Mathematical Logic 2016

Lecture 17: First order theorem provers I

Instructor: Ashutosh Gupta

TIFR, India

Compile date: 2016-10-18

Where are we and where are we going?

We have seen

- FOL proof methods
- Normal forms - FOL clauses

We are looking at the design of modern theorem provers

- ordering constraints on resolution proof system
- completeness under the constraints

Topic 17.1

Order

Partial order

Definition 17.1

A partial order $\succ$ is a transitive and irreflexive relation over a domain D.

Definition 17.2

The reflexive closure $\succeq$ of $\succ$ is $\succ \cup \{(x,x)|x \in D\}$.

Definition 17.3

A partial order $\succ$ is total if for each $x, y \in D$, either $x \succ y$ or $y \succ x$.

Definition 17.4

A partial order $\succ$ is well-founded if there is no infinite chain $x_1, x_2, ..$ s.t. $x_1 \succ x_2 \succ \dots$.

Reduction order

We will use expression for both terms and formulas.

Definition 17.5

A reduction order $\succ$ over expressions is a well-founded partial order and if $t \succ s$ then $u(t) \succ u(s)$.

Theorem 17.1

Let $\succ$ be a reduction order then for each $u(t)$, $t \not\succ u(t)$

Proof.

Assume $t \succ u(t)$. Since $\succ$ is reduction order, $u(t) \succ u(u(t))$.
Therefore, There is a infinite chain, $t \succ u(t) \succ u(u(t))\dots$
Contradiction. $\square$

Definition 17.6

A order $\succ$ has subterm property if for each $u(t)$, $u(t) \succ t$

Exercise 17.1

If reduction order $\succ$ is total then it has subterm property.

Example : reduction order

Example 17.1

Consider a total well-founded order $\succ$ over each predicate, function, and logical symbols.

We extend the order over all expressions as follows s.t. $\succ$ is reduction order over expression.

$s = f(s_1, \ldots, s_m) \succ g(t_1, \ldots, t_n) = t$ *iff*

1. $f \succ g$ *and* $s \succ t_i$ *for each* $i \in 1..n$
2. $f = g$, *there is a* j *s.t.* $(s_1, .., s_{j-1}) = (t_1, .., t_{j-1})$, $s_j \succ t_j$, *and* $s \succ t_k$ *for* $k \in (j+1)..n$
3. $s_j \succeq t$ *for some* $j \in 1..m$

Exercise 17.2

a. Prove the above order is a reduction order

b. Prove the above order is total

Topic 17.2

Completeness of ground resolution

Resolution proof system for ground clauses

Now we present a proof rule that mixes resolution and factoring in one rule.

Let us suppose $A \vee ... \vee A \vee C$ and $\neg A \vee D$ are ground clauses.

$$\textsc{Resolution}\frac{A \vee ... \vee A \vee C \quad \neg A \vee D}{C \vee D}$$

The order of premises is not a coincidence.The last premise is called the main premise and others are side premises.

In implementation these distinctions seems to matter.

Progress using term order

First we will demonstrate the progress towards proving unsatisfiablity due to resolution over closed clauses using term order.

Later we will use the results to

- restrict application of inferences to reduce redundancies and
- generalize to deal with free variables

Note that closed atoms are almost like propositional variables in propositional logic

Admissible order

We need to define order over terms and formulas for our purposes.

Definition 17.7

We consider a total reduction order $\succ$ over closed formulas admissible *if*

- $A \succ \top$
- $A \succ \bot$
- $F \succ G$*, whenever for each atom B in G there is an atom A in F s.t.* $A \succ B$

We will later show that such an ordering exists and easy to evaluate.

Extension to clauses

Since clauses are multisets, we need to define a multiset extension of $\succ$.

Definition 17.8

A finite multiset extension of $\succ$ over closed formulas is defined as follows. For closed clauses C and D, $C \succ D$ if

- *$C \neq D$ and*
- *if $D(A) > C(A)$ then there is a B s.t. $B \succ A$ and $C(B) > D(B)$,*

where $C(A)$ denotes the number of occurrences of A in C.

Model

Definition 17.9

Consider Σ *be a set of closed clauses.*
A model m *of* Σ *is a set of atoms s.t. each clause* $C \in \Sigma$ *is true in* m*, i.e., there is a positive literal* $A \in C$ *s.t.* $A \in m$ *or a negative literal* $\neg A \in C$ *s.t.* $A \notin m$.

Definition 17.10

m *is a partial model of* Σ *if some clauses in* Σ *are not true in* m.

Example 17.2

Consider clauses $\Sigma = \{(A_1 \vee \neg A_2), (A_3 \vee A_2), (\neg A_4 \vee \neg A_5)\}$.
$m = \{A_1, A_3\}$ *is model of* Σ.
$\neg A_1 \vee \neg A_3$ *is false in* m.

Partial model below/at C

Definition 17.11

Let $\succ$ be an admissible order. For a closed clause C, the partial model below C, denoted by m_C, and increment ϵ_C are recursively defined as follows.

- $m_C = \cup_{C \succ D} \epsilon_D$
-
  - *If C is in Σ,*
  - *the maximal literal in C is a positive literal A, and*
  - *C is false in m_C*

  then $\epsilon_C = \{A\}$. Otherwise, $\epsilon_C = \emptyset$.

Definition 17.12

the partial model at C is $m^C = m_C \cup \epsilon_C$.

Definition 17.13

the candidate model of Σ is $m_\Sigma = \cup_{C \in \Sigma} \epsilon_C$.

Definition 17.14

A clause $C \in \Sigma$ is a counterexample if C if false in m_Σ.

Exercise 17.3

If $\epsilon_C \neq \emptyset$ then C is true in m_Σ

Example: partial model

Example 17.3

Consider order over atoms $B_2 \succ A_2 \succ B_1 \succ A_1 \succ B_0 \succ A_0$.
Consider the following clauses, listed according to $\succ$

C	m_C	ϵ_C
$A_0 \lor B_0$	$\emptyset$	$\{B_0\}$
$A_1 \lor B_0$	$\{B_0\}$	$\emptyset$
$A_1 \lor \neg B_0$	$\{B_0\}$	$\{A_1\}$
$B_1 \lor A_2 \lor \neg B_0$	$\{B_0, A_1\}$	$\{A_2\}$
$B_1 \lor \neg A_2 \lor B_0$	$\{B_0, A_1, A_2\}$	$\emptyset$
$\neg B_1 \lor B_2$	$\{B_0, A_1, A_2\}$	$\emptyset$

$m_\Sigma = \{B_0, A_1, A_2\}$

Monotonicity of truthness

Theorem 17.2

Let C and D be clauses such that $D \succeq C$. If C is true in m_D or m^D then C is true in m_Σ and also in $m^{D'}$ and $m_{D'}$, where $D' \succeq D$.

Proof.

We observe that $m_D \subseteq m^D \subseteq m_{D'} \subseteq m^{D'} \subseteq m_\Sigma$. If there is $A \in C$ that $A \in m_D$ or m^D then A is in m_Σ, and also in $m^{D'}$ and $m_{D'}$.

Otherwise, there is a $\neg A \in C$ such that $A \notin m_D$. Note $C \succeq \neg A$.
claim: No clause introduces A.
Assume $\epsilon_{D''} = \{A\}$.
Therefore, A is a maximal literal in D''.
Due to the subterm property $\neg A \succ A$.
Therefore, $\neg A \succ D''$. Therefore, $D \succeq C \succeq \neg A \succ D''$.
Therefore, $A \in m_D$. Contradiction. □

Exercise 17.4

Prove if maximal literal of C is positive then C is true in m_Σ.

Monotonicity of falseness

Theorem 17.3

Let D and D' be clauses s.t. $D \succeq D'$ and either $D' \in \Sigma$ or the maximal atom in D is strictly greater than the maximal atom in D'.
If D' is false in m^D, then it is also false in m_Σ, m_C and m^C for each $C \succeq D$.

Proof.

Assuming facts before 'then'.

Let $A \in D'$.
claim: no $C' \succeq D$ will make D' true
Assume $C' \succeq D$ s.t. $\epsilon_{C'} = \{A\}$.
Since A is maximal in C', A must be maximal in D'.
Due to the previous theorem and D' is false in m^D, D' must be false $m^{D'}$.
Therefore, $\epsilon_{D'} = \emptyset$.
Therefore, D' is not in Σ.
Since A is strictly smaller than maximal atom in D, $D \succ C'$.
Contradiction. □

Ensuring truth

Theorem 17.4

Let D and C be clauses, and $D \in \Sigma$.
If C is true in $m^{D'}$ for each $D \succ D'$ then C is true in m_D.

Proof.

case: If for some $A \in C$, there is a D' s.t. $D \succ D'$ and $\epsilon_{D'} = \{A\}$.
C is true in m_D.

case: If for each $A \in C$ and $D \succ D'$, $\epsilon_{D'} \neq \{A\}$.
Assume for each $\neg A \in C$, there is a D' s.t. $D \succ D'$ and $\epsilon_{D'} = \{A\}$.
Consider the maximal negative literal $\neg A' \in C$.
There must be a $D \succ D''$ s.t. $\epsilon_{D''} = \{A\}$.
Therefore, C is false $m^{D''}$. Contradiction.
Therefore there is a $\neg A \in C$ that does not occur in m_D.
Therefore, C is true in m_D. □

Smaller counterexample due to resolution

Theorem 17.5

Let $C \in \Sigma$ be non empty minimal counterexample. Then, there is a binary resolution step between C and another clause D in Σ such that the conclusion clause is false in m_Σ and smaller than C.

Proof.

Due to previous theorems, $\epsilon_C = \emptyset$.
Due to monotonicity of truthness and C is false in m_Σ, C is false in m_C.
Therefore, the maximal element of C is a negative literal $\neg A$.
Let $C' \vee \neg A = C$. Therefore, $C \succ C'$ and C' is false in m_Σ.

Since A occurs in m_Σ, there is a clause $D = D' \vee A \vee .. \vee A \in \Sigma$ s.t. $\epsilon_D = A$.
Therefore, A is maximal literal in D, $A \not\in D'$, and D' is false in m_D.
Therefore, $C \succ D'$. Due to monotonicity of falseness, D' is false in m_Σ.

By resolution between $C' \vee \neg A$ and $D' \vee A \vee .. \vee A$, we obtain $C' \vee D'$.
Therefore, $C \succ C' \vee D'$ and $C' \vee D'$ is false in m_Σ. □

Exercise 17.5

Show $\neg A$ need not be the maximal in C.

Resolution with factoring is complete

Theorem 17.6

If Σ is saturated with respect to resolution with factoring and does not contain empty clause then m_Σ is a model of Σ.

Proof.

If m_Σ is not a model then there must be a counterexample.
Therefore, resolution should be able to produce even smaller counterexample.
Since Σ is saturated with respect to resolution, Σ must contain empty clause. $\square$

Topic 17.3

Ordered Resolution

Selection function

Due to the previous theorems, we only need to apply resolution when progress towards smaller clauses happens.

A few observations due to the previous theorem

- The positive literal that participates in a resolution needs to be the maximal in the clause
- The negative literal may be chosen non-deterministically
- The produced clause is always smaller

The non-determinism gives rise to the following concept.

Definition 17.15

A selection function S chooses a subset of negative literals form a given clause

Ordered Resolution

For a given selection function S and an order $\succ$, the following is a ordering aware proof system.

$$\text{RESOLUTION}\frac{A_1 \lor ... \lor A_1 \lor D_1 \quad .. \quad A_n \lor ... \lor A_n \lor D_n \quad \neg A_1 \lor .. \lor \neg A_n \lor C}{D_1 \lor .. \lor D_n \lor C}$$

1. Either $S(\neg A_1 \lor .. \lor \neg A_n \lor C) = \neg A_1 \lor .. \lor \neg A_n$, or
   else $S(\neg A_1 \lor .. \lor \neg A_n \lor C) = \emptyset$, then $n = 1$, and A_1 is maximal with respect to C,
2. each atom A_i is strictly maximal with respect to D_i, and
3. $S(A_i \lor ... \lor A_i \lor D_i) = \emptyset$ for each $i \in 1..n$

Exercise 17.6

Show the conclusion is always smaller than the main premise.

Partial model redefined

Definition 17.16

Let $\succ$ be an admissible order. For a closed clause C, the partial model below C, denoted by m_C, and increment ϵ_C are recursively defined as follows.

- $m_C = \cup_{C \succ D} \epsilon_D$
-
  - *If C is in Σ,*
  - *the maximal literal in C is a positive literal A, and*
  - *C is false in m_C*
  - *nothing is selected in C*

  then $\epsilon_C = \{A\}$. Otherwise, $\epsilon_C = \emptyset$.

The other definitions for candidate model etc. do not change.

Exercise 17.7

a. Monotonicity of truthness still holds

b. Suggest a modification in monotonicity of falseness

Ordered resolution is complete

Theorem 17.7

Let $C \in \Sigma$ be non empty minimal counterexample. Then, there is a ordering aware resolution step between C and clauses $D_1, .., D_n$ in Σ such that the conclusion clause is false in m_Σ.

Proof.

Due to previous theorems, $\epsilon_C = \emptyset$.

Due to monotonicity of truthness and C is false in m_Σ, C is false in m_C.

Therefore, either

max in C is a negative literal	or	$S(C) \neq \emptyset$.
Let $n = 1$ and choose a negative literal s.t. $C = C' \vee \neg A_1$.		Let $S(C) = \neg A_1 \vee .. \vee \neg A_n$ and $C' = C - S(C)$.

Therefore, $C \succ C'$ and C' is false in m_Σ.

Ordered resolution is complete(contd.)

Proof(contd.)

Since A_i occurs in m_Σ, there is $D_i = D_i' \vee A_i \vee .. \vee A_i \in \Sigma$ s.t. $\epsilon_{D_i} = A_i$.
Therefore, A_i is maximal literal in D_i, D' is false in m_D, and $S(D_i) = \emptyset$.
Since A_i does not occur in D_i', max literal in D_i' is smaller than A_i.
Due to monotonicity of falseness, D_i' is false in m_Σ.
And, also implies $C \succ D_i'$.

Therefore, $C \succ D_1' \vee .. \vee D_n' \vee C'$, which is false in m_Σ.

The following resolution satisfied the conditions of ordered resolution.

$$\frac{A_1 \vee ... \vee A_1 \vee D_1' \quad .. \quad A_n \vee ... \vee A_n \vee D_n' \quad \neg A_1 \vee .. \vee \neg A_n \vee C'}{D_1' \vee .. \vee D_n' \vee C'}.$$

$\square$

Topic 17.4

Problems

Exercise 17.8

Consider the following axioms of equality.

1. $\forall x. x \approx x$
2. $\forall x, y. x \approx y \Rightarrow y \approx x$
3. $\forall x, y, z.\ x \approx y \land y \approx z \Rightarrow x \approx z$
4. *for each* $f/n \in \mathbf{F}$
   $\forall x_1, .., x_n, y_1, .., y_n.\ x_1 \approx y_1 \land .. \land x_n \approx y_n \Rightarrow f(x_1, .., x_n) \approx f(y_1, .., y_n)$
5. *for each* $P/n \in \mathbf{R}$
   $\forall x_1, .., x_n, y_1, .., y_n.\ x_1 \approx y_1 \land .. \land x_n \approx y_n P(x_1, .., x_n) \Rightarrow P(y_1, .., y_n)$

Show that PARAMODULATION *and* RELEXIVITY *rules derive consequences that can be derived using the above axioms and without the rules.*

End of Lecture 17