Integrating Simplex with Tableaux

Guillaume Bury   David Delahaye

October 14, 2015

PPS, Université Paris Diderot

Cedric/Cnam/Inria, Paris, France

Introduction

Why linear arithmetic ?

- Used natively in programs
- Used in formalization of compiler optimizations
- Decidable

Loop Optimization

Simple loop

```
for (i=1;i<=10;i++)
  a[j+i]=a[j];
```

Optimized loop

```
tmp = a[j];
for (i=1;i<=10;i++)
  a[j+i]=tmp;
```

$$\vdash \forall i \in \mathbb{Z}, 1 \leq i \leq 10 \Rightarrow j \neq j + i$$

Goals

Prove two kinds of formulas:

- Universally quantified:
  $\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0$
- Existentially quantified: $\exists x \in \mathbb{Q}. x \geq 0 \land x \geq 42$

The Simplex Algorithm

General form

A linear system in general form has two types of constraints :

1. Equations of the form : $v = \sum_i a_i x_i$, $a_i \in \mathbb{Q}$
2. Bounds on variables : $l_i \leq v \leq u_i$, $l_i, u_i \in \mathbb{Q} \cup \{-\infty, +\infty\}$

General form

A linear system in general form has two types of constraints :

1. Equations of the form : $v = \sum_i a_i x_i$, $a_i \in \mathbb{Q}$
2. Bounds on variables : $l_i \leq v \leq u_i$, $l_i, u_i \in \mathbb{Q} \cup \{-\infty, +\infty\}$

The simplex returns:

- either a solution for the system
- or an unsatisfiability certificate

Unsatisfiability Explanation

An unsatisfiability certificate for a system S is a deducible linear expression $x = \sum_i a_i y_i$, that verifies:

- There exists b s.t. $x \geq b \in S$
- There exist l_i, u_i s.t. for all i:
  - if $a_i > 0$ then $y_i \leq u_i \in S$
  - if $a_i < 0$, then $y_i \geq l_i \in S$
- $\sum_{a_i>0} a_i u_i + \sum_{a_i<0} a_i l_i < b$

So that:

$$b \leq x = \sum_{a_i>0} a_i y_i + \sum_{a_i<0} a_i y_i \leq \sum_{a_i<0} a_i u_{y_i} + \sum_{a_i>0} a_i l_{y_i} < b$$

The Tableau Method

Closure and Analytical Rules

$$\odot_{\perp}\ \frac{\perp}{\odot} \qquad\qquad \odot\ \frac{P, \neg P}{\odot}$$

$$\alpha_{\wedge}\ \frac{P \wedge Q}{P, Q} \qquad\qquad \beta_{\vee}\ \frac{P \vee Q}{P \qquad Q}$$

Rules for quantifiers

$$\delta_{\exists}\ \frac{\exists x, P(x)}{P(\epsilon(x).P(x))} \qquad \delta_{\neg\forall}\ \frac{\neg\forall x, P(x)}{\neg P(\epsilon(x).\neg P(x))}$$

$$\gamma_{\forall}\ \frac{\forall x, P(x)}{P(X)} \qquad \gamma_{\neg\forall}\ \frac{\neg\exists x, P(x)}{\neg P(X)}$$

Proof example

$$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$$

$$\frac{\neg \exists y. \forall x. p(y) \Rightarrow p(x)}{\cdots}$$

Proof example

$$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$$

$$\dfrac{\dfrac{\neg \exists y. \forall x. p(y) \Rightarrow p(x)}{\neg \forall x. p(Y) \Rightarrow p(x)}\ \textsf{NotExists}}{\cdots}$$

Proof example

$$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$$

$$\dfrac{\dfrac{\dfrac{\neg\exists y.\forall x.p(y) \Rightarrow p(x)}{\neg\forall x.p(Y) \Rightarrow p(x)}\,\textsf{NotExists}}{\neg p(Y) \Rightarrow p(\epsilon_1)}\,\textsf{NotAll}}{\cdots}$$

Proof example

$$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$$

$$\textsf{NotExists}\ \dfrac{\neg\exists y.\forall x.p(y) \Rightarrow p(x)}{\textsf{NotAll}\ \dfrac{\neg\forall x.p(Y) \Rightarrow p(x)}{\textsf{NotImply}\ \dfrac{\neg p(Y) \Rightarrow p(\epsilon_1)}{\dfrac{p(Y), \neg p(\epsilon_1)}{\cdots}}}}$$

Proof example

$$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$$

$$
\begin{array}{rc}
 & \neg\exists y.\forall x.p(y) \Rightarrow p(x) \\ \hline
\text{NotExists} & \neg\forall x.p(Y) \Rightarrow p(x) \\ \hline
\text{NotAll} & \neg p(Y) \Rightarrow p(\epsilon_1) \\ \hline
\text{NotImply} & p(Y), \neg p(\epsilon_1) \\ \hline
\text{NotExists} & \neg\forall x.p(\epsilon_1) \Rightarrow p(x) \\ \hline
 & \cdots
\end{array}
$$

Proof example

$$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg \exists y. \forall x. p(y) \Rightarrow p(x)}{\neg \forall x. p(Y) \Rightarrow p(x)}\ \text{NotExists}}{\neg p(Y) \Rightarrow p(\epsilon_1)}\ \text{NotAll}}{p(Y), \neg p(\epsilon_1)}\ \text{NotImply}}{\neg \forall x. p(\epsilon_1) \Rightarrow p(x)}\ \text{NotExists}}{\neg p(\epsilon_1) \Rightarrow p(\epsilon_2)}\ \text{NotAll}}{\cdots}$$

Proof example

$\vdash \exists y, \forall x, p(y) \Rightarrow p(x)$

$$
\begin{array}{rc}
 & \neg\exists y.\forall x.p(y) \Rightarrow p(x) \\ \cline{2-2}
\text{NotExists} & \neg\forall x.p(Y) \Rightarrow p(x) \\ \cline{2-2}
\text{NotAll} & \neg p(Y) \Rightarrow p(\epsilon_1) \\ \cline{2-2}
\text{NotImply} & p(Y), \neg p(\epsilon_1) \\ \cline{2-2}
\text{NotExists} & \neg\forall x.p(\epsilon_1) \Rightarrow p(x) \\ \cline{2-2}
\text{NotAll} & \neg p(\epsilon_1) \Rightarrow p(\epsilon_2) \\ \cline{2-2}
\text{NotImply} & p(\epsilon_1), \neg p(\epsilon_2) \\ \cline{2-2}
\text{Axiom} & \odot
\end{array}
$$

Unsat Systems

Unsat Rules – Pre-processing

$$\text{Const}\ \frac{a \bowtie b}{\odot} \qquad \text{Const}\ \frac{a = b}{\odot}$$

$$\text{Eq}\ \frac{e = e'}{e \leq e', e' \leq e} \qquad \text{Neq}\ \frac{e \neq e'}{e < e' \qquad e > e'} \qquad \text{Neg}\ \frac{\neg e \bowtie e'}{e\ \overline{\bowtie}\ e'}$$

$$\text{Int-Lt}\ \frac{e < f}{e \leq f - 1} \qquad \text{Int-Gt}\ \frac{e > f}{e \geq f + 1}$$

$$\bowtie \in \{<, \leq, >, \geq\}$$

Unsat Rules – Simplex Explanations

$$\text{Var}\ \frac{e \bowtie c}{s = e, s \bowtie c}\ s \text{ fresh}$$

$$\text{Simplex-lin}\ \frac{e_1 = 0, \ldots, e_n = 0}{\sum_{i=1}^{n} a_i e_i = 0}\ \forall i, a_i \in \mathbb{Q}$$

$$\text{Leq}\ \frac{x_j \leq u_j | j \in N^+, x_j \geq l_j | j \in N^-, x = \sum_{j \in N^+ \cup N^-} a_j x_j}{x \leq \sum_{j \in N^+} a_j u_j + \sum_{j \in N^-} a_j l_j}\ \begin{array}{l} a_j > 0, j \in N^+ \\ a_j < 0, j \in N^- \end{array}$$

$$\text{Conflict}\ \frac{x \leq k, x \geq k'}{\odot}\ k < k' \text{ numeric constants}$$

Branch & Bound

- Run the simplex algorithm on S.
  - If the system is unsatisfiable, return UNSAT
  - If the system has a solution :
    - If a non-integer value v is assigned to a variable x, call the branch-and-bound twice, with the systems, $S \cup \{x \leq \lfloor v \rfloor\}$ and $S \cup \{x \geq \lfloor v \rfloor + 1\}$. If both are unsat, then return UNSAT
    - If all the variables have an integer assignment, return SAT

New inference rule :

$$\text{Branch}\ \frac{}{x \leq k \qquad x \geq k+1}\ k \in \mathbb{Z}$$

Example

$$\frac{\dfrac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \wedge u + 2v + w = 10 \Rightarrow w \neq 0}{\vdots}}{\cdots}$$

Example

$$\dfrac{\dfrac{\vdots}{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \wedge u + 2v + w = 10 \Rightarrow w \neq 0}}{}$$

$$\dfrac{\dfrac{\vdots}{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}\,\text{Eq}}{\cdots}$$

Example

$$\dfrac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0}{\dfrac{\vdots}{\text{Eq}\ \dfrac{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}{\text{Var}\ \dfrac{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}{\cdots}}}}$$

Example

$$\frac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0}{\begin{array}{c}\vdots \\ \text{Eq}\ \overline{\begin{array}{c} 2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10 \end{array}} \\ \text{Var}\ \overline{\begin{array}{c} a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10 \\ \text{Var}\ \overline{\begin{array}{c} b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10 \end{array}} \\ \hline \cdots \end{array}} \end{array}}$$

Example

$$
\begin{array}{rc}
 & \neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \wedge u + 2v + w = 10 \Rightarrow w \neq 0 \\ \cline{2-2}
 & \vdots \\ \cline{2-2}
\text{Eq} & 2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10 \\ \cline{2-2}
\text{Var} & \begin{array}{rc} & a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10 \\ \cline{2-2} \text{Var} & b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10 \end{array} \\ \cline{2-2}
\text{Eq} & \epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10 \\ \cline{2-2}
 & \cdots
\end{array}
$$

Example

$$
\begin{array}{c}
\neg \forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0 \\
\hline
\vdots \\
\text{Eq} \quad \overline{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10} \\
\text{Var} \quad \overline{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10} \\
\text{Var} \quad \overline{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10} \\
\text{Eq} \quad \overline{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10} \\
\text{Var} \quad \overline{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10} \\
\hline
\cdots
\end{array}
$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{2\epsilon_0 + \epsilon_1 + \epsilon_2 \le 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \ge 10}\,\text{Eq}}{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \le 10}\,\text{Var}}{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \ge 10}\,\text{Var}}{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \le 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \ge 10}\,\text{Eq}}{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \le 10}\,\text{Var}}{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \ge 10}\,\text{Var}}{\cdots}$$

$$\dfrac{\neg \forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0}{}$$

Example

$$
\begin{array}{rc}
 & \neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0 \\
\hline
 & \vdots \\
\text{Eq} & \\
\hline
 & 2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10 \\
\text{Var} & \\
\hline
 & a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10 \\
\text{Var} & \\
\hline
 & b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10 \\
\text{Eq} & \\
\hline
 & \epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10 \\
\text{Var} & \\
\hline
 & c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10 \\
\text{Var} & \\
\hline
 & d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10 \\
\text{Eq} & \\
\hline
 & \epsilon_2 \leq 0, \epsilon_2 \geq 0 \\
\hline
 & \cdots
\end{array}
$$

Rational Solution:

$$\epsilon_0 = \epsilon_1 = \frac{10}{3}, \epsilon_2 = 0$$

Example

$$
\begin{array}{rc}
 & \neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \wedge u + 2v + w = 10 \Rightarrow w \neq 0 \\
\hline
 & \vdots \\
\text{Eq} & \overline{} \\
 & 2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10 \\
\text{Var} & \overline{} \\
 & a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10 \\
\text{Var} & \overline{} \\
 & b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10 \\
\text{Eq} & \overline{} \\
 & \epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10 \\
\text{Var} & \overline{} \\
 & c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10 \\
\text{Var} & \overline{} \\
 & d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10 \\
\text{Eq} & \overline{} \\
 & \epsilon_2 \leq 0, \epsilon_2 \geq 0 \\
\text{Branch} & \overline{} \\
 & \dfrac{\epsilon_1 \leq 3}{\cdots} \qquad \dfrac{\epsilon_1 \geq 4}{\cdots}
\end{array}
$$

Example

$$
\begin{array}{rc}
 & \neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0 \\ \hline
 & \vdots \\ \hline
\text{Eq} & 2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10 \\ \hline
\text{Var} & a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10 \\ \hline
\text{Var} & b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10 \\ \hline
\text{Eq} & \epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10 \\ \hline
\text{Var} & c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10 \\ \hline
\text{Var} & d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10 \\ \hline
\text{Eq} & \epsilon_2 \leq 0, \epsilon_2 \geq 0 \\ \hline
\text{Branch} & \begin{array}{cc} \begin{array}{c} \epsilon_1 \leq 3 \\ \hline \text{Simplex-Lin} \quad a = 2d - 3\epsilon_1 - \epsilon_2 \\ \hline \cdots \end{array} & \begin{array}{c} \epsilon_1 \geq 4 \\ \hline \cdots \end{array} \end{array}
\end{array}
$$

Example

$$\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0$$

$$\vdots$$

$$\text{Eq}\quad 2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10$$

$$\text{Var}\quad a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10$$

$$\text{Var}\quad b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10$$

$$\text{Eq}\quad \epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10$$

$$\text{Var}\quad c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10$$

$$\text{Var}\quad d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10$$

$$\text{Eq}\quad \epsilon_2 \leq 0, \epsilon_2 \geq 0$$

$$\text{Branch}\quad \epsilon_1 \leq 3 \qquad\qquad \dfrac{\epsilon_1 \geq 4}{\cdots}$$

$$\text{Simplex-Lin}\quad a = 2d - 3\epsilon_1 - \epsilon_2$$

$$\text{Geq}\quad \dfrac{a \geq 11}{\cdots}$$

Example

$$\frac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0}{\vdots}$$

$$\text{Eq}\ \frac{\vdots}{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}$$

$$\text{Var}\ \frac{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}$$

$$\text{Var}\ \frac{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}$$

$$\text{Eq}\ \frac{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}$$

$$\text{Var}\ \frac{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10}$$

$$\text{Var}\ \frac{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10}{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10}$$

$$\text{Eq}\ \frac{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10}{\epsilon_2 \leq 0, \epsilon_2 \geq 0}$$

$$\text{Branch}\ \frac{\epsilon_2 \leq 0, \epsilon_2 \geq 0}{\epsilon_1 \leq 3 \qquad\qquad \epsilon_1 \geq 4}$$

$$\text{Simplex-Lin}\ \frac{\epsilon_1 \leq 3}{a = 2d - 3\epsilon_1 - \epsilon_2} \qquad \frac{\epsilon_1 \geq 4}{\cdots}$$

$$\text{Geq}\ \frac{a = 2d - 3\epsilon_1 - \epsilon_2}{a \geq 11}$$

$$\text{Conflict}\ \frac{a \geq 11}{\odot}$$

Example

$$
\dfrac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \wedge u + 2v + w = 10 \Rightarrow w \neq 0}{
\text{Eq}\;\dfrac{\vdots}{
\text{Var}\;\dfrac{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}{
\text{Var}\;\dfrac{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}{
\text{Eq}\;\dfrac{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}{
\text{Var}\;\dfrac{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}{
\text{Var}\;\dfrac{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10}{
\text{Eq}\;\dfrac{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10}{
\text{Branch}\;\dfrac{\epsilon_2 \leq 0, \epsilon_2 \geq 0}{
\text{Simplex-Lin}\;\dfrac{\epsilon_1 \leq 3}{\text{Geq}\;\dfrac{a = 2d - 3\epsilon_1 - \epsilon_2}{\text{Conflict}\;\dfrac{a \geq 11}{\odot}}}
\qquad
\text{Simplex-Lin}\;\dfrac{\epsilon_1 \geq 4}{\dfrac{c = \frac{1}{2}b + \frac{3}{2}\epsilon_1 + \frac{1}{2}\epsilon_2}{\cdots}}
}}}}}}}}}
$$

Example

$$\dfrac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \wedge u + 2v + w = 10 \Rightarrow w \neq 0}{\vdots}$$

$$\text{Eq}\ \dfrac{\vdots}{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}$$

$$\text{Var}\ \dfrac{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}$$

$$\text{Var}\ \dfrac{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}$$

$$\text{Eq}\ \dfrac{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}$$

$$\text{Var}\ \dfrac{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10}$$

$$\text{Var}\ \dfrac{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10}{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10}$$

$$\text{Eq}\ \dfrac{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10}{\epsilon_2 \leq 0, \epsilon_2 \geq 0}$$

$$\text{Branch}\ \dfrac{\epsilon_2 \leq 0, \epsilon_2 \geq 0}{\epsilon_1 \leq 3 \qquad\qquad \epsilon_1 \geq 4}$$

$$\text{Simplex-Lin}\ \dfrac{\epsilon_1 \leq 3}{a = 2d - 3\epsilon_1 - \epsilon_2} \qquad \text{Geq}\ \dfrac{a = 2d - 3\epsilon_1 - \epsilon_2}{a \geq 11} \qquad \text{Conflict}\ \dfrac{a \geq 11}{\odot}$$

$$\text{Simplex-Lin}\ \dfrac{\epsilon_1 \geq 4}{c = \frac{1}{2}b + \frac{3}{2}\epsilon_1 + \frac{1}{2}\epsilon_2} \qquad \text{Geq}\ \dfrac{c = \frac{1}{2}b + \frac{3}{2}\epsilon_1 + \frac{1}{2}\epsilon_2}{c \geq 11} \qquad \dfrac{c \geq 11}{\cdots}$$

Example

$$\frac{\neg\forall uvw \in \mathbb{Z}, 2u + v + w = 10 \land u + 2v + w = 10 \Rightarrow w \neq 0}{\vdots}$$

$$\text{Eq}\ \frac{\vdots}{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}$$

$$\text{Var}\ \frac{2\epsilon_0 + \epsilon_1 + \epsilon_2 \leq 10, 2\epsilon_0 + \epsilon_1 + \epsilon_2 \geq 10}{\text{Var}\ \dfrac{a = 2\epsilon_0 + \epsilon_1 + \epsilon_2, a \leq 10}{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}}$$

$$\text{Eq}\ \frac{b = 2\epsilon_0 + \epsilon_1 + \epsilon_2, b \geq 10}{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}$$

$$\text{Var}\ \frac{\epsilon_0 + 2\epsilon_1 + \epsilon_2 \leq 10, \epsilon_0 + 2\epsilon_1 + \epsilon_2 \geq 10}{\text{Var}\ \dfrac{c = \epsilon_0 + 2\epsilon_1 + \epsilon_2, c \leq 10}{\text{Eq}\ \dfrac{d = \epsilon_0 + 2\epsilon_1 + \epsilon_2, d \geq 10}{\epsilon_2 \leq 0, \epsilon_2 \geq 0}}}$$

$$\text{Branch}\ \frac{\epsilon_2 \leq 0, \epsilon_2 \geq 0}{\text{Simplex-Lin}\ \dfrac{\epsilon_1 \leq 3}{\text{Geq}\ \dfrac{a = 2d - 3\epsilon_1 - \epsilon_2}{\text{Conflict}\ \dfrac{a \geq 11}{\odot}}} \qquad \text{Simplex-Lin}\ \dfrac{\epsilon_1 \geq 4}{\text{Geq}\ \dfrac{c = \frac{1}{2}b + \frac{3}{2}\epsilon_1 + \frac{1}{2}\epsilon_2}{\text{Conflict}\ \dfrac{c \geq 11}{\odot}}}}$$

Finding Instantiations

Problem with Instantiation

$\vdash \exists x \in \mathbb{N}, x \geq 0 \wedge x \geq 42$

$$
\gamma_{\neg\exists M}\,\dfrac{\neg\exists x \in \mathbb{N}, x \geq 0 \wedge x \geq 42}{\beta_{\neg\wedge}\,\dfrac{\neg(X \geq 0 \wedge X \geq 42)}{\text{Neg }(\geq)\,\dfrac{\neg X \geq 0}{\text{Int-Lt}\,\dfrac{X < 0}{\dfrac{X \leq -1}{}}} \qquad \dfrac{\neg X \geq 42}{\cdots}}}
$$

Problem with Instantiation

$\vdash \exists x \in \mathbb{N}, x \geq 0 \land x \geq 42$

$$
\gamma_{\neg\exists M}\ \dfrac{\neg\exists x \in \mathbb{N}, x \geq 0 \land x \geq 42}{\beta_{\neg\land}\ \dfrac{\neg(X \geq 0 \land X \geq 42)}{\text{Neg } (\geq)\ \dfrac{\neg X \geq 0}{\text{Int-Lt}\ \dfrac{X < 0}{\gamma_{\neg\exists\text{Inst}}\ \dfrac{X \leq -1}{\neg(0 \geq 0 \land 0 \geq 42)}}} \qquad \dfrac{\neg X \geq 42}{\cdots}}}
$$

Problem with Instantiation

$\vdash \exists x \in \mathbb{N}, x \geq 0 \land x \geq 42$

$$\gamma_{\neg\exists M}\ \dfrac{\neg\exists x \in \mathbb{N}, x \geq 0 \land x \geq 42}{\beta_{\neg\land}\ \dfrac{\neg(X \geq 0 \land X \geq 42)}{\text{Neg }(\geq)\ \dfrac{\neg X \geq 0}{\text{Int-Lt}\ \dfrac{X < 0}{\gamma_{\neg\exists\text{Inst}}\ \dfrac{X \leq -1}{\beta_{\neg\land}\ \dfrac{\neg(0 \geq 0 \land 0 \geq 42)}{\text{Neg }(\geq)\ \dfrac{\neg 0 \geq 0}{\text{Int-Lt}\ \dfrac{0 < 0}{\text{Const}\ \dfrac{0 \leq -1}{\odot}}} \quad \text{Neg }(\geq)\ \dfrac{\neg 0 \geq 42}{\text{Int-Lt}\ \dfrac{0 < 42}{\dfrac{0 \leq 41}{\cdots}}}}}}} \quad \dfrac{\neg X \geq 42}{\cdots}}}$$

Closing multiples branches

Idea: Close all open branches simultaneously

$$\dfrac{\dfrac{\vdots}{\varphi(1,1),\cdots,\varphi(1,m_1)} \qquad \dfrac{\vdots}{\cdots} \qquad \dfrac{\vdots}{\varphi(n,1),\cdots,\varphi(n,m_n)}}{\Phi}$$

Closing multiples branches

Idea: Close all open branches simultaneously

$$\dfrac{\Phi}{\dfrac{\vdots}{\varphi_{(1,1)}, \cdots, \varphi_{(1,m_1)}} \quad \dfrac{\vdots}{\cdots} \quad \dfrac{\vdots}{\varphi_{(n,1)}, \cdots, \varphi_{(n,m_n)}}}$$

Satisfy a set E such that:

$$\forall i \in \{1, \ldots, n\}, \exists j \in \{1, \ldots, m_i\}, \neg\varphi_{(i,j)} \in E$$

Instantiation – Example

$$\vdash \exists x \in \mathbb{Z}, (x \geq 0 \vee x \geq 1) \wedge (x \leq -1 \vee (x \geq -5 \wedge x \leq 0))$$

$$\vdash \exists x \in \mathbb{Z}, (x \geq 0 \vee x \geq 1) \wedge (x \leq -1 \vee (x \geq -5 \wedge x \leq 0))$$

$$\dfrac{\neg \exists x \in \mathbb{Z}, (x \geq 0 \vee x \geq 1) \wedge (x \leq -1 \vee (x \geq -5 \wedge x \leq 0))}{\dfrac{\neg\left((X \geq 0 \vee X \geq 1) \wedge (X \leq -1 \vee (X \geq -5 \wedge X \leq 0))\right)}{\begin{array}{cc} \dfrac{\neg\left((X \geq 0 \vee X \geq 1)\right)}{\dfrac{\neg(X \geq 0), \neg(X \geq 1)}{\dfrac{X < 0}{\dfrac{X \leq -1 \ *}{\dfrac{X < 1}{X \leq 0 \ *}}}}} & \dfrac{\neg\left((X \leq -1 \vee (X \geq -5 \wedge X \leq 0))\right)}{\dfrac{\neg(X \leq -1), \neg(X \geq -5 \wedge X \leq 0)}{\dfrac{X > -1}{\dfrac{X \geq 0 \ *}{\begin{array}{cc} \dfrac{\neg(X \geq -5)}{\dfrac{X < -5}{X \leq -6 \ *}} & \dfrac{\neg(X \leq 0)}{\dfrac{X > 0}{X \geq 1 \ *}} \end{array}}}}} \end{array}}}$$

Instantiation – Example

- $[]$
  - $[X \leq -1^\dagger; X \leq 0]$
  - $[X \geq 0]$
    - $[X \leq -6^\dagger]$
    - $[X \geq 1^\dagger]$

Instantiation – Example

- $[]$
  - $[X \leq -1^{\dagger}; X \leq 0]$
  - $[X \geq 0]$
    - $[X \leq -6^{\dagger}]$
    - $[X \geq 1^{\dagger}]$

$$\neg \begin{cases} X \leq -1 \\ X \leq -6 \\ X \geq 1 \end{cases} \quad \rightarrow \quad \begin{cases} X \geq 0 \\ X \geq -5 \\ X \leq 0 \end{cases}$$

Instantiation – Example

$[]$

$[X \leq -1^{\dagger}; X \leq 0]$ $\quad$ $[X \geq 0]$

$[X \leq -6^{\dagger}]$ $\quad$ $[X \geq 1^{\dagger}]$

$$\neg \begin{cases} X \leq -1 \\ X \leq -6 \\ X \geq 1 \end{cases} \quad \rightarrow \quad \begin{cases} X \geq 0 \\ X \geq -5 \\ X \leq 0 \end{cases}$$

Counter-example: $X \mapsto 0$

$$
\dfrac{\neg\exists x \in \mathbb{Z}, (x \geq 0 \vee x \geq 1) \wedge (x \leq -1 \vee (x \geq -5 \wedge x \leq 0))}{\dfrac{\neg\left((0 \geq 0 \vee 0 \geq 1) \wedge (0 \leq -1 \vee (0 \geq -5 \wedge 0 \leq 0))\right)}{\begin{array}{cc} \dfrac{\neg\left((0 \geq 0 \vee 0 \geq 1)\right)}{\dfrac{\neg (0 \geq 0), \neg (0 \geq 1)}{\dfrac{0 < 0}{\odot}}} & \dfrac{\neg\left((0 \leq -1 \vee (0 \geq -5 \wedge 0 \leq 0))\right)}{\dfrac{\neg (0 \leq -1), \neg (0 \geq -5 \wedge 0 \leq 0)}{\begin{array}{cc} \dfrac{\neg(0 \geq -5)}{\dfrac{0 < -5}{\odot}} & \dfrac{\neg(0 \leq 0)}{\dfrac{0 > 0}{\odot}} \end{array}}} \end{array}}}
$$

Benchmarks

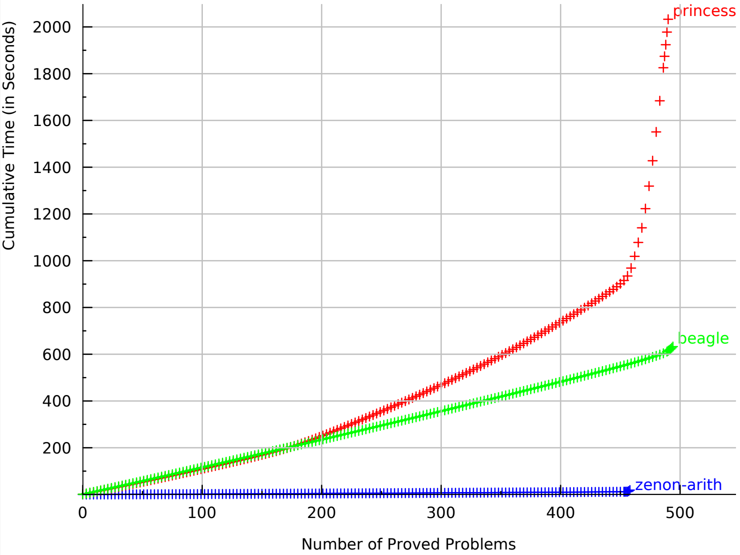
TPTP: ARI section

Prover	Problems solved	%	Avg Time (1)	Avg Time (2)
Zenon (arith.)	459	92%	0.05 s	0.05 s
Princess	491	98%	4.34 s	4.52 s
Beagle	495	99%	1.37 s	1.32 s

- (1) Average time on all 500 problems
- (2) Average time on the 453 problems solved by all provers

Zenon outputs Coq proof certificates for all solved problems.

Cumulative times



CASC 25 - Results

TFA using Integers	VampireZ 1.0	CVC4 TFA-1.5	Vampire 4.0	Beagle 0.9.22	SPASS+T 2.2.22	ZenonArith 0.1.0	Princess 20150706	CVC4 1.4-TFF
Solved/150	126/150	116/150	114/150	81/150	60/150	12/150	100/150	84/150
Av. CPU Time	16.04	24.27	15.09	34.69	17.19	14.23	22.18	16.64
Solutions	126/150	116/150	114/150	81/150	60/150	12/150	0/150	0/150
µEfficiency	354	253	257	100	88	55	106	213
SOTAC	0.24	0.24	0.23	0.18	0.16	0.17	0.20	0.20
Core Usage	0.93	0.95	0.93	1.24	1.13	0.93	1.63	0.93
New Solved	4/5	3/5	4/5	0/5	2/5	2/5	0/5	4/5

TFA using Rationals	CVC4 TFA-1.5	ZenonArith 0.1.0	Beagle 0.9.22	SPASS+T 2.2.22	Vampire 4.0	VampireZ 1.0	CVC4 1.4-TFF	Princess 20150706
Solved/35	35/35	35/35	35/35	35/35	34/35	34/35	35/35	33/35
Av. CPU Time	0.00	0.01	0.64	1.11	0.00	0.27	0.00	5.61
Solutions	35/35	35/35	35/35	35/35	34/35	34/35	0/35	0/35
µEfficiency	1000	1000	834	500	971	914	1000	315
SOTAC	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.13
Core Usage	0.00	0.01	0.29	0.45	0.00	0.19	0.00	1.18
New Solved	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0

TFA using Reals	Beagle 0.9.22	ZenonArith 0.1.0	SPASS+T 2.2.22	CVC4 TFA-1.5	Vampire 4.0	VampireZ 1.0	CVC4 1.4-TFF	Princess 20150706
Solved/15	15/15	13/15	13/15	12/15	12/15	12/15	12/15	10/15
Av. CPU Time	1.20	0.02	1.12	0.00	0.00	0.66	0.00	8.21
Solutions	15/15	13/15	13/15	12/15	12/15	12/15	0/15	0/15
µEfficiency	723	867	433	800	800	700	800	237
SOTAC	0.25	0.14	0.14	0.13	0.13	0.13	0.13	0.13
Core Usage	0.50	0.02	0.42	0.00	0.00	0.37	0.00	1.41
New Solved	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0

Conclusion

Results

- Inference rules for integer/rational/real arithmetic
- Proof search algorithm
- Implementation as a Zenon extension
- Backend to output Coq proof certificates

Perspectives

- Simplex optimizations (Gomory's cuts)
- Mixed problems (integer/rationals)
- Alternation of quantifiers
- Non-linear arithmetic
- Better support for uninterpreted functions and predicates

Questions ?

Definition: Covering Tree

Given a tree $\mathcal{T}$ labelled with set of formulas, and a set of formula $\mathcal{E}$, the set of nodes of $\mathcal{T}$ covered by $\mathcal{E}$ is the least set of nodes n such that :

- Either $\mathrm{label}(n) \cap \mathcal{E} \neq \emptyset$ (we say the node is directly covered)
- Or all children of n are covered by $\mathcal{E}$

$\mathcal{E}$ covers $\mathcal{T}$ iff it covers the root of $\mathcal{T}$.

Enumeration of covering sets

A sufficient set of covering sets for a tree $\mathcal{T}$ can be enumerated:

$$\text{cover}(\mathcal{T}) = \{\{f\} \mid f \in \text{label}(\mathcal{T})\} \cup \{\bigcup_{1 \leq i \leq n} s_i \mid s_i \in \text{cover}(\mathcal{T}[i])\}$$

with

- label($\mathcal{T}$) the label of the root of $\mathcal{T}$
- $\mathcal{T}[i]$ the *i*-th children of the root of $\mathcal{T}$.