P^{UP} \subseteq PH$ ,  $UP = PH \rightarrow P^{UP} = UP$   
Lemma 4.14  $\rightarrow PP^{\oplus P} \subseteq P^{PP}$ ,  $P^{PP} = UP$ ,  $UP \subseteq \bigoplus P \subseteq PP^{\oplus P}$   
 $\rightarrow UP = \bigoplus P$ 

$$UP = NP = CoNP = PH = \bigoplus P = PP \cup PP^{PP} \cup ...$$

$$\begin{split} P^{NP} \subseteq PH, \, NP = UP \to P^{UP} \subseteq PH, \, UP = PH \to P^{UP} = UP \\ Lemma \, 4.14 \to PP^{\oplus P} \subseteq P^{PP}, \, PP^{PP} = UP, \, UP \subseteq \bigoplus P \subseteq PP^{\oplus P} \\ \to UP = \bigoplus P \\ \bigoplus P = PP, \, PP^{\oplus P} = PP \to PP^{PP} = PP^{\oplus P} = PP \end{split}$$

→ any stack of **PP**s of arbitrary height can be reduced to **PP** 

**Theorem 5.9** The following statements are equivalent

- 1. **#P** is closed under integer division
- 2. #P is closed under every polynomial-time computable operation
- 3. UP = PP

**Definition 5.8** Let  $\mathcal{F}$  be a class of functions from  $\mathbb{N}$  to  $\mathbb{N}$ . We say that  $\mathcal{F}$  is closed under integer division  $(\bigcirc)$  if

$$(\forall f_1 \in \mathcal{F})(\forall f_2 \in \mathcal{F} : (\forall n)[f_2(n) > 0])[f_1 \oslash f_2 \in \mathcal{F}]$$

**Theorem 5.9** *The following statements are equivalent* 

- #P is closed under integer division
   #P is closed under every polynomial-time computable operation
   UP = PP

$$Closed(\#P, \bigcirc) \rightarrow UP = PP$$

Let *L* be any **PP** set, there is a NPTM *N* and integer  $k \ge 1$  such that

- 1. On each input x, N(x) has exactly  $2^{|x|^k}$  computation paths, each containing  $|x|^k$  binary choices,
- 2. On each input  $x, x \in L$  iff N(x) has at least  $2^{|x|^k 1}$  accepting paths, and
- 3. On each input x, N(x) has at least one rejecting path.

$$Closed(\#P, \bigcirc) \rightarrow UP = PP$$

Let f be the #**P** function for N

Let *g* be the #**P** function  $g(x) = 2^{|x|^k - 1}$ 

By assumption of closure under integer division

$$h(x) = f(x) \oslash g(x)$$

is a #P function

$$Closed(\#P, \bigcirc) \rightarrow UP = PP$$

If 
$$x \in L$$
,  $h(x) = \left[ \frac{2^{|x|^k - 1} \le f(x) \le 2^{|x|^k} - 1}{2^{|x|^k - 1}} \right] = 1$ 

If 
$$x \notin L$$
,  $h(x) = \left| \frac{0 \le f(x) < 2^{|x|^k - 1}}{2^{|x|^k - 1}} \right| = 0$ 

The NPTM corresponding to  $\hbar$  is a **UP** machine for L

# Intermediate Potential Closure Properties

# P vs NP Analogues

 $2CNF-SAT \in P$ 

Closed(#P, +)

SAT is NP-complete

Closed(#P,  $\ominus$ )  $\Leftrightarrow$ 

 $\forall$ poly-time op, Closed(#P, op)

 $SAT \in P \iff P = NP$ 

 $Closed(\#P, \ominus) \Leftrightarrow UP = PP$ 

PRIME ∈ NP, not known to be NP-complete or in P

????

#### Is #P closed under proper decrement?

- Decrement a restrictive form of subtraction
  - Intuitively more likely that #P could be closed under proper decrement than proper subtraction
- Ideal result:
  - Two classes C and D s.t.:
     #P is closed under proper decrement if and only if C = D
- How to approach this? Witness reduction technique!

#### Is #P closed under proper decrement?

#### Theorem 5.11

- 1. If #P is closed under proper decrement, then NP  $\subseteq$  SPP.
- 2. If UP = NP, then #P is closed under proper decrement.

#### SPP - Generalized UP

Polynomial-time computable function fNPTM N

$$x \notin L \implies \#acc_N(x) = f(x) - 1$$
  
 $x \in L \implies \#acc_N(x) = f(x)$ 

#### Is #P closed under proper decrement?

#### Theorem 5.11

- 1. If #P is closed under proper decrement, then NP  $\subseteq$  SPP.
- 2. If UP = NP, then #P is closed under proper decrement.

Closed(
$$\#P$$
,  $\Theta$ 1)  $\Longrightarrow$  NP  $\subseteq$  SPP

$$L \in NP \longrightarrow NPTM \ N \longrightarrow f(x) = \#acc_N(x) \in \#P$$

Closed(#P, 
$$\Theta$$
1)  $\Longrightarrow$  NP  $\subseteq$  SPP

$$L \in \mathbb{NP} \longrightarrow \mathbb{NPTM} \ N \longrightarrow f(x) = \#acc_N(x) \in \#P$$
assume closure under proper decrement
$$g(x) = f(x) \ominus 1 \in \#P$$

Closed(#P, 
$$\Theta$$
1)  $\Longrightarrow$  NP  $\subseteq$  SPP

$$L \in \operatorname{NP} \longrightarrow \operatorname{NPTM} N \longrightarrow f(x) = \#\operatorname{acc}_N(x) \in \#\operatorname{P}$$
assume closure under proper decrement
$$g(x) = f(x) \ominus 1 \in \#\operatorname{P}$$

$$e^{p(|x|)} - g(x) \in \#\operatorname{P}$$

$$2^{p(|x|)} - g(x) \in \#\operatorname{P}$$

Closed(#P, 
$$\Theta$$
1)  $\Longrightarrow$  NP  $\subseteq$  SPP

$$L \in \operatorname{NP} \longrightarrow \operatorname{NPTM} N \longrightarrow f(x) = \operatorname{\#acc}_N(x) \in \operatorname{\#P}$$
assume closure under proper decrement
$$g(x) = f(x) \ominus 1 \in \operatorname{\#P}$$

$$f(x) = g(x) = f(x) \ominus 1 \in \operatorname{\#P}$$

$$g(x) = f(x) \ominus 1 \in \operatorname{\#P}$$

$$g(x) = f(x) \ominus 1 \in \operatorname{\#P}$$

$$g(x) = g(x) = \operatorname{\#P}$$

$$f(x) + 2^{p(|x|)} - g(x) \in \operatorname{\#P}$$

# Closed(#P, $\ominus$ 1) $\Longrightarrow$ NP $\subseteq$ SPP

$$x \notin L \to f(x) = 0 \to 2^{p(|x|)} + 0 - (0 \oplus 1) = 2^{p(|x|)}$$

$$x \in L \to f(x) > 0 \to 2^{p(|x|)} + f(x) - (f(x) - 1) = 2^{p(|x|)} + 1$$

$$f(x) + 2^{p(|x|)} - g(x) \in \#P$$

Closed(#P, 
$$\Theta$$
1)  $\Longrightarrow$  NP  $\subseteq$  SPP

$$L \in \text{NP} \longrightarrow \text{NPTM } N \longrightarrow f(x) = \#\text{acc}_{N}(x) \in \#P$$

$$g(x) = f(x) \bigoplus 1 \in \#P$$

$$f(x) = g(x) = f(x) \bigoplus 1 \in \#P$$

$$g(x) = f(x) \bigoplus 1 \in \#P$$

$$g(x) = f(x) \bigoplus 1 \in \#P$$

$$g(x) = g(x) = f(x) \bigoplus 1 \in \#P$$

$$g(x) = g(x) = f(x) \bigoplus 1 \in \#P$$

$$g(x) = g(x) = g(x) \in \#P$$

$$g(x) = g(x)$$

#### Is #P closed under proper decrement?

#### Theorem 5.11

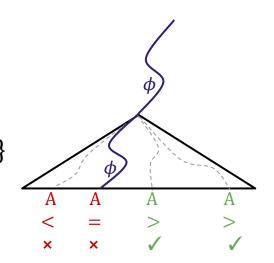
- 1. If #P is closed under proper decrement, then NP  $\subseteq$  SPP.
- 2. If UP = NP, then #P is closed under proper decrement.

$$f \in \text{\#P} \longrightarrow \exists \text{ NPTM } N \text{ s.t. } \text{\#acc}_N(x) = f(x)$$

$$B = \{\langle x, \phi \rangle : \phi \text{ is an accepting path of } N(x) \land \exists \phi' \text{ s.t } \phi < \phi' \land \phi' \text{ is acc. path of } N(x) \}$$

$$f \in \text{\#P} \longrightarrow \exists \text{ NPTM } N \text{ s.t. } \text{\#acc}_N(x) = f(x)$$

 $B = \{\langle x, \phi \rangle : \phi \text{ is an accepting path of } N(x) \land \exists \phi' \text{ s.t } \phi < \phi' \land \phi' \text{ is acc. path of } N(x) \}$ 

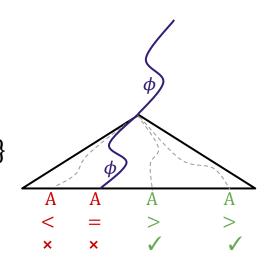


$$f \in \text{\#P} \longrightarrow \exists \text{ NPTM } N \text{ s.t. } \text{\#acc}_N(x) = f(x)$$

$$B = \{\langle x, \phi \rangle : \phi \text{ is an accepting path of } N(x) \land \exists \phi' \text{ s.t } \phi < \phi' \land \phi' \text{ is acc. path of } N(x) \}$$

by assumption that 
$$UP = NP$$

$$B \in NP \longrightarrow B \in UP$$

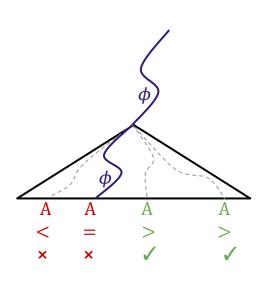


$$f \in \text{\#P} \longrightarrow \exists \text{ NPTM } N \text{ s.t. } \text{\#acc}_N(x) = f(x)$$

$$B = \{\langle x, \phi \rangle : \phi \text{ is an accepting path of } N(x) \land \exists \phi' \text{ s.t } \phi < \phi' \land \phi' \text{ is acc. path of } N(x) \}$$

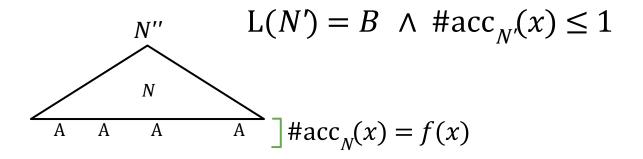
$$B \in \operatorname{NP} \xrightarrow{\operatorname{by assumption that UP} = \operatorname{NP}} B \in \operatorname{UP}$$

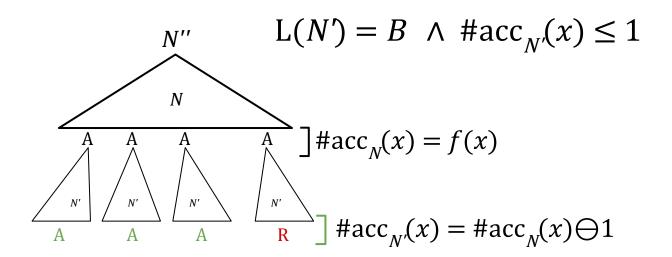
 $\exists \text{ NPTM } N' \text{ s.t. } L(N') = B \land \#acc_{N'}(x) \leq 1$ 



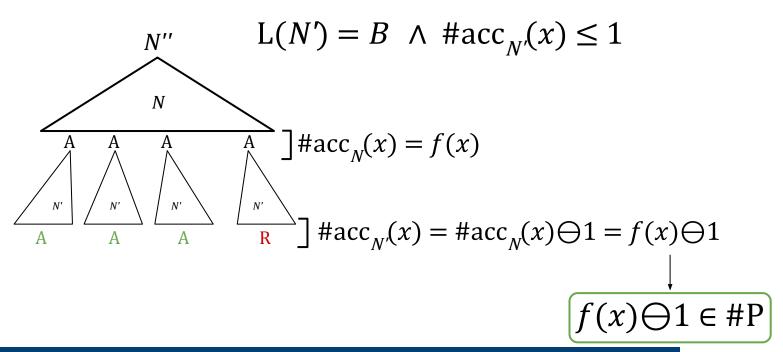
$$UP = NP \Longrightarrow Closed(\#P, \Theta1)$$

$$L(N') = B \wedge \#acc_N(x) \le 1$$





#### $UP = NP \Longrightarrow Closed(\#P, \Theta1)$



#### Is #P closed under integer division by 2?

- Restricting subtraction to decrement was successful
- Restricting division to division by 2 might be similar

#### Is #P closed under integer division by 2?

- Restricting subtraction to decrement was successful
- Restricting division to division by 2 might be similar

#### Theorem 5.12

If #P is closed under integer division by two, then  $\bigoplus P = SPP$  (and thus PH  $\subseteq$  PP)

Note: SPP  $\subseteq \bigoplus P$  holds unconditionally, we need only show that  $\bigoplus P \subseteq SPP$ .

Closed(#P, 
$$\bigcirc$$
2)  $\Longrightarrow$   $\bigoplus$ P = SPP

$$L \in \bigoplus P \longrightarrow NPTM \ N \longrightarrow f(x) = \#acc_N(x) \in \#P$$

Closed(#P, 
$$\bigcirc$$
2)  $\Longrightarrow$   $\bigoplus$ P = SPP

$$L \in \bigoplus P \longrightarrow NPTM \ N \longrightarrow f(x) = \#acc_N(x) \in \#P$$
assume closure under integer division by 2
$$g(x) = 2(f(x) \bigcirc 2) \in \#P$$

Closed(#P, 
$$\bigcirc$$
2)  $\Longrightarrow$   $\bigoplus$ P = SPP

$$L \in \bigoplus P \longrightarrow NPTM \ N \longrightarrow f(x) = \#acc_N(x) \in \#P$$
assume closure under integer division by 2
$$g(x) = 2(f(x) \bigcirc 2) \in \#P$$

$$f(x) = 2(f(x) \bigcirc 2) \in \#P$$
reverse acceptance behavior of all paths
$$2^{p(|x|)} - f(x) \in \#P$$

Closed(#P, 
$$\bigcirc 2$$
)  $\Longrightarrow \bigoplus P = SPP$ 
 $L \in \bigoplus P \longrightarrow NPTM \ N \longrightarrow f(x) = \#acc_N(x) \in \#P$ 

assume closure under integer division by 2

 $g(x) = 2(f(x) \bigcirc 2) \in \#P$ 

reverse acceptance behavior of all paths
$$2^{p(|x|)} - f(x) \in \#P$$

#P is closed under addition
$$2^{p(|x|)} - f(x) + 2(f(x) \bigcirc 2) \in \#P$$

# Closed(#P, $\bigcirc$ 2) $\Longrightarrow$ $\bigoplus$ P = SPP

$$x \notin L \to f(x) \text{ even } \to 2^{p(|x|)} - f(x) + 2(-f(x))/2 = 2^{p(|x|)}$$
  
 $x \in L \to f(x) \text{ odd } \to 2^{p(|x|)} - f(x) + 2(f(x)-1)/2 = 2^{p(|x|)} - 1$   
 $2^{p(|x|)} - f(x) + 2(f(x) \oslash 2) \in \#P$ 

Closed(#P, 
$$\bigcirc$$
2)  $\Longrightarrow$   $\bigoplus$ P = SPP

$$L \in \bigoplus P \longrightarrow NPTM \ N \longrightarrow f(x) = \#acc_{N}(x) \in \#P$$

$$g(x) = 2(f(x) \bigcirc 2) \in \#P$$

$$g(x) = 2(f(x) \bigcirc 2) \in \#P$$

$$2^{p(|x|)} - f(x) \in \#P$$

$$L \in SPP$$

$$proverse acceptance behavior of all paths 
$$2^{p(|x|)} - f(x) \in \#P$$

$$2^{p(|x|)} - f(x) + 2(f(x) \bigcirc 2) \in \#P$$$$

#### Other operators?

We know UP = NP  $\Rightarrow$  Closed(#P,  $\ominus$ 1), is there any operator that can reverse the direction?

# $Closed(\#P, ???) \Longrightarrow UP = NP$

UP is like NP with at most 1 accepting path

For NPTM *N* where  $f(x) = \#acc_N(x)$ , what function could we use to coerce this into a UP machine?

Closed(#P, min) 
$$\Longrightarrow$$
 UP = NP

UP is like NP with at most 1 accepting path

For NPTM *N* where  $f(x) = \#acc_N(x)$ , what function could we use to coerce this into a UP machine?

$$\min(f(x), 1)$$

(Theorem 5.13.1)



Closed(#P, min) 
$$\Longrightarrow$$
 UP = NP

$$L \in NP \longrightarrow f(x) \in \#P$$

$$\downarrow$$

$$L \in UP \longrightarrow \min(f(x), 1) \in \#P$$

#### Closed(#P, min) $\Longrightarrow$ Closed(#P, $\bigcirc$ 1)

Recall that  $UP = NP \Rightarrow Closed(\#P, \ominus 1)$ 

We just proved Closed(#P, min)  $\Rightarrow$  UP = NP

So as a direct corollary we get

 $Closed(\#P, min) \Rightarrow Closed(\#P, \bigoplus 1)$ 

We can continue chaining prior results to get

 $Closed(\#P, min) \Rightarrow NP \subseteq SPP$ 

## Is #P closed under min/max?

#### Theorem 5.13

- 1. If #P is closed under minimum then UP = NP
- 2. If #P is closed under maximum or under minimum then  $C_P = SPP$

#### SPP - Generalized UP

Polynomial-time computable function fNPTM N

$$x \notin L \implies \#acc_N(x) = f(x) - 1$$
  
 $x \in L \implies \#acc_N(x) = f(x)$ 

# C\_P - Exact Counting

Polynomial-time computable function fNPTM N

$$x \in L \iff \#\mathrm{acc}_{N}(x) = f(x)$$

Polynomial qPolynomial-time predicate RPolynomial-time function f

$$x \in L \Leftrightarrow ||\{y : |y| = q(|x|) \land R(x, y)\}|| = f(x)$$

Certificates (paths in *N*) Polynomial length of path

Does N accept *x* along path *y*?

Polynomial q

Polynomial-time predicate *R* 

Polynomial-time function f ----

$$x \in L \Leftrightarrow ||\{y : |y| = q(|x|) \land R(x, y)\}|| = f(x)$$

Exact number of accepting paths

# C\_P - Alternate Definition, Fixed *f*

Polynomial qPolynomial-time predicate RPolynomial-time function f

$$x \in L \iff ||\{y : |y| = q(|x|) \land R(x, y)\}|| = 2^{q(|x|)-1}$$

Fix f to be exactly half of all possibilities

Polynomial rPolynomial-time predicate S

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$
  
 $x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$ 

$$r(n) = 2q(n) \quad \text{z is two paths in N rather than just one}$$

$$S(x,z) = (\exists w_1, w_2 : |w_1| = |w_2| = q(|x|))$$

$$[w_1 \cdot w_2 = z \land R(x, w_1) \land \neg R(x, w_2)]$$

$$1^{\text{st path accepts}} \quad 2^{\text{nd path rejects}}$$

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x,y)\}|| = 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x,y)\}|| < 2^{r(|x|)-2}$$

$$r(n) = 2q(n)$$

$$S(x, z) = (\exists w_1, w_2 : |w_1| = |w_2| = q(|x|))$$

$$[w_1 \cdot w_2 = z \land R(x, w_1) \land \neg R(x, w_2)]$$

$$h(x) = f(x)(2^{q(|x|)} - f(x))$$

$$h(x) = 2^{2q(|x|)-2} = 2^{r(|x|)-2}$$

$$f(x) = 2^{q(|x|)-1}$$

$$h(x) = f(x)(2^{q(|x|)} - f(x))$$

$$h(x) = 2^{2q(|x|)-2} = 2^{r(|x|)-2}$$

$$f(x) = 2^{q(|x|)-1}$$

$$h(x) = f(x)(2^{q(|x|)} - f(x))$$

$$\max(h(x)) = 2^{r(|x|)-2}$$

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$
  
 $x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$ 

$$h(x) = f(x)(2^{q(|x|)} - f(x))$$

$$\max(h(x)) = 2^{r(|x|)-2}$$

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$
  
 $x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$ 

$$q = r \qquad R = S \qquad f(x) = 2^{r(|x|)-2}$$
$$x \in L \iff ||\{y : |y| = q(|x|) \land R(x, y)\}|| = f(x)$$

## Is #P closed under min/max?

#### Theorem 5.13

- 1. If #P is closed under minimum then UP = NP
- 2. If #P is closed under maximum or under minimum then  $C_P = SPP$

Note: SPP  $\subseteq$  C\_P holds unconditionally, proof is trivial.

We need only show  $C_P \subseteq SPP$ .

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$
  
 $x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$ 

$$x \in L \Longrightarrow f(x) = 2^{r(|x|)-2}$$
  
 $x \notin L \Longrightarrow f(x) < 2^{r(|x|)-2}$   
 $g(x) = 2^{r(|x|)-2} - 1 \in \#P$ 

$$x \in L \Longrightarrow f(x) = 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow f(x) < 2^{r(|x|)-2}$$

$$g(x) = 2^{r(|x|)-2} - 1 \in \#P$$

$$h(x) = \max(f(x), g(x))$$

$$x \in L \implies f(x) = 2^{r(|x|)-2}$$

$$x \notin L \implies f(x) < 2^{r(|x|)-2}$$

$$g(x) = 2^{r(|x|)-2} - 1 \in \#P$$

$$k(x) = \max(f(x), g(x))$$

$$x \in L \implies \max(2^{r(|x|)-2}) \quad 2^{r(|x|)-2} - 1) = 2^{r(|x|)-2}$$

$$x \notin L \implies \max(<2^{r(|x|)-2}) \quad 2^{r(|x|)-2} - 1) = 2^{r(|x|)-2} - 1$$

$$x \in L \Longrightarrow f(x) = 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow f(x) < 2^{r(|x|)-2}$$

$$g(x) = 2^{r(|x|)-2} - 1 \in \#P$$

$$M(x) = \max(f(x), g(x))$$

$$NPTM N$$

$$L \in SPP$$

## Is #P closed under min/max?

#### Theorem 5.13

- 1. If #P is closed under minimum then UP = NP
- 2. If #P is closed under maximum or under minimum then  $C_P = SPP$

# Closed(#P, min) $\Longrightarrow$ C\_P = SPP

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$
  
 $x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$ 

# Closed(#P, min) $\Longrightarrow$ C\_P = SPP

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$$

$$\downarrow \text{ negate } S, \text{ essentially flipping accepting/rejecting paths}$$

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land \neg S(x, y)\}|| = 2^{r(|x|)} - 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land \neg S(x, y)\}|| > 2^{r(|x|)} - 2^{r(|x|)-2}$$

# Closed(#P, min) $\Rightarrow$ C\_P = SPP

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| = 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land S(x, y)\}|| < 2^{r(|x|)-2}$$

$$\downarrow \text{ negate } S, \text{ essentially flipping accepting/rejecting paths}$$

$$x \in L \Longrightarrow ||\{y : |y| = r(|x|) \land \neg S(x, y)\}|| = 2^{r(|x|)} - 2^{r(|x|)-2}$$

$$x \notin L \Longrightarrow ||\{y : |y| = r(|x|) \land \neg S(x, y)\}|| > 2^{r(|x|)} - 2^{r(|x|)-2}$$

$$x \in L \Longrightarrow f(x) = (\sqrt[3]{4})2^{r(|x|)}$$

$$x \notin L \Longrightarrow f(x) > (\sqrt[3]{4})2^{r(|x|)}$$

# Closed(#P, min) $\Rightarrow$ C\_P = SPP

$$x \in L \Longrightarrow f(x) = (\frac{3}{4})2^{r(|x|)}$$
  
 $x \notin L \Longrightarrow f(x) > (\frac{3}{4})2^{r(|x|)}$   $g(x) = (\frac{3}{4})2^{r(|x|)} + 1 \in \#P$ 

# Closed(#P, min) $\Rightarrow$ C\_P = SPP

$$x \in L \Longrightarrow f(x) = (\frac{3}{4})2^{r(|x|)}$$
  $g(x) = (\frac{3}{4})2^{r(|x|)} + 1 \in \#P$   
 $x \notin L \Longrightarrow f(x) > (\frac{3}{4})2^{r(|x|)}$   $g(x) = (\frac{3}{4})2^{r(|x|)} + 1 \in \#P$   
 $h(x) = \min(f(x), g(x))$ 

# Closed(#P, min) $\Longrightarrow$ C\_P = SPP

$$x \in L \Longrightarrow f(x) = (\frac{3}{4})2^{r(|x|)}$$

$$x \notin L \Longrightarrow f(x) > (\frac{3}{4})2^{r(|x|)}$$

$$g(x) = (\frac{3}{4})2^{r(|x|)} + 1 \in \#P$$

$$\chi \in L \Longrightarrow \min(\frac{3}{4})2^{r(|x|)}, \quad (\frac{3}{4})2^{r(|x|)} + 1 = (\frac{3}{4})2^{r(|x|)}$$

$$\chi \notin L \Longrightarrow \min(>(\frac{3}{4})2^{r(|x|)}, \quad (\frac{3}{4})2^{r(|x|)} + 1 = (\frac{3}{4})2^{r(|x|)} + 1$$

# Closed(#P, min) $\Longrightarrow$ C\_P = SPP

$$x \in L \Longrightarrow f(x) = (\frac{3}{4})2^{r(|x|)}$$

$$x \notin L \Longrightarrow f(x) > (\frac{3}{4})2^{r(|x|)}$$

$$g(x) = (\frac{3}{4})2^{r(|x|)} + 1 \in \#P$$

$$M(x) = \min(f(x), g(x))$$

$$NPTM N$$

$$L \in SPP$$

#### More to consider

- Classes other than #P
  - OptP (max output)
  - SpanP (cardinality of set of outputs)
- Complete characterizations
  - Open issue for #P under proper decrement

### References

- [1] Hemaspaandra, Lane A., and Mitsunori Ogihara. "The complexity theory companion." Acm Sigact News 32, no. 4 (2001): 66-68.
- [2] Barak, Boaz (Spring 2006). "Complexity of counting". Computer Science 522: Computational Complexity. Princeton University.
- [3] wikipedia: Nondeterministic Turing machine.
- [4] https://courses.corelab.ntua.gr/pluginfile.php/74/mod\_resource/content/0/pthak p-talk-7.pdf
- [5] wikipedia: UP (complexity). https://en.wikipedia.org/wiki/UP\_(complexity)

# Thanks!

# Bonus Content: OptP

## OptP - Optimization Functions

 $f \in \text{OptP iff, for some NPTM } N$ :

 $f(x) = \max\{i \in \mathbb{N} : \text{a path of } N(x) \text{ outputs } i\}$ 

- 1. OptP is closed under proper subtraction
- 2. OptP is closed under every polynomial-time operation
- 3. NP = coNP

- OptP is closed under proper subtraction
   OptP is closed under every polynomial-time operation
  - 3. NP = coNP

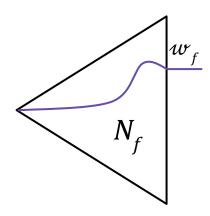
- 1. OptP is closed under proper subtraction
- 2. OptP is closed under every polynomial-time operation
- 3. NP = coNP

$$f \in \mathsf{OptP} \longrightarrow \mathsf{NPTM}\ N_f$$
 
$$g \in \mathsf{OptP} \longrightarrow \mathsf{NPTM}\ N_g$$

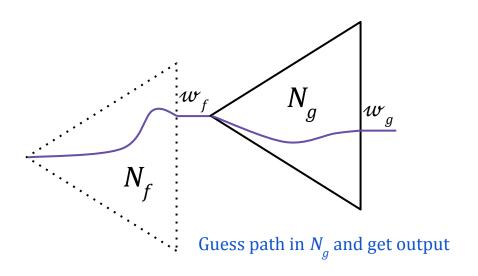
$$f \in \text{OptP} \longrightarrow \text{NPTM } N_f$$
 
$$g \in \text{OptP} \longrightarrow \text{NPTM } N_g$$
 
$$L_f = \{\langle x, i \rangle : f(x) > i\} \in \text{NP}$$
 
$$L_g = \{\langle x, i \rangle : g(x) > i\} \in \text{NP}$$

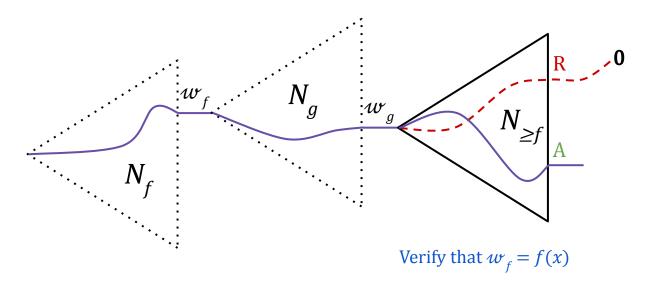
$$f \in \mathsf{OptP} \longrightarrow \mathsf{NPTM} \ N_f$$
 
$$g \in \mathsf{OptP} \longrightarrow \mathsf{NPTM} \ N_g$$
 
$$L_f = \{\langle x, i \rangle : f(x) > i\} \in \mathsf{NP} = \mathsf{coNP}$$
 by assumption 
$$L_g = \{\langle x, i \rangle : g(x) > i\} \in \mathsf{NP} = \mathsf{coNP}$$

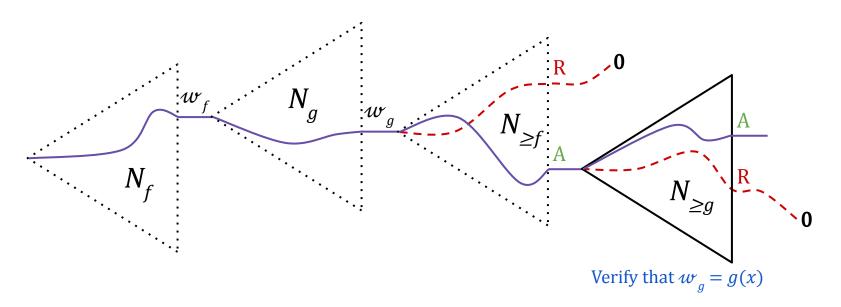
$$f \in \mathsf{OptP} \longrightarrow \mathsf{NPTM} \ N_f$$
 
$$g \in \mathsf{OptP} \longrightarrow \mathsf{NPTM} \ N_g$$
 
$$L_f = \{\langle x, i \rangle : f(x) > i\} \in \mathsf{NP} = \mathsf{coNP}$$
 by assumption 
$$L_g = \{\langle x, i \rangle : g(x) > i\} \in \mathsf{NP} = \mathsf{coNP}$$
 
$$\bar{L}_f \in \mathsf{NP} \longrightarrow \mathsf{NPTM} \ N_{\geq f}$$
 
$$\bar{L}_g \in \mathsf{NP} \longrightarrow \mathsf{NPTM} \ N_{\geq g}$$

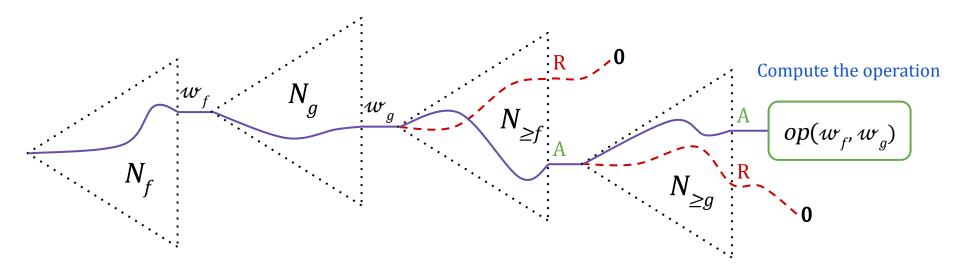


Guess path in  $N_f$  and get output









- OptP is closed under proper subtraction
- 2. OptP is closed under every polynomial-time operation NP = coNP

- OptP is closed under proper subtraction
- 2. OptP is closed under every polynomial-time operation
  3. NP = coNP

Closed(OptP, 
$$\Theta$$
)  $\Longrightarrow$  NP = coNP

$$L \in NP \longrightarrow NPTM \ N \longrightarrow f(x) = \begin{cases} 1 \text{ if } x \in L \\ 0 \text{ otherwise} \end{cases} \in OptP$$

Closed(OptP, 
$$\Theta$$
)  $\Longrightarrow$  NP = coNP

$$L \in \text{NP} \longrightarrow \text{NPTM } N \longrightarrow f(x) = \begin{cases} 1 \text{ if } x \in L \\ 0 \text{ otherwise} \end{cases} \in \text{OptP}$$
assume closure under proper subtraction  $g(x) = 1 \ominus f(x) \in \text{OptP}$ 

Closed(OptP, 
$$\Theta$$
)  $\Longrightarrow$  NP = coNP

$$L \in \text{NP} \longrightarrow \text{NPTM } N \longrightarrow f(x) = \begin{cases} 1 \text{ if } x \in L \\ 0 \text{ otherwise} \end{cases} \in \text{OptP}$$

$$assume closure under proper subtraction} \downarrow$$

$$g(x) = 1 \bigoplus_{i=1}^{n} f(x) \in \text{OptP}$$

$$g(x) = \begin{cases} 0 \text{ if } x \in L \\ 1 \text{ otherwise} \end{cases} \in \text{OptP}$$

Closed(OptP, 
$$\Theta$$
)  $\Longrightarrow$  NP = coNP

$$L \in \text{NP} \longrightarrow \text{NPTM } N \longrightarrow f(x) = \begin{cases} 1 \text{ if } x \in L \\ 0 \text{ otherwise} \end{cases} \in \text{OptP}$$

$$assume closure under proper subtraction} \downarrow$$

$$g(x) = 1 \bigoplus f(x) \in \text{OptP}$$

$$accept only on paths that output 1 \\ \text{NPTM } N' \longrightarrow g(x) = \begin{cases} 0 \text{ if } x \in L \\ 1 \text{ otherwise} \end{cases} \in \text{OptP}$$

Closed(OptP, 
$$\Theta$$
)  $\Longrightarrow$  NP = coNP

$$L \in \text{NP} \longrightarrow \text{NPTM } N \longrightarrow f(x) = \begin{cases} 1 \text{ if } x \in L \\ 0 \text{ otherwise} \end{cases} \in \text{OptP}$$

$$assume closure under proper subtraction} \downarrow$$

$$g(x) = 1 \bigoplus_{x \in L} f(x) \in \text{OptP}$$

$$accept only on paths that output 1 \\ L \in \text{coNP} \longrightarrow \text{NPTM } N' \longrightarrow g(x) = \begin{cases} 0 \text{ if } x \in L \\ 1 \text{ otherwise} \end{cases} \in \text{OptP}$$

- OptP is closed under proper subtraction
   OptP is closed under every polynomial-time operation
   NP = coNP

# SpanP - Output Cardinality

 $f \in \text{SpanP iff, for some NPTM } N$ :

 $f(x) = \|\{w \in \Sigma^* : \text{an accepting path of } N(x) \text{ outputs } w\}\|$ 

#### **Theorem 5.16** The following are equivalent:

- 1. SpanP is closed under proper subtraction
- 2. SpanP is closed under every polynomial-time operation
- 3.  $PP^{NP} = PH = NP$

Proof is left as an exercise for the reader.