COMP30026 Models of Computation

Mathematical Proof

Harald Søndergaard

Lecture 10

Semester 2, 2017

Distinctive Types of Proof

A proof (or refutation) by construction produces a witness, either to prove a claim of the form "there exists ...", or to refute a claim of the form "for all ...".

A proof by contradiction proceeds by assuming the claim to be false, and then showing that an absurdity follows.

A proof by induction is used to show that some infinite set of objects (with some structure) all have some property.

Types of Statements

- A conjecture is an unproven claim.
- A theorem is a claim that has been proved true.
- A lemma is a statement that is of interest only because it assists in the proof of a more significant statement.
- A corollary is a simple consequence of a theorem.
- A proposition is a more technical theorem, perhaps of less significance.

A Refutation

Conjecture: For all prime numbers $p > 5$, $2^p - 1$ is not prime.

Refutation: Take $p = 31$ and verify that $2^{31} - 1 = 2147483647$ is a prime.

(A prime number of the form $2^p - 1$ is called a Mersenne prime.)

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proof: Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{m}{n}$ for some integers m and n, $n \neq 0$. We can assume, without loss of generality, that at least one of m and n is odd. Multiplying both sides by n and then squaring, we get

$$2n^2 = m^2$$

Hence m^2, and therefore m, is even, so we can write $m = 2k$ for some integer k:

$$2n^2 = 4k^2$$

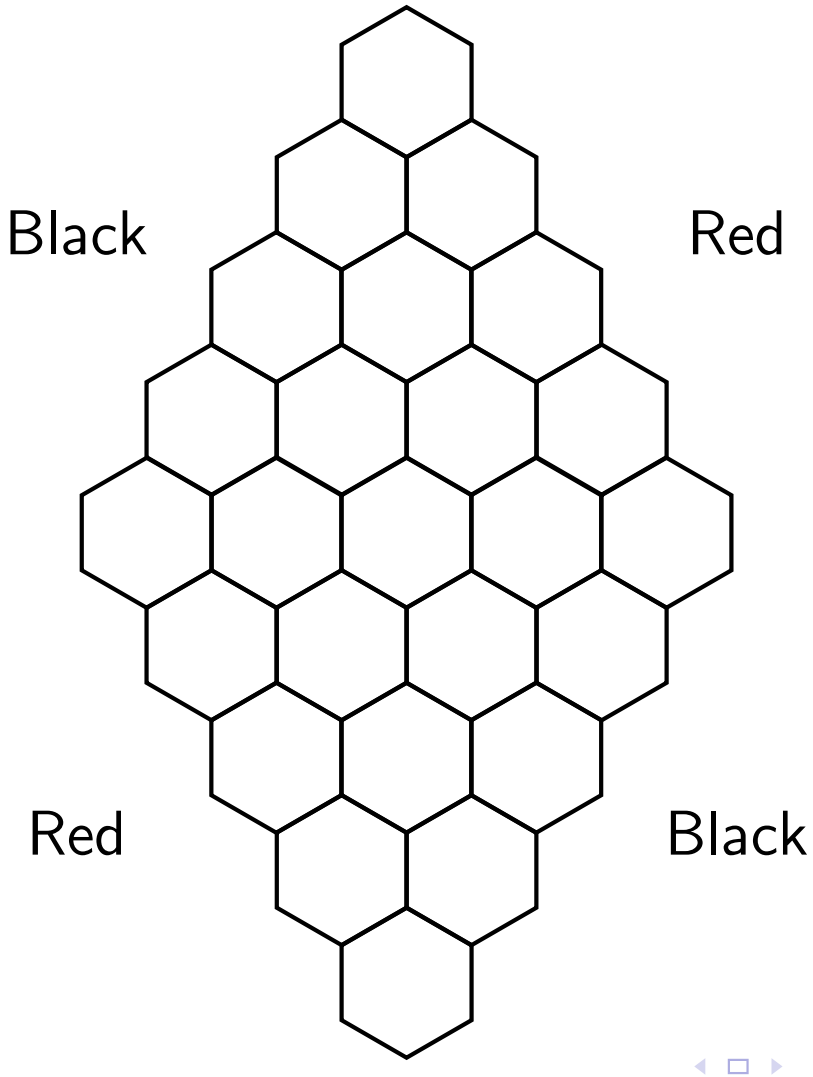
But then

$$n^2 = 2k^2$$

so n is also even. A contradiction, so $\sqrt{2}$ is irrational.

Exercise

Find a winning strategy for Piet Hein's Hex:



Non-Constructive Proofs

Theorem: There are irrational numbers p and q such that p^q is rational.

Proof: We know that $\sqrt{2}$ is irrational. What about $\sqrt{2}^{\sqrt{2}}$?

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational, and we have proved the assertion correct, taking $p = q = \sqrt{2}$.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational, so call it p and let q be $\sqrt{2}$. Then $p^q = 2$, which is rational, and again the assertion is correct.

In either case, the assertion is correct.

Intuitionistic Logic

This proof didn't actually deliver two irrational numbers p and q.
The school of intuitionism insists that such a proof is inadmissible.
To claim that something exists, we have to show a witness.

To the intuitionist, it is not enough to say, as we did, that

$$\sqrt{2}^{\sqrt{2}} \text{ is rational and the assertion holds}$$
$$\text{or}$$
$$\sqrt{2}^{\sqrt{2}} \text{ is not rational and the assertion holds}$$

and therefore the assertion holds.

A proof of "A or B" must indicate which of A and B was proved.

Similarly, intuitionists do not accept proof by contradiction in general.

Mathematical Induction

"Mathematical" induction is always a proof about the natural numbers, $\mathbb{N}$.

We're usually given a statement "for all n, $S(n)$."

We proceed in two steps:

1. In the basis step, we show $S(0)$.
2. In the inductive step, we take $S(n)$ as the induction hypothesis and use it to establish $S(n+1)$.

Proof by Induction

Theorem: For all $n \geq 0$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof: For the basis step, note that the statement is true for $n = 0$.

For the inductive step, assume the statement is true for some fixed n, and we shall show that it also holds true with $n+1$ substituted for n.

So the statement to prove is

$$\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

Proof by Induction

But the claim

$$\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

is the same as

$$\left(\sum_{i=1}^{n} i^2\right) + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

By the induction hypothesis, it suffices to show that

$$\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

This is done by simple polynomial algebra.

More General Induction

Sometimes more base cases may be needed.

Sometimes we need to use several statements $S(i), \ldots S(n)$ to establish $S(n+1)$.

Theorem: For all $n \geq 8$, n can be written as a sum of 3s and 5s.

Proof: For the basis step, observe that $S(8)$, $S(9)$, and $S(10)$ are true.

For the inductive step, assume that $n \geq 10$ and $S(8), \ldots, S(n)$ are true. Since $S(n-2)$ is true, also $n+1$ can be written as a sum of 3s and 5s – just add 3 to the sum we had for $n-2$. Hence we have established $S(n+1)$.

We conclude that $S(n)$ holds for all $n \geq 8$.

Recursive Structure and Induction

We often deal with recursively defined objects. Lists and trees are examples.

The set of well-formed propositional logic formulas is another example.

Induction is the natural way of proving assertions about such objects.

In many cases we then rely on structural induction.

Structural Induction: A Simple Example

Suppose we want to prove that, in any well-formed formula, the number of left parentheses is the same as the number of right parentheses.

This is a statement about the set of propositional formulas generated by a grammar

$$\mathit{formula} \rightarrow \mathbf{f} \mid \mathbf{t} \mid \mathit{var} \mid \neg \mathit{formula} \mid (\ \mathit{formula} \Leftrightarrow \mathit{formula}\ ) \mid \ldots$$

The base cases say: Any (propositional) constant or variable is a formula.

The "inductive" cases say that $\neg f$ is a formula if f is, $(f_1 \Leftrightarrow f_2)$ is a formula if f_1 and f_2 are, and so on.

A Trivial Proof by Structural Induction

Theorem: In any well-formed formula, the number p of left parentheses is the same as the number r of right parentheses.

Proof: Basis step: The statement is true for a constant and for a variable, since in those cases $p = r = 0$.

Inductive case 1: Consider $\neg f$. By the induction hypothesis, f has p left parentheses and r right parentheses, and $p = r$. But $\neg f$ has exactly the same numbers of parentheses.

Inductive case 2: Consider $(f_1\ op\ f_2)$ Let p_1 and r_1 be the number of left and right parentheses, respectively, in f_1, and let p_2 and r_2 be the numbers for f_2. By the induction hypothesis, $p_1 = r_1$ and $p_2 = r_2$. Hence $p_1 + p_2 + 1 = r_1 + r_2 + 1$. But these are the number of left and right parentheses, respectively, in $(f_1\ op\ f_2)$.

Converse and Contrapositive

Consider the statement "B follows from A".

The statement "A follows from B" is its converse.
Logically, the two are unrelated.

However, sometimes we may prove

"B follows from A"

by proving instead its contrapositive form

"not-A follows from not-B".

That's admissible—those are logically equivalent.

Writing Proofs

Write clear English; write for your peers; put yourself in the reader's shoes.

Be neat.

Be persistent. A proof is usually a concise summary of some deep thinking. Don't expect it to come easily; you may have to sleep on it.

Use signposting in your writing. Words like 'therefore', 'it follows', 'suppose', etc., are important markers of the line of thought.

There are certain rules that it may help to follow, leading to disciplined structure and layout of proofs. As an aid, the rest of this slide set provides some structural rules.

Proof Strategy (Useful But Not Examinable)

Here are some detailed proof recipes in a style known as natural deduction.

For each connective, there are rules for how to introduce it, and how to eliminate it.

Start by rephrasing the problem

Given: ...
To be proved: ...
Proof: ...

Concentrate primarily on the proof goal, not the given.

Proof Rules for Implication

Introduction:
If "to be proved" has the form $\Phi \Rightarrow \Psi$, your proof should start with

Suppose that Φ holds.

This tells the reader that we now shift the focus to trying to show Ψ.

If you succeed in deriving Ψ by considering Φ part of the 'given', then you have established $\Phi \Rightarrow \Psi$.

Elimination is modus ponens: Given $\Phi \Rightarrow \Psi$ and Φ, conclude Ψ.

Proof Rules for Biimplication

Introduction:
To prove $\Phi \Leftrightarrow \Psi$, split into two: First add Φ to the 'given' and derive Ψ ($\Rightarrow$). Then add instead Ψ as given and derive Φ ($\Leftarrow$).

Elimination:
From $\Phi \Leftrightarrow \Psi$, together with one of Φ or Ψ, derive the other.

Example Proof

Show that from $P \Leftrightarrow Q$ follows $(P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R)$.

Assume $P \Leftrightarrow Q$.
  Suppose $P \Rightarrow R$.
    Assume Q.
    From $P \Leftrightarrow Q$, Q we have P, and so from $P \Rightarrow R$, we have R.
  Hence $Q \Rightarrow R$.
  Suppose $Q \Rightarrow R$.
    Assume P.
    From $P \Leftrightarrow Q$, P we have Q, and so from $Q \Rightarrow R$, we have R.
  Hence $P \Rightarrow R$.
Therefore, from $P \Leftrightarrow Q$ follows $(P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R)$.

Proof Rules for Negation

To prove $\neg\Phi$, where P is complex, it is almost always best to try to push negation in.

Proof by contradiction: To prove Φ, add $\neg\Phi$ as given, and try to deduce an evidently false statement.

We saw an example on slide 5.

Proof Rules for Disjunction

Introduction:
From Φ (or from Ψ), derive $\Phi \vee \Psi$.

Elimination:
To show that, given $\Phi \vee \Psi$, some Υ follows, give two proofs. First show Υ given Φ, then show Υ given Ψ.

We saw an example on slide 7.

Rules for Universal Quantification

Introduction:
To prove $\forall x\ P(x)$, start the proof by saying

> Let c be arbitrary.

Then go on to prove $P(c)$ without making any assumptions about c.

Elimination:
Given $\forall x\ P(x)$, deduce $P(t)$ for any object t.

Rules for Existential Quantification

Introduction:
Given $P(t)$ for some object t, deduce $\exists x\ P(x)$.

Elimination:
To use $\exists x\ P(x)$ in a proof deriving Ψ, start the proof by saying

Let c satisfy P.

Then proceed to prove Ψ without making any assumptions about c, apart from $P(c)$.