Virtual Substitution for SMT-Solving

Florian Corzilius Erika Ábrahám

RWTH Aachen University, Germany

18^{th} International Symposium on Fundamentals of Computation Theory

August 23rd, 2011

Oslo

Motivation

Are there solutions for x, y in the domain $\mathbb{R}$, such that:

$$(y = 0 \lor y^2 + 1 < 0) \land x - 3 \leq 0 \land xy + 1 < 0$$

Motivation

Are there solutions for $x,\ y$ in the domain $\mathbb{R}$, such that:

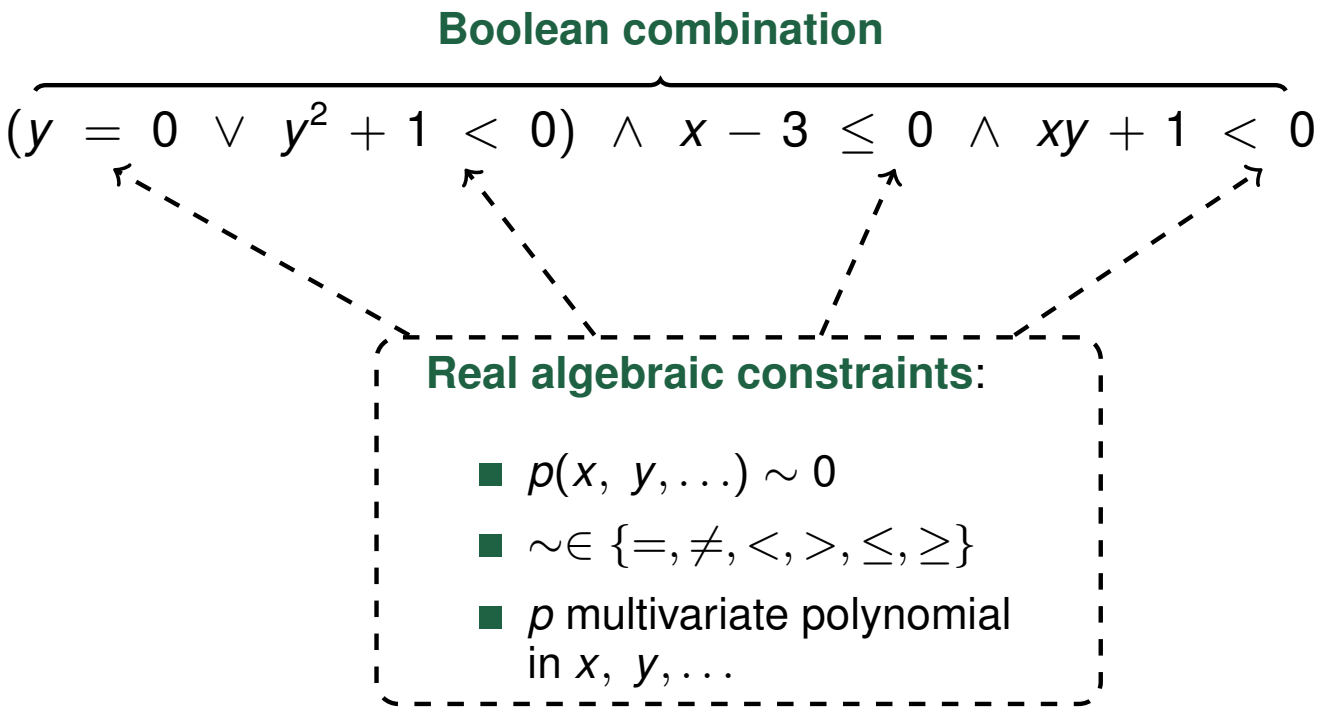
$$(y = 0 \lor y^2 + 1 < 0) \land x - 3 \leq 0 \land xy + 1 < 0$$

Real algebraic constraints:

- $p(x,\ y, \ldots) \sim 0$
- $\sim \in \{=, \neq, <, >, \leq, \geq\}$
- p multivariate polynomial in $x,\ y, \ldots$

Motivation

Are there solutions for $x,\ y$ in the domain $\mathbb{R}$, such that:



Approaches for nonlinear real algebraic formulas

Quantifier elimination:

- Methods:
  - *Cylindrical algebraic decomposition*
  - *Gröbner basis*
  - *Virtual substitution*
  - *Realizable sign conditions*
- Eliminates the variables iteratively
- **But**: blows up the formula

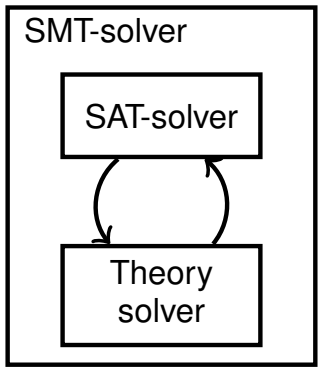
Approaches for nonlinear real algebraic formulas

Quantifier elimination:

- Methods:
  - *Cylindrical algebraic decomposition*
  - *Gröbner basis*
  - *Virtual substitution*
  - *Realizable sign conditions*
- Eliminates the variables iteratively
- **But**: blows up the formula

SMT-solving:

- Tools: `HySAT`, `ABsolver`, `Z3`
- Benefits from a SAT-solver
- **But**: no SMT-solver supports nonlinear constraints completely



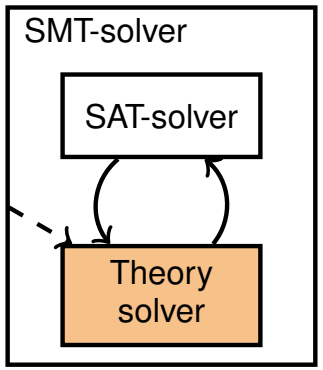
Approaches for nonlinear real algebraic formulas

Quantifier elimination:

- Methods:
  - *Cylindrical algebraic decomposition*
  - *Gröbner basis*
  - *Virtual substitution*
  - *Realizable sign conditions*
- Eliminates the variables iteratively
- **But**: blows up the formula

SMT-solving:

- Tools: `HySAT`, `ABsolver`, `Z3`
- Benefits from a SAT-solver
- **But**: no SMT-solver supports nonlinear constraints completely



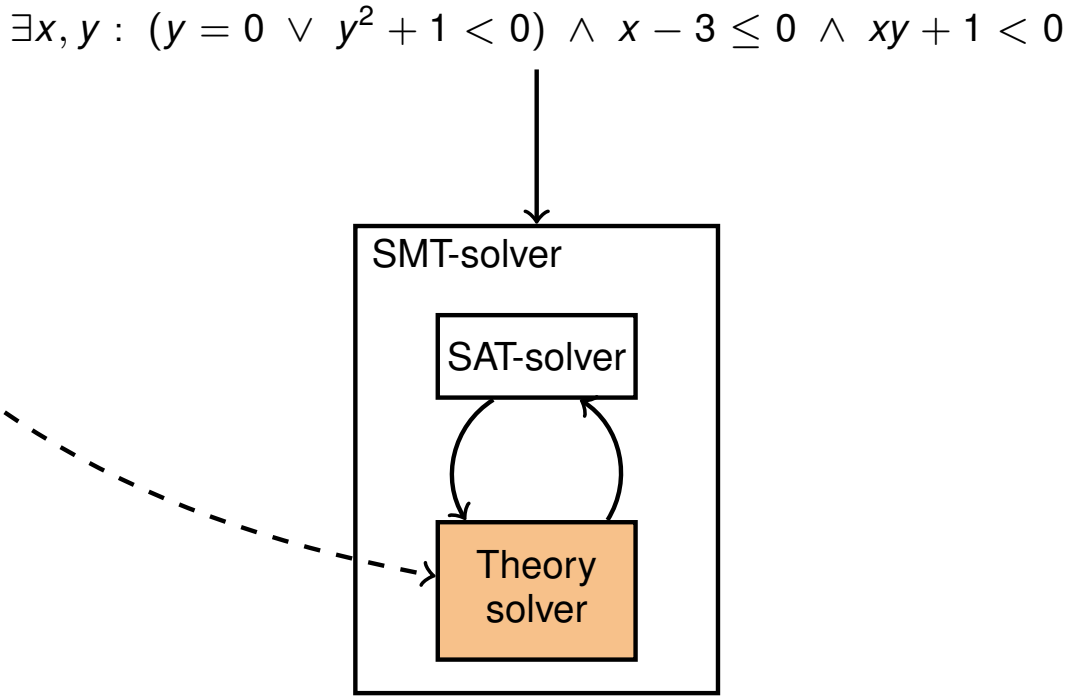
Structure of the talk

1.) Virtual substitution

Structure of the talk

1.) Virtual substitution

2.) Adaption to SMT
shown by an example

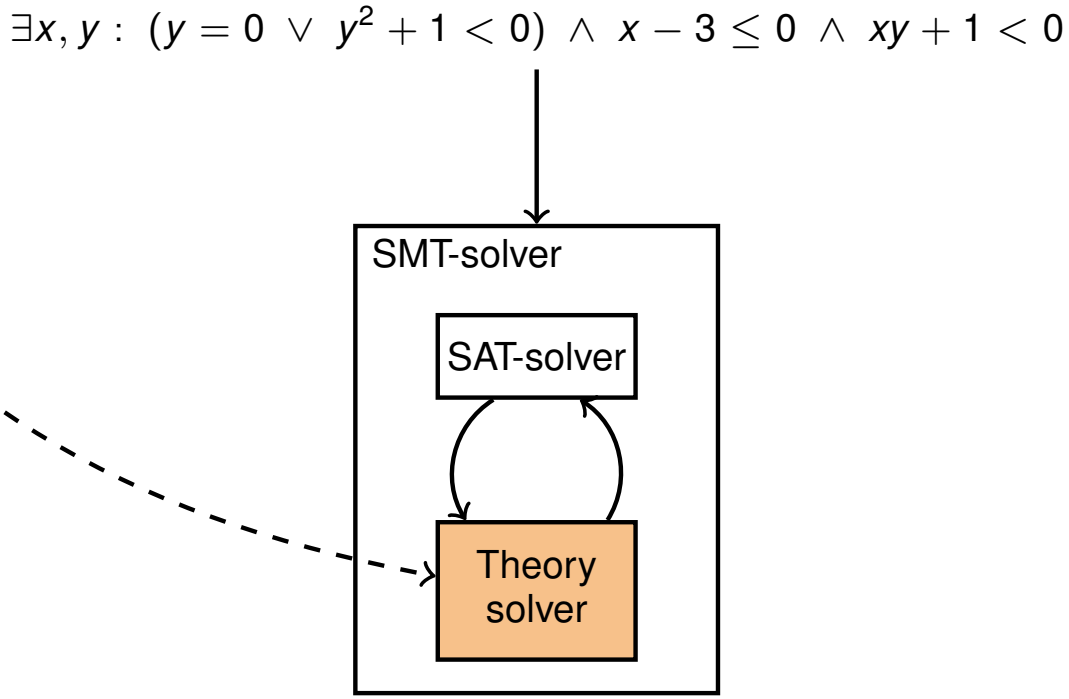


Structure of the talk

1.) Virtual substitution

2.) Adaption to SMT
shown by an example

3.) Experimental results



Construction of a **finite** number of solution candidates for a variable

Idea: We search the smallest value fulfilling all constraints.

Construction of a **finite** number of solution candidates for a variable

Idea: We search the smallest value fulfilling all constraints.

The constraints provide finitely many **test candidates**:

- $p = 0$
  1. Zeros of the polynomial p

Construction of a **finite** number of solution candidates for a variable

Idea: We search the smallest value fulfilling all constraints.

The constraints provide finitely many **test candidates**:

- $p = 0$
  1. Zeros of the polynomial p
- $p \leq 0,\ p \geq 0$
  1. Zeros of the polynomial p
  2. $-\infty$ $(:=$ sufficient small value$)$

Construction of a **finite** number of solution candidates for a variable

Idea: We search the smallest value fulfilling all constraints.

The constraints provide finitely many **test candidates**:

- $p = 0$
  1. Zeros of the polynomial p
- $p \leq 0,\ p \geq 0$
  1. Zeros of the polynomial p
  2. $-\infty$ ($:=$ sufficient small value)
- $p < 0,\ p > 0,\ p \neq 0$
  1. Zeros of the polynomial p plus an infinitesimal ϵ
  2. $-\infty$

Construction of a **finite** number of solution candidates for a variable

Idea: We search the smallest value fulfilling all constraints.

The constraints provide finitely many **test candidates**:

- $p = 0$
  1. Zeros of the polynomial p
- $p \leq 0,\ p \geq 0$
  1. Zeros of the polynomial p
  2. $-\infty$ (:= sufficient small value)
- $p < 0,\ p > 0,\ p \neq 0$
  1. Zeros of the polynomial p plus an infinitesimal ϵ
  2. $-\infty$
- Example: $xy + 1 < 0 \quad \rightarrow \quad \begin{cases} \frac{1}{y} + \epsilon & \text{if } y \neq 0 \\ -\infty \end{cases}$

Construction of a **finite** number of solution candidates for a variable

For our example: $\exists x, y : \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$

Test candidates

eliminate x

$\Leftrightarrow$

$$\begin{aligned}
\exists y : \quad & ((y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0)[-\infty/\mathbf{x}] \\
\vee \quad & ((y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0)[\mathbf{3}/\mathbf{x}] \quad) \\
\vee (\ \mathbf{y \neq 0} \quad \wedge \quad & ((y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0)[-\tfrac{\mathbf{1}}{\mathbf{y}} + \epsilon/\mathbf{x}] \quad)
\end{aligned}$$

Side condition

eliminate y

$\Leftrightarrow$

$\cdots$

How to apply $\varphi[t/x]$

Standard substitution:

- Leads to terms containing $-\infty$, $\sqrt{\ }$ and fractions
- Introduces new variables ϵ

Example:

$$(x + 2y = 0)\ [\frac{\sqrt{4y}}{z}/x] \qquad \mapsto \qquad \frac{\sqrt{4y}}{z} + 2y = 0$$

How to apply $\varphi[t/x]$

Standard substitution:

- Leads to terms containing $-\infty$, $\sqrt{}$ and fractions
- Introduces new variables ϵ

Example:

$$(x + 2y = 0)\ [\frac{\sqrt{4y}}{z}/x] \quad \mapsto \quad \frac{\sqrt{4y}}{z} + 2y = 0$$

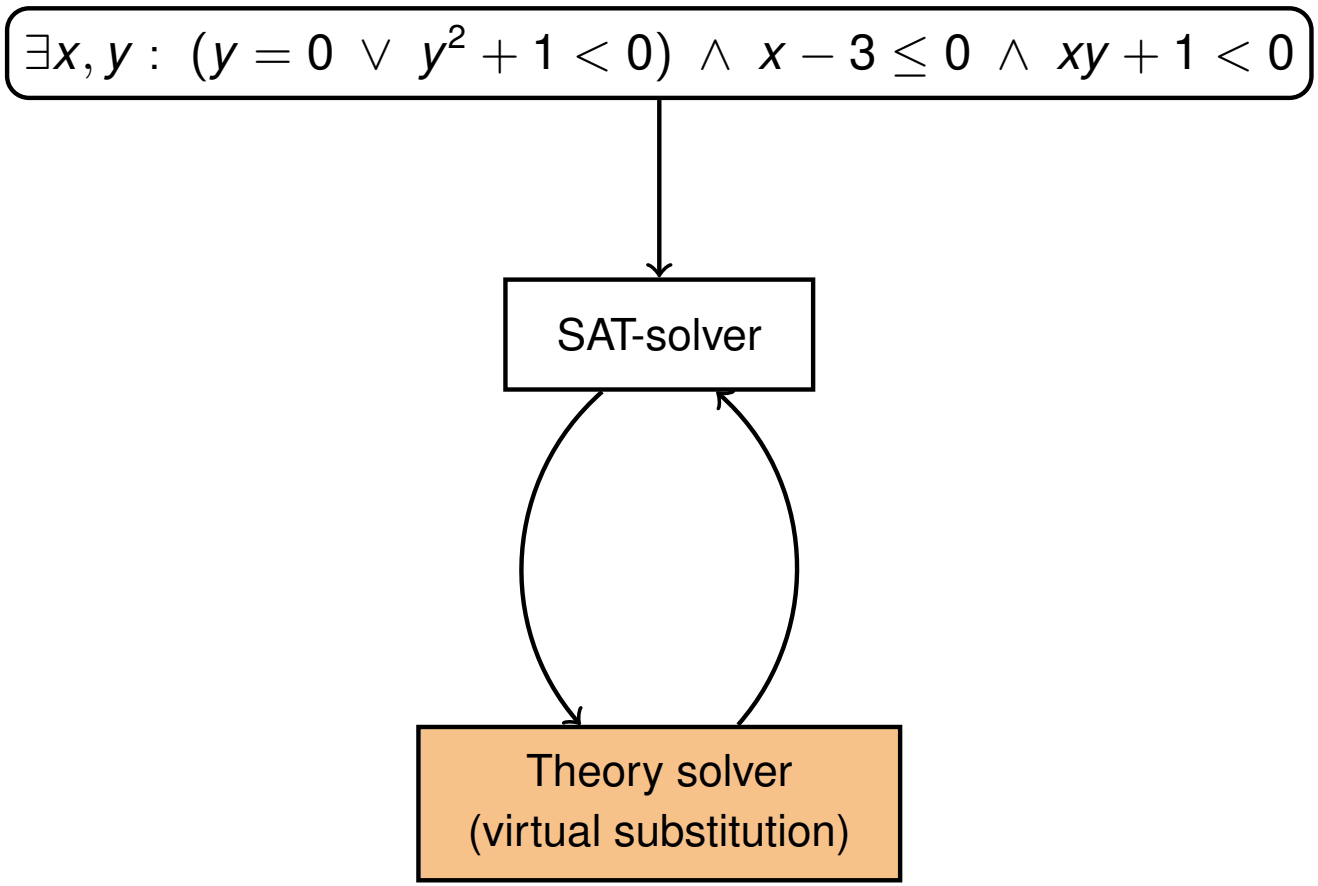
Substitution rules

Virtual substitution defines rules, which give an equivalent DNF over $(\mathbb{R}, +, \cdot, 0, 1, <)$ to the expression resulting by the above standard substitution.

Example:

$$\frac{2yz + \sqrt{4y}}{z} = 0 \quad \Leftrightarrow \quad 2yz \leq 0 \quad \wedge \quad (2yz)^2 - 4y = 0$$

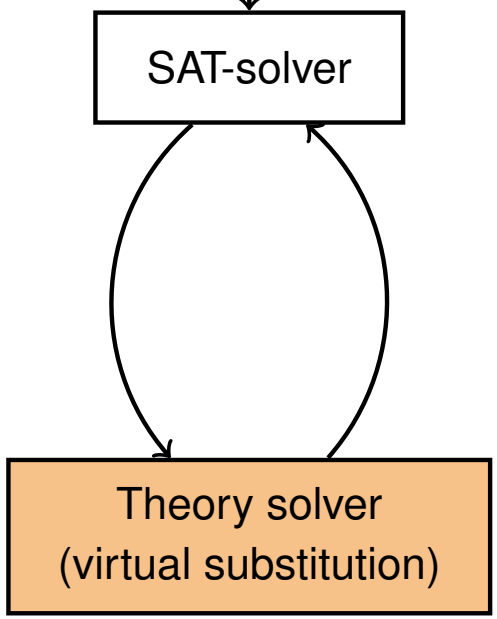
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
SAT-solver
Theory solver
(virtual substitution)

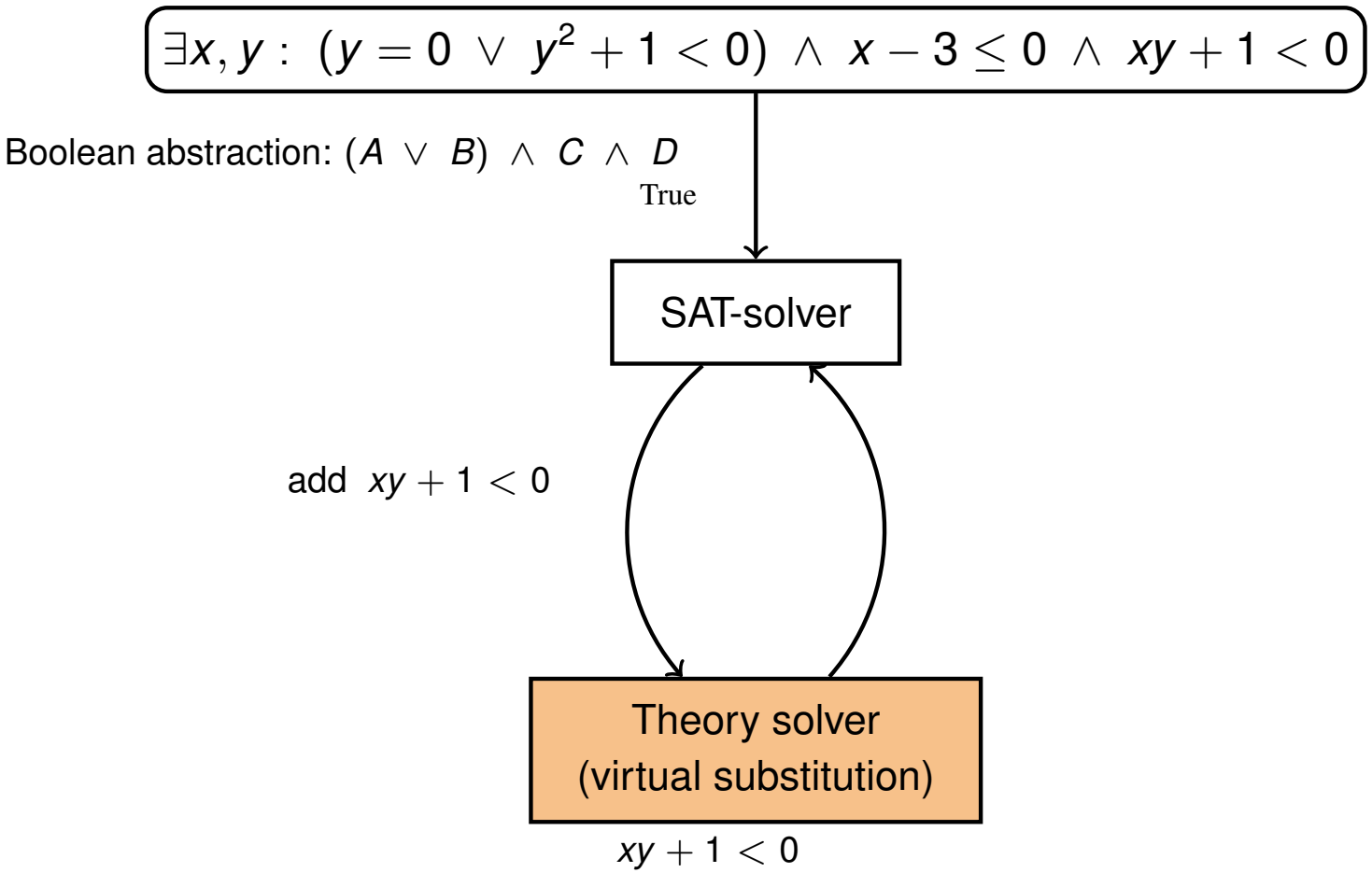
SMT-solver

$$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$$

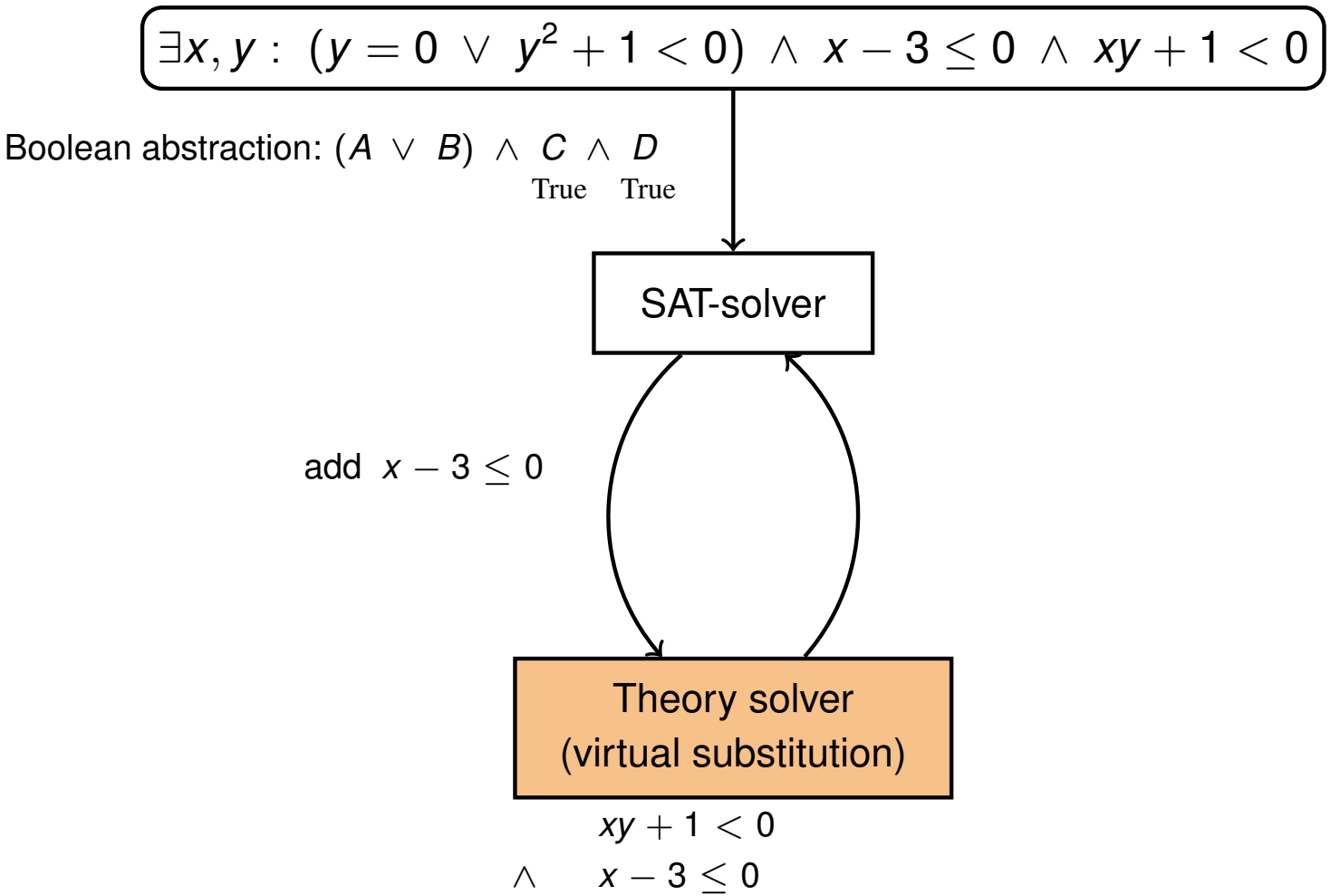
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$



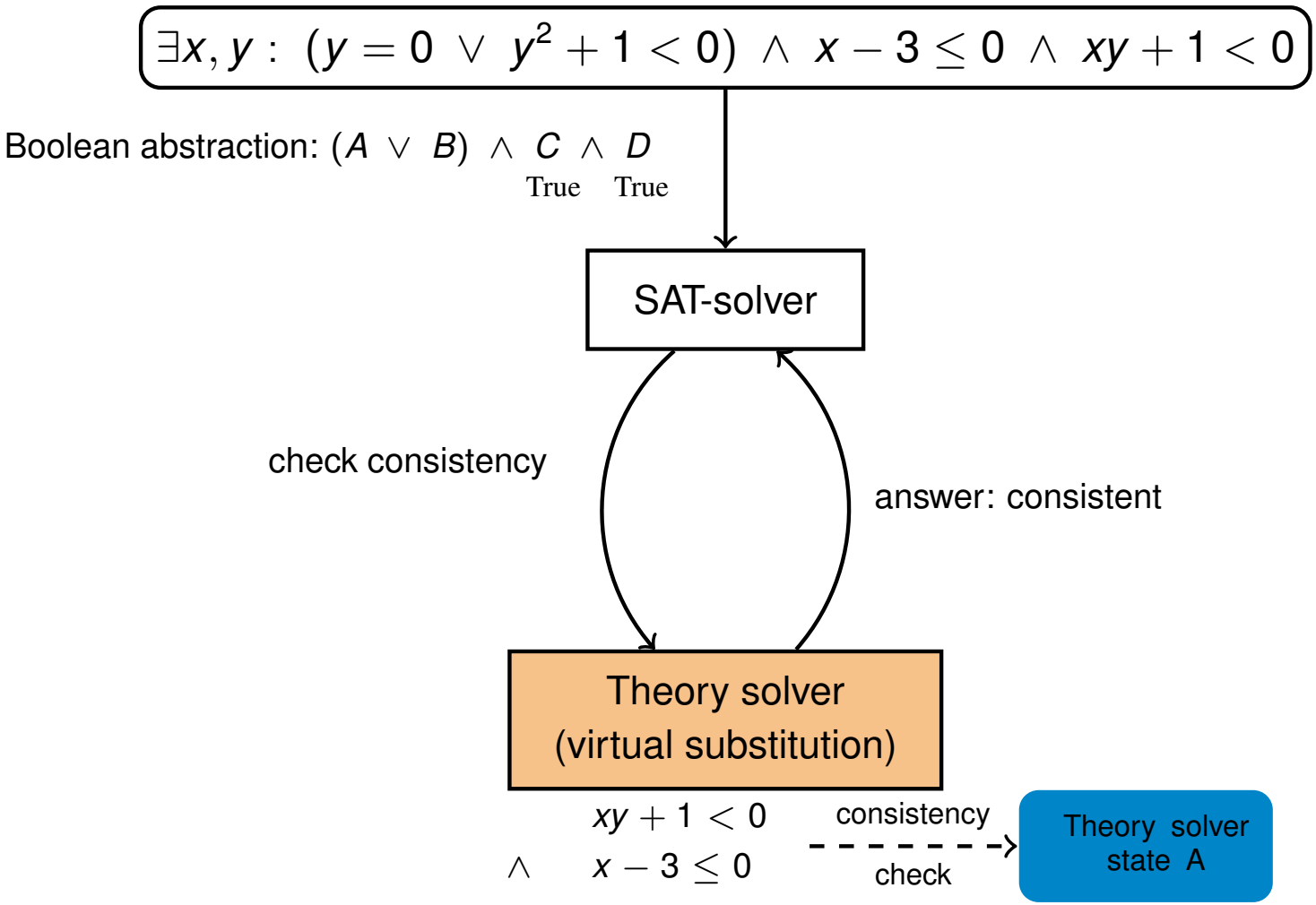
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
SAT-solver
add $xy + 1 < 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$

SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
SAT-solver
add $x - 3 \leq 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$

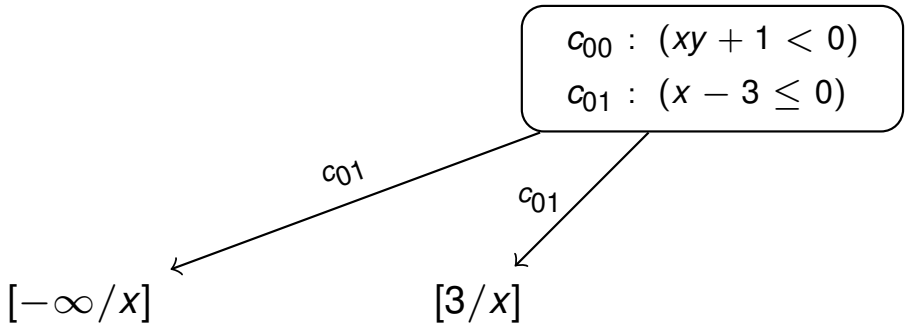
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
SAT-solver
check consistency
answer: consistent
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
consistency
check
Theory solver
state A

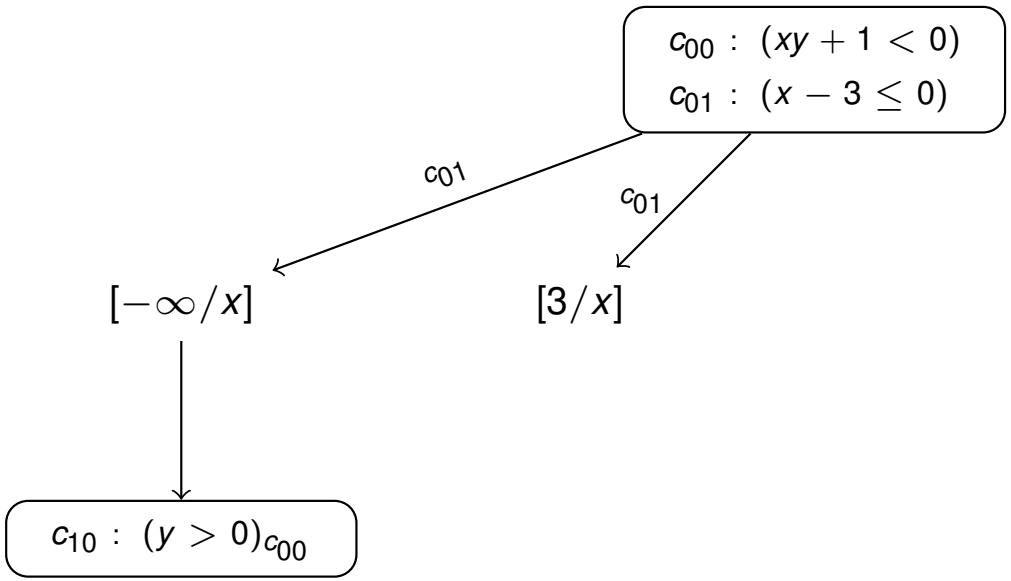
Theory solver: add $xy + 1 < 0$ and $x - 3 \leq 0$ and check for consistency

$$c_{00} : (xy + 1 < 0)$$
$$c_{01} : (x - 3 \leq 0)$$

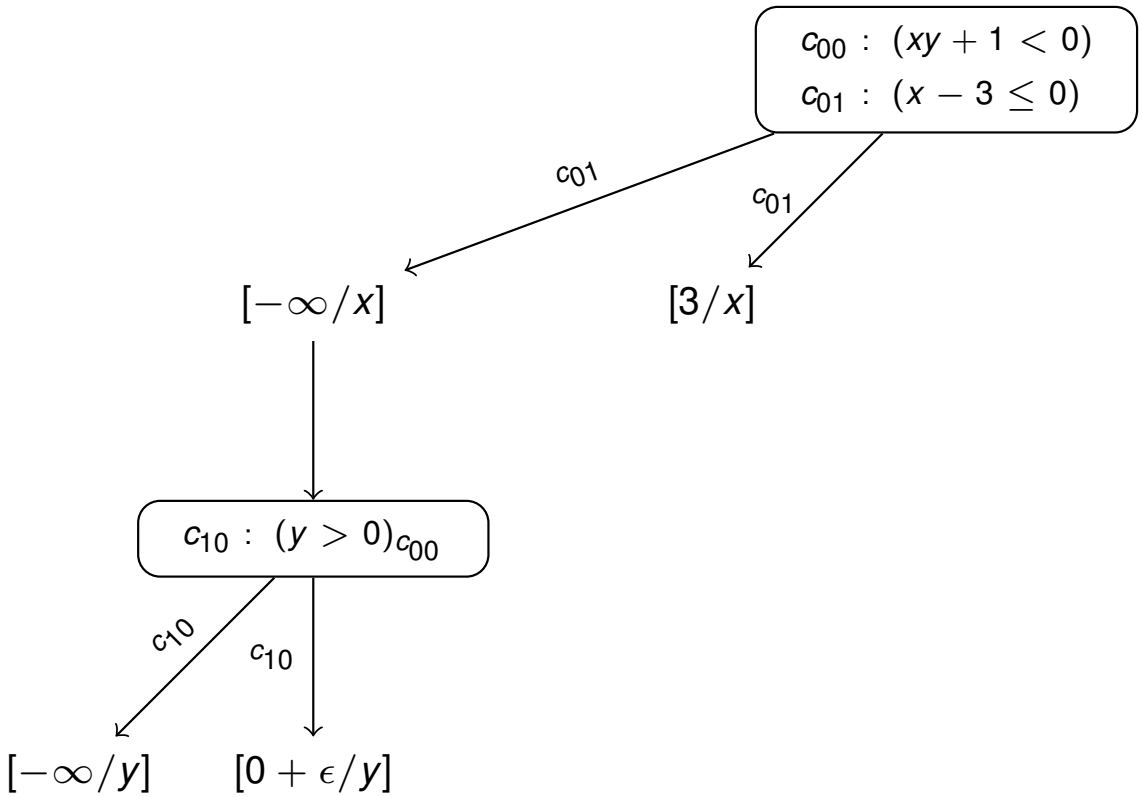
Theory solver: add $xy + 1 < 0$ and $x - 3 \leq 0$ and check for consistency



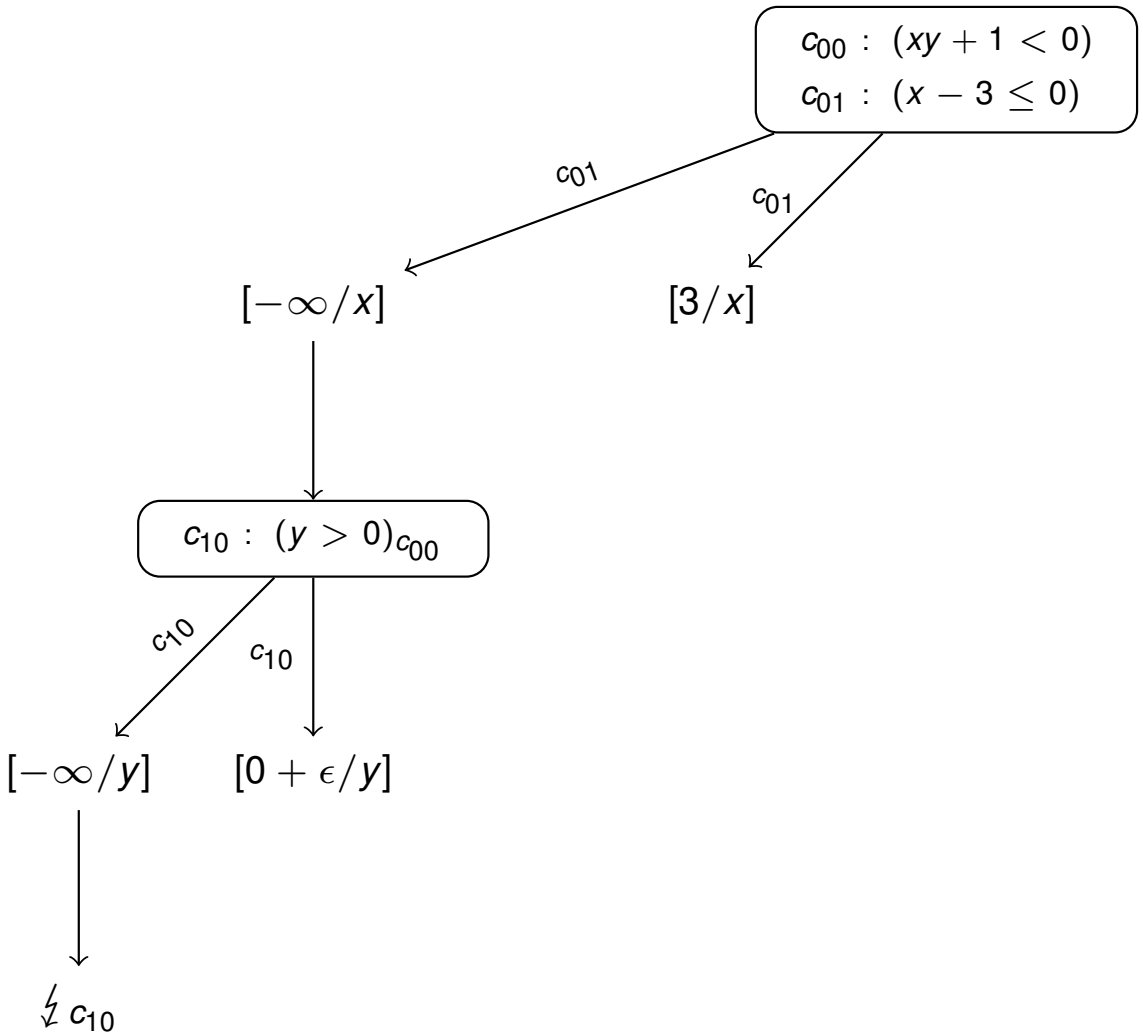
Theory solver: add $xy + 1 < 0$ and $x - 3 \leq 0$ and check for consistency



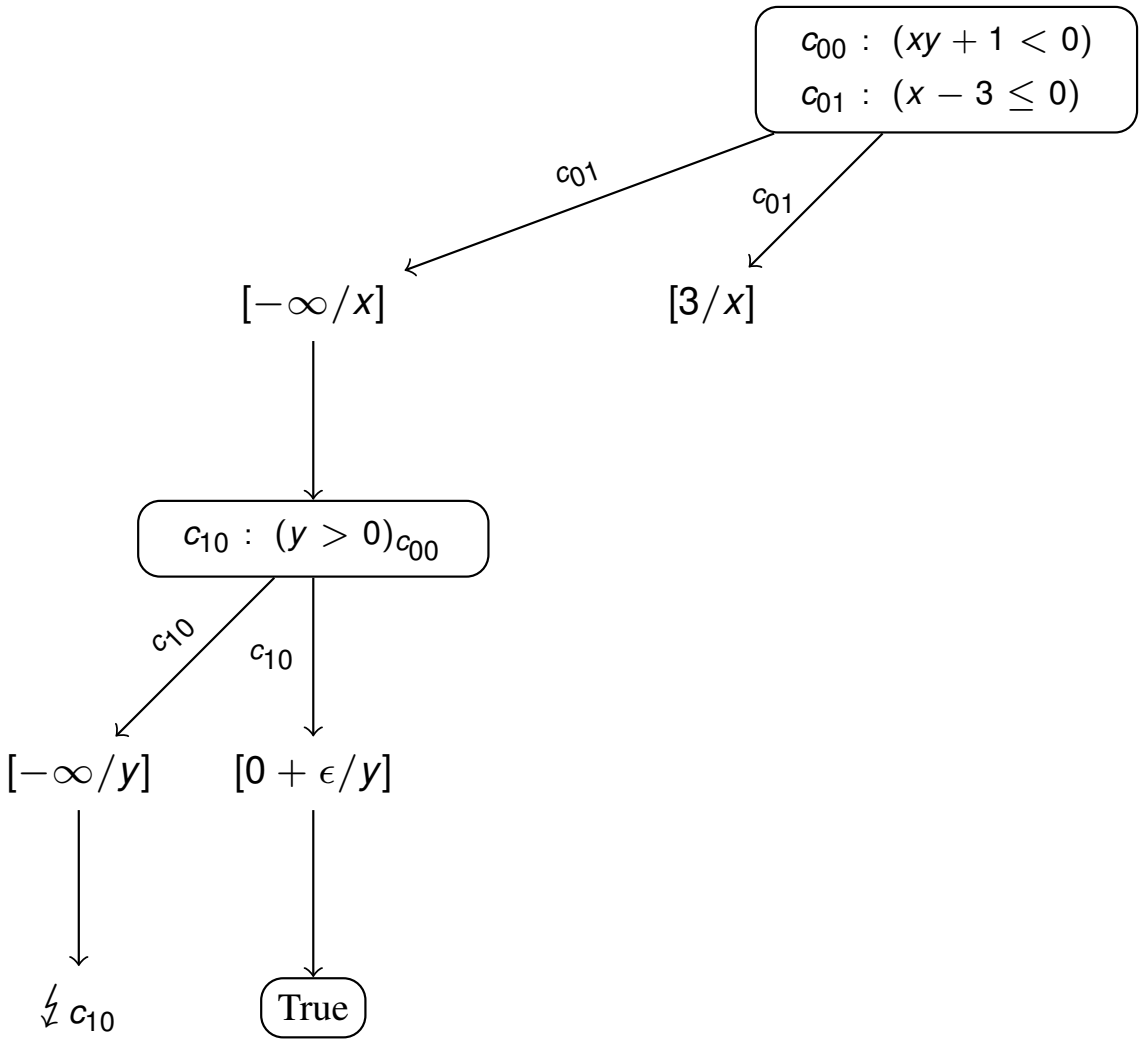
Theory solver: add $xy + 1 < 0$ and $x - 3 \leq 0$ and check for consistency



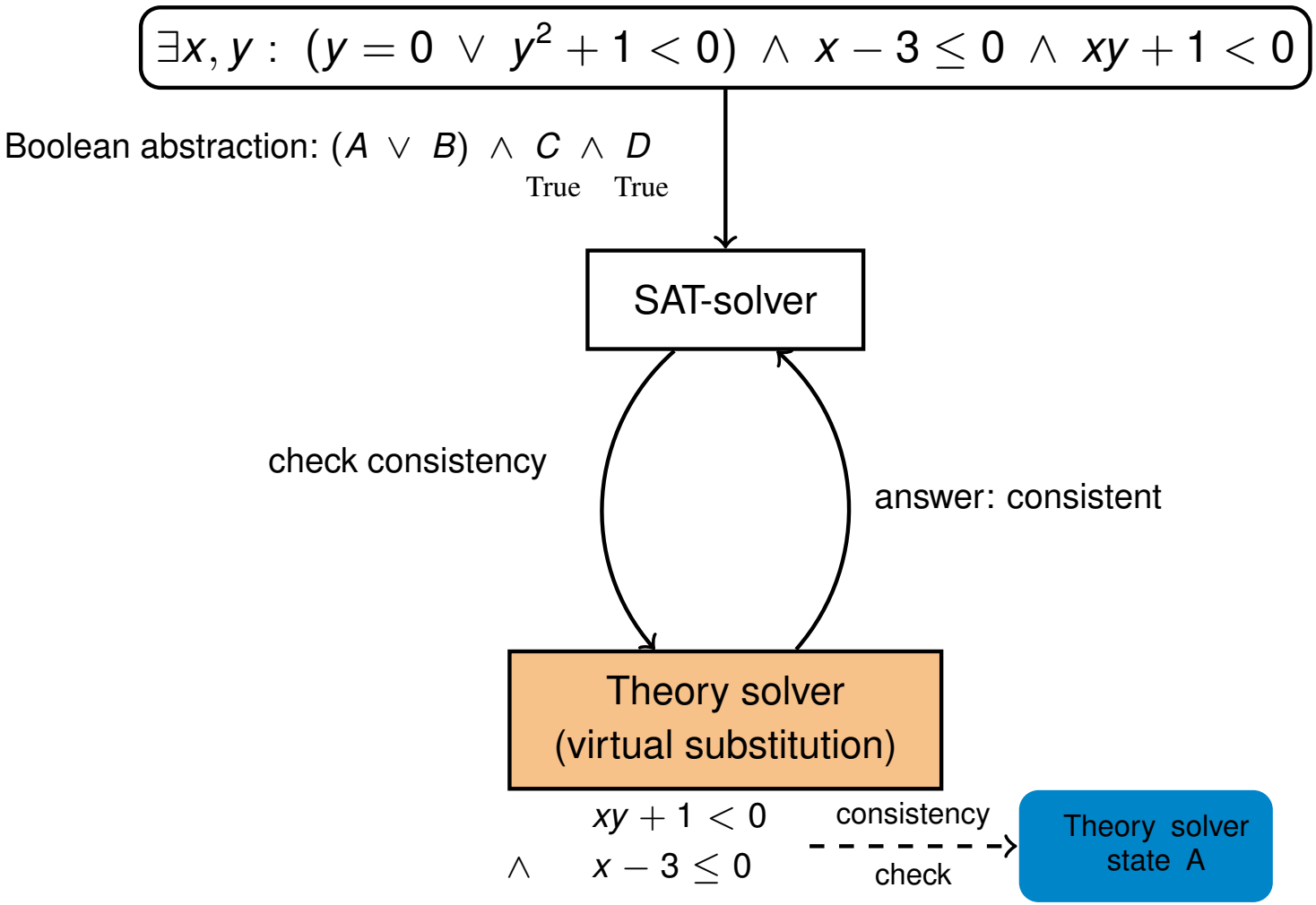
Theory solver: add $xy + 1 < 0$ and $x - 3 \leq 0$ and check for consistency



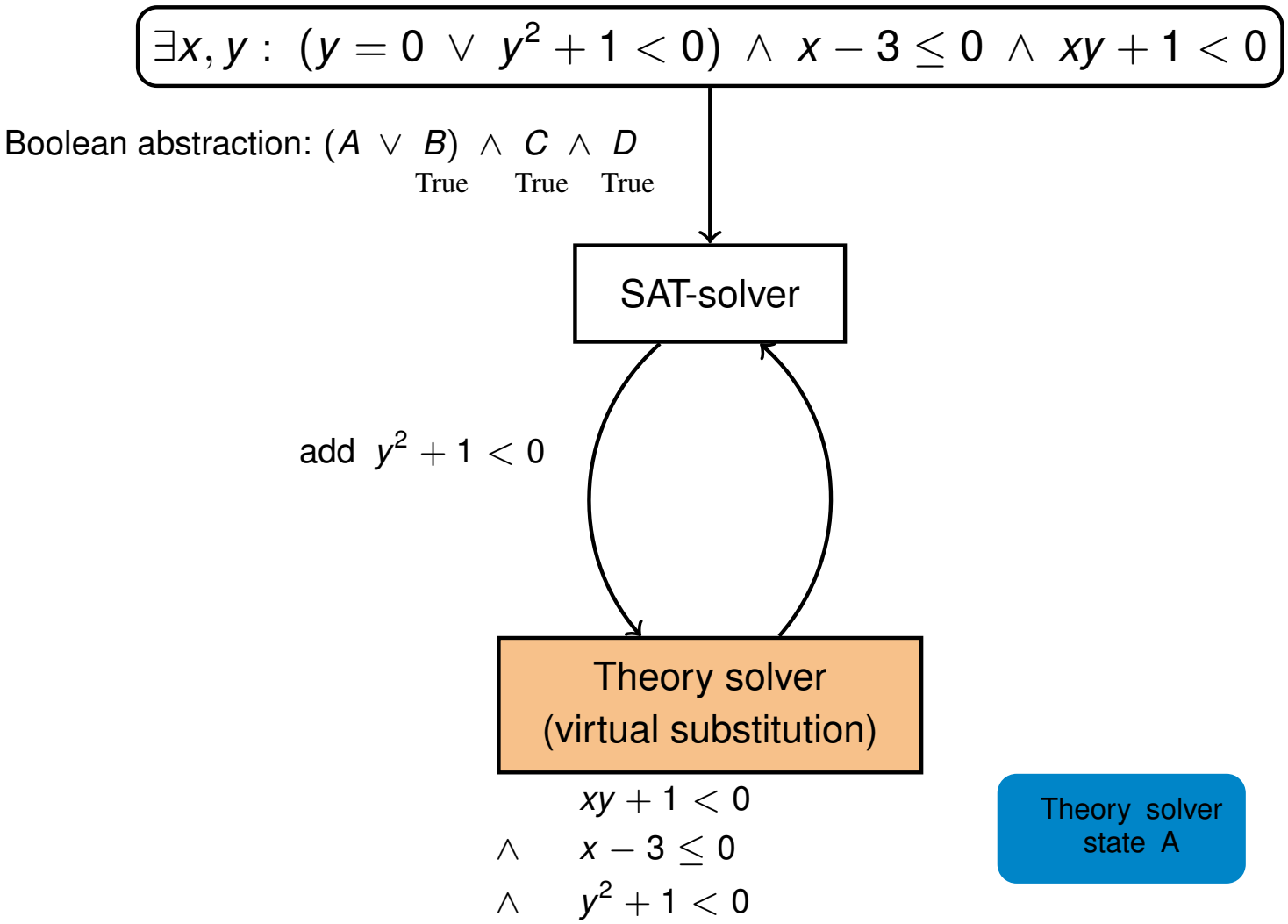
Theory solver: add $xy + 1 < 0$ and $x - 3 \leq 0$ and check for consistency



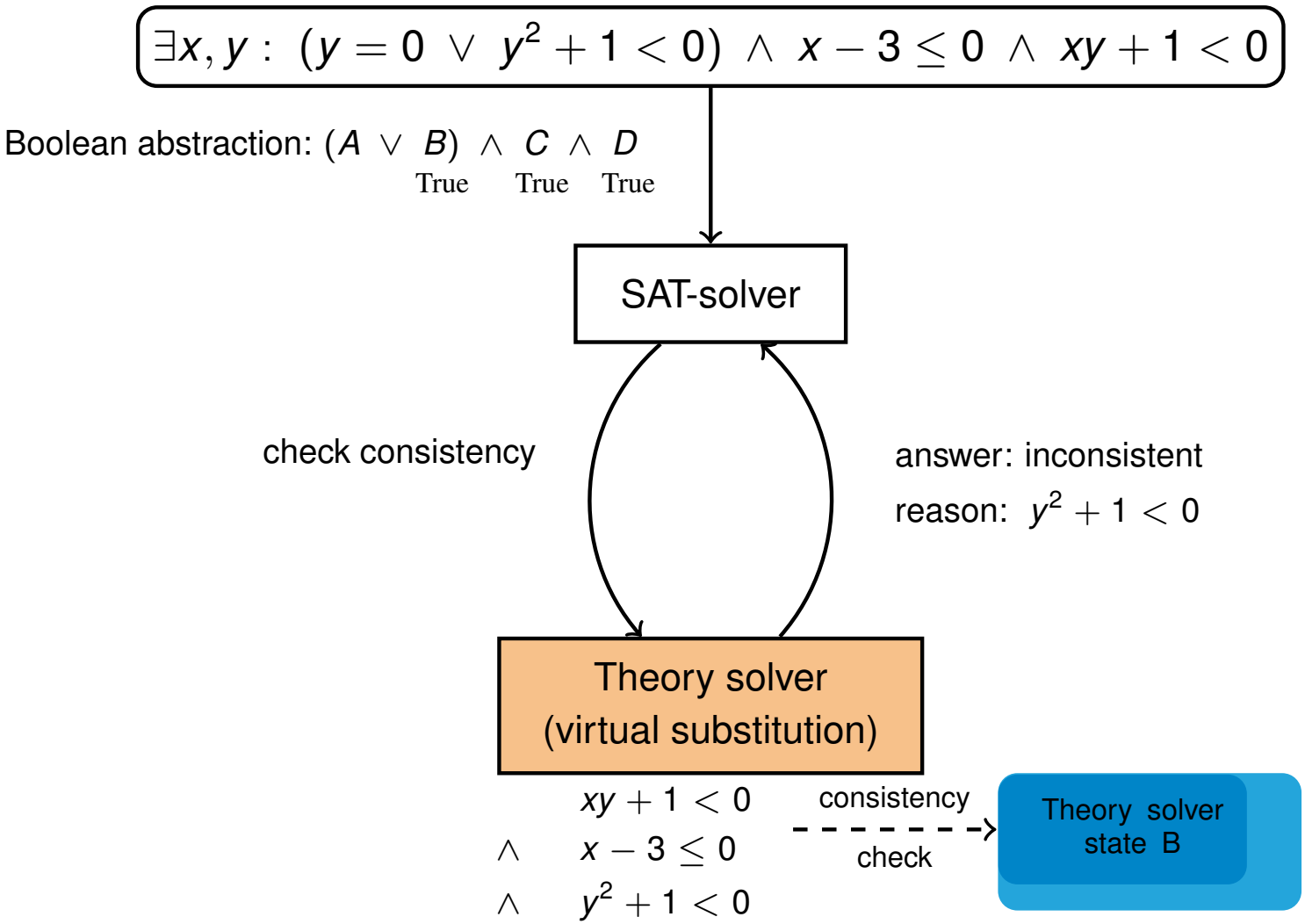
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
SAT-solver
check consistency
answer: consistent
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
consistency
check
Theory solver
state A

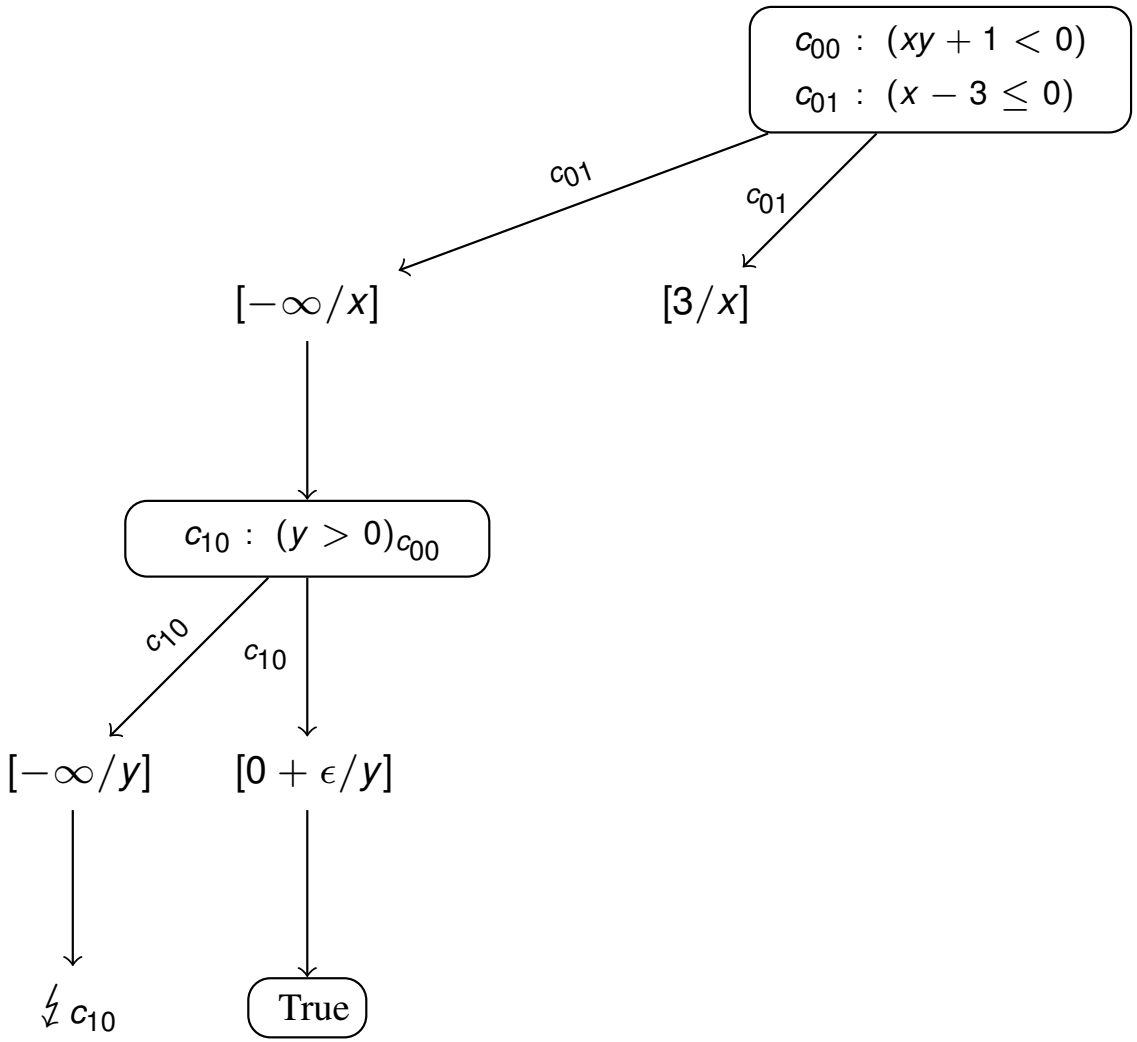
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True True True
SAT-solver
add $y^2 + 1 < 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
$\wedge \quad y^2 + 1 < 0$
Theory solver state A

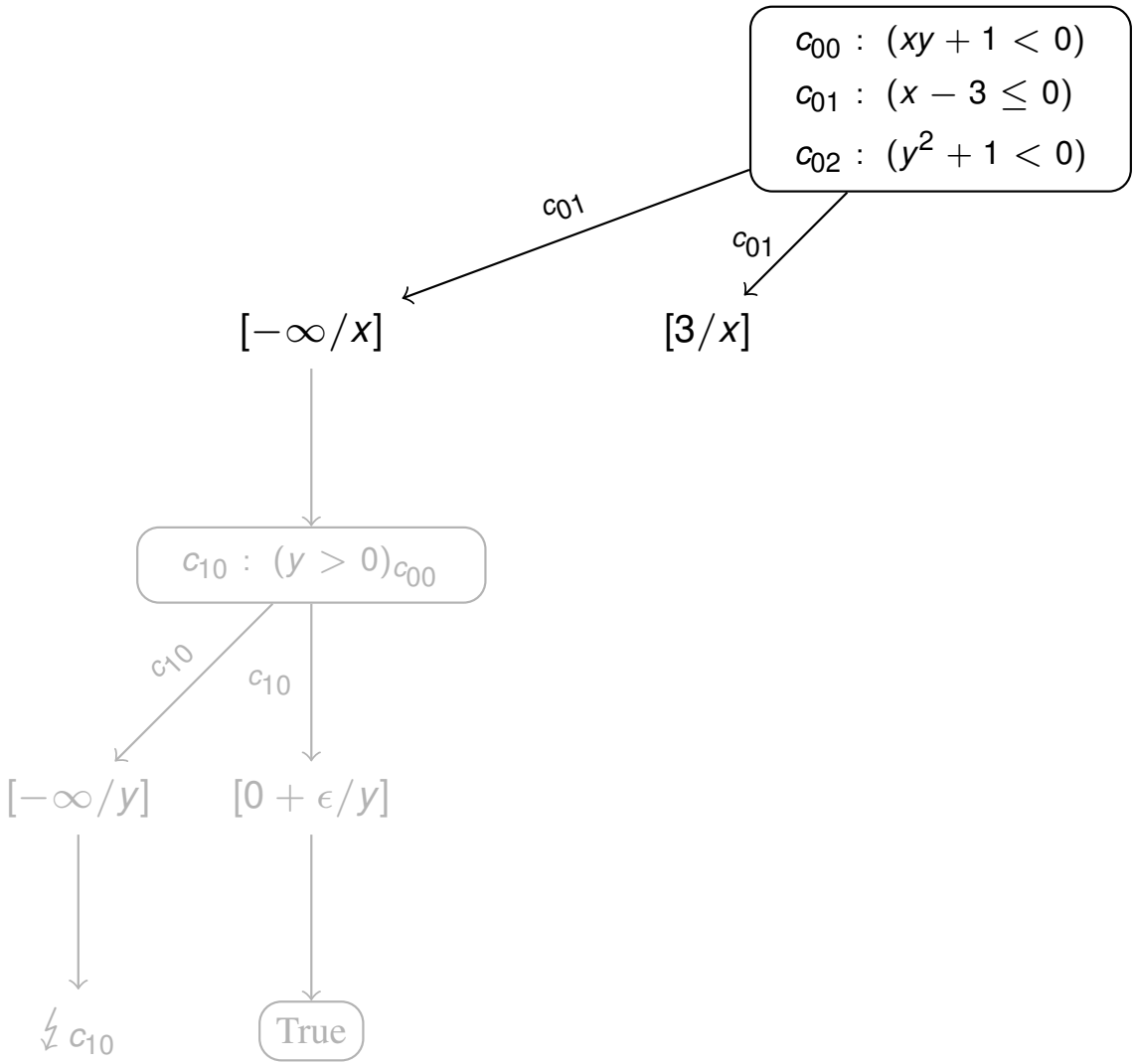
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True True True
SAT-solver
check consistency
answer: inconsistent
reason: $y^2 + 1 < 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
$\wedge \quad y^2 + 1 < 0$
consistency
check
Theory solver
state B

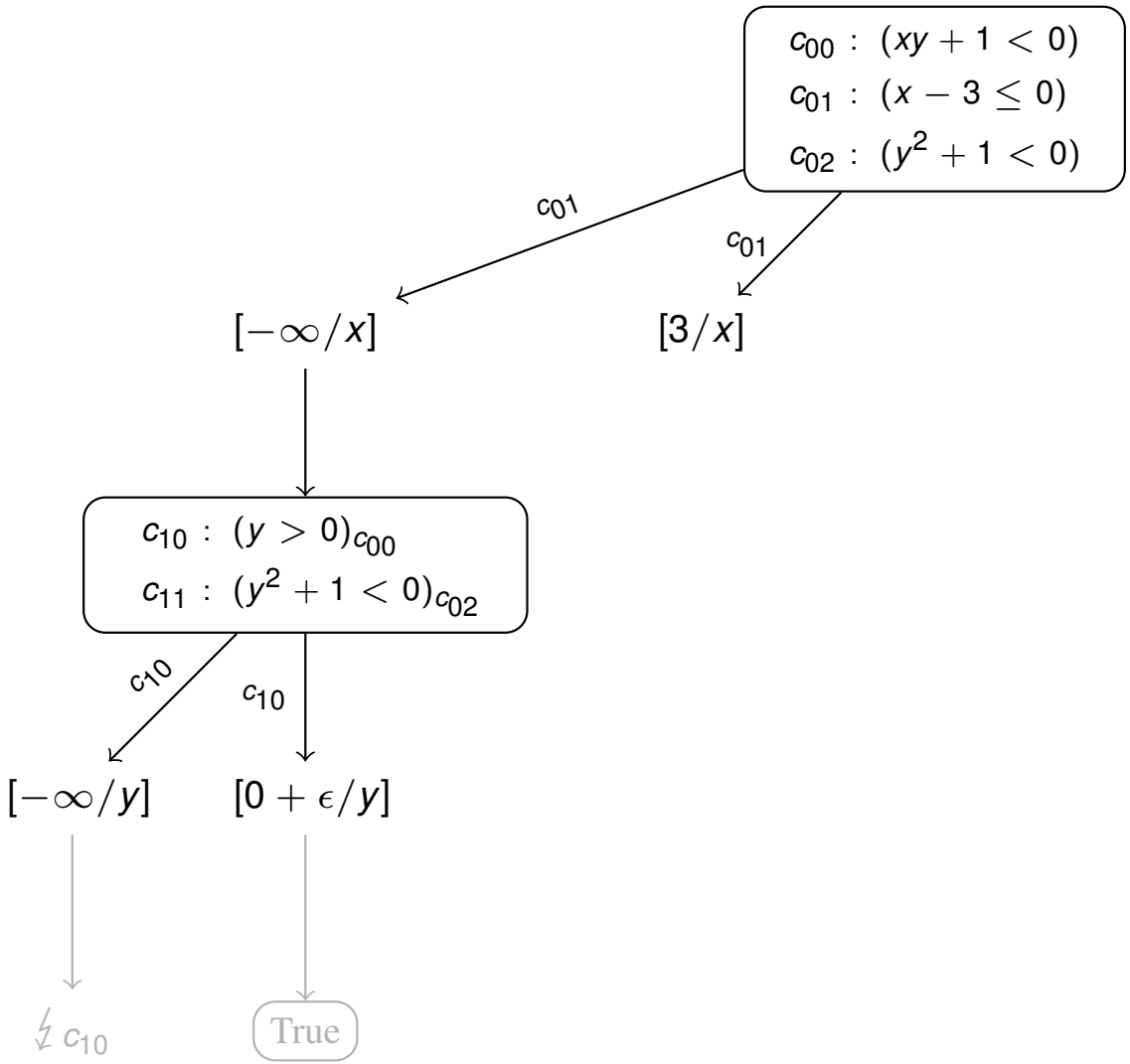
Theory solver: add $y^2 + 1 < 0$ and check for consistency



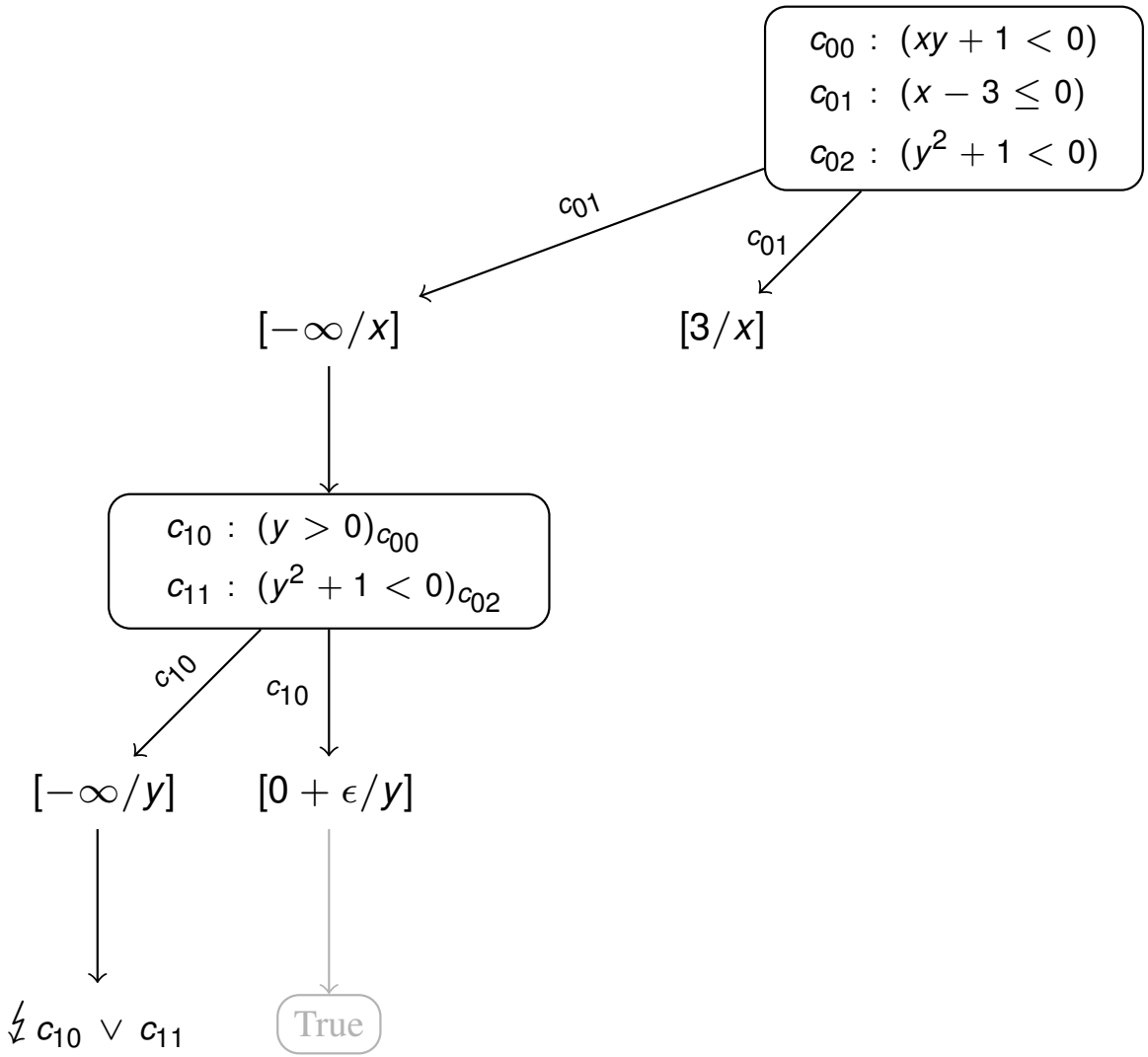
Theory solver: add $y^2 + 1 < 0$ and check for consistency



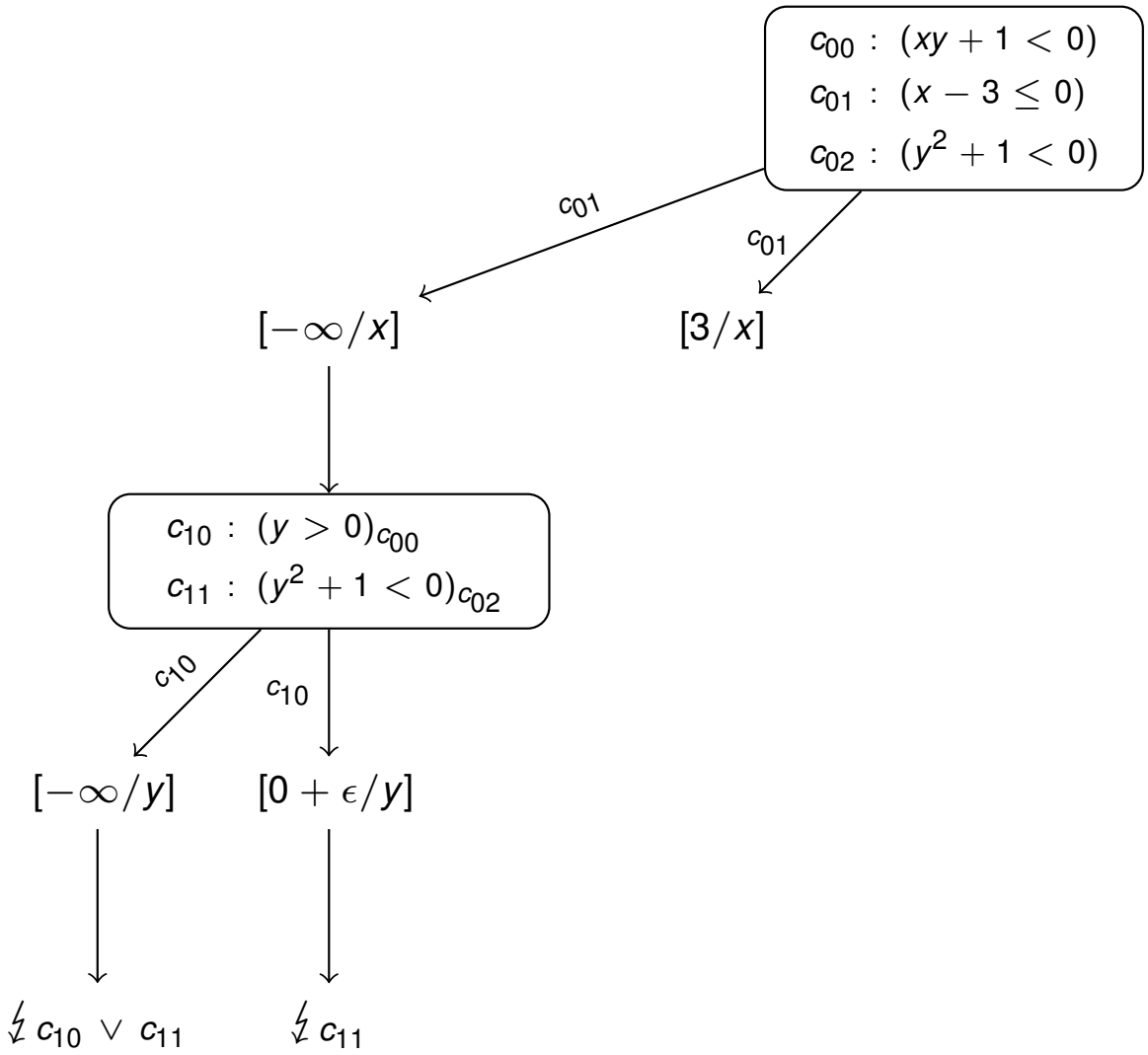
Theory solver: add $y^2 + 1 < 0$ and check for consistency



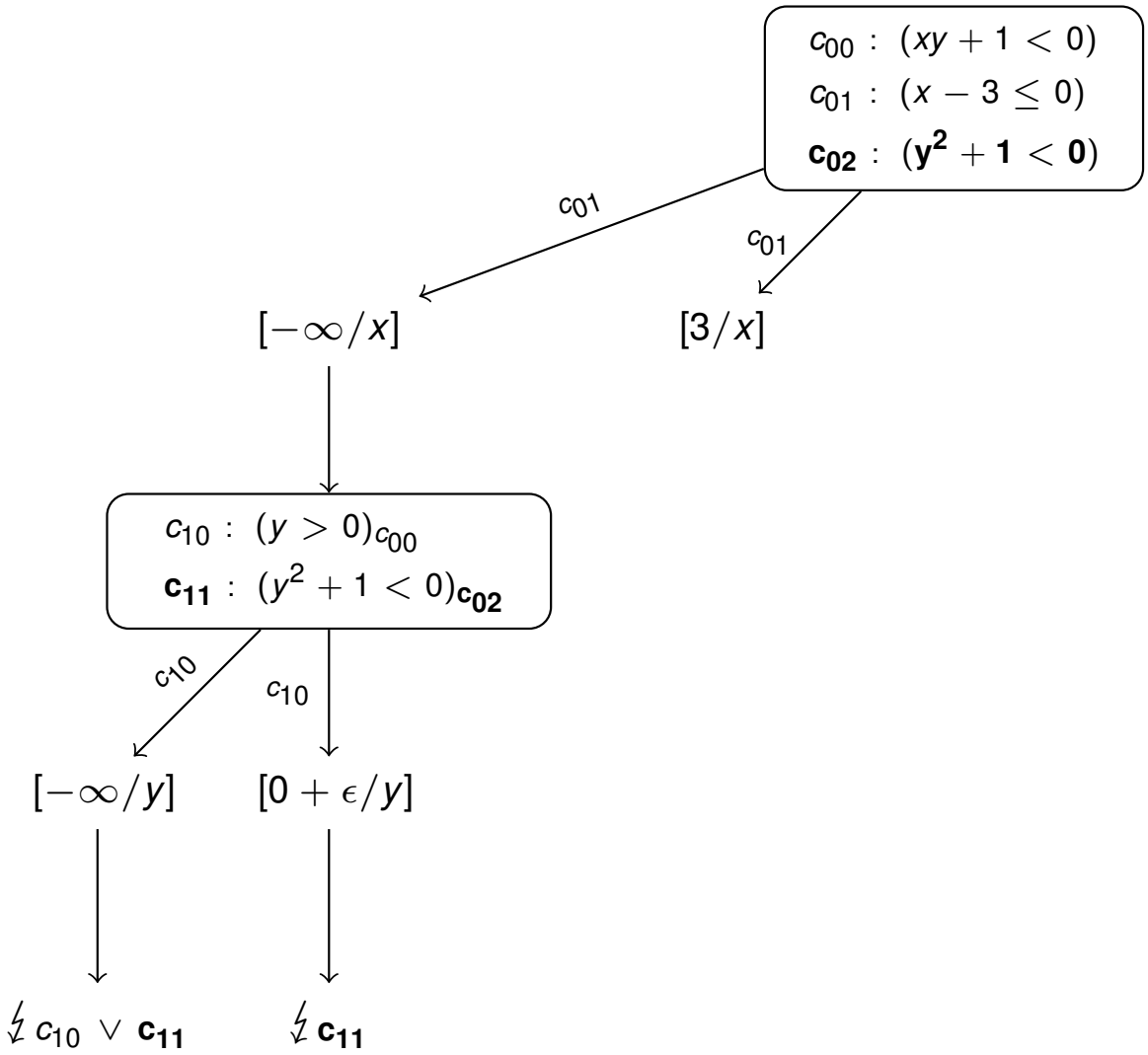
Theory solver: add $y^2 + 1 < 0$ and check for consistency



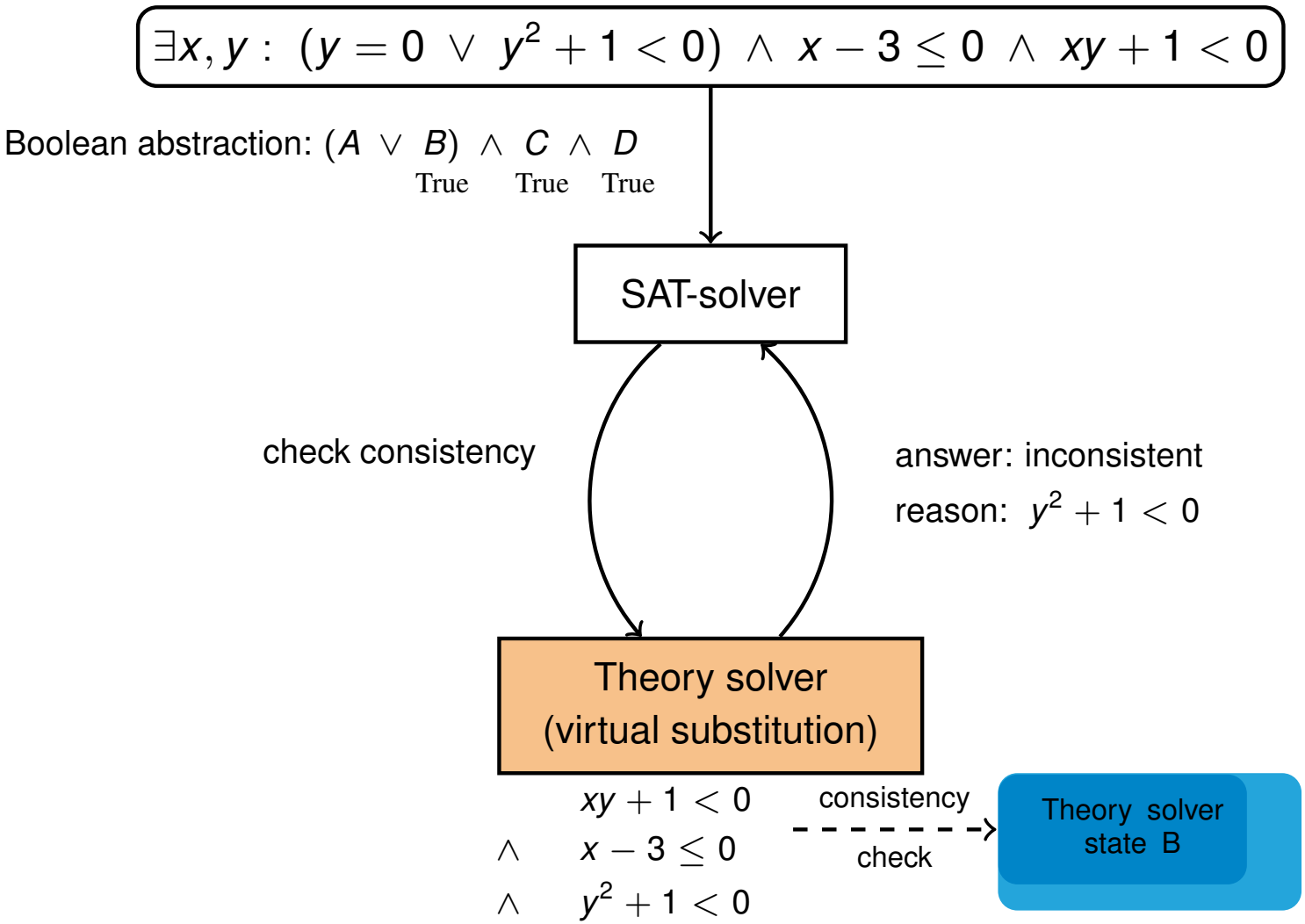
Theory solver: add $y^2 + 1 < 0$ and check for consistency



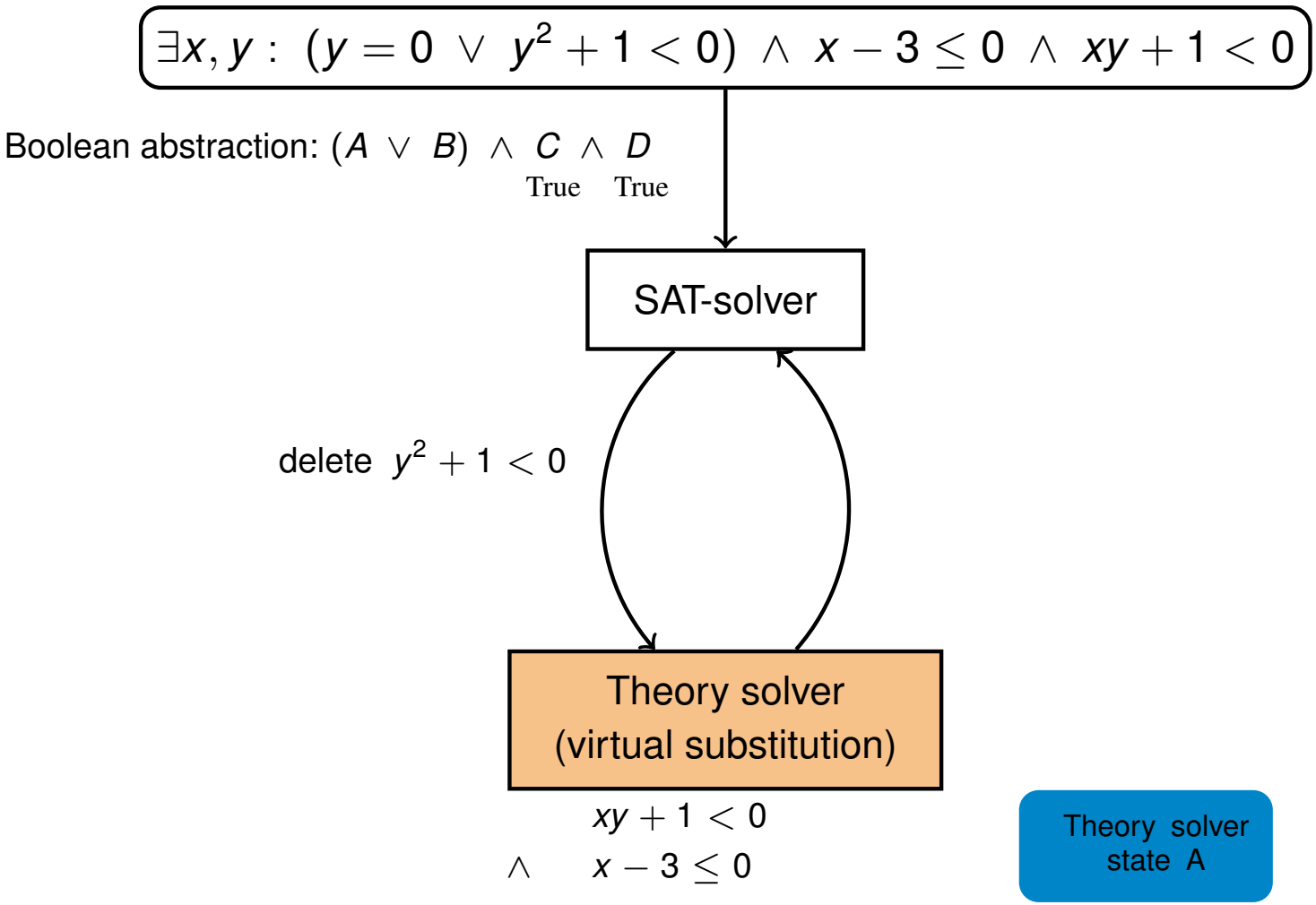
Theory solver: add $y^2 + 1 < 0$ and check for consistency



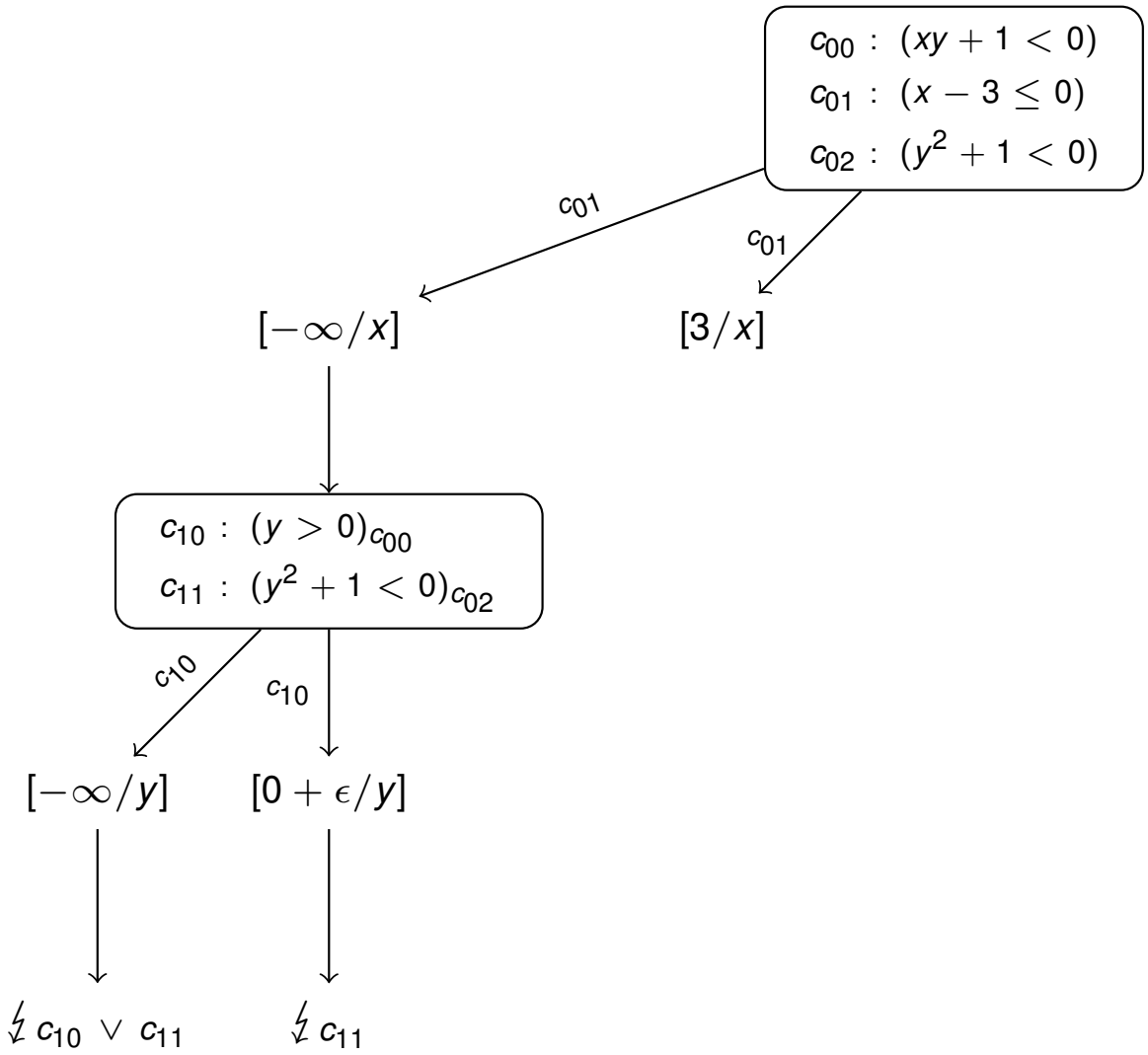
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True True True
SAT-solver
check consistency
answer: inconsistent
reason: $y^2 + 1 < 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
$\wedge \quad y^2 + 1 < 0$
consistency
check
Theory solver
state B

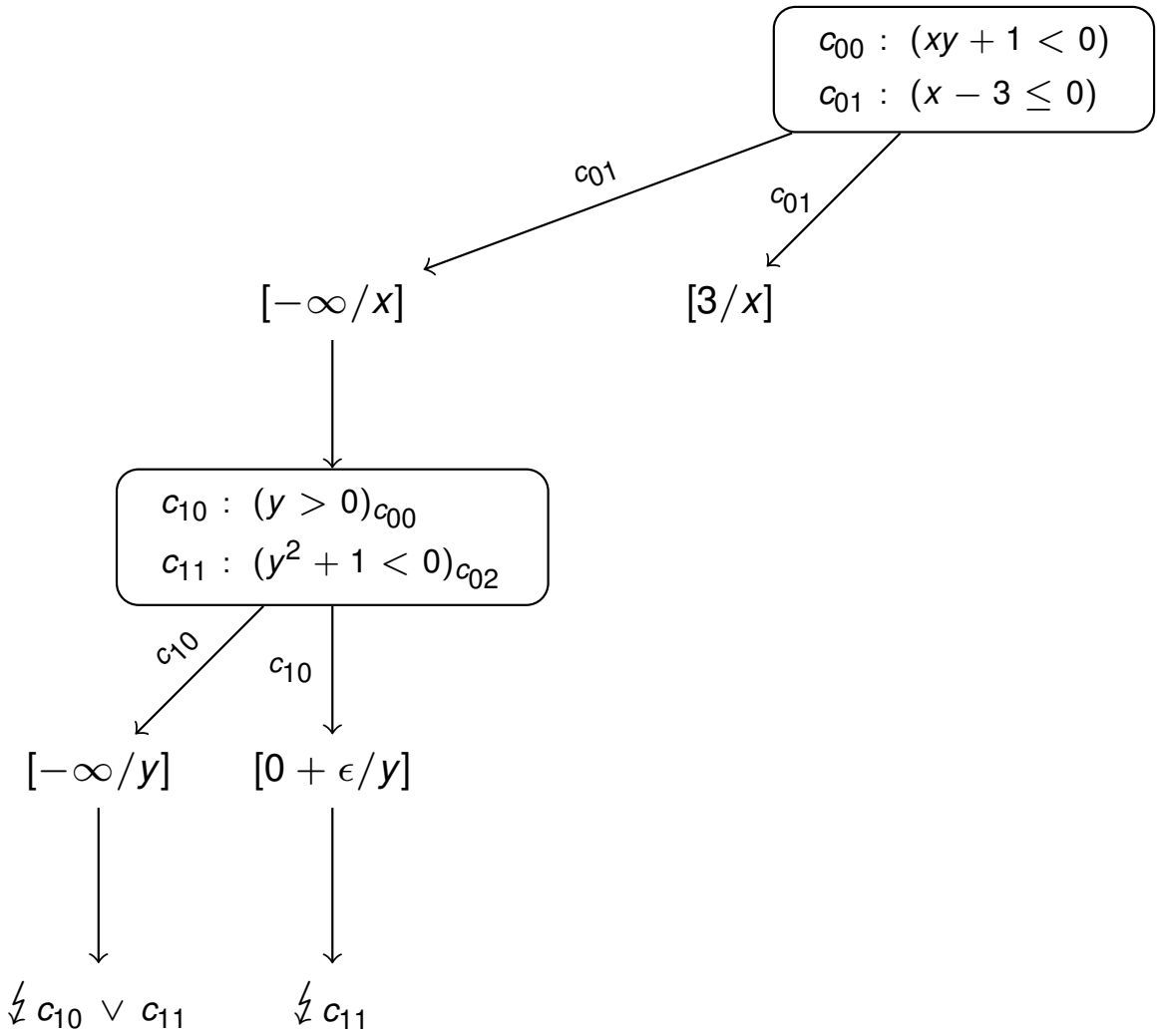
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
SAT-solver
delete $y^2 + 1 < 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
Theory solver
state A

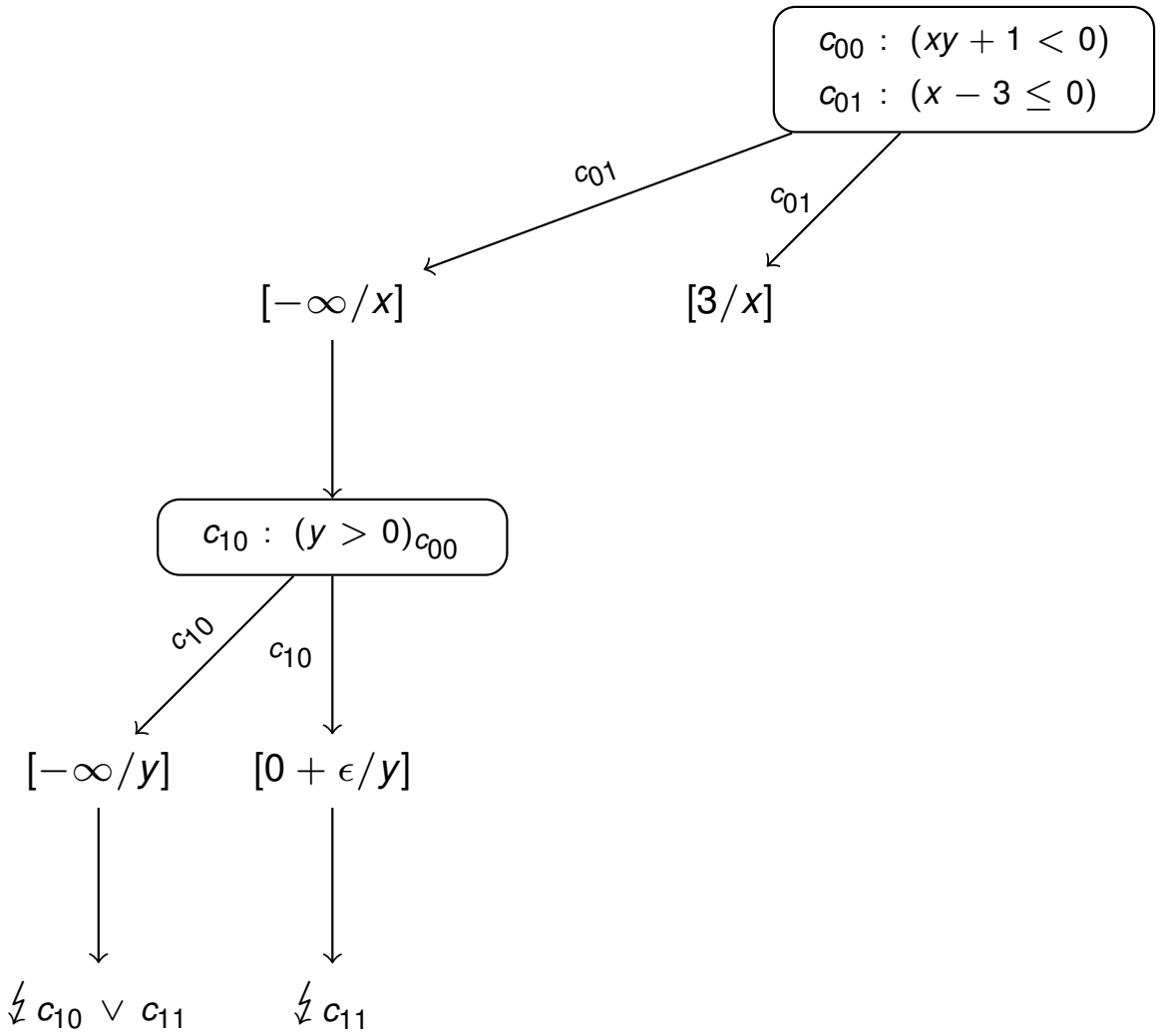
Theory solver: delete $y^2 + 1 < 0$



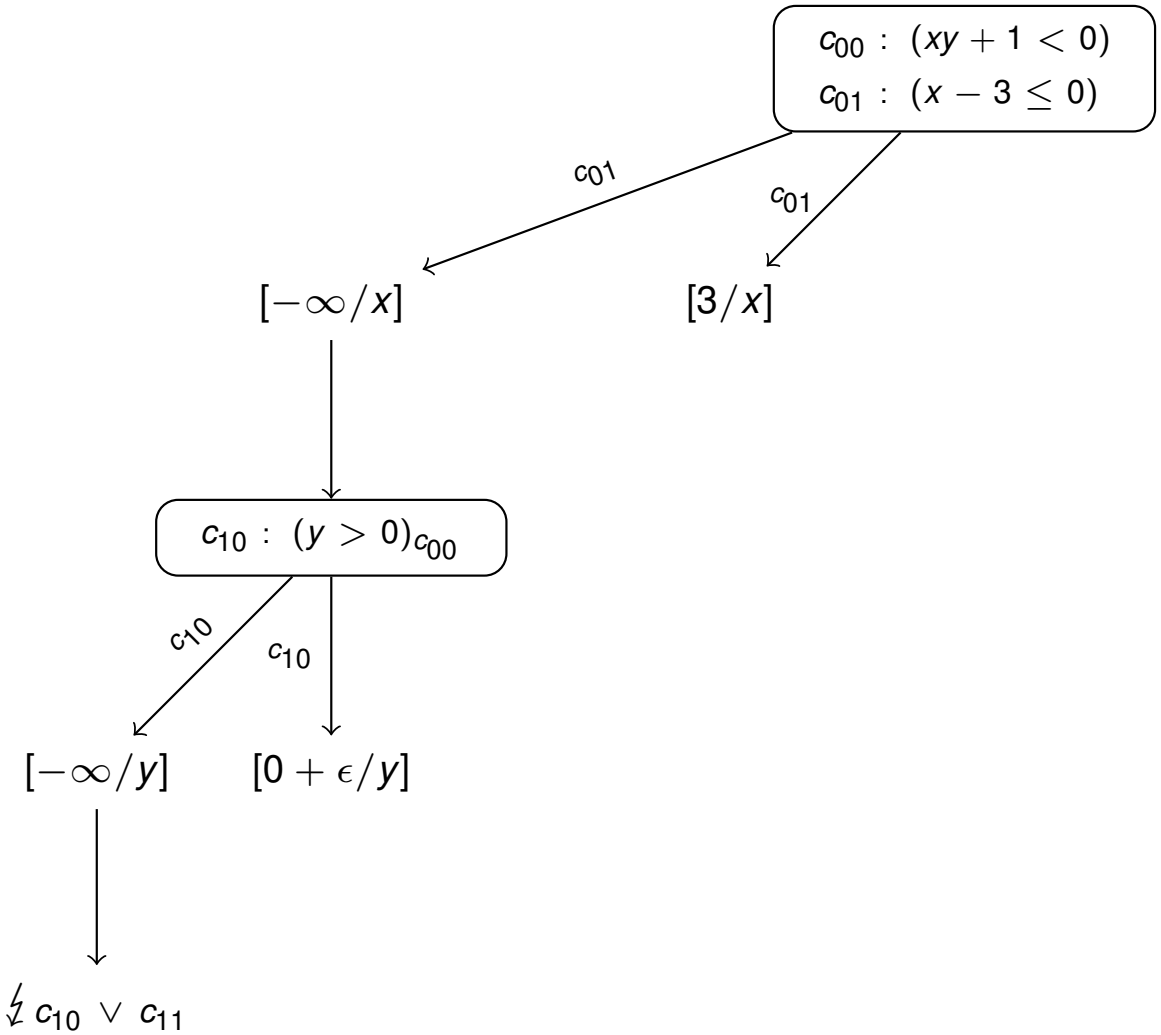
Theory solver: delete $y^2 + 1 < 0$



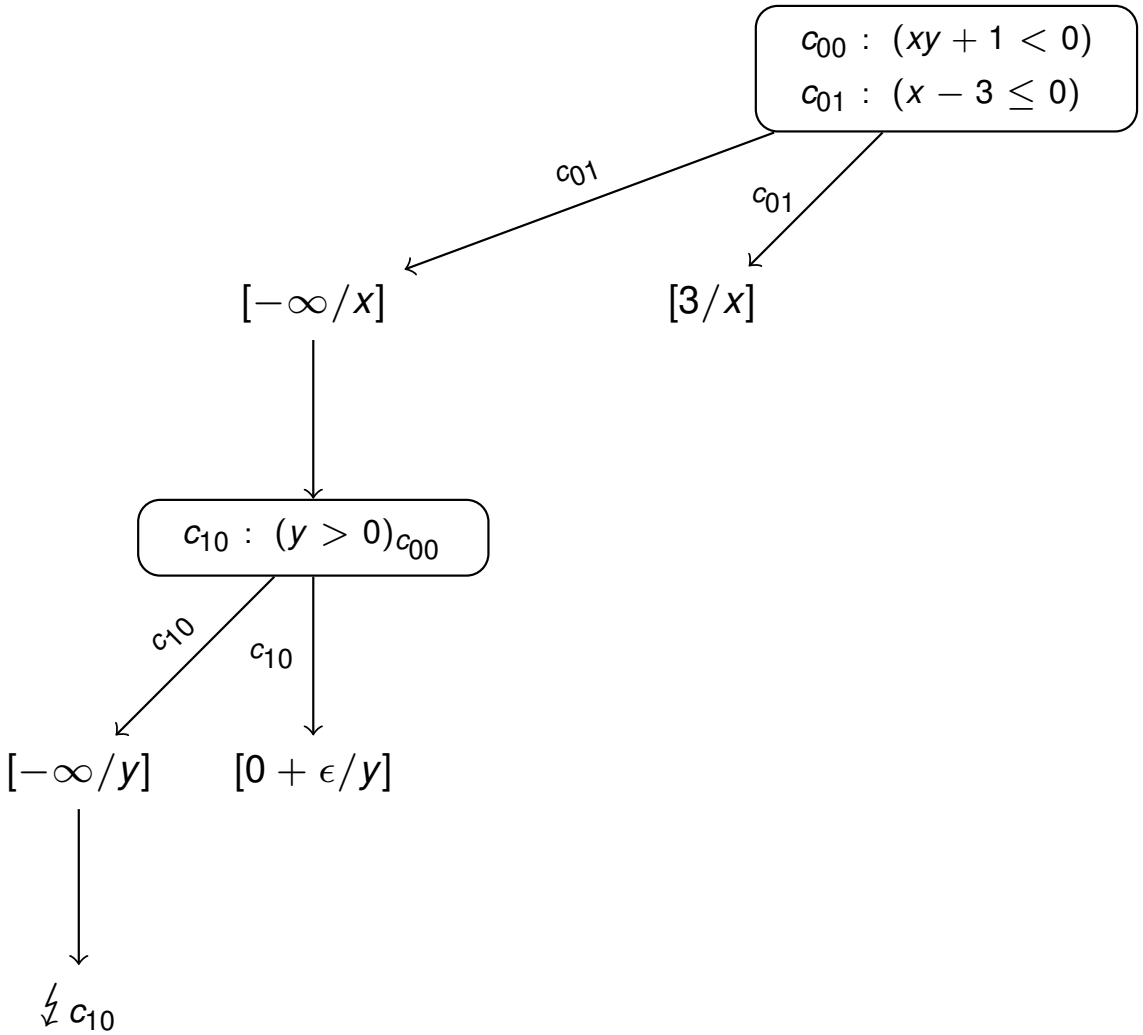
Theory solver: delete $y^2 + 1 < 0$



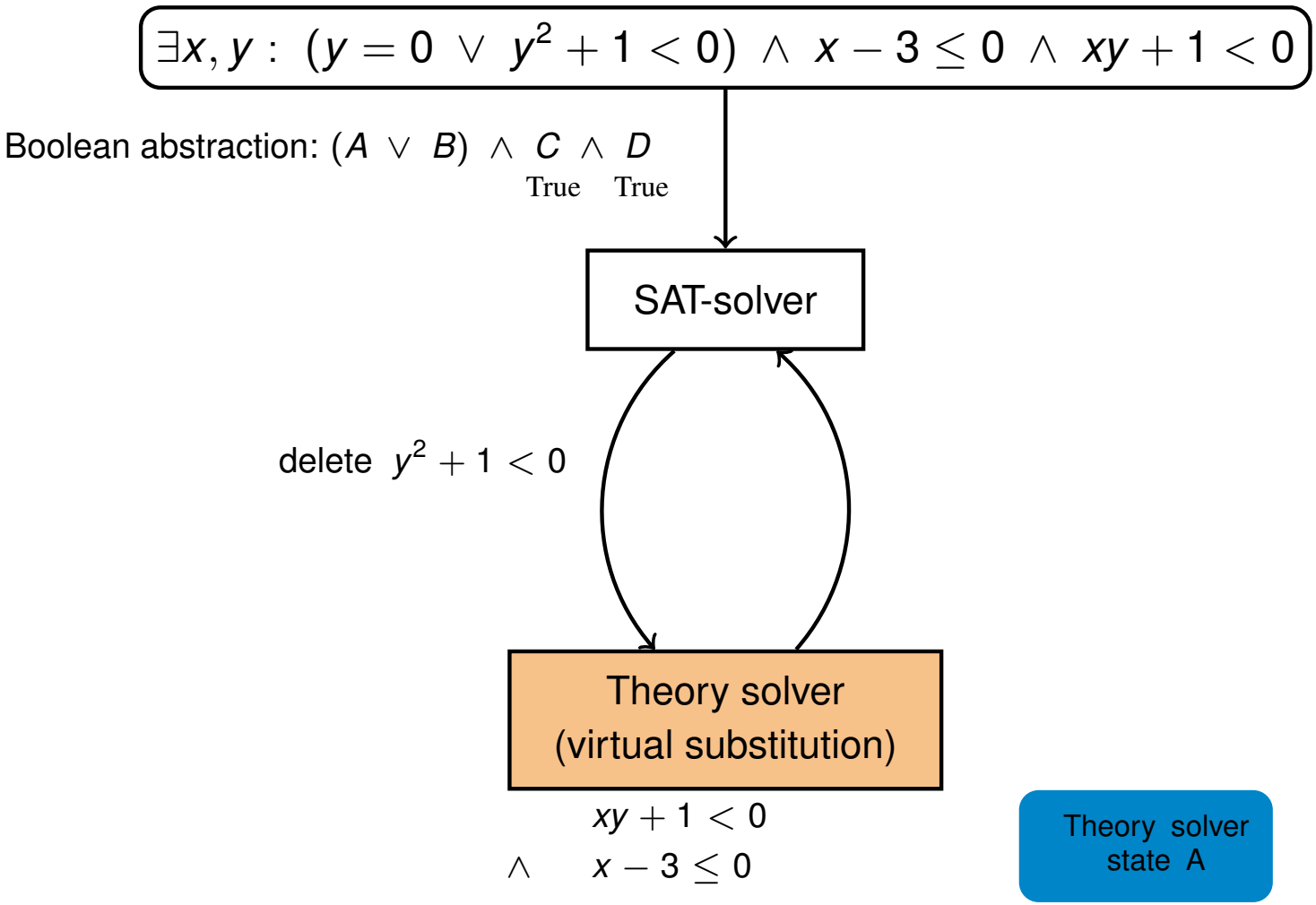
Theory solver: delete $y^2 + 1 < 0$



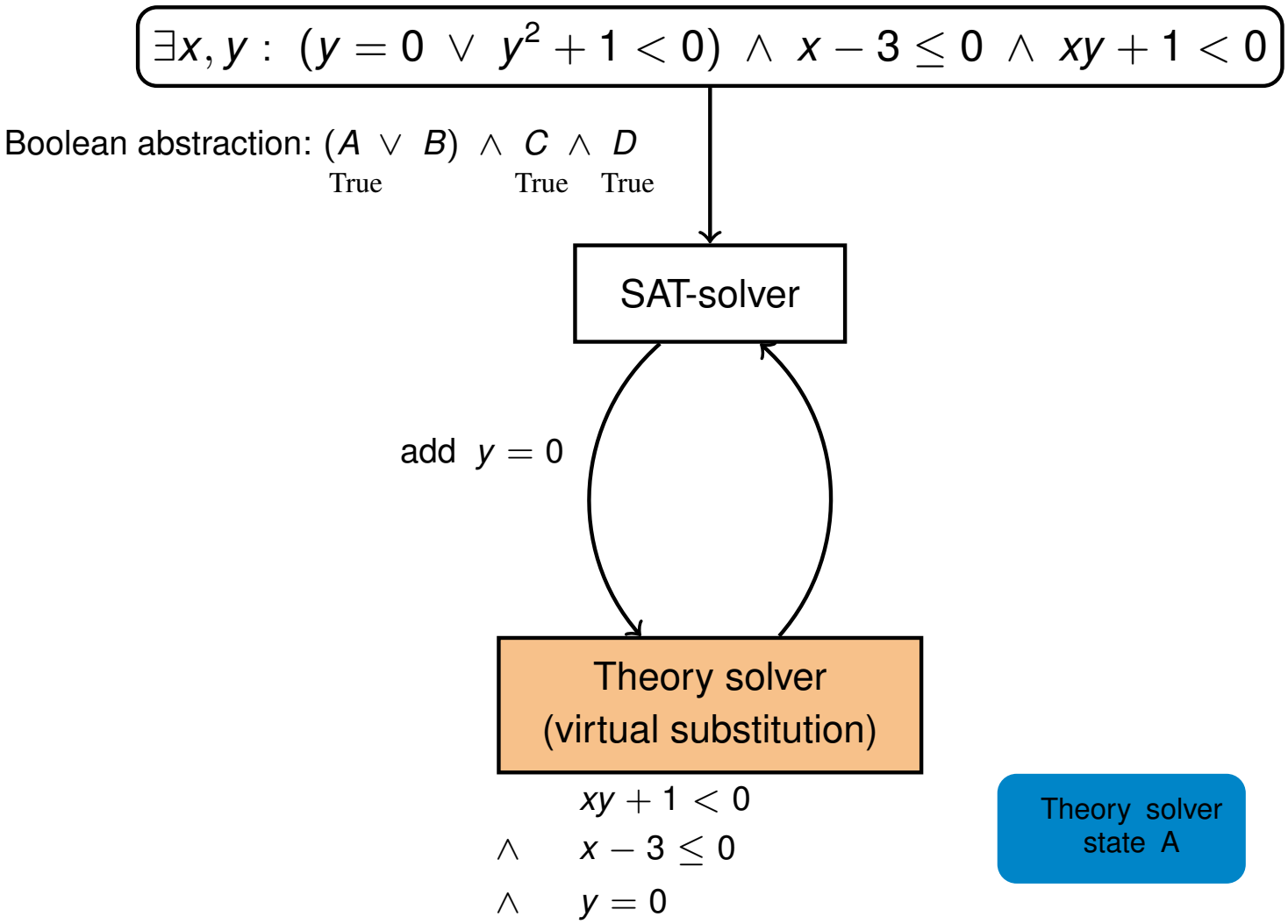
Theory solver: delete $y^2 + 1 < 0$



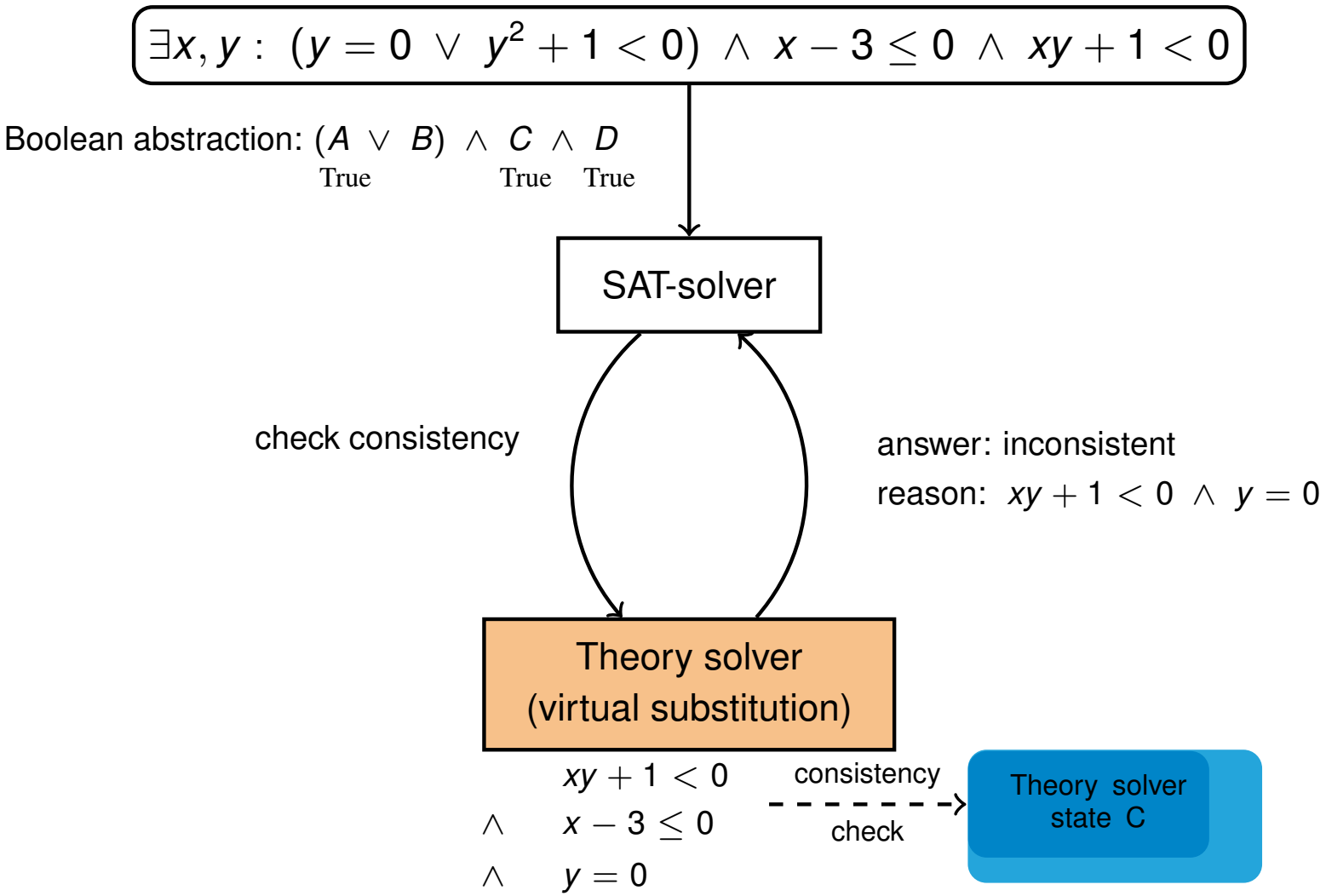
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
SAT-solver
delete $y^2 + 1 < 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
Theory solver
state A

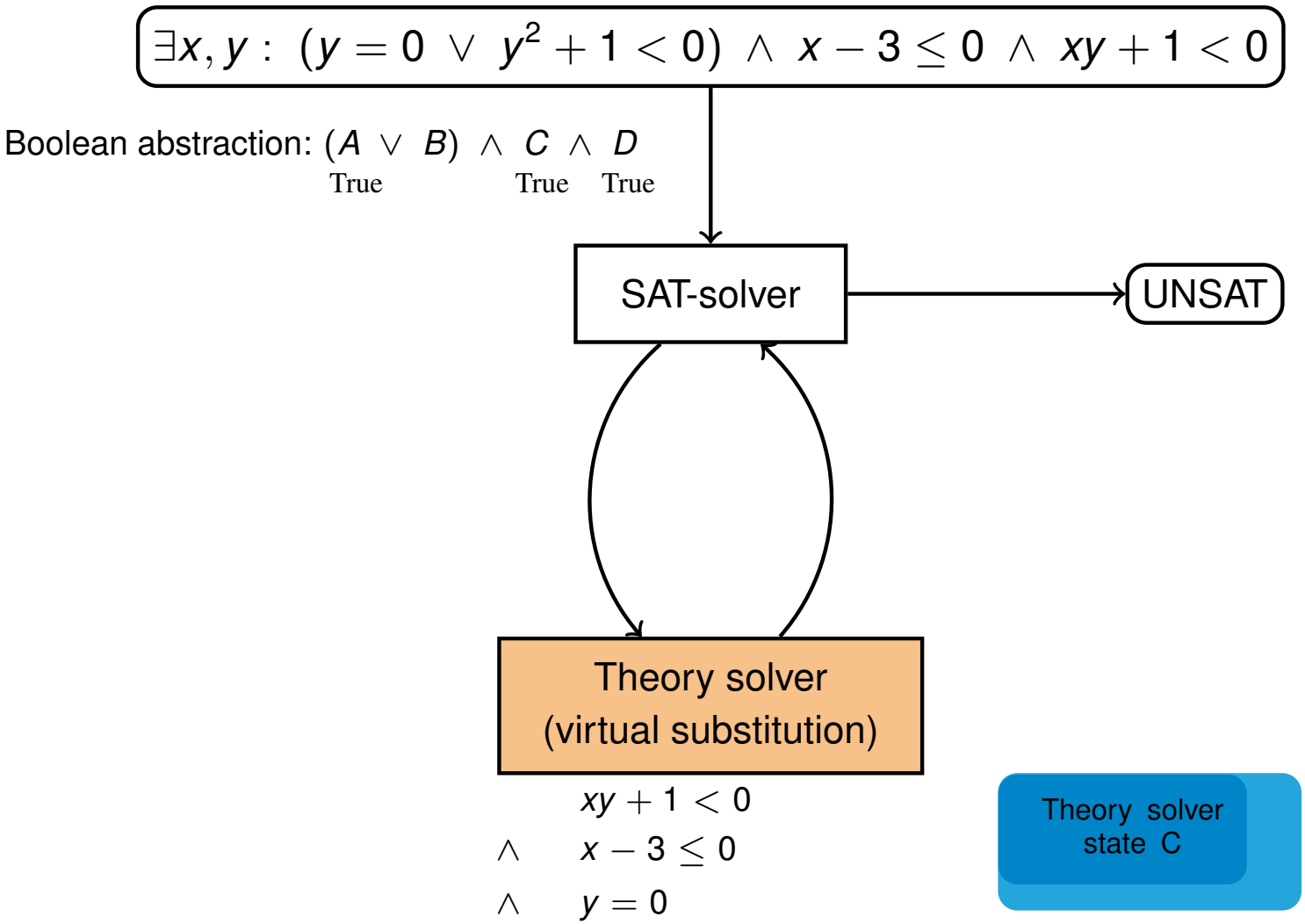
SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
True
SAT-solver
add $y = 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
$\wedge \quad y = 0$
Theory solver state A

SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
True
SAT-solver
check consistency
answer: inconsistent
reason: $xy + 1 < 0 \ \wedge \ y = 0$
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
$\wedge \quad y = 0$
consistency
check
Theory solver
state C

SMT-solver


$\exists x, y: \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$
Boolean abstraction: $(A \ \vee \ B) \ \wedge \ C \ \wedge \ D$
True
True
True
SAT-solver
UNSAT
Theory solver
(virtual substitution)
$xy + 1 < 0$
$\wedge \quad x - 3 \leq 0$
$\wedge \quad y = 0$
Theory solver
state C

Example formula:

- 11 clauses each having 10 randomly generated constraints
- 20 variables

- Compared to the elaborated tool Redlog using virtual substitution

	Ø Runtime
Non-incremental with backjumping:	17.858s
Incremental:	33.576s
Non-incremental:	81.867s
Redlog:	1338.701s

- Achieved:
  - Theory solver using virtual substitution
    1. Incremental
    2. Supports backtracking
    3. Generates reasons (infeasible subsets)
  - Implementation of a theory solver
  - Embedding it into an SMT-solver

- Achieved:
  - Theory solver using virtual substitution
    1. Incremental
    2. Supports backtracking
    3. Generates reasons (infeasible subsets)
  - Implementation of a theory solver
  - Embedding it into an SMT-solver
- Future work:
  - Enable elimination of constraints with degree > 2 and ≤ 4
  - Interaction with the realizable sign conditions method
  - Optimize, optimize, optimize