Algorithmic Foundations 2 - Tutorial Sheet 5

Methods of Proof

1. Write out the following arguments using quantifiers, connectives, and symbols to stand for propositions as necessary, explaining which rules of inference are used for each step.

   (a) "Linda, a student in this class, owns a Porsche. Everyone who owns a Porsche has been caught speeding. Therefore, someone in this class has been caught speeding".

Solution: Let x be in the universe of all students and define the following predicates:

- $C(x)$: x is in this class;
- $P(x)$: x owns a Porsche;
- $S(x)$: x has been caught speeding.

We are therefore given the premises $C(\mathit{Linda})$, $P(\mathit{Linda})$ and $\forall x.\,(P(x) \rightarrow S(x))$. We want to conclude that $\exists x\,.(C(x) \wedge S(x))$.

1. $\forall x.\,(P(x) \rightarrow S(x))$	premise
2. $P(\mathit{Linda}) \rightarrow S(\mathit{Linda})$	universal instantiation using 1
3. $P(\mathit{Linda})$	premise
4. $S(\mathit{Linda})$	modus ponens using 2,3
5. $C(\mathit{Linda})$	premise
6. $C(\mathit{Linda}) \wedge S(\mathit{Linda})$	conjunction using 4,5
7. $\exists x.(C(x) \wedge S(x))$	existential generalisation using 6

   (b) "Each of five flatmates, Tracy, Alan, Susan, John and Catherine, has taken AF2. Every student who has taken AF2 can take Algorithmics 3. Therefore, all five flatmates can take Algorithmics 3 next year".

Solution: Let x be in the universe of all students and define the following predicates:

- $F(x)$: x is one of the five flatmates listed;
- $\mathit{AF2}(x)$: x has taken AF2;
- $\mathit{Alg3}(x)$: x can take Algorithmics 3.

We are therefore given the premises $\forall x.\,(F(x) \rightarrow \mathit{AF2}(x))$ and $\forall x.\,(\mathit{AF2}(x) \rightarrow \mathit{Alg3}(x))$ and we want to conclude that $\forall x.\ (F(x) \rightarrow \mathit{Alg3}(x))$. In the below, let y be an arbitrary student.

1. $\forall x.\,(F(x) \rightarrow \mathit{AF2}(x))$	premise
2. $F(y) \rightarrow \mathit{AF2}(y)$	universal instantiation using 1
3. $\forall x.\,(\mathit{AF2}(x) \rightarrow \mathit{Alg3}(x))$	premise
4. $\mathit{AF2}(y) \rightarrow \mathit{Alg3}(y)$	universal instantiation using 3
5. $F(y) \rightarrow \mathit{Alg3}(y)$	hypothetical syllogism using 2,4
6. $\forall x.\,(F(x) \rightarrow \mathit{Alg3}(x))$	universal generalisation using 5

2. The following argument is an incorrect proof of the conjecture "if n^2 is not divisible by 3, then n is not divisible by 3".

   > "If n^2 is not divisible by 3, then n^2 does not equal $3{\cdot}k$ for some integer k. Hence n does not equal $3{\cdot}l$ for some integer l. Therefore, n is not divisible by 3".

   The reason it is incorrect is that circular reasoning has been used. Where has the error in reasoning been made?

   Ignoring the incorrect proof, does the original conjecture hold (i.e. if n^2 is not divisible by 3, then n is not divisible by 3)? If it is `true`, then give a proof; if not, give a counterexample.

   Solution: The statement beginning with the word "Hence" does not follow from what has preceded it. The writer has implied that it does, but nothing in the statement "n^2 does not equal $3{\cdot}k$ for some integer k" immediately allows us to conclude that "n does not equal $3{\cdot}l$ for some integer l". The writer must prove this.

   Even though this particular proof is incorrect, the conjecture is `true`. This can be demonstrated using for example an indirect proof. In other words, we prove that if n is divisible by 3, then n^2 is divisible by 3.

   Suppose that n is divisible by 3, then $n = 3{\cdot}l$ for some integer l. Hence $n^2 = 9{\cdot}l^2 = 3{\cdot}(3{\cdot}l^2)$, and therefore n^2 is divisible by 3 as required.

3. (a) Prove the proposition $P(0)$, where $P(n)$ is the proposition "if n is a positive integer greater than 1, then $n^2 > n$". What kind of proof did you use?

   Solution: The proposition is vacuously `true` since 0 is not a positive integer greater than 1. So a vacuous proof was used.

   (b) Prove the proposition $P(1)$, where $P(n)$ is the proposition "if n is a positive integer, then $n^2 \geq n$". What kind of proof did you use?

   Solution: We need to prove the proposition "if 1 is a positive integer, then $1^2 \geq 1$". The conclusion is the `true` statement $1 \geq 1$. Therefore the implication is `true`. This is an example of a trivial proof, since we did not use the hypothesis in order to show that the conclusion is `true`.

4. Prove that the square of an even integer is an even integer by using:

   (a) a direct proof

   Solution: If n is an even integer, then $n = 2{\cdot}k$ for some integer k. Hence, $n^2 = 4{\cdot}k^2 = 2{\cdot}(2{\cdot}k^2)$, and therefore n^2 is an even integer as required.

   (b) an indirect proof

   Solution: In an indirect proof we need to show that if n^2 is not even, then n is not even, i.e. if n^2 is odd, then n is odd. Therefore we assume n^2 is odd, by definition there exists $k \in \mathbb{N}$ such that

   $$\begin{aligned} n^2 = 2{\cdot}k+1 \ &\Rightarrow n^2 - 1 = 2{\cdot}k && \text{rearranging} \\ &\Rightarrow (n{-}1)(n{+}1) = 2{\cdot}k && \text{rearranging.} \end{aligned}$$

Therefore, by definition, we have that $(n-1)(n+1)$ is even, which implies that either $(n-1)$ or $(n+1)$ is even, in either case this implies that n is odd as required.

(c) a proof by contradiction.

Solution: Suppose that n is even and for a contradiction that n^2 is not even (i.e. n^2 is odd). Using the same arguments as in the indirect proof above, from the fact that n^2 is odd, we can show that n is odd yielding a contradiction, and hence n^2 is even.

5. Prove that the product of two rational numbers is rational.

   Note: a rational number is a number which can be expressed as a fraction of the form p/q, where p and q are integers and $q{\neq}0$.

Solution: If a and b are rational numbers, then we can write $a = p/q$ and $b = r/s$ for integers p, q, r and s such that $q{\neq}0$ and $s{\neq}0$. Therefore $a{\cdot}b = (p{\cdot}r)/(q{\cdot}s)$ which is a rational number, since $p{\cdot}r$ and $r{\cdot}s$ are integers and $q{\cdot}s \neq 0$.

Note this is a direct proof.

6. Prove or disprove that the product of two irrational numbers is irrational

   Note: an irrational number is a number that cannot be expressed as a fraction p/q, where p and q are integers and $q{\neq}0$.

Solution: The statement is `false`. If $a = b = \sqrt{2}$ ($\sqrt{2}$ was shown to be irrational in the lectures), then $a{\cdot}b = 2$ which is a rational number.

Note this is a proof by counterexample.

7. Prove that the following statements are equivalent, where n is an integer:

   1. n is even;
   2. $n + 1$ is odd;
   3. $3{\cdot}n + 1$ is odd.

Solution:

1 → 2: If n is even, then $n = 2{\cdot}k$ for some integer k. Therefore $n{+}1 = 2{\cdot}k{+}1$, and hence $n{+}1$ is odd.

2 → 3: If $n{+}1$ is odd, then $n{+}1 = 2{\cdot}k{+}1$ for some integer k. Therefore $n = 2{\cdot}k$ and $3{\cdot}n{+}1 = 3{\cdot}(2{\cdot}k){+}1 = 2{\cdot}(3{\cdot}k){+}1$, and hence $3{\cdot}n{+}1$ is odd.

3 → 1: If $3{\cdot}n{+}1$ is odd and for a contradiction that n is odd. Then $n = 2{\cdot}k{+}1$ for some integer k, so that $3{\cdot}n{+}1 = 3{\cdot}(2{\cdot}k{+}1){+}1 = 2{\cdot}(3{\cdot}k{+}2)$, and hence $3{\cdot}n{+}1$ is even yielding a contradiction. Hence n is even.

As explained in the lectures, using the hypothetical syllogism rule of inference the equivalences between the statements follows. In particular, we have:

- from **2** → **3** and **3** → **1**, it follow (using hypothetical syllogism) that **2** → **1**.
- from **1** → **2** and **2** → **3**, it follows (using hypothetical syllogism) that **1** → **3**.
- from **3** → **1** and **1** → **2**, it follows (using hypothetical syllogism) that **3** → **2**.

8. Use a proof by cases to show that if x and y are real numbers, then $\min(x, y)+\max(x, y) = x+y$.

Solution: We have the following cases to consider.

- If $x<y$, then $\min(x, y) = x$ and $\max(x, y) = y$. Hence $\min(x, y)+ \max(x, y) = x+y$.
- If $x=y$, then $\min(x, y) = \max(x, y) = x = y$. Hence $\min(x, y)+ \max(x, y) = x+y$.
- If $x>y$, then $\min(x, y) = y$ and $\max(x, y) = x$. Hence $\min(x, y)+ \max(x, y) = x+y$.

Since these are the only cases to consider the property holds.

9. Give a constructive proof of the proposition "for every positive integer n, there is an integer divisible by more than n primes".

Solution: Let n be a given positive integer, and assume that p_1, p_2, . . . ,p_n, p_{n+1} denotes the first n+1 primes (from the lectures we have shown there are an infinite number of primes). Then the integer $p_1{\cdot}p_2{\cdots}p_n{\cdot}p_{n+1}$ is divisible by more than n primes.

Difficult/challenging questions.

10. Prove that the cube root of 3 is irrational.

Hint: As a preliminary result, show if a^3 is divisible by 3, then a is divisible by 3. This can be proved using the fundamental theorem of arithmetic and the fact the 3 is prime.

Solution: As suggested in the hint we first show: if a^3 is divisible by 3, then a is divisible by 3. Using the fundamental theorem of arithmetic (FTA) we can express a as a unique product of primes, i.e. we have $a = p_1^{n_1}{\cdot}p_2^{n_2} \cdots p_k^{n_k}$ such that p_i is prime and n_i>0 for 1≤i≤k, and hence $a^3 = p_1^{3\cdot n_1}{\cdot}p_2^{3\cdot n_2} \cdots p_k^{3\cdot n_k}$. Using the FTA again, we have that this is the unique representation of a^3 in terms of primes and, since 3 dividies a^3 and 3 is prime, it follows that $p_i = 3$ for some 1≤i≤k, giving 3 divides a as required.

Now for the main part of the proof. Suppose for a contradiction that the cube root of 3 is rational. By definition $\sqrt[3]{3} = a/b$ for some integers a and b such that gcd(a, b)=1, and hence $a^3 = 3{\cdot}b^3$. Therefore a^3 is divisible by 3 which, using the property above, implies that a is divisible by 3, and therefore $a = 3{\cdot}k$ for some integer k. Thus $3{\cdot}b^3 = (3{\cdot}k)^3 = 3^3{\cdot}k^3$ which rearranging yields $b^3 = 3{\cdot}(3{\cdot}k^3)$ which, again using the property above, gives us that b is divisible by 3. This contradicts our assumption that $\gcd(a, b) = 1$, since both a and b are divisible by 3. Hence our hypothesis that the cube root of 3 is rational is `false`, and the cube root of 3 must be irrational as required.

11. Let $S = x_1{\cdot}y_1 + x_2{\cdot}y_2 + \cdots + x_n{\cdot}y_n$ where $x_1, x_2, \ldots, x_n$'s and the $y_1, y_2, \ldots, y_n$ are both sequences of real numbers. Show that:

    - S takes the maximum value when both sequences are sorted (e.g. in non-decreasing order).
    - S takes minimum value when one sequence is in non-decreasing while the other is in non-increasing order.

    Hint: Any other arrangement of the sequences can be obtained by permuting one sequence and any permutation can be written as a sequence of transpositions which act on distinct elements, i.e. each element is transposed at most once (a transposition is a permutation which only changes two elements and everything else remains the same).

Solution: The idea here is to consider the transposition steps required to get to any other arrangement of the summation and show that after each step the summation does not decrease (for the first part) or increase (for the second part). Note that this is only possible under the assumption that each element is transposed at most once, as otherwise we cannot use the fact the sequences are initially ordered.

For example consider the first case and suppose in one of the transposition steps we swap x_i with x_j and move from summation S' to summation S''. Now with out loss of generality we can suppose $i < j$ and since this is the only time x_i and x_j are transposed, since the sequence $x_1, x_2, \ldots, x_n$ is sorted we have $x_i \leq x_j$. Now since all that differs in the summations S' and S'' is that x_i and x_j are swapped we have:

$$\begin{aligned}
S' - S'' &= (x_i{\cdot}y_i + x_j{\cdot}y_j) - (x_j{\cdot}y_i + x_i{\cdot}y_j) && \\
&= (x_i{\cdot}y_i - x_j{\cdot}y_i) + (x_j{\cdot}y_j - x_i{\cdot}y_j) && \text{rearranging} \\
&= y_i{\cdot}(x_i - x_j) + y_j{\cdot}(x_j - x_i) && \text{rearranging} \\
&= -y_i{\cdot}(x_j - x_i) + y_j{\cdot}(x_j - x_i) && \text{rearranging} \\
&= y_j{\cdot}(x_j - x_i) - y_i{\cdot}(x_j - x_i) && \text{rearranging}
\end{aligned}$$

Now, from above we have since the sequence $y_1, y_2, \ldots, y_n$ is in non-decreasing order and $i < j$ we have $y_i \leq y_j$ and combining this with the fact $x_i \leq x_j$ it follows that $S' - S'' \geq 0$. Since this was for an arbitrary transposition step it follows that the resulting summation will be no larger, and hence S is maximal when both sequences are sorted (e.g. in non-decreasing order) as the other sequence was also arbitrary.

The second part follows similarly, if we assume the first sequence is ordered non-decreasing and the second non-increasing, then we derive that:

$$S' - S'' = y_j{\cdot}(x_j - x_i) - y_i{\cdot}(x_j - x_i)$$

and then use the fact that $x_i \leq x_j$ and $y_i \geq y_j$ to show $S' - S'' \leq 0$.