# Satisfiability of Algebraic Circuits over Sets of Natural Numbers

Christian Glaßer, Christian Reitwießner, Stephen Travers, Matthias Waldherr

Department of Computer Science
University of Würzburg, Germany

FSTTCS 2007, New Delhi, India

# Previous Work

Most important papers on algebraic circuits:

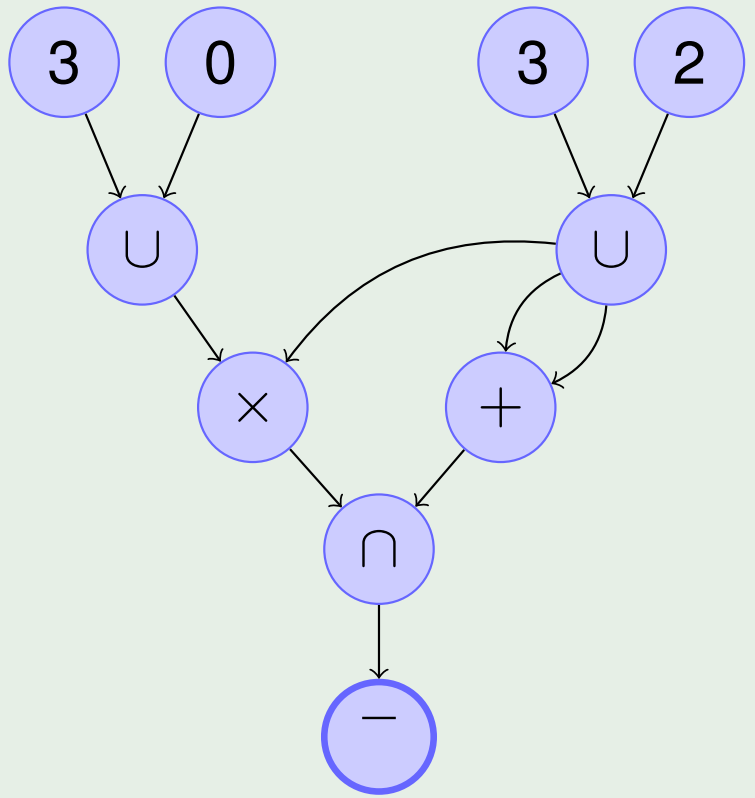
- 1973 Stockmeyer and Meyer
- 1984 Wagner
- 2000 Yang
- 2003 McKenzie and Wagner

# Definition of Algebraic Circuits

## Definition (Algebraic $\mathcal{O}$-Circuit)

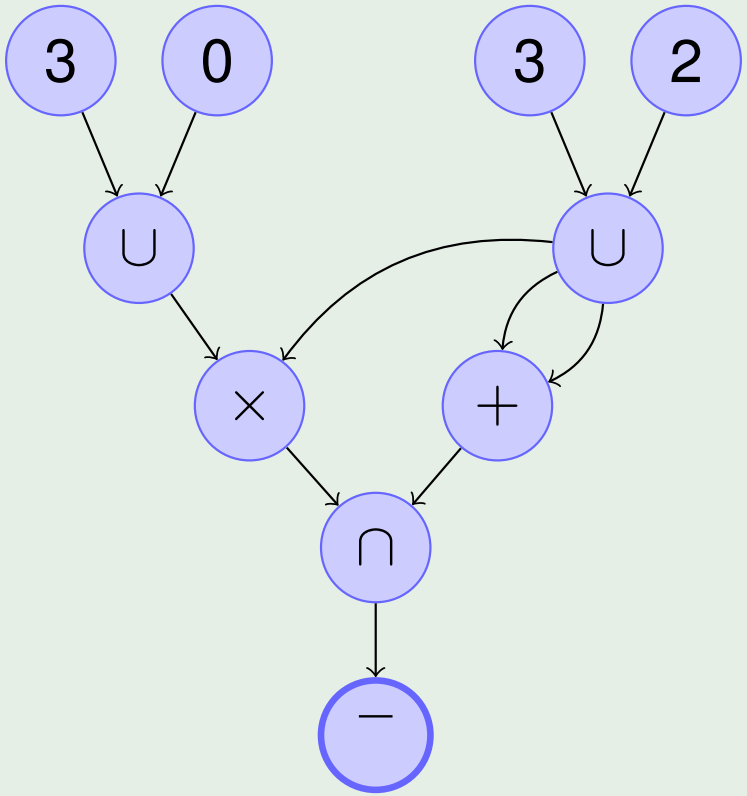
- Finite, directed, acyclic graph
- Several input gates, one output gate
- Input gates: indegree 0, label: natural number
- Other gates: label from $\mathcal{O} \subseteq \{\overline{\ }, \cup, \cap, +, \times\}$, $\overline{\ }$-gates: indegree 1, all other gates: indegree 2

## Example



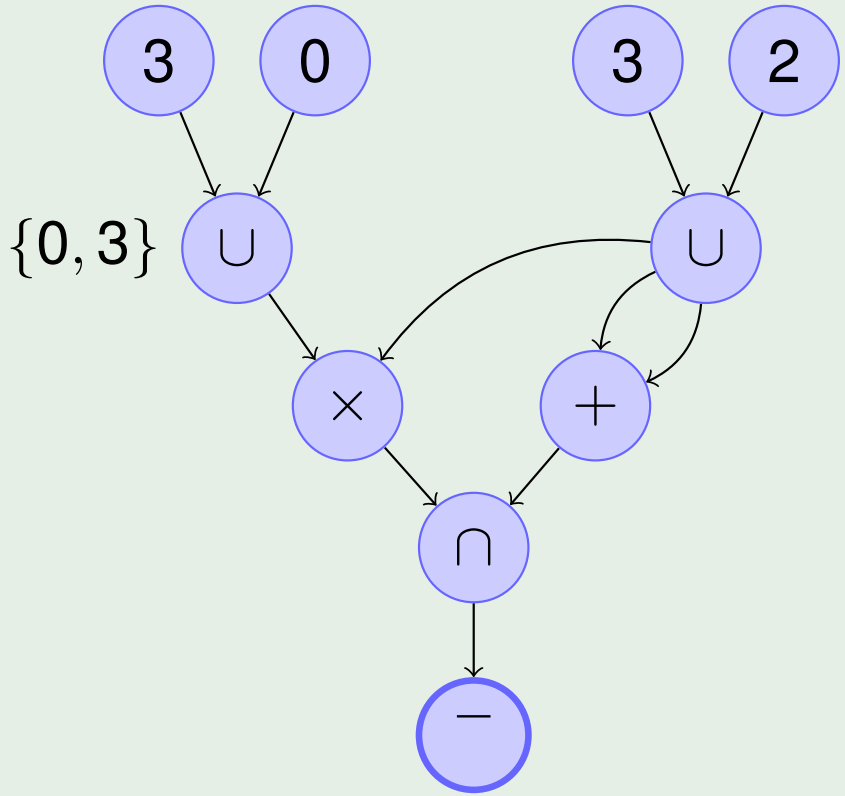
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



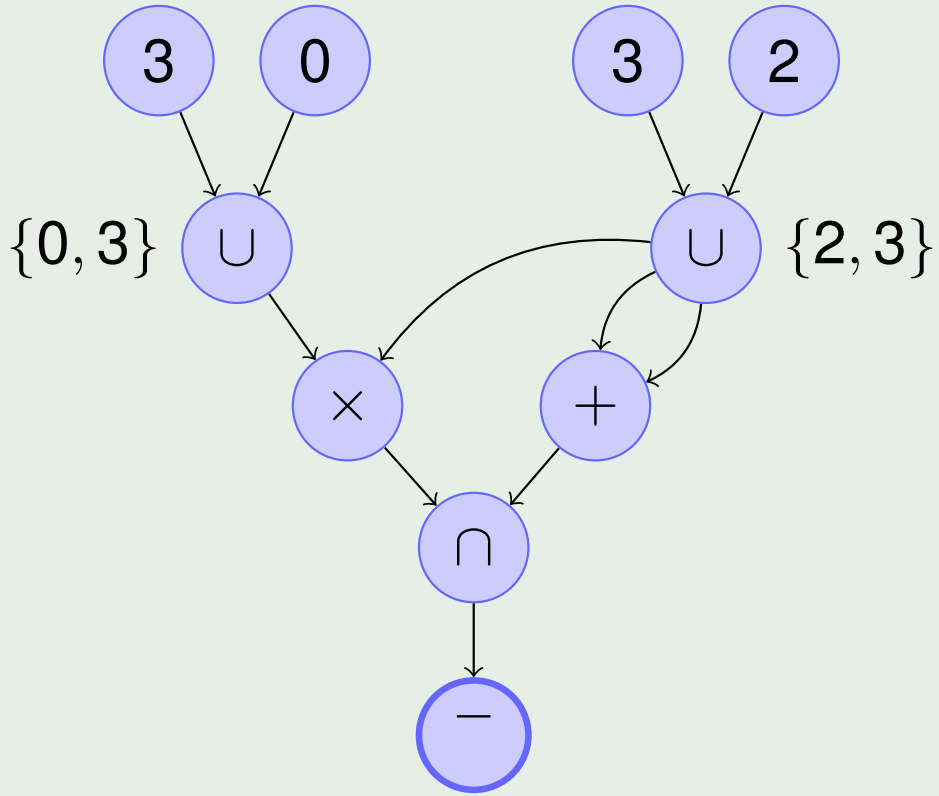
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



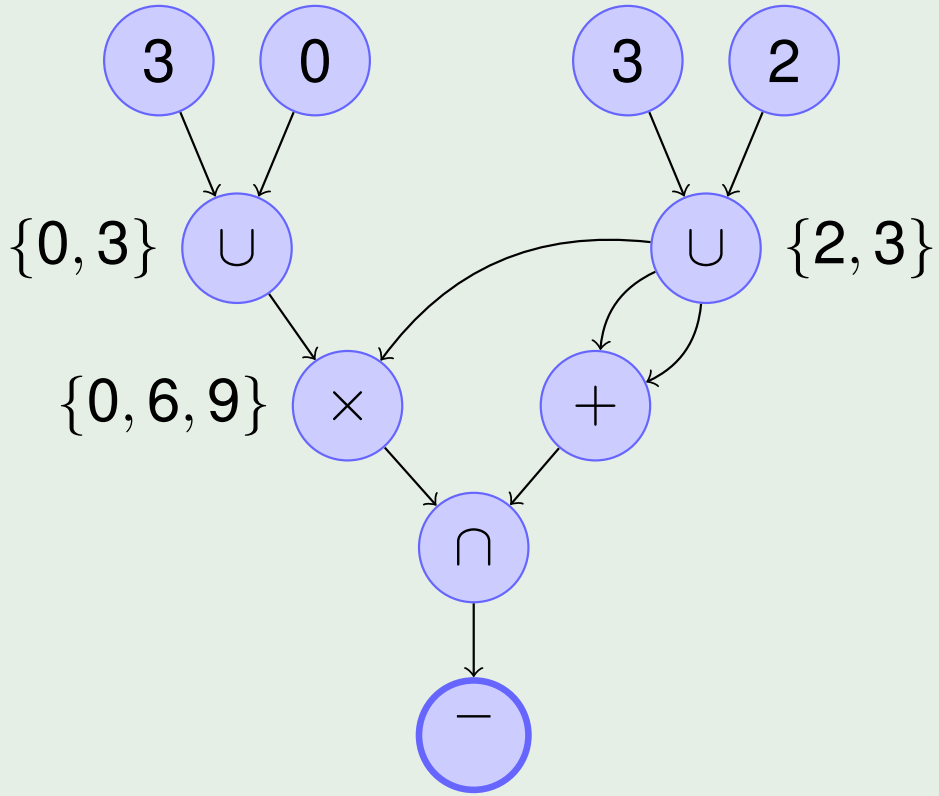
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



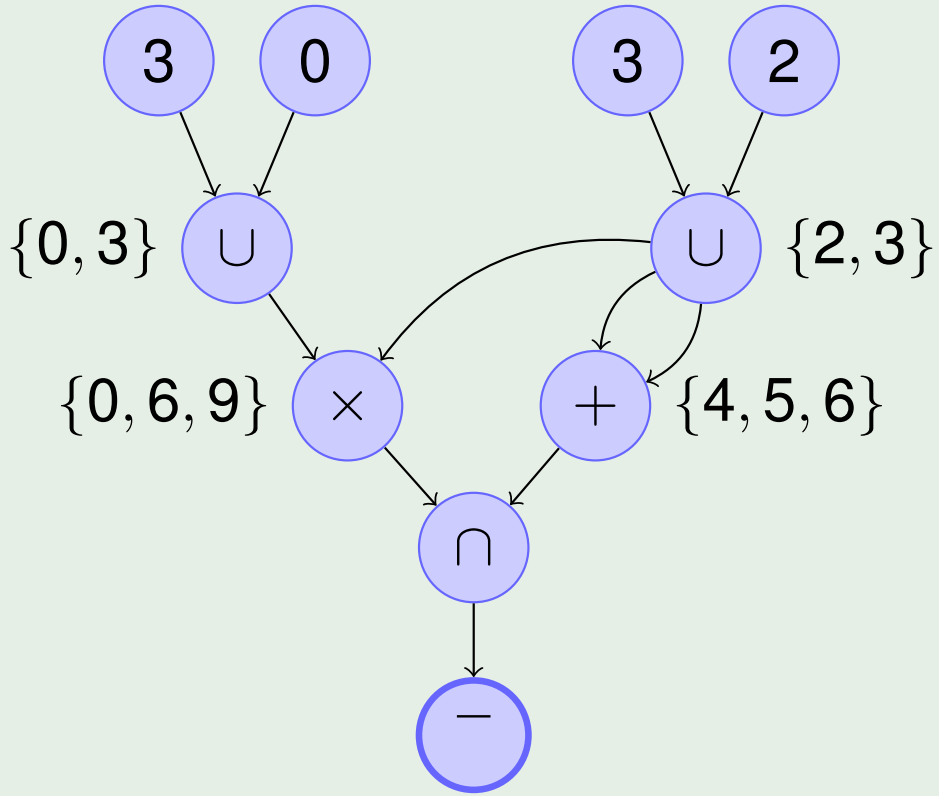
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



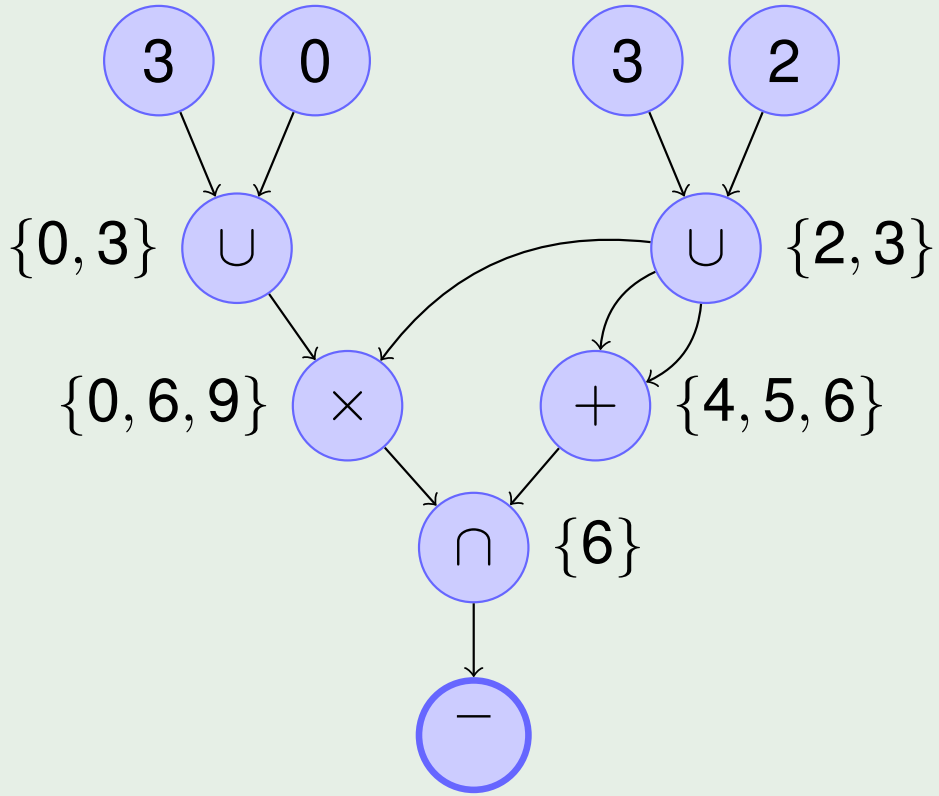
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



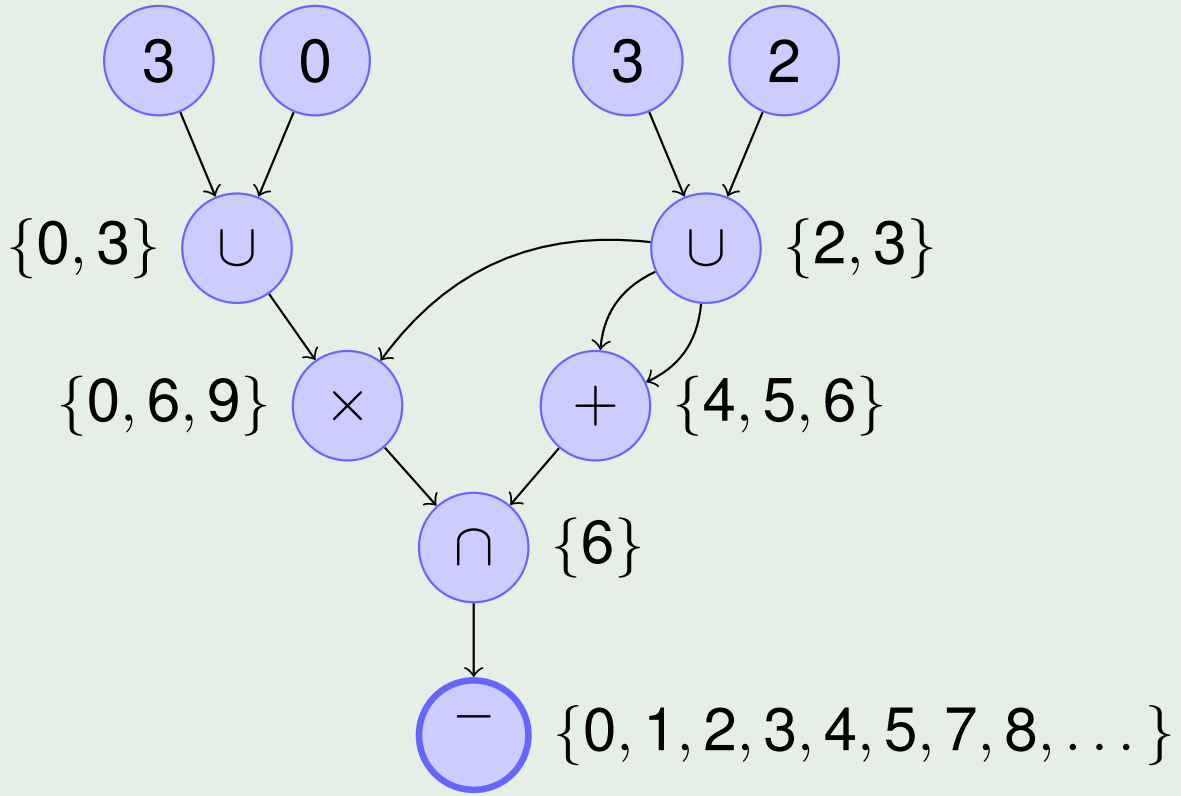
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



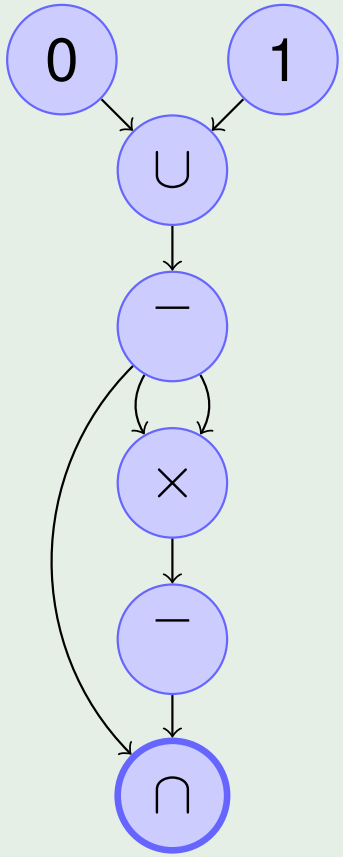
# Sets Computed by an Algebraic Circuit

## Example (Algebraic Circuit and Its Computed Sets)



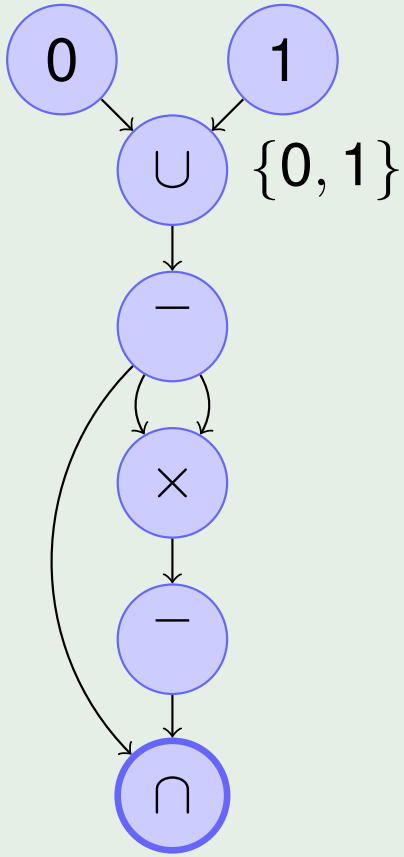
# A More Sophisticated Example For a Circuit

## Example (More Sophisticated Circuit)



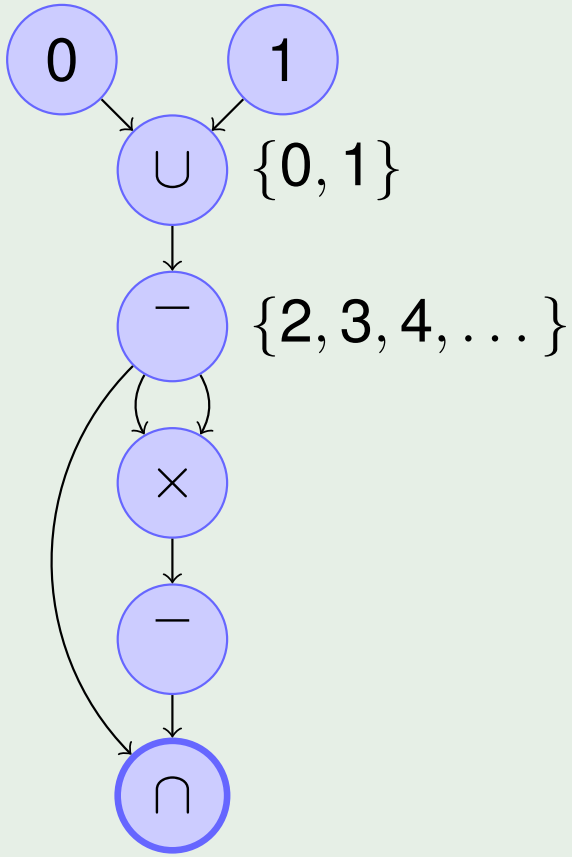
# A More Sophisticated Example For a Circuit

## Example (More Sophisticated Circuit)



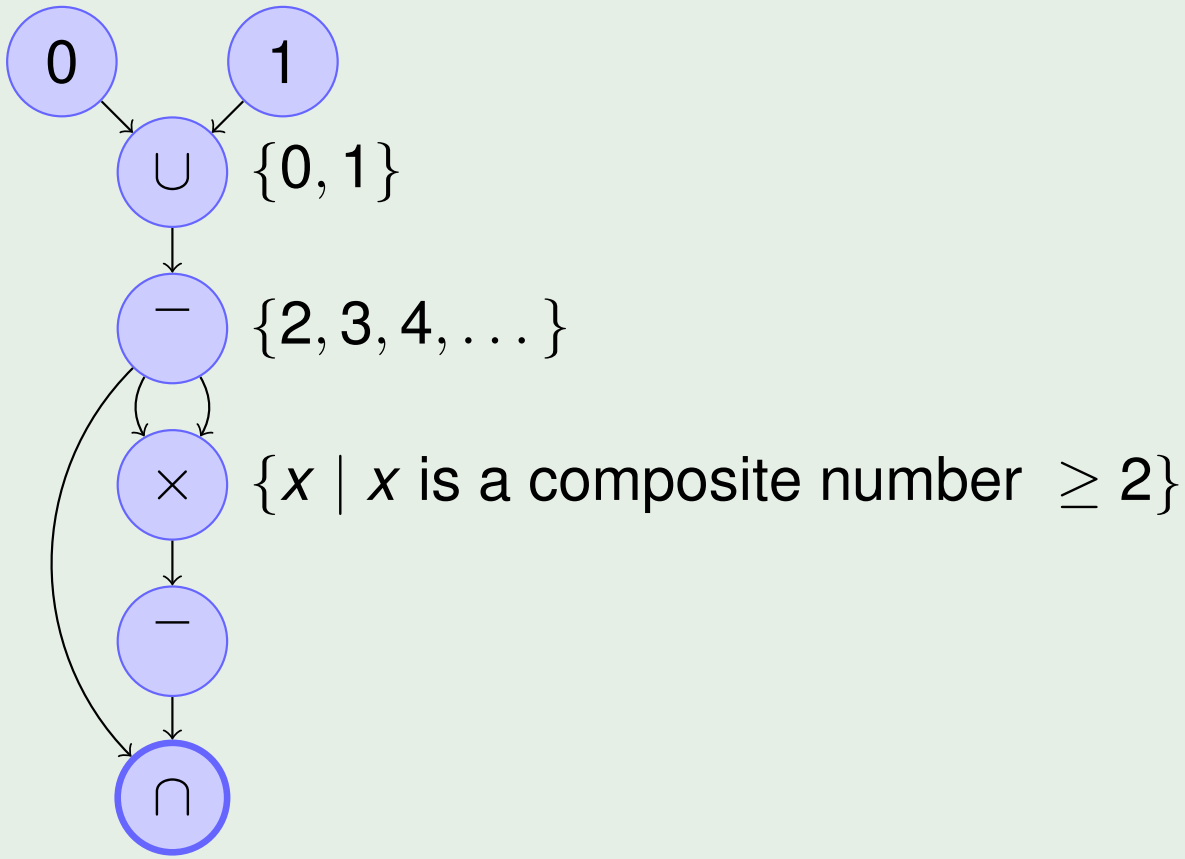
# A More Sophisticated Example For a Circuit

## Example (More Sophisticated Circuit)



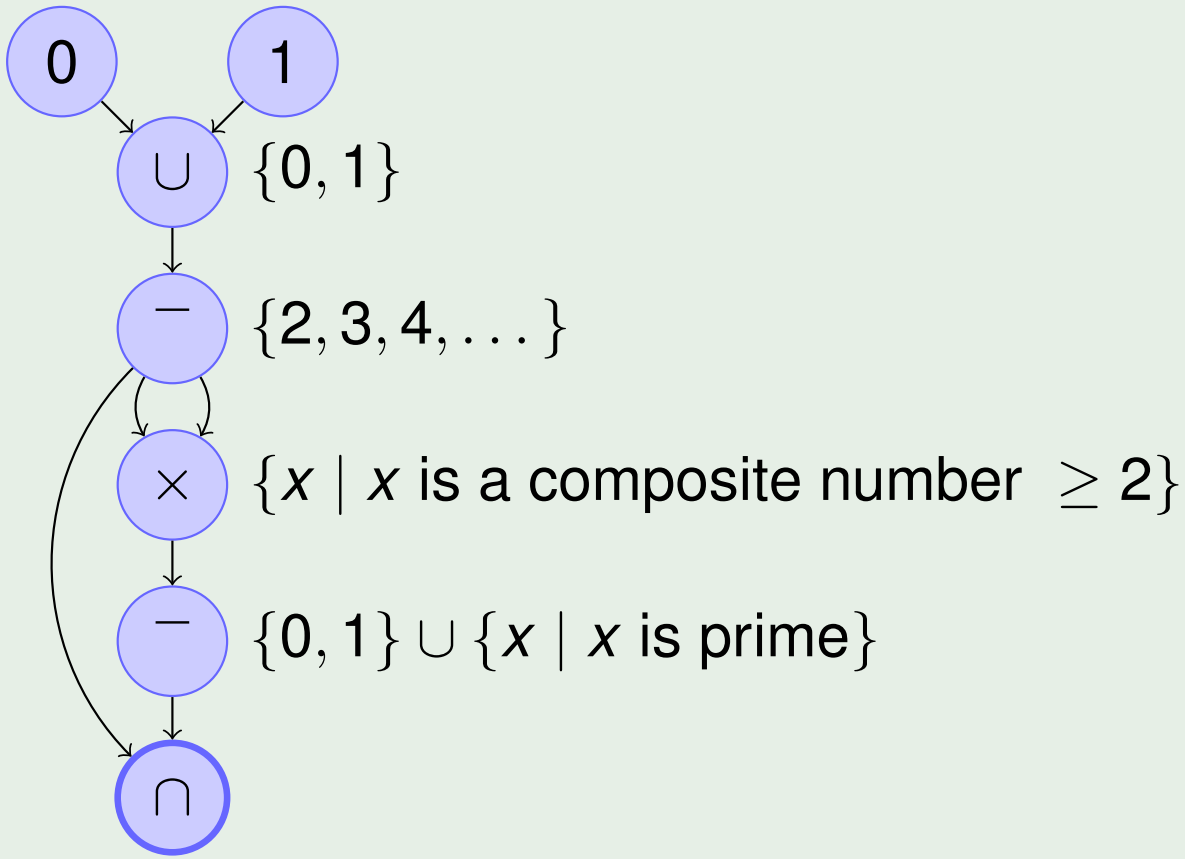
# A More Sophisticated Example For a Circuit

## Example (More Sophisticated Circuit)



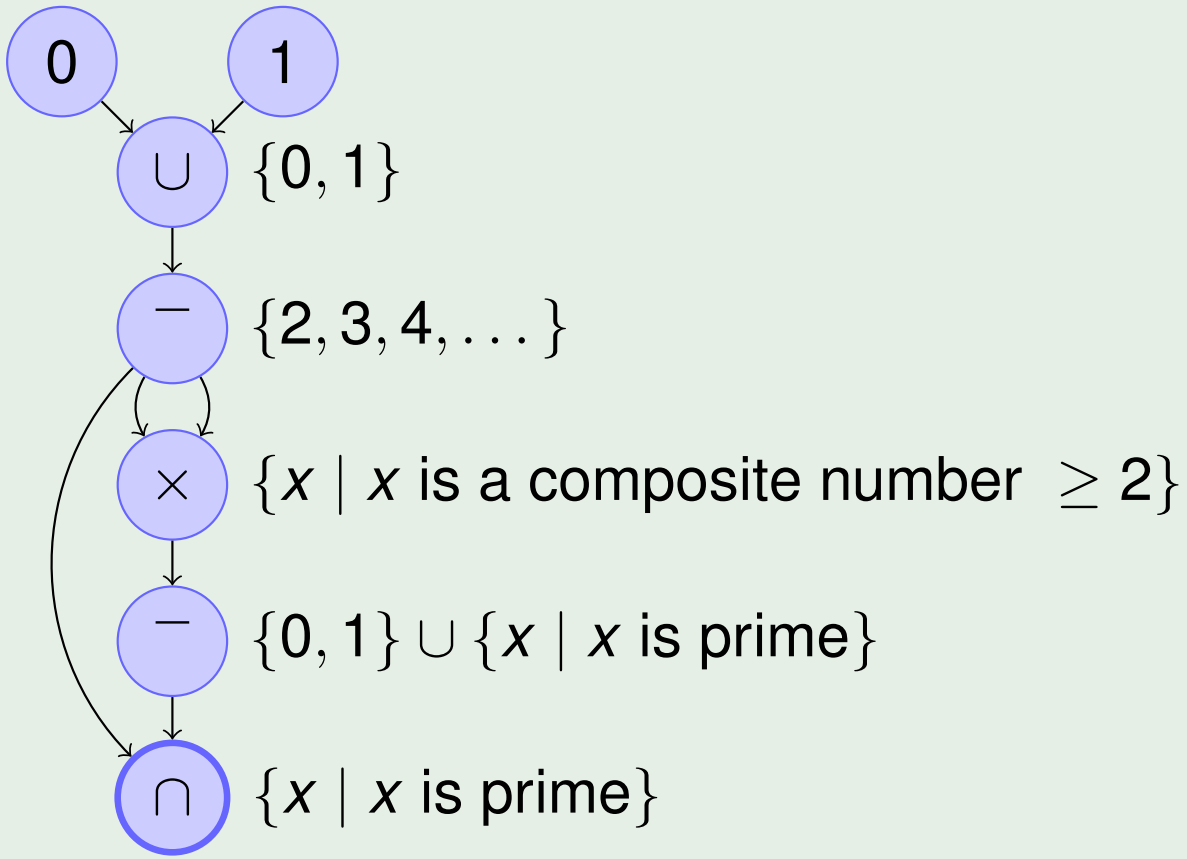
# A More Sophisticated Example For a Circuit

## Example (More Sophisticated Circuit)



# A More Sophisticated Example For a Circuit

## Example (More Sophisticated Circuit)



# Membership Problems for Algebraic Circuits

## Definition (Membership Problems)

Given a circuit $C$ and a number $b \in \mathbb{N}$, is $b \in I(C)$?

$\mathrm{MC}(\mathcal{O}) := \{(C, b) \mid C \text{ is an } \mathcal{O}\text{-circuit}, b \in \mathbb{N} \text{ and } b \in I(C)\}$

- Different problems with different complexities for different subsets $\mathcal{O} \subseteq \{\overline{\ }, \cup, \cap, +, \times\}$.
- Extensive study by McKenzie and Wagner in 2003.
- Complexity ranges from NL to NEXPTIME.
- Major open problem: Unknown if $\mathrm{MC}(\overline{\ }, \cup, \cap, +, \times)$ (i.e. the general problem) is decidable or not.

# Complexity of the General Membership Problem

A terminating algorithm for MC($^{-}, \cup, \cap, +, \times$) would solve Goldbach's conjecture (and many other number-theoretic problems):

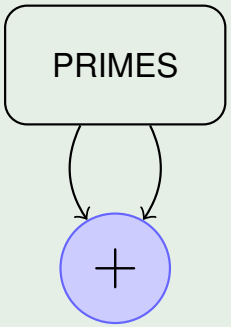
## Goldbach's Conjecture (1742)

*Every even integer greater than 2*
*can be written as the sum of two primes.*

# Complexity of the General Membership Problem

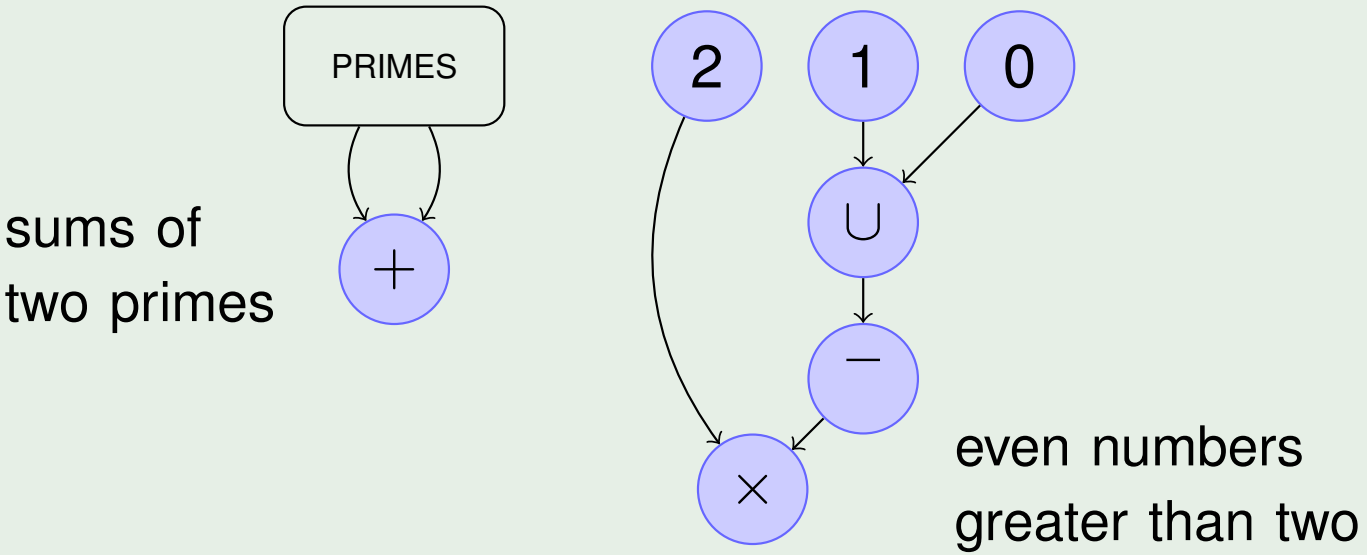
## Example (Circuit for Goldbach's Conjecture)

sums of two primes



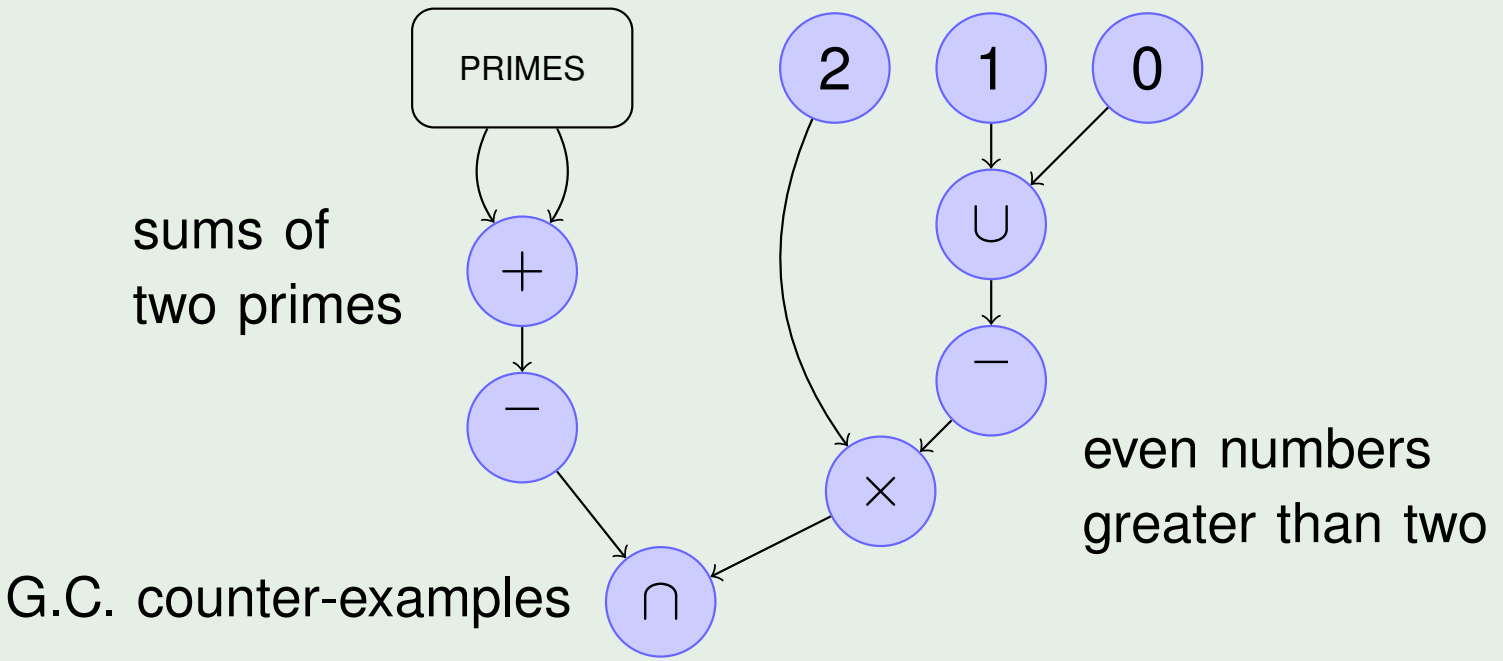
# Complexity of the General Membership Problem

## Example (Circuit for Goldbach's Conjecture)



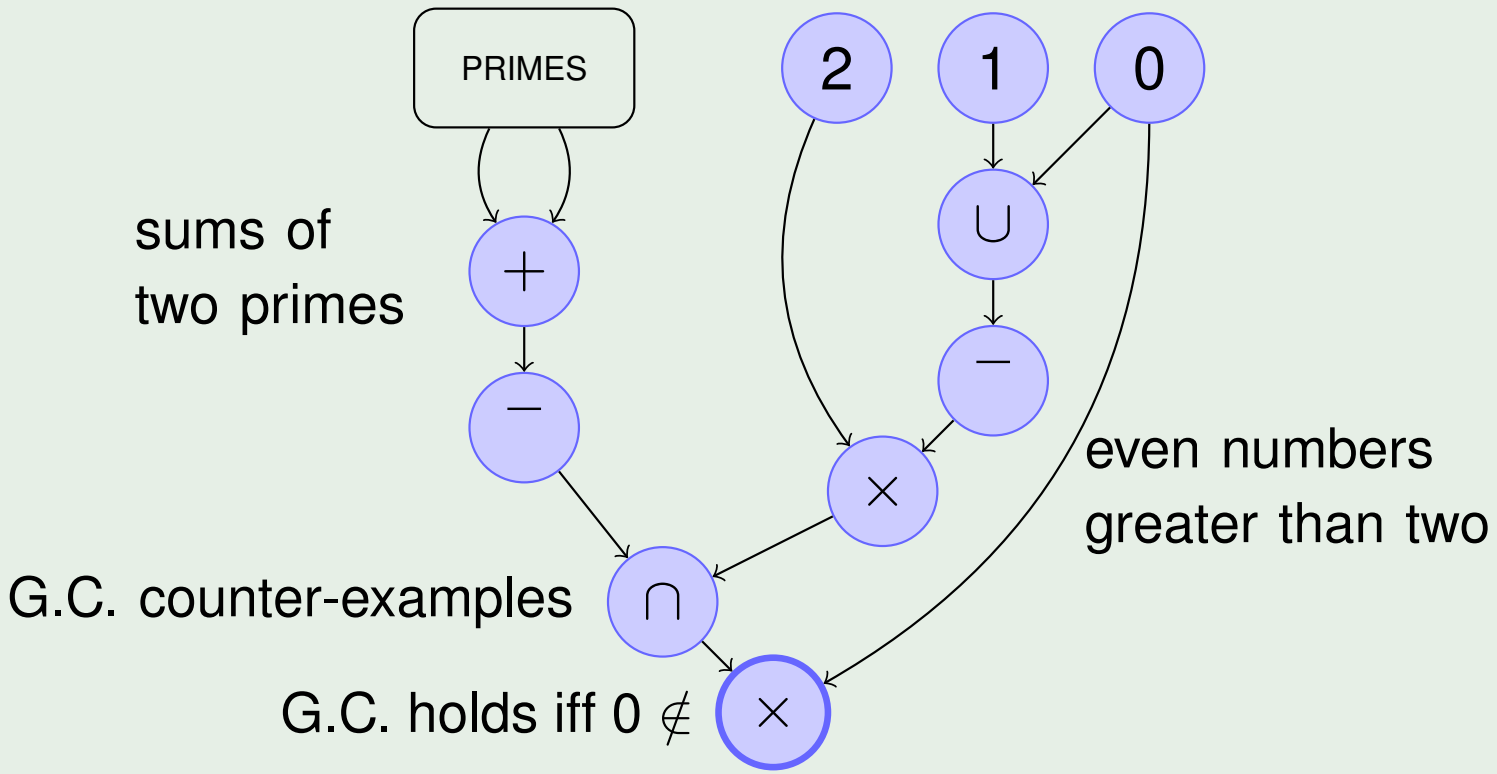
# Complexity of the General Membership Problem

## Example (Circuit for Goldbach's Conjecture)



# Complexity of the General Membership Problem

## Example (Circuit for Goldbach's Conjecture)



# Satisfiability Problems for Algebraic Circuits

## Satisfiability Problems

- showing MC($^-, \cup, \cap, +, \times$) undecidable seems out of reach
- but it could be done for a generalization of MC($^-, \cup, \cap, +, \times$)
- our approach: introduction of variables

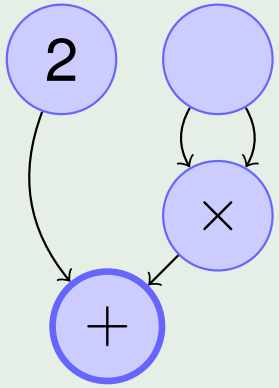
# Definition of Satisfiability Problems

## Definition (Satisfiability Problems)

$$\mathrm{SC}(\mathcal{O}) := \{(C, b) \mid C \text{ is an } \mathcal{O}\text{-circuit with some unlabeled input gates } (x_1, x_2, \ldots, x_n), b \in \mathbb{N} \text{ and there is an assignment } (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n \text{ of these inputs such that } b \in I(C(a_1, a_2, \ldots, a_n))\}$$

# Example for Satisfiability

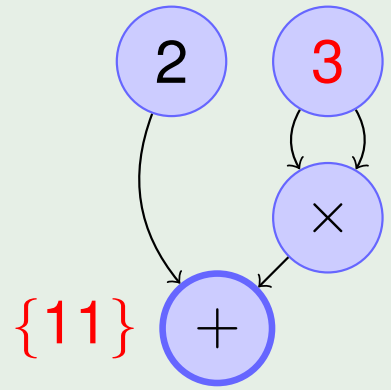
## Example (Satisfiability of an Algebraic Circuit)

$C :=$ 


Is $(C, 11) \in \mathrm{SC}(\{+, \times\})$?

# Example for Satisfiability

## Example (Satisfiability of an Algebraic Circuit)

$C :=$ 


Is $(C, 11) \in \mathrm{SC}(\{+, \times\})$? Yes!

# Undecidability of SC($\cap, +, \times$)

**Theorem**

*SC($\cap, +, \times$) is undecidable (and thus also SC($\overline{\ }, \cup, \cap, +, \times$)).*

**Proof Idea.**

Reduction from Diophantine Equations.
Minor obstacle to overcome:
Circuits cannot use negative numbers. □

# Complexities of the Satisfiability Problems

| $\mathcal{O}$ | Lower Bound | Upper Bound |
|---|---|---|
| $^{-}\cup\cap+\times$ | undecidable | |
| $^{-}\cup\cap+$ | PSPACE | PSPACE |
| $^{-}\cup\cap\ \times$ | PSPACE | |
| $^{-}\cup\cap$ | NP | NP |
| $\cup\cap+\times$ | undecidable | |
| $\cup\cap+$ | PSPACE | PSPACE |
| $\cup\cap\ \times$ | PSPACE | NEXP |
| $\cup\cap$ | P | P |
| $\cup\ +\times$ | PSPACE | PSPACE |
| $\cup\ +$ | NP | NP |
| $\cup\ \times$ | NP | NP |
| $\cup$ | NL | NL |
| $\cap+\times$ | undecidable | |
| $\cap+$ | NP | NP |
| $\cap\ \times$ | NP | NP |
| $\cap$ | NL | NL |
| $+\times$ | NP | NP |
| $+$ | NP | NP |
| $\times$ | NL | UP $\cap$ coUP |

# Open Problems

## Open Problems

- Is SC($\overline{\ }, \cup, \cap, +$) decidable or not?
- Exact complexity of SC($\times$) (connections to factorization)
- And of course the decidability/undecidability of MC($\overline{\ }, \cup, \cap, +, \times$)