Monash University
Faculty of Information Technology

FIT2014 Theory of Computation

Lecture 5

Proofs: the Good, the Bad and the Ugly

slides by Graham Farr

Overview

- Good proofs
  - three proofs from The Book

- Bad proofs
- Ugly proofs

Good proofs

Theorem. (Euclid)
There are infinitely many prime numbers.

Proof.
Suppose, by way of contradiction, that there are only finitely many primes.
Let n be the number of primes.
Let $p_1, p_2, \ldots, p_n$ be all the primes.

Define: $\quad q \;:=\; p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1.$
This is bigger than every prime p_i. Therefore q must be composite.
Therefore q is a multiple of some prime.
But, for each prime p_i, if you divide q by p_i, you get a remainder of 1.

So q cannot be a multiple of p_i.
So q cannot be a multiple of any prime. **This is a contradiction.**
So our initial assumption was wrong.
So there are infinitely many primes. $\square$

Good proofs

Theorem. (Pythagoras)
$\sqrt{2}$ is irrational.

Proof.
Suppose, by way of contradiction, that $\sqrt{2}$ is rational.
Then, by definition, there exist positive integers m, n such that $\sqrt{2} = \frac{m}{n}$.
Among all such pairs m, n, choose a pair that have no common factors.

Squaring each side of our equation gives: $2 = \frac{m^2}{n^2}$.
Rewrite slightly: $2n^2 = m^2$.
This tells us that m^2 is even. Therefore m is even. Therefore $m = 2k$ for some k.

Substituting this back in gives: $2n^2 = (2k)^2$, i.e., $2n^2 = 4k^2$, i.e., $n^2 = 2k^2$.
This tells us that n^2 is even. Therefore n is even.
Since m and n are both even, they both have a common factor, namely 2.
But we chose them so that they have no common factors. **This is a contradiction.**
Therefore our initial assumption, that $\sqrt{2}$ is rational, must be wrong.
Therefore $\sqrt{2}$ is *irrational*. $\square$

Good proofs

Definition: A set is **countable** if *either*

- it is finite, *or*
- it can be put in one-to-one correspondence (i.e., bijection) with $\mathbb{N}$.

FIT2014 students

{Dakṣiputra, Muḥammad, Ramon, Blaise, Gottfried, Nicole-Reine, Maria, Charles, Ada, George, Augustus, Annie, Henrietta, Radhanath, Williamina, Kurt, Rózsa, Alonzo, Alan, Konrad, Bill, Tommy, Hedy, Trevor, Maston, Noam, Winsome, Stephen, Grace, John, Péisù, Katherine, Margaret, Richard, . . . }

finite

		$\mathbb{N}$
1	$\longleftrightarrow$	1
2	$\longleftrightarrow$	2
3	$\longleftrightarrow$	3
4	$\longleftrightarrow$	4
5	$\longleftrightarrow$	5
$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$

		$\mathbb{Z}$
1	$\longleftrightarrow$	0
2	$\longleftrightarrow$	1
3	$\longleftrightarrow$	-1
4	$\longleftrightarrow$	2
5	$\longleftrightarrow$	-2
$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$

				Σ^*
1	$\longleftrightarrow$	1	$\longleftrightarrow$	ε
2	$\longleftrightarrow$	10	$\longleftrightarrow$	a
3	$\longleftrightarrow$	11	$\longleftrightarrow$	b
4	$\longleftrightarrow$	100	$\longleftrightarrow$	aa
5	$\longleftrightarrow$	101	$\longleftrightarrow$	ab
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Good proofs

Theorem. (Cantor)
The set of *all languages* is *uncountable*.

Idea of proof: If {all languages} were countable . . .

			ε	a	b	aa	ab	ba	bb	aaa	aab	. . .
1	$\longleftrightarrow$	L_1:	✓	✗	✗	✓	✗	✓	✓	✓	✗	. . .
2	$\longleftrightarrow$	L_2:	✗	✗	✓	✓	✗	✗	✗	✓	✓	. . .
3	$\longleftrightarrow$	L_3:	✓	✓	✗	✗	✗	✓	✗	✗	✓	. . .
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	. . .
m	$\longleftrightarrow$	L_m:	✓	✗	✗	✓	✗	✗	✓	✗	✗	. . .
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$\hat{L}$: ✗ ✓ ✓ . . .

Good proofs

Theorem. (Cantor)
The set of *all languages* is *uncountable*.

Proof. **Suppose, by way of contradiction,** that the set of all languages is countable.
Since we know it's not finite, there must be a bijection between $\mathbb{N}$ and $\{\text{all languages}\}$.
Let the members of the set of all languages be $L_m,\ m \in \mathbb{N}$.
Recall that the set of all finite strings is countable, so we can list them as $x_n,\ n \in \mathbb{N}$.
Define the language $\hat{L}$ as follows

$$\forall n \in \mathbb{N} : x_n \in \hat{L} \Leftrightarrow x_n \notin L_n.$$

We have constructed $\hat{L}$ so that, for each n, it differs from L_n in whether or not it contains x_n.
So it differs from all languages. Yet it is a language! **This is a contradiction.**
So our initial assumption was wrong.
So the set of languages is uncountable. $\square$

Bad proofs

From a falsehood, you can prove *anything*.

Recall the truth table of $P \Rightarrow Q$: always True when P is false, regardless of Q.

$$
\begin{array}{lrcl}
 & 2+2 & = & 5 \\
\text{Therefore} & 4 & = & 5 \\
\text{Therefore} & 1 & = & 2 \\
\text{Now,} & |\{\text{McTaggart, The Pope}\}| & = & \mathbf{2}. \\
\text{Therefore} & |\{\text{McTaggart, The Pope}\}| & = & \mathbf{1}. \\
\text{Therefore} & \text{McTaggart is the Pope} & &
\end{array}
$$

attributed to G. H. Hardy in:
Harold Jeffreys, *Scientific Inference*,
Cambridge University Press, 1931/1957/1973.

Bad proofs

"Theorem": Every graph has a cycle.
For all n: every graph on n vertices has a cycle.
This implies that trees do not exist.

"Proof": We prove this by induction on the number of vertices.

1. Assume that **every graph on n vertices has a cycle**.
2. Let G be any graph on $n+1$ vertices.
3. Let v be a vertex of G. Obtain the graph $G-v$ by removing v, and all its incident edges, from G.
4. Now, the graph $G-v$ has n vertices.
5. By the **Inductive Hypothesis**, $G-v$ has a cycle.
6. But, since $G-v$ is a subgraph of G, any cycle in $G-v$ is also a cycle in G.
7. Therefore G has a cycle.
8. Therefore, by Mathematical Induction, the result is true for all n.
   So every graph has a cycle.

Bad proofs

Definition: A string is *uniform* if all its letters are identical.

- i.e., it consists entirely of `a`s or entirely of `b`s

- i.e., it's either $\mathtt{aa}\cdots\mathtt{a}$ or $\mathtt{bb}\cdots\mathtt{b}$

Now, it is commonly thought that not all strings are uniform.

But we will now try to “prove”, by induction, that *all* strings are uniform!

Bad proofs

"Theorem": Every string over the alphabet {a,b} is uniform.

"Proof". We prove this by induction on the string length n.

1. Inductive basis: when $n = 1$, the string can only be "a" or "b", and these are each of the required form, so the "theorem" is true in this case.
2. Now assume $n \geq 2$, and suppose every string of length n is uniform.
3. Let w be any string of length $n + 1$.
4. Let w_1 be the string obtained from w by deleting the *first* letter of w, and let w_2 be the string obtained from w by deleting the *last* letter of w.
5. Both w_1 and w_2 are of length n.
6. By the Inductive Hypothesis, both w_1 and w_2 must be uniform.
7. w_1 and w_2 overlap in $n - 1$ letters. Since $n - 1 > 0$, this means that the number of letters shared by w_1 and w_2 is nonzero. So w_1 and w_2 must each consist entirely of the *same letter*, i.e., either they both consist entirely of as or they both consist entirely of bs.
8. It follows that w also consists entirely of as or entirely of bs, so it is uniform too.
9. The result follows for all n, by Mathematical Induction.

Ugly proofs

Theorem.
DOUBLEWORD $\subseteq$ EVEN-EVEN

Proof. Let $w \in$ DOUBLEWORD.
Assume w is not in EVEN-EVEN.
Then $w = xx$ for some word x.

So, # a's in w = $2 \times$ (# a's in x), so it's even.
Also, # b's in w = $2 \times$ (# b's in x), so it's even too.
This contradicts our assumption that w is not in EVEN-EVEN.
Therefore that assumption was wrong.

Therefore $w \in$ EVEN-EVEN. $\square$

When you have a *direct* proof of your theorem, there's no need to dress it up as a proof by contradiction!

Ugly proofs?

A **colouring** of a graph G is a function that assigns a colour to each vertex of G such that *adjacent* vertices receive *different* colours.

- i.e., a function $f : V(G) \to \{\text{colours}\}$ such that $\forall u, v \in V(G) : u \sim v \Rightarrow f(u) \neq f(v)$.

A colouring is a k-**colouring** if the number of colours used is $\leq k$.

Applications:

- scheduling (timetabling)
- compilers (register allocation)
- communications (frequency assignment)

Theorem.
If G is planar then it has a 4-colouring.

Ugly proofs?

Theorem.
If G is planar then it has a 4-colouring.

Proofs:

- very long proof using computer to check 1476 configurations spanning 400 pages.
  - K. Appel and W. Haken, Every planar map is four colorable. I. Discharging, *Illinois Journal of Mathematics* **21** (3) (1977) 429–490.
  - K. Appel, W. Haken and J. Koch, Every planar map is four colorable. II. Reducibility, *Illinois Journal of Mathematics* **21** (3) (1977) 491–567.
- long proof using computer to check 633 configurations
  - N. Robertson, D. Sanders, P. Seymour and R. Thomas, The four-colour theorem, *Journal of Combinatorial Theory, Series B* **70** (1997) 2–44.
- proof by Robertson *et al.* (1997) formalised and formally verified by computer
  - G. Gonthier, Formal proof — the Four Color Theorem, *Notices of the American Mathematical Society*, **55** (11) (Dec. 2008) 1382–1393.

Ugly proofs?

Recall: to solve quadratic equations, $ax^2 + bx + c = 0$: $\qquad x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Formulas also exist for cubic and quartic equations. *But* ...

Abel-Ruffini Theorem

There is no general algebraic formula (using arithmetic operations, powers & roots) for the roots of polynomials of degree ≥ 5.

Incomplete proof, $>$ 500 pages:

- Paolo Ruffini, *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto*, Stamperia di S. Tommaso d'Aquino, Bologna, 1799.

Complete proof, six pages:

- Niels Henrik Abel, *Mémoire sur les équations algébriques, ou l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, Groendahl, Christiania (Oslo), 1824.