Automated Reasoning for Systems Engineering

Laura Kovács
Vienna University of Technology
Future and Our Motivation

1. **Automated reasoning**, in particular **theorem proving** will remain central in software verification and program analysis. The role of theorem proving in these areas will be growing.

2. Theorem provers will be used by a large number of users who do not understand theorem proving and by users with very elementary knowledge of logic.

3. Reasoning with both quantifiers and theories will remain the main challenge in practical applications of theorem proving (at least) for the next decade.

4. Theorem provers will be used in reasoning with very large theories. These theories will appear in knowledge mining and natural language processing.
Future and Our Motivation

1. **Automated reasoning**, in particular theorem proving will remain central in software verification and program analysis. The role of theorem proving in these areas will be growing.

2. Theorem provers will be used by a large number of users who do not understand theorem proving and by users with very elementary knowledge of logic.

3. Reasoning with both quantifiers and theories will remain the main challenge in practical applications of theorem proving (at least) for the next decade.

4. Theorem provers will be used in reasoning with very large theories. These theories will appear in knowledge mining and natural language processing.
Future and Our Motivation

1. **Automated reasoning**, in particular theorem proving will remain central in software verification and program analysis. The role of theorem proving in these areas will be growing.

2. Theorem provers will be used by a large number of users who do not understand theorem proving and by users with very elementary knowledge of logic.

3. Reasoning with both quantifiers and theories will remain the main challenge in practical applications of theorem proving (at least) for the next decade.

4. Theorem provers will be used in reasoning with very large theories. These theories will appear in knowledge mining and natural language processing.
1. **Automated reasoning**, in particular **theorem proving** will remain central in software verification and program analysis. The role of theorem proving in these areas will be growing.

2. Theorem provers will be used by a large number of **users who do not understand theorem proving** and by users with very elementary knowledge of logic.

3. Reasoning with both **quantifiers and theories** will remain the main challenge in practical applications of theorem proving (at least) for the next decade.

4. Theorem provers will be used in reasoning with **very large theories**. These theories will appear in knowledge mining and natural language processing.
Outline

Automated Theorem Proving - An Overview

Challenges of Automated Theorem Proving
Group theory theorem: if a group satisfies the identity $x^2 = 1$, then it is commutative.
First-Order Theorem Proving. Example

Group theory theorem: if a group satisfies the identity $x^2 = 1$, then it is commutative.
More formally: in a group “assuming that $x^2 = 1$ for all $x$ prove that $x \cdot y = y \cdot x$ holds for all $x, y$.”
First-Order Theorem Proving. Example

Group theory theorem: if a group satisfies the identity $x^2 = 1$, then it is commutative.
More formally: in a group “assuming that $x^2 = 1$ for all $x$ prove that $x \cdot y = y \cdot x$ holds for all $x, y$.”
What is implicit: axioms of the group theory.

\[
\forall x (1 \cdot x = x) \\
\forall x (x^{-1} \cdot x = 1) \\
\forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))
\]
Formulation in First-Order Logic

Axioms (of group theory):
\[ \forall x (1 \cdot x = x) \]
\[ \forall x (x^{-1} \cdot x = 1) \]
\[ \forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z)) \]

Assumptions:
\[ \forall x (x \cdot x = 1) \]

Conjecture:
\[ \forall x \forall y (x \cdot y = y \cdot x) \]
In the TPTP Syntax

The TPTP library (Thousands of Problems for Theorem Provers), http://www.tptp.org contains a large collection of first-order problems. For representing these problems it uses the TPTP syntax, which is understood by all modern theorem provers, including our Vampire prover.
In the TPTP Syntax

The TPTP library (Thousands of Problems for Theorem Provers), http://www.tptp.org contains a large collection of first-order problems. For representing these problems it uses the TPTP syntax, which is understood by all modern theorem provers, including our Vampire prover.

<table>
<thead>
<tr>
<th>First-Order Logic (FOL)</th>
<th>TPTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bot, \top$</td>
<td>$false, true$</td>
</tr>
<tr>
<td>$\neg F$</td>
<td>$\sim F$</td>
</tr>
<tr>
<td>$F_1 \land \ldots \land F_n$</td>
<td>$F_1 &amp; \ldots &amp; F_n$</td>
</tr>
<tr>
<td>$F_1 \lor \ldots \lor F_n$</td>
<td>$F_1 \mid \ldots \mid F_n$</td>
</tr>
<tr>
<td>$F_1 \rightarrow F_n$</td>
<td>$F_1 \Rightarrow F_n$</td>
</tr>
<tr>
<td>$(\forall x_1) \ldots (\forall x_n) F$</td>
<td>$! [x_1,\ldots,x_n] : F$</td>
</tr>
<tr>
<td>$(\exists x_1) \ldots (\exists x_n) F$</td>
<td>$? [x_1,\ldots,x_n] : F$</td>
</tr>
</tbody>
</table>
%---- 1 * x = x
fof(left_identity,axiom,(  
  ! [X] : mult(e,X) = X )).

%---- i(x) * x = 1
fof(left_inverse,axiom,(  
  ! [X] : mult(inverse(X),X) = e )).

%---- (x * y) * z = x * (y * z)
fof(associativity,axiom,(  
  ! [X,Y,Z] :  
    mult(mult(X,Y),Z) = mult(X,mult(Y,Z)) )).

%---- x * x = 1
fof(group_of_order_2,hypothesis,  
  ! [X] : mult(X,X) = e ).

%---- prove x * y = y * x
fof(commutativity,conjecture,  
  ! [X,Y] : mult(X,Y) = mult(Y,X) ).
Example in the TPTP Syntax

Comments:

%---- 1 * x = x
fof(left_identity,axiom,(        
    ! [X] : mult(e,X) = X )).
%---- i(x) * x = 1
fof(left_inverse,axiom,(        
    ! [X] : mult(inverse(X),X) = e )).
%---- (x * y) * z = x * (y * z)
fof(associativity,axiom,(        
    ! [X,Y,Z] :    
        mult(mult(X,Y),Z) = mult(X,mult(Y,Z)) )).
%---- x * x = 1
fof(group_of_order_2,hypothesis,           
    ! [X] : mult(X,X) = e ).
%---- prove x * y = y * x
fof(commutativity,conjecture,            
    ! [X,Y] : mult(X,Y) = mult(Y,X) ).
Example in the TPTP Syntax

- Comments;
- Input formula names;

%---- 1 * x = x
fof(left_identity, axiom, (
  ! [X] : mult(e, X) = X ))).

%---- i(x) * x = 1
fof(left_inverse, axiom, (
  ! [X] : mult(inverse(X), X) = e ))).

%---- (x * y) * z = x * (y * z)
fof(associativity, axiom, (  
  ! [X, Y, Z] : 
    mult(mult(X, Y), Z) = mult(X, mult(Y, Z)) )).

%---- x * x = 1
fof(group_of_order_2, hypothesis, 
  ! [X] : mult(X, X) = e ).

%---- prove x * y = y * x
fof(commutativity, conjecture, 
  ! [X, Y] : mult(X, Y) = mult(Y, X )).
Example in the TPTP Syntax

- Comments;
- Input formula names;
- Input formula roles (very important);

%---- 1 * x = x
fof(left_identity,axiom,(  
    ! [X] : mult(e,X) = X ).
)

%---- i(x) * x = 1
fof(left_inverse,axiom,(  
    ! [X] : mult(inverse(X),X) = e ).
)

%---- (x * y) * z = x * (y * z)
fof(associativity,axiom,(  
    ! [X,Y,Z] :  
        mult(mult(X,Y),Z) = mult(X,mult(Y,Z)) ).
)

%---- x * x = 1
fof(group_of_order_2,hypothesis,  
    ! [X] : mult(X,X) = e ).

%---- prove x * y = y * x
fof(commutativity,conjecture,  
    ! [X,Y] : mult(X,Y) = mult(Y,X) ).
Example in the TPTP Syntax

- **Comments**;
- **Input formula names**;
- **Input formula roles** *(very important)*;
- **Equality**

%---- 1 * x = x
fof(left_identity,axiom,( ! [X] : mult(e,X) = X )).

%---- i(x) * x = 1
fof(left_inverse,axiom,( ! [X] : mult(inverse(X),X) = e )).

%---- (x * y) * z = x * (y * z)
fof(associativity,axiom,( ! [X,Y,Z] :
    mult(mult(X,Y),Z) = mult(X,mult(Y,Z)) )).

%---- x * x = 1
fof(group_of_order_2,hypothesis,
    ! [X] : mult(X,X) = e ).

%---- prove x * y = y * x
fof(commutativity,conjecture,
    ! [X,Y] : mult(X,Y) = mult(Y,X) ).
Running a Theorem Prover on a TPTP file

is easy: for example

vampire <filename>
is easy: for example

vampire <filename>

One can also run Vampire with various options. For example, save the group theory problem in a file group.tptp and try

vampire group.tptp
Running a Theorem Prover on a TPTP file

is easy: for example

\texttt{vampire <filename>}

One can also run Vampire with various \texttt{options}. For example, save the group theory problem in a file \texttt{group.tptp} and try

\texttt{vampire --thanks ECSS group.tptp}
Proof by Vampire (Slightly Modified)

Refutation found.

270. $false$ [trivial inequality removal 269]
269. $\text{mult}(sk0, sk1) \neq \text{mult}(sk0, sk1)$ [superposition 14, 125]
125. $\text{mult}(x2, x3) = \text{mult}(x3, x2)$ [superposition 21, 90]
90. $\text{mult}(x4, \text{mult}(x3, x4)) = x3$ [forward demodulation 75, 27]
75. $\text{mult}(\text{inverse}(x3), e) = \text{mult}(x4, \text{mult}(x3, x4))$ [superposition 22, 19]
27. $\text{mult}(\text{inverse}(x2), e) = x2$ [superposition 21, 11]
22. $\text{mult}(\text{inverse}(x4), \text{mult}(x4, x5)) = x5$ [forward demodulation 17, 10]
21. $\text{mult}(x0, \text{mult}(x0, x1)) = x1$ [forward demodulation 15, 10]
19. $e = \text{mult}(x0, \text{mult}(x1, \text{mult}(x0, x1)))$ [superposition 12, 13]
17. $\text{mult}(e, x5) = \text{mult}(\text{inverse}(x4), \text{mult}(x4, x5))$ [superposition 12, 11]
15. $\text{mult}(e, x1) = \text{mult}(x0, \text{mult}(x0, x1))$ [superposition 12, 13]
14. $\text{mult}(sk0, sk1) \neq \text{mult}(sk1, sk0)$ [cnf transformation 9]
13. $e = \text{mult}(x0, x0)$ [cnf transformation 4]
12. $\text{mult}(x0, \text{mult}(x1, x2)) = \text{mult}(\text{mult}(x0, x1), x2)$ [cnf transformation 3]
11. $e = \text{mult}(\text{inverse}(x0), x0)$ [cnf transformation 2]
10. $\text{mult}(e, x0) = x0$ [cnf transformation 1]
9. $\text{mult}(sk0, sk1) \neq \text{mult}(sk1, sk0)$ [skolemisation 7, 8]
8. $\exists[x0, x1]: \text{mult}(x0, x1) \neq \text{mult}(x1, x0) \iff \text{mult}(sk0, sk1) \neq \text{mult}(sk1, sk0)$ [choice axiom]
7. $\exists[x0, x1]: \text{mult}(x0, x1) \neq \text{mult}(x1, x0)$ [ennf transformation 6]
6. $\neg \exists[x0, x1]: \text{mult}(x0, x1) = \text{mult}(x1, x0)$ [negated conjecture 5]
5. $\exists[x0, x1]: \text{mult}(x0, x1) = \text{mult}(x1, x0)$ [input]
4. $\exists[x0]: e = \text{mult}(x0, x0)$ [input]
3. $\exists[x0, x1, x2]: \text{mult}(x0, \text{mult}(x1, x2)) = \text{mult}(\text{mult}(x0, x1), x2)$ [input]
2. $\exists[x0]: e = \text{mult}(\text{inverse}(x0), x0)$ [input]
1. $\exists[x0]: \text{mult}(e, x0) = x0$ [input]
Proof by Vampire (Slightly Modified)

Refutation found.

270. $false$ [trivial inequality removal 269]
269. mult(sk0,sk1) != mult(sk0,sk1) [superposition 14,125]
125. mult(X2,X3) = mult(X3,X2) [superposition 21,90]
90. mult(X4,mult(X3,X4)) = X3 [forward demodulation 75,27]
75. mult(inverse(X3),e) = mult(X4,mult(X3,X4)) [superposition 22,19]
27. mult(inverse(X2),e) = X2 [superposition 21,11]
22. mult(inverse(X4),mult(X4,X5)) = X5 [forward demodulation 17,10]
21. mult(X0,mult(X0,X1)) = X1 [forward demodulation 15,10]
19. e = mult(X0,mult(X1,mult(X0,X1))) [superposition 12,13]
17. mult(e,X5) = mult(inverse(X4),mult(X4,X5)) [superposition 12,11]
15. mult(e,X1) = mult(X0,mult(X0,X1)) [superposition 12,13]
14. mult(sK0,sK1) != mult(sK1,sK0) [cnf transformation 9]
13. e = mult(X0,X0) [cnf transformation 4]
12. mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [cnf transformation 3]
11. e = mult(inverse(X0),X0) [cnf transformation 2]
10. mult(e,X0) = X0 [cnf transformation 1]
9. mult(sK0,sK1) != mult(sK1,sK0) [skolemisation 7,8]
8. ?[X0,X1]: mult(X0,X1) != mult(X1,X0) <=> mult(sK0,sK1) != mult(sK1,sK0) [choice axiom]
7. ?[X0,X1]: mult(X0,X1) != mult(X1,X0) [ennf transformation 6]
6. ![X0,X1]: mult(X0,X1) = mult(X1,X0) [negated conjecture 5]
5. ![X0,X1]: mult(X0,X1) = mult(X1,X0) [input]
4. ![X0]: e = mult(X0,X0) [input]
3. ![X0,X1,X2]: mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [input]
2. ![X0]: e = mult(inverse(X0),X0) [input]
1. ![X0]: mult(e,X0) = X0 [input]

Each inference derives a formula from zero or more other formulas;
Proof by Vampire (Slightly Modified)

Refutation found.

270. \textit{false } [trivial inequality removal 269]
269. \textit{mult} (sk0, sk1) \neq \textit{mult} (sk0, sk1) \textit{[superposition 14, 125]}
125. \textit{mult} (X2, X3) = \textit{mult} (X3, X2) \textit{[superposition 21, 90]}
90. \textit{mult} (X4, \textit{mult} (X3, X4)) = X3 \textit{[forward demodulation 75, 27]}
75. \textit{mult} (inverse(X3), e) = \textit{mult} (X4, \textit{mult} (X3, X4)) \textit{[superposition 22, 19]}
27. \textit{mult} (inverse(X2), e) = X2 \textit{[superposition 21, 11]}
22. \textit{mult} (inverse(X4), \textit{mult} (X4, X5)) = X5 \textit{[forward demodulation 17, 10]}
21. \textit{mult} (X0, \textit{mult} (X0, X1)) = X1 \textit{[forward demodulation 15, 10]}
19. e = \textit{mult} (X0, \textit{mult} (X1, \textit{mult} (X0, X1))) \textit{[superposition 12, 13]}
17. \textit{mult} (e, X5) = \textit{mult} (\textit{inverse}(X4), \textit{mult} (X4, X5)) \textit{[superposition 12, 11]}
15. \textit{mult} (e, X1) = \textit{mult} (X0, \textit{mult} (X0, X1)) \textit{[superposition 12, 13]}
14. \textit{mult} (sk0, sk1) \neq \textit{mult} (sk1, sk0) \textit{[cnf transformation 9]}
13. e = \textit{mult} (X0, X0) \textit{[cnf transformation 4]}
12. \textit{mult} (X0, \textit{mult} (X1, X2)) = \textit{mult} (\textit{mult} (X0, X1), X2) \textit{[cnf transformation 3]}
11. e = \textit{mult} (\textit{inverse}(X0), X0) \textit{[cnf transformation 2]}
10. \textit{mult} (e, X0) = X0 \textit{[cnf transformation 1]}
9. \textit{mult} (sk0, sk1) \neq \textit{mult} (sk1, sk0) \textit{[skolemisation 7, 8]}
8. ?[X0, X1]: \textit{mult} (X0, X1) \neq \textit{mult} (X1, X0) \textit{\textless\textgreater} \textit{mult} (sk0, sk1) \neq \textit{mult} (sk1, sk0) \textit{[choice axiom]}
7. ?[X0, X1]: \textit{mult} (X0, X1) \neq \textit{mult} (X1, X0) \textit{[ennf transformation 6]}
6. \neg ![X0, X1]: \textit{mult} (X0, X1) = \textit{mult} (X1, X0) \textit{[negated conjecture 5]}
5. ![X0, X1]: \textit{mult} (X0, X1) = \textit{mult} (X1, X0) \textit{[input]}
4. ![X0]: e = \textit{mult} (X0, X0) \textit{[input]}
3. ![X0, X1, X2]: \textit{mult} (X0, \textit{mult} (X1, X2)) = \textit{mult} (\textit{mult} (X0, X1), X2) \textit{[input]}
2. ![X0]: e = \textit{mult} (\textit{inverse}(X0), X0) \textit{[input]}
1. ![X0]: \textit{mult} (e, X0) = X0 \textit{[input]}

- Each inference derives a formula from zero or more other formulas;
- Input, preprocessing, new symbols introduction, superposition calculus
Proof by Vampire (Slightly Modified)

Refutation found.
270. $\text{false}$ [trivial inequality removal 269]
269. $\text{mult}(\text{sk0},\text{sk1}) \neq \text{mult}(\text{sk0},\text{sk1})$ [superposition 14, 125]
125. $\text{mult}(\text{X2},\text{X3}) = \text{mult}(\text{X3},\text{X2})$ [superposition 21, 90]
90. $\text{mult}(\text{X4},\text{mult}(\text{X3},\text{X4})) = \text{X3}$ [forward demodulation 75, 27]
75. $\text{mult}((\text{inverse}(\text{X3}),\text{e}) = \text{mult}(\text{X4},\text{mult}(\text{X3},\text{X4}))$ [superposition 22, 19]
27. $\text{mult}((\text{inverse}(\text{X2}),\text{e}) = \text{X2}$ [superposition 21, 11]
22. $\text{mult}(\text{inverse}(\text{X4}),\text{mult}(\text{X4},\text{X5})) = \text{X5}$ [forward demodulation 17, 10]
21. $\text{mult}(\text{X0},\text{mult}(\text{X0},\text{X1})) = \text{X1}$ [forward demodulation 15, 10]
19. $\text{e} = \text{mult}(\text{X0},\text{mult}(\text{X1},\text{mult}(\text{X0},\text{X1})))$ [superposition 12, 13]
17. $\text{mult}(\text{e},\text{X5}) = \text{mult}(\text{inverse}(\text{X4}),\text{mult}(\text{X4},\text{X5}))$ [superposition 12, 11]
15. $\text{mult}(\text{e},\text{X1}) = \text{mult}(\text{X0},\text{mult}(\text{X0},\text{X1}))$ [superposition 12, 13]
14. $\text{mult}(\text{sK0},\text{sK1}) \neq \text{mult}(\text{sK1},\text{sK0})$ [cnf transformation 9]
13. $\text{e} = \text{mult}(\text{X0},\text{X0})$ [cnf transformation 4]
12. $\text{mult}(\text{X0},\text{mult}(\text{X1},\text{X2})) = \text{mult}(\text{mult}(\text{X0},\text{X1}),\text{X2})$ [cnf transformation 3]
11. $\text{e} = \text{mult}(\text{inverse}(\text{X0}),\text{X0})$ [cnf transformation 2]
10. $\text{mult}(\text{e},\text{X0}) = \text{X0}$ [cnf transformation 1]
9. $\text{mult}(\text{sK0},\text{sK1}) \neq \text{mult}(\text{sK1},\text{sK0})$ [skolemisation 7, 8]
8. $\neg\neg\exists[\text{X0},\text{X1}]: \text{mult}(\text{X0},\text{X1}) \neq \text{mult}(\text{X1},\text{X0})$ [choice axiom]
7. $\exists[\text{X0},\text{X1}]: \text{mult}(\text{X0},\text{X1}) \neq \text{mult}(\text{X1},\text{X0})$ [ennf transformation 6]
6. $\neg\neg[\text{X0},\text{X1}]: \text{mult}(\text{X0},\text{X1}) = \text{mult}(\text{X1},\text{X0})$ [negated conjecture 5]
5. $\exists[\text{X0},\text{X1}]: \text{mult}(\text{X0},\text{X1}) = \text{mult}(\text{X1},\text{X0})$ [input]
4. $\exists[\text{X0}]: \text{e} = \text{mult}(\text{X0},\text{X0})$ [input]
3. $\exists[\text{X0},\text{X1},\text{X2}]: \text{mult}(\text{X0},\text{mult}(\text{X1},\text{X2})) = \text{mult}(\text{mult}(\text{X0},\text{X1}),\text{X2})$ [input]
2. $\exists[\text{X0}]: \text{e} = \text{mult}(\text{inverse}(\text{X0}),\text{X0})$ [input]
1. $\exists[\text{X0}]: \text{mult}(\text{e},\text{X0}) = \text{X0}$ [input]

▶ Each inference derives a formula from zero or more other formulas;
▶ Input, preprocessing, new symbols introduction, superposition calculus
Proof by Vampire (Slightly Modified)

Refutation found.

270. $false$ [trivial inequality removal 269]
269. mult(sk0,sk1) != mult(sk0,sk1) [superposition 14,125]
125. mult(X2,X3) = mult(X3,X2) [superposition 21,90]
90. mult(X4,mult(X3,X4)) = X3 [forward demodulation 75,27]
75. mult(inverse(X3),e) = mult(X4,mult(X3,X4)) [superposition 22,19]
27. mult(inverse(X2),e) = X2 [superposition 21,11]
22. mult(inverse(X4),mult(X4,X5)) = X5 [forward demodulation 17,10]
21. mult(X0,mult(X0,X1)) = X1 [forward demodulation 15,10]
19. e = mult(X0,mult(X1,mult(X0,X1))) [superposition 12,13]
17. mult(e,X5) = mult(inverse(X4),mult(X4,X5)) [superposition 12,11]
15. mult(e,X1) = mult(X0,mult(X0,X1)) [superposition 12,13]
14. mult(sk0,sk1) != mult(sk1,sk0) [cnf transformation 9]
13. mult(X0,X0) = X0 [cnf transformation 4]
12. mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [cnf transformation 3]
11. e = mult(inverse(X0),X0) [cnf transformation 2]
10. mult(e,X0) = X0 [cnf transformation 1]
9. mult(sk0,sk1) != mult(sk1,sk0) [skolemisation 7,8]
8. $?X0,X1$: mult(X0,X1) != mult(X1,X0) <=> mult(sk0,sk1) != mult(sk1,sk0) [choice axiom]
7. $?X0,X1$: mult(X0,X1) != mult(X1,X0) [ennf transformation 6]
6. $\neg$?X0,X1$: mult(X0,X1) = mult(X1,X0) [negated conjecture 5]
5. $?X0,X1$: mult(X0,X1) = mult(X1,X0) [input]
4. $?X0$: e = mult(X0,X0) [input]
3. $?X0,X1,X2$: mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [input]
2. $?X0$: e = mult(inverse(X0),X0) [input]
1. $?X0$: mult(e,X0) = X0 [input]

▶ Each inference derives a formula from zero or more other formulas;
▶ Input, preprocessing, new symbols introduction, superposition calculus
Refutation found.

270. $false$ [trivial inequality removal 269]  
269. mult(sk0,sk1) != mult(sk0,sk1) [superposition 14, 125]  
125. mult(X2,X3) = mult(X3,X2) [superposition 21, 90]  
90. mult(X4,mult(X3,X4)) = X3 [forward demodulation 75, 27]  
75. mult(inverse(X3),e) = mult(X4,mult(X3,X4)) [superposition 22, 19]  
27. mult(inverse(X2),e) = X2 [superposition 21, 11]  
22. mult(inverse(X4),mult(X4,X5)) = X5 [forward demodulation 17, 10]  
21. mult(X0,mult(X0,X1)) = X1 [forward demodulation 15, 10]  
19. e = mult(X0,mult(X1,mult(X0,X1))) [superposition 12, 13]  
17. mult(e,X5) = mult(inverse(X4),mult(X4,X5)) [superposition 12, 11]  
15. mult(e,X1) = mult(X0,mult(X0,X1)) [superposition 12, 13]  
14. mult(sK0,sK1) != mult(sK1,sK0) [cnf transformation 9]  
13. e = mult(X0,X0) [cnf transformation 4]  
12. mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [cnf transformation 3]  
11. e = mult(inverse(X0),X0) [cnf transformation 2]  
10. mult(e,X0) = X0 [cnf transformation 1]  
9. mult(sK0,sK1) != mult(sK1,sK0) [skolemisation 7, 8]  
8. $?[X0,X1]: mult(X0,X1) != mult(X1,X0) <=> mult(sK0,sK1) != mult(sK1,sK0)$  
[choice axiom]  
7. $?[X0,X1]: mult(X0,X1) != mult(X1,X0)$ [ennf transformation 6]  
6. !?[X0,X1]: mult(X0,X1) = mult(X1,X0) [negated conjecture 5]  
5. !?[X0,X1]: mult(X0,X1) = mult(X1,X0) [input]  
4. !?[X0]: e = mult(X0,X0) [input]  
3. !?[X0,X1,X2]: mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [input]  
2. !?[X0]: e = mult(inverse(X0),X0) [input]  
1. !?[X0]: mult(e,X0) = X0 [input]  

▶ Each inference derives a formula from zero or more other formulas;  
▶ Input, preprocessing, new symbols introduction, superposition calculus
Refutation found.

270. $false$ [trivial inequality removal 269]
269. $\text{mult}(sk0,sk1) \neq \text{mult}(sk0,sk1)$ [superposition 14,125]
125. $\text{mult}(X2,X3) = \text{mult}(X3,X2)$ [superposition 21,90]
90. $\text{mult}(X4,\text{mult}(X3,X4)) = X3$ [forward demodulation 75,27]
75. $\text{mult}(\text{inverse}(X3),e) = \text{mult}(X4,\text{mult}(X3,X4))$ [superposition 22,19]
27. $\text{mult}(\text{inverse}(X2),e) = X2$ [superposition 21,11]
22. $\text{mult}(\text{inverse}(X4),\text{mult}(X4,X5)) = X5$ [forward demodulation 17,10]
21. $\text{mult}(X0,\text{mult}(X0,X1)) = X1$ [forward demodulation 15,10]
19. $e = \text{mult}(X0,\text{mult}(X1,\text{mult}(X0,X1)))$ [superposition 12,13]
17. $\text{mult}(e,X5) = \text{mult}(\text{inverse}(X4),\text{mult}(X4,X5))$ [superposition 12,11]
15. $\text{mult}(e,X1) = \text{mult}(X0,\text{mult}(X0,X1))$ [superposition 12,13]
14. $\text{mult}(sK0,sK1) \neq \text{mult}(sK1,sK0)$ [cnf transformation 9]
13. $e = \text{mult}(X0,X0)$ [cnf transformation 4]
12. $\text{mult}(X0,\text{mult}(X1,X2)) = \text{mult}(\text{mult}(X0,X1),X2)$ [cnf transformation 3]
11. $e = \text{mult}(\text{inverse}(X0),X0)$ [cnf transformation 2]
10. $\text{mult}(e,X0) = X0$ [cnf transformation 1]
9. $\text{mult}(sK0,sK1) \neq \text{mult}(sK1,sK0)$ [skolemisation 7,8]
8. $?[X0,X1]: \text{mult}(X0,X1) \neq \text{mult}(X1,X0) \iff \text{mult}(sK0,sK1) \neq \text{mult}(sK1,sK0)$ [choice axiom]
7. $?[X0,X1]: \text{mult}(X0,X1) \neq \text{mult}(X1,X0)$ [ennf transformation 6]
6. $\neg ![X0,X1]: \text{mult}(X0,X1) = \text{mult}(X1,X0)$ [negated conjecture 5]
5. ![X0,X1]: $\text{mult}(X0,X1) = \text{mult}(X1,X0)$ [input]
4. ![X0]: $e = \text{mult}(X0,X0)$ [input]
3. ![X0,X1,X2]: $\text{mult}(X0,\text{mult}(X1,X2)) = \text{mult}(\text{mult}(X0,X1),X2)$ [input]
2. ![X0]: $e = \text{mult}(\text{inverse}(X0),X0)$ [input]
1. ![X0]: $\text{mult}(e,X0) = X0$ [input]

- Each inference derives a formula from zero or more other formulas;
- Input, preprocessing, new symbols introduction, superposition calculus
- Proof by refutation, generating and simplifying inferences, unused formulas . . .
Proof by Vampire (Slightly Modified)

Refutation found.
270. $false$ [trivial inequality removal 269]
269. mult(sk0,sk1) != mult(sk0,sk1) [superposition 14,125]
125. mult(X2,X3) = mult(X3,X2) [superposition 21,90]
90. mult(X4,mult(X3,X4)) = X3 [forward demodulation 75,27]
75. mult(inverse(X3),e) = mult(X4,mult(X3,X4)) [superposition 22,19]
27. mult(inverse(X2),e) = X2 [superposition 21,11]
22. mult(inverse(X4),mult(X4,X5)) = X5 [forward demodulation 17,10]
21. mult(X0,mult(X0,X1)) = X1 [forward demodulation 15,10]
19. e = mult(X0,mult(X1,mult(X0,X1))) [superposition 12,13]
17. mult(e,X5) = mult(inverse(X4),mult(X4,X5)) [superposition 12,11]
15. mult(e,X1) = mult(X0,mult(X0,X1)) [superposition 12,13]
14. mult(sK0,sK1) != mult(sK1,sK0) [cnf transformation 9]
13. e = mult(X0,X0) [cnf transformation 4]
12. mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [cnf transformation 3]
11. e = mult(inverse(X0),X0) [cnf transformation 2]
10. mult(e,X0) = X0 [cnf transformation 1]
9. mult(sK0,sK1) != mult(sK1,sK0) [skolemisation 7,8]
8. ![X0,X1]: mult(X0,X1) != mult(X1,X0) <=> mult(sK0,sK0) != mult(sK1,sK0) [choice axiom]
7. ![X0,X1]: mult(X0,X1) != mult(X1,X0) [ennf transformation 6]
6. ![X0,X1]: mult(X0,X1) = mult(X1,X0) [negated conjecture 5]
5. ![X0,X1]: mult(X0,X1) = mult(X1,X0) [input]
4. ![X0]: e = mult(X0,X0) [input]
3. ![X0,X1,X2]: mult(X0,mult(X1,X2)) = mult(mult(X0,X1),X2) [input]
2. ![X0]: e = mult(inverse(X0),X0) [input]
1. ![X0]: mult(e,X0) = X0 [input]

- Each inference derives a formula from zero or more other formulas;
- Input, preprocessing, new symbols introduction, superposition calculus
- Proof by refutation, generating and simplifying inferences, unused formulas ...
Proof by Vampire (Slightly Modified)

Refutation found.

270. \$false \ [trivial inequality removal 269]
269. \text{mult}(sk0, sk1) \neq \text{mult}(sk0, sk1) \ [superposition 14, 125]
125. \text{mult}(X2, X3) = \text{mult}(X3, X2) \ [superposition 21, 90]
90. \text{mult}(X4, \text{mult}(X3, X4)) = X3 \ [forward demodulation 75, 27]
75. \text{mult} (\text{inverse}(X3), e) = \text{mult}(X4, \text{mult}(X3, X4)) \ [superposition 22, 19]
27. \text{mult} (\text{inverse}(X2), e) = X2 \ [superposition 21, 11]
22. \text{mult} (\text{inverse}(X4), \text{mult}(X4, X5)) = X5 \ [forward demodulation 17, 10]
21. \text{mult}(X0, \text{mult}(X0, X1)) = X1 \ [forward demodulation 15, 10]
19. e = \text{mult}(X0, \text{mult}(X1, \text{mult}(X0, X1))) \ [superposition 12, 13]
17. \text{mult}(e, X5) = \text{mult}(\text{inverse}(X4), \text{mult}(X4, X5)) \ [superposition 12, 11]
15. \text{mult}(e, X1) = \text{mult}(X0, \text{mult}(X0, X1)) \ [superposition 12, 13]
14. \text{mult}(sk0, sk1) \neq \text{mult}(sk1, sk0) \ [cnf transformation 9]
13. e = \text{mult}(X0, X0) \ [cnf transformation 4]
12. \text{mult}(X0, \text{mult}(X1, X2)) = \text{mult}(\text{mult}(X0, X1), X2) \ [cnf transformation 3]
11. e = \text{mult}(\text{inverse}(X0), X0) \ [cnf transformation 2]
10. \text{mult}(e, X0) = X0 \ [cnf transformation 1]
9. \text{mult}(sk0, sk1) \neq \text{mult}(sk1, sk0) \ [skolemisation 7, 8]
8. ?[X0, X1]: \text{mult}(X0, X1) \neq \text{mult}(X1, X0) \iff \text{mult}(sk0, sk1) \neq \text{mult}(sk1, sk0)
\ [choice axiom]
7. ?[X0, X1]: \text{mult}(X0, X1) \neq \text{mult}(X1, X0) \ [ennf transformation 6]
6. \neg ![X0, X1]: \text{mult}(X0, X1) = \text{mult}(X1, X0) \ [negated conjecture 5]
5. ![X0, X1]: \text{mult}(X0, X1) = \text{mult}(X1, X0) \ [input]
4. ![X0]: e = \text{mult}(X0, X0) \ [input]
3. ![X0, X1, X2]: \text{mult}(X0, \text{mult}(X1, X2)) = \text{mult}(\text{mult}(X0, X1), X2) \ [input]
2. ![X0]: e = \text{mult}(\text{inverse}(X0), X0) \ [input]
1. ![X0]: \text{mult}(e, X0) = X0 \ [input]

- Each inference derives a formula from zero or more other formulas;
- Input, preprocessing, new symbols introduction, superposition calculus
- Proof by refutation, generating and simplifying inferences, unused formulas ...
Vampire

- **Completely automatic:** once you started a proof attempt, it can only be interrupted by terminating the process.
Vampire

- Completely automatic: once you started a proof attempt, it can only be interrupted by terminating the process.

- Champion of the CASC world-cup in first-order theorem proving: won CASC 38 times.
What an Automated Theorem Prover is Expected to Do

Input:
▶ a set of axioms (first order formulas) or clauses;
▶ a conjecture (first-order formula or set of clauses).

Output:
▶ proof (hopefully).
Proof by Refutation

Given a problem with axioms and assumptions $F_1, \ldots, F_n$ and conjecture $G$,

1. negate the conjecture ($\neg G$);
2. establish unsatisfiability of the set of formulas $F_1, \ldots, F_n, \neg G$. 
Proof by Refutation

Given a problem with axioms and assumptions $F_1, \ldots, F_n$ and conjecture $G$,

1. negate the conjecture ($\neg G$);
2. establish unsatisfiability of the set of formulas $F_1, \ldots, F_n, \neg G$.

Thus, we reduce the theorem proving problem to the problem of checking unsatisfiability.
Proof by Refutation

Given a problem with axioms and assumptions $F_1, \ldots, F_n$ and conjecture $G$,

1. negate the conjecture ($\neg G$);
2. establish unsatisfiability of the set of formulas $F_1, \ldots, F_n, \neg G$.

Thus, we reduce the theorem proving problem to the problem of checking unsatisfiability.

In this formulation the negation of the conjecture $\neg G$ is treated like any other formula.

In fact, Vampire (and other provers) internally treat conjectures differently, to make proof search more goal-oriented.
General Scheme (simplified)

- Read a problem;
- Determine proof-search options to be used for this problem;
- Preprocess the problem;
- Convert it into a normal form (CNF);
- Run a saturation algorithm on it, try to derive false.
- If false is derived, report the result, maybe including a refutation.
General Scheme (simplified)

- Read a problem;
- Determine proof-search options to be used for this problem;
- Preprocess the problem;
- Convert it into a normal form (CNF);
- Run a saturation algorithm on it, try to derive \textit{false}.
- If \textit{false} is derived, report the result, maybe including a refutation.

Trying to derive \textit{false} using a saturation algorithm is the hardest part, which in practice may not terminate or run out of memory.
How to Establish Unsatisfiability?

Idea:

- Take a set of clauses $S$ (the search space), initially $S = S_0$.

  Repeatedly apply inferences to clauses in $S$ and add their conclusions to $S$, unless these conclusions are already in $S$.

- If, at any stage, we obtain false, we terminate and report unsatisfiability of $S_0$. 
Saturation Algorithms

search space
Saturation Algorithms

- given clause

search space
Saturation Algorithms

- given clause
- candidate clause
- search space
Saturation Algorithms

- **search space**
- **given clause**
- **candidate clause**
- **children**
Saturation Algorithms

- children
- search space
Saturation Algorithms

- children
- search space
Saturation Algorithms

search space
Saturation Algorithms

- given clause

search space
Saturation Algorithms

- given clause
- candidate clause
- search space
Saturation Algorithms

- Given clause
- Candidate clause
- Search space
- Children
Saturation Algorithms

children

search space
Saturation Algorithms

Search space

Children
Saturation Algorithms

search space
Saturation Algorithms

search space
Saturation Algorithms

MEMORY

search space
In practice there are three possible scenarios:

1. At some moment \textit{false} is generated, in this case the input set of clauses is unsatisfiable.

2. Saturation will terminate without ever generating \textit{false}, in this case the input set of clauses is satisfiable.

3. Saturation will run until we run out of resources, but without generating \textit{false}. In this case it is \textit{unknown} whether the input set is unsatisfiable.
In practice, saturation theorem provers implement:

- Preprocessing and CNF transformation;
- Superposition system;
- Orderings and selection functions;
- Fairness (saturation algorithms);
- Deletion and generation of clauses in the search space;
- Many, many proof options and strategies.
In practice, saturation theorem provers implement:

- Preprocessing and CNF transformation;
- Superposition system;
- Orderings and selection functions;
- Fairness (saturation algorithms);
- Deletion and generation of clauses in the search space;
- Many, many proof options and strategies.
In practice, saturation theorem provers implement:

- Preprocessing and CNF transformation;
- Superposition system;
- Orderings and selection functions;
- Fairness (saturation algorithms);
- Deletion and generation of clauses in the search space;
- Many, many proof options and strategies
  - example: limited resource strategy.
From Theory to Practice

In practice, saturation theorem provers implement:

- Preprocessing and CNF transformation;
- Superposition system;
- Orderings and selection functions;
- Fairness (saturation algorithms);
- Deletion and generation of clauses in the search space;
- Many, many proof options and strategies
  – example: limited resource strategy.

Try:

```
vampire --age_weight_ratio 10:1
   --time_limit 86400
GRP140-1.p
```
Outline

Automated Theorem Proving - An Overview

Challenges of Automated Theorem Proving
Automated Theorem Prover was Expected to Do

Input:
- a set of axioms (first order formulas) or clauses;
- a conjecture (first-order formula or set of clauses).

Output:
- proof (hopefully).
What an Automated Theorem Prover is Expected to Do

Input:

- a set of **axioms** (first order formulas) or clauses;
- a **conjecture** (first-order formula or set of clauses).

Output:

- readable **proof**;
- relevant **lemmas** extracted from proofs;
- **Craig interpolants** extracted from software safety proofs;
- **program analysis**;
- **invariant generation**;
- **inductive reasoning**;
- Reasoning with **first-order theories of data structures**;
- ...
Focus of my Research:
Automated Reasoning for Program Analysis
(ex. ~200kLoC, Vampire prover)
a=0, b=0, c=0;
while (a<n) do
  if A[a]>0 then B[b]=A[a]+h(b); b=b+1;
  else C[c]=A[a]; c=c+1;
  a=a+1;
end do
Focus of my Research:
Automated Reasoning for Program Analysis

Program property:

\((\forall p)(0 \leq p < b \Rightarrow \\
  (\exists q)(0 \leq q < a \land B[p] = A[q] + h(p) \land A[q] > 0))\)

```plaintext
a=0, b=0, c=0;
while (a<n) do
  if A[a] > 0 then B[b] = A[a] + h(b); b = b+1;
    else C[c] = A[a]; c = c+1;
  a = a+1;
end do
```
cnt=0, fib1=1, fib2=0;
while (cnt<n) do
  t=fib1; fib1=fib1+fib2; fib2=t; cnt++;
end do

a=0, b=0, c=0;
while (a<n) do
  if A[a]>0 then B[b]=A[a]+h(b); b=b+1;
  else C[c]=A[a]; c=c+1;
  a=a+1;
end do

Focus of my Research:
Automated Reasoning for Program Analysis
Focus of my Research:
Automated Reasoning for Program Analysis

```plaintext
a=0, b=0, c=0;
while (a<n) do
if A[a]>0 then B[b]=A[a]+h(b); b=b+1;
else C[c]=A[a]; c=c+1;
a=a+1;
end do

b=1, c=0;
while (cnt<n) do
    t=fib1; fib1=fib1+fib2; fib2=t; cnt++;
end do

cnt=0, fib1=1, fib2=0;
while (cnt<n) do
    t=fib1; fib1=fib1+fib2; fib2=t; cnt++;
end do

Program property:
fib1^4 + fib2^4 + 2*fib1*fib2^3 - 2*fib1^3*fib2 - fib1^2*fib2^2 - 1 = 0
```
Focus of my Research:
Automated Reasoning for Program Analysis

cnt=0, fib1=1, fib2=0;
while (cnt<n) do
  t=fib1; fib1=fib1+fib2; fib2=t; cnt++;
end do

fib1^4 + fib2^4 + 2*fib1*fib2^3 - 2*fib1^3*fib2 - fib1^2*fib2^2 - 1 = 0

(∀p)(0≤p<b ⇒
My Research

Math

Logic

Vampire prover

Program Analysis