Proof techniques[1]

Myrto Arapinis
School of Informatics
University of Edinburgh

September 22, 2014

[1] Slides mainly borrowed from Richard Mayr

Revisiting the Socrates Example

We have the two premises:

- "All men are mortal"
- "Socrates is a man"

And the conclusion:

- "Socrates is mortal"

How do we get the conclusion from the premises?

Rules of inference

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array} \qquad \begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array} \qquad \begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array} \qquad \begin{array}{l} p \lor q \\ \neg p \\ \hline \therefore q \end{array} \qquad \begin{array}{l} p \\ \hline \therefore p \lor q \end{array}$$

$$\begin{array}{l} p \land q \\ \hline \therefore p \end{array} \qquad \begin{array}{l} p \\ q \\ \hline \therefore p \land q \end{array} \qquad \begin{array}{l} \neg p \lor q \\ p \lor r \\ \hline \therefore q \lor r \end{array}$$

$$\begin{array}{l} P(u) \text{ for an arbitrary } u \in \mathcal{U} \\ \hline \therefore\ \forall x.\ P(x) \end{array} \qquad \begin{array}{l} \forall x.\ P(x) \\ \hline \therefore\ P(u) \text{ for any arbitrary } u \in \mathcal{U} \end{array}$$

$$\begin{array}{l} \exists x.\ P(x) \\ \hline \therefore\ P(u) \text{ for some } u \in \mathcal{U} \end{array} \qquad \begin{array}{l} P(u) \text{ for some } u \in \mathcal{U} \\ \hline \therefore\ \exists x.\ P(x) \end{array}$$

Revisiting the Socrates Example

$$\begin{array}{l} \forall x.\ Man(x) \rightarrow Mortal(x) \\ Man(Socrates) \\ \hline \therefore\ Mortal(Socrates) \end{array}$$

Proving $\forall x.\ P(x) \to Q(x)$

- Many theorems have the form:

$$\forall x \in \mathcal{U}.\ P(x) \to Q(x)$$

- To prove them, we show that where c is an arbitrary element of the domain $\mathcal{U}$, $P(c) \to Q(c)$
- By universal generalization the truth of the original formula follows

$$\frac{R(u) \text{ for an arbitrary } u \in \mathcal{U}}{\therefore\ \forall x.\ R(x)}$$

- So, we must prove something of the form: $p \to q$

Proving $\forall x.\ P(x) \to Q(x)$: trivial proof

If we know $\forall x.\ Q(x)$ is true, then $\forall x.\ P(x) \to Q(x)$ is true as well

Proving $\forall x.\ P(x) \to Q(x)$: trivial proof

If we know $\forall x.\ Q(x)$ is true, then $\forall x.\ P(x) \to Q(x)$ is true as well

For all $x \in \mathbb{N}$, if x is even, then $x = x$

Proving $\forall x.\ P(x) \to Q(x)$: trivial proof

If we know $\forall x.\ Q(x)$ is true, then $\forall x.\ P(x) \to Q(x)$ is true as well

For all $x \in \mathbb{N}$, if x is even, then $x = x$

Proof Let $n \in \mathbb{N}$. We need to show that if n is even then $n = n$. But we trivially have that $n = n$, and thus by definition of $\to$ we can conclude that if n is even then $n = n$. Finally by universal generalization we can conclude that $\forall x.\ P(x) \to Q(x)$. $\square$

Proving $\forall x.\ P(x) \rightarrow Q(x)$: vacuous proof

If we know $\forall x.\ \neg P(x)$ is true, then $\forall x.\ P(x) \rightarrow Q(x)$ is true as well

Proving $\forall x.\ P(x) \to Q(x)$: vacuous proof

If we know $\forall x.\ \neg P(x)$ is true, then $\forall x.\ P(x) \to Q(x)$ is true as well

For all $x \in \mathbb{N}$, if $x < x$, then x is even

Proving $\forall x.\ P(x) \rightarrow Q(x)$: vacuous proof

If we know $\forall x.\ \neg P(x)$ is true, then $\forall x.\ P(x) \rightarrow Q(x)$ is true as well

For all $x \in \mathbb{N}$, if $x < x$, then x is even

Proof Let $n \in \mathbb{N}$. We need to show that if $n < n$ then n is even. But we trivially have that $\neg(n < n)$, and thus by definition of $\rightarrow$ we can conclude that if $n < n$ then n is even. Finally by universal generalization we can conclude that $\forall x.\ P(x) \rightarrow Q(x)$. $\square$

Proving $\forall x.\ P(x) \to Q(x)$: direct proof

Let $u \in \mathcal{U}$. Assume that $P(u)$ is true. Use rules of inference, axioms, and logical equivalences to show that $Q(u)$ must also be true. Finally by universal generalization we can conclude that $\forall x.\ P(x) \to Q(x)$.

Proving $\forall x.\ P(x) \to Q(x)$: direct proof

Let $u \in \mathcal{U}$. Assume that $P(u)$ is true. Use rules of inference, axioms, and logical equivalences to show that $Q(u)$ must also be true. Finally by universal generalization we can conclude that $\forall x.\ P(x) \to Q(x)$.

For all $x \in \mathbb{Z}$, if x is odd, then $x + 1$ is even

Proving $\forall x.\ P(x) \to Q(x)$: direct proof

Let $u \in \mathcal{U}$. Assume that $P(u)$ is true. Use rules of inference, axioms, and logical equivalences to show that $Q(u)$ must also be true. Finally by universal generalization we can conclude that $\forall x.\ P(x) \to Q(x)$.

For all $x \in \mathbb{Z}$, if x is odd, then $x + 1$ is even

Proof Let $n \in \mathbb{Z}$. Assume n is odd, that is $n = 2k + 1$ for some integer k. In that case $n + 1 = 2(k + 1)$. And thus $n + 1$ is even. Finally by universal generalization we can conclude that for all $x \in \mathbb{Z}$, if x is odd, then $x + 1$ is even. $\square$

Proving $\forall x.\ P(x) \to Q(x)$: proof by contraposition

Let $u \in \mathcal{U}$. Prove that $\neg Q(u) \to \neg P(u)$. By equivalence of a statement with it contrapositive derive that $P(u) \to Q(u)$. Finally by universal generalization we can conclude that
$\forall x.\ P(x) \to Q(x)$.

Proving $\forall x.\ P(x) \to Q(x)$: proof by contraposition

Let $u \in \mathcal{U}$. Prove that $\neg Q(u) \to \neg P(u)$. By equivalence of a statement with it contrapositive derive that $P(u) \to Q(u)$. Finally by universal generalization we can conclude that $\forall x.\ P(x) \to Q(x)$.

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

Proving $\forall x.\ P(x) \to Q(x)$: proof by contraposition

Let $u \in \mathcal{U}$. Prove that $\neg Q(u) \to \neg P(u)$. By equivalence of a statement with it contrapositive derive that $P(u) \to Q(u)$. Finally by universal generalization we can conclude that
$\forall x.\ P(x) \to Q(x)$.

> For all integers x and y, if $x + y$ is even, then x and y have the same parity

Proof Let $n, m \in \mathbb{Z}$. 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. Finally by universal generalization we can conclude that for all $x \in \mathbb{Z}$, if x is odd, then $x + 1$ is even.

Proof by contradiction

- The idea is to assume the opposite of what one is trying to prove and then show that this leads to something that is clearly nonsensical: a contradiction.

Proof by contradiction

- The idea is to assume the opposite of what one is trying to prove and then show that this leads to something that is clearly nonsensical: a contradiction.

- To prove that P is true, we assume that it is not. That is we assume $\neg P$, and then prove both R and $\neg R$. But for any proposition R, $R \wedge \neg R \equiv \mathrm{F}$. So we have shown that $\neg P \to \mathrm{F}$. The only way this implication can be true is if $\neg P$ is false, *i.e.* P is true.

Proof by contradiction (Example 1)

$\sqrt{2}$ is irrational

Proof by contradiction (Example 1)

$\sqrt{2}$ is irrational

<u>Proof</u> 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 last week 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. $\square$

Proof by contradiction (Example 2)

There are infinitely many prime numbers

Proof by contradiction (Example 2)

There are infinitely many prime numbers

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

Proof by contradiction (Example 2)

There are infinitely many prime numbers

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. $\square$

Proof by cases

- To prove a conditional statement of the form:

$$p_1 \vee \cdots \vee p_k \to q$$

- Use the tautology:

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

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

Proof by cases (Example)

$$\forall n, m \in \mathbb{N}.\ \mathsf{max}(n, m) \stackrel{\mathsf{def}}{=} \begin{cases} n & \text{if } n \geq m \\ m & \text{otherwise} \end{cases}$$

For all $n, m, \ell \in \mathbb{N}.\ \mathsf{max}(n, \mathsf{max}(m, \ell)) = \mathsf{max}(\mathsf{max}(n, m), \ell)$

Proof by cases (Example)

$$\forall n, m \in \mathbb{N}.\ \max(n, m) \stackrel{\text{def}}{=} \begin{cases} n & \text{if } n \geq m \\ m & \text{otherwise} \end{cases}$$

For all $n, m, \ell \in \mathbb{N}$. $\max(n, \max(m, \ell)) = \max(\max(n, m), \ell)$

Proof Let $n, m, \ell \in \mathbb{N}$
Case $n \geq m \geq \ell$. $\max(n, \max(m, \ell)) = \max(n, m) = n = \max(n, \ell) = \max(\max(n, m), \ell)$
Case $n \geq \ell \geq m$. $\max(n, \max(m, \ell)) = \max(n, \ell) = n = \max(n, \ell) = \max(\max(n, m), \ell)$
...
In any possible case we proved that $\max(n, \max(m, \ell)) = \max(\max(n, m), \ell)$. Finally by universal generalization we can conclude that for all $n, m, \ell \in \mathbb{N}$. $\max(n, \max(m, \ell)) = \max(\max(n, m), \ell)$. $\square$

Proving $\exists x.\ P(x)$: constructive proof

- Find an explicit value of $u \in \mathcal{U}$, for which $P(u)$ is true
- Then is true by Existential Generalization:

$$\frac{R(u) \text{ for some element } u}{\therefore\ \exists x.\ R(x)}$$

Proving $\exists x.\ P(x)$: constructive proof

- Find an explicit value of $u \in \mathcal{U}$, for which $P(u)$ is true
- Then is true by Existential Generalization:

$$\frac{R(u) \text{ for some element } u}{\therefore\ \exists x.\ R(x)}$$

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

Proving $\exists x.\ P(x)$: constructive proof

- Find an explicit value of $u \in \mathcal{U}$, for which $P(u)$ is true
- Then is true by Existential Generalization:

$$\frac{R(u) \text{ for some element } u}{\therefore\ \exists x.\ R(x)}$$

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

Proof 1729 is such a number since $1729 = 10^3 + 9^3 = 12^3 + 1^3 \square$

Proving $\exists x.\ P(x)$: non-constructive proof

In a non-constructive existence proof, we prove that there must exist a $u \in \mathcal{U}$ exists which makes $P(u)$ without actually finding this u

Proving $\exists x.\ P(x)$: non-constructive proof

In a non-constructive existence proof, we prove that there must exist a $u \in \mathcal{U}$ exists which makes $P(u)$ without actually finding this u

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

Proving $\exists x.\ P(x)$: non-constructive proof

In a non-constructive existence proof, we prove that there must exist a $u \in \mathcal{U}$ exists which makes $P(u)$ without actually finding this u

There exist some 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

Proving $\exists x.\ \neg P(x)$: counter-examples

- Recall $\exists x.\ \neg P(x) \equiv \neg\forall x.\ P(x)$
- To establish that $\neg\forall x.\ P(x)$ is true (or is false) find a $u \in \mathcal{U}$ such that $\neg P(u)$ is true or $P(u)$ is false.
- In this case u is called a counterexample to the assertion

Proving $\exists x.\ \neg P(x)$: counter-examples

- Recall $\exists x.\ \neg P(x) \equiv \neg\forall x.\ P(x)$
- To establish that $\neg\forall x.\ P(x)$ is true (or is false) find a $u \in \mathcal{U}$ such that $\neg P(u)$ is true or $P(u)$ is false.
- In this case u is called a counterexample to the assertion

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

Proving $\exists x.\ \neg P(x)$: counter-examples

- Recall $\exists x.\ \neg P(x) \equiv \neg\forall x.\ P(x)$
- To establish that $\neg\forall x.\ P(x)$ is true (or is false) find a $u \in \mathcal{U}$ such that $\neg P(u)$ is true or $P(u)$ is false.
- In this case u is called a counterexample to the assertion

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

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

“Proof” that $1 = 2$

Step	**Reason**
1. $a = b$	Premise
2. $a^2 = ab$	Multiply both sides by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides
4. $(a - b)(a + b) = b(a - b)$	Algebra
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b because $a = b$
7. $2 = 1$	Divide both sides by b

“Proof” that $1 = 2$

Step	**Reason**
1. $a = b$	Premise
2. $a^2 = ab$	Multiply both sides by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides
4. $(a - b)(a + b) = b(a - b)$	Algebra
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b because $a = b$
7. $2 = 1$	Divide both sides by b

Step5. $a - b = 0$ by the premise and division by 0 is undefined!