Lecture Notes

6.101 Video: Introduction to Proofs

- A **proof** is a valid argument that is used to prove the truth of a statement
- To build a proof, we need:
  - Variables and predicates
  - Quantifiers
  - Laws of logic
  - Rules of inference

Terminology

- **Theorem:** a formal statement that can be shown to be true
- **Axiom:** a statement we assume to be true to serve as a premise for futher arguments
- **Lemma:** a proven statement used as a step to a larger result rather than as a statement of interest by itself
- **Corollary:** a theorem that can be established by a short proof from a theorem

Direct proof

- based on showing that a conditional statement is true ($p \rightarrow q$)
- start by assuming p is true, and use the above rules to show that q must also be true

▼ Example

There exists a real number between any two not equal real numbers.

Proof
Let x, y be arbitrary elements in $\mathbb{R}$
Let's suppose $x < y$
Let $z = (x + y)/2$
$z \in \mathbb{R}$, satisfying $x < z < y$

Therefore, using the universal generalization rule, we can conclude that: $\forall x, y \in \mathbb{R}$ if $x < y$ then $\exists z \in \mathbb{R}$ where $x < z < y$

Proof by contrapositive

- based on proving the conditional statement is equivalent to proving its contrapositive
- start by assuming $\neg q$ is true, and use the above rules to show that $\neg p$ must also be true

▼ Example

If n^2 is even then n is even.

Proof

- *Direct proof*
  Let $n \in \mathbb{Z}$. If n^2 is even then $\exists k \in \mathbb{Z},\ n^2 = 2k$
  Then $\exists k \in \mathbb{Z},\ n = \pm\sqrt{2k}$. From this equation it doesn't seem intuitive to prove that n is even
- *Proof by contraposition*
  Let's suppose n is odd
  Then $\exists k \in \mathbb{Z},\ n = 2k + 1$
  Then $\exists k \in \mathbb{Z}, n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$

Then n^2 is also odd
We have succeeded in proving the contrapositive: if n is odd then n^2 is odd.

- based on assuming the statement we want to prove is **false**, and then showing that this leads to a **false** proposition
- start by assuming $\neg p$ is true, and use the above rules to show that $\neg p$ is false. We can the conclude that it was wrong to assume p is false, so it must be true.

▼ Example

There are infinitely many prime numbers.

Proof:
Let's suppose there are finitely many prime numbers
Let's list them as $p_1, p_2, p_3, ..., p_n$ where $p_1 = 2, p_2 = 3, p_3 = 5$ and so on
Let's consider the number $c = p_1 p_2 p_3 ... p_n + 1$, the product of all the prime numbers, plus 1
Then, as c is a natural number, it has at least one prime divisor.
Then $\exists k \in \{1...n\}$, where p_k / c
Then $\exists k \in \{1...n\}, \exists d \in \mathbb{N}$ where $dp_k = c = p_1 p_2 p_3 ... p_n + 1$
Then $\exists k \in \{1...n\}, \exists d \in \mathbb{N}$ where $d = p_1 p_2 ... \ p_{k-1} \ p_{k+1} ... \ p_n + \frac{1}{p_k}$
Then, $\frac{1}{p_k}$, in the expression above, is an integer, which is a contradiction

6.102 Practice Quiz: Introduction to Proofs

1. Which of the following statements is true?

   ☐ A theorem is a formal statement that can be shown to be true

   ☐ An axiom comprises necessarily multiple quantifiers

   ☐ A lemma is equivalent to a specific rule of inference

2. Given the statement S : *For every integer n, there exist a number dividing n*

   ☐ S can be proved only using contrapositive

   ☐ S is a law of logic

   ☐ S can be formalised as: $\forall n \in \mathbb{N} \ \exists p \in \mathbb{N} \ p/n$

3. How can we build a valid direct proof?

   ☐ We start by assuming that p is true and then prove q is true

   ☐ We show that the conditional statement: $\neg q \rightarrow \neg p$ is true

   ☐ We use axioms, definitions and theorems, together with rules of inference, to prove that it is wrong to assume p

4. How can we build a valid proof by contrapositive?

   ☐ We show that the conditional statement: $p \rightarrow q$ is true

   ☐ We start by assuming that $\neg q$ is true and then prove that $\neg p$ must also be true

   ☐ We use axioms, definitions and theorems, together with rules of inference, to show that if $\neg q$ is true then $\neg p$ must also be true

5. How can we build a valid proof by contradiction?

   ☐ We use axioms, definitions and theorems, together with rules of inference, to prove that it's wrong to assume p is false

   ☐ We start by assuming that $\neg q$ is true and then prove that $\neg p$ must also be true

   ☐ We show that the conditional statement: $p \rightarrow q$ is true

6.103 Video: The principle of mathematical induction

- can be used to assert that a propositional function $P(n)$ is true for all positive integers n.

  $P(1)$ is true
  $\forall k \ P((k) \rightarrow P(k+1))$
  $---------------$
  $\therefore \forall n \ P(n)$

Structure of induction

1. **Basis Step**: where we show that $P(1)$ is true
2. **Inductive Step**: where we show that for $\forall k \in \mathbb{N}$: if $P(k)$ is true, called **inductive hypothesis**, then $P(k+1)$ is true

Uses of induction

- Proving formulas
- Proving inequalities
- Proving divisibility
- Proving properties of subsets and their cardinality

6.105 Practice Quiz: The principle of mathematical induction

1. What is the main use of mathematical induction?

   ☐ Mathematical induction can be used to assert that a propositional function $P(n)$ is true for all positive integers n.

   ☐ Mathematical induction is always more difficult than using a direct proof

   ☐ Mathematical induction can always harder than proof by contrapositive

   ☐ Mathematical induction can sometimes be simpler then using a direct proof

   ☐ Mathematical induction is never useful to assert that a propositional function $P(n)$ is true for all positive integers n.

   ☐ ~~Mathematical induction is always more difficult than using a direct proof~~

2. What is the rule of inference behind mathematical induction?

   ☐ Hypothetical syllogism

   ☐ $P(1)$ is true, $\forall k \in \mathbb{N}\ (P(k) \rightarrow P(k+1))$, therefore $\forall n \in \mathbb{N}\ P(n)$

   ☐ $P(1)$ is true, $\forall k \in \mathbb{N}\ P(1),\ P(2)\ ...\ P(k) \rightarrow P(k+1)$, therefore $\forall n \in \mathbb{N}\ P(n)$

   ☐ Universal instantiation

3. What are the main steps in building a mathematical induction?

   ☐ Show that $P(1)$ is true

   ☐ Show that $\exists k \in \mathbb{N}$: if $P(k)$ is true, then $P(k+1)$ is true

   ☐ Show that $\forall k \in \mathbb{N}$: if $P(k)$ is true, then $P(k+1)$ is false

4. What are the intuitions behind mathematical induction?

   ☐ Every step is completely independent from the previous one

   ☐ The base case shows that the property initially holds true

   ☐ The base case shows that the property initially does not hold true

   ☐ Mathematical induction is like climbing an infinite ladder

   ☐ ~~Every step is completely independent from the previous one~~

5. Which of the following is an example of the use of mathematical induction?

   ☐ Proving all the rules of inference

   ☐ Definition of all the Boolean algebra

   ☐ Proving inequalities

   ☐ Building all the predicate logic

   ☐ Proving formulas

6.106 Video: Proof by induction

Proving formulas

▼ Example

$P(n) : 1 + 2 + 3 + ... + n = n(n+1)/2$

1. **Basis Step:**
   $P(1)$ reduces to $1 = 1(1+1)/2$
2. **Inductive Step:**
   Let $\forall k \in \mathbb{N}$
   If $P(k)$ is true, we have $1 + 2 + 3 + ... + k = k(k+1)/2$
   then, $1 + 2 + 3 + ... + k + (k+1)$
   $= k(k+1)/2 + (k+1)$
   $= (k(k+1) + 2(k+1))2$
   $= (k+1)((k+1)+1)/2$
   which varifies, $P(k+1)$

Proving inequalities

▼ Example

$P(n) : 3^n < n!$ *if* n *is an integer greater then or equal to* 7.

1. **Basis Step:**
   $P(7)$ reduces to $3^7 < 7!$ because $2187 < 5040$
2. **Inductive Step:**
   Let $k \in \mathbb{N}$ and $k \geq 7$
   If $P(k)$ is true, then $3^{k+1} = 3 * 3^k < (k+1) * k!$ which verifies $P(k+1)$ is true

Proving divisibility

▼ Example

$P(n) : \forall n \in \mathbb{N} \quad 6^n + 4$ *is divisible by* 4.

1. **Basis Step:**
   $P(0)$ reduces to $6^0 + 4$ is divisible by 5, because $6^0 + 4 = 5$
2. **Inductive Step:**
   Let $k \in \mathbb{N}$
   If $P(k)$ is true, then $6^k + 4 = 5p$, where $p \in \mathbb{N}$
   then $6^{k+1} + 4 = 6 * (5p - 4) + 4$
   $= 30p - 20 = 5(6p - 4)$ which is divisible by 5 and verfies $P(k+1)$ is true

Incorrect Induction

▼ Example

$P(n) : \forall n \in \mathbb{N}\ \Sigma_{i=0}^{n-1} 2^i = 2^n$

Proof
Let $k \in \mathbb{N}$. Let's suppose $P(k)$ is true, which means $\Sigma_{i=0}^{k-1} 2^i = 2^k$
Now let's examine $P(k+1)$
$\Sigma_{i=0}^{k} 2^i = \Sigma_{i=0}^{k-1} 2^i + 2^k = 2^k + 2^k = 2^{k+1}$
This means that $P(k+1)$ is also true and verifies the induction step.

Counterexample

$2^0 + 2^1 = 3 \neq 2^2 = 4$

No base case, and have made false assumptions

6.107 Practice Quiz: Proof by induction

1. We want to use induction to prove the following formula:
   $U_n = 1^2 + 2^2 + ... + n^2 = n(n+1)(2n+1)/6$
   What is the base step we need to verify?

   ☐ $U_n = 1^2 + 2^2 + ... + n^2 = n(n+1)(2n+1)/6$

   ☐ $1^2 = 1(1+1)(2*1+1)/6$

   ☐ $n^2 = n(n+1)(2n+1)/6$

   ☐ $1^2 + 2^2 = 2(2+1)(2*2+1)/6$

2. We want to use induction to prove the following formula:
   $U_n = 1^2 + 2^2 + ... + n^2 = n(n+1)(2n+1)/6$
   What is the inductive step we need to verify?

   ☐ $\forall n \in \mathbb{N}$ if $U_n = n(n+1)(2n+1)$ then $U_{n+2} = (n+2)(n+2+1)(2(n+2)+1)$

   ☐ $\forall n \in \mathbb{N}$ if $U_n = n(n+1)(2n+1)$ then $U_{n+1} = (n+1)(n+1+1)(2(n+1)+1)$

   ☐ $\exists n \in \mathbb{N}$ if $U_n = n(n+1)(2n+1)$ then $U_{n+2} = (n+2)(n+2+1)(2(n+2)+1)$

3. We want to prove the formula $P(k) : 2^k < k!$ holds for all $k \geq 5$
   What is the basis step we need to verify?

   ☐ $P(5)$

   ☐ $P(1)$

   ☐ $P(\text{infinity})$

   ☐ $P(0)$

4. We want to use induction to prove the following formula:
   $\forall n \in \mathbb{N},\ P(n) : 21$ divides $4^{n+1} + 5^{2n-1}$
   What is the inductive step we need to verify?

   ☐ $\exists n \in \mathbb{N}$, if 21 divides $4^{n+1} + 5^{2n-1}$ is true, then 21 divides $4^{n+2} + 5^{2n+1}$ is true

   ☐ $\forall n \in \mathbb{N}$, if 21 divides $4^{n+1} + 5^{2n-1}$ is true, then 21 divides $4^{n+2} + 5^{2n-1}$ is true

   ☐ $\forall n \in \mathbb{N}$ if $P(n)$ is true, then $P(n+1)$ is true

5. After finishing the writing of an induction proof, we realise that the induction does not hold true for at least one integer.
   What mistakes have we probably made while building the proof?

   ☐ We have not made any mistake in the proof

   ☐ We proved the basis step without making sure that the inductive step is verified

   ☐ The basis step and the inductive step are both verified

6.108 Video: Strong Induction

- is sometimes easier to prove statements using strong induction

  $P(1)$ is true
  $\forall k \in \mathbb{N}\ P(1), P(2), ...\ P((k) \rightarrow P(k+1))$
  $---------------$
  $\therefore \forall n \in \mathbb{N},\ P(n)$

- Also known as *second principle of induction* or *complete induction*

▼ Example

$P(n)$: *$\forall n \in \mathbb{N}$ and $n \geq 2$, n is divisible by a prime number*

1. **Basis Step:**
   $P(2)$ reduces to 2, which is divisible by itself as a prime number

2. **Inductive Step:**
   Let $k \in \mathbb{N}$ be greater than 2
   If $P(k)$ is true, let's assume $P(2)...P(k+1)$ is true. Then $\forall m \in \mathbb{N}$ and $2 \leq m \leq k+1 : \exists p$ is a prime number dividing m
   We have two cases:
   - $k+2$ is a prime number, in which case it is trivially divisible by itself
   - $k+2$ is not a prime number, in which case $\exists m$ dividing $k+2$

   as $2 \leq m \leq k+1, \exists p$ is a prime number dividing m. p also divides $k+2$
   Which verifies $P(k+2)$ is true and proves the strong induction

Well-Ordering property

1. The number 1 is a positive integer.
2. If $n \in \mathbb{N}$, then $n+1$, the successor of n, is also a positive integer.
3. Every postive integer other than 1 is the successor of a positive intger.

4. The well-ordering property: every nonempty subset of the set of positive integers has at least one element.

▼ Example (con't)

Proof

Let S be the set of positive integers greater than 1 with no prime divisor
Suppose S is nonempty. Let n be its smallest element
n cannot be prime, it would be its own prime divisor
So n is composite: it must have a divisor d with $1 < d < n$. Then, d must have a prime divisor (by the minimality of n), let's call it p
Then p/d and d/n, so p/n, which is a contradiction
Therefore S is empty, which verifies $P(n)$

Equivalence of the three concepts

- Mathematical induciton → the Well-Ordering property
- the Well-Ordering property → Strong Induction
- Strong Induction → Mathematical Induction

The validity of each of these three proof techniques imples the validity of the other two.

6.109 Practice Quiz: Strong Induction

1. Which of the following statements is true?

   ☐ It is always easiest to prove statements using mathematical induction

   ☐ Sometimes it is easiest to prove statements using contrapositive proof

   ☐ It is always hardest to prove statements using strong induction

2. Strong induction is based on which of the following rule of inference?

   ☐ $P(1)$ is true, $\exists k \in \mathbb{N}\ P(1), P(2)...P(k) \rightarrow P(k+1)$, therefore $\forall n \in \mathbb{N}\ P(n)$

   ☐ $P(1)$ is true, $\forall k \in \mathbb{N}\ P(1), P(2)...P(k) \rightarrow P(k+1)$, therefore $\forall n \in \mathbb{N}\ P(n)$

   ☐ $P(1)$ is true, $\forall k \in \mathbb{N}\ (P(k) \rightarrow P(k+1))$, therefore $\forall n \in \mathbb{N}\ P(n)$

3. We want to use strong induction to prove the following formula:
   $\forall k \in \mathbb{N},\ 12$ divides $n^4 - n^2$
   What is the inductive step that we need to verify?

   ☐ $\exists n \in \mathbb{N}\ P(1), P(2)...P(k) \rightarrow P(k+1)$

   ☐ $\forall k \in \mathbb{N}$ divides $0, 12$ divides $2^4 - 2^2, ..., 12$ divides $k^4 - k^2$ implies: 12 divides $(k+1)^4 - (k+1)^2$

   ☐ $\forall k \in \mathbb{N}$ divides $0, 12$ divides $2^4 - 2^2, 12$ divides $k^4 - k^2$ implies: 12 divides $k^4 - k^2$

4. In this lesson we prove that in $\forall k \in \mathbb{N}$ and $n \geq 2$, n is divisible by a prime number.
   When defining n as the smallest element of S, what property did we use?

   ☐ The disjunctive syllogism property

   ☐ The well-ordering property

   ☐ The adjacency property

5. Which of the following equivalences is true?

   ☐ The well-ordering property is equivalent to strong induction

   ☐ In some cases strong induction is equivalent to mathematical induction

   ☐ In some cases mathematical induction is not equivalent to the well-ordering property