CS1113
Proof

Lecturer:

Professor Barry O'Sullivan

Office: 2.65, Western Gateway Building

email: *b.osullivan@cs.ucc.ie*

http://osullivan.ucc.ie/teaching/cs1113/

Proof

Proof methods:
direct proof
proof by induction
proof by contradiction
proof by cases

Example proofs of statements from Algorithm Analysis

What is a ‘Proof’?

- A proof is a valid argument that shows that some statement is true

- Proofs can be formal
  - E.g. Proofs in propositional logic applying inference rules and logical equivalences

- Or informal - but even an informal proof must be convincing, and must cover all loopholes
  - no gaps, no handwaving, no wishful thinking
  - must be precise and unambiguous
  - use mathematical and logical notation
  - explain and justify every step

Uses of proof in computing

- Showing that an algorithm (or program) does what it is supposed to do
- Showing that one algorithm has, in the worst case, a lower runtime than another algorithm
- Showing that an operating system is secure
- Showing that a protocol for computing across a network is safe and will not enter deadlock
- Showing that a system specification is consistent
- Checking that a decision is justified in an intelligent program

We have already seen ...

- Direct proof
  - E.g. Proof of the Handshaking Lemma in Lecture 9
  - E.g. Proof that x^2+1 is $O(x^2)$ in Lecture 18

- Proof by contradiction
  - E.g. Proof that x^3+2x^2+2 is not $O(x^2)$ in Lecture 18

- Proof by induction
  - Prove a statement is true for a simple base case
  - Prove that **if** statement is true for an intermediate case (e.g. of size k) **then** it must be true for the next case (e.g. of size $k+1$)
  - E.g. Proof that n^2+n is even in Lecture 20

$$\forall n \geq 4 \quad 2^n < n!$$

Proof

$n!$ is not $O(2^n)$

Proof

Proof by contrapositive

Revision: For a statement $p \to q$, its contrapositive is $\neg q \to \neg p$
A conditional is true if and only if its contrapositive is true

Sometimes, it is easier to prove the contrapositive.

Example: if n^2 is even, then n is even

<u>Direct proof attempt</u>
Suppose n^2 is even. Then $n^2 = 2k$ for some k. *... but now what?*

<u>Proof</u> (by contrapositive)
We will show that if n is not even, then n^2 is not even
Suppose n is not even. Then $n=2k+1$, for some k.
Then $n^2 = (2k+1)^2 = 4k^2 + 4k +1 = 2(2k^2+2) + 1$, which must be odd.

Therefore, by the contrapositive, if n^2 is even, n is even

Proof by counter example

Sometimes, we will want to prove that a statement is false.

Example claim: for any integer x, we can find two integers y and z so that $y^2+z^2 = x$.

We will prove this false by finding an integer x which does not obey this pattern.

Consider $x = 3$. y^2 and z^2 are both positive.
If $|y| \geq 2$, then $y^2 \geq 4$, and so $y^2+z^2 \geq 4$.
So $|y|$ must be either 0 or 1. If $|y| = 0$, then $y^2=0$, so z^2 must be 3. But there is no integer z such that $z^2 = 3$. Therefore y cannot be 0.
Suppose $y = 1$. Then $y^2 = 1$, so $z^2 = 2$. But there is no integer z such that $z^2=2$. So y cannot be 1. But those were the only possible values for y.
Therefore, there are no integers y and z such that $y^2+z^2=3$, and so the statement is false.

Proof by cases

Sometimes, we will need to break a statement down into a number of different cases, and show each one is true.

Example: for two integers x and y, if $x=y^2$, then x is of the form $4k$ or $4k+1$, for some other integer k.

<u>Proof</u>

Case(i): y is even. So there is an integer p with $y=2p$.
Then $x = y^2 = (2p)^2 = 4p^2 = 4k$, if we set $k=p^2$.

Case(ii): y is odd. So there is an integer q with $y=2q+1$.
Then $x = y^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2+q)+1$
and so $x = 4k+1$, if we set $k=q^2+q$

These are all possible cases for y, so the statement is true.

What can go wrong?

- showing something works for one or two examples, instead of for all possible values
- assuming the result you want to prove
- not covering all cases
- making jumps in the logic that are not true
- not presenting it as a convincing argument
- leaving large gaps in the argument and assuming it is clear what is happening

THE END

of the new material ...

Next lecture ...

Revision