Microsoft Research

# Satisfiability Modulo Theories (SMT): ideas and applications

## Università Degli Studi Di Milano
## Scuola di Dottorato in Informatica, 2010

Leonardo de Moura
Microsoft Research

# Linear Arithmetic

- Many approaches
  - Graph-based for difference logic: $a - b \leq 3$
  - Fourier-Motzkin elimination:

$$t_1 \leq ax, \;\; bx \leq t_2 \;\; \Rightarrow \;\; bt_1 \leq at_2$$

  - Standard Simplex
  - General Form Simplex

Microsoft Research

# Difference Logic: $a - b \leq 5$

Very useful in practice!

Most arithmetical constraints in software verification/analysis are in this fragment.

$x := x + 1$

$x_1 = x_0 + 1$

$x_1 - x_0 \leq 1, x_0 - x_1 \leq -1$

Microsoft Research

# Job shop scheduling

| $d_{i,j}$ | Machine 1 | Machine 2 |
|---|---|---|
| Job 1 | 2 | 1 |
| Job 2 | 3 | 1 |
| Job 3 | 2 | 3 |

$max = 8$

**Solution**

$t_{1,1} = 5,\ t_{1,2} = 7,\ t_{2,1} = 2,$
$t_{2,2} = 6,\ t_{3,1} = 0,\ t_{3,2} = 3$

**Encoding**

$$(t_{1,1} \geq 0) \wedge (t_{1,2} \geq t_{1,1} + 2) \wedge (t_{1,2} + 1 \leq 8) \wedge$$
$$(t_{2,1} \geq 0) \wedge (t_{2,2} \geq t_{2,1} + 3) \wedge (t_{2,2} + 1 \leq 8) \wedge$$
$$(t_{3,1} \geq 0) \wedge (t_{3,2} \geq t_{3,1} + 2) \wedge (t_{3,2} + 3 \leq 8) \wedge$$
$$((t_{1,1} \geq t_{2,1} + 3) \vee (t_{2,1} \geq t_{1,1} + 2)) \wedge$$
$$((t_{1,1} \geq t_{3,1} + 2) \vee (t_{3,1} \geq t_{1,1} + 2)) \wedge$$
$$((t_{2,1} \geq t_{3,1} + 2) \vee (t_{3,1} \geq t_{2,1} + 3)) \wedge$$
$$((t_{1,2} \geq t_{2,2} + 1) \vee (t_{2,2} \geq t_{1,2} + 1)) \wedge$$
$$((t_{1,2} \geq t_{3,2} + 3) \vee (t_{3,2} \geq t_{1,2} + 1)) \wedge$$
$$((t_{2,2} \geq t_{3,2} + 3) \vee (t_{3,2} \geq t_{2,2} + 1))$$

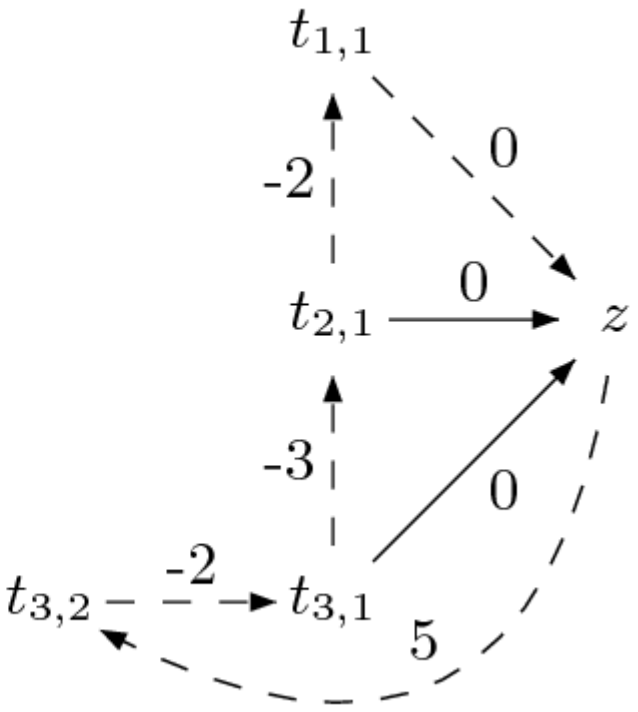
Microsoft Research

# Difference Logic

Chasing negative cycles!

Algorithms based on Bellman-Ford (O(mn)).

$$
\begin{array}{lcll}
z & - & t_{1,1} & \leq & 0 \\
z & - & t_{2,1} & \leq & 0 \\
z & - & t_{3,1} & \leq & 0 \\
t_{3,2} & - & z & \leq & 5 \\
t_{3,1} & - & t_{3,2} & \leq & -2 \\
t_{2,1} & - & t_{3,1} & \leq & -3 \\
t_{1,1} & - & t_{2,1} & \leq & -2
\end{array}
$$




Microsoft Research

# Standard Simplex

Many solvers (e.g., ICS, Simplify) are based on the Standard Simplex.

$$
\begin{aligned}
a - d + 2e &= 3 \\
b - d &= 1 \\
c + d - e &= -1 \\
a, b, c, d, e &\geq 0
\end{aligned}
$$

# Standard Simplex

Many solvers (e.g., ICS, Simplify) are based on the Standard Simplex.

$$a - d + 2e = 3$$
$$b - d = 1$$
$$c + d - e = -1$$
$$a, b, c, d, e \geq 0$$

$$\begin{pmatrix} 1 & 0 & 0 & -1 & 2 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ -1 \end{pmatrix}$$

$$Ax = b \text{ and } x \geq 0.$$

Microsoft Research

# Standard Simplex

Many solvers (e.g., ICS, Simplify) are based on the Standard Simplex.

$$
\begin{aligned}
a - d + 2e &= 3 \\
b - d &= 1 \\
c + d - e &= -1 \\
a, b, c, d, e &\geq 0
\end{aligned}
$$

We say a,b,c are the basic (or dependent) variables

$$
\begin{pmatrix} 1 & 0 & 0 & -1 & 2 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & -1 \end{pmatrix}
\begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix}
=
\begin{pmatrix} 3 \\ 1 \\ -1 \end{pmatrix}
$$

$$Ax = b \text{ and } x \geq 0.$$

Microsoft Research

# Standard Simplex

Many solvers (e.g., ICS, Simplify) are based on the Standard Simplex.

$$
\begin{aligned}
a - d + 2e &= 3 \\
b - d &= 1 \\
c + d - e &= -1 \\
a, b, c, d, e &\geq 0
\end{aligned}
$$

We say a,b,c are the basic (or dependent) variables

We say d,e are the non-basic (or non-dependent) variables.

$$
\begin{pmatrix} 1 & 0 & 0 & -1 & 2 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & -1 \end{pmatrix}
\begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix}
=
\begin{pmatrix} 3 \\ 1 \\ -1 \end{pmatrix}
$$

$$Ax = b \text{ and } x \geq 0.$$

Microsoft Research

# Standard Simplex

- Incrementality: add/remove equations
- Slow backtracking
- No theory propagation

# Fast Linear Arithmetic

- Simplex General Form
- Algorithm based on the dual simplex
- Non redundant proofs
- Efficient backtracking
- Efficient theory propagation
- Support for string inequalities: t > 0
- Preprocessing step
- Integer problems:

  Gomory cuts,  Branch & Bound, GCD test

# General Form

General Form: $Ax = 0$ and $l_j \leq x_j \leq u_j$

Example:

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

$$\rightsquigarrow$$

$$s_1 \equiv x + y, s_2 \equiv x + 2y,$$

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

Only bounds (e.g., $s_1 \leq 2$) are asserted during the search.

Unconstrained variables can be eliminated before the beginning of the search.

# From Definitions to a Tableau

$s_1 \equiv x + y, \quad s_2 \equiv x + 2y$

# From Definitions to a Tableau

$s_1 \equiv x + y, \quad s_2 \equiv x + 2y$

$s_1 = x + y,$

$s_2 = x + 2y$

# From Definitions to a Tableau

$s_1 \equiv x + y, \quad s_2 \equiv x + 2y$

$s_1 = x + y,$

$s_2 = x + 2y$

$s_1 - x - y = 0$

$s_2 - x - 2y = 0$

# From Definitions to a Tableau

$s_1 \equiv x + y, \quad s_2 \equiv x + 2y$

$s_1 = x + y,$

$s_2 = x + 2y$

$s_1 - x - y = 0$

$s_2 - x - 2y = 0$

$s_1, s_2$ are basic (dependent)

x,y are non-basic

Microsoft Research

# Pivoting

A way to swap a basic with a non-basic variable!

It is just equational reasoning.

Key invariant: a basic variable occurs in only one equation.

Example: swap $s_1$ and y

$$s_1 - x - y = 0$$
$$s_2 - x - 2y = 0$$

Microsoft Research

# Pivoting

A way to swap a basic with a non-basic variable!

It is just equational reasoning.

Key invariant: a basic variable occurs in only one equation.

Example: swap $s_1$ and y

$$s_1 - x - y = 0$$
$$s_2 - x - 2y = 0$$

$$-s_1 + x + y = 0$$
$$s_2 - x - 2y = 0$$

# Pivoting

A way to swap a basic with a non-basic variable!

It is just equational reasoning.

Key invariant: a basic variable occurs in only one equation.

Example: swap $s_1$ and y

$$s_1 - x - y = 0$$
$$s_2 - x - 2y = 0$$

$$-s_1 + x + y = 0$$
$$s_2 - x - 2y = 0$$

$$-s_1 + x + y = 0$$
$$s_2 - 2s_1 + x = 0$$

Microsoft Research

# Pivoting

A way to swap a basic with a non-basic variable!

It is just equational reasoning.

Key invariant: a basic variable occurs in only one equation.

Example: swap $s_1$ and y

$s_1 - x - y = 0$

$s_2 - x - 2y = 0$

$-s_1 + x + y = 0$

$s_2 - x - 2y = 0$

$-s_1 + x + y = 0$

$s_2 - 2s_1 + x = 0$

It is just substituting equals by equals.

Microsoft Research

# Pivoting

**Definition:**
An assignment (model) is a mapping from variables to values

A way to swap a basic with a non-basic variable!

It is just equational reasoning.

Key invariant: a basic variable occurs in only one equation.

Example: swap $s_1$ and y

$s_1 - x - y = 0$

$s_2 - x - 2y = 0$

$-s_1 + x + y = 0$

$s_2 - x - 2y = 0$

$-s_1 + x + y = 0$

$s_2 - 2s_1 + x = 0$

It is just substituting equals by equals.

**Key Property:**
If an assignment satisfies the equations before a pivoting step, then it will also satisfy them after!

# Pivoting

**Definition:**
An assignment (model) is a mapping from variables to values

A way to swap a basic with a non-basic variable!

It is just equational reasoning.

Key invariant: a basic variable occurs in only one equation.

Example: swap $s_2$ and y

$s_1 - x - y = 0$

$s_2 - x - 2y = 0$

$-s_1 + x + y = 0$

$s_2 - x - 2y = 0$

$-s_1 + x + y = 0$

$s_2 - 2s_1 + x = 0$

It is just substituting equals by equals.

Example:
$M(x) = 1$
$M(y) = 1$
$M(s_1) = 2$
$M(s_2) = 3$

Key Property:
If an assignment satisfies the equations before a pivoting step, then it will also satisfy them after!

# Equations + Bounds + Assignment

An assignment (model) is a mapping from variables to values.

We maintain an assignment that satisfies all equations and bounds.

The assignment of non dependent variables implies the assignment of dependent variables.

Equations + Bounds can be used to derive new bounds.

Example: $x = y - z,\ y \leq 2,\ z \geq 3 \rightsquigarrow x \leq -1.$

The new bound may be inconsistent with the already known bounds.

Example: $x \leq -1,\ x \geq 0.$

# “Repairing Models”

If the assignment of a non-basic variable does not satisfy a bound, then fix it and propagate the change to all dependent variables.

$a = c - d$

$b = c + d$

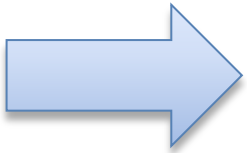
$M(a) = 0$

$M(b) = 0$

$M(c) = 0$

$M(d) = 0$

$1 \leq c$



$a = c - d$

$b = c + d$

$M(a) = 1$

$M(b) = 1$

$M(c) = 1$

$M(d) = 0$

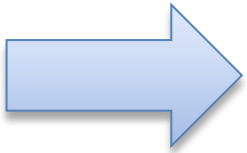
$1 \leq c$

Microsoft Research

# "Repairing Models"

If the assignment of a non-basic variable does not satisfy a bound, then fix it and propagate the change to all dependent variables. Of course, we may introduce new "problems".

$a = c - d$
$b = c + d$
$M(a) = 0$
$M(b) = 0$
$M(c) = 0$
$M(d) = 0$
$1 \leq c$
$a \leq 0$



$a = c - d$
$b = c + d$
$M(a) = 1$
$M(b) = 1$
$M(c) = 1$
$M(d) = 0$
$1 \leq c$
$\mathbf{a \leq 0}$

Microsoft Research

# “Repairing Models”

If the assignment of a basic variable does not satisfy a bound, then pivot it, fix it, and propagate the change to its new dependent variables.

| | | |
|---|---|---|
| $a = c - d$ | $c = a + d$ | $c = a + d$ |
| $b = c + d$ | $b = a + 2d$ | $b = a + 2d$ |
| $M(a) = 0$ | $M(a) = 0$ | $M(a) = 1$ |
| $M(b) = 0$ | $M(b) = 0$ | $M(b) = 1$ |
| $M(c) = 0$ | $M(c) = 0$ | $M(c) = 1$ |
| $M(d) = 0$ | $M(d) = 0$ | $M(d) = 0$ |
| $1 \leq a$ | $1 \leq a$ | $1 \leq a$ |

Microsoft Research

# "Repairing Models"

Sometimes, a model cannot be repaired. It is pointless to pivot.

$a = b - c$

$a \leq 0, 1 \leq b, c \leq 0$

$M(a) = 1$

$M(b) = 1$

$M(c) = 0$

The value of M(a) is too big. We can reduce it by:

- reducing M(b)
  - not possible b is at lower bound
- increasing M(c)
  - not possible c is at upper bound

Microsoft Research

# “Repairing Models”

Extracting proof from failed repair attempts is easy.

$s_1 \equiv a + d$, $s_2 \equiv c + d$

$a = s_1 - s_2 + c$

$a \leq 0$, $1 \leq s_1$, $s_2 \leq 0$, $0 \leq c$

$M(a) = 1$

$M(s_1) = 1$

$M(s_2) = 0$

$M(c) = 0$

Microsoft Research

# "Repairing Models"

Extracting proof from failed repair attempts is easy.

$s_1 \equiv a + d$, $s_2 \equiv c + d$

$a = s_1 - s_2 + c$

$a \leq 0$, $1 \leq s_1$, $s_2 \leq 0$, $0 \leq c$

$M(a) = 1$

$M(s_1) = 1$

$M(s_2) = 0$

$M(c) = 0$

$\{ a \leq 0, 1 \leq s_1, s_2 \leq 0, 0 \leq c \}$ is inconsistent

Microsoft Research

# "Repairing Models"

Extracting proof from failed repair attempts is easy.

$s_1 \equiv a + d$, $s_2 \equiv c + d$

$a = s_1 - s_2 + c$

$a \leq 0,\ 1 \leq s_1,\ s_2 \leq 0,\ 0 \leq c$

$M(a) = 1$

$M(s_1) = 1$

$M(s_2) = 0$

$M(c) = 0$

$\{ a \leq 0,\ 1 \leq s_1,\ s_2 \leq 0,\ 0 \leq c \}$ is inconsistent

$\{ a \leq 0,\ 1 \leq a + d,\ c + d \leq 0,\ 0 \leq c \}$ is inconsistent

Microsoft Research

# Strict Inequalities

The method described only handles non-strict inequalities (e.g., $x \leq 2$).

For integer problems, strict inequalities can be converted into non-strict inequalities. $x < 1 \rightsquigarrow x \leq 0$.

For rational/real problems, strict inequalities can be converted into non-strict inequalities using a small $\delta$. $x < 1 \rightsquigarrow x \leq 1 - \delta$.

We do not compute a $\delta$, we treat it symbolically.

$\delta$ is an infinitesimal parameter: $(c, k) = c + k\delta$

# Example

- Initial state

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$ assignment does not satisfy new bound.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$ pivot $s$ and $x$ ($s$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$ pivot $s$ and $x$ ($s$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$ pivot $s$ and $x$ ($s$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$ update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $s \geq 1$ update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $x \geq 0$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $x \geq 0$ assignment satisfies new bound.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Case split $\neg y \leq 1$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Case split $\neg y \leq 1$ assignment does not satisfies new bound.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Case split $\neg y \leq 1$ update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Case split $\neg y \leq 1$ update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $x$ and $s$ ($x$ is a dependent variables).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $x$ and $s$ ($x$ is a dependent variables).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $x$ and $s$ ($x$ is a dependent variables).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Theory propagation $x \geq 0, y > 1 \rightsquigarrow u > 2$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Theory propagation $u > 2 \rightsquigarrow \neg u \leq -1$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Boolean propagation $\neg y \leq 1 \rightsquigarrow v \geq 2$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Theory propagation $v \geq 2 \rightsquigarrow \neg v \leq -2$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Conflict empty clause

$$s \geq 1, x \geq 0$$

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

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

# Example

- Backtracking

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $y \leq 1$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $y \leq 1$ assignment does not satisfy new bound.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $y \leq 1$ update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Asserting $y \leq 1$ update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Theory propagation $s \geq 1, y \leq 1 \rightsquigarrow v \geq -1$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Theory propagation $v \geq -1 \rightsquigarrow \neg v \leq -2$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Boolean propagation $\neg v \leq -2 \rightsquigarrow v \geq 0$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation assignment does not satisfy new bound.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $u$ and $s$ ($u$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $u$ and $s$ ($u$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $u$ and $s$ ($u$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Boolean propagation $\neg v \leq -2 \rightsquigarrow u \leq -1$

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation assignment does not satisfy new bound.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $u$ and $y$ ($u$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $u$ and $y$ ($u$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation pivot $u$ and $y$ ($u$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violation update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violations

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violations pivot $s$ and $v$ ($s$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violations pivot $s$ and $v$ ($s$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violations pivot $s$ and $v$ ($s$ is a dependent variable).

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violations update assignment.

$$s \geq 1, x \geq 0$$

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

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

# Example

- Bound violations update dependent variables assignment.

$$s \geq 1, x \geq 0$$

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

| Model | | | Equations | | | Bounds | | |
|---|---|---|---|---|---|---|---|---|
| $M(x)$ | $=$ | $3$ | $x$ | $=$ | $2s - u$ | $s$ | $\geq$ | $1$ |
| $M(y)$ | $=$ | $-2$ | $y$ | $=$ | $-s + u$ | $x$ | $\geq$ | $0$ |
| $M(s)$ | $=$ | $1$ | $v$ | $=$ | $3s - 2u$ | $y$ | $\leq$ | $1$ |
| $M(u)$ | $=$ | $-1$ | | | | $v$ | $\geq$ | $0$ |
| $M(v)$ | $=$ | $5$ | | | | $u$ | $\leq$ | $-1$ |

# Example

- Found satisfying assignment

$$s \geq 1, x \geq 0$$

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

| Model | | | Equations | | | Bounds | | |
|---|---|---|---|---|---|---|---|---|
| $M(x)$ | $=$ | $3$ | $x$ | $=$ | $2s - u$ | $s$ | $\geq$ | $1$ |
| $M(y)$ | $=$ | $-2$ | $y$ | $=$ | $-s + u$ | $x$ | $\geq$ | $0$ |
| $M(s)$ | $=$ | $1$ | $v$ | $=$ | $3s - 2u$ | $y$ | $\leq$ | $1$ |
| $M(u)$ | $=$ | $-1$ | | | | $v$ | $\geq$ | $0$ |
| $M(v)$ | $=$ | $5$ | | | | $u$ | $\leq$ | $-1$ |

# Correctness

Completeness: trivial

Soundness: also trivial

Termination: non trivial.

We cannot choose arbitrary variable to pivot.

Assume the variables are ordered.

Bland's rule: select the smallest basic variable c that does not satisfy its bounds, then select the smallest non-basic in the row of c that can be used for pivoting.

Too technical.

Uses the fact that a tableau has a finite number of configurations. Then, any infinite trace will have cycles.

# Data-structures

Array of rows (equations).

Each row is a dynamic array of tuples:

(coefficient, variable, pos_in_occs, is_dead)

Each variable x has a “set” (dynamic array) of occurrences:

(row_idx, pos_in_row, is_dead)

Each variable x has a “field” row[x]

row[x] is -1 if x is non basic

otherwise, row[x] contains the idx of the row containing x

Each variable x has “fields”: lower[x], upper[x], and value[x]

# Data-structures

rows: array of rows (equations).

Each row is a dynamic array of tuples:

(coefficient, variable, pos_in_occs, is_dead)

occs[x]: Each variable x has a “set” (dynamic array) of occurrences:

(row_idx, pos_in_row, is_dead)

row[x]:

row[x] is -1 if x is non basic

otherwise, row[x] contains the idx of the row containing x

Other “fields”: lower[x], upper[x], and value[x]

atoms[x]: atoms (assigned/unassigned) that contains x

# Data-structures

$s_1 \equiv a + b$, $s_2 \equiv c - b$

$p_1 \equiv a \leq 0$, $p_2 \equiv 1 \leq s_1$, $p_3 \equiv 1 \leq s_2$

$p_1$, $p_2$ were already assigned

$a - s_1 + s_2 + c = 0$

$b - c + s_2 = 0$

$a \leq 0$, $1 \leq s_1$

M(a) = 0 value[a] = 0

M(b) = -1 value[a] = -1

M(c) = 0 value[c] = 0

$M(s_1) = 1$ $value[s_1] = 1$

$M(s_2) = 1$ $value[s_2] = 1$

rows = [

[(1, a, 0, t), (-1, $s_1$, 0, t), (1, $s_2$, 1, t), (1, c, 0, t)],

[(1,b, 0, t), (-1, c, 1, t), (1, $s_2$, 2, t)] ]

occs[a] = [(0, 0, f)]

occs[b] = [(1,0,f)]

occs[c] = [(0,3,f), (1,1,f)]

$occs[s_1]$ = [(0,1,f)]

$occs[s_2]$ = [(0,0,t), (0,2,f), (1,2,f)]

row[a] = 0, row[b] = 1, row[c] = -1, …

upper[a] = 0, $lower[s_1] = 1$

atoms[a] = $\{p_1\}$, $atoms[s_1] = \{p_2\}$, …

Microsoft Research

# Combining Theories

In practice, we need a combination of theories.

$b + 2 = c$ and $f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

A theory is a set (potentially infinite) of first-order sentences.

**Main questions**:

Is the union of two theories $T1 \cup T2$ consistent?

Given a solvers for T1 and T2, how can we build a solver for $T1 \cup T2$?

Microsoft Research

# Disjoint Theories

Two theories are disjoint if they do not share function/constant and predicate symbols.

= is the only exception.

Example:

The theories of arithmetic and arrays are disjoint.

Arithmetic symbols: {0, -1, 1, -2, 2, …, +, -, *, >, <, ≥, ≤}

Array symbols: { read, write }

# Purification

It is a different name for our “naming” subterms procedure.

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

$b + 2 = c,\ v_6 \neq v_7$

$v_1 \equiv 3,\ v_2 \equiv write(a, b, v_1),\ v_3 \equiv c-2,\ v_4 \equiv read(v_2, v_3),$

$v_5 \equiv c-b+1,\ v_6 \equiv f(v_4),\ v_7 \equiv f(v_5)$

Microsoft Research

# Purification

It is a different name for our "naming" subterms procedure.

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

$b + 2 = c,\ v_6 \neq v_7$

$v_1 \equiv 3,\ v_2 \equiv write(a, b, v_1),\ v_3 \equiv c-2,\ v_4 \equiv read(v_2, v_3),$

$v_5 \equiv c-b+1,\ v_6 \equiv f(v_4),\ v_7 \equiv f(v_5)$

$b + 2 = c,\ v_1 \equiv 3,\ v_3 \equiv c-2,\ v_5 \equiv c-b+1,$

$v_2 \equiv write(a, b, v_1),\ v_4 \equiv read(v_2, v_3),$

$v_6 \equiv f(v_4),\ v_7 \equiv f(v_5),\ v_6 \neq v_7$

Microsoft Research

# Stably Infinite Theories

A theory is stably infinite if every satisfiable QFF is satisfiable in an infinite model.

EUF and arithmetic are stably infinite.

Bit-vectors are not.

Microsoft Research

# Important Result

**The union of two consistent, disjoint, stably infinite theories is consistent.**

Microsoft Research

# Convexity

A theory T is convex iff

for all finite sets S of literals and

for all $a_1 = b_1 \vee \ldots \vee a_n = b_n$

S implies $a_1 = b_1 \vee \ldots \vee a_n = b_n$

iff

S implies $a_i = b_i$ for some $1 \leq i \leq n$

Microsoft Research

# Convexity: Results

Every convex theory with non trivial models is stably infinite.

All Horn equational theories are convex.

formulas of the form $s_1 \neq r_1 \vee \ldots \vee s_n \neq r_n \vee t = t'$

Linear rational arithmetic is convex.

# Convexity: Negative Results

Linear integer arithmetic is not convex

$1 \leq a \leq 2, b = 1, c = 2$ implies $a = b \vee a = c$

Nonlinear arithmetic

$a^2 = 1, b = 1, c = -1$ implies $a = b \vee a = c$

Theory of bit-vectors

Theory of arrays

$c_1 = \text{read}(\text{write}(a, i, c_2), j), c_3 = \text{read}(a, j)$

implies $c_1 = c_2 \vee c_1 = c_3$

Microsoft Research

# Combination of non-convex theories

EUF is convex (O(n log n))

IDL is non-convex (O(nm))

EUF $\cup$ IDL is NP-Complete

Reduce 3CNF to EUF $\cup$ IDL

For each boolean variable $p_i$ add $0 \leq a_i \leq 1$

For each clause $p_1 \vee \neg p_2 \vee p_3$ add

$f(a_1, a_2, a_3) \neq f(0, 1, 0)$

# Combination of non-convex theories

EUF is convex (O(n log n))

IDL is non-convex (O(nm))

EUF $\cup$ IDL is NP-Complete

Reduce 3CNF to EUF $\cup$ IDL

For each boolean variable $p_i$ add $0 \leq a_i \leq 1$

For each clause $p_1 \vee \neg p_2 \vee p_3$ add

$f(a_1, a_2, a_3) \neq f(0, 1, 0)$

implies

$a_1 \neq 0 \vee a_2 \neq 1 \vee a_3 \neq 0$

Microsoft Research

# Nelson-Oppen Combination

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be consistent, stably infinite theories over disjoint (countable) signatures. Assume satisfiability of conjunction of literals can decided in $O(T_1(n))$ and $O(T_2(n))$ time respectively. Then,

1. The combined theory $\mathcal{T}$ is consistent and stably infinite.
2. Satisfiability of quantifier free conjunction of literals in $\mathcal{T}$ can be decided in $O(2^{n^2} \times (T_1(n) + T_2(n))$.
3. If $\mathcal{T}_1$ and $\mathcal{T}_2$ are convex, then so is $\mathcal{T}$ and satisfiability in $\mathcal{T}$ is in $O(n^3 \times (T_1(n) + T_2(n)))$.

Microsoft Research

# Nelson-Oppen Combination

The combination procedure:

**Initial State:** $\phi$ is a conjunction of literals over $\Sigma_1 \cup \Sigma_2$.

**Purification:** Preserving satisfiability transform $\phi$ into $\phi_1 \wedge \phi_2$, such that, $\phi_i \in \Sigma_i$.

**Interaction:** Guess a partition of $\mathcal{V}(\phi_1) \cap \mathcal{V}(\phi_2)$ into disjoint subsets. Express it as conjunction of literals $\psi$.

Example. The partition $\{x_1\}, \{x_2, x_3\}, \{x_4\}$ is represented as $x_1 \neq x_2, x_1 \neq x_4, x_2 \neq x_4, x_2 = x_3$.

**Component Procedures** : Use individual procedures to decide whether $\phi_i \wedge \psi$ is satisfiable.

**Return:** If both return yes, return yes. No, otherwise.

# Soundness

Each step is satisfiability preserving.

Say $\phi$ is satisfiable (in the combination).

- Purification: $\phi_1 \wedge \phi_2$ is satisfiable.
- Iteration: for some partition $\psi$, $\phi_1 \wedge \phi_2 \wedge \psi$ is satisfiable.
- Component procedures: $\phi_1 \wedge \psi$ and $\phi_2 \wedge \psi$ are both satisfiable in component theories.
- Therefore, if the procedure return unsatisfiable, then $\phi$ is unsatisfiable.

# Completeness

Suppose the procedure returns satisfiable.

- Let $\psi$ be the partition and $A$ and $B$ be models of $\mathcal{T}_1 \wedge \phi_1 \wedge \psi$ and $\mathcal{T}_2 \wedge \phi_2 \wedge \psi$.
- The component theories are stably infinite. So, assume the models are infinite (of same cardinality).
- Let $h$ be a bijection between $|A|$ and $|B|$ such that $h(A(x)) = B(x)$ for each shared variable.
- Extend $B$ to $\bar{B}$ by interpretations of symbols in $\Sigma_1$:
  $\bar{B}(f)(b_1, \ldots, b_n) = h(A(f)(h^{-1}(b_1), \ldots, h^{-1}(b_n)))$
- $\bar{B}$ is a model of:
  $\mathcal{T}_1 \wedge \phi_1 \wedge \mathcal{T}_2 \wedge \phi_2 \wedge \psi$

# NO deterministic procedure (for convex theories)

Instead of guessing, we can deduce the equalities to be shared.

**Purification:** no changes.

**Interaction:** Deduce an equality $x = y$:

$$\mathcal{T}_1 \vdash (\phi_1 \Rightarrow x = y)$$

Update $\phi_2 := \phi_2 \wedge x = y$. And vice-versa. Repeat until no further changes.

**Component Procedures** : Use individual procedures to decide whether $\phi_i$ is satisfiable.

Remark: $\mathcal{T}_i \vdash (\phi_i \Rightarrow x = y)$ iff $\phi_i \wedge x \neq y$ is not satisfiable in $\mathcal{T}_i$.

# NO deterministic procedure Completeness

Assume the theories are convex.

- Suppose $\phi_i$ is satisfiable.
- Let $E$ be the set of equalities $x_j = x_k$ $(j \neq k)$ such that, $\mathcal{T}_i \nvdash \phi_i \Rightarrow x_j = x_k$.
- By convexity, $\mathcal{T}_i \nvdash \phi_i \Rightarrow \bigvee_E x_j = x_k$.
- $\phi_i \wedge \bigwedge_E x_j \neq x_k$ is satisfiable.
- The proof now is identical to the nondeterministic case.
- Sharing equalities is sufficient, because a theory $\mathcal{T}_1$ can assume that $x^B \neq y^B$ whenever $x = y$ is not implied by $\mathcal{T}_2$ and vice versa.

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

Arithmetic

$b + 2 = c,$

$v_1 \equiv 3,$

$v_3 \equiv c-2,$

$v_5 \equiv c-b+1$

Arrays

$v_2 \equiv write(a, b, v_1),$

$v_4 \equiv read(v_2, v_3)$

EUF

$v_6 \equiv f(v_4),$

$v_7 \equiv f(v_5),$

$v_6 \neq v_7$

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

**Arithmetic**

$b + 2 = \mathbf{c}$,

$v_1 \equiv 3$,

$v_3 \equiv c-2$,

$v_5 \equiv c-b+1$

**Arrays**

$v_2 \equiv write(a, b, v_1)$,

$v_4 \equiv read(v_2, v_3)$

**EUF**

$v_6 \equiv f(v_4)$,

$v_7 \equiv f(v_5)$,

$v_6 \neq v_7$

Substituting c

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

| Arithmetic | Arrays | EUF |
|---|---|---|
| $b + 2 = c,$ | $v_2 \equiv write(a, b, v_1),$ | $v_6 \equiv f(v_4),$ |
| $v_1 \equiv 3,$ | $v_4 \equiv read(v_2, v_3),$ | $v_7 \equiv f(v_5),$ |
| $\mathbf{v_3 \equiv b},$ | | $v_6 \neq v_7$ |
| $v_5 \equiv 3$ | | |

Propagating $v_3 = b$

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

**Arithmetic**

$b + 2 = c,$

$v_1 \equiv 3,$

$v_3 \equiv b,$

$v_5 \equiv 3$

**Arrays**

$\mathbf{v_2} \equiv write(a, \mathbf{b}, v_1),$

$v_4 \equiv read(\mathbf{v_2}, \mathbf{v_3}),$

$v_3 = b$

**EUF**

$v_6 \equiv f(v_4),$

$v_7 \equiv f(v_5),$

$v_6 \neq v_7,$

$v_3 = b$

Deducing $v_4 = v_1$

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

| Arithmetic | Arrays | EUF |
|---|---|---|
| $b + 2 = c,$ | $v_2 \equiv write(a, b, v_1),$ | $v_6 \equiv f(v_4),$ |
| $v_1 \equiv 3,$ | $v_4 \equiv read(v_2, v_3),$ | $v_7 \equiv f(v_5),$ |
| $v_3 \equiv b,$ | $v_3 = b,$ | $v_6 \neq v_7,$ |
| $v_5 \equiv 3$ | $\mathbf{v_4 = v_1}$ | $v_3 = b$ |

Propagating $v_4 = v_1$

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

| Arithmetic | Arrays | EUF |
|---|---|---|
| $b + 2 = c,$ | $v_2 \equiv write(a, b, v_1),$ | $v_6 \equiv f(v_4),$ |
| $\mathbf{v_1 \equiv 3},$ | $v_4 \equiv read(v_2, v_3),$ | $v_7 \equiv f(v_5),$ |
| $v_3 \equiv b,$ | $v_3 = b,$ | $v_6 \neq v_7,$ |
| $\mathbf{v_5 \equiv 3},$ | $v_4 = v_1$ | $v_3 = b,$ |
| $v_4 = v_1$ | | $v_4 = v_1$ |

Propagating $v_5 = v_1$

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

**Arithmetic**

$b + 2 = c,$

$v_1 \equiv 3,$

$v_3 \equiv b,$

$v_5 \equiv 3,$

$v_4 = v_1$

**Arrays**

$v_2 \equiv write(a, b, v_1),$

$v_4 \equiv read(v_2, v_3),$

$v_3 = b,$

$v_4 = v_1$

**EUF**

$v_6 \equiv f(\mathbf{v_4}),$

$v_7 \equiv f(\mathbf{v_5}),$

$v_6 \neq v_7,$

$v_3 = b,$

$\mathbf{v_4 = v_1},$

$\mathbf{v_5 = v_1}$

Congruence: $v_6 = v_7$

Microsoft Research

# NO procedure: Example

$b + 2 = c,\ f(read(write(a,b,3), c-2)) \neq f(c-b+1)$

Arithmetic

$b + 2 = c,$

$v_1 \equiv 3,$

$v_3 \equiv b,$

$v_5 \equiv 3,$

$v_4 = v_1$

Arrays

$v_2 \equiv write(a, b, v_1),$

$v_4 \equiv read(v_2, v_3),$

$v_3 = b,$

$v_4 = v_1$

EUF

$v_6 \equiv f(v_4),$

$v_7 \equiv f(v_5),$

$\mathbf{v_6 \neq v_7},$

$v_3 = b,$

$v_4 = v_1,$

$v_5 = v_1\ ,$

$\mathbf{v_6 = v_7}$

Unsatisfiable

Microsoft Research

# NO deterministic procedure

Deterministic procedure may fail for non-convex theories.

$0 \leq a \leq 1, 0 \leq b \leq 1, 0 \leq c \leq 1$,

$f(a) \neq f(b)$,

$f(a) \neq f(c)$,

$f(b) \neq f(c)$

Microsoft Research

# Combining Procedures in Practice

Propagate all implied equalities.

- Deterministic Nelson-Oppen.
- Complete only for convex theories.
- It may be expensive for some theories.

Delayed Theory Combination.

- Nondeterministic Nelson-Oppen.
- Create set of interface equalities ($x = y$) between shared variables.
- Use SAT solver to guess the partition.
- Disadvantage: the number of additional equality literals is quadratic in the number of shared variables.

Microsoft Research

# Combining Procedures in Practice

Common to these methods is that they are pessimistic about which equalities are propagated.

Model-based Theory Combination

- Optimistic approach.
- Use a candidate model $M_i$ for one of the theories $\mathcal{T}_i$ and propagate all equalities implied by the candidate model, hedging that other theories will agree.

  **if** $M_i \models \mathcal{T}_i \cup \Gamma_i \cup \{u = v\}$ **then** propagate $u = v$ .
- If not, use backtracking to fix the model.
- It is cheaper to enumerate equalities that are implied in a particular model than of all models.

Microsoft Research

# Example

$$x = f(y-1), f(x) \neq f(y), 0 \leq x \leq 1, 0 \leq y \leq 1$$

Purifying

Microsoft Research

# Example

$$x = f(z), f(x) \neq f(y), 0 \leq x \leq 1, 0 \leq y \leq 1, z = y - 1$$

Microsoft Research

# Example

| $\mathcal{T}_E$ | | | $\mathcal{T}_A$ | |
|---|---|---|---|---|
| *Literals* | *Eq. Classes* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $\{x, f(z)\}$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $\{y\}$ | $E(y) = *_2$ | $0 \leq y \leq 1$ | $A(y) = 0$ |
| | $\{z\}$ | $E(z) = *_3$ | $z = y - 1$ | $A(z) = -1$ |
| | $\{f(x)\}$ | $E(f) = \{*_1 \mapsto *_4,$ | | |
| | $\{f(y)\}$ | $*_2 \mapsto *_5,$ | | |
| | | $*_3 \mapsto *_1,$ | | |
| | | $\mathit{else} \mapsto *_6\}$ | | |

Assume x = y

# Example

| $\mathcal{T}_E$ | | | $\mathcal{T}_A$ | |
|---|---|---|---|---|
| *Literals* | *Eq. Classes* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $\{x, y, f(z)\}$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $\{z\}$ | $E(y) = *_1$ | $0 \leq y \leq 1$ | $A(y) = 0$ |
| $x = y$ | $\{f(x), f(y)\}$ | $E(z) = *_2$ | $z = y - 1$ | $A(z) = -1$ |
| | | $E(f) = \{*_1 \mapsto *_3,$ | $x = y$ | |
| | | $*_2 \mapsto *_1,$ | | |
| | | *else* $\mapsto *_4\}$ | | |

Unsatisfiable

# Example

| $\mathcal{T}_E$ | | | $\mathcal{T}_A$ | |
|---|---|---|---|---|
| *Literals* | *Eq. Classes* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $\{x, f(z)\}$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $\{y\}$ | $E(y) = *_2$ | $0 \leq y \leq 1$ | $A(y) = 0$ |
| $x \neq y$ | $\{z\}$ | $E(z) = *_3$ | $z = y - 1$ | $A(z) = -1$ |
| | $\{f(x)\}$ | $E(f) = \{*_1 \mapsto *_4,$ | $x \neq y$ | |
| | $\{f(y)\}$ | $*_2 \mapsto *_5,$ | | |
| | | $*_3 \mapsto *_1,$ | | |
| | | *else* $\mapsto *_6\}$ | | |

Backtrack, and assert $x \neq y$.

$\mathcal{T}_A$ model need to be fixed.

# Example

| $\mathcal{T}_E$ | | | $\mathcal{T}_A$ | |
|---|---|---|---|---|
| *Literals* | *Eq. Classes* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $\{x, f(z)\}$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $\{y\}$ | $E(y) = *_2$ | $0 \leq y \leq 1$ | $A(y) = 1$ |
| $x \neq y$ | $\{z\}$ | $E(z) = *_3$ | $z = y - 1$ | $A(z) = 0$ |
| | $\{f(x)\}$ | $E(f) = \{*_1 \mapsto *_4,$ | $x \neq y$ | |
| | $\{f(y)\}$ | $*_2 \mapsto *_5,$ | | |
| | | $*_3 \mapsto *_1,$ | | |
| | | $\mathit{else} \mapsto *_6\}$ | | |

Assume x = z

# Example

| $\mathcal{T}_E$ | | | $\mathcal{T}_A$ | |
|---|---|---|---|---|
| *Literals* | *Eq. Classes* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $\{x, z,$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $f(x), f(z)\}$ | $E(y) = *_2$ | $0 \leq y \leq 1$ | $A(y) = 1$ |
| $x \neq y$ | $\{y\}$ | $E(z) = *_1$ | $z = y - 1$ | $A(z) = 0$ |
| $x = z$ | $\{f(y)\}$ | $E(f) = \{*_1 \mapsto *_1,$ | $x \neq y$ | |
| | | $*_2 \mapsto *_3,$ | $x = z$ | |
| | | *else* $\mapsto *_4\}$ | | |

Satisfiable

# Example

| $\mathcal{T}_E$ | | | $\mathcal{T}_A$ | |
|---|---|---|---|---|
| *Literals* | *Eq. Classes* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $\{x, z,$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $f(x), f(z)\}$ | $E(y) = *_2$ | $0 \leq y \leq 1$ | $A(y) = 1$ |
| $x \neq y$ | $\{y\}$ | $E(z) = *_1$ | $z = y - 1$ | $A(z) = 0$ |
| $x = z$ | $\{f(y)\}$ | $E(f) = \{*_1 \mapsto *_1,$ | $x \neq y$ | |
| | | $*_2 \mapsto *_3,$ | $x = z$ | |
| | | *else* $\mapsto *_4\}$ | | |

Let $h$ be the bijection between $|E|$ and $|A|$.

$$h = \{*_1 \mapsto 0, *_2 \mapsto 1, *_3 \mapsto -1, *_4 \mapsto 2, \ldots\}$$

# Example

| $\mathcal{T}_E$ | | $\mathcal{T}_A$ | |
|---|---|---|---|
| *Literals* | *Model* | *Literals* | *Model* |
| $x = f(z)$ | $E(x) = *_1$ | $0 \leq x \leq 1$ | $A(x) = 0$ |
| $f(x) \neq f(y)$ | $E(y) = *_2$ | $0 \leq y \leq 1$ | $A(y) = 1$ |
| $x \neq y$ | $E(z) = *_1$ | $z = y - 1$ | $A(z) = 0$ |
| $x = z$ | $E(f) = \{*_1 \mapsto *_1,$ | $x \neq y$ | $A(f) = \{0 \mapsto 0$ |
| | $*_2 \mapsto *_3,$ | $x = z$ | $1 \mapsto -1$ |
| | *else* $\mapsto *_4\}$ | | *else* $\mapsto 2\}$ |

Extending $A$ using $h$.

$$h = \{*_1 \mapsto 0, *_2 \mapsto 1, *_3 \mapsto -1, *_4 \mapsto 2, \ldots\}$$

# Model Mutation

Sometimes $M(x) = M(y)$ by accident.

$$\bigwedge_{i=1}^{N} f(x_i) \geq 0 \ \wedge \ x_i \geq 0$$

Model mutation: diversify the current model.

# Freedom Intervals

Model mutation without pivoting

For each non basic variable $x_j$ compute $[L_j, U_j]$

Each row containing $x_j$ enforces a limit on how much it can be increase and/or decreased without violating the bounds of the basic variable in the row.

# Opportunistic Equality Propagation

We say a variable is fixed if the lower and upper bound are the same.

$1 \leq x \leq 1$

A polynomial P is fixed if all its variables are fixed.

Given a fixed polynomial P of the forma $2x_1 + x_2$,

we use M(P) to denote $2M(x_1) + M(x_2)$

# Opportunistic Equality Propagation

FixedEq

$$l_i \le x_i \le u_i,\ \ l_j \le x_j \le u_j \Longrightarrow\ \ x_i = x_j \ \textbf{if}\ \ l_i = u_i = l_j = u_j$$

EqRow

$$x_i = x_j + P \quad \Longrightarrow\ \ x_i = x_j \ \textbf{if}\ \ P \text{ is fixed, and } \mathsf{M}(P) = 0$$

EqOffsetRows

$$\left.\begin{aligned} x_i &= x_k + P_1 \\ x_j &= x_k + P_2 \end{aligned}\right\} \Longrightarrow\ \ x_i = x_j \ \textbf{if}\ \left\{\begin{array}{l} P_1 \text{ and } P_2 \text{ are fixed, and} \\ \mathsf{M}(P_1) = \mathsf{M}(P_2) \end{array}\right.$$

EqRows

$$\left.\begin{aligned} x_i &= P + P_1 \\ x_j &= P + P_2 \end{aligned}\right\} \Longrightarrow\ \ x_i = x_j \ \textbf{if}\ \left\{\begin{array}{l} P_1 \text{ and } P_2 \text{ are fixed, and} \\ \mathsf{M}(P_1) = \mathsf{M}(P_2) \end{array}\right.$$

# Non-stably infinite theories in practice

Bit-vector theory is not stably-infinite.

How can we support it?

Solution: add a predicate *is-bv*$(x)$ to the bit-vector theory (intuition: *is-bv*$(x)$ is true iff $x$ is a bitvector).

The result of the bit-vector operation *op*$(x, y)$ is not specified if $\neg$*is-bv*$(x)$ or $\neg$*is-bv*$(y)$.

The new bit-vector theory is stably-infinite.

# Reduction Functions

A reduction function reduces the satifiability problem for a complex theory into the satisfiability problem of a simpler theory.

Ackermannization is a reduction function.

# Reduction Functions

Theory of commutative functions.

- $\forall x, y. f(x, y) = f(y, x)$
- Reduction to EUF
- For every $f(a, b)$ in $\phi$, do $\phi := \phi \wedge f(a, b) = f(b, a)$.