Discrete Mathematics

Topic 02 — Methods of Mathematical Proof

Lecture 01 — Concepts and Direct Proofs

Dr Kieran Murphy ©(i)(s)

Department of Computing and Mathematics,
Waterford IT.
(kmurphy@wit.ie)

Autumn Semester, 2021

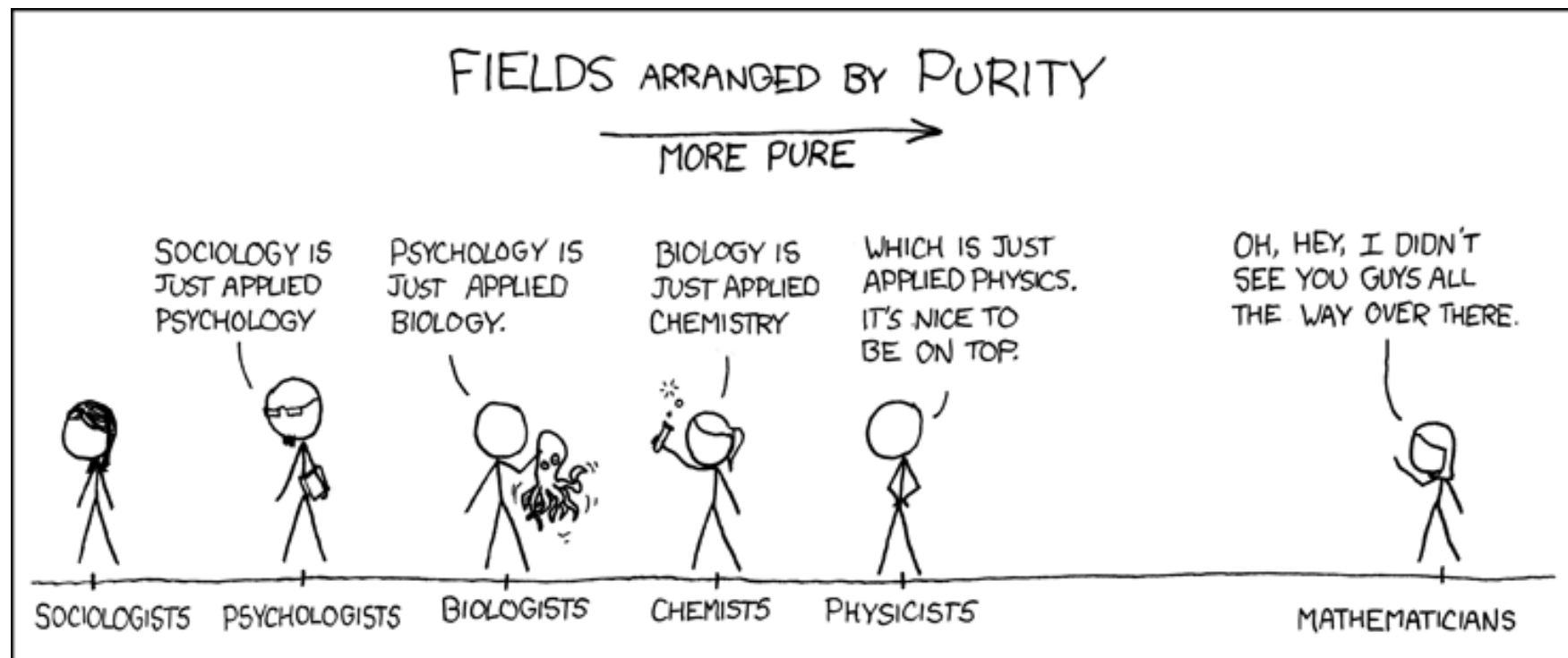## Outline

- Review of Mathematical Proofs
- Direct Proofs

Why do we Need Proofs?

Mathematics is perhaps the only field in which absolute certainty is possible.

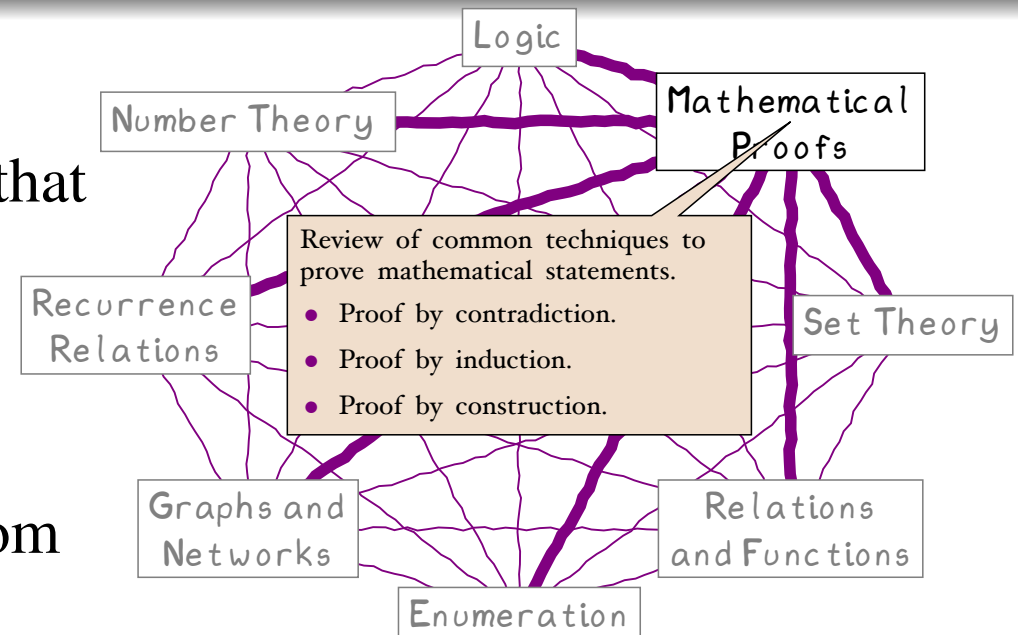This certainty come with a price — it takes effort and patience.

> *For God's sake, I beseech you, give it up. Fear it no less than sensual passions and because it, too, may take all your time, and deprive you of your health, peace of mind and happiness in life.*
>
> — *mathematician Farkas Bolyai (1775–1856) advice to his son to stay away from mathematics.*

https://xkcd.com/435

Motivation for Focusing on Techniques

Regardless of the area of Discrete
Mathematics or the type of problem that
we are studying we often have
claims that we want to either
prove or disprove.

The utility of Mathematics comes from
the fact that

Review of common techniques to
prove mathematical statements.
- Proof by contradiction.
- Proof by induction.
- Proof by construction.

While the area/problem may vary the techniques remain the same.

Main Techniques

- **Proof by Contradiction**

  Assume the negative of the claim and show that this leads to a contradiction.

- **Proof by Cases**

  List all possibilities (case) and analyse each separably.

- **Proof by Construction**, **Direct Proof**, …

Often a proof
is a mixture of
techniques.

Some Miscellaneous Mathematical Facts I

> Properties of Integers

- The negative of an integer is an integer.
- The sum, difference and product of two integers is an integer.
- An integer, n, is even if $n = 2k$ for some integer k.
- An integer, n, is odd if $n = 2k + 1$ for some integer k.
- Any real number, x, can be written as a sum of an integer x_n, and a fractional part, x_f, where $0 \le x_f < 1$.

$$x = \underbrace{x_n}_{\substack{\text{integer} \\ \text{part}}} + \underbrace{x_f}_{\substack{\text{fractional} \\ \text{part}}}$$
$$0 \le x_f < 1$$

- The floor function, denoted by $\text{floor}(x) = \lfloor x \rfloor$ returns the largest integer less than or equal to x, i.e., the integer part of x.
- The ceiling function, denoted by $\text{ceil}(x) = \lceil x \rceil$ returns the smallest integer greater than or equal to x.

The floor and ceiling functions can be confusing, especially for negative integers*

x	integer part, x_n	fractional part, x_f	floor$(x) = \lfloor x \rfloor$	ceil$(x) = \lceil x \rceil$
7	7	0	7	7
7.2	7	0.2	7	8
7.9	7	0.9	7	8
-7.9	-8	0.1	-8	-7
-7.2	-8	0.8	-8	-7
-7	-7	0	-7	-7

The important things to remember are :

- The fractional part is always zero (for integers) or positive.
- The ceiling is equal to the floor for integers.
- The ceiling is equal to the floor plus one for non-integers.

*Microsoft Excel had implemented the ceiling function incorrectly up until Excel 2010.

Types of Mathematical Statements

Theorems

Very important statements that have many and varied consequences.

Propositions

Less important and consequential statements.

Corollaries

Statements for which the truth can be deduced almost immediately from other statements.

Lemmas

Statements that don't have much intrinsic interest but help to prove other theorems.

Outline

- We use the premises in the problem to show that the claim must be true.

Direct Proof

Direct Proof

In a direct proof argument you apply the given premises to show that the claim must be correct.

Direct Proof (Formal Structure)

Given claim

$$P \implies Q$$

You

1. Assume P.

2. Demonstrate that Q must follow from P.

Example 1

> ## Example 1
>
> Let a and b be consecutive integers. Then, show that $a + b$ is odd.

> ### Proof (Direct Proof).
>
> Since a and b are consecutive integers, we can assume without loss of generality that $a = b + 1$. Then, we have
>
> $$a + b = (b + 1) + b = \underbrace{\underbrace{2b}_{\text{even}} + 1}_{\text{odd}}$$
>
> Therefore, $a + b$ is odd. □

Example 2   I

Example 2

In a cave you find three boxes. One contains gold, the other two are empty. Each box has imprinted on it a clue as to its contents; the clues are:

A: The gold is not here   B: The gold is not here   C: The gold is in box B

Only one message is true; the other two are false. Prove that the gold is in box A.

Note: The claim, may often be expressed as a question, e.g., "Is the gold in box A?", "Where is the gold?" etc.

Example 2 II

A direct proof here, would be to formalise the problem in propositional logic and find the solution using properties of logical operators (or using a truth table).

> (Atomic) Propositions

- A = "*Gold is in box A*"
- B = "*Gold is in box B*"
- C = "*Gold is in box C*"

A: The gold is not here   B: The gold is not here   C: The gold is in box B

> Statements (Not premises since, we don't asumme their truth value)

- S_1 = "*Gold is not here*"   (box A message)

$$S_1 = \neg A$$

- S_2 = "*Gold is not here*"   (box B message)

$$S_2 = \neg B$$

- S_3 = "*Gold is in box B*"   (box C message)

$$S_3 = B$$

Example 2 III

> Premises

- $P_1 = $ *"One box contains gold, the other two are empty."*

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or ...}} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 = $ *"Only one message is true; the other two are false"*

$$\text{(messages are } S_1, S_2 \text{ and } S_3)$$

$$P_2 = \left(S_1 \wedge \neg S_2 \wedge \neg S_3 \right) \vee \left(\neg S_1 \wedge S_2 \wedge \neg S_3 \right) \vee \left(\neg S_1 \wedge \neg S_2 \wedge S_3 \right)$$

$\boxed{S_1 = \neg A, S_2 = \neg B, S_3 = B}$

$$= \left(\neg A \wedge \neg \neg B \wedge \neg B \right) \vee \left(\neg \neg A \wedge \neg B \wedge \neg B \right) \vee \left(\neg \neg A \wedge \neg \neg B \wedge B \right)$$

$\boxed{\neg \neg p = p}$

$$= \left(\neg A \wedge B \wedge \neg B \right) \vee \left(A \wedge \neg B \wedge \neg B \right) \vee \left(A \wedge B \wedge B \right)$$

$\boxed{p \wedge \neg p = \mathbf{F}}$

$$= \left(\mathbf{F} \right) \vee \left(A \wedge \neg B \right) \vee \left(A \wedge B \right)$$
$$= \left(A \wedge \neg B \right) \vee \left(A \wedge B \right)$$

Example 2 IV

So, to recap, we have two true statements

- $P_1 = (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$
- $P_2 = (A \wedge \neg B) \vee (A \wedge B)$

and we want to prove the statement

- A = "*Gold is in box A*"

Let's build a truth table using *A*, *B*, and *C* as inputs, and $P_1 \wedge P_2$ as output. Then check:

"in rows with output True is *A* always True?"

A	B	C	P_1	P_2	$P_1 \wedge P_2$
F	F	F	F	F	F
F	F	T	T	F	F
F	T	F	T	F	F
F	T	T	F	F	F
T	F	F	T	T	T
T	F	T	F	T	F
T	T	F	F	T	F
T	T	T	F	T	F

Hence the claim is true and the gold is in box A.

Only interested in rows where both premises are True.

Examples

a) The sum of two odd numbers is even.

b) The product of two odd numbers is odd.

c) The square of an even natural number is even.

d) If A and B are real positive numbers, then

$$\underbrace{\frac{A+B}{2}}_{\text{arithmetic mean}} \geq \underbrace{\sqrt{AB}}_{\text{geometric mean}}$$

Hint: Use fact that $(a-b)^2 = a^2 - 2ab + b^2 \geq 0$.

e) Prove the Pythagorean theorem.

f) Prove that $x = y$ if and only if $xy = \frac{(x+y)^2}{4}$. Note, you will need to prove in two "directions" here: the "if" and the "only if" part.