Predicate Calculus

Simon Foster & Jim Woodcock

University of York

PROF

11th December 2021

Overview

Outline

Introduction

- Predicate quantifiers: extent that proposition is true over range of elements.
- Predicate = proposition with abstracted subject: $P(x)$.
- Universal Quantification Predicate true for all the values over domain.
- $\forall x \bullet P(x)$: states that $P(x)$ is true for all values of x in this domain.
- Existential Quantification Predicate true for some value of x in the domain.
- $\exists x \bullet P(x)$: states that $P(x)$ is true for at least one value in the domain.

Syntax

- In Z, quantifiers share a similar syntax: $\exists x : s \mid P \bullet Q$.
- $\exists$ is the quantifier, x is the bound variable, and s is the range of x.
- P is the (optional) constraint and Q is the predicate.
- Two syntactic equivalences explain the constraint:

  $\exists x : s \mid P \bullet Q$ is a shorthand for $\exists x : s \bullet P \wedge Q$

  $\forall x : s \mid P \bullet Q$ is a shorthand for $\forall x : s \bullet P \Rightarrow Q$
- $\exists x : s \mid P \bullet Q$ read as "there exists an x in s satisfying P, such that Q" holds.
- $\forall x : s \mid P \bullet Q$ read as "for all x in s satisfying P, Q holds".

Bound Variables

- Each quantifier introduces a bound variable.
- Scoped, like local variables in a block-structured programming language.
- Consider the quantified predicate "$\forall x : s \mid P \bullet Q$".
- Bound variable scope: exactly the constraint P and predicate Q: $\forall x : s \mid \underbrace{P \bullet Q}_{\text{scope of } x}$.
- Quantifiers take the widest possible scope, binding very loosely: $\forall x : s \bullet P \wedge Q$.
- This means "$\forall x : s \bullet (P \wedge Q)$". Not "$(\forall x : s \bullet P) \wedge Q$".
- Variables not yet bound are free. Example: $x > 3$ has one free variable: x.
- Truth-tables are useless for quantifiers, in general.
- Because bound variables can range over sets that are too large to tabulate.

Substitution

- Suppose P is a predicate containing free variable x.
- "$\forall x : s \bullet P$": asserts P is true for every x.
- Specific theorems are obtained by substituting a term t for bound variable x.
- $P[t/x]$ denotes P with term t substituted for x. Read as "P with t for x".

  Some authors use replacement notation: $P[x \backslash t]$, $P[x := t]$.

  Remember your English grammar: Substitute new for old. Replace old by new.
- Substitution also defined on terms themselves: $u[t/x]$.
- In Isabelle, we write $P(x)$ to show that x is free for substitution in P.
- Substitution is done by supplying an actual parameter: $P(t)$.

Substitution

- Bound variables must sometimes be renamed before substitution.
- Consider the theorem $\forall x : \mathbb{Z} \bullet \exists y : \mathbb{Z} \bullet x \neq y$.
- True for all numbers, so why not specialise it? Is it true for y: $\exists y : \mathbb{Z} \bullet y \neq y$?
- Contradiction! — What's gone wrong? Free variable capture.
- Free variable y enters scope of $\exists y : \mathbb{Z} \bullet \cdots$ and becomes a bound variable.
- Change the bound variable before substitution to avoid capture:

$$(\exists y : \mathbb{Z} \bullet x \neq y)[y/x] \;=\; (\exists z : \mathbb{Z} \bullet x \neq z)[y/x] \;=\; \exists z : \mathbb{Z} \bullet y \neq z$$

Outline

Reasoning with Quantifiers

- Variable capture example suggests: the name of a bound variable doesn't matter.
- Predicates that differ up to renaming of bound variables are equivalent.

$$\exists y : \mathbb{Z} \bullet x \neq y \;=\; \exists z : \mathbb{Z} \bullet x \neq z$$

- What about other equivalences in the predicate calculus?
- Here's a simple question about two quantified predicates:

  Are these two predicates equivalent?

$$\exists x : s \bullet P(x) \Rightarrow Q(x) \quad ?{=}? \quad (\exists x : s \bullet P(x)) \Rightarrow (\exists x : s \bullet Q(x))$$

- Are they equivalent? Does one imply the other? Are they at all related?
- We need identities to reason about quantifiers to check the answer.
- Before that, we need rules for reasoning about quantifiers.

Reasoning with Universal Quantification

- Suppose $P(x)$ is true for every possible value of x in s: then $\forall x : s \bullet P(x)$.
- Otherwise, $\forall x : s \bullet P(x)$ is false.
- This gives us an argument.
- Generalisation: $x \in s, P(x) \vdash \forall x : s \bullet P(x)$
- This is an argument with two premises and one conclusion.
- This argument is valid only if its premises are true for every x.
- A new kind of restriction: the variable x must be arbitrary.
- Valid: $x \in \mathbb{Z}, x + 1 > x \vdash \forall x : \mathbb{Z} \bullet x + 1 > x$
- Fallacy: $x \in \mathbb{Z}, x = 5 \vdash \forall x : \mathbb{Z} \bullet x = 5$

Reasoning with Universal Quantification

- If $\forall x : s \bullet P(x)$ is true, then for any term t in s, $P(t)$ will be true.
- This gives us an argument.
- Specialisation: $\forall x : s \bullet P(x), t \in s \vdash P(t)$
- Example: $\forall x : \mathbb{Z} \bullet x^2 \geq 0, y - 1 \in \mathbb{Z} \vdash (y-1)^2 \geq 0$
- This is another argument with two premises and one conclusion.

Reasoning with Existential Quantification

- Suppose $P(x)$ is true for at least one element of s: $\exists x : s \bullet P(x)$.
- Otherwise, $\exists x : s \bullet P(x)$ is false.
- This gives us an argument: $t \in s, P(t) \vdash \exists x : s \bullet P(x)$
- Existential introduction. This hides information by giving a name to a witness.
- Existential elimination: prove a predicate R from the predicate $\exists x : s \bullet P(x)$.
- Show that R follows from an arbitrary element of s satisfying P.

$$\exists x : s \bullet P(x), (x \in s, P(x) \vdash R) \vdash R$$

- Similar to generalisation (universal introduction).
- Note the sub-argument $x \in s, P(x) \vdash R$ as a premise to the overall argument.
- How are existential elimination and universal introduction linked?
- De Morgan's laws for quantifiers.

Outline

De Morgan's Laws for Quantifiers: Motivation

- Can the predicate $\neg \, \forall x : \mathbb{N} \bullet x > 3$ be simplified? Semi-formal argument:

$$
\begin{array}{ll}
 & \neg \, \forall x : \mathbb{N} \bullet x > 3 \\
\Leftrightarrow & \quad \{ \text{universal quantification as conjunction} \} \\
 & \neg \, (0 > 3 \land 1 > 3 \land 2 > 3 \land 3 > 3 \land \ldots) \\
\Leftrightarrow & \quad \{ \text{by De Morgan's Law} \} \\
 & \neg \, (0 > 3) \lor \neg \, (1 > 3) \lor \neg \, (2 > 3) \lor \neg \, (3 > 3) \lor \ldots \\
\Leftrightarrow & \quad \{ \text{existential quantification as disjunction} \} \\
 & \exists x : \mathbb{N} \bullet \neg \, (x > 3)
\end{array}
$$

- Motivates De Morgan's Laws for generalised conjunction and disjunction:

$$\neg \, (\forall x : s \bullet P(x)) \Leftrightarrow \exists x : s \bullet \neg \, P(x) \quad \text{and} \quad \neg \, (\exists x : s \bullet P(x)) \Leftrightarrow \forall x : s \bullet \neg \, P(x)$$

Example: A Classic Logic Puzzle

- Suppose that if you don't love someone, then you hate them.
- Is there no one who loves everybody? Draw conclusions if it's true.
- Let's calculate. Let *Person* be the set of all people:

$$
\begin{array}{ll}
& \neg\ \exists\, x : \mathit{Person} \bullet \forall\, y : \mathit{Person} \bullet x \mathrel{\mathit{loves}} y \\
\Leftrightarrow & \quad \{ \text{ by De Morgan } \} \\
& \forall\, x : \mathit{Person} \bullet \neg\ \forall\, y : \mathit{Person} \bullet x \mathrel{\mathit{loves}} y \\
\Leftrightarrow & \quad \{ \text{ by De Morgan } \} \\
& \forall\, x : \mathit{Person} \bullet \exists\, y : \mathit{Person} \bullet \neg\ (x \mathrel{\mathit{loves}} y) \\
\Leftrightarrow & \quad \{ \text{ by definition } \} \\
& \forall\, x : \mathit{Person} \bullet \exists\, y : \mathit{Person} \bullet x \mathrel{\mathit{hates}} y
\end{array}
$$

- So, our sentence means everybody hates someone.

Example: De Morgan for Quantifiers

- For every pair of integers x and y, there's a z, such that $x + z = y$.
- Formalised as: $\forall\, x : \mathbb{Z} \bullet \forall\, y : \mathbb{Z} \bullet \exists\, z : \mathbb{Z} \bullet x + z = y$ ($\mathbb{Z}$ is the set of integers)
- Or more simply as: $\forall\, x : \mathbb{Z};\ y : \mathbb{Z} \bullet \exists\, z : \mathbb{Z} \bullet x + z = y$.
- Or even more simply as: $\forall\, x, y : \mathbb{Z} \bullet \exists\, z : \mathbb{Z} \bullet x + z = y$.
- Predicate is false for all positive integers in $\mathbb{N}$: $\forall\, x, y : \mathbb{N} \bullet \exists\, z : \mathbb{N} \bullet x + z = y$.
- To see this, take $x = 2$ and $y = 1$, then we must prove that $\exists\, z : \mathbb{N} \bullet 2 + z = 1$.
- Which is patently false: there is no such z. $\exists\, z : \mathbb{N} \bullet z = -1$.
- How do we prove it's a contradiction?

Let's Calculate

It's false. Negate the predicate and show that the result is true.

$$
\begin{array}{ll}
 & \neg\ \forall x, y : \mathbb{N} \bullet \exists z : \mathbb{N} \bullet x + z = y \\
\Leftrightarrow & \quad \{ \text{by De Morgan} \} \\
 & \exists x, y : \mathbb{N} \bullet \neg\ \exists z : \mathbb{N} \bullet x + z = y \\
\Leftrightarrow & \quad \{ \text{by De Morgan} \} \\
 & \exists x, y : \mathbb{N} \bullet \forall z : \mathbb{N} \bullet \neg\ (x + z = y) \\
\Leftrightarrow & \quad \{ \text{by definition} \} \\
 & \exists x, y : \mathbb{N} \bullet \forall z : \mathbb{N} \bullet x + z \neq y
\end{array}
$$

We can prove our result more easily in this form.

Finishing it off

- So how do we prove $\exists x, y : \mathbb{N} \bullet \forall z : \mathbb{N} \bullet x + z \neq y$?
- Use existential introduction!
- Find values for x and y that make the following true

  $$\forall z : \mathbb{N} \bullet x + z \neq y$$

- If we select 1 for x and 0 for y, we have

  $$\forall z : \mathbb{N} \bullet 1 + z \neq 0$$

  which is a property of every natural number: $succ(z) \neq 0$.
- So, given this property, we've proved that

  $$\neg \forall x, y : \mathbb{N} \bullet \exists z : \mathbb{N} \bullet x + z = y$$

More on De Morgan

- What happens to the range of the bound variable? Consider the following:

$$
\begin{array}{ll}
 & \neg \, \forall x : \mathbb{N} \bullet x^2 + x - 2 > 0 \\
\Leftrightarrow & \quad \{ \text{since } \forall x : s \bullet P \text{ is the same as } \forall x : X \bullet x \in s \Rightarrow P \} \\
 & \neg \, \forall x : \mathbb{Z} \bullet x \in \mathbb{N} \Rightarrow x^2 + x - 2 > 0 \\
\Leftrightarrow & \quad \{ \text{by De Morgan} \} \\
 & \exists x : \mathbb{Z} \bullet \neg \, (x \in \mathbb{N} \Rightarrow x^2 + x - 2 > 0) \\
\Leftrightarrow & \quad \{ \text{by propositional calculus} \} \\
 & \exists x : \mathbb{Z} \bullet x \in \mathbb{N} \wedge x^2 + x - 2 \leq 0 \\
\Leftrightarrow & \quad \{ \text{since } \exists x : s \bullet P \text{ is the same as } \exists x : X \bullet x \in s \wedge P \} \\
 & \exists x : \mathbb{N} \bullet x^2 + x - 2 \leq 0
\end{array}
$$

- Range of the quantification remains unchanged.

Outline

Proving and Disproving Universal Quantifications

- Proving $\forall x : s \bullet P(x)$ can be quite demanding.
- We need an argument that proves P whatever the value of x.
- Not enough to give some examples of values of x that satisfy P.
- Disproving $\forall x : s \bullet P(x)$ may be much easier.
- By De Morgan, it's the same as proving $\exists x : s \bullet \neg P(x)$.
- We need only a single x for which P is false.
- Value for x provides a counterexample to $\forall x : s \bullet P(x)$.

Example: Disproving a Universal Quantification

- Show the following statement is false

$$\forall x : \mathbb{Q} \mid x > 0 \bullet (x^2 - 3x + 2 \geq 0)$$

$\mathbb{Q}$ is the rational numbers (those expressible as the ratio of two integers a/b).

- A single counterexample suffices.
- An appropriate value is $\frac{3}{2} > 0$.
- We have that

$$(\tfrac{3}{2})^2 - 3 * (\tfrac{3}{2}) + 2 \quad = \quad -\tfrac{1}{4} \quad < \quad 0$$

Moving Quantifier Scopes

- Suppose our predicate is a disjunct or conjunct within a quantifier.
- Suppose none of its variables are bound by the quantifier.
- Then the predicate can be pulled out of the quantifier scope.
- Let N stand for a predicate in which x doesn't occur free.
- We have the following equivalences

$$\begin{array}{lcl}
\forall x : s \bullet P(x) \land N & \Leftrightarrow & \big(\forall x : s \bullet P(x)\big) \land N \\
\forall x : s \bullet P(x) \lor N & \Leftrightarrow & \big(\forall x : s \bullet P(x)\big) \lor N \\
\exists x : s \bullet P(x) \land N & \Leftrightarrow & \big(\exists x : s \bullet P(x)\big) \land N \\
\exists x : s \bullet P(x) \lor N & \Leftrightarrow & \big(\exists x : s \bullet P(x)\big) \lor N
\end{array}$$

Moving Quantifiers Around

- Suppose we have a predicate that is a universally quantified conjunction.
- Suppose the bound variable occurs in both parts of the conjunction.

$$\forall x : s \bullet P(x) \land Q(x)$$

- Can we move the quantifier inwards?
- Distributivity laws for the quantifiers

$$(\forall x : s \bullet P(x) \land Q(x)) \quad \Leftrightarrow \quad (\forall x : s \bullet P(x)) \land (\forall x : s \bullet Q(x))$$
$$(\exists x : s \bullet P(x) \lor Q(x)) \quad \Leftrightarrow \quad (\exists x : s \bullet P(x)) \lor (\exists x : s \bullet Q(x))$$

- Maybe they're really associativity laws?

Example: Distributivity

- WARNING: Universal quantification doesn't distribute over disjunction:

$$\neg \Big(\big(\forall\, x : s \bullet P(x) \vee Q(x)\big) \;\Leftrightarrow\; \big(\forall\, x : s \bullet P(x)\big) \vee \big(\forall\, x : s \bullet Q(x)\big) \Big)$$

- Counterexample to distribution:

Every number is either even or odd:

$$\forall\, n : \mathbb{Z} \bullet (n \bmod 2 = 0) \vee (n \bmod 2 = 1)$$

But it's false that either every number is even, or every number is odd:

$$\big(\forall\, n : \mathbb{Z} \bullet (n \bmod 2 = 0)\big) \vee \big(\forall\, n : \mathbb{Z} \bullet (n \bmod 2 = 1)\big)$$

Example: Distributivity

- WARNING: Existential quantification doesn't distribute over conjunction:

$$\neg \Big((\exists x : s \bullet P(x) \land Q(x)) \;\Leftrightarrow\; (\exists x : s \bullet P(x)) \land (\exists x : s \bullet Q(x)) \Big)$$

- Counterexample to distribution:

  There's a number that's even and there's a number that's odd:

  $$(\exists n : \mathbb{Z} \bullet (n \bmod 2 = 0)) \land (\exists n : \mathbb{Z} \bullet (n \bmod 2 = 1))$$

  But there isn't a number that's both even and odd:

  $$\exists n : \mathbb{Z} \bullet (n \bmod 2 = 0) \land (n \bmod 2 = 1)$$

Semi-distribution

- Universal quantification doesn't distribute over disjunction as an equivalence.
- But it does as an implication (strengthening):

$$\big(\forall x : s \bullet P(x)\big) \vee \big(\forall x : s \bullet Q(x)\big) \;\Rightarrow\; \big(\forall x : s \bullet P(x) \vee Q(x)\big)$$

- Existential quantification doesn't distribute over conjunction as equivalence.
- But it does as an implication (weakening)

$$\big(\exists x : s \bullet P(x) \wedge Q(x)\big) \;\Rightarrow\; \big(\exists x : s \bullet P(x)\big) \wedge \big(\exists x : s \bullet Q(x)\big)$$

Identities and Semi-identities

$$
\begin{array}{rrcll}
1. & (\forall x : s \bullet P(x)) & \Rightarrow & P(c) & c \in s \\
2. & P(c) & \Rightarrow & (\exists x : s \bullet P(x)) & c \in s \\
3. & (\neg\ \exists x : s \bullet P(x)) & \Leftrightarrow & (\forall x : s \bullet \neg\ P(x)) & \\
4. & (\forall x : s \bullet P(x)) & \Rightarrow & (\exists x : s \bullet P(x)) & \\
5. & (\neg\ \forall x : s \bullet P(x)) & \Leftrightarrow & (\exists x : s \bullet \neg\ P(x)) & \\
6. & (\forall x : s \bullet P(x) \land N) & \Leftrightarrow & (\forall x : s \bullet P(x)) \land N & \\
7. & (\forall x : s \bullet P(x) \lor N) & \Leftrightarrow & (\forall x : s \bullet P(x)) \lor N & \\
8. & (\forall x : s \bullet P(x)) \land (\forall x : s \bullet Q(x)) & \Leftrightarrow & (\forall x : s \bullet P(x) \land Q(x)) & \\
9. & (\forall x : s \bullet P(x)) \lor (\forall x : s \bullet Q(x)) & \Rightarrow & (\forall x : s \bullet P(x) \lor Q(x)) & \\
10. & (\exists x : s \bullet P(x) \land N) & \Leftrightarrow & (\exists x : s \bullet P(x)) \land N & \\
11. & (\exists x : s \bullet P(x) \lor N) & \Leftrightarrow & (\exists x : s \bullet P(x)) \lor N & \\
12. & (\exists x : s \bullet P(x) \land Q(x)) & \Rightarrow & (\exists x : s \bullet P(x)) \land (\exists x : s \bullet Q(x)) & \\
13. & (\exists x : s \bullet P(x)) \lor (\exists x : s \bullet Q(x)) & \Leftrightarrow & (\exists x : s \bullet P(x) \lor Q(x)) &
\end{array}
$$

Example: Multiple Quantifiers

- Order of universal and existential quantifiers is significant.
- "No matter what value x in s, a value y in t can be found such that..."

$$\forall x : s \bullet \exists y : t \bullet \ldots$$

- Value of y may depend on value of x. Example: "there's a larger one"

$$\forall x : \mathbb{N} \bullet \exists y : \mathbb{N} \bullet y > x \tag{1}$$

- "There's a value y in t so that no matter what value x in s is chosen,..."

$$\exists y : t \bullet \forall x : s \bullet \ldots$$

- Since y is bound first, y must be specified independently of x.
- "There's a number that's greater than every other number":

$$\exists y : \mathbb{N} \bullet \forall x : \mathbb{N} \bullet y > x \tag{2}$$

- Which is true and which is false?

Outline

Summary

- Previously: Propositional logic: truth-valued propositions.
- Truth functional connectives:
  - conjunction, disjunction, negation, implication, equivalence.
- First-order predicate logic adds predicates and quantification.
- Predicates: parametrised propositions with abstracted subjects.
- Quantifiers: universal and existential: for all ..., exists at least one ...
- Quantifiers apply to variables in parametrised predicates:
  - bound, free, substitution.
- Rich set of algebraic laws.
- Next lecture: Extending the natural deduction system to quantifiers.