European Research Council
Established by the European Commission

logics LOGICAL METHODS IN COMPUTER SCIENCE

Program Synthesis in Saturation

Petra Hozzová[1]
joint work with Laura Kovács[1], Chase Norman[2] and Andrei Voronkov[3]

[1] TU Wien
[2] UC Berkeley
[3] University of Manchester and EasyChair

The main idea

Synthesize a program computing $\overline{y}$ for any $\overline{x}$ such that $F(\overline{x}, \overline{y})$ holds using a saturation-based prover proving $\forall \overline{x}. \exists \overline{y}. F(\overline{x}, \overline{y})$.

The main idea

first-order formula

Synthesize a program computing $\overline{y}$ for any $\overline{x}$ such that $F(\overline{x}, \overline{y})$ holds

using a saturation-based prover proving $\forall\overline{x}.\exists\overline{y}.F(\overline{x}, \overline{y})$.

The main idea

term, possibly using `if−then−else`,
and only containing computable symbols

first-order formula

Synthesize a program computing $\overline{y}$ for any $\overline{x}$ such that $F(\overline{x}, \overline{y})$ holds

using a saturation-based prover proving $\forall \overline{x}. \exists \overline{y}. F(\overline{x}, \overline{y})$.

The main idea

term, possibly using $\texttt{if}-\texttt{then}-\texttt{else}$,
and only containing computable symbols

first-order formula

Synthesize a program computing $\overline{y}$ for any $\overline{x}$ such that $F(\overline{x}, \overline{y})$ holds

using a saturation-based prover proving $\forall\overline{x}.\exists\overline{y}.F(\overline{x}, \overline{y})$.

using answer literals,
supporting derivation of clauses $C \vee \texttt{ans}(r)$ where C is computable,
expressing "if $\neg C$, then r is the program"

Background: Saturation algorithm

Proving $A_1 \wedge \cdots \wedge A_n \rightarrow \forall \overline{x}.\exists \overline{y}.F(\overline{x}, \overline{y})$ by refutation using a saturation algorithm:

1. Create the set of formulas $\mathcal{S} = \{A_1, \ldots, A_n, \neg\forall \overline{x}.\exists \overline{y}.F(\overline{x}, \overline{y})\}$

Background: Saturation algorithm

Proving $A_1 \wedge \cdots \wedge A_n \rightarrow \forall \overline{x}. \exists \overline{y}. F(\overline{x}, \overline{y})$ by refutation using a saturation algorithm:

1. Create the set of formulas $\mathcal{S} = \{A_1, \ldots, A_n, \forall \overline{y}. CNF(\neg F(\overline{\sigma}, \overline{y}))\}$

Background: Saturation algorithm

Proving $A_1 \wedge \cdots \wedge A_n \rightarrow \forall \overline{x}.\exists \overline{y}.F(\overline{x}, \overline{y})$ by refutation using a saturation algorithm:

1. Create the set of formulas $\mathcal{S} = \{A_1, \ldots, A_n, \forall \overline{y}.CNF(\neg F(\overline{\sigma}, \overline{y}))\}$
2. Repeat:
   2.1 Choose $C \in \mathcal{S}$
   2.2 Apply rules to derive consequences $C_1, \ldots, C_n$ of C and clauses from $\mathcal{S}$
   2.3 Add $C_1, \ldots, C_n$ to $\mathcal{S}$
   2.4 If $\mathcal{S}$ contains $\square$, return TRUE (proved)

Background: Saturation algorithm

Proving $A_1 \wedge \cdots \wedge A_n \rightarrow \forall \overline{x}.\exists \overline{y}.F(\overline{x}, \overline{y})$ by refutation using a saturation algorithm:

1. Create the set of formulas $\mathcal{S} = \{A_1, \ldots, A_n, \forall \overline{y}.CNF(\neg F(\overline{\sigma}, \overline{y}))\}$
2. Repeat:
   2.1 Choose $C \in \mathcal{S}$
   2.2 Apply rules to derive consequences $C_1, \ldots, C_n$ of C and clauses from $\mathcal{S}$
   2.3 Add $C_1, \ldots, C_n$ to $\mathcal{S}$
   2.4 If $\mathcal{S}$ contains $\square$, return TRUE (proved)

Depending on the calculus, termination might imply that the original formula is not valid.
In practice, termination is rare.

Background: Saturation algorithm

Proving $A_1 \wedge \cdots \wedge A_n \rightarrow \forall \overline{x}. \exists \overline{y}. F(\overline{x}, \overline{y})$ by refutation using a saturation algorithm:

1. Create the set of formulas $\mathcal{S} = \{A_1, \ldots, A_n, \forall \overline{y}. CNF(\neg F(\overline{\sigma}, \overline{y}))\}$
2. Repeat:
    - 2.1 Choose $C \in \mathcal{S}$
    - 2.2 Apply rules to derive consequences $C_1, \ldots, C_n$ of C and clauses from $\mathcal{S}$
    - 2.3 Add $C_1, \ldots, C_n$ to $\mathcal{S}$
    - 2.4 If $\mathcal{S}$ contains $\square$, return TRUE (proved)

Depending on the calculus, termination might imply that the original formula is not valid.
In practice, termination is rare.

```
% Refutation found. Thanks to Tanya!
 1. ![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 | X1 = X2)) [input]
 2. ~![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 |
                                                                   X1 = X2)) [negated conjecture 1]
 3. ~![X1:$int,X0:$int]:?[X2:$int]:(~$less(X2,X0) & ~$less(X2,X1) & (X0 = X2 | X1 = X2)) [theory
                                                                                  normalization 2]
 9. ~$less(X0,X0) [theory axiom 144]
10. ~$less(X1,X2) | ~$less(X0,X1) | $less(X0,X2) [theory axiom 145]
16. ~![X0 :  $int,X1 :  $int] :  ?[X2 :  $int] :  (~$less(X2,X1) & ~$less(X2,X0) & (X1 = X2 | X0 = X2))
                                                                                        [rectify 3]
17. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
                                                                            [ennf transformation 16]
18. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
         => !  [X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [choice axiom]
19. ![X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [skolemisation 17,18]
20. $less(X2,sK1) | $less(X2,sK0) | sK0 != X2 [cnf transformation 19]
21. $less(X2,sK1) | $less(X2,sK0) | sK1 != X2 [cnf transformation 19]
22. $less(sK1,sK1) | $less(sK1,sK0) [equality resolution 21]
23. $less(sK0,sK1) | $less(sK0,sK0) [equality resolution 20]
24. $less(sK1,sK0) [subsumption resolution 22,9]
25. $less(sK0,sK1) [subsumption resolution 23,9]
66. ~$less(X0,sK1) | $less(X0,sK0) [resolution 10,24]
71. $less(sK0,sK0) [resolution 66,25]
72. $false [subsumption resolution 71,9]
```

```
% Refutation found.  Thanks to Tanya!
 1. ![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 | X1 = X2)) [input]
 2. ~![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 |
                                                          X1 = X2)) [negated conjecture 1]
 3. ~![X1:$int,X0:$int]:?[X2:$int]:(~$less(X2,X0) & ~$less(X2,X1) & (X0 = X2 | X1 = X2)) [theory
                                                                         normalization 2]
 9. ~$less(X0,X0) [theory axiom 144]
10. ~$less(X1,X2) | ~$less(X0,X1) | $less(X0,X2) [theory axiom 145]
16. ~![X0 :  $int,X1 :  $int] :  ?[X2 :  $int] :  (~$less(X2,X1) & ~$less(X2,X0) & (X1 = X2 | X0 = X2))
                                                                              [rectify 3]
17. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
                                                                 [ennf transformation 16]
18. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
        => !  [X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [choice axiom]
19. ![X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [skolemisation 17,18]
20. $less(X2,sK1) | $less(X2,sK0) | sK0 != X2 [cnf transformation 19]
21. $less(X2,sK1) | $less(X2,sK0) | sK1 != X2 [cnf transformation 19]
22. $less(sK1,sK1) | $less(sK1,sK0) [equality resolution 21]
23. $less(sK0,sK1) | $less(sK0,sK0) [equality resolution 20]
24. $less(sK1,sK0) [subsumption resolution 22,9]
25. $less(sK0,sK1) [subsumption resolution 23,9]
66. ~$less(X0,sK1) | $less(X0,sK0) [resolution 10,24]
71. $less(sK0,sK0) [resolution 66,25]
72. $false [subsumption resolution 71,9]
```

Proof by refutation, inferences deriving formulas from zero or more other formulas, theory reasoning, preprocessing, superposition calculus

```
% Refutation found.  Thanks to Tanya!
 1. ![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 | X1 = X2)) [input]
 2. ~![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 |
                                                            X1 = X2)) [negated conjecture 1]
 3. ~![X1:$int,X0:$int]:?[X2:$int]:(~$less(X2,X0) & ~$less(X2,X1) & (X0 = X2 | X1 = X2)) [theory
                                                                            normalization 2]
 9. ~$less(X0,X0) [theory axiom 144]
10. ~$less(X1,X2) | ~$less(X0,X1) | $less(X0,X2) [theory axiom 145]
16. ~![X0 :  $int,X1 :  $int] :  ?[X2 :  $int] :  (~$less(X2,X1) & ~$less(X2,X0) & (X1 = X2 | X0 = X2))
                                                                                 [rectify 3]
17. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
                                                                    [ennf transformation 16]
18. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
         => !  [X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [choice axiom]
19. ![X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [skolemisation 17,18]
20. $less(X2,sK1) | $less(X2,sK0) | sK0 != X2 [cnf transformation 19]
21. $less(X2,sK1) | $less(X2,sK0) | sK1 != X2 [cnf transformation 19]
22. $less(sK1,sK1) | $less(sK1,sK0) [equality resolution 21]
23. $less(sK0,sK1) | $less(sK0,sK0) [equality resolution 20]
24. $less(sK1,sK0) [subsumption resolution 22,9]
25. $less(sK0,sK1) [subsumption resolution 23,9]
66. ~$less(X0,sK1) | $less(X0,sK0) [resolution 10,24]
71. $less(sK0,sK0) [resolution 66,25]
72. $false [subsumption resolution 71,9]
```

Proof by refutation, inferences deriving formulas from zero or more other formulas, theory reasoning, preprocessing, superposition calculus

```
% Refutation found.  Thanks to Tanya!
 1. ![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 | X1 = X2)) [input]
 2. ~![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 |
                                                      X1 = X2)) [negated conjecture 1]
 3. ~![X1:$int,X0:$int]:?[X2:$int]:(~$less(X2,X0) & ~$less(X2,X1) & (X0 = X2 | X1 = X2)) [theory
                                                                          normalization 2]
 9. ~$less(X0,X0) [theory axiom 144]
10. ~$less(X1,X2) | ~$less(X0,X1) | $less(X0,X2) [theory axiom 145]
16. ~![X0 :  $int,X1 :  $int] :  ?[X2 :  $int] :  (~$less(X2,X1) & ~$less(X2,X0) & (X1 = X2 | X0 = X2))
                                                                              [rectify 3]
17. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
                                                                    [ennf transformation 16]
18. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
        => !  [X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [choice axiom]
19. ![X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [skolemisation 17,18]
20. $less(X2,sK1) | $less(X2,sK0) | sK0 != X2 [cnf transformation 19]
21. $less(X2,sK1) | $less(X2,sK0) | sK1 != X2 [cnf transformation 19]
22. $less(sK1,sK1) | $less(sK1,sK0) [equality resolution 21]
23. $less(sK0,sK1) | $less(sK0,sK0) [equality resolution 20]
24. $less(sK1,sK0) [subsumption resolution 22,9]
25. $less(sK0,sK1) [subsumption resolution 23,9]
66. ~$less(X0,sK1) | $less(X0,sK0) [resolution 10,24]
71. $less(sK0,sK0) [resolution 66,25]
72. $false [subsumption resolution 71,9]
```

Proof by refutation, inferences deriving formulas from zero or more other formulas, theory reasoning, preprocessing, superposition calculus

```
% Refutation found.  Thanks to Tanya!
 1. ![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 | X1 = X2)) [input]
 2. ~![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 |
                                                        X1 = X2)) [negated conjecture 1]
 3. ~![X1:$int,X0:$int]:?[X2:$int]:(~$less(X2,X0) & ~$less(X2,X1) & (X0 = X2 | X1 = X2)) [theory
                                                                     normalization 2]
 9. ~$less(X0,X0) [theory axiom 144]
10. ~$less(X1,X2) | ~$less(X0,X1) | $less(X0,X2) [theory axiom 145]
16. ~![X0 :  $int,X1 :  $int] :  ?[X2 :  $int] :  (~$less(X2,X1) & ~$less(X2,X0) & (X1 = X2 | X0 = X2))
                                                                           [rectify 3]
17. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
                                                                [ennf transformation 16]
18. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
       => !  [X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [choice axiom]
19. ![X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [skolemisation 17,18]
20. $less(X2,sK1) | $less(X2,sK0) | sK0 != X2 [cnf transformation 19]
21. $less(X2,sK1) | $less(X2,sK0) | sK1 != X2 [cnf transformation 19]
22. $less(sK1,sK1) | $less(sK1,sK0) [equality resolution 21]
23. $less(sK0,sK1) | $less(sK0,sK0) [equality resolution 20]
24. $less(sK1,sK0) [subsumption resolution 22,9]
25. $less(sK0,sK1) [subsumption resolution 23,9]
66. ~$less(X0,sK1) | $less(X0,sK0) [resolution 10,24]
71. $less(sK0,sK0) [resolution 66,25]
72. $false [subsumption resolution 71,9]
```

Proof by refutation, inferences deriving formulas from zero or more other formulas, theory reasoning, preprocessing, superposition calculus

```
% Refutation found.  Thanks to Tanya!
 1. ![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 | X1 = X2)) [input]
 2. ~![X1:$int,X0:$int]:?[X2:$int]:($greatereq(X2,X0) & $greatereq(X2,X1) & (X0 = X2 |
                                                       X1 = X2)) [negated conjecture 1]
 3. ~![X1:$int,X0:$int]:?[X2:$int]:(~$less(X2,X0) & ~$less(X2,X1) & (X0 = X2 | X1 = X2)) [theory
                                                                    normalization 2]
 9. ~$less(X0,X0) [theory axiom 144]
10. ~$less(X1,X2) | ~$less(X0,X1) | $less(X0,X2) [theory axiom 145]
16. ~![X0 :  $int,X1 :  $int] :  ?[X2 :  $int] :  (~$less(X2,X1) & ~$less(X2,X0) & (X1 = X2 | X0 = X2))
                                                                        [rectify 3]
17. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
                                                              [ennf transformation 16]
18. ?[X0 :  $int,X1 :  $int] :  ![X2 :  $int] :  ($less(X2,X1) | $less(X2,X0) | (X1 != X2 & X0 != X2))
        => !  [X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [choice axiom]
19. ![X2 :  $int] :  ($less(X2,sK1) | $less(X2,sK0) | (sK1 != X2 & sK0 != X2)) [skolemisation 17,18]
20. $less(X2,sK1) | $less(X2,sK0) | sK0 != X2 [cnf transformation 19]
21. $less(X2,sK1) | $less(X2,sK0) | sK1 != X2 [cnf transformation 19]
22. $less(sK1,sK1) | $less(sK1,sK0) [equality resolution 21]
23. $less(sK0,sK1) | $less(sK0,sK0) [equality resolution 20]
24. $less(sK1,sK0) [subsumption resolution 22,9]
25. $less(sK0,sK1) [subsumption resolution 23,9]
66. ~$less(X0,sK1) | $less(X0,sK0) [resolution 10,24]
71. $less(sK0,sK0) [resolution 66,25]
72. $false [subsumption resolution 71,9]
```

Proof by refutation, inferences deriving formulas from zero or more other formulas, theory reasoning, preprocessing, superposition calculus

Background: Selected rules of superposition calculus (simplified)

Equality resolution: $\dfrac{s \neq s' \vee C}{C\theta}$ where $\theta := \mathrm{mgu}(s, s')$.

Binary resolution: $\dfrac{L \vee C \quad \neg L' \vee D}{(C \vee D)\theta}$ where $\theta := \mathrm{mgu}(L, L')$.

Superposition: $\dfrac{l = r \vee C \quad L[l'] \vee D}{(L[r] \vee C \vee D)\theta}$ where $\theta := \mathrm{mgu}(l, l')$.

Background: Selected rules of superposition calculus (simplified)

Equality resolution: $\dfrac{s \neq s' \vee C}{C\theta}$ where $\theta := \mathtt{mgu}(s, s')$.

Binary resolution: $\dfrac{L \vee C \quad \neg L' \vee D}{(C \vee D)\theta}$ where $\theta := \mathtt{mgu}(L, L')$.

Superposition: $\dfrac{l = r \vee C \quad L[l'] \vee D}{(L[r] \vee C \vee D)\theta}$ where $\theta := \mathtt{mgu}(l, l')$.

Extension of the superposition calculus: theories, induction, ...

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$
Axioms: $\forall x \in \mathbb{Z}.\neg x < x,\quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \to x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \wedge y \geq x_2 \wedge (y = x_1 \vee y = x_2))$

Axioms: $\forall x \in \mathbb{Z}.\neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \wedge x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \vee y < \sigma_2 \vee \underline{y \neq \sigma_1}$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \vee \neg x_0 < x_1 \vee x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \vee x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor \underline{y \neq \sigma_2}$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x$, $\quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\underline{\sigma_1 < \sigma_1} \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\underline{\neg x < x}$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \wedge y \geq x_2 \wedge (y = x_1 \vee y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \wedge x_1 < x_2) \to x_0 < x_2)$

1.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \vee \underline{\sigma_2 < \sigma_2}$	[ER 2; $y \mapsto \sigma_2$]
5.	$\underline{\neg x < x}$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \vee \neg x_0 < x_1 \vee x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \vee x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$
Axioms: $\forall x \in \mathbb{Z}.\neg x < x$, $\forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \to x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \wedge y \geq x_2 \wedge (y = x_1 \vee y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \wedge x_1 < x_2) \to x_0 < x_2)$

1.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\underline{\sigma_2 < \sigma_1}$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\underline{\neg x_1 < x_2} \vee \neg x_0 < x_1 \vee x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \vee x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x$, $\quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1$	[negated, skolemized and clausified input]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2$	[negated, skolemized and clausified input]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\underline{\sigma_1 < \sigma_2}$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\underline{\neg x_0 < \sigma_2} \lor x_0 < \sigma_1$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\square$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \wedge y \geq x_2 \wedge (y = x_1 \vee y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \wedge x_1 < x_2) \rightarrow x_0 < x_2)$

1. $y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_1$ [negated, skolemized and clausified input]
2. $y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2$ [negated, skolemized and clausified input]
3. $\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2$ [ER 1; $y \mapsto \sigma_1$]
4. $\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2$ [ER 2; $y \mapsto \sigma_2$]
5. $\underline{\neg x < x}$ [axiom]
6. $\sigma_1 < \sigma_2$ [BR 3, 5; $x \mapsto \sigma_1$]
7. $\sigma_2 < \sigma_1$ [BR 4, 5; $x \mapsto \sigma_2$]
8. $\neg x_1 < x_2 \vee \neg x_0 < x_1 \vee x_0 < x_2$ [axiom]
9. $\neg x_0 < \sigma_2 \vee x_0 < \sigma_1$ [BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10. $\underline{\sigma_1 < \sigma_1}$ [BR 9, 6; $x_0 \mapsto \sigma_1$]
11. $\square$ [BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers with answer literals [Green 1969]

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}.\neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1 \lor \mathtt{ans}(y)$	[neg. input with answer literal]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2 \lor \mathtt{ans}(y)$	[neg. input with answer literal]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2 \lor \mathtt{ans}(\sigma_1)$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2 \lor \mathtt{ans}(\sigma_2)$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2 \lor \mathtt{ans}(\sigma_1)$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1 \lor \mathtt{ans}(\sigma_2)$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1 \lor \mathtt{ans}(\sigma_2)$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1 \lor \mathtt{ans}(\sigma_1) \lor \mathtt{ans}(\sigma_2)$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\mathtt{ans}(\sigma_1) \lor \mathtt{ans}(\sigma_2)$	[BR 10, 5; $x \mapsto \sigma_1$]

Background: Maximum of two numbers with answer literals [Green 1969]

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \land y \geq x_2 \land (y = x_1 \lor y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x, \quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \land x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1 \lor \mathtt{ans}(y)$	[neg. input with answer literal]
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2 \lor \mathtt{ans}(y)$	[neg. input with answer literal]
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2 \lor \mathtt{ans}(\sigma_1)$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2 \lor \mathtt{ans}(\sigma_2)$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2 \lor \mathtt{ans}(\sigma_1)$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1 \lor \mathtt{ans}(\sigma_2)$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1 \lor \mathtt{ans}(\sigma_2)$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1 \lor \mathtt{ans}(\sigma_1) \lor \mathtt{ans}(\sigma_2)$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\mathtt{ans}(\sigma_1) \lor \mathtt{ans}(\sigma_2)$	[BR 10, 5; $x \mapsto \sigma_1$]

Witness: either x_1 or x_2 (corresponding to σ_1 or σ_2)

Background: Maximum of two numbers with answer literals [Green 1969]

Conjecture: $\forall x_1, x_2 \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.(y \geq x_1 \wedge y \geq x_2 \wedge (y = x_1 \vee y = x_2))$

Axioms: $\forall x \in \mathbb{Z}. \neg x < x,\quad \forall x_0, x_1, x_2 \in \mathbb{Z}.((x_0 < x_1 \wedge x_1 < x_2) \rightarrow x_0 < x_2)$

1.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_1 \vee \mathtt{ans}(y)$	[neg. input with answer literal]
2.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2 \vee \mathtt{ans}(y)$	[neg. input with answer literal]
3.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2 \vee \mathtt{ans}(\sigma_1)$	[ER 1; $y \mapsto \sigma_1$]
4.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2 \vee \mathtt{ans}(\sigma_2)$	[ER 2; $y \mapsto \sigma_2$]
5.	$\neg x < x$	[axiom]
6.	$\sigma_1 < \sigma_2 \vee \mathtt{ans}(\sigma_1)$	[BR 3, 5; $x \mapsto \sigma_1$]
7.	$\sigma_2 < \sigma_1 \vee \mathtt{ans}(\sigma_2)$	[BR 4, 5; $x \mapsto \sigma_2$]
8.	$\neg x_1 < x_2 \vee \neg x_0 < x_1 \vee x_0 < x_2$	[axiom]
9.	$\neg x_0 < \sigma_2 \vee x_0 < \sigma_1 \vee \mathtt{ans}(\sigma_2)$	[BR 7, 8; $x_1 \mapsto \sigma_2, x_2 \mapsto \sigma_1$]
10.	$\sigma_1 < \sigma_1 \vee \mathtt{ans}(\sigma_1) \vee \mathtt{ans}(\sigma_2)$	[BR 9, 6; $x_0 \mapsto \sigma_1$]
11.	$\mathtt{ans}(\sigma_1) \vee \mathtt{ans}(\sigma_2)$	[BR 10, 5; $x \mapsto \sigma_1$]

Witness: either x_1 or x_2 (corresponding to σ_1 or σ_2) ... how to tell which one?

Our solution

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1 \lor \mathtt{ans}(y)$	[preprocessed input]	
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2 \lor \mathtt{ans}(y)$	[preprocessed input]	
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2 \lor \mathtt{ans}(\sigma_1)$	[ER 1]	
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2 \lor \mathtt{ans}(\sigma_2)$	[ER 2]	
5.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ans removal 3]	if $\neg 5$ then σ_1
6.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ans removal 4]	if $\neg 6$ then σ_2
7.	$\neg x < x$	[axiom]	
8.	$\sigma_1 < \sigma_2$	[BR 5, 7]	
9.	$\sigma_2 < \sigma_1$	[BR 6, 7]	
10.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]	
11.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 9, 10]	
12.	$\sigma_1 < \sigma_1$	[BR 11, 8]	
13.	$\square$	[BR 12, 7]	

Our solution

1.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_1 \lor \mathtt{ans}(y)$	[preprocessed input]	
2.	$y < \sigma_1 \lor y < \sigma_2 \lor y \neq \sigma_2 \lor \mathtt{ans}(y)$	[preprocessed input]	
3.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2 \lor \mathtt{ans}(\sigma_1)$	[ER 1]	
4.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2 \lor \mathtt{ans}(\sigma_2)$	[ER 2]	
5.	$\sigma_1 < \sigma_1 \lor \sigma_1 < \sigma_2$	[ans removal 3]	$\mathtt{if}\ \neg 5\ \mathtt{then}\ \sigma_1$
6.	$\sigma_2 < \sigma_1 \lor \sigma_2 < \sigma_2$	[ans removal 4]	$\mathtt{if}\ \neg 6\ \mathtt{then}\ \sigma_2$
7.	$\neg x < x$	[axiom]	
8.	$\sigma_1 < \sigma_2$	[BR 5, 7]	
9.	$\sigma_2 < \sigma_1$	[BR 6, 7]	
10.	$\neg x_1 < x_2 \lor \neg x_0 < x_1 \lor x_0 < x_2$	[axiom]	
11.	$\neg x_0 < \sigma_2 \lor x_0 < \sigma_1$	[BR 9, 10]	
12.	$\sigma_1 < \sigma_1$	[BR 11, 8]	
13.	$\square$	[BR 12, 7]	

Synthesized program: $max(x_1, x_2) = \mathtt{if}\ \sigma_1 \geq \sigma_1 \land \sigma_1 \geq \sigma_2\ \mathtt{then}\ \sigma_1\ \mathtt{else}\ \sigma_2$

Our solution

1.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_1 \vee \mathtt{ans}(y)$	[preprocessed input]	
2.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2 \vee \mathtt{ans}(y)$	[preprocessed input]	
3.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2 \vee \mathtt{ans}(\sigma_1)$	[ER 1]	
4.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2 \vee \mathtt{ans}(\sigma_2)$	[ER 2]	
5.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2$	[ans removal 3]	$\mathtt{if}\ \neg 5\ \mathtt{then}\ \sigma_1$
6.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2$	[ans removal 4]	$\mathtt{if}\ \neg 6\ \mathtt{then}\ \sigma_2$
7.	$\neg x < x$	[axiom]	
8.	$\sigma_1 < \sigma_2$	[BR 5, 7]	
9.	$\sigma_2 < \sigma_1$	[BR 6, 7]	
10.	$\neg x_1 < x_2 \vee \neg x_0 < x_1 \vee x_0 < x_2$	[axiom]	
11.	$\neg x_0 < \sigma_2 \vee x_0 < \sigma_1$	[BR 9, 10]	
12.	$\sigma_1 < \sigma_1$	[BR 11, 8]	
13.	$\square$	[BR 12, 7]	

Synthesized program: $max(x_1, x_2) = \mathtt{if}\ x_1 \geq x_1 \wedge x_1 \geq x_2\ \mathtt{then}\ x_1\ \mathtt{else}\ x_2$

Our solution

1.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_1 \vee \mathtt{ans}(y)$	[preprocessed input]	
2.	$y < \sigma_1 \vee y < \sigma_2 \vee y \neq \sigma_2 \vee \mathtt{ans}(y)$	[preprocessed input]	
3.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2 \vee \mathtt{ans}(\sigma_1)$	[ER 1]	
4.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2 \vee \mathtt{ans}(\sigma_2)$	[ER 2]	
5.	$\sigma_1 < \sigma_1 \vee \sigma_1 < \sigma_2$	[ans removal 3]	$\mathtt{if}\ \neg 5\ \mathtt{then}\ \sigma_1$
6.	$\sigma_2 < \sigma_1 \vee \sigma_2 < \sigma_2$	[ans removal 4]	$\mathtt{if}\ \neg 6\ \mathtt{then}\ \sigma_2$
7.	$\neg x < x$	[axiom]	
8.	$\sigma_1 < \sigma_2$	[BR 5, 7]	
9.	$\sigma_2 < \sigma_1$	[BR 6, 7]	
10.	$\neg x_1 < x_2 \vee \neg x_0 < x_1 \vee x_0 < x_2$	[axiom]	
11.	$\neg x_0 < \sigma_2 \vee x_0 < \sigma_1$	[BR 9, 10]	
12.	$\sigma_1 < \sigma_1$	[BR 11, 8]	
13.	$\square$	[BR 12, 7]	

Synthesized program: $max(x_1, x_2) = \mathtt{if}\ x_1 \geq x_2\ \mathtt{then}\ x_1\ \mathtt{else}\ x_2$

Modifying saturation algorithm

Deriving a program for $A_1 \wedge \cdots \wedge A_n \rightarrow \forall \overline{x}.\exists \overline{y}.F(\overline{x}, \overline{y})$:

1. Create the set of formulas $\mathcal{S} = \{A_1, \ldots, A_n, \forall \overline{y}.CNF(\neg F(\overline{\sigma}, \overline{y}) \vee \mathtt{ans}(y))\}$
2. Repeat:
   2.1 Choose $C \in \mathcal{S}$
   2.2 Apply rules to derive consequences $C_1, \ldots, C_n$ of C and clauses from $\mathcal{S}$
   2.3 Add $C_1, \ldots, C_n$ to $\mathcal{S}$
   2.4 If $\mathcal{S}$ contains $D[\overline{\sigma}] \vee \mathtt{ans}(r[\overline{\sigma}])$ where $D[\overline{\sigma}]$ is computable, then
   remove $D[\overline{\sigma}] \vee \mathtt{ans}(r[\overline{\sigma}])$ from $\mathcal{S}$, add $D[\overline{\sigma}]$ to $\mathcal{S}$, and record $\langle D[\overline{\sigma}], r[\overline{\sigma}] \rangle$
   2.5 If $\mathcal{S}$ contains $\square$, construct a program from recorded fragments as

$$
\begin{array}{l}
\mathtt{if}\ \neg D_1[\overline{x}]\ \mathtt{then}\ r_1[\overline{x}] \\
\mathtt{else\ if}\ \neg D_2[\overline{x}]\ \mathtt{then}\ r_2[\overline{x}] \\
\qquad \ldots \\
\mathtt{else\ if}\ \neg D_{k-1}[\overline{x}]\ \mathtt{then}\ r_{k-1}[\overline{x}] \\
\mathtt{else}\ r_k[\overline{x}]
\end{array}
$$

Modifying inference rules

At most 1 answer literal in each clause. Only computable functions allowed in answer literals.

Modifying inference rules

At most 1 answer literal in each clause. Only computable functions allowed in answer literals.

Equality resolution: $\dfrac{s \neq s' \vee C \vee \mathtt{ans}(\overline{t})}{(C \vee \mathtt{ans}(\overline{t}))\theta}$ where $\theta := \mathrm{mgu}(s, s')$, and $\overline{t}\theta$ is computable.

Binary resolution: $\dfrac{L \vee C \vee \mathtt{ans}(\overline{t_1}) \quad \neg L' \vee D \vee \mathtt{ans}(\overline{t_2})}{(C \vee D \vee \mathtt{ans}(\mathtt{if}\ L\ \mathtt{then}\ \overline{t_2}\ \mathtt{else}\ \overline{t_1}))\theta}$ where $\theta := \mathrm{mgu}(L, L')$, and $L\theta$ is computable (partially [Tammet 1995]).

Superposition: $\dfrac{l = r \vee C \vee \mathtt{ans}(\overline{t_1}) \quad L[l'] \vee D \vee \mathtt{ans}(\overline{t_2})}{(L[r] \vee C \vee D \vee \mathtt{ans}(\mathtt{if}\ l = r\ \mathtt{then}\ \overline{t_2}\ \mathtt{else}\ \overline{t_1}))\theta}$ where $\theta := \mathrm{mgu}(l, l')$, and $l\theta, r\theta$ are computable.

More complex rules when some functions are not computable.

More examples (1)

- Maximum for up to 23 variables
- Group examples, given

  $$\forall x.\, i(x) * x = e, \qquad \forall x.\, e * x = x, \qquad \forall x, y, z.\, x * (y * z) = (x * y) * z$$

  find:

  - right inverse: $\forall x. \exists y.\ x * y = e$
    program: $i(x)$
  - inverse of $i(x) * i(y)$ without using i: $\forall x, y. \exists z.\ z * (i(x) * i(y)) = e$
    program: $y * x$
  - an element whose square is not e, if the group is not commutative:
    $\forall x, y. \exists z. (x * y \neq y * x \rightarrow z * z \neq e)$
    program: $\texttt{if } x*(y*x)=x \texttt{ then } x \texttt{ else } (\texttt{if } e=x*(y*(x*y)) \texttt{ then } x \texttt{ else } x*y)$

More examples (2)

- Quadratic equation: $\forall x_1, x_2. \exists y. (y^2 = x_1^2 + 2x_1x_2 + x_2^2)$
  program: $x_1 + x_2$
- SyGuS competition examples:
  - $\forall x_1, x_2, k. \exists y. ((x_1 < x_2 \rightarrow (k < x_1 \rightarrow y = 0)) \wedge$
    $(x_1 < x_2 \rightarrow (k > x_2 \rightarrow y = 2)) \wedge$
    $(x_1 < x_2 \rightarrow ((k > x_1 \wedge k < x_2) \rightarrow y = 1)))$
  - $\forall x_1, x_2. \exists y. ((x_1 + x_2 > 5 \rightarrow y = x_1 + x_2) \wedge (x_1 + x_2 \leq 5 \rightarrow y = 0))$
  - $\forall x, y. \exists f_1, f_2, f_3, f_4, f_5. (f_1 + f_1 = f_2 \wedge (f_1 + f_2) - y = f_3 \wedge f_2 + f_2 = f_4 \wedge f_4 + f_1 = f_5)$

Summary and challenges

What we do:

- Synthesis from specification
- Extended the saturation algorithm (including AVATAR) and superposition calculus
- Implementation in Vampire

Challenges:

- Future work: recursive programs, postprocessing
- How to get good benchmarks?