Predicate Calculus

COMP SCI 2LC3

Ryszard Janicki

Department of Computing and Software, McMaster University, Hamilton, Ontario, Canada

Introduction

- Predicate logic is an extension of propositional logic
- It allows the use of variables of types other than $\mathbb{B}$
- This extension leads to a logic with enhanced expressive
- Propositional calculus permits reasoning about formulas constructed from boolean variables and boolean operators
- Predicate calculus permits reasoning about a more expressive class of formulas

- A predicate-calculus formula is a boolean expression in which some boolean variables may have been replaced by:
  - Predicates : applications of boolean functions whose arguments may be of types other than $\mathbb{B}$
  - Universal and existential quantification

Example

1. $x < y \ \wedge \ x = z \ \Longrightarrow \ q(x, z + x)$
2. $\forall(x, y \ |: \ f(x, y) = f(y, x))$

Introduction

The pure predicate calculus includes

1. The axioms of propositional calculus
2. The axioms for quantifications $\forall(x \mid R : P)$ and $\exists(x \mid R : P)$
3. The inference rules of the predicate calculus
   1. Substitution: $\dfrac{E}{E[v{:=}F]}$
   2. Transitivity: $\dfrac{X{=}Y, \quad Y{=}Z}{X{=}Z}$
   3. Leibniz: $\dfrac{X{=}Y}{E[z{:=}X]{=}E[z{:=}Y]}$
   4. Leibniz for quantification:
      - $\dfrac{P{=}Q}{*(x \mid E[z{:=}P] : S) \;=\; *(x \mid E[z{:=}Q] : S)}$
      - $\dfrac{R \Longrightarrow P{=}Q}{*(x \mid R : E[z{:=}P]) \;=\; *(x \mid R : E[z{:=}Q])}$

Introduction

- In the pure predicate calculus, the function symbols $(<, >, +, \cdot,$ etc.$)$ are uninterpreted
  - except for equality $=$
  - the logic provides no specific rules for manipulating function symbols
  - general rules for manipulation that are sound independently of the meanings of the function symbols
  - so, the pure predicate calculus is sound in all domains that may be of interest

- We get a theory by adding axioms that give meanings to some of the (uninterpreted) function symbols
- The theory of integers consists of the pure predicate calculus together with axioms for manipulating the operators $+, -, ., <, \leq$, etc.
- For example, the axioms say that $\cdot$ is
  - symmetric,
  - associative, and
  - has the zero 0

Introduction

- The theory of sets provides axioms for manipulating expressions containing operators like $\in, \subseteq, \cup, \cap$, etc.
- We can also form a joint theory of sets and integers, allowing us to reason about expressions that contain both
- The core of all these theories is the pure predicate calculus (provides the basic machinery)

Universal quantification

- Conjunction $\wedge$ (i.e., $\forall$) is symmetric and associative and has the identity true
- Therefore, it is an instance of * (previous set of slides)
- The quantification $\wedge(x \mid R : P)$ is conventionally written as $\forall(x \mid R : P)$
- The symbol $\forall$, which is read as "for all", is called the universal quantifier
- All the axioms of quantifition hold
- We now introduce additional axioms and theorems for universal quantification

- Axiom, Trading:

$$\forall(x \mid R : P) \iff \forall(x \mid: R \implies P)$$

- Trading theorems for $\forall$:

1. $\forall(x \mid R : P) \iff \forall(x \mid: \neg R \vee P)$
2. $\forall(x \mid R : P) \iff \forall(x \mid: R \wedge P \iff R)$
3. $\forall(x \mid R : P) \iff \forall(x \mid: R \vee P \iff P)$

Universal quantification

- Trading theorems for $\forall$ (continued):

1. $\forall(x \mid Q \wedge R : P) \iff \forall(x \mid Q : R \implies P)$
2. $\forall(x \mid Q \wedge R : P) \iff \forall(x \mid Q : \neg R \vee P)$
3. $$\forall(x \mid Q \wedge R : P)$$ $$\iff \forall(x \mid Q : R \wedge P \iff R)$$
4. $$\forall(x \mid Q \wedge R : P)$$ $$\iff \forall(x \mid Q : R \vee P \iff P)$$

Universal quantification

- Axiom, Distributivity of $\vee$ over $\forall$: Provided $\neg occurs('x', 'P')$,

$$P \vee \forall(x \mid R : Q) \iff \forall(x \mid R : P \vee Q)$$

- Additional theorems for $\forall$:

1. Provided $\neg occurs('x', 'P')$,

$$\forall(x \mid R : P) \iff P \vee \forall(x \mid: \neg R)$$

- Additional theorems for $\forall$ (Continued):

1. Provided $\neg$occurs$('x', 'P')$,

$$\neg \forall(x \mid : \neg R)$$
$$\Longrightarrow$$
$$(\forall(x \mid R : P \land Q) \iff P \land \forall(x \mid R : Q))$$

2. $\forall(x \mid R : \text{true}) \iff \text{true}$

3. $$\forall(x \mid R : P \iff Q)$$
$$\Longrightarrow$$
$$(\forall(x \mid R : P) \iff \forall(x \mid R : Q))$$

Theorems: Weakening/strengthening and monotonicity for $\forall$

1. Range weakening/strengthening :

$$\forall(x \mid Q \vee R : P) \implies \forall(x \mid Q : P)$$

2. Body weakening/strengthening:

$$\forall(x \mid R : P \wedge Q) \implies \forall(x \mid R : P)$$

3. Monotonicity of $\forall$:

$$\forall(x \mid R : Q \implies P)$$

$$\implies$$

$$(\forall(x \mid R : Q) \implies \forall(x \mid R : P))$$

Existential quantification

- Disjunction $\vee$ is symmetric and associative and has the identity false
- Therefore, it is an instance of $*$
- The quantification

$$\vee\,(x \mid R : P)$$

  is typically written as

$$\exists(x \mid R : P)$$

- The symbol $\exists$, which is read as "there exists", is called the existential quantifier

Existential quantification

- The expression is called an existential quantification
- $\exists(x \mid R : P)$ is read as "there exists an x in the range R such that P holds"
- A value $\hat{x}$ for which $(R \wedge P)[x := \hat{x}]$ is valid is called a witness for x in $\exists(x \mid R : P)$
- General axioms, from previous set of slides, that hold for $\exists(x \mid R : P)$ not repeated here
- Note that $\vee$ is idempotent, so that existential quantification satisfies Range split for idempotent $*$

Existential quantification

- Idea behind this generalization with an example

$$\vee\,(i \mid 1 \leq i \leq 2 : p_i) \iff \neg \wedge (i \mid 1 \leq i \leq 2 : \neg p_i)$$

$$\vee\,(i \mid 1 \leq i \leq 4 : p_i) \iff \neg \wedge (i \mid 1 \leq i \leq 4 : \neg p_i)$$

- The generalisation of De Morgan can be viewed as a definition of $\exists$
- It can be used along with the strategy of definition elimination, to prove all theorems concerning existential quantification

Existential quantification

- Axiom, Generalised De Morgan:

$$\exists(x \mid R : P) \iff \neg\forall(x \mid R : \neg P)$$

- Generalised De Morgan theorems:

1. $\neg\exists(x \mid R : \neg P) \iff \forall(x \mid R : P)$
2. $\neg\exists(x \mid R : P) \iff \forall(x \mid R : \neg P)$
3. $\exists(x \mid R : \neg P) \iff \neg\forall(x \mid R : P)$

Existential quantification

- Theorems: Trading theorems for $\exists$
  1. $\exists(x \mid R : P) \iff \exists(x \mid: R \wedge P)$
  2. $\exists(x \mid Q \wedge R : P) \iff \exists(x \mid Q : R \wedge P)$

- More theorems for $\exists$
  1. Distributivity of $\wedge$ over $\exists$: Provided $\neg occurs('x', 'P')$

$$P \wedge \exists(x \mid R : Q) \iff \exists(x \mid R : P \wedge Q)$$

  2. Provided $\neg occurs('x', 'P')$

$$\exists(x \mid R : P) \iff P \wedge \exists(x \mid: R)$$

Existential quantification

- Theorems: More theorems for $\exists$ (Continued)

1. Distributivity of $\vee$ over $\exists$: Provided $\neg occurs('x', 'P')$

$$\exists(x \mid : R) \implies (\exists(x \mid R : P \vee Q) \iff P \vee \exists(x \mid R : Q))$$

2. $\exists(x \mid R : \text{false}) \iff \text{false}$

Theorems: Weakening/strengthening and monotonicity for $\exists$

1. Range weakening/strengthening :

$$\exists(x \mid R : P) \implies \exists(x \mid Q \vee R : P)$$

2. Body weakening/strengthening:

$$\exists(x \mid R : P) \implies \exists(x \mid R : P \vee Q)$$

3. Monotonicity of $\exists$:

$$\exists(x \mid R : Q \implies P)$$
$$\implies$$
$$(\exists(x \mid R : Q) \implies \exists(x \mid R : P))$$

Existential quantification

1. ∃-Introduction:

$$P[x := e] \implies \exists(x \;|:\; P)$$

2. Interchange of quantifications: Provided $\neg \text{occurs}('x', \; 'Q')$,

$$\exists(x \mid R : \forall(y \mid Q : P))$$
$$\implies$$
$$\forall(y \mid Q : \exists(x \mid R : P))$$