Lecture 3: Proof by Contradiction

Dr John Levine

CS103 Machines, Languages and Computation
October 2nd 2015

University of Strathclyde Science

The Rules of the Game

- Lectures are Mon 10 in RC 345, Fri 10 in RC 641
- Tutorials: Thu 10 in JA505, Thu 1 in TG 227
- Lectures run Weeks 1-11 (no lectures in Week 12)
- Class materials will appear on the class web page:

  http://www.cis.strath.ac.uk/~johnl/CS103
- Facebook page: MLAC 2015
- Email: John.Levine@strath.ac.uk
- Room LT1420, extension 4524

University of Strathclyde Science

Tutorial Allocation

- You attend **one** tutorial per week
- The Thursday 1pm tutorial is for those students taking:
  - BSc Computer Science
- The Thursday 10am tutorial is for those students taking:
  - MEng Computer Science
  - BSc Mathematics and Computer Science
  - MEng Computer and Electronic Systems
  - BEng Computer and Electronic Systems
  - BSc Software Engineering
  - BSc Business Information Systems
  - Everyone else not already mentioned

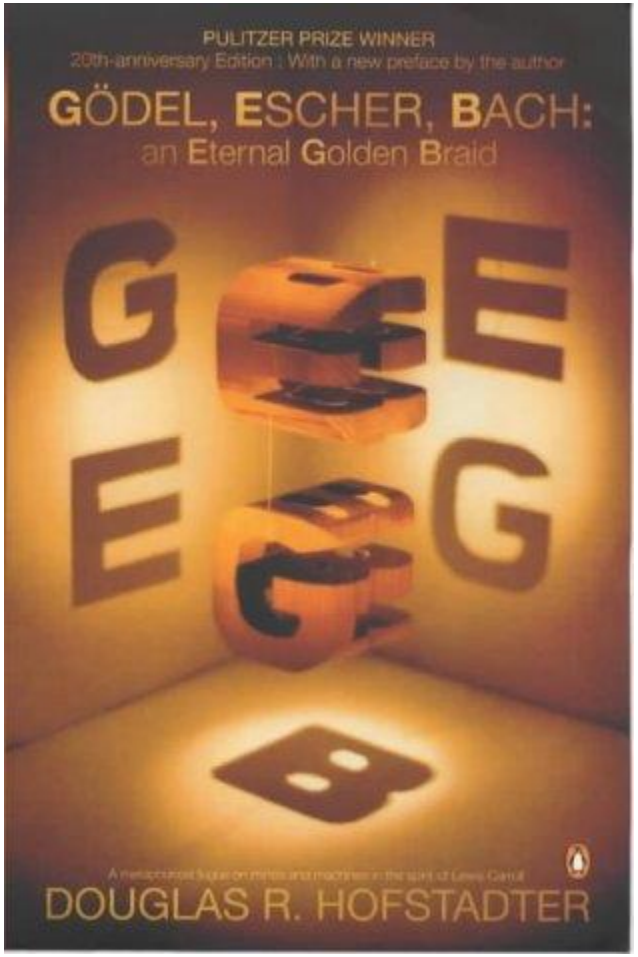
University of Strathclyde Science

Course Book

"Gödel, Escher, Bach: an Eternal Golden Braid"
by
Douglas R. Hofstadter

Publisher: Penguin Books Ltd
ISBN: 0140289208
Cost: £18.99 (amazon.co.uk)

You will need your own copy of this book as we will be reading from it every week.



All Computers are Equivalent

- In mathematical terms, all computers are equivalent (in the same way that all cars are equivalent).
- If you have a problem which can be solved on one computer, then it can be solved on *all* of them! This fundamental idea is called *The Church-Turing Thesis.*
- There are some problems which cannot be solved on *any* computer, no matter how powerful the computer is.
- The mathematical properties of *all* computers can be exactly modelled by very simple abstract devices.

University of Strathclyde Science

Non-Computable Functions

- The first 5 weeks of the course will build up towards the proof that non-computable functions exist:

  If P is the set of all computer programs and F is the set of all functions $f: n \rightarrow m$ such that n,m are members of the set of natural numbers N, then $|F| > |P|$ and therefore there are some functions in F for which no computer program can exist.

University of Strathclyde Science

Non-Computable Functions

- The first 5 weeks of the course will build up towards the proof that non-computable functions exist:

  If P is the set of all computer programs and F is the set of all functions $f: n \rightarrow m$ such that n,m are members of the set of natural numbers N, then $|F| > |P|$ and therefore there are some functions in F for which no computer program can exist.

University of Strathclyde Science

What is a Mathematical Proof?

- In mathematics, a proof is a logical argument showing that some statement (a *theorem*) is necessarily true
- A statement is an expression that is either true or false, such as “for every integer $n > 0$, the sum of the first n odd numbers is equal to n^2” or “all even numbers can be expressed as the sum of two prime numbers”
- The first of these can be proved – we will prove it later in the class
- The latter statement has not been proved – it is known as “Goldbach’s Conjecture”

University of Strathclyde Science

What is a Mathematical Proof?

- In mathematics, a proof is a logical argument showing that some statement (a *theorem*) is necessarily true
- A statement is an expression that is either true or false, such as “for every integer $n > 0$, the sum of the first n odd numbers is equal to n^2” or “all even numbers greater than 2 can be expressed as the sum of two prime numbers”
- The first of these can be proved – we will prove it later in the class
- The latter statement has not been proved – it is known as “Goldbach’s Conjecture”

University of Strathclyde Science

Infinite sets and proof

- The theorems we are trying to prove often have to hold true for infinite sets of numbers
- Example: prove that the sum of any two even numbers is also an even number
- The two numbers chosen can be any two members of the set of all of the even numbers (an infinite set)
- We deal with this by not naming specific numbers, but by using letters to stand for any two even numbers
- If our argument works using those letters, we know it will work for any two specific even numbers

University of Strathclyde Science

A Simple Proof

Theorem: adding two even numbers always gives an even number.

- Proof: let the sum be $s = a + b$ where a and b are *any* two even numbers
- Let $p = a/2$ and $q = b/2$. Because a and b are even, p and q are both whole numbers (integers)
- The sum is now: $s = 2p + 2q$
- We can rewrite this as: $s = 2(p + q)$
- Because p and q are integers, $(p + q)$ is also an integer
- s is 2 times an integer, and so this means that s must be an even number. ■

University of Strathclyde Science

Types of Proof

- *Direct proof* is where the conclusion is established by logically combining the axioms, definitions and earlier theorems.
- *Proof by contradiction* is where it is shown that if some statement were false, a logical contradiction occurs, hence the statement must be true.
- *Proof by induction* is where a “base case” is proved, and an “induction rule” used to prove an (often infinite) series of other cases. Since the base case is true, the infinity of other cases must also be true.

University of Strathclyde Science

Prime Numbers

- The usual definition of a prime number is “any integer greater than 1 that divides exactly only by itself and 1”
- 1 is not prime, because of The Fundamental Theorem of Arithmetic (due to Euclid): “Every positive integer greater than one can be written *uniquely* as a product of primes”
- Those numbers which can be written as a product of prime factors are known as *composite* numbers
- So, all integers > 1 are either prime or composite

University of Strathclyde Science

Prime Numbers

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

University of Strathclyde Science

Prime Numbers

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

University of Strathclyde Science

Proof by Contradiction

Theorem: There are infinitely many prime numbers.

- Proof: assume that there are finitely many prime numbers, and call the biggest prime number *N*.
- Now form the number $K = 1 \times 2 \times 3 \times \ldots \times N\text{-}1 \times N$.
- *K* divides exactly by every integer up to *N*.
- Now form the number $M = K + 1$.
- *M* can't be a multiple of 2, as it leaves 1 over when you divide it by 2.
- Or a multiple of 3, 4, 5 , … , *N*-1, *N.*
- So either *M* is prime, or it has a prime divisor > *N*. ■

University of Strathclyde Science

Gödel, Escher, Bach, Chapter 1

- In Chapter 1 of GEB ("The MU Puzzle") we are given the axiom MI and we have to make the theorem MU, using these four purely symbolic rules:

  I. $x\mathrm{I} \rightarrow x\mathrm{IU}$
  II. $\mathrm{M}x \rightarrow \mathrm{M}xx$
  III. $x\mathrm{III}y \rightarrow x\mathrm{U}y$
  IV. $x\mathrm{UU}y \rightarrow xy$

- Hofstadter asks: can you make MU?
- Levine asks: given some *arbitrary* string, can I write a algorithm to determine whether or not it is a theorem?

University of Strathclyde Science

Homework for next week

- Read Chapter 1 of Gödel, Escher, Bach and try out the MIU puzzle. Can you turn MI into MU?
- Start thinking about the “Levine asks” question on the previous slide.
- In the workbook, do Assignment 2, part (c). Try to do it without looking at the proof contained in this lecture!
- Next week: more on MIU, proof by induction.