Deciding Presburger Arithmetic using reflection

M1 internship under T. Altenkirch's supervision

G. Allais

Univ. of Nottingham

July 21st, 2010

Definitions

$$e \quad ::= \quad k | x | k * e | e + e$$

$$\begin{aligned} f \quad ::= \quad & \top | \bot | f \wedge f | f \vee f | \forall . f | \exists . f | \neg f | f \rightarrow f | \\ & e = e | e < e | e \leq e | e > e | e \geq e | k \ div \ e \end{aligned}$$

Key dates

- 1929: Presburger introduces his arithmetic without multiplication
  - Coherent
  - Decidable

Key dates

- 1929: Presburger introduces his arithmetic without multiplication
  - Coherent
  - Decidable
- 1972: Cooper's theorem proving for arithmetic without multiplication
  - Decision procedure
  - Quantifier elimination

Key dates

- 1929: Presburger introduces his arithmetic without multiplication
  - Coherent
  - Decidable
- 1972: Cooper's theorem proving for arithmetic without multiplication
  - Decision procedure
  - Quantifier elimination
- 1974: Fischer & Rabin's super-exponential complexity of PA

Key dates

- 1929: Presburger introduces his arithmetic without multiplication
  - Coherent
  - Decidable
- 1972: Cooper's theorem proving for arithmetic without multiplication
  - Decision procedure
  - Quantifier elimination
- 1974: Fischer & Rabin's super-exponential complexity of PA
- 2001: CALIFE: ROmega (Universally quantified PA formulas)

Key dates

- 1929: Presburger introduces his arithmetic without multiplication
  - Coherent
  - Decidable
- 1972: Cooper's theorem proving for arithmetic without multiplication
  - Decision procedure
  - Quantifier elimination
- 1974: Fischer & Rabin's super-exponential complexity of PA
- 2001: CALIFE: ROmega (Universally quantified PA formulas)
- 2005–08: Nipkow's quantifier elimination for PA (HOL)

What is obviously decidable?

- Equality on $\mathbb{Z}$
- Canonical order on $\mathbb{Z}$
- Divisibility

In other words: every variable-free formula is decidable.

What is obviously decidable?

- Equality on $\mathbb{Z}$
- Canonical order on $\mathbb{Z}$
- Divisibility

In other words: every variable-free formula is decidable.

$\Rightarrow$ **We want a quantifier elimination procedure**

How?

1. Normalisation of the input formula
2. Generation of an "elimination set"
3. Quantifier elimination theorem

Example

$$\forall x_1, \forall x_0, 3 + 6 * x_1 = 2 * x_0$$
$$\wedge \neg (4 * x_1 + 7 > 0 \vee 5 * x_0 \neq 25 + 12 * x_1)$$

N-step

Negation normal form:

- Pushing negation inwards
- Using De Morgan's laws
- Negations only in front of equalities & divisibility statements

Few other simplifications:

- Using only $\leq$
- Elimination of implications

N-step

Negation normal form:

- Pushing negation inwards
- Using De Morgan's laws
- Negations only in front of equalities & divisibility statements

Example

$$3 + 6 * x_1 = 2 * x_0 \wedge \neg(4 * x_1 + 7 > 0 \vee 5 * x_0 \neq 25 + 12 * x_1)$$

$$\downarrow$$

$$3 + 6 * x_1 = 2 * x_0 \wedge (4 * x_1 + 7 \leq 0 \wedge 5 * x_0 = 25 + 12 * x_1)$$

L-step

Linearisation of the expression:

- Structural recursion
- Merge

Properties:

- Factorisation
- Nonzero coefficients
- Variables sorted
- Expressions' representation's uniqueness

L-step

Properties:

- Factorisation
- Nonzero coefficients
- Variables sorted
- Expressions' representation's uniqueness

Example

$$3 + 6 * x_1 = 2 * x_0 \wedge (4 * x_1 + 7 \leq 0 \wedge 5 * x_0 = 25 + 12 * x_1)$$

$$\downarrow$$

$$-2 * x_0 + 6 * x_1 + 3 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 5 * x_0 - 12 * x_1 - 25 = 0)$$

U-step

- Compute lcm_Φ
- Normalize x_0's coefficients

U-step

- Compute lcm_Φ
- Normalize x_0's coefficients

Example: $lcm_\Phi = 10$

$$-2 * x_0 + 6 * x_1 + 3 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 5 * x_0 - 12 * x_1 - 25 = 0)$$

$$\downarrow$$

$$-10 * x_0 + 30 * x_1 + 15 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 10 * x_0 - 24 * x_1 - 50 = 0)$$

U-step

- Compute lcm_Φ
- Normalize x_0's coefficients

Example: $lcm_\Phi = 10$

$$-10 * x_0 + 30 * x_1 + 15 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 10 * x_0 - 24 * x_1 - 50 = 0)$$

$$\downarrow$$

$$-1 * x_0 + 30 * x_1 + 15 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 1 * x_0 - 24 * x_1 - 50 = 0)$$

U-step

- Compute lcm_Φ
- Normalize x_0's coefficients

A kind of equivalence

$$\exists x, P(k * x) \Leftrightarrow \exists x.(k \ div \ x \wedge P(x))$$

A few remarks

1. Equivalent statement when $x_0 \to -\infty$ is simpler ($P_{-\infty}$)
2. Set of remarkable values (**B-set**)
3. Some kind of periodicity

A few remarks

1. Equivalent statement when $x_0 \to -\infty$ is simpler ($P_{-\infty}$)

$$
\begin{array}{rlcl}
x_0 & +r \leq 0 & \Leftrightarrow & \top \\
-x_0 & +r \leq 0 & \Leftrightarrow & \bot \\
k * x_0 & +r = 0 & \Leftrightarrow & \bot \\
k * x_0 & +r \neq 0 & \Leftrightarrow & \top
\end{array}
$$

2. Set of remarkable values (**B-set**)
3. Some kind of periodicity

A few remarks

1. Equivalent statement when $x_0 \to -\infty$ is simpler ($P_{-\infty}$)

Example

$$-1 * x_0 + 30 * x_1 + 15 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 1 * x_0 - 24 * x_1 - 50 = 0)$$

$$\downarrow$$

$$\bot \wedge (4 * x_1 + 7 \leq 0 \wedge \bot)$$

2. Set of remarkable values (**B-set**)
3. Some kind of periodicity

A few remarks

1. Equivalent statement when $x_0 \to -\infty$ is simpler ($P_{-\infty}$)
2. Set of remarkable values (**B-set**)

   Values such that if $\Phi(x)$ is provable $\Phi(x - lcm_{dvd}(\Phi))$ might not be.

$$\begin{array}{rlcl} -x_0 & +r \leq 0 & \Rightarrow & \{r-1\} \\ x_0 & +r = 0 & \Rightarrow & \{-r-1\} \\ -x_0 & +r = 0 & \Rightarrow & \{r-1\} \\ k * x_0 & +r \neq 0 & \Rightarrow & \{-k*r\} \end{array}$$

3. Some kind of periodicity

A few remarks

1. Equivalent statement when $x_0 \to -\infty$ is simpler ($P_{-\infty}$)
2. Set of remarkable values (**B-set**)

Example

$$-1 * x_0 + 30 * x_1 + 15 = 0 \wedge (4 * x_1 + 7 \leq 0 \wedge 1 * x_0 - 24 * x_1 - 50 = 0)$$

$$\downarrow$$

$$B = \{30 * x_1 + 14, 24 * x_1 + 49\}$$

3. Some kind of periodicity

A few remarks

1. Equivalent statement when $x_0 \to -\infty$ is simpler ($P_{-\infty}$)
2. Set of remarkable values (**B-set**)
3. Some kind of periodicity

- If $P(x)$ and $\neg(\exists b \in B, \exists j \in [|0; lcm_{dvd}(P)|], P(b+j))$ then $P(x - lcm_{dvd}(P))$
- $\exists x, P_{-\infty}(x) \Leftrightarrow \exists x, P_{-\infty}(x + k * lcm_{dvd}(P_{-\infty}))$

Cooper's theorem

$$\exists x, P(x)$$

$$\Updownarrow$$

$$\exists b \in B, \exists j \in [|0; lcm_{dvd}|], P(b+j)$$

$$\vee$$

$$\exists j \in [|0; lcm_{dvd} - 1|], P_{-\infty}(j)$$

Motivations

Why reflection?

1. Bug-free
   - complete
   - correct
2. Properties of programs
3. Nice separations:
   - syntactic vs. semantic
   - computations vs. proofs

Datastructures

- Expressions
- Formulas
- Properties
- Formulas subsets

Expressions

```
data exp (n : ℕ) : Set where
 val : ℤ → exp n
 var : Fin n → exp n
 :-_ : exp n → exp n
 _:+_ _:-_ : exp n → exp n → exp n
 _:*_ : ℤ → exp n → exp n
```

Formulas

```
data form : ℕ → Set where
 T F : ∀ {n} → form n
 _dvd_ : ∀ {n} → ℤ → exp n → form n
 _lt_ _gt_ _le_ _ge_ _eq_ : ∀ {n} → exp n →
                            exp n → form n
 not_ : ∀ {n} → form n → form n
 ex_ all_ : ∀ {n : ℕ} → form (suc n) → form n
 _and_ _or_ _→_ : ∀ {n} → form n → form n → form n
```