Checking Unsatisfiability

Theorem:
Unsatisfiability of finite sets of first-order formulas (or clauses) is **undecidable**.

Theorem:
Unsatisfiability of finite sets of first-order formulas (or clauses) is **recursively enumerable**.

Proposition:
The **resolution calculus** and the **tableaux calculus** are sound and refutationally complete **semi-decision procedures** for unsatisfiability of finite sets of first-order clauses without equality.
Handling Equality Naively

Proposition:
Let $F$ be a closed first-order formula with equality. Let $\varnothing \notin \Omega$ be a new predicate symbol. The set $Eq(\Sigma)$ contains the formulas

$$
\forall x (x \sim x)
$$
$$
\forall x, y (x \sim y \rightarrow y \sim x)
$$
$$
\forall x, y, z (x \sim y \land y \sim z \rightarrow x \sim z)
$$
$$
\forall \vec{x}, \vec{y} (x_1 \sim y_1 \land \cdots \land x_n \sim y_n \rightarrow f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n))
$$
$$
\forall \vec{x}, \vec{y} (x_1 \sim y_1 \land \cdots \land x_n \sim y_n \land p(x_1, \ldots, x_n) \rightarrow p(y_1, \ldots, y_n))
$$

for every $f/n \in \Omega$ and $p/n \in \Pi$. Let $\tilde{F}$ be the formula that one obtains from $F$ if every occurrence of $\approx$ is replaced by $\sim$. Then $F$ is satisfiable if and only if $Eq(\Sigma) \cup \{\tilde{F}\}$ is satisfiable.
Handling Equality Naively

By giving the equality axioms explicitly, first-order problems with equality can in principle be solved by a standard resolution or tableaux prover.

But this is unfortunately not efficient (mainly due to the transitivity and congruence axioms).
Roadmap

How to proceed:

1. Arbitrary binary relations.
2. Term rewrite systems.
3. Expressing semantic consequence syntactically.
4. Entailment for equations (unit clauses).
5. Entailment for equational clauses.
2 Abstract Reduction Systems
Abstract Reduction Systems

Abstract reduction system: \((A, \rightarrow)\), where

\[ A \text{ is a set,} \]
\[ \rightarrow \subseteq A \times A \text{ is a binary relation on } A. \]
Abstract Reduction Systems

$\rightarrow^0 = \{ (x, x) \mid x \in A \}$  
identity

$\rightarrow^{i+1} = \rightarrow^i \circ \rightarrow$  
$i + 1$-fold composition

$\rightarrow^+ = \bigcup_{i>0} \rightarrow^i$  
transitive closure

$\rightarrow^* = \rightarrow^+ \cup \rightarrow^0$  
reflexive transitive closure

$\rightarrow^=$  
reflexive closure

$\rightarrow^{-1} = \leftarrow = \{ (x, y) \mid y \rightarrow x \}$  
inverse

$\leftrightarrow = \rightarrow \cup \leftarrow$  
symmetric closure

$\leftrightarrow^+ = (\leftrightarrow)^+$  
transitive symmetric closure

$\leftrightarrow^* = (\leftrightarrow)^*$  
refl. trans. symmetric closure
Abstract Reduction Systems

\( x \in A \) is reducible, if there is a \( y \) such that \( x \rightarrow y \).

\( x \) is in normal form (irreducible), if it is not reducible.

\( y \) is a normal form of \( x \), if \( x \rightarrow^* y \) and \( y \) is in normal form.
Notation: \( x \downarrow \) (if the normal form of \( x \) is uniquely determined).

\( x \) and \( y \) are joinable, if there is a \( z \) such that \( x \rightarrow^* z \leftarrow^* y \).
Notation: \( x \downarrow y \).
Abstract Reduction Systems

A relation $\rightarrow$ is called

Church-Rosser, if $x \leftrightarrow^* y$ implies $x \downarrow y$.

confluent, if $x \leftarrow^* z \rightarrow^* y$ implies $x \downarrow y$.

locally confluent, if $x \leftarrow z \rightarrow y$ implies $x \downarrow y$.

terminating, if there is no infinite decreasing chain $x_0 \rightarrow x_1 \rightarrow x_2 \rightarrow \ldots$.

normalizing, if every $x \in A$ has a normal form.

convergent, if it is confluent and terminating.
Abstract Reduction Systems

Lemma:
If $\rightarrow$ is terminating, then it is normalizing.

Note: The reverse implication does not hold.
Abstract Reduction Systems

Theorem:
The following properties are equivalent:

(i) \( \rightarrow \) has the Church-Rosser property.

(ii) \( \rightarrow \) is confluent.

Proof:
(i) \( \Rightarrow \) (ii): trivial.

(ii) \( \Rightarrow \) (i): by induction on the number of peaks in
the derivation \( x \leftrightarrow^* y \).
Abstract Reduction Systems

Lemma:
If $\rightarrow$ is confluent, then every element has at most one normal form.

Corollary:
If $\rightarrow$ is normalizing and confluent, then every element $x$ has a unique normal form.

Theorem:
If $\rightarrow$ is normalizing and confluent, then $x \leftrightarrow^* y$ if and only if $x \downarrow = y \downarrow$. 
Well-Founded Orderings

A (strict) partial ordering \((A, >)\) is a transitive and irreflexive binary relation on \(A\).

A (strict) partial ordering \(>\) is called well-founded (Noetherian), if there is no infinite decreasing chain \(x_0 > x_1 > x_2 > \ldots\).
Well-Founded Orderings

Lemma:
If $\rightarrow$ is a terminating binary relation over $A$, then $\rightarrow^+$ is a well-founded partial ordering.

Lemma:
If $>$ is a well-founded partial ordering and $\rightarrow \subseteq >$, then $\rightarrow$ is terminating.
Proposition: 
\((A, >)\) is well-founded, if and only if every non-empty subset of \(A\) has a minimal element.

Proof: 
If \((A, >)\) is not well-founded, then there exists an infinite decreasing chain \(x_0 > x_1 > x_2 > \ldots\). 
Then \(\{x_i \mid i \in \mathbb{N}\}\) does not have a minimal element.

Conversely, if there exists a non-empty subset \(B \subseteq A\) without minimal element, then for every \(x \in B\) there exists a smaller \(y \in B\). 
Hence there is an infinite decreasing chain of elements of \(B\).
Well-Founded Orderings

Theorem ("Well-founded induction principle"): Let \((A, >)\) be a well-founded partial ordering; let \(P\) be a unary predicate on \(A\).

If for all \(x \in A\) the following property holds:

\[
\text{if } P(y) \text{ for all } y < x, \text{ then } P(x) \quad (\ast)
\]

then \(P(x)\) for all \(x \in A\).

Proof:
Assume that \(B = \{ x \in A \mid \neg P(x) \}\) is not empty.
Since \(>\) is well-founded, \(B\) has a minimal element.
This element violates \((\ast)\).
Lemma ("Newman’s Lemma"):
If a terminating relation $\rightarrow$ is locally confluent, then it is confluent.

Proof:
Let $\rightarrow$ be a terminating and locally confluent relation. Then $\rightarrow^+$ is a well-founded ordering.
Define $P(z) \iff (\forall x, y : x \leftarrow^* z \rightarrow^* y \Rightarrow x \downarrow y)$.
Prove $P(z)$ for all $x \in A$ by well-founded induction over $\rightarrow^+$:
Case 1: $x \leftarrow^0 z \rightarrow^* y$: trivial.
Case 2: $x \leftarrow^* z \rightarrow^0 y$: trivial.
Case 3: $x \leftarrow^* x' \leftarrow z \rightarrow y' \rightarrow^* y$: use local confluence, then use the induction hypothesis.