Discrete Mathematics & Mathematical Reasoning
Predicates, Quantifiers and Proof Techniques

Colin Stirling

Informatics

Some slides based on ones by Myrto Arapinis

Recall propositional logic from last year (in Inf1CL)

Propositions can be constructed from other propositions using logical connectives

Recall propositional logic from last year (in Inf1CL)

Propositions can be constructed from other propositions using logical connectives

- Negation: $\neg$
- Conjunction: $\wedge$
- Disjunction: $\vee$
- Implication: $\rightarrow$
- Biconditional: $\leftrightarrow$

Recall propositional logic from last year (in Inf1CL)

Propositions can be constructed from other propositions using logical connectives

- Negation: $\neg$
- Conjunction: $\wedge$
- Disjunction: $\vee$
- Implication: $\rightarrow$
- Biconditional: $\leftrightarrow$

The truth of a proposition is defined by the truth values of its elementary propositions and the meaning of connectives

Recall propositional logic from last year (in Inf1CL)

Propositions can be constructed from other propositions using logical connectives

- Negation: $\neg$
- Conjunction: $\wedge$
- Disjunction: $\vee$
- Implication: $\rightarrow$
- Biconditional: $\leftrightarrow$

The truth of a proposition is defined by the truth values of its elementary propositions and the meaning of connectives

The meaning of logical connectives can be defined using truth tables

Propositional logic is not enough

Propositional logic is not enough

In propositional logic, from

- All men are mortal
- Socrates is a man

we cannot derive

- Socrates is mortal

Propositional logic is not enough

In propositional logic, from

- All men are mortal
- Socrates is a man

we cannot derive

- Socrates is mortal

We need a language to talk about objects, their properties and their relations

Predicate logic

Extends propositional logic by the new features

- Variables: x, y ,z, ...
- Predicates: $P(x)$, $Q(x)$, $R(x, y)$, $M(x, y, z)$, ...
- Quantifiers: $\forall$, $\exists$

Predicate logic

Extends propositional logic by the new features

- Variables: x, y ,z, ...
- Predicates: $P(x)$, $Q(x)$, $R(x, y)$, $M(x, y, z)$, ...
- Quantifiers: $\forall$, $\exists$

Predicates are a generalisation of propositions

- Can contain variables $M(x, y, z)$
- Variables stand for (and can be replaced by) elements from their domain
- The truth value of a predicate depends on the values of its variables

Examples

$P(x)$ is "$x > 5$" and x ranges over $\mathbb{Z}$ (integers)

- $P(8)$ is true
- $P(5)$ is false

Examples

$P(x)$ is "$x > 5$" and x ranges over $\mathbb{Z}$ (integers)

- $P(8)$ is true
- $P(5)$ is false

$Q(x)$ is "x is irrational" and x ranges over $\mathbb{R}$ (real numbers)

- $Q(\sqrt{2})$ is true
- $Q(\sqrt{4})$ is false

Examples

$P(x)$ is "$x > 5$" and x ranges over $\mathbb{Z}$ (integers)

- $P(8)$ is true
- $P(5)$ is false

$Q(x)$ is "x is irrational" and x ranges over $\mathbb{R}$ (real numbers)

- $Q(\sqrt{2})$ is true
- $Q(\sqrt{4})$ is false

$R(x, y)$ is "x divides y" and x, y range over $\mathbb{Z}^+$ (positive integers)

- $R(3, 9)$ is true
- $R(2, 9)$ is false

Quantifiers

- Universal quantifier, "For all": $\forall$
  $\forall x\ P(x)$ asserts that $P(x)$ is true for every x in the assumed domain

Quantifiers

- Universal quantifier, "For all": $\forall$
  $\forall x\ P(x)$ asserts that $P(x)$ is true for every x in the assumed domain
- Existential quantifier, "There exists": $\exists$
  $\exists x\ P(x)$ asserts that $P(x)$ is true for some x in the assumed domain

Quantifiers

- Universal quantifier, "For all": $\forall$
  $\forall x\ P(x)$ asserts that $P(x)$ is true for every x in the assumed domain
- Existential quantifier, "There exists": $\exists$
  $\exists x\ P(x)$ asserts that $P(x)$ is true for some x in the assumed domain
- The quantifiers are said to bind the variable x in these expressions. Variables in the scope of some quantifier are called bound variables. All other variables in the expression are called free variables

Quantifiers

- Universal quantifier, "For all": $\forall$
  $\forall x\ P(x)$ asserts that $P(x)$ is true for every x in the assumed domain
- Existential quantifier, "There exists": $\exists$
  $\exists x\ P(x)$ asserts that $P(x)$ is true for some x in the assumed domain
- The quantifiers are said to bind the variable x in these expressions. Variables in the scope of some quantifier are called bound variables. All other variables in the expression are called free variables
- A formula that does not contain any free variables is a proposition and has a truth value

Example: If n is an odd integer then n^2 is odd

- First, notice the quantifier is implicit

Example: If n is an odd integer then n^2 is odd

- First, notice the quantifier is implicit
- Let $P(n)$ mean n is odd where n is an integer (in $\mathbb{Z}$)

Example: If n is an odd integer then n^2 is odd

- First, notice the quantifier is implicit
- Let $P(n)$ mean n is odd where n is an integer (in $\mathbb{Z}$)
- So is: $\forall x$ (if $P(x)$ then $P(x^2)$)

Example: If n is an odd integer then n^2 is odd

- First, notice the quantifier is implicit
- Let $P(n)$ mean n is odd where n is an integer (in $\mathbb{Z}$)
- So is: $\forall x$ (if $P(x)$ then $P(x^2)$)
- $\forall x(P(x) \rightarrow P(x^2))$

Direct proof of $\forall x\ (P(x) \rightarrow Q(x))$

- Assume c is an arbitrary element of the domain

Direct proof of $\forall x\, (P(x) \rightarrow Q(x))$

- Assume c is an arbitrary element of the domain
- Prove that $P(c) \rightarrow Q(c)$

Direct proof of $\forall x \, (P(x) \rightarrow Q(x))$

- Assume c is an arbitrary element of the domain
- Prove that $P(c) \rightarrow Q(c)$
- That is, assume $P(c)$ then show $Q(c)$

Direct proof of $\forall x\ (P(x) \rightarrow Q(x))$

- Assume c is an arbitrary element of the domain
- Prove that $P(c) \rightarrow Q(c)$
- That is, assume $P(c)$ then show $Q(c)$
- Use the definition/properties of $P(c)$

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \to P(x^2))$ where $P(n)$ is n is odd

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \rightarrow P(x^2))$ where $P(n)$ is n is odd
- Assume n is arbitrary odd integer; what does that mean?

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \rightarrow P(x^2))$ where $P(n)$ is n is odd
- Assume n is arbitrary odd integer; what does that mean?
- that for some k, $n = 2k + 1$

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \rightarrow P(x^2))$ where $P(n)$ is n is odd
- Assume n is arbitrary odd integer; what does that mean?
- that for some k, $n = 2k + 1$
- Show n^2 is odd

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \rightarrow P(x^2))$ where $P(n)$ is n is odd
- Assume n is arbitrary odd integer; what does that mean?
- that for some k, $n = 2k + 1$
- Show n^2 is odd
- $n^2 = (2k + 1)^2$

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \rightarrow P(x^2))$ where $P(n)$ is n is odd
- Assume n is arbitrary odd integer; what does that mean?
- that for some k, $n = 2k + 1$
- Show n^2 is odd
- $n^2 = (2k + 1)^2$
- So, $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Example: If n is an odd integer then n^2 is odd

- $\forall x\ (P(x) \rightarrow P(x^2))$ where $P(n)$ is n is odd
- Assume n is arbitrary odd integer; what does that mean?
- that for some k, $n = 2k + 1$
- Show n^2 is odd
- $n^2 = (2k + 1)^2$
- So, $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
- n^2 has the form for some m, $n^2 = 2m + 1$; so n^2 is odd

Any odd integer is the difference of two squares

Nested quantifiers

- Every real number has an inverse w.r.t addition
  The domain is $\mathbb{R}$
  $$\forall x \, \exists y \, (x + y = 0)$$

- Every real number except zero has an inverse w.r.t multiplication
  The domain is $\mathbb{R}$
  $$\forall x \, (x \neq 0 \; \rightarrow \; \exists y \, (x \times y = 1))$$

Proving $\forall x\,(P(x) \rightarrow Q(x))$ by contraposition

- Uses equivalence of $(p \rightarrow q)$ and $(\neg q \rightarrow \neg p)$

Proving $\forall x\ (P(x) \rightarrow Q(x))$ by contraposition

- Uses equivalence of $(p \rightarrow q)$ and $(\neg q \rightarrow \neg p)$
- Assume c is an arbitrary element of the domain

Proving $\forall x\,(P(x) \rightarrow Q(x))$ by contraposition

- Uses equivalence of $(p \rightarrow q)$ and $(\neg q \rightarrow \neg p)$
- Assume c is an arbitrary element of the domain
- Prove that $\neg Q(c) \rightarrow \neg P(c)$

Proving $\forall x\,(P(x) \rightarrow Q(x))$ by contraposition

- Uses equivalence of $(p \rightarrow q)$ and $(\neg q \rightarrow \neg p)$
- Assume c is an arbitrary element of the domain
- Prove that $\neg Q(c) \rightarrow \neg P(c)$
- That is, assume $\neg Q(c)$ then show $\neg P(c)$

Proving $\forall x\ (P(x) \rightarrow Q(x))$ by contraposition

- Uses equivalence of $(p \rightarrow q)$ and $(\neg q \rightarrow \neg p)$
- Assume c is an arbitrary element of the domain
- Prove that $\neg Q(c) \rightarrow \neg P(c)$
- That is, assume $\neg Q(c)$ then show $\neg P(c)$
- Use the definition/properties of $\neg Q(c)$

if $x + y$ is even, then x and y have the same parity

if $x + y$ is even, then x and y have the same parity

Proof Let $n, m \in \mathbb{Z}$ be arbitrary. We will prove that if n and m do not have the same parity then $n + m$ is odd. Without loss of generality we assume that n is odd and m is even, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$, and $m = 2\ell$ for some $\ell \in \mathbb{Z}$. But then
$n + m = 2k + 1 + 2\ell = 2(k + \ell) + 1$. And thus $n + m$ is odd. Now by equivalence of a statement with it contrapositive derive that if $n + m$ is even, then n and m have the same parity.

If $n = ab$ where a, b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Proof by contradiction

- Want to prove that P is true

Proof by contradiction

- Want to prove that P is true
- Assume $\neg P$

Proof by contradiction

- Want to prove that P is true
- Assume $\neg P$
- Derive both R and $\neg R$ (a contradiction equivalent to False)

Proof by contradiction

- Want to prove that P is true
- Assume $\neg P$
- Derive both R and $\neg R$ (a contradiction equivalent to False)
- Therefore, $\neg\neg P$ which is equivalent to P

$\sqrt{2}$ is irrational

$\sqrt{2}$ is irrational

Proof Assume towards a contradiction that $\sqrt{2}$ is rational, that is there are integers a and b with no common factor other than 1, such that $\sqrt{2} = a/b$. In that case $2 = a^2/b^2$. Multiplying both sides by b^2, we have $a^2 = 2b^2$. Since b is an integer, so is b^2, and thus a^2 is even. As we saw previously this implies that a is even, that is there is an integer c such that $a = 2c$. Hence $2b^2 = 4c^2$, hence $b^2 = 2c^2$. Now, since c is an integer, so is c^2, and thus b^2 is even. Again, we can conclude that b is even. Thus a and b have a common factor 2, contradicting the assertion that a and b have no common factor other than 1. This shows that the original assumption that $\sqrt{2}$ is rational is false, and that $\sqrt{2}$ must be irrational.

There are infinitely many primes

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

Proof Suppose towards a contradiction that there are only finitely many primes $p_1, p_2, p_3, \ldots, p_k$. Consider the number $q = p_1 p_2 p_3 \ldots p_k + 1$, the product of all the primes plus one. By hypothesis q cannot be prime because it is strictly larger than all the primes. Thus, by the lemma, it has a prime divisor, p. Because $p_1, p_2, p_3, \ldots, p_k$ are all the primes, p must be equal to one of them, so p is a divisor of their product. So we have that p divides $p_1 p_2 p_3 \ldots p_k$, and p divides q, but that means p divides their difference, which is 1. Therefore $p \leq 1$. Contradiction. Therefore there are infinitely many primes.

Proof by cases

- To prove a conditional statement of the form

$$(p_1 \vee \cdots \vee p_k) \rightarrow q$$

- Use the tautology

$$((p_1 \vee \cdots \vee p_k) \rightarrow q) \leftrightarrow ((p_1 \rightarrow q) \wedge \cdots \wedge (p_k \rightarrow q))$$

- Each of the implications $p_i \rightarrow q$ is a case

If n is an integer then $n^2 \geq n$

Constructive proof of $\exists x \; P(x)$

Constructive proof of $\exists x \ P(x)$

- Exhibit an actual witness w from the domain such that $P(w)$ is true

Constructive proof of $\exists x \; P(x)$

- Exhibit an actual witness w from the domain such that $P(w)$ is true
- Therefore, $\exists x \; P(x)$

There exists a positive integer that can be written as the sum of cubes of positive integers in two different ways

There exists a positive integer that can be written as the sum of cubes of positive integers in two different ways

- 1729 is such a number because

There exists a positive integer that can be written as the sum of cubes of positive integers in two different ways

- 1729 is such a number because
- $10^3 + 9^3 = 1729 = 12^3 + 1^3$

Nonconstructive proof of $\exists x \; P(x)$

Nonconstructive proof of $\exists x\ P(x)$

- Show that there must be a value v such that $P(v)$ is true

Nonconstructive proof of $\exists x \; P(x)$

- Show that there must be a value v such that $P(v)$ is true
- but we don't know what this value v is

There exist irrational numbers x and y such that x^y is rational

There exist irrational numbers x and y such that x^y is rational

Proof We need only prove the existence of at least one example. Consider the case $x = \sqrt{2}$ and $y = \sqrt{2}$. We distinguish two cases:

Case $\sqrt{2}^{\sqrt{2}}$ is rational. In that case we have shown that for the irrational numbers $x = y = \sqrt{2}$, we have that x^y is rational

Case $\sqrt{2}^{\sqrt{2}}$ is irrational. In that case consider $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We then have that

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$$

But since 2 is rational, we have shown that for $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, we have that x^y is rational

We have thus shown that in any case there exist some irrational numbers x and y such that x^y is rational

Disproving $\forall x\ P(x)$ with a counter-example

- $\neg\forall x\ P(x)$ is equivalent to $\exists x\ \neg P(x)$

Disproving $\forall x\ P(x)$ with a counter-example

- $\neg\forall x\ P(x)$ is equivalent to $\exists x\ \neg P(x)$
- To establish that $\neg\forall x\ P(x)$ is true find a w such that $P(w)$ is false

Disproving $\forall x\ P(x)$ with a counter-example

- $\neg\forall x\ P(x)$ is equivalent to $\exists x\ \neg P(x)$
- To establish that $\neg\forall x\ P(x)$ is true find a w such that $P(w)$ is false
- So, w is a counterexample to the assertion $\forall x\ P(x)$

Every positive integer is the sum of the squares of 3 integers

Every positive integer is the sum of the squares of 3 integers

The integer 7 is a counterexample. So the claim is false