The complexity of circuit evaluation over the natural numbers

Pierre McKenzie, Université de Montréal
Klaus Wagner, Universität Würzburg

October 2002

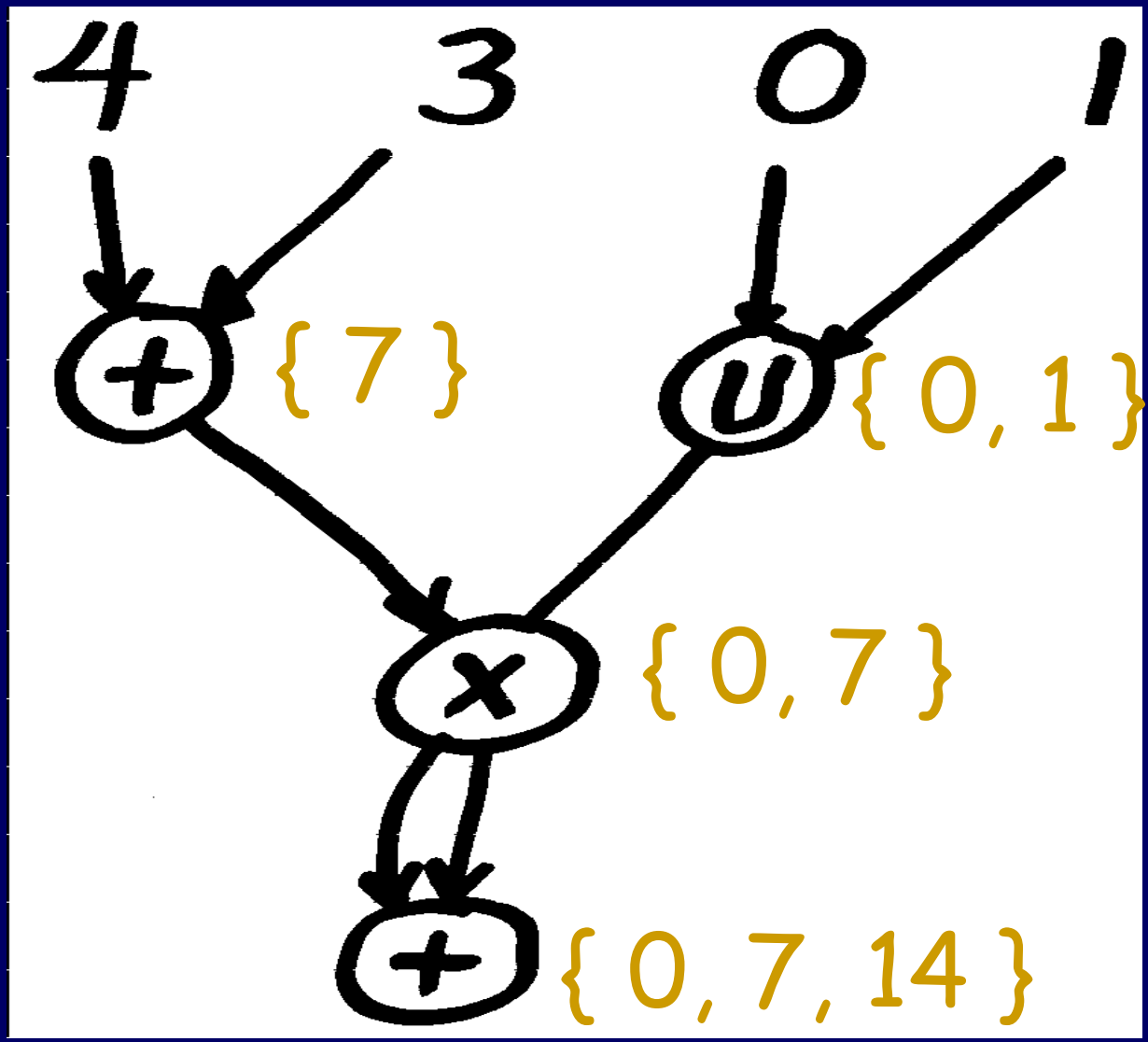
Natural numbers: { 0, 1, 2, … }

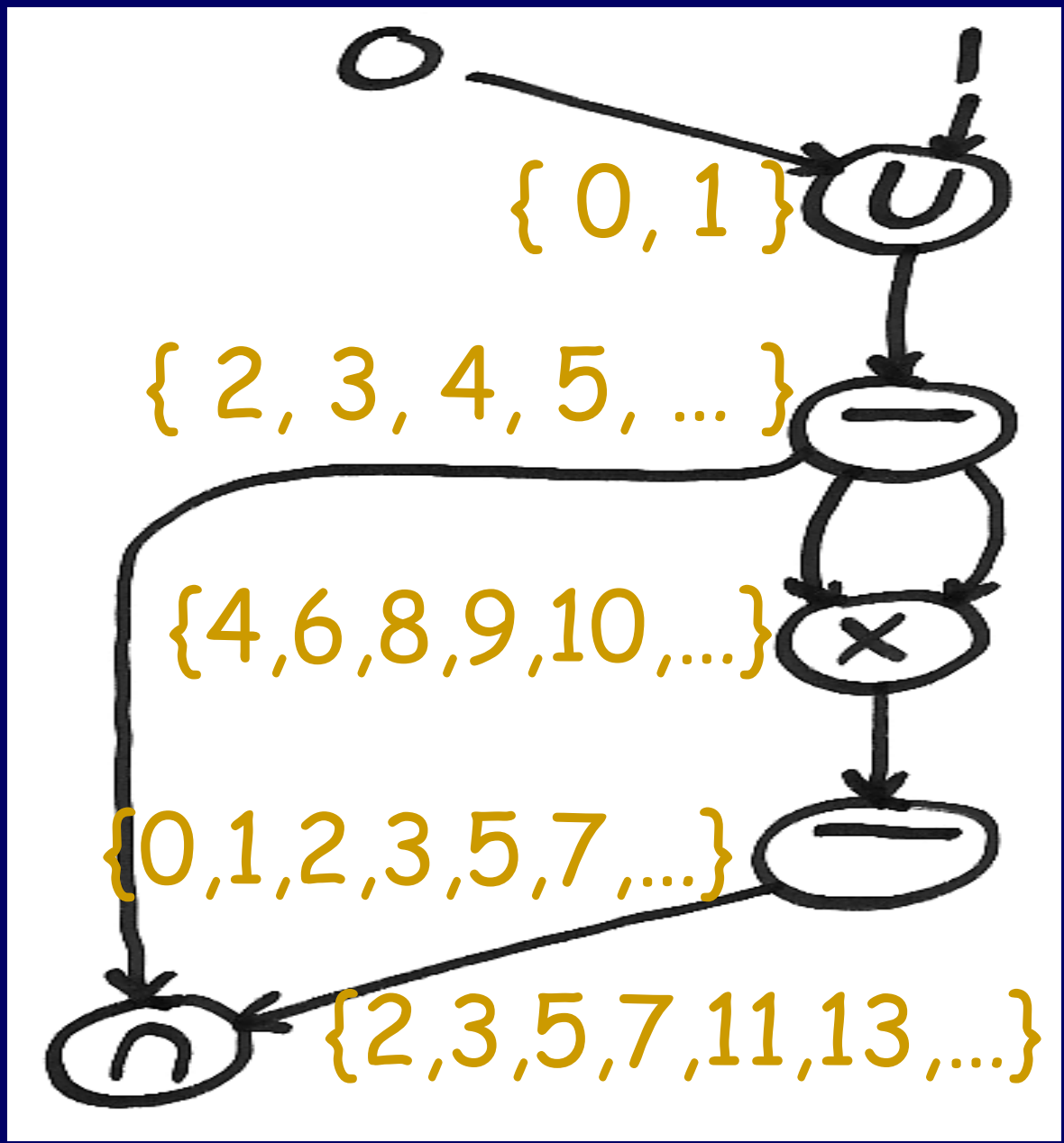
Operations: { +, x, $\cup$, $\cap$, $\overline{}$ }

Computational problem:

Given: Circuit with natural number inputs, natural number **t**

Question: Is **t** in the set computed at the output gate of the circuit?


4
3
0
1
+
{ 7 }
u
{ 0, 1 }
x
{ 0, 7 }
+
{ 0, 7, 14 }


{ 0, 1 }
{ 2, 3, 4, 5, ... }
{4,6,8,9,10,...}
{0,1,2,3,5,7,...}
{2,3,5,7,11,13,...}

Why care?

Circuits and formulas are everywhere

Natural numbers are everywhere

Includes Boolean: $(\wedge, \vee, \neg ; \{0,1\})$

$\simeq \quad (\cap, \cup, \bar{} ; \{\emptyset, \mathbf{N}\})$

Generalizes alternation

Generalizes monotonicity: $(\cap, \cup, +, \times)$

Why care? Past work:

SM73: { ∪ ∩ ¯ + } formula PSPACE-complete

{ ∪ +} formula NP-complete

Wa84: { ∪ + x } circuit in PSPACE

Ya00: { ∪ + x } circuit PSPACE-complete

McVoWa01:

counting proofs in boolean circuits is #P-compl.,

polynomial replacement systems

Is $\{ \cup \cap \ \overline{\ } + \times \}$ decidable?

Non-emptyness test for a set S **is available:**

$$0 \in \{0\} \times S \ ?$$

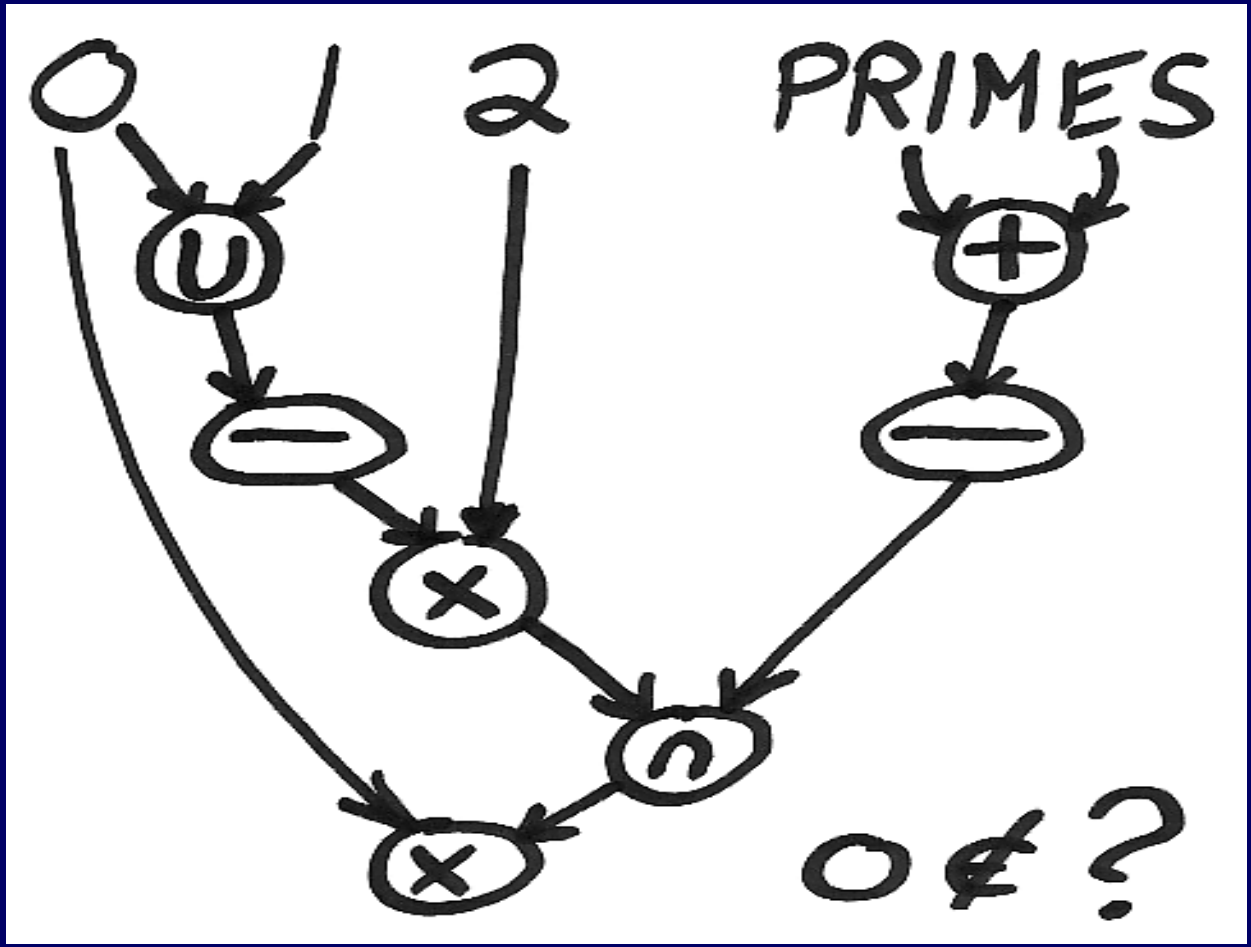
Inclusion test for $S \subseteq T$ **is available:**

$$S \cap \overline{T} = \emptyset \ ?$$

Every even $n > 2$ is the sum of two primes iff

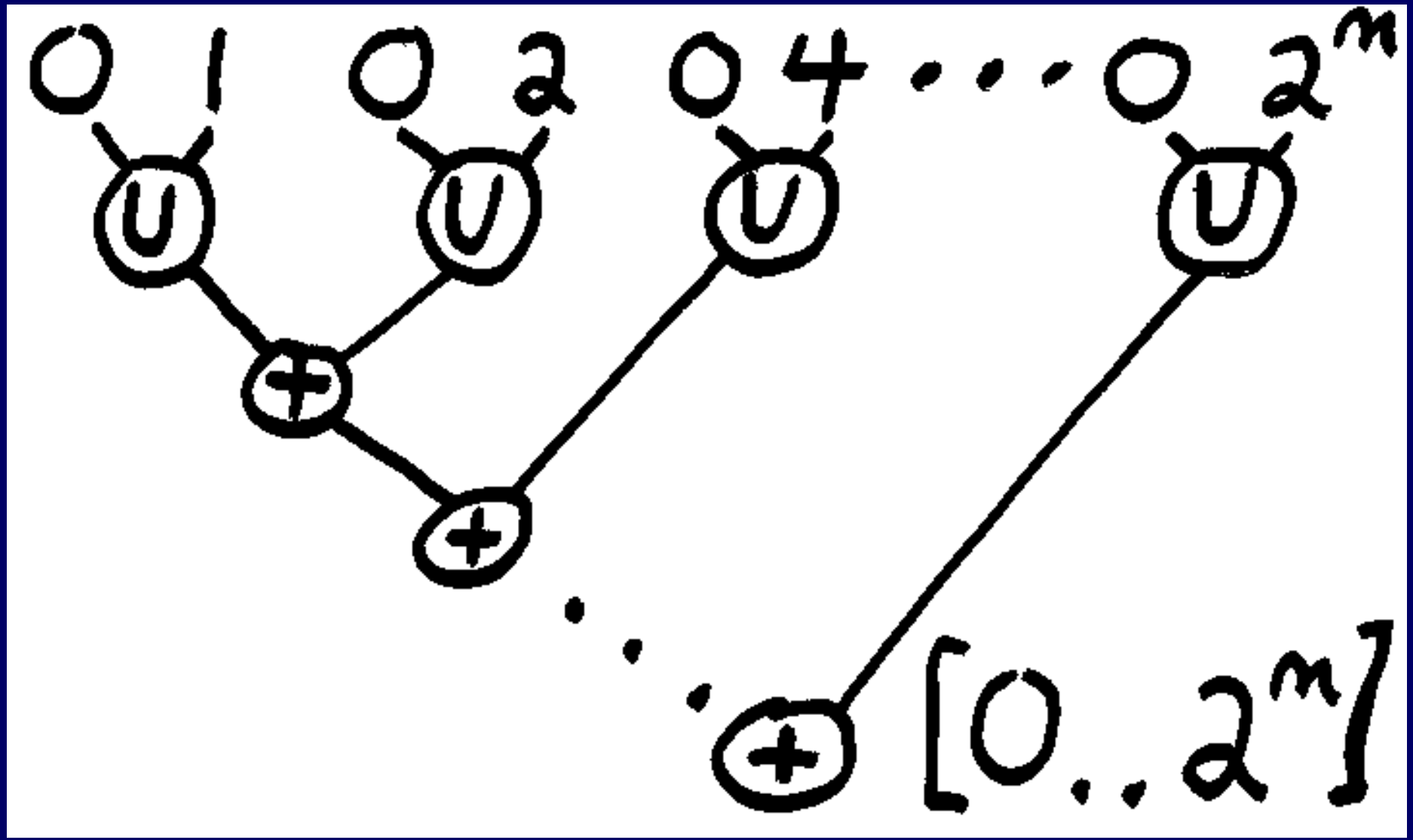
$$\{2\} \times \overline{\{0,1\}} \subseteq \text{PRIMES} + \text{PRIMES}$$

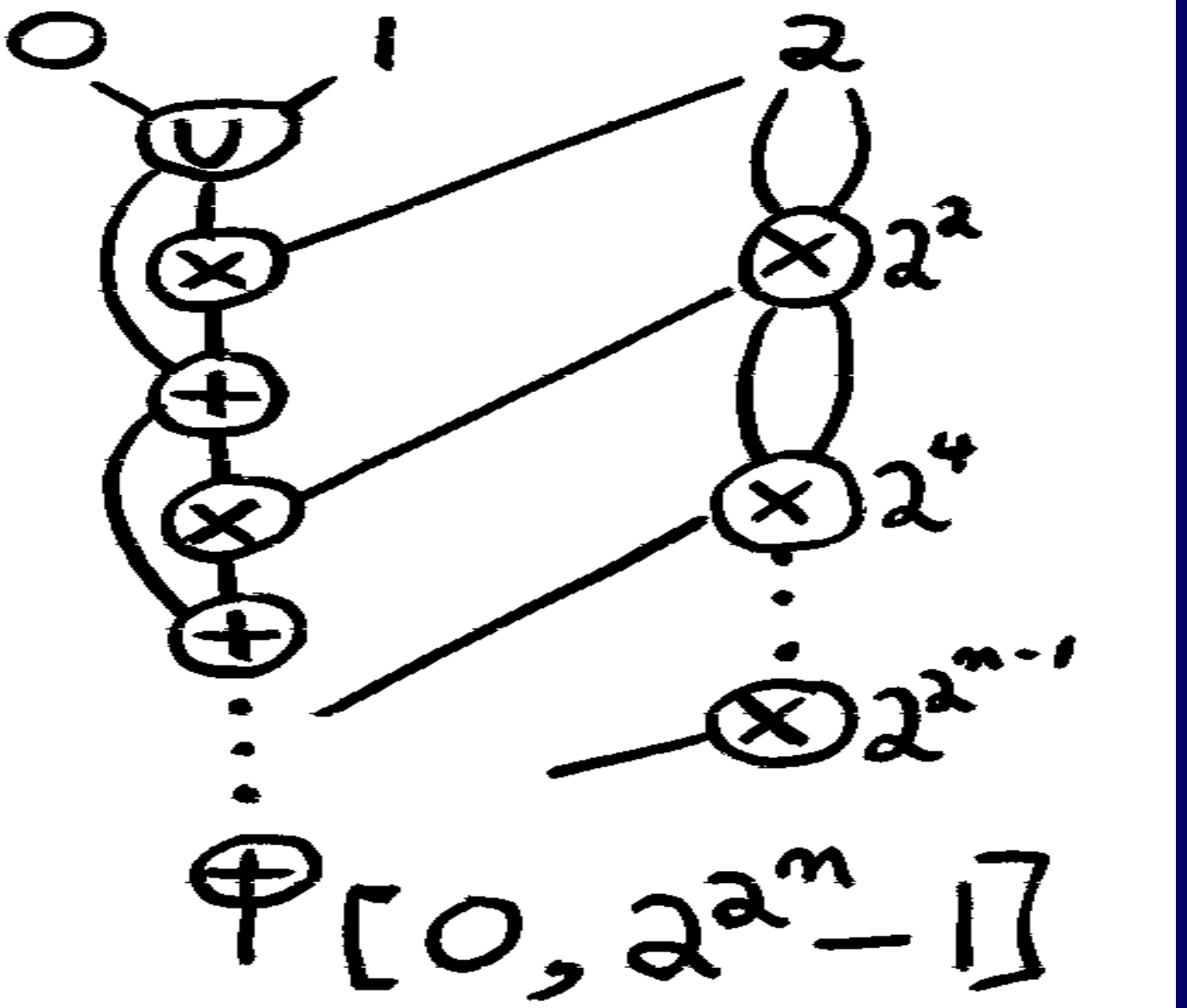
Formula for Goldbach's conjecture



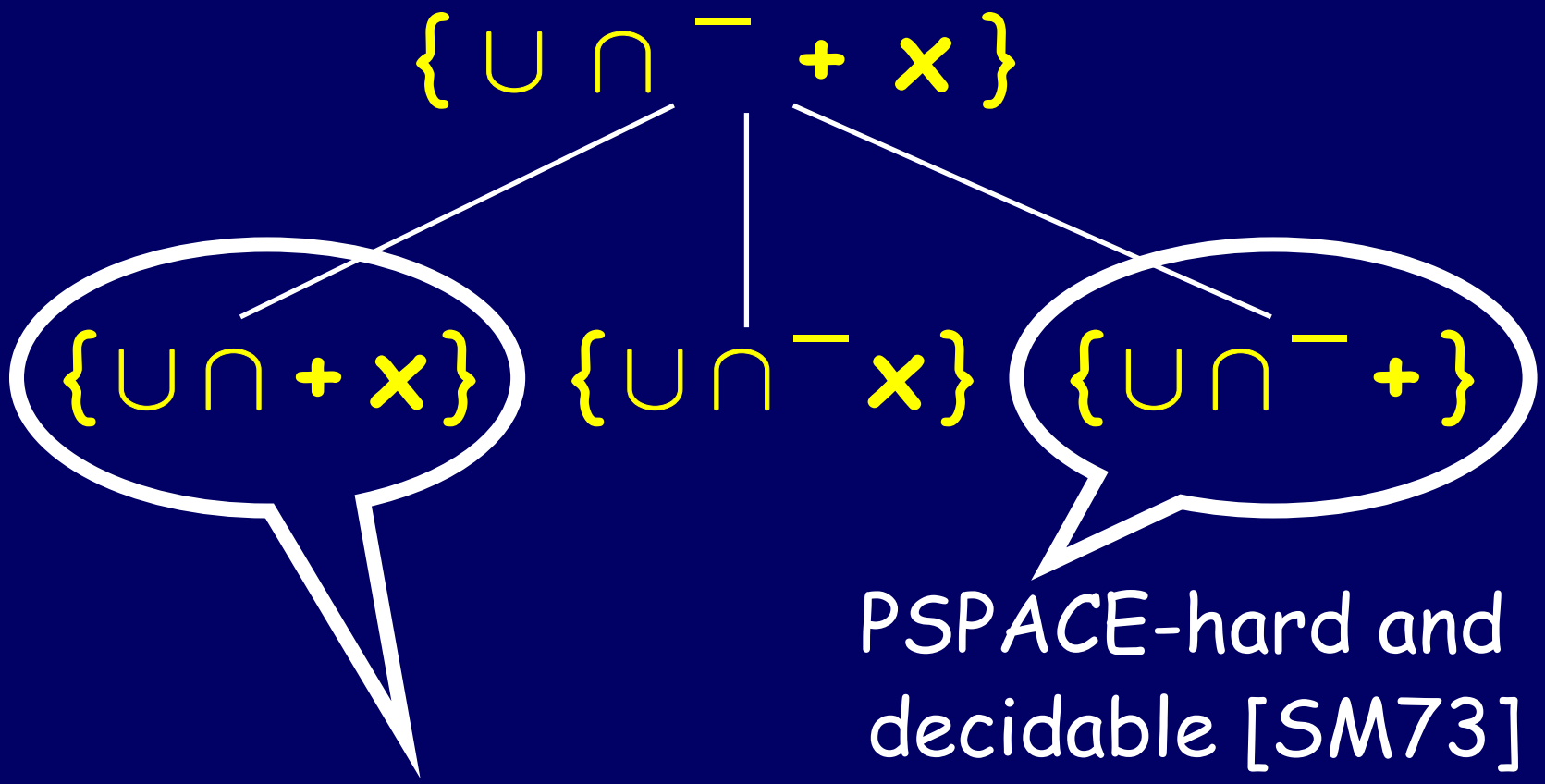
So { ∪ ∩ ¯ + x } still open !

$\mathcal{O}$	MC($\mathcal{O}$) lower bound	MC($\mathcal{O}$) upper bound	Thm.	MF($\mathcal{O}$) lower bound	MF($\mathcal{O}$) upper bound	Thm.
$\cup, \cap, ^-, +, \times$	NEXPTIME	?	6.4	PSPACE	?	5.5
$\cup, \cap, +, \times$	NEXPTIME	NEXPTIME	6.2	NP	NP	4.4
$\cup, +, \times$	PSPACE	PSPACE	5.1	NP	NP	4.4
$\cap, +, \times$	P	co-R	8.3	-	DLOGCFL	9.2
$+, \times$	P	P	7.1	-	DLOGCFL	9.2
$\cup, \cap, ^-, +$	PSPACE	PSPACE	5.5	PSPACE	PSPACE	5.1
$\cup, \cap, +$	PSPACE	PSPACE	5.5	NP	NP	4.4
$\cup, +$	NP	NP	4.4	NP	NP	4.4
$\cap, +$	$C_=L$	$C_=L$	8.2	-	L	9.5
$+$	$C_=L$	$C_=L$	8.2	-	L	9.5
$\cup, \cap, ^-, \times$	PSPACE	PSPACE	5.5	PSPACE	PSPACE	5.5
$\cup, \cap, \times$	PSPACE	PSPACE	5.5	NP	NP	4.4
$\cup, \times$	NP	NP	4.4	NP	NP	4.4
$\cap, \times$	$C_=L$	P	8.4	-	L	9.5
$\times$	NL	NL	8.5	-	L	9.5
$\cup, \cap, ^-$	P	P	7.2	NC^1	NC^1	9.3
$\cup, \cap$	P	P	7.2	-	NC^1	9.4
$\cup$	NL	NL	9.1	-	NC^1	9.4
$\cap$	NL	NL	9.1	-	NC^1	9.4


0 1 0 2 0 4 ... 0 2^n
U U U U
+ +
+
[0..2^n]


0
1
2
2^2
2^4
$2^{2^{n-1}}$
$\Phi[0, 2^{2^n}-1]$

Some cases of circuits



PSPACE-hard and decidable [SM73]

Clearly decidable, though numbers of expon. many bits and sets of doubly expon. size

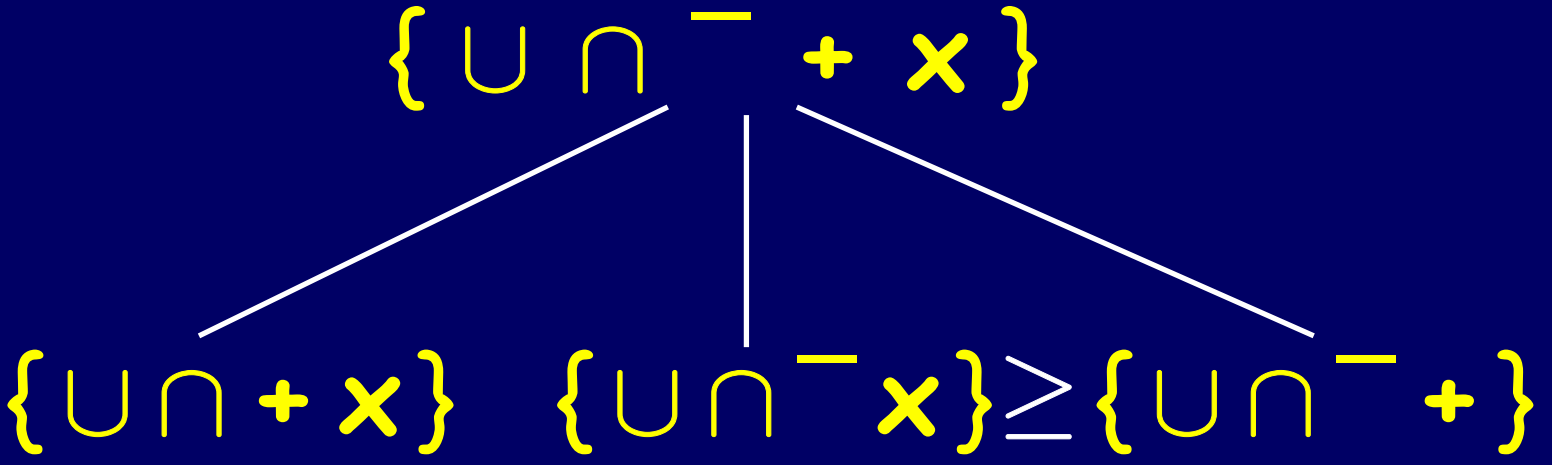
Does + always reduce to x ?

input a	→	subcircuit for 2^a
+ gate	→	x gate
test number t	→	subcircuit for 2^t
$t \in$ final S	→	$\{2^t\} \subseteq$ new final S

Notes:

- fails when + and x are mixed
- $\{ \cap \ ^- \}$ needed to test containment, so also fails for $\{ \cap +\}$ circuits and $\{+\}$ circuits

Some cases of circuits



Now, does x reduce to + ?

$15 \times 20 \rightarrow 2^0 3^1 5^1 \times 2^2 3^0 5^1$

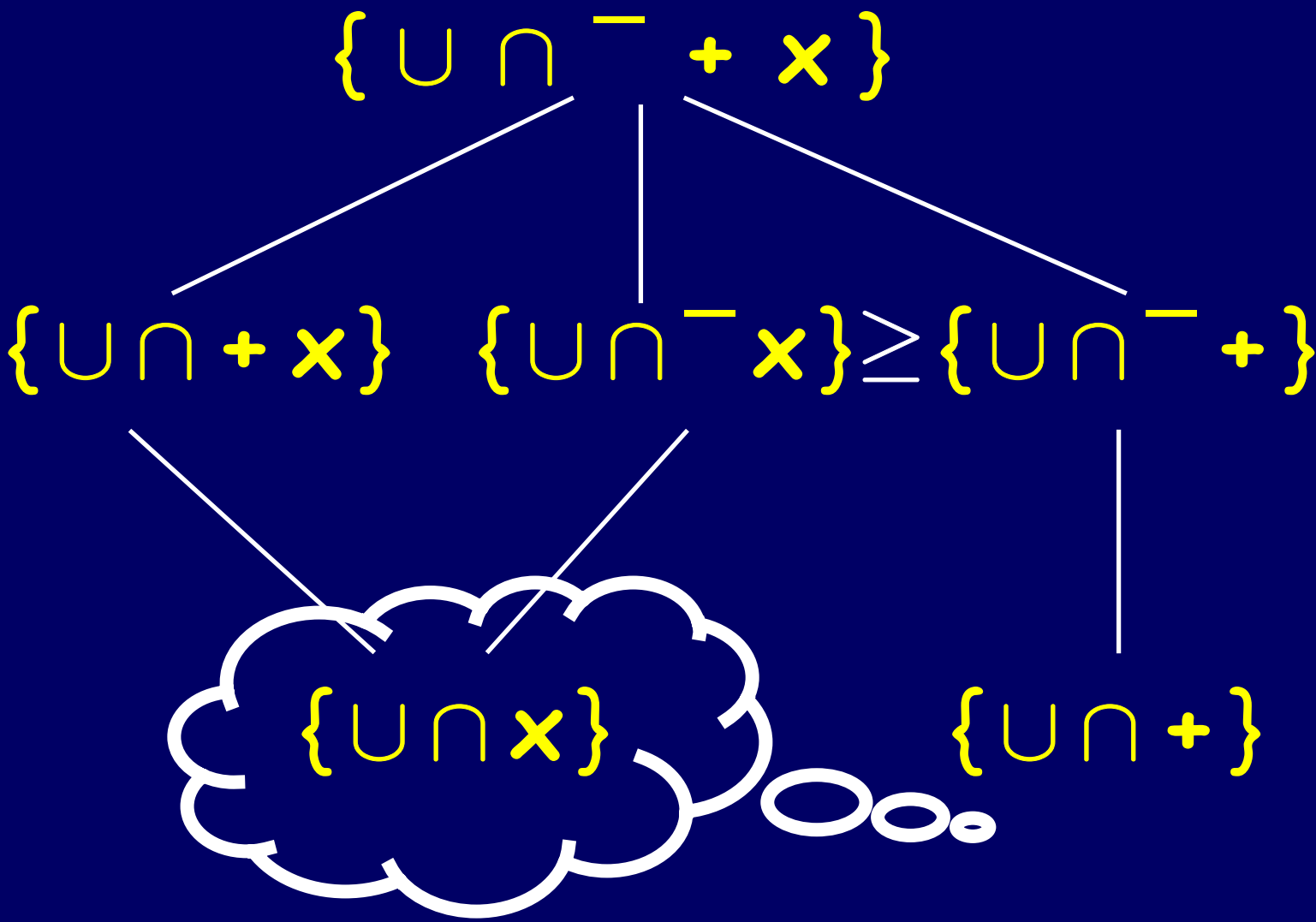
$\rightarrow (0, 1, 1) + (2, 0, 1)$

$\rightarrow (0 \cdot 2^0 + 1 \cdot 2^m + 1 \cdot 2^{2m}) + (2 \cdot 2^0 + 0 \cdot 2^m + 1 \cdot 2^{2m})$

Problems:

1. Factoring is expensive
2. With **+**, must work over $\mathbf{N}^k \cup \{\infty\}$
3. $\overline{\{300\}}$ contains numbers that are not expressible as $2^i 3^j 5^k$

Some cases of circuits



$\{\cup \cap \times\}$-circuits

Any number computed is a multiple product of the inputs … why not use the inputs as 'primes' in a reduction to $\{\cup \cap +\}$?

GCD-free basis problem:
Given: natural nonzero numbers $a_1, a_2, a_3, \ldots, a_n$.
Compute: pairwise relatively prime numbers $q_1, q_2, q_3, \ldots, q_m$ such that each a_k is expressible as a product of the q_i's.

$\{\cup \cap \mathbf{x}\}$-circuits (continued)

Fact [BaSh96]:
GCD-free basis can be solved in poly time.

Simple poly time algorithm:

$S \leftarrow \{ a_1, a_2, a_3, \ldots, a_n \}$

while $(\exists\ \mathbf{a,b} \in S)$ such that $g = \gcd(a, b) > 1$

$S \leftarrow S \setminus \{ a, b \} \cup \{ g, a/g, b/g \}$

$\{\cup \cap \mathbf{x}\}$-circuits (continued)

$15 \times 20 \rightarrow \quad 2^0 3^1 5^1 \quad \times \quad 2^2 3^0 5^1$

$\rightarrow \quad (0, 1, 1) \quad + \quad (2, 0, 1)$

$\rightarrow \quad (0 \cdot 2^0 + 1 \cdot 2^m + 1 \cdot 2^{2m}) + (2 \cdot 2^0 + 0 \cdot 2^m + 1 \cdot 2^{2m})$

Problems:

1. Factoring is expensive
2. $0 \times \{\ldots\} \rightarrow \infty + \{\ldots\}$ (but ∞ unavailable)
3. $\overline{\{300\}}$ contains numbers that are not expressible as $2^i 3^j 5^k$

$\{\cup \cap \mathbf{x}\}$-circuits (continued)

$15 \times 20 \rightarrow \quad 2^0 3^1 5^1 \quad \times \quad 2^2 3^0 5^1$

$\rightarrow \quad (0, 1, 1) \quad + \quad (2, 0, 1)$

$\rightarrow \quad (0 \cdot 2^0 + 1 \cdot 2^m + 1 \cdot 2^{2m}) + (2 \cdot 2^0 + 0 \cdot 2^m + 1 \cdot 2^{2m})$

Problems:

2. $0 \times \{\ldots\} \rightarrow \infty + \{\ldots\}$ (but ∞ unavailable)
3. $\overline{\{300\}}$ contains numbers that are not expressible as $2^i 3^j 5^k$

$\{\cup \cap \mathbf{x}\}$-circuits (continued)

$15 \times 20 \rightarrow \quad 2^0 3^1 5^1 \quad \times \quad 2^2 3^0 5^1$

$\rightarrow \quad (0, 1, 1) \quad + \quad (2, 0, 1)$

$\rightarrow \quad (0 \cdot 2^0 + 1 \cdot 2^m + 1 \cdot 2^{2m}) + (2 \cdot 2^0 + 0 \cdot 2^m + 1 \cdot 2^{2m})$

Problem:

2. $0 \times \{\ldots\} \rightarrow \infty + \{\ldots\}$ (but ∞ unavailable)

$\{\cup \cap \mathbf{x}\}$-circuits (continued)

$15 \times 20 \rightarrow \quad 2^0 3^1 5^1 \quad \times \quad 2^2 3^0 5^1$

$\rightarrow \quad (0, 1, 1) \quad + \quad (2, 0, 1)$

$\rightarrow \quad (0 \cdot 2^0 + 1 \cdot 2^m + 1 \cdot 2^{2m}) + (2 \cdot 2^0 + 0 \cdot 2^m + 1 \cdot 2^{2m})$

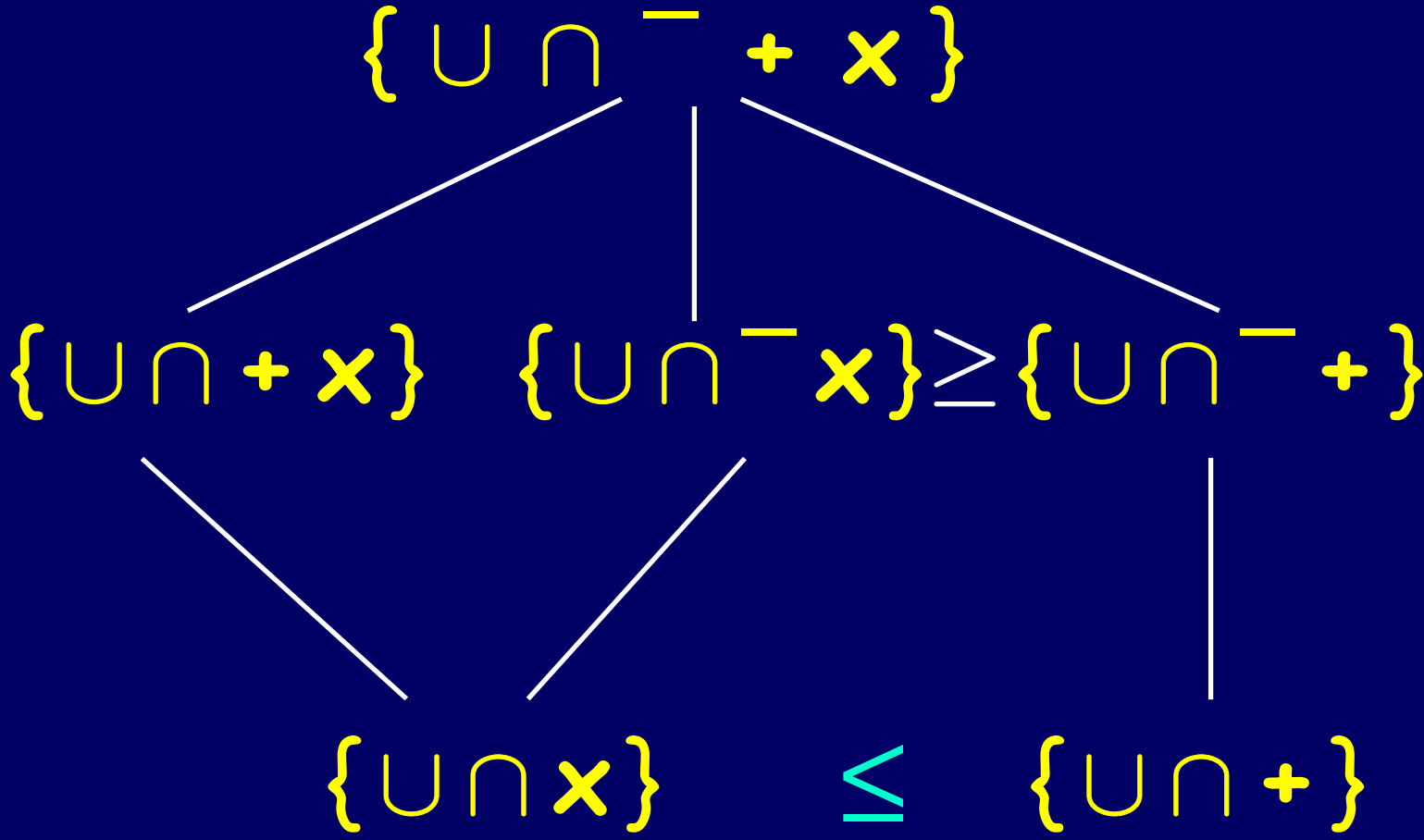
Soln: Replace each $+ \{\infty\}$ in vector circuit by

$$+ \{ 0, M, M+1, M+2, M+3, \ldots, M+\Delta \}$$

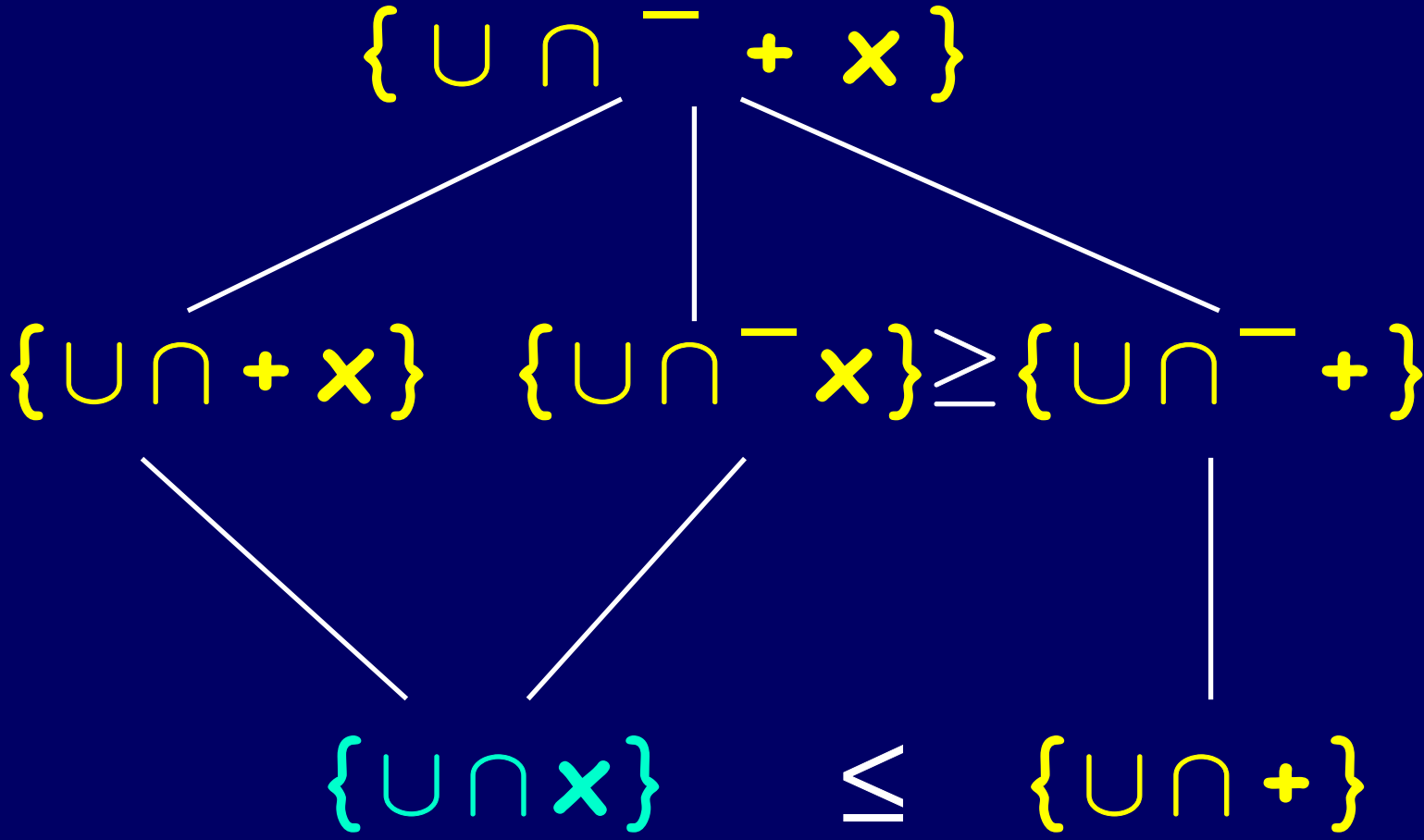
where M is larger than any accessible number and $\Delta = M^n$. Then ($\infty \in$ final S before) iff

($2M + \Delta \in$ final S after).

Some cases of circuits



Some cases of circuits



$\{\cup \cap \mathbf{x}\}$ PSPACE-hard: sketch

Poly time reduction from Quantified 3SAT:

$(\exists x_1 \forall x_2 \exists x_3 \ldots Q x_m)\ [H(x_1, x_2, x_3, \ldots, x_m)]$ (*)

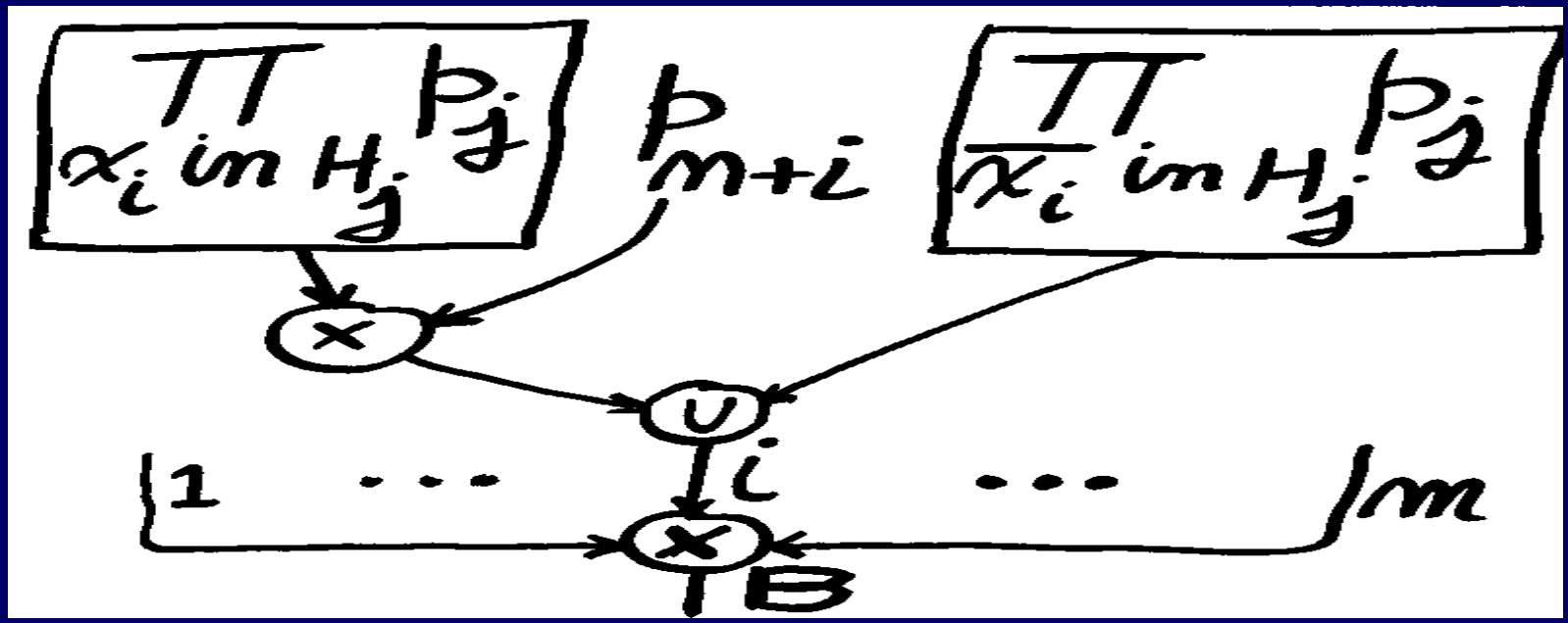
where

$H(x_1, x_2, x_3, \ldots, x_m) = H_1 \wedge H_2 \wedge H_3 \ldots \wedge H_n$

$H_j(x_1, x_2, x_3, \ldots, x_m) = (x_2 \vee \overline{x_5} \vee x_7)$

Construct circuit C such that (*) holds iff

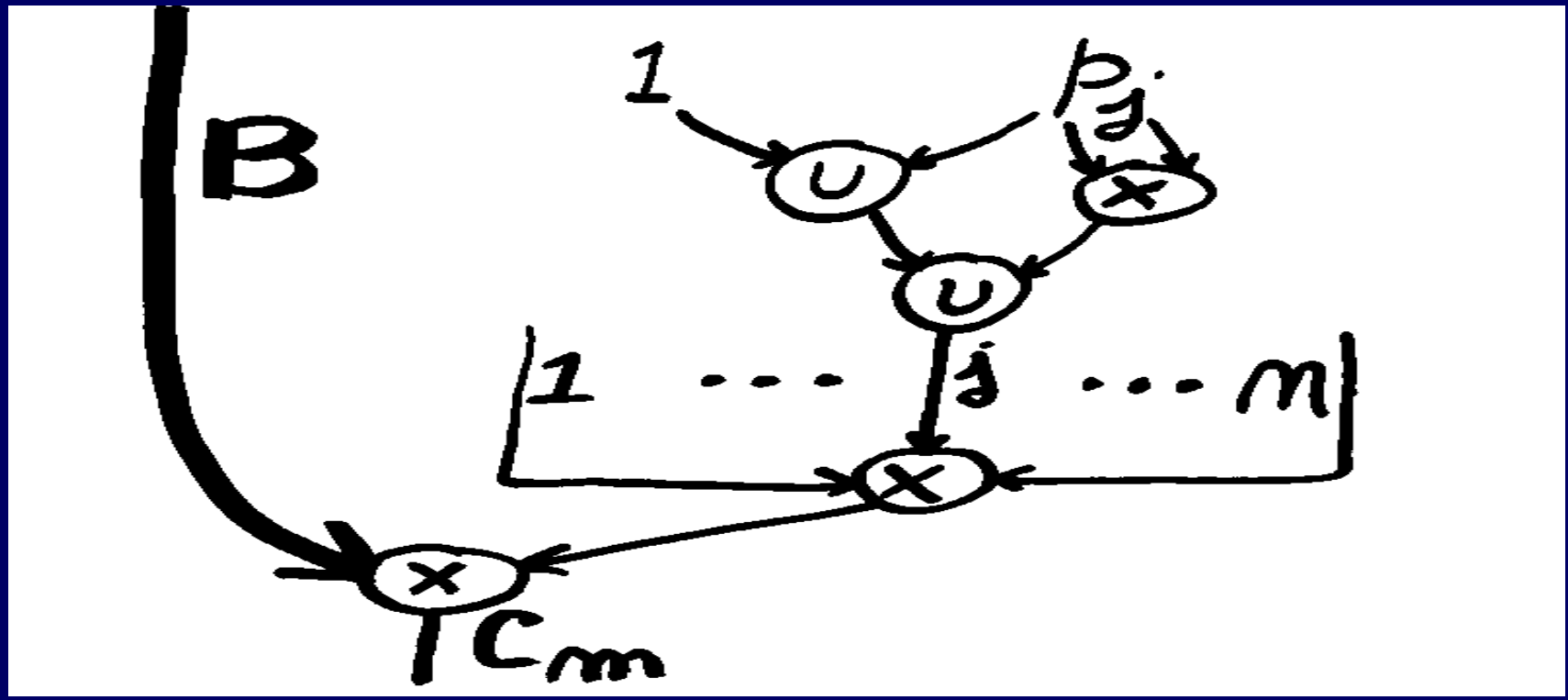
$$p_1^3\, p_2^3\, p_3^3 \ldots\, p_n^3\, p_{n+1}\, p_{n+2} \ldots\, p_{n+m} \in S(C)$$



Consider boolean assignment $A = (0, 1, 1, \ldots, 0)$.

Consider $q\ p_{n+1}^{\,0}\ p_{n+2}^{\,1}\ p_{n+3}^{\,1} \cdots\ p_{n+m}^{\,0} \in S(B)$:

p_1 occurs in q iff [A satisfies H_1]
p_2 occurs in q iff [A satisfies H_2]
... ...
p_n occurs in q iff [A satisfies H_n]



Boolean assignment (0, 1, 1, …, 0) satisfies H

iff

$p_1^3\, p_2^3\, p_3^3 \ldots\, p_n^3\, p_{n+1}^0\, p_{n+2}^1\, p_{n+3}^1 \ldots\, p_{n+m}^0 \in S(C_m)$.

$$(\exists x_m)\, H(\cdot, \cdot, \cdot, \ldots, x_m)$$

iff

$$H(\cdot, \cdot, \cdot, \ldots, 0) \;\vee\; H(\cdot, \cdot, \cdot, \ldots, 1)$$

iff

$$p_1^{3}\, p_2^{3}\, p_3^{3} \ldots\, p_n^{3}\, p_{n+1}^{\cdot}\, p_{n+2}^{\cdot}\, p_{n+3}^{\cdot} \ldots\, p_{n+m}^{0} \in S(C_m)$$

or $$p_1^{3}\, p_2^{3}\, p_3^{3} \ldots\, p_n^{3}\, p_{n+1}^{\cdot}\, p_{n+2}^{\cdot}\, p_{n+3}^{\cdot} \ldots\, p_{n+m}^{1} \in S(C_m)$$

iff

$$p_1^{3}\, p_2^{3}\, p_3^{3} \ldots\, p_n^{3}\, p_{n+1}^{\cdot}\, p_{n+2}^{\cdot}\, p_{n+3}^{\cdot} \ldots\, p_{n+m}^{1} \in S(C_{m-1})$$

$$(\forall x_m)\, H(\cdot, \cdot, \cdot, \ldots, x_m)$$

iff

$$H(\cdot, \cdot, \cdot, \ldots, 0) \;\wedge\; H(\cdot, \cdot, \cdot, \ldots, 1)$$

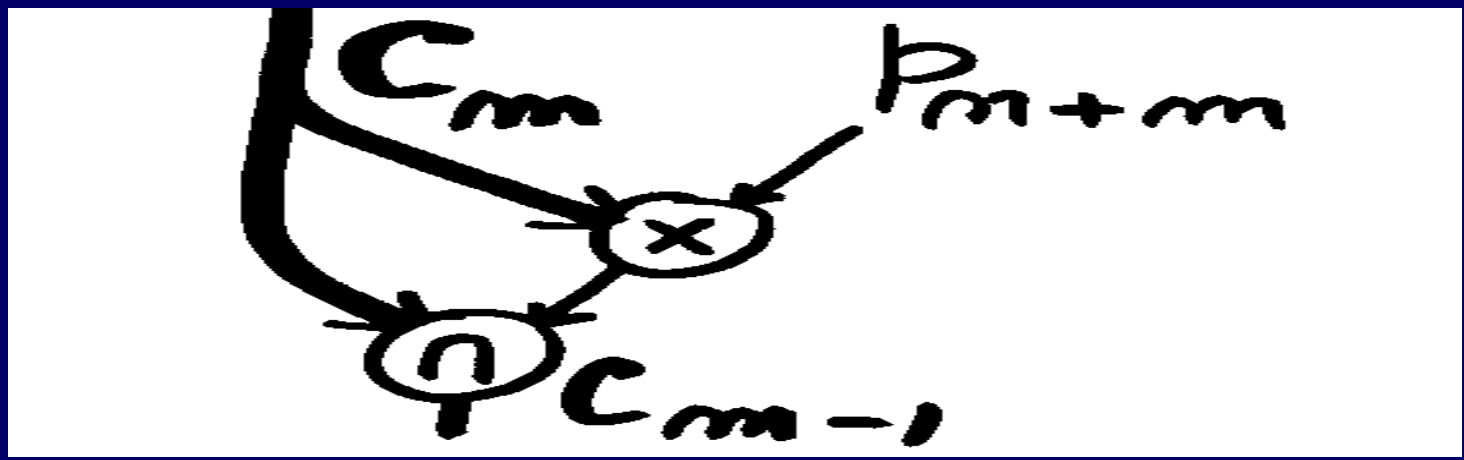
iff

$$p_1^{3}\, p_2^{3}\, p_3^{3} \ldots\, p_n^{3}\, p_{n+1}^{\cdot}\, p_{n+2}^{\cdot}\, p_{n+3}^{\cdot} \ldots\, p_{n+m}^{0} \in S(C_m)$$

and $$p_1^{3}\, p_2^{3}\, p_3^{3} \ldots\, p_n^{3}\, p_{n+1}^{\cdot}\, p_{n+2}^{\cdot}\, p_{n+3}^{\cdot} \ldots\, p_{n+m}^{1} \in S(C_m)$$

iff

$$p_1^{3}\, p_2^{3}\, p_3^{3} \ldots\, p_n^{3}\, p_{n+1}^{\cdot}\, p_{n+2}^{\cdot}\, p_{n+3}^{\cdot} \ldots\, p_{n+m}^{1} \in S(C_{m-1})$$



$\{\cup \cap \mathbf{x}\}$ PSPACE-hard: end.

Eventually,

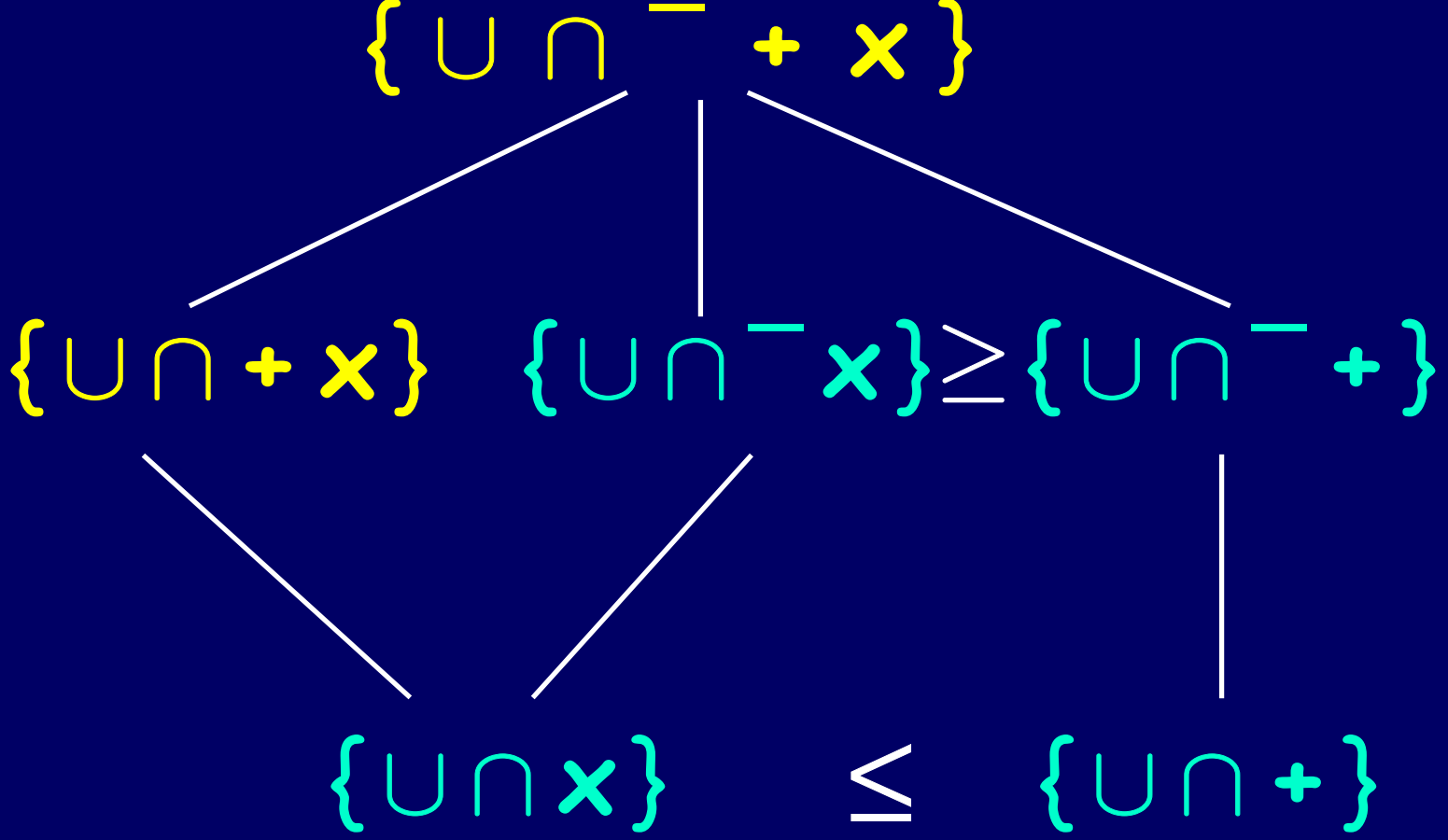
$(\exists x_1 \forall x_2 \exists x_3 \ldots Q x_n)\ [H(x_1, x_2, x_3, \ldots, x_m)]$

iff

$p_1^3\, p_2^3\, p_3^3 \ldots\, p_n^3\, p_{n+1}^1\, p_{n+2}^1\, p_{n+3}^1 \ldots\, p_{n+m}^1 \in S(C_0)$.

Slight modification proves PSPACE-hardness for $\{\cup \cap \bar{} \mathbf{x}\}$ formulas.

Some cases of circuits



PSPACE upper bounds

$\{\cup \cap^{-} \mathbf{x}\} \leq \{\cup \cap^{-} +\}$ "vector circuit" :

$15 \times 20 \rightarrow$	$2^0 3^1 5^1$	$\times$	$2^2 3^0 5^1$
$\rightarrow$	$(0, 1, 1)$	$+$	$(2, 0, 1)$

To handle complements:

1. Full prime decomposition into $p_1, p_2, p_3, \ldots, p_k$.
2. "Vector circuits" over $\mathbf{N}^{k+1} \cup \{ \infty \}$.

3. Automatically the number $p_1^* p_2^* p_3^* \ldots p_k^* q$ maps to (*, *, *, …, *, # of prime factors in q).

$\{\cup \cap^{-} +\}$ vector circuits in PSPACE:

Idea: alternating polynomial time proof starting at the output gate … but does it work?

Problem: verifying nonemptyness of the set feeding into a + gate when ∞ is its output.

Lemma: Every nonempty set computed anywhere in a $\{\cup \cap^{-} +\}$ vector-circuit over $\mathbf{N}^k \cup \{\infty\}$ intersects $\{1, 2, \ldots, 2^{n+1}\}^k \cup \{\infty\}$.

Some cases of circuits

$\{\cup, \cap, \neg, +, \times\}$

NEXPTIME-complete

$\{\cup, \cap, +, \times\}$

$\{\cup, \cap, \neg, \times\}$ $\{\cup, \cap, \neg, +\}$

PSPACE-complete

$\{\cup, \cap, \times\}$ $\{\cup, \cap, +\}$

{∪ ∩ + x} NEXPTIME-hard

3-line sketch:

1. New generic proof that nonemptyness for (union, intersection, concatenation)-circuits is NEXPTIME-hard.
2. Ensure that words in any computed set share a common length.
3. Use + and x to pack the binary word $w_1 w_2$ tightly as consecutive bits in a number.

{∪ ∩ + x} in NEXPTIME

Alternating proof needs expon time, so instead:

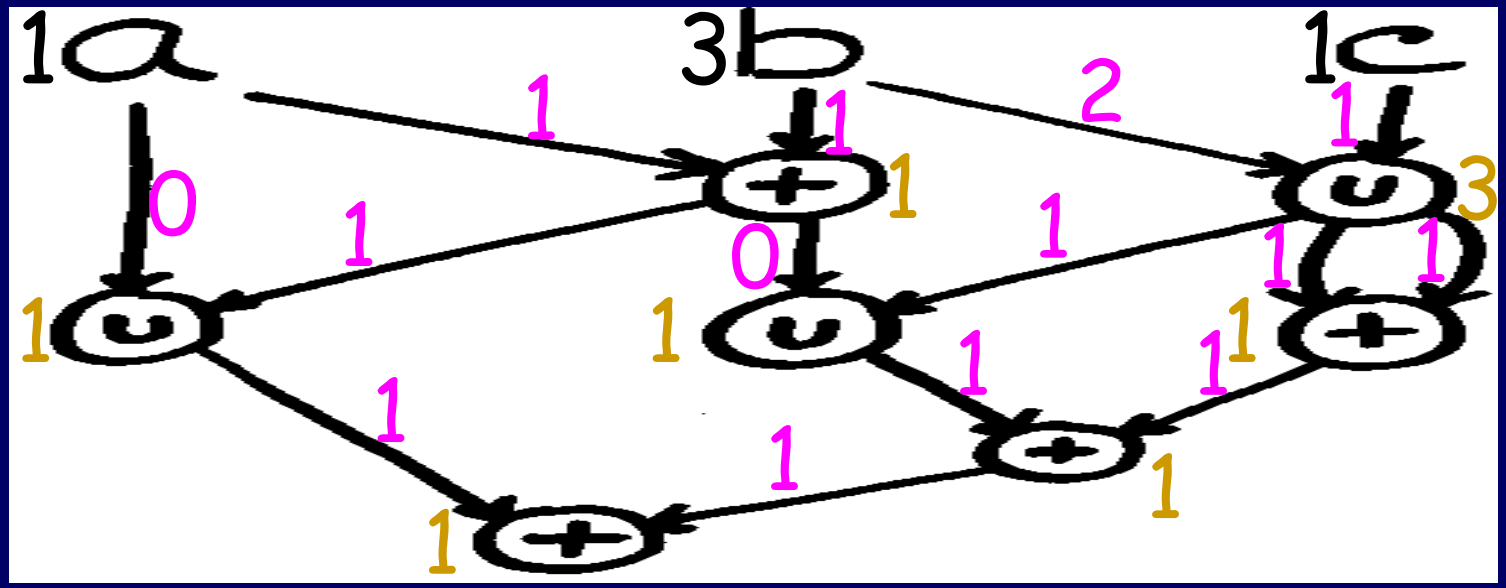
1. Expand circuit into an exponential size formula
2. Guess a proof tree, ie a minimal tree including
   - the output gate
   - a single input to any connected ∪ gate
   - both inputs to any ∩ or + or x gate
3. Guess for each edge in the tree a number less than the product of all the formula inputs
4. Accept iff consistent

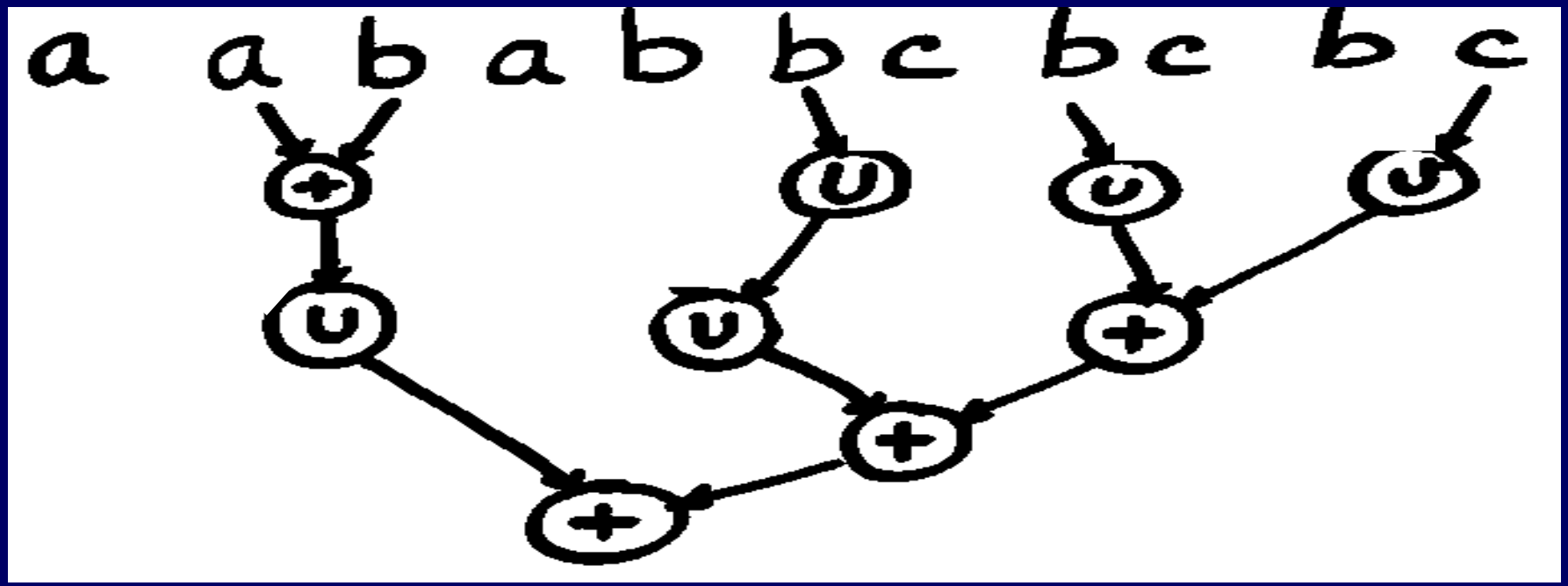
A nontrivial upper bound: $\{\cup, \times\}$ in NP

$\{\cup, \times\} \leq \{\cup, +\}$, so suffices to show

$\{\cup, +\}$ in NP

- Can't guess a « proof circuit » : why?
- Can't expand into a formula: too big.

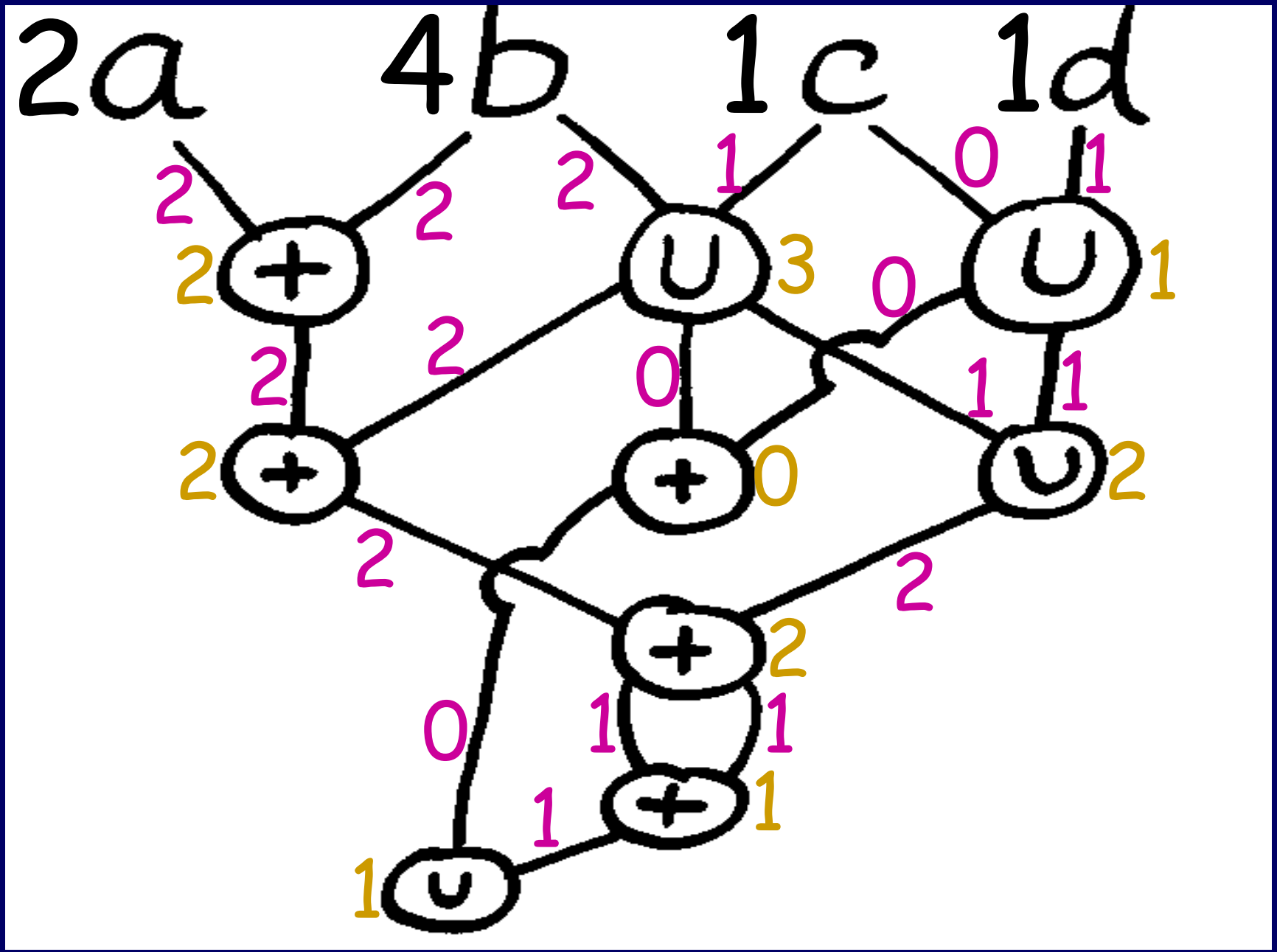

1a
3b
1c
1
2
0
1
0
1
3
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1


a
a b
a b
b c
b c
b c

{∪ +} in NP (continued)

Defn: A valuation assigns to each wire and to each gate a natural number:

1. The output gate gets 1
2. Both input wires to a + gate get the + gate
3. The input wires to a union gate get values that sum to the union gate
4. The output wires from any gate get values that sum to the gate


2a
4b
1c
1d

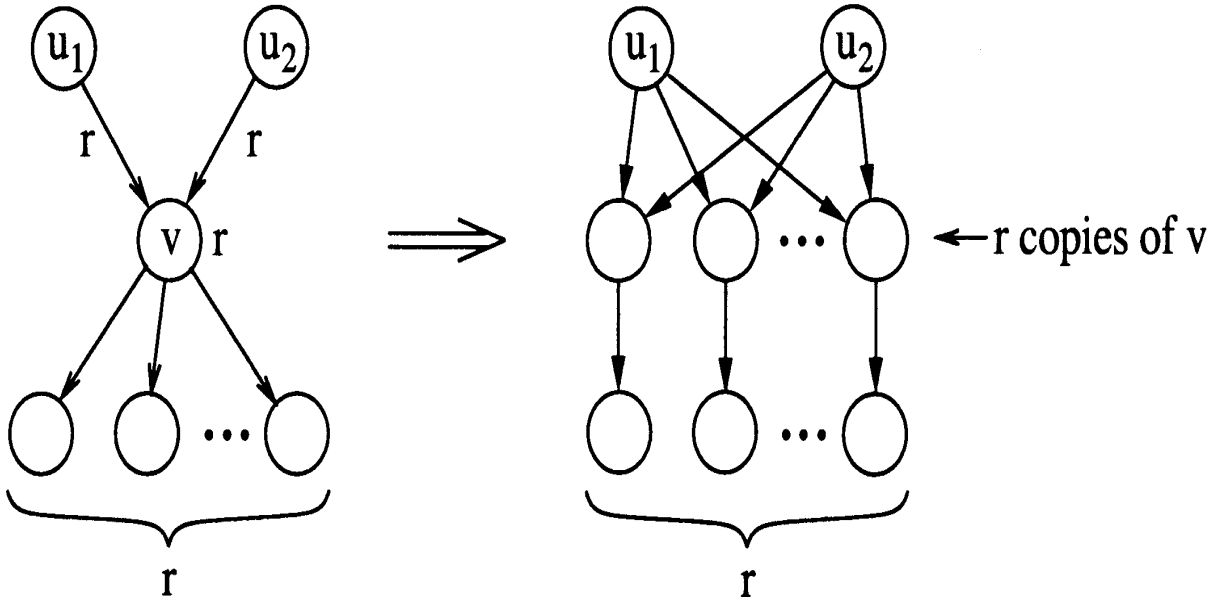
{∪ +} in NP (continued)

Claim:

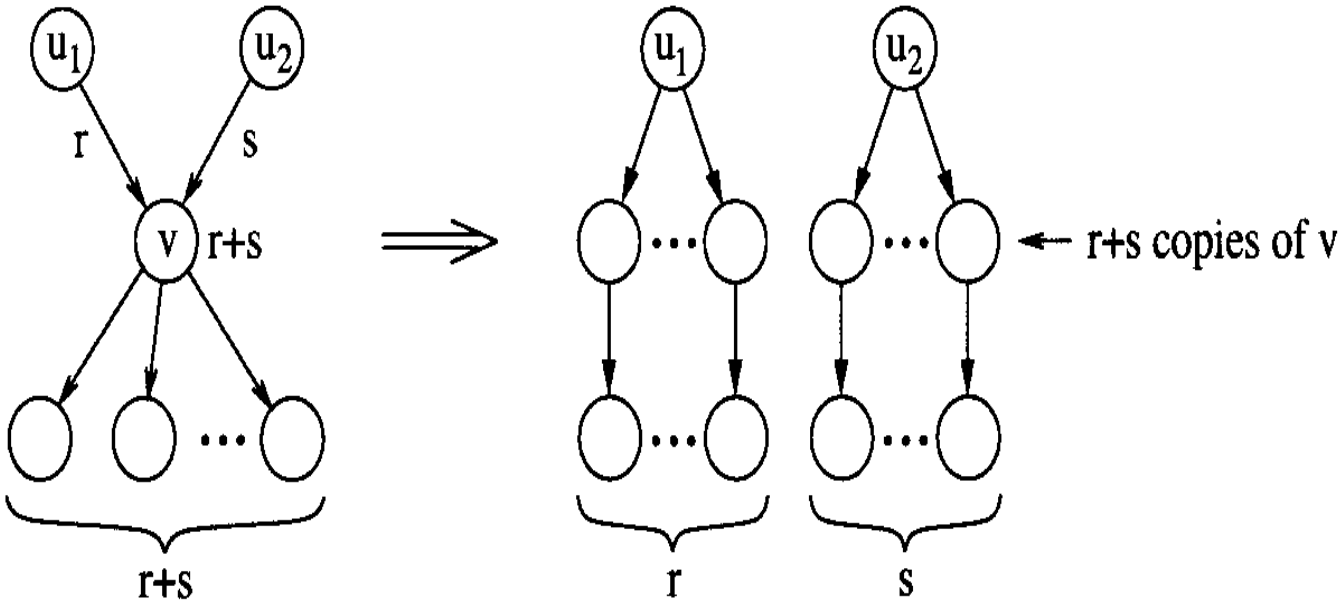
To each proof tree, in the huge formula blown up from the circuit, corresponds a (unique) valuation of the circuit.

To each valuation of the circuit corresponds (at least one) proof tree in the huge formula.

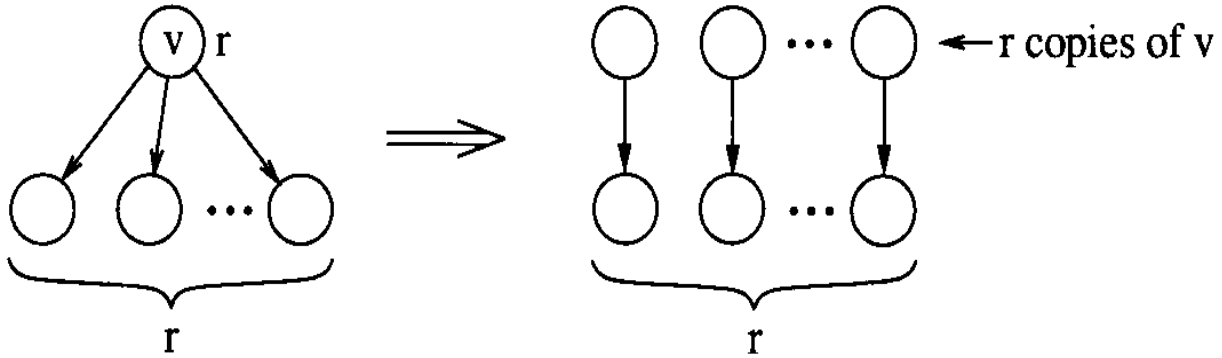
If v is a +-gate then apply:



If v is a $\cup$-gate then apply:



If v is an input gate then apply:



{∪ +} in NP (end)

NP algorithm:

1. Guess a valuation of the circuit
2. Sum the circuit inputs weighted according to the valuation
3. Accept if sum equals test integer t

Some cases of circuits

NEXPTIME-complete		$\{\cup, \cap, +, \times\}$
PSPACE-complete	$\{\cup, \cap, \bar{}, \times\}$	$\{\cup, \cap, \bar{}, +\}$
	$\{\cup, \cap, \times\}$	$\{\cup, \cap, +\}$
NP-complete	$\{\cup, \times\}$	$\{\cup, +\}$
		$\{\times, +\}$

{x +} P-complete

In P:

1. Locate all 0-gates
   - Non-zero inputs replaced by 1
   - x replaced by AND, + replaced by OR
2. If not done then
   - Delete 0-gates
   - Evaluate rest and reject if a number bigger than t is encountered

P-hard: using monotone Circuit Value Problem.

Some cases of circuits

NEXPTIME-complete		$\{\cup, \cap, +, \times\}$
PSPACE-complete	$\{\cup, \cap, \bar{}, \times\}$	$\{\cup, \cap, \bar{}, +\}$
	$\{\cup, \cap, \times\}$	$\{\cup, \cap, +\}$
NP-complete	$\{\cup, \times\}$	$\{\cup, +\}$
P-complete		$\{\times, +\}$
Complete for $C_=L$		$\{\cap, +\}$

Class $C_{=}L$

1. Class of the week (Fortnow Sept02 :-)
2. Languages of words on which a nondet logspace machine has an equal number of accepting and rejecting paths
3. Languages reducible to singular matrices [AlOg 96]

In $C_=L$: $\{\cap, +\}$ $C_=L$-complete

A. Reduce to {+} circuit equality:

1) Assume no empty intersection ever (else empty).
2) For each gate, build a separate {+} circuit computing the gate value under assumption (1)
3) Build two {+} circuits having equal values iff the circuit outputs t and assumption (1) holds.

B. Solve {+} circuit equality:

Modify the circuits so that their output values become the number of paths from the output to some input

$C_=L$-hard: view logspace machine configuration graph as circuit, and use other $C_=L$ characterization

Some cases of circuits

NEXPTIME-complete		$\{\cup, \cap, +, \times\}$
PSPACE-complete	$\{\cup, \cap, \overline{\ }, \times\}$	$\{\cup, \cap, \overline{\ }, +\}$
	$\{\cup, \cap, \times\}$	$\{\cup, \cap, +\}$
NP-complete	$\{\cup, \times\}$	$\{\cup, +\}$
P-complete		$\{\times, +\}$
Complete for $C_{=}L$	$\{+\}$	$\{\cap, +\}$

Some cases of circuits

NEXPTIME-complete		$\{\cup, \cap, +, \times\}$
PSPACE-complete	$\{\cup, \cap, \bar{}, \times\}$	$\{\cup, \cap, \bar{}, +\}$
	$\{\cup, \cap, \times\}$	$\{\cup, \cap, +\}$
NP-complete	$\{\cup, \times\}$	$\{\cup, +\}$
P-complete		$\{\times, +\}$
$C_=L$-complete $\{+\}$		NL-complete $\{\times\}$

Open

1. Decidability of $\{ \cup \cap \overline{\ } + \times \}$
2. Some specific cases:
   - P versus co-R for $\{ \cap + \times \}$
   - $C_=L$ versus P for $\{ \cap \times \}$
   - Some formulas
3. GCD-free basis versus GCD

Thanks to Steven Rudich for the blue color

$\mathcal{O}$	MC($\mathcal{O}$) lower bound	MC($\mathcal{O}$) upper bound	Thm.	MF($\mathcal{O}$) lower bound	MF($\mathcal{O}$) upper bound	Thm.
$\cup, \cap, ^-, +, \times$	NEXPTIME	?	6.4	PSPACE	?	5.5
$\cup, \cap, +, \times$	NEXPTIME	NEXPTIME	6.2	NP	NP	4.4
$\cup, +, \times$	PSPACE	PSPACE	5.1	NP	NP	4.4
$\cap, +, \times$	P	co-R	8.3	-	DLOGCFL	9.2
$+, \times$	P	P	7.1	-	DLOGCFL	9.2
$\cup, \cap, ^-, +$	PSPACE	PSPACE	5.5	PSPACE	PSPACE	5.1
$\cup, \cap, +$	PSPACE	PSPACE	5.5	NP	NP	4.4
$\cup, +$	NP	NP	4.4	NP	NP	4.4
$\cap, +$	$C_=L$	$C_=L$	8.2	-	L	9.5
$+$	$C_=L$	$C_=L$	8.2	-	L	9.5
$\cup, \cap, ^-, \times$	PSPACE	PSPACE	5.5	PSPACE	PSPACE	5.5
$\cup, \cap, \times$	PSPACE	PSPACE	5.5	NP	NP	4.4
$\cup, \times$	NP	NP	4.4	NP	NP	4.4
$\cap, \times$	$C_=L$	P	8.4	-	L	9.5
$\times$	NL	NL	8.5	-	L	9.5
$\cup, \cap, ^-$	P	P	7.2	NC^1	NC^1	9.3
$\cup, \cap$	P	P	7.2	-	NC^1	9.4
$\cup$	NL	NL	9.1	-	NC^1	9.4
$\cap$	NL	NL	9.1	-	NC^1	9.4

Encoding a case statement on distinct cases: $a_1, a_2, a_3, \ldots, a_{k+1}$.

For all $1 \leq \cup \in \forall \exists \subseteq \supseteq \infty \neg \emptyset$

$\equiv \sim \cdot \geq - \times \div \cap \wedge \vee \approx$ **$j \leq k+1$**

—

For all **1** $\leq \cup \acute{\in} \forall \exists \subseteq \supseteq \infty \neg \emptyset$

$\equiv \sim \cdot \geq - \times \div \cap \wedge \vee \approx$ **$j \leq k+1$**

—

define $h_j(X) \doteq \Pi_{i \neq j} (X - a$

Enc $a_1, a_2, a_{432}, \ldots, a_{k+1}$.

$\{ \cup \cap \bar{} + \times \}$-circuits

For all $1 \leq \cup \in \forall \exists \subseteq \supseteq \infty \neg \emptyset$

$\equiv \sim \cdot \geq - \times \div \cap \wedge \vee \approx$ $j \leq k+1$

define $h_j(X) = \prod_{i \neq j} (X - a$

$\{ \cup \cap \bar{} + \times \}$-circuits