Exercises Week 7
Argument and Proof

Hans Georg Schaathun

12th November 2015

Period 30 September – 6 October 2015

Reading Stein *et al* cover this material in Chapter 3.

Programme This document details the programme for the week, including exercises and pointers to other material. It is available in two versions:

1. as a PDF document.
2. as a web site. This depends on MathML and may require firefox/iceweasel to display correctly.

The web version includes inline video. The pdf version shows a still image from the video, providing a hyperlink directly to the video on the web site.

1 Wednesday 30 September 2015

Having learnt direct proofs last week, we are going to study how we can make such proofs with quantified statements.

1.1 Universal Generalisation

Related reading: Stein *et al.* p. 180–181 or Rosen p. 72–73

THEORY

Universal generalisation is the straight-forward direct proof of a universally quantified statements. This is essentially similar to the conditional proof, to prove an implication.

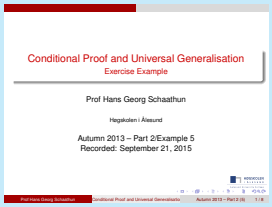
Slides

EXERCISE EXAMPLE

Problem 1.1 *Consider the following assertation which we want to prove:*

The sum of two odd integers is even.

1. *Rephrase the statement symbolically as an implication.*
2. *Prove the implication.*
3. *Rephrase the statement symbolically as a quantified statements, making all quantifiers explicit.*
4. *Prove the quantified statement.*



OGG MP4 Slides

Exercise 1.1 *Consider the assertion that* if m is odd, then m^2 is odd.

1. *Formulate the assertion symbolically as an implication.*
2. *Prove the resulting statement using a conditional proof.*
3. *Rephrase the assertion with explicit quantification.*
4. *Prove the resulting statement using universal generalisation.*

Exercise 1.2 *Are there any implicit quantifiers in the statement,* the product of odd integers is odd*? Which?*

Exercise 1.3 *Prove that the product of two odd integers is odd.*

1.2 Analysing quantified expressions

Related reading: Stein *et al.* p. 168–173 or Rosen p. 41–45

THEORY

Theorem 1 *The following two statements are equivalent:*

$$\neg\forall x \in U,\ p(x) \tag{1}$$
$$\exists x \in U,\ \neg p(x) \tag{2}$$

Slides

THEORY

Theorem 2 *Let U_2 be a universe, and $U_1 = \{x \mid x \in U_2 \wedge q(x)\}$ is another universe. Let $p(x)$ and $q(x)$ be statements over U_2.*

$$\exists x \in U_1, p(x) \text{ equivalent to } \exists x \in U_2, (q(x) \wedge p(x))$$

OGG MP4 Slides

Exercise 1.4 *Consider the following slight modification of the theorem:*

$$\exists x \in U_1, p(x) \text{ equivalent to } \exists x \in U_2, (q(x) \Rightarrow p(x)).$$

Is this statement true? Either give a counter-example or an argument to justify it.

THEORY

Theorem 3 *Using the definitions in Theorem 2, we have*

$$\forall x \in U_1, p(x) \text{ equivalent to } \forall x \in U_2, (q(x) \Rightarrow p(x)).$$

OGG MP4 Slides

Exercise 1.5 *Consider the following slight modification of the theorem:*

$$\forall x \in U_1, p(x) \text{ equivalent to } \forall x \in U_2, (q(x) \wedge p(x)).$$

Is this statement true? Either give a counter-example or an argument to justify it.

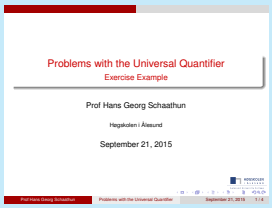
EXERCISE EXAMPLE

Problem 1.2 *Which of the following statements are true and which are false?*

1. $\forall z \in \mathbb{Z},\ z^2 \geq z$
2. $\forall z \in \mathbb{R},\ z^2 \geq z$

The following definitions are used

$$\mathbb{Z} = \{\ldots, -1, 0, +1, \ldots\} \quad \text{the integers} \tag{3}$$
$$\mathbb{R} \text{ is the set of real numbers} \tag{4}$$



OGG MP4 Slides

SUPPORTING THEORY

This video presents a summary of the different principles we have used for direct proofs.

Related reading: Stein *et al.* p. 181–182 or Rosen p. 62 and 72

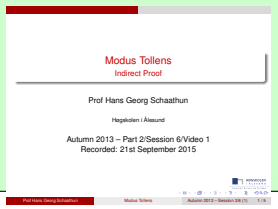
OGG MP4 Slides

2 Thursday 1 October 2015

Related reading: Stein *et al.* p. 183–188 or Rosen p. 43–45 and 88–91

THEORY

Modus Tollens is the basic example of an *indirect proof.*



OGG MP4 Slides

Exercise 2.1 *Consider each of these arguments. For each one, decide whether the argument is valid, and if it is, what principle has been used.*

1. *All men are mortal. Sokrates is mortal. Therefore Sokrates is a man.*
2. *All men are mortal. Sokrates is a man. Therefore Sokrates is mortal.*
3. *All men are mortal. Dracula is immortal. Therefore Dracula is not a man.*

THEORY

Definition 1 *The statement* $(\neg q) \Rightarrow (\neg p)$ *is called the contrapositive statement of* $p \Rightarrow q$.

Lemma 1 *A statement and its contrapositive have the same truth value:* $(\neg q) \Rightarrow (\neg p) \equiv p \Rightarrow q$

OGG MP4 Slides

THEORY

Definition 2 *We call* $q \Rightarrow p$ *the converse statement of* $p \Rightarrow q$.

Clearly, the converse statement has a different truth value in general.

OGG MP4 Slides

EXERCISE EXAMPLE

Problem 2.1 *Prove that* $x^2 > 4$ *implies* $|x| > 2$.

OGG MP4 Slides

Exercise 2.2 (Video 'contraposition' and 'converse') *Write down the contrapositive and converse statements of each of the following:*

1. *If the alarm clock is broken, then I will oversleep.*
2. *Alice will mow the lawn tomorrow, if it is not raining.*
3. *You can catch the six o'clock bus home, only if you complete these exercises in ten minutes,*

Theory

Reductio ad Absurdum — proof by contradiction — is a very important class of proofs. It is nothing more than Modus Tollens put into practice.

OGG MP4 Slides

Exercise 2.3 (Video 'contradiction') *Prove (by contradiction) that for all real numbers x, $x^2 - x \neq 0$ implies $x \neq 0$.*

Exercise Example

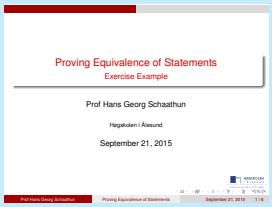
Problem 2.2 *Prove that there is no largest prime number.*

OGG MP4 Slides

Exercise Example

Problem 2.3 *Prove that the following four statements are equivalent*

1. *n is odd*
2. *$n+1$ is even*
3. *$3n$ is odd*
4. *$3n+1$ is even*



OGG MP4 Slides

2.1 Some practical examples

Exercise 2.4 *Consider the two predicates*

$$P(a) := \exists a^{-1} \in \mathbb{Z}_n, \tag{5}$$

$$Q(a) := \forall b \in \mathbb{Z}_n, \quad xa = b \text{ has a solution.} \tag{6}$$

Answer the following

Lemma 2 *If a has a multiplicative inverse $a^{-1} \in \mathbb{Z}_n$, then the equation $a \cdot x = b$ in $\mathbb{Z}_n$ has the solution $x = a^{-1} \cdot b$.*

Lemma 3 *Suppose there is a $b \in \mathbb{Z}_n$ such that the equation $a \cdot x = b$ does not have a solution. Then a does not have a multiplicative inverse.*

Table 1: Lemmata for Exercise 2.4.

1. *Formulate Lemma 2 as a logic formula using $P(a)$ and $Q(a)$*
2. *Formulate Lemma 3 as a logic formula using $P(a)$ and $Q(a)$*
3. *What logic relationship is there between the corollary and the lemma?*
4. *Prove the corollary, using the ideas from the previous three questions.*

Hint: review the material on indirect proofs.

Exercise 2.5 *Review the slides on «Euclid's Algorithm» and write pseudo-code for Euclid's algorithm.*

Exercise 2.6 *Based on your pseudo-code in the previous exercise, prove that Euclid's algorithm correctly returns the highest common factor.*

3 Compulsory Assignment (Tuesday 6 October 2015)

Exercise 3.1 *Make truth tables for the following expressions:*

1. $s \Leftrightarrow t$
2. $((\neg s) \wedge (\neg t)) \vee (s \wedge t)$

Compare the two truth tables and comment.

Exercise 3.2 *Rewrite the following arguments in symbolic form. For each argument, decide whether it is valid or not, and if it is valid, which form of argument is used.*

1. *When it is morning, the rooster crows. The rooster crows. Therefore it is morning.*
2. *When it is morning, the rooster crows. It is morning. Therefore the rooster crows.*
3. *When it is morning, the rooster crows. The rooster is silent. Therefore it is not morning.*

Exercise 3.3 *Rewrite the following arguments in symbolic form. For each argument, decide whether it is valid or not, and if it is valid, which form of argument is used.*

Theorem 4 (The Chinese Remainder Theorem) *If m and n are relatively prime integers, and $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$, then the set of equations*

$$x \mod m = a, \tag{7}$$
$$x \mod n = b \tag{8}$$

has exactly one solution for an an integer $x \in \mathbb{Z}_{mn}$, given by

$$x = a \cdot m' \cdot m + b \cdot n' \cdot n,$$

where m' is m^{-1} modulo n and n' is n^{-1} modulo m.

Table 2: Chinese Remainder Theorem for Exercise 3.6.

1. *When the sun is shining, I cycle to work. The sun is not shining. Therefore I do not cycle to work.*
2. *When the sun is shining, I cycle to work. The sun is shining. Therefore I cycle to work.*
3. *When the sun is shining, I cycle to work. The I cycle to work. Therefore the sun is shining.*

Exercise 3.4 *Prove that if $x^3 > 8$, then $x > 2$.*

Exercise 3.5 *Prove the following statement*

The product of two even integers is even.

Exercise 3.6 *Prove that the solution we designed for the Chinese Remainder Theorem is indeed unique.*

Hint *You can do the proof by contradiction. Suppose there are two distinct solutions $x \neq x'$, and use the ideas used in the video proving RSA.*

4 Summary of proof techniques

Students should be able to recognise and use the following proof techniques.

Modus ponens The most direct proof technique in the collection.

Conditional proof Another direct proof technique in the collection, used to proof implications.

Universal generalisation The direct proof technique for universally quantified statements. This is hardly distinguishable from conditional proofs.

Modus tollens An indirect analog of modus ponens.

Reductio ad Absurdum (proof by contradiction) The most generic indirect analog.

Mathematical induction Used to prove $P(x)$ for any natural number x.

Contrapositive This is not a proof technique, but an approach to rephrase statements to apply other proof techniques that would not otherwise be applicable.