First-order logic
Resolution

Mario Alviano

University of Calabria, Italy

A.Y. 2018/2019

Outline

Outline

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are “equal”?

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are “equal”?

$$\forall x\ (H(x) \to M(x)) \land H(\mathit{socrates})$$

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are "equal"?

$$\forall x\ (H(x) \to M(x)) \land H(socrates)$$

- Resolution works on Skolem CNF formulas!
  1. $\{\neg H(x), M(x)\}$
  2. $\{H(socrates)\}$

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are “equal”?

$$\forall x \; (H(x) \rightarrow M(x)) \land H(\mathit{socrates})$$

- Resolution works on Skolem CNF formulas!
  1. $\{\neg H(x), M(x)\}$
  2. $\{H(\mathit{socrates})\}$
- Can we derive $M(\mathit{socrates})$?

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are "equal"?

$$\forall x\ (H(x) \to M(x)) \land H(socrates)$$

- Resolution works on Skolem CNF formulas!
  1. $\{\neg H(x), M(x)\}$
  2. $\{H(socrates)\}$
- Can we derive $M(socrates)$?
  - $H(x)$ is different from $H(socrates)$

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are “equal”?

$$\forall x \; (H(x) \rightarrow M(x)) \land H(socrates)$$

- Resolution works on Skolem CNF formulas!
  1. $\{\neg H(x), M(x)\}$
  2. $\{H(socrates)\}$
- Can we derive $M(socrates)$?
  - $H(x)$ is different from $H(socrates)$
- Can we substitute x by $socrates$?

First-order resolution

How to generalize propositional resolution to first-order?

Biggest obstacle: When two atoms are "equal"?

$$\forall x\ (H(x) \rightarrow M(x)) \land H(socrates)$$

- Resolution works on Skolem CNF formulas!
  1. $\{\neg H(x), M(x)\}$
  2. $\{H(socrates)\}$
- Can we derive $M(socrates)$?
  - $H(x)$ is different from $H(socrates)$
- Can we substitute x by *socrates*?
- Let's formalize this idea!

Outline

Composition of substitutions

Recall that $[t_1/x_1, \dots, t_n/x_n]$ denotes the (simultaneous) substitution of $x_1, \dots, x_n$ with $t_1, \dots, t_n$.

Definition

Let $\sigma = [t_1/x_1, \dots, t_n/x_n]$, $\vartheta = [s_1/y_1, \dots, s_m/y_m]$ be substitutions. The composition of σ and ϑ, denoted $\sigma \circ \vartheta$ (or $\sigma\vartheta$), is obtained from $[t_1\vartheta/x_1, \dots, t_n\vartheta/x_n, s_1/y_1, \dots, s_m/y_m]$

- by removing each $t_i\vartheta/x_i$ such that $t_i\vartheta = x_i$, and
- by removing each s_j/y_j such that $y_j \in \{x_1, \dots, x_n\}$.

Composition of substitutions

Recall that $[t_1/x_1, \dots, t_n/x_n]$ denotes the (simultaneous) substitution of $x_1, \dots, x_n$ with $t_1, \dots, t_n$.

Definition

Let $\sigma = [t_1/x_1, \dots, t_n/x_n]$, $\vartheta = [s_1/y_1, \dots, s_m/y_m]$ be substitutions. The composition of σ and ϑ, denoted $\sigma \circ \vartheta$ (or $\sigma\vartheta$), is obtained from $[t_1\vartheta/x_1, \dots, t_n\vartheta/x_n, s_1/y_1, \dots, s_m/y_m]$

- by removing each $t_i\vartheta/x_i$ such that $t_i\vartheta = x_i$, and
- by removing each s_j/y_j such that $y_j \in \{x_1, \dots, x_n\}$.

Just remember that substitutions are functions!

Composition of substitutions

Recall that $[t_1/x_1, \ldots, t_n/x_n]$ denotes the (simultaneous) substitution of $x_1, \ldots, x_n$ with $t_1, \ldots, t_n$.

Definition

Let $\sigma = [t_1/x_1, \ldots, t_n/x_n]$, $\vartheta = [s_1/y_1, \ldots, s_m/y_m]$ be substitutions. The composition of σ and ϑ, denoted $\sigma \circ \vartheta$ (or $\sigma\vartheta$), is obtained from $[t_1\vartheta/x_1, \ldots, t_n\vartheta/x_n, s_1/y_1, \ldots, s_m/y_m]$

- by removing each $t_i\vartheta/x_i$ such that $t_i\vartheta = x_i$, and
- by removing each s_j/y_j such that $y_j \in \{x_1, \ldots, x_n\}$.

Just remember that substitutions are functions!

Properties

- $\sigma[] = []\sigma = \sigma$
- $(\sigma\vartheta)\rho = \sigma(\vartheta\rho)$
- $\sigma\vartheta \neq \vartheta\sigma$
- $(t\sigma)\vartheta = t(\sigma\vartheta) = t\sigma\vartheta$
- $(\phi\sigma)\vartheta = \phi(\sigma\vartheta) = \phi\sigma\vartheta$
- $(E\sigma)\vartheta = E(\sigma\vartheta) = E\sigma\vartheta$

Unification (1)

Definition

Let E_1,E_2 be first-order expressions (i.e., terms or formulas).

- A substitution σ is a unifier of E_1,E_2 if $E_1\sigma = E_2\sigma$
- A unifier σ is a most general unifier (mgu) if for any unifier ϑ of E_1, E_2 it holds that $\vartheta = \sigma\rho$ for some substitution ρ

Unification (1)

Definition

Let E_1,E_2 be first-order expressions (i.e., terms or formulas).

- A substitution σ is a unifier of E_1,E_2 if $E_1\sigma = E_2\sigma$
- A unifier σ is a most general unifier (mgu) if for any unifier ϑ of E_1, E_2 it holds that $\vartheta = \sigma\rho$ for some substitution ρ

Properties

- If E_1,E_2 are unifiable then an mgu exists
- Moreover, the mgu is unique modulo variable renaming

Unification (2)

Let $\perp$ denote failure.

- $\mathit{unify}(P(t_1, \ldots, t_n), Q(s_1, \ldots, s_m)) = \perp$ if $P \neq Q$ or $n \neq m$
- $\mathit{unify}(P(t_1, \ldots, t_n), P(s_1, \ldots, s_n)) = \mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n))$

Unification

Let $\perp$ denote failure.

- $\mathit{unify}(P(t_1, \ldots, t_n), Q(s_1, \ldots, s_m)) = \perp$ if $P \neq Q$ or $n \neq m$
- $\mathit{unify}(P(t_1, \ldots, t_n), P(s_1, \ldots, s_n)) = \mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n))$
- $\mathit{unify}((), ()) = []$
- $\mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n)) = \perp$ if $\mathit{unify}(t_1, s_1) = \perp$
- $\mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n)) =$
  $\sigma \circ \mathit{unify}((t_2\sigma, \ldots, t_n\sigma), (s_2\sigma, \ldots, s_n\sigma))$ where $\sigma = \mathit{unify}(t_1, s_1)$
  and $\sigma \neq \perp$

Unification (2)

Let $\perp$ denote failure.

- $\mathit{unify}(P(t_1, \ldots, t_n), Q(s_1, \ldots, s_m)) = \perp$ if $P \neq Q$ or $n \neq m$
- $\mathit{unify}(P(t_1, \ldots, t_n), P(s_1, \ldots, s_n)) = \mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n))$

- $\mathit{unify}((), ()) = []$
- $\mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n)) = \perp$ if $\mathit{unify}(t_1, s_1) = \perp$
- $\mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n)) =$
  $\sigma \circ \mathit{unify}((t_2\sigma, \ldots, t_n\sigma), (s_2\sigma, \ldots, s_n\sigma))$ where $\sigma = \mathit{unify}(t_1, s_1)$
  and $\sigma \neq \perp$

- $\mathit{unify}(f(t_1, \ldots, t_n), g(s_1, \ldots, s_m)) = \perp$ if $f \neq g$ or $n \neq m$
- $\mathit{unify}(f(t_1, \ldots, t_n), f(s_1, \ldots, s_n)) = \mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n))$

Unification (2)

Let $\bot$ denote failure.

- $\mathit{unify}(P(t_1, \ldots, t_n), Q(s_1, \ldots, s_m)) = \bot$ if $P \neq Q$ or $n \neq m$
- $\mathit{unify}(P(t_1, \ldots, t_n), P(s_1, \ldots, s_n)) = \mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n))$

- $\mathit{unify}((), ()) = []$
- $\mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n)) = \bot$ if $\mathit{unify}(t_1, s_1) = \bot$
- $\mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n)) =$
  $\sigma \circ \mathit{unify}((t_2\sigma, \ldots, t_n\sigma), (s_2\sigma, \ldots, s_n\sigma))$ where $\sigma = \mathit{unify}(t_1, s_1)$
  and $\sigma \neq \bot$

- $\mathit{unify}(f(t_1, \ldots, t_n), g(s_1, \ldots, s_m)) = \bot$ if $f \neq g$ or $n \neq m$
- $\mathit{unify}(f(t_1, \ldots, t_n), f(s_1, \ldots, s_n)) = \mathit{unify}((t_1, \ldots, t_n), (s_1, \ldots, s_n))$

- $\mathit{unify}(t, x) = \mathit{unify}(x, t)$ if t is not a variable
- $\mathit{unify}(x, t) = [t/x]$ if $x \notin \mathit{free}(t)$
- $\mathit{unify}(x, t) = \bot$ if $x \in \mathit{free}(t)$ and $x \neq t$
- $\mathit{unify}(x, x) = []$

Unification (3)

Examples

1. $unify(P(x, f(x)), P(y, f(g(b))))$
2. $unify(A(x, y), A(y, f(z)))$
3. $unify(B(a, y, f(y)), B(z, z, u))$
4. $unify(A(x, g(x)), A(y, y)))$

Outline

Resolvent and factorization

Resolvent

Let C_1, C_2 be two clauses.

- Assume two variable renaming substitutions σ_1 and σ_2 such that $C_1\sigma_1$ and $C_2\sigma_2$ do not share variables.
- If $A_1 \in C_1\sigma_1$ and $\neg A_2 \in C_2\sigma_2$ such that A_1 and A_2 are unifiable with mgu ϑ, then

  $$((C_1\sigma_1 \setminus \{A_1\}) \cup (C_2\sigma_2 \setminus \{\neg A_2\}))\vartheta$$

  is a resolvent of C_1 and C_2.

Resolvent and factorization

Resolvent

Let C_1, C_2 be two clauses.

- Assume two variable renaming substitutions σ_1 and σ_2 such that $C_1\sigma_1$ and $C_2\sigma_2$ do not share variables.
- If $A_1 \in C_1\sigma_1$ and $\neg A_2 \in C_2\sigma_2$ such that A_1 and A_2 are unifiable with mgu ϑ, then

  $$((C_1\sigma_1 \setminus \{A_1\}) \cup (C_2\sigma_2 \setminus \{\neg A_2\}))\vartheta$$

  is a resolvent of C_1 and C_2.

Factorization

Given a clause C, if there are literals A_1, A_2 (or $\neg A_1, \neg A_2$) of C such that A_1 and A_2 are unifiable with mgu ϑ, then $C\vartheta$ is a factor of C.

Refutation

Derivation

Given a set Γ of clauses, a derivation by resolution of a clause C from Γ, denoted $\Gamma \vdash_R C$, is a sequence $C_1, \ldots, C_n$ such that $C_n = C$ and for each C_i ($1 \leq i \leq n$) we have

1. $C_i \in \Gamma$, or
2. C_i is a resolvent of C_j and C_k, where $j < i$ and $k < i$, or
3. C_i is a factor of C_j, where $j < i$.

Refutation

Derivation

Given a set Γ of clauses, a derivation by resolution of a clause C from Γ, denoted $\Gamma \vdash_R C$, is a sequence $C_1, \ldots, C_n$ such that $C_n = C$ and for each C_i ($1 \leq i \leq n$) we have

1. $C_i \in \Gamma$, or
2. C_i is a resolvent of C_j and C_k, where $j < i$ and $k < i$, or
3. C_i is a factor of C_j, where $j < i$.

We can now use all other definitions and claims from propositional resolution!

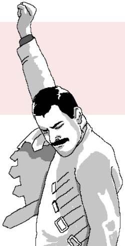
Refutation

Derivation

Given a set Γ of clauses, a derivation by resolution of a clause C from Γ, denoted $\Gamma \vdash_R C$, is a sequence $C_1, \ldots, C_n$ such that $C_n = C$ and for each C_i $(1 \leq i \leq n)$ we have

1. $C_i \in \Gamma$, or
2. C_i is a resolvent of C_j and C_k, where $j < i$ and $k < i$, or
3. C_i is a factor of C_j, where $j < i$.

We can now use all other definitions and claims from propositional resolution!



Outline

Exercises (1)

1. Find the most general unifier for $A(r(c, x), r(z, z))$ and $A(y, y)$ (if it exists)
2. Decide by means of resolution whether the following formulas (in SCNF) are satisfiable:
    1. $\{R(x, g(y))\}, \{\neg R(v, v), S(v)\}, \{\neg S(g(c))\}$
    2. $\{R(x, g(x))\}, \{\neg R(z, z), S(z)\}, \{\neg S(g(x))\}$
    3. $\{R(x, y), R(z, c), S(z)\}, \{\neg R(f(u), u), \neg R(v, w)\}, \{\neg S(f(d))\}$

Exercises (2)

1. Use resolution to prove that
   - $\forall x \forall y \forall z (P(x,y) \wedge P(y,z) \rightarrow P(x,z))$
   - $\forall x \forall y (P(x,y) \rightarrow P(y,x))$

   entail
   - $\forall x \forall y \forall z (P(x,y) \wedge P(z,y) \rightarrow P(x,z))$
2. Use resolution to prove that
   - $\forall x \, A(a,x,x)$
   - $\forall x \forall y \forall z (A(x,y,z) \rightarrow A(x,s(y),s(z)))$
   - $\forall x \forall y \forall z (A(x,y,z) \rightarrow A(y,x,z))$

   entail
   - $\exists x \, A(s(s(a)), s(s(s(a))), x)$

Exercises 6.18 and 6.19 from *Logica a Informatica*.

1. Prove using resolution that 1 entails 2:
   1. All students are citizens
   2. Votes by students are votes by citizens

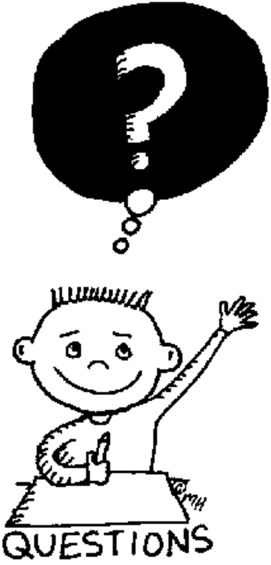
   Hint: Use *Student*(x), *Citizen*(x) and *Votes*(x, y) for "x is a student", "x is a citizen" and "x votes y", respectively.
2. Check whether 3 is a logical consequence of 1 and 2:
   1. Every lion chases some gazelle
   2. Every gazelle fears anyone chasing it
   3. Every gazelle fears someone

   In case your answer is negative, provide a Herbrand model.

Exercise 6.20 from *Logica a Informatica*.

1. Check whether 4 is a logical consequence of the other sentences:
    1. Policemen searched all those who have stepped off the plane and were not member of the crew
    2. Some thieves (one or more) stepped off the plane and were searched only by thieves
    3. No thief was a member of the crew
    4. Some policemen (one or more) were thieves

    In case your answer is negative, provide a Herbrand model.



END OF THE LECTURE