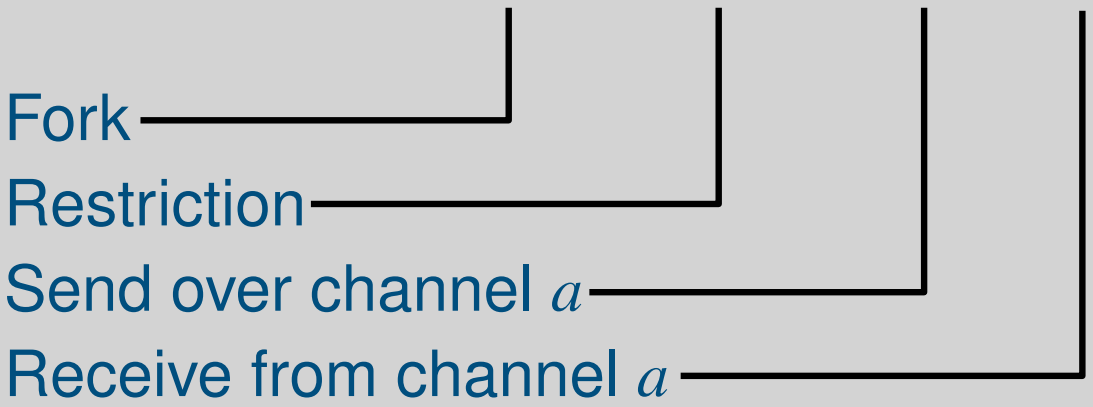
Protocol Security

Refined Concurrent FPC (RPC)
SAT/SMT-solvers

Adding π-calculus-like constructs to FPC

New Terms

$$A, B ::= \ldots \mid A \mathbin{↱} B \mid (\nu a)A \mid a!M \mid a?$$



Example

$$a!42 \mathbin{↱} (\nu c)((\text{let } x = a? \text{ in } c!x) \mathbin{↱} (\text{let } y = c? \text{ in } y))$$

Operational Semantics

As in π-calculus, one introduces a set of structural congruences-like rules to the language, called **Heating**.

The Heating Relation: (not necessarily symmetric)

$A \Rrightarrow A$

$A \Rrightarrow A'$ and $A' \Rrightarrow A''$ then $A \Rrightarrow A''$

$A \Rrightarrow A'$ implies let $x = A$ in $B \Rrightarrow$ let $x = A'$ in B

$A \Rrightarrow B' \longrightarrow B' \Rrightarrow A'$ implies that $A \longrightarrow A'$

Message Passing:

$a!M \Rrightarrow a!M \Rsh ()$

$a!M \Rsh a? \longrightarrow M$

Operational Semantics

Parallel Composition: ($\equiv$ is $\Rrightarrow \cap \Lleftarrow$):

$() \Rsh A \equiv A$

$(A \Rsh A') \Rsh A'' \equiv A \Rsh (A' \Rsh A'')$

$(A \Rsh B) \Rsh A' \equiv (B \Rsh A) \Rsh A'$

let $x = (A \Rsh A')$ in $B \equiv A \Rsh$ (let $x = A'$) in B)

$A \Rrightarrow A'$ implies $(A \Rsh B) \Rrightarrow (A' \Rsh B)$

$A \Rrightarrow A'$ implies $(B \Rsh A) \Rrightarrow (B \Rsh A')$

$A \longrightarrow A'$ implies $(A \Rsh B) \Rrightarrow (A' \Rsh B)$

$A \longrightarrow A'$ implies $(B \Rsh A) \Rrightarrow (B \Rsh A')$

Name Generation

$A \Rsh ((\nu a)A') \Rrightarrow (\nu a)(A \Rsh A')$ if a not free in A

$((\nu a)A \Rsh A') \Rrightarrow (\nu a)(A \Rsh A')$ if a not free in A'

let $x = (\nu a)A$ in $B \equiv (\nu a)$(let $x = A$ in B) if a not free in B

$A \Rrightarrow A'$ implies $(\nu a)A \Rrightarrow (\nu a)A'$

$A \longrightarrow A'$ implies $(\nu a)A \longrightarrow (\nu a)A'$

Type System

Typing environments are formed by type variables α, variable typings $x : T$ and channel typings $a \updownarrow T$.

Type Rules

$$\frac{E \vdash A_1 : T_1 \quad E \vdash A_2 : T_2}{E \vdash A_1 \Rsh A_2 : T_2} \qquad \frac{E, a \updownarrow T \vdash A : U}{E \vdash (\nu a)A : U}$$

$$\frac{E \vdash M : T \quad a \updownarrow T \in E}{E \vdash a!M : unit} \qquad \frac{a \updownarrow T \in E}{E \vdash a? : T}$$

Concurrent FPC has type preservation, but not subject reduction as processes may reach a deadlock or diverge.

Refined Concurrent FPC

New Terms

$A, B ::= \ldots \mid \text{assume } C \mid \text{expect } C$

where C are formulas from first-order logic.

$C ::= p(M_1, \ldots, M_n) \mid M = M' \mid \ldots$

assuming a deduction relation:

$$C_1, \ldots, C_n \vdash C$$

Heating Relations

assume $C \Rrightarrow$ assume $C \nearrow ()$
assert $C \longrightarrow ()$

Structural and Statical Safety

A **Structure** is a term of the following shape:

$$(\nu a_1)\ldots(\nu a_l)\left(\prod_{i=1}^{m}\text{assume } C_i \;\Rsh\; \prod_{j=1}^{n} c_j!M_j \;\Rsh\; \prod_{j=1}^{n}\mathcal{L}_k\{e_k\}\right)$$

where:

$$\mathcal{L} ::= \{\} \mid \text{let } x = \mathcal{L} \text{ in } B$$

$$e ::= M \mid M\ N \mid M = N \mid \text{let } (x, y) = \ldots \mid \text{match} \ldots \mid M? \mid \text{assert } C$$

Statically Safe

For all $k \in 1\ldots 0$ and C, if $e_k = \text{assert } C'_k$ then $C_1 \ldots C_m \vdash C)k'$

Expression Safety

For all A and S, if $A \longrightarrow^* A'$ and $A \Rrightarrow S$, then S is statically safe.

Type System

Types:

$$T, U, V ::= \alpha \mid \text{unit} \mid \{x : T \mid C\} \mid \Pi x : T.U \mid \Sigma x : T.U \mid T + U \mid \mu\alpha.\, T$$

For Refinement Types to work, we need notion of subtyping. For example:

$$\{x : \text{nat} \mid x > 3\} <: \{x : \text{nat} \mid x > 0\}$$

That is, each term of type $\{x : \text{nat} \mid x > 3\}$ also has type $\{x : \text{nat} \mid x > 0\}$.

Contexts may also have declarations of the form $\alpha <: \alpha'$.

Some Judgments:

$E \vdash C$ – context E entails formula C.
$E \vdash T <: U$ – in context E, T is a subtype of U.
$E \vdash A : T$ – in context E, A has type T.

Type System

Derivations:

$$\frac{fv(C) \subseteq fv(E) \quad \text{forms}(E) \vdash C}{E \vdash C}$$

where $\text{forms}(E) = \begin{cases} \{C[y/x]\} \cup \text{forms}(y : T) & \text{if } E = (y : \{x : T \mid C\}) \\ \text{forms}(E_1) \cup \text{forms}(E_2) & \text{if } E = (E_1, E_2) \\ \emptyset & \text{otherwise} \end{cases}$

Assert and Assume:

$$\frac{fv(C) \subseteq dom(E)}{E \vdash \text{assume } C : \{\_ : \text{unit} \mid C\}} \qquad \frac{E \vdash C}{E \vdash \text{assert } C : \text{unit}}$$

Refinement Types: (plus standard subtyping rules)

$$\frac{E \vdash T <: T' \quad E \vdash \{x : T \mid C\}}{E \vdash \{x : T \mid C\} <: T'} \qquad \frac{E \vdash T' <: T \quad E \vdash \{x : T \mid C\}}{E \vdash T' <: \{x : T \mid C\}}$$

$$\frac{E \vdash M : T \quad E \vdash C\{M/x\}}{E \vdash M : \{x : T \mid C\}}$$

Example – Request/Response protocol

```
let rec service (s:service) (f:int → int ) : unit =
    let x,r = recv s:service_payload in
    assert(Request(x));
    let y = f x in
    assume(Response(x, y));
    send r y;
    service s f
```

```
let client (s:service) (x:int ) =
    let r = chan() in
    assume(Request(x));
    send s (x,r);
    let y = recv r in
    assert(Response(x, y));
    y
```

We saw that this program can be typechecked in F7.

$(;x)\mathsf{reply} = \{y : \mathsf{int} \mid \mathsf{Response}(x, y)\ \}$

$\mathsf{service} = (\Sigma x : \{x{:}\mathsf{int} \mid \mathsf{Request}(x)\ \}.\ (;x)\mathsf{reply})\mathsf{chan}$

SAT Solvers – Abstract DPLL algorithm

Input: A **propositional formula** in conjunctive normal form (CNF).

Output: If satisfiable a model, otherwise (should output) a proof.

Method: Build a model M from the CNF F.

Representation: A model is represented as a sequence of literals.

- Order in M matters;
- No repetition of literals;
- M is consistent.

$M(a) = \top$, $M(b) = \bot$, and $M(c) = \bot$, will be modelled as $a\bar{b}\bar{c}$

During execution, a literal l may be marked as a decision literal, written l^d.

States: pairs of the form $M||F$, where F is in CNF.

SAT Solvers – Abstract DPLL algorithm

Extending the Model

UnitProp

$$M||F, C \vee l \longrightarrow M, l||F, C \vee l$$

if $M \models \neg C$ and l is undefined in M.

Decide

$$M||F \longrightarrow M, l^d||F$$

if l or $\neg l$ occurs in F and l is undefined in M.

Repairing the Model

Fail

$$M||F, C \longrightarrow fail$$

if $M \models \neg C$ and M contains no decision literals.

Backtrack

$$Ml^dN||F, C \longrightarrow M\neg l||F, C$$

if $Ml^dN \models \neg C$ and N contains no decision literals.

Example

$$\emptyset \parallel \overline{1} \vee 2, \overline{3} \vee 4, \overline{5} \vee \overline{6}, 6 \vee \overline{5} \vee \overline{2}$$

SMT Solvers

SAT Solvers + Theory Solvers = SMT Solvers

First-order logic, Arithmetic Solvers, Multiset Solvers, Bit-Vectors, etc

Basic Idea

$$x \geq 0, y = x + 1, (y > 2 \vee y < 1)$$

$p_1 = x \geq 0$ $\quad p_3 = y > 2$

$p_2 = y = x + 1$ $\quad p_4 = y < 1$

SAT Solver

CNF $\quad p_1, p_2, (p_3 \vee p_4)$

Assignment $\quad p_1, p_2, \neg p_3, p_4$

Theory Solver

$x \geq 0, y = x + 1, y < 2, y < 1$

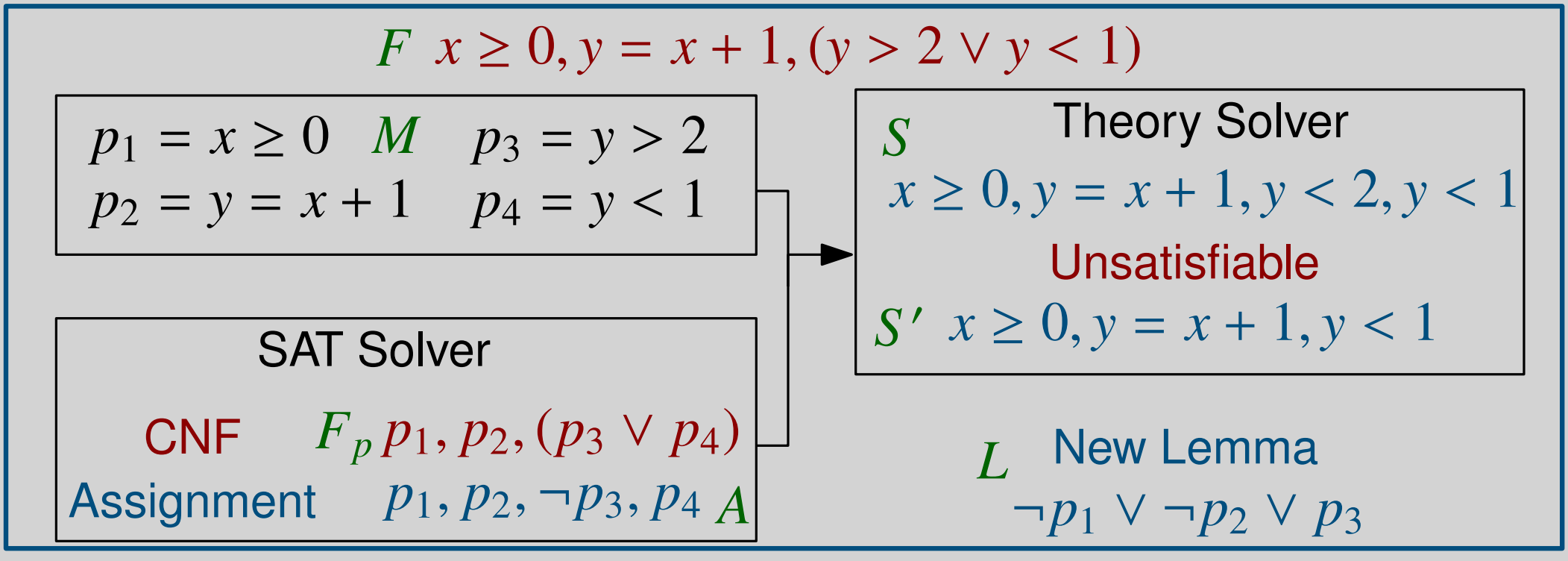
Unsatisfiable

$x \geq 0, y = x + 1, y < 1$

New Lemma

$\neg p_1 \vee \neg p_2 \vee p_3$

```
procedure SMTSolver(F)
    (F_p, M) := Abstract(F)
    loop
        (R, A) := SATSolver(F_p)
        if R is unsatisfiable then return unsatisfiable
        S := Concretize(A, M)
        (R, S') := TheorySolver(S)
        if R is satisfiable then return
        else
            L := NewLemmas(S', M)
            Add L to F_p
```



SMT Solvers

Some Optimizations

Incrementality: send literals to the Theory Solver as they are assigned by the SAT Solver.

Efficient Lemma Generation: Avoiding redundant literals, such as $y < 1$ and $y < 2$.

Theory Propagation: Equivalent to the Unit Propagation:

$$x > 0 \text{ and } y = x + 1 \text{ implies } \neg(y < 1).$$

Theory Solvers by Example

Linear Arithmetic

General form $Ax = 0$ and $l_j \leq x_j \leq u_j$.

$$x \geq 0, (x + y \leq 0 \vee x + 2y \geq 6), (x + y = 2 \vee x + 2y > 4)$$

$s_1 = x + y$ and $s_2 = x + 2y$.

$x \geq 0, (s_1 \leq 0 \vee s_2 \geq 6), (s_1 = 2 \vee s_2 > 4)$

Method: Only bounds are searched for, e.g., $x \leq 2$

Equations and Bounds and generate new bounds:

$$x = y - z, y \leq 2, z \geq 3 \longrightarrow x \leq 1$$

New bounds may be inconsistent with already known bounds.

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x + y$	
$M(y) = 0$	$u = s + 2y$	
$M(s) = 0$	$v = x - y$	
$M(u) = 0$		
$M(v) = 0$		

Theory Solvers by Example

Linear Arithmetic – Example

Asserting:

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x + y$	$s \geq 1$
$M(y) = 0$	$u = s + 2y$	
$M(s) = 0$	$v = x - y$	
$M(u) = 0$		
$M(v) = 0$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x + y$	$s \geq 1$
$M(y) = 0$	$u = s + 2y$	
$M(s) = 0$ False	$v = x - y$	
$M(u) = 0$		
$M(v) = 0$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$x = s - y$	Pivot	$s \geq 1$
$M(y) = 0$	$u = s + 2y$		
$M(s) = 0$	$v = x - y$		
$M(u) = 0$			
$M(v) = 0$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$x = s - y$	Pivot	$s \geq 1$
$M(y) = 0$	$u = s + 2y$		
$M(s) = 0$	$v = s - 2y$		
$M(u) = 0$			
$M(v) = 0$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = 1$	Update	$x = s - y$	$s \geq 1$
$M(y) = 0$		$u = s + 2y$	
$M(s) = 1$		$v = s - 2y$	
$M(u) = 1$	Update		
$M(v) = 1$	Update		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 1$	$x = s - y$	$s \geq 1$
$M(y) = 0$	$u = s + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	
$M(u) = 1$		
$M(v) = 1$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 1$ OK	$x = s - y$	$s \geq 1$
$M(y) = 0$	$u = s + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	
$M(u) = 1$		
$M(v) = 1$		

Theory Solvers by Example

Linear Arithmetic – Example

$\neg(y \leq 1)$

$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$

Model	Equations	Bounds
$M(x) = 1$	$x = s - y$	$s \geq 1$
$M(y) = 0$	$u = s + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y > 1$
$M(u) = 1$		
$M(v) = 1$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 1$	$x = s - y$	$s \geq 1$
$M(y) = 0$ False	$u = s + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y > 1$
$M(u) = 1$		
$M(v) = 1$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 1$	$x = s - y$	$s \geq 1$
$M(y) = 1 + \delta$ Update	$u = s + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y > 1$
$M(u) = 1$		
$M(v) = 1$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = -\delta$ Update	$x = s - y$	$s \geq 1$
$M(y) = 1 + \delta$	$u = s + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y > 1$
$M(u) = 2 + \delta$ Update		
$M(v) = -1 - 2\delta$ Update		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = -\delta$	$x = s - y$	$s \geq 1$
$M(y) = 1 + \delta$	$u = s + 2y$	$x \geq 0$ Violation
$M(s) = 1$	$v = s - 2y$	$y > 1$
$M(u) = 2 + \delta$		
$M(v) = -1 - 2\delta$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = -\delta$	$s = x - y$ Pivot	$s \geq 1$
$M(y) = 1 + \delta$	$u = x + 2y$	$x \geq 0$
$M(s) = 1$	$v = x - y$	$y > 1$
$M(u) = 2 + \delta$		
$M(v) = -1 - 2\delta$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = 0$	Update	$s = x - y$	$s \geq 1$
$M(y) = 1 + \delta$		$u = x + 2y$	$x \geq 0$
$M(s) = 1$		$v = x - y$	$y > 1$
$M(u) = 2 + \delta$			
$M(v) = -1 - 2\delta$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x - y$	$s \geq 1$
$M(y) = 1 + \delta$	$u = x + 2y$	$x \geq 0$
$M(s) = 1 + \delta$ Update	$v = x - y$	$y > 1$
$M(u) = 2 + 2\delta$ Update		
$M(v) = -1 - \delta$ Update		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$s = x - y$		$s \geq 1$
$M(y) = 1 + \delta$	$u = x + 2y$	Theory Propagation	$x \geq 0$
$M(s) = 1 + \delta$	$v = x - y$		$y > 1$
$M(u) = 2 + 2\delta$			$u > 2$
$M(v) = -1 - \delta$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$s = x - y$		$s \geq 1$
$M(y) = 1 + \delta$	$u = x + 2y$		$x \geq 0$
$M(s) = 1 + \delta$	$v = x - y$	Wrong Decision	$y > 1$
$M(u) = 2 + 2\delta$			$u > 2$
$M(v) = -1 - \delta$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x - y$	$s \geq 1$
$M(y) = 1 + \delta$	$u = x + 2y$	$x \geq 0$
$M(s) = 1 + \delta$	$v = x - y$	
$M(u) = 2 + 2\delta$		
$M(v) = -1 - \delta$		

Backtrack

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$s = x - y$		$s \geq 1$
$M(y) = 1 + \delta$	$u = x + 2y$		$x \geq 0$
$M(s) = 1 + \delta$	$v = x - y$	Backtrack	$y \leq 1$
$M(u) = 2 + 2\delta$			
$M(v) = -1 - \delta$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = 0$		$s = x - y$	$s \geq 1$
$M(y) = 1$	Update	$u = x + 2y$	$x \geq 0$
$M(s) = 1 + \delta$		$v = x - y$	$y \leq 1$
$M(u) = 2 + 2\delta$			
$M(v) = -1 - \delta$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = 0$		$s = x - y$	$s \geq 1$
$M(y) = 1$		$u = x + 2y$	$x \geq 0$
$M(s) = 1$	Update	$v = x - y$	$y \leq 1$
$M(u) = 2$	Update		
$M(v) = -1$	Update		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$s = x - y$		$s \geq 1$
$M(y) = 1$	$u = x + 2y$		$x \geq 0$
$M(s) = 1$	$v = s - 2y$	Theory Propagation	$y \leq 1$
$M(u) = 2$			$v \geq 1$
$M(v) = -1$			

Theory Solvers by Example

Linear Arithmetic – Example

$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$

Model	Equations	Bounds
$M(x) = 0$	$s = x - y$	$s \geq 1$
$M(y) = 1$	$u = x + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y \leq 1$
$M(u) = 2$		$v \geq 0$ Update
$M(v) = -1$		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x - y$	$s \geq 1$
$M(y) = 1$	$u = x + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y \leq 1$
$M(u) = 2$		$v \geq 0$
$M(v) = -1$ False		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 0$	$s = x - y$	$s \geq 1$
$M(y) = 1$	$u = x + 2y$	$x \geq 0$
$M(s) = 1$	$v = s - 2y$	$y \leq 1$
$M(u) = 2$		$v \geq 0$
$M(v) = 0$ Update		

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 0$	$x = v + y$		$s \geq 1$
$M(y) = 1$	$u = v + 3y$		$x \geq 0$
$M(s) = 1$	$s = v + 2y$	Pivot	$y \leq 1$
$M(u) = 2$			$v \geq 0$
$M(v) = 0$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = 1$	Update	$x = v + y$	$s \geq 1$
$M(y) = 1$		$u = v + 3y$	$x \geq 0$
$M(s) = 2$	Update	$s = v + 2y$	$y \leq 1$
$M(u) = 3$	Update		$v \geq 0$
$M(v) = 0$			

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 1$	$x = v + y$	$s \geq 1$
$M(y) = 1$	$u = v + 3y$	$x \geq 0$
$M(s) = 2$	$s = v + 2y$	$y \leq 1$
$M(u) = 3$		$v \geq 0$
$M(v) = 0$		$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations		Bounds
$M(x) = 1$	$x = \frac{1}{3}u + \frac{2}{3}v$		$s \geq 1$
$M(y) = 1$	$y = \frac{1}{3}u - \frac{1}{3}v$	Pivot	$x \geq 0$
$M(s) = 2$	$s = \frac{2}{3}u + \frac{1}{3}v$		$y \leq 1$
$M(u) = 3$			$v \geq 0$
$M(v) = 0$			$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = 1$	$x = \frac{1}{3}u + \frac{2}{3}v$	$s \geq 1$
$M(y) = 1$	$y = \frac{1}{3}u - \frac{1}{3}v$	$x \geq 0$
$M(s) = 2$	$s = \frac{2}{3}u + \frac{1}{3}v$	$y \leq 1$
$M(u) = -1$ Update		$v \geq 0$
$M(v) = 0$		$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = -\frac{1}{3}$	Update	$x = \frac{1}{3}u + \frac{2}{3}v$	$s \geq 1$
$M(y) = -\frac{1}{3}$	Update	$y = \frac{1}{3}u - \frac{1}{3}v$	$x \geq 0$
$M(s) = -\frac{2}{3}$	Update	$s = \frac{2}{3}u + \frac{1}{3}v$	$y \leq 1$
$M(u) = -1$	Update		$v \geq 0$
$M(v) = 0$			$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = -\frac{1}{3}$	$x = \frac{1}{3}u + \frac{2}{3}v$	$s \geq 1$
$M(y) = -\frac{1}{3}$	$y = \frac{1}{3}u - \frac{1}{3}v$	$x \geq 0$
$M(s) = -\frac{2}{3}$	$s = \frac{2}{3}u + \frac{1}{3}v$	$y \leq 1$
$M(u) = -1$		$v \geq 0$
$M(v) = 0$	Bound Violations	$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model	Equations	Bounds
$M(x) = -\frac{1}{3}$	$x = 2s - u$	$s \geq 1$
$M(y) = -\frac{1}{3}$	$y = -s + u$	$x \geq 0$
$M(s) = -\frac{2}{3}$	$v = 3s - 2u$ Pivot	$y \leq 1$
$M(u) = -1$		$v \geq 0$
$M(v) = 0$		$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = -\frac{1}{3}$		$x = 2s - u$	$s \geq 1$
$M(y) = -\frac{1}{3}$		$y = -s + u$	$x \geq 0$
$M(s) = 1$	Update	$v = 3s - 2u$	$y \leq 1$
$M(u) = -1$			$v \geq 0$
$M(v) = 0$			$u \leq -1$

Theory Solvers by Example

Linear Arithmetic – Example

$$s \geq 1, x \geq 0, (y \leq 1 \vee v \geq 2), (v \leq -2 \vee v \geq 0), (v \leq -2 \vee u \leq -1)$$

Model		Equations	Bounds
$M(x) = 3$	Update	$x = 2s - u$	$s \geq 1$
$M(y) = -2$	Update	$y = -s + u$	$x \geq 0$
$M(s) = 1$		$v = 3s - 2u$	$y \leq 1$
$M(u) = -1$			$v \geq 0$
$M(v) = 0$			$u \leq -1$