FIRST-ORDER LOGIC: SOFTWARE FOR PROVING

Course “Computational Logic”

Wolfgang Schreiner
Research Institute for Symbolic Computation (RISC)
Wolfgang.Schreiner@risc.jku.at
Software for Proving

We will give examples for two classes of such software.

- **Automated Theorem Provers**
  - Fully automatic execution (until successful termination or timeout/abortion).
  - Logics with complete inference systems (mostly).
    - Typically: first-order logic (FOL) with equality.
  - Example: *Vampire* (others: E, Prover9, Waldmeister, SPASS, Theorema, ...)

- **Proof Assistants**
  - User-guided proof elaboration.
    - Supported by automatic proof tactics, decision procedures, external provers.
  - Also logics without complete inference systems.
    - Typically: higher-order logic (HOL).
  - Example: *Isabelle/HOL* (others: Coq, HOL4, HOL Light, ACL2, PVS, ...)

While automated theorem provers have become very strong, complex problems still require the application of proof assistants.
Vampire

Software: https://vprover.github.io/
Tutorial:  First-Order Theorem Proving and Vampire (Laura Kovács and Andrei Voronkov)

- Automated theorem prover
  - A. Voronkov (Univ. Manchester), K. Hoder, L. Kovács, I. Dragan, and others.
  - First implementation in 1993, current implementation started in 2009.
- First-order logic with equality
  - Based on the inference calculi of resolution and superposition.
  - Also supports various theories such as linear integer arithmetic.
- Very efficient algorithms and fast C++ implementation.
  - Regular winner of the CASC categories FOF and TFA.
    - CASC (CADE ATP System Competition): http://www.tptp.org/CASC
- TPTP and SMTLIB languages supported.
  - Established standards in automated theorem proving.

Vampire represents the state of the art in automated first-order proving.
TPTP: Thousands of Problems for Theorem Provers

http://www.tptp.org

System on TPTP

This interface is for solving problems. If you want to prepare problems, use the SystemAtTPTP interface. If you want to process solutions, use the SystemOnTPTP interface.

The TPTP Needs Money

See the TPTP web page for details, benefits, and process of making a donation.

Problem

- TPTP Problem (e.g., sin4x=1)
- Input Format (EFG example, CNF example)
- Don't return here

TPTP problem and solution finder

- Local file to upload
- Browse...
- No ReAssociated

Solve the Problem

Solution attempts are limited to a few users at a time (until I get more resources - see the note at the top of the page).

Your job may be rejected if the computers are too busy.

Overwrite password:

Output mode

- Nothing
- Result
- Progress
- System
- Everything
- Extras (Nothing else)

Transform

- TPTP format
- EHF image
- ScTSTP

Parallel mode

- Selected
- Naive...
- SSSCPA...
- Eager SSSCPA...

300 s

3 systems

System Recommendations and Reports

The recommendations and reports are based on the system/ results for the TPTP. There is no guarantee that they are right for your application. If no problem is specified then all possibilities will be used.

Reports required

- System Info
- Completeness
- Soundness
- Correctness
- TPTP Data

Output mode

- Summary
- Full

Our server does not output results until all tasks are completed. Be patient while the systems do their thing. Results are presented using the SRS problem status ontology.

System

- amwy13121.0
- CPU s
- Transform
- Format
- Command
- Application

- Nov6421: 1.0
- none
- tppgrow
- pmsg:alg:greg:time-out:4
- Prover for Full
The TPTP Language


<TPTP_file> ::= <fof.annotated>*
<fof.annotated> ::= fof(<name>,<formula_role>,<fof.formula> <annotations>).
<formula_role> ::= axiom | conjecture | negated_conjecture | ... 
...
<fof.quantified_formula> ::= <fof.quantifier> [<fof.variable_list>] : <fof.unit_formula>
<fof.quantifier> ::= ! | ?
<fof.variable_list> ::= <variable> | <variable>,<fof.variable_list>
...
<connective> ::= ¬ | & | [] | => | <= | => | ¬& | ¬[] | <~>
...
<fof.plain.atomic.formula> ::= <atomic_word> | <atomic_word>(<fof.arguments>)
<fof.term> ::= <variable> | <atomic_word> | <atomic_word>(<fof.arguments>)
<fof.arguments> ::= <fof.term> | <fof.term>,<fof.arguments>
...
<variable> ::= <upper_word>
<atomic_word> ::= <lower_word> | <single_quoted>

FOF: first-order form (TFF: typed first-order form).
Syntactic Pitfalls

**WARNING:** several common errors give formulas unintended meanings.

- **Missing Parentheses:** precedence among binary connectives is *undefined*.
  
  (`...`) (..&..) (..|..) (..=>..) (..<=>..) (![X]:..) (?[X]:..)

- **Variables Not Capitalized:** treated as fresh constants.
  
  ![X,Y]:(.x.Y..)

- **Constants Capitalized:** treated as universally quantified variables.
  
  .. Zero ..

- **Misspellings:** introduce uninterpreted constants, functions, predicates.
  
  .. bijective_function_f .. bijectiv_function_f ..

In FOF, identifiers are “implicitly declared”, no static checks prevent misspellings (which generally lead to failed proofs or to successful but meaningless proofs)!
A First-Order Problem

% file fol6a.p: a simple first-order problem

% the assumptions (note the parentheses around the body of a quantified formula!)
fof(a1, axiom, p(a) | q(b)).
fof(a2, axiom, ![X]: (p(X) => r(X))).
fof(a3, axiom, ![X]: (q(X) => r(f(x)))).

% the goal to prove
fof(g, conjecture, ![X]: (r(X))).

debian10!1> vampire -om smtcomp fol6a.p
unsat

The conjunction of the axioms and the negation of the conjecture is unsatisfiable, thus the conjecture is a logical consequence of the axioms.
Semantic Pitfalls

The axioms might be inconsistent and thus prove every goal.

% file fol6a.p: a simple first-order problem

% the assumptions (note the parentheses around the body of a quantified formula!)
fof(a1, axiom, p(a) | q(b)).
fof(a2, axiom, ![X]: (p(X) => r(X))).
fof(a3, axiom, ![X]: (q(X) => r(f(x))))).

% the goal to prove (commented out)
% fof(g, conjecture, ![X]: (r(X))).

debian10!1> vampire -om smtcomp fol6a.p
sat

After the successful proof of a conjecture, better check that this success is not just achieved from inconsistent axioms.
Proof Statistics for the Problem

debian10!1> vampire --proof off fol6a.p
% Refutation found. Thanks to Tanya!
% SZS status Theorem for fol6a
% --------------------------------------
% Version: Vampire 4.5.1 (commit 57a6f78c on 2020-07-15 11:59:04 +0200)
% Termination reason: Refutation

% Memory used [KB]: 4861
% Time elapsed: 0.028 s
% --------------------------------------
% --------------------------------------

“Refutation found”: the system could prove the unsatisfiability of the conjunction of the axioms and the negation of the conjecture.
A detailed description of every transformation step and every inference step in a proof based on the principle of “resolution”. 9/36
A Proof for External Checking

debian10!1> vampire --proof proofcheck fol6a.p
% Refutation found. Thanks to Tanya!
% SZS status Theorem for fol6a
% SZS output start Proof for fol6a
fof(r30,conjecture, $false ). %subsumption resolution
fof(pr20,axiom, q(b) ).
fof(pr24,axiom, ( ![X0] : (~q(X0)) ) ).
%#
fof(r32,conjecture, r(a) ). %resolution
fof(pr10,axiom, ( ![X0] : (~p(X0) | r(X0)) ) ).
fof(pr16,axiom, p(a) ).
%#
fof(r33,conjecture, $false ). %subsumption resolution
fof(pr32,axiom, r(a) ).
fof(pr12,axiom, ( ![X0] : (~r(X0)) ) ).
%#
fof(r35,conjecture, $false ). %subsumption resolution
fof(pr28,axiom, r(f(x)) ).
fof(pr12,axiom, ( ![X0] : (~r(X0)) ) ).
%#
% ...

The resolution proof as a sequence of TPTP problems for external checking.
A Problem in First-Order Logic with Equality

% fol6b.p: the group theory example from the tutorial paper.
% "if all elements in a group have order 2, then the group is commutative"

% the group axioms
fof(leftidentity,axiom, ![X]: (mult(e,X) = X)).
fof(leftinverse,axiom, ![X]: (mult(inverse(X),X) = e)).
fof(associativity,axiom, ![X,Y,Z]: (mult(mult(X,Y),Z) = mult(X,mult(Y,Z)))).

% all elements have order two
fof(groupoforder2,hypothesis, ![X]: (mult(X,X) = e)).

% the group is commutative
fof(commutativity,conjecture, ![X]: (mult(X,Y) = mult(Y,X))).

debian10!1> vampire -om smtcomp fol6b.p
unsat

The atomic predicate = has the fixed interpretation “equality”.
A Proof of the Problem

debian10!1> vampire fo16b.p
% Refutation found. Thanks to Tanya!
% SZS status Theorem for fo16b
% SZS output start Proof for fo16b
1. ! [X0] : mult(e,X0) = X0 [input]
2. ! [X0] : e = mult(inverse(X0),X0) [input]
3. ! [X0,X1,X2] : mult(mult(X0,X1),X2) = mult(X0,mult(X1,X2))
   [input]
4. ! [X0] : e = mult(X0,X0) [input]
5. ! [X0] : mult(X0,X1) = mult(X1,X0) [input]
6. ~! [X1] : ! [X0] : mult(X0,X1) = mult(X1,X0)
   [negated conjecture 5]
7. ~! [X0,X1] : mult(X0,X1) = mult(X1,X0) [rectify 6]
8. ~! [X0,X1] : mult(X0,X1) = mult(X1,X0) [flattening 7]
9. ? [X0,X1] : mult(X0,X1) != mult(X1,X0)
10. ? [X0,X1] : mult(X0,X1) != mult(X1,X0) => mult(sK0,sK1) !=
    mult(sK1,sK0) [choice axiom]
11. mult(sK0,sK1) != mult(sK1,sK0) [skolemisation 9,10]
12. mult(e,X0) = X0 [cnf transformation 1]
13. e = mult(inverse(X0),X0) [cnf transformation 2]
14. mult(mult(X0,X1),X2) = mult(X0,mult(X1,X2))
   [cnf transformation 3]
15. e = mult(X0,X0) [cnf transformation 4]
16. mult(sK0,sK1) != mult(sK1,sK0) [cnf transformation 11]
17. mult(X0,mult(X0,X1)) = mult(e,X1) [superposition 14,15]
19. mult(inverse(X4),mult(X4,X5)) = mult(e,X6)
   [superposition 14,13]
21. e = mult(X0,mult(X1,mult(X0,X1))) [superposition 14,15]
23. mult(X0,mult(X0,X1)) = X1 [forward demodulation 17,12]
24. mult(inverse(X4),mult(X4,X5)) = X5
   [forward demodulation 19,12]
29. mult(inverse(X2),e) = X2 [superposition 23,13]
77. mult(X4,mult(X3,X4)) = mult(inverse(X3),e)
   [superposition 24,21]
92. mult(X4,mult(X3,X4)) = X3 [forward demodulation 77,29]
127. mult(X2,X3) = mult(X3,X2) [superposition 23,92]
271. mult(sK0,sK1) != mult(sK1,sK0) [superposition 16,127]
272. $false [trivial inequality removal 271]
% SZS output end Proof for fo16b
% ------------------------------
% Version: Vampire 4.5.1 (commit 57a6f78c on ...)
% Termination reason: Refutation
% ------------------------------
% Memory used [KB]: 5117
% Time elapsed: 0.037 s
% ------------------------------
% ------------------------------

Equality reasoning based on the principle of “superposition”. 12/36
An Incorrect Conjecture

% file fol6c.p: an incorrect conjecture
fof(a1, axiom, p(a) | q(b)).
fof(a2, axiom, ![X]: (p(X) => r(X))).
fof(g, conjecture, ![X]: (r(X))).

debian10!1> vampire fol6c.p
% SZS status CounterSatisfiable for fol6c
% # SZS output start Saturation.
% # SZS output end Saturation.
% ------------------------------
% Version: Vampire 4.5.1 (commit 57a6f78c on 2020-07-15 11:59:04 +0200)
% Termination reason: Satisfiable

% Memory used [KB]: 4861
% Time elapsed: 0.029 s
% ------------------------------
% ------------------------------

The system may be also able to show that the conjecture is incorrect by a model that satisfies the conjunction of the axioms and of the negated conjecture.
An Incorrect Conjecture

Sometimes the counterexample model is reasonably intuitive.

debian10!1> vampire --mode casc_sat fol6c.p
...
% SZS status CounterSatisfiable for fol6c
% # SZS output start Saturation.
cnf(u7,negated_conjecture, 
    ~r(X0)).

cnf(u11,negated_conjecture, 
    q(b)).

cnf(u10,negated_conjecture, 
    ~p(X0)).
...

A counterexample model where \( q(b) \) is true and \( p(x) \) and \( r(x) \) are false for all \( x \).
Problem: Does Superman Exist?

Consider the following assumptions:

1. If Superman were able and willing to prevent evil, he would do so.
2. If Superman were unable to prevent evil, he would be impotent.
3. If Superman were unwilling to prevent evil, he would be malevolent.
4. Superman does not prevent evil.
5. If Superman exists, he is neither impotent nor malevolent.

Prove the following conjecture: “Superman does not exist”.

% file fol6f.p: does superman exist?
fof(a1, axiom, ![X]: (superman(X) => ((able(X) & willing(X)) => prevent(X)))).
fof(a2, axiom, ![X]: (superman(X) => ((~able(X)) => impotent(X)))).
fof(a3, axiom, ![X]: (superman(X) => ((~willing(X)) => malevolent(X)))).
fof(a4, axiom, ![X]: (superman(X) => (~prevent(X)))).
fof(a5, axiom, ![X]: (superman(X) => ((~impotent(X)) & (~malevolent(X)))).
fof(g, conjecture, ~?[X]: (superman(X))).

debian10!1> vampire -om smtcomp fol6f.p
unsat
Problem: Who Killed Agatha?

Pelletier Problem 55 (Francis Jeffry Pelletier, 1986):

Someone who lives in Dreadbury Mansion killed Aunt Agatha. Agatha, the butler, and Charles live in Dreadbury Mansion, and are the only people who live therein. A killer always hates his victim, and is never richer than his victim. Charles hates no one that Aunt Agatha hates. Agatha hates everyone except the butler. The butler hates everyone not richer than Aunt Agatha. The butler hates everyone Aunt Agatha hates. No one hates everyone. Agatha is not the butler.

Prove the following conjecture: “Agatha killed herself”.
Solution

% fol6d.p Pelletier problem 55 (TPTP problem PUZ001+1)
fof(pel55_1, axiom, \(\forall [X] : (\text{lives}(X) \land \text{killed}(X, \text{agatha}))\)).
fof(pel55_2_1, axiom, \text{lives}(\text{agatha})).
fof(pel55_2_2, axiom, \text{lives}(\text{butler})).
fof(pel55_2_3, axiom, \text{lives}(\text{charles})).
fof(pel55_3, axiom, \(\forall [X] : (\text{lives}(X) \implies (X = \text{agatha} \lor X = \text{butler} \lor X = \text{charles}))\)).
fof(pel55_4, axiom, \(\forall [X,Y] : (\text{killed}(X,Y) \implies \text{hates}(X,Y))\)).
fof(pel55_5, axiom, \(\forall [X,Y] : (\text{killed}(X,Y) \implies \neg\text{richer}(X,Y))\)).
fof(pel55_6, axiom, \(\forall [X] : (\text{hates}(\text{agatha},X) \implies \neg\text{hates}(\text{charles},X))\)).
fof(pel55_7, axiom, \(\forall [X] : (X \neq \text{butler} \implies \text{hates}(\text{agatha},X))\)).
fof(pel55_8, axiom, \(\forall [X] : (\neg\text{richer}(X,\text{agatha}) \implies \text{hates}(\text{butler},X))\)).
fof(pel55_9, axiom, \(\forall [X] : (\text{hates}(\text{agatha},X) \implies \text{hates}(\text{butler},X))\)).
fof(pel55_10, axiom, \(\forall [X] : (? [Y] : (\neg\text{hates}(X,Y)))\)).
fof(pel55_11, axiom, \text{agatha} \neq \text{butler}).
fof(pel55, conjecture, \text{killed}(\text{agatha}, \text{agatha})).

debian10!^>\text{vampire -om smtcomp fol6d.p}
unsat
Problem: Composition of Bijective Functions

Prove the following theorem:

Let $f: D \to D$ and $g: D \to D$ be functions on some domain $D$. If $f$ and $g$ are bijective, then also their composition is.

% file fol6h.p: if f and j are bijective, then also their composition is.
fof(goal, conjecture, (bijective_f & bijective_g & composition_f_g_h) => bijective_h).
fof(a1, axiom, bijective_f <=> ( (![Y]:(?[X]:f(X)=Y)) & ([X1,X2,Y]:((f(X1)=Y & f(X2)=Y) => X1=X2))))).
fof(a2, axiom, bijective_g <=> ( ![Y]:(?[X]:g(X)=Y)) & ([X1,X2,Y]:((g(X1)=Y & g(X2)=Y) => X1=X2))))).
fof(a3, axiom, composition_f_g_h <=> ( ![X]: (h(X) = g(f(X))))).
fof(a4, axiom, bijective_h <=> ( ![Y]:(?[X]:h(X)=Y)) & ([X1,X2,Y]:((h(X1)=Y & h(X2)=Y) => X1=X2))))).

debian10!1> vampire -om smtcomp fol6h.p
unsat

18/36
Problem: Inversion of a Bijective Function

Let \( f \subseteq D \times D \). Prove that, if \( f: D \rightarrow D \) is a bijective function, also its inverse is.

\[
\text{Let } f \subseteq D \times D. \text{ Prove that, if } f: D \rightarrow D \text{ is a bijective function, also its inverse is.}
\]

% file fol6g.p: if f is a bijective function, also its inverse is.
fof(goal, conjecture, (bijective_function_f & inverse_f_g) => bijective_function_g).

% atomic predicate apply(f,X,Y): "tuple (X,Y) is in binary relation f" (aka "f(X)=Y")
fof(a1, axiom, bijective_function_f <=> ( 
  (![X]:(?[Y]:((apply(f,X,Y)))) & 
  (![X,Y1,X2]:((apply(f,X,Y1) & apply(f,X,Y2)) => Y1=Y2)) & 
  (![Y]:(?[X]:((apply(f,X,Y)))) & 
  (![X1,X2,Y]:((apply(f,X1,Y) & apply(f,X2,Y)) => X1=X2)))).

fof(a2, axiom, inverse_f_g <=> ![X,Y]:((apply(f,X,Y) <=> apply(g,Y,X))).

fof(a3, axiom, bijective_function_g <=> ( 
  (![X]:(?[Y]:((apply(g,X,Y)))) & 
  (![X,Y1,X2]:((apply(g,X,Y1) & apply(g,X,Y2)) => Y1=Y2)) & 
  (![Y]:(?[X]:((apply(g,X,Y)))) & 
  (![X1,X2,Y]:((apply(g,X1,Y) & apply(g,X2,Y)) => X1=X2)))).

debian10!1> vampire -om smtcomp fol6g.p
unsat
N Queens Problem

Prove that every “flipped” solution to the $N$ queens problem is also a solution:

$$\text{queens}(p) \land \text{symmetric}(p,q) \Rightarrow \text{queens}(q)$$

$$\text{queens}(p) : \iff$$
$$p: \{1, \ldots, N\} \rightarrow \{1, \ldots, N\} \land$$
$$\forall i \in \mathbb{Z}, j \in \mathbb{Z}. \ 1 \leq i < j \land j \leq N \Rightarrow$$
$$p(i) \neq p(j) \land p(i) + i \neq p(j) + j \land p(i) - i \neq p(j) - j$$

$$\text{symmetric}(p,q) : \iff \forall i \in \mathbb{Z}. \ 1 \leq i \leq N \Rightarrow q(i) = p(N + 1 - i)$$

Arithmetic with constant $1$, functions $+$ and $-$, and predicate $\leq$. 
% file fol6e-leq.p: solution with "zero" "succ" "plus" "minus" and "leq"
fof(goal, conjecture, (queens_p & symmetric_pq) => queens_q).

% p and q are solutions to the N queens problem
fof(queens_p, axiom, queens_p <=> ![I,J]:((leq(succ(zero),I) & leq(succ(I),J) & leq(J,n)) =>
   (p(I) != p(J) & plus(p(I),I) != plus(p(J),J) & minus(p(I),I) != minus(p(J),J)))).
fof(queens_q, axiom, queens_q <=> ![I,J]:((leq(succ(zero),I) & leq(succ(I),J) & leq(J,n)) =>
   (q(I) != q(J) & plus(q(I),I) != plus(q(J),J) & minus(q(I),I) != minus(q(J),J)))).

% q is symmetric to p: q(i) = p(pos(i)) = p(n+1-i)
fof(symmetric, axiom, symmetric_pq <=>
   ![I]:((leq(succ(zero),I) & leq(I,n)) => q(I)=p(pos(I)))).

% the definition of pos is actually not helpful, the properties below are required
% fof(symmetric, axiom, pos <=> ![I]: (pos(I) = minus(succ(n),I))).
...
% file fol6e-leq.p: solution with "zero" "succ" "plus" "minus" and "leq"

First Solution: plus, succ, zero, leq, minus

% property required from minus: i+j = k+1 <=> i-k = l-j
fof(plus_minus, axiom, ![I,J,K,L]: (plus(I,J) = plus(K,L) <=> minus(I,K) = minus(L,J))).

% properties required from leq: i <= i+1 and (i <= j & j <= k => i <= k)
fof(le_succ, axiom, ![I]: (leq(I, succ(I)))).
fof(le_tran, axiom, ![I,J,K]: (leq(I,J) & leq(J,K) => leq(I,K))).

% properties required from pos
fof(pos1, axiom, % 1 <= i & i <= n => 1 <= pos(i) & pos(i) <= n
 ![I]: (leq(succ(zero), I) & leq(I, n)) => (leq(succ(zero), pos(I)) & leq(pos(I), n)))).
fof(pos2, axiom, % i-j = pos(j)-pos(i)
 ![J,I]: (minus(I,J) = minus(pos(J), pos(I)))).
fof(pos3, axiom, % 1 <= i & i < j & j <= n => pos(j) < pos(i)
 ![J,I]: (leq(succ(zero), I) & leq(succ(I), J) & leq(J, n) => leq(succ(pos(J)), pos(I)))).
First Solution: \texttt{plus, zero, succ, leq, minus}

\begin{verbatim}
debian10!1> vampire fol6e-leq.p
  \% Refutation found. Thanks to Tanya!
  
  \% Time elapsed: 12.504 s
  \% ------------------------------

 debian10!1> vampire --mode casc fol6e-leq.p
  \% Refutation found. Thanks to Tanya!
  
  \% ------------------------------

  debian10!1> vampire --mode casc fol6e-leq.p
  \% Refutation found. Thanks to Tanya!
  
  \% ------------------------------

  debian10!1> vampire --mode casc fol6e-leq.p
  \% Refutation found. Thanks to Tanya!
  
  \% ------------------------------

  debian10!1> vampire --mode casc fol6e-leq.p
  \% Refutation found. Thanks to Tanya!
  
  \% ------------------------------

The proof can be found much faster by trying a portfolio of search strategies.
\end{verbatim}
% file fol6e-typed.p: typed solution

tff(queens_p_type, type, queens_p: $o).
tff(queens_q_type, type, queens_q: $o).
tff(symmetric_pq_type, type, symmetric_pq: $o).
tff(p_type, type, p: $int > $int).
tff(q_type, type, q: $int > $int).
tff(n_type, type, n: $int).

tff(goal, conjecture, (queens_p & symmetric_pq) => queens_q).
...

Actually, Vampire also provides built-in support for the theory of integers.
Second Solution: Typed First-Order Logic

\% file fol6e-typed.p: typed solution

... tff(queens_p, axiom, queens_p <-> \% much faster with $\text{lesseq}$ and $\neq$ than with $\text{less}$
      ![I:$\text{int},J:$\text{int}]:((\text{lesseq}(1,I) \& \text{lesseq}(I,J) \& \text{lesseq}(J,n) \& I \neq J) \Rightarrow
      (p(I) \neq p(J) \& \text{sum}(p(I),I) \neq \text{sum}(p(J),J) \& \text{sum}(p(I),J) \neq \text{sum}(p(J),I))))).

tff(queens_q, axiom, queens_q <-> \% much faster with $\text{lesseq}$ and $\neq$ than with $\text{less}$
      ![I:$\text{int},J:$\text{int}]:((\text{lesseq}(1,I) \& \text{lesseq}(I,J) \& \text{lesseq}(J,n) \& I \neq J) \Rightarrow
      (q(I) \neq q(J) \& \text{sum}(q(I),I) \neq \text{sum}(q(J),J) \& \text{sum}(q(I),J) \neq \text{sum}(q(J),I))))).

tff(symmetric, axiom, symmetric_pq <->
      ![I:$\text{int}]:((\text{lesseq}(1,I) \& \text{lesseq}(I,n)) \Rightarrow q(I)=p(\text{difference}(\text{sum}(n,1),I))))).

debian10!1> vampire --mode casc fol6e-typed.p
\% Refutation found. Thanks to Tanya!

... 
\% Success in time 7.42 s

Indeed the integer support is sufficient for solving this problem.
Automated first-order theorem proving has some caveats.

- Problems must be captured by a finite number of first-order axioms.
  - *Incompleteness Theorem* (Kurt Gödel, 1930): the arithmetic of natural numbers cannot be completely captured by any sound logical calculus.
- For every problem, sufficiently strong axioms have to be provided.
  - TPTP provides a library of axiom sets that are shared by many problems.
- However, the axiomatization should be minimal to facilitate proof search.
  - The size of the search space quickly explodes.
- Ultimately, it requires experience to find adequate problem formalizations.
  - Many formalizations possible, minor changes may have drastic consequences.
- Last but not least, the generated proofs are typically not “human-oriented”.
  - See *Theorema*: [https://www.risc.jku.at/research/theorema/software](https://www.risc.jku.at/research/theorema/software)

Automated first-order provers may also integrate/interact with SMT solvers or be applied for proof search in interactive proof assistants.
Isabelle

Software: https://isabelle.in.tum.de/
Tutorial: Programming and Proving in Isabelle/HOL (Tobias Nipkow)

- **Generic proof assistant:**
  - Larry Paulson (Univ. Cambridge), Tobias Nipkow (TU Munich), and many others.
  - Initial release in 1986, yearly updates (“Isabelle 2021”).
- **Generic**: typed meta-logic to encode various object-logics.
  - Polymorphic type system similar to ML-like programming languages.
- **Proof assistant**: interactive elaboration of procedural/declarative proofs.
  - Procedural: application of proof procedures (“tactics”).
    - Declarative: writing of formal proofs in the “Isar” language.
- **Automation**: combination of various reasoning tools.
  - Term rewriting, tableaux method, resolution, decision procedures, external automated provers and SMT solvers (tool “Sledgehammer”).
  - Counterexample generators Nitpick and Nunchaku.

Many applications in mathematics and computer science.
The Archive of Formal Proofs is a collection of proof libraries, examples, and larger scientific developments, mechanically checked in the theorem prover Isabelle. It is organized in the way of a scientific journal, is indexed by dblp and has an ISSN: 2150-914x. Submissions are refereed. The preferred citation style is available [here]. We encourage companion AFP submissions to conference and journal publications.

A development version of the archive is available as well.

<table>
<thead>
<tr>
<th>Year</th>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021</td>
<td>Finitely Generated Abelian Groups</td>
<td>Joseph Thrommes and Manuel Eberl</td>
</tr>
<tr>
<td>2021</td>
<td>SpecCheck - Specification-Based Testing for Isabelle/ML</td>
<td>Kevin Koppelmann, Lukas Bulwahn, and Sebastian Willenbrink</td>
</tr>
<tr>
<td>2021</td>
<td>Van der Waerden's Theorem</td>
<td>Katharina Kreuzer and Manuel Eberl</td>
</tr>
<tr>
<td>2021</td>
<td>MiniSail - A kernel language for the ISA specification language SAIL</td>
<td>Mark Wassell</td>
</tr>
<tr>
<td>2021</td>
<td>Public Announcement Logic</td>
<td>Asta Halkjær From</td>
</tr>
<tr>
<td>2021</td>
<td>A Shorter Compiler Correctness Proof for Language IMP</td>
<td>Pasquale Noce</td>
</tr>
</tbody>
</table>
Formal proof documents with semantic markup and continuous checking.
theory models (* file models.thy, type \forall to select symbol ∀ from popup window *)
imports Main
begin

type_synonym 'a seq = "nat \rightarrow 'a"

definition isconst :: "'a \rightarrow 'a seq \rightarrow 'a" where
"isconst c s = (\forall i :: nat. s i = c)"

definition cseq :: "'a \rightarrow 'a seq" where
"cseq c = (\lambda i :: nat. c)"

lemma S1: "\forall (c :: 'a) (s :: 'a seq). isconst c (cseq c)"
by (simp add: cseq_def isconst_def)

end

Automatic proof search: move cursor to lemma; press in tab “Sledgehammer” button Apply
(“search for first-order proof using automatic theorem provers”); output Proof found...
Displays proof command by (…); click on command to insert it into document.
definition vpos :: "'a seq nat" where
"vpos c s = (SOME n::nat. (\exists i::nat. s i = c) \&\& s n = c)"

lemma S2 : "\forall (c::'a)(s::'a seq). \neg(\forall i::nat. s i \noteq c) \\\n\\langle longrightarrow \rangle s(vpos c s) = c" by (metis (mono_tags, lifting) someI_ex vpos_def)

definition vpos :: "'a seq nat" where
"vpos c s = (SOME n::nat. (\exists i::nat. s i = c) \&\& s n = c)"

lemma S2 : "\forall (c::'a)(s::'a seq). \neg(\forall i::nat. s i \noteq c) \\\n\\langle longrightarrow \rangle s(vpos c s) = c"
by (metis (mono_tags, lifting) someI_ex vpos_def)

definition const :: "'a seq" where
"const s = (SOME c::'a. isconst c s)"

lemma S3: "\forall c::'a. const (cseq c) = c"
by (metis S1 const_def isconst_def someI_ex)
definition iscseq :: "'a seq \Rightarrow bool" where 
"iscseq s = (\exists c::'a. isconst c s)"

lemma S4: "\forall s::'a seq. iscseq s \longrightarrow (\forall i::nat. s i = const s)"
by (metis const_def isconst_def iscseq_def someI_ex)

definition addseq :: "('a::ring) seq \Rightarrow 'a seq" where 
"addseq s1 s2 = (\lambda i::nat. (s1 i) + (s2 i))"

lemma S5: "\forall (c1::'a::ring)(c2::'a::ring). iscseq(addseq (cseq c1) (cseq c2))"
by (simp add: addseq_def cseq_def isconst_def iscseq_def)
Isabelle/HOL Syntax: A Theory of Sets

type_synonym iset = "int set"

lemma U1: "\(\forall (a::iset)(b::iset)(c::iset). a \ union\ b \ inter\ c) = (a \ union\ b) \ inter\ (a \ union\ c)" by auto

lemma U2: "\(\forall (a::iset)(b::iset). a \ subseteq\ b \longrightarrow a \ union\ b = b)" by auto

lemma U3: "\(\forall (a::iset)(b::iset). a \ inter\ b \ noteq\ \{} \longrightarrow a - b \ subset\ a)" by blast

definition notempty :: "iset \ Rightarrow\ bool" where "notempty s = (\{x::int. x \ in\ s\})"

definition ints :: "int \ Rightarrow\ int \ Rightarrow\ iset" where "ints n m = \{i::int. n \ le\ i \ and\ i \ le\ m\}"

lemma L1: "\(\forall (n::int)(m::int). n \ le\ m \longrightarrow notempty (ints n m))" using notempty_def ints_def by auto
(* adding an integer to a set *)
definition add :: "int \<Rightarrow> iset \<Rightarrow> iset" where
"add i s = { (i+x) | (x::int). x \<in> s }"

(* some lemmas about adding an integer to a set *)
lemma L2: "\forall(i::int). add 0 s = s"
by (simp add: add_def)
lemma L3: "\forall(s::iset)(i::int)(x::int). x \<in> (add i s)
\longleftarrow x-i \<in> s"
using add_def by force
lemma L4: "\forall(s::iset)(i::int)(j::int). add i (add j s) = add (i+j) s"
by (smt Collect_cong L3 add_def mem_Collect_eq)
definition ismax :: "int \(\rightarrow\) iset \(\rightarrow\) bool" where  
ismax m s = (m \in s \&\& (\forall x::int. x \in s \rightarrow x \leq m))

definition hasmax :: "iset \(\rightarrow\) bool" where  
hasmax s = (\exists m::int. ismax m s)

definition max :: "iset \(\rightarrow\) int" where  
max s = (SOME (m::int). ismax m s)

lemma M1: "\forall (s::iset). hasmax s \rightarrow max s \in s \&\& (\forall x::int. x \in s \rightarrow x \leq max s)"
by (metis hasmax_def ismax_def models.max_def someI_ex)

lemma M2: "\forall (s::iset). hasmax s \rightarrow (\forall x::int. x \in s \&\& x \neq max s \rightarrow x < max s)"
using M1 by fastforce

lemma M3: "\forall (s::iset). hasmax s \&\& hasmax(s - { max s }) \rightarrow max s > max (s - { max s })"
using M1 M2 by blast

All proofs can be found by automatic proof search.
Isar Proofs

Theorem \( \sqrt{2} \notin \mathbb{Q} \) formalized and checked by Isabelle.

A reasonably understandable argument that \( \sqrt{2} \notin \mathbb{Q} \), formally checked by Isabelle.