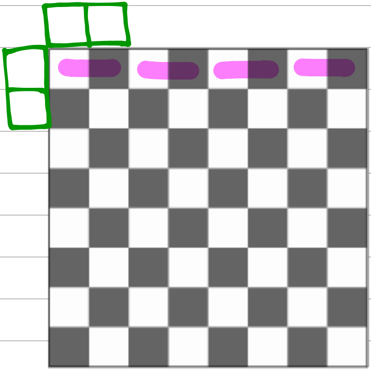
§§ 1.3–1.4 Methods of Proof

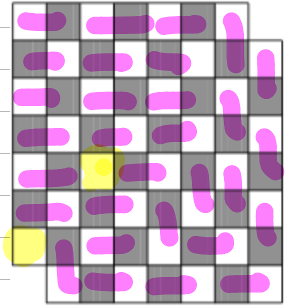
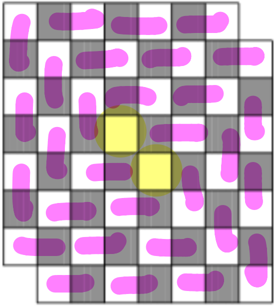
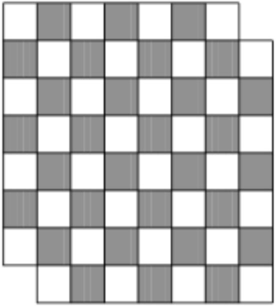
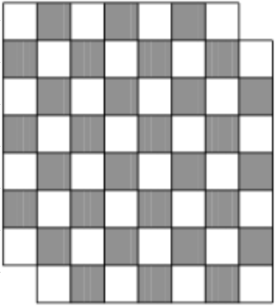
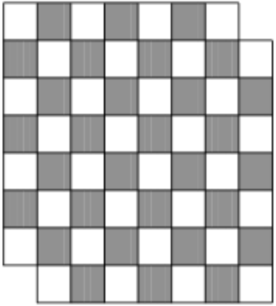
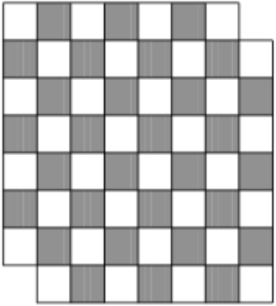
Words like "proof" and "theorem/theory" have very different meanings in math than in other fields...

Ex Mutilated Checkerboard problem



Given dominos which cover two adjacent squares, can cover whole board with 32 dominos.

Can we still cover ("tile") the checkerboard if we remove two opposite corners?

Scientific Approach

After 2 (5, 100, 200, 20,000, ...) attempts we suspect can't be done. Might eventually be called "theory." BUT eventually may be replaced by more accurate explanation.

Mathematical Approach

We want airtight logical argument. A correct mathematical proof is true for all eternity (!!)

Pf that it can't be done:

Each domino covers 1 B, 1 W.

After 30 dominos, 2 W remain, which cannot be covered by 1 domino.

In symbols, to prove $p \Rightarrow q$, construct a series of implications $p \Rightarrow s_1 \Rightarrow s_2 \Rightarrow s_3 \Rightarrow \cdots \Rightarrow s_n \Rightarrow q$

Key: if p is true and each implication is true, then q is true as well!

⚠ Before we start, what can you assume in these sections?

- arithmetic, algebra
- n is <u>even</u> integer if $n = 2k$, some integer k
- n is <u>odd</u> if $n = 2k+1$, some integer k.

  $0 = 2 \cdot 0$, so 0 is even
- x is rational if $x = \frac{a}{b}$, a, b integers, $b \neq 0$

  (else irr'l)

Ex Direct Proof of "if n is odd, then n^2 is odd."

One approach: start by writing given information, rephrase, write out def$^{\text{s}}$, etc. Do same at bottom of page for what we want to show. Connect by filling in between.

Pf: Let n be odd, so $n=2k+1$ for some integer k.

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ &= 2(2k^2+2k)+1 \end{aligned}$$

← Oklahoma Rule

$n^2 = 2\ell+1$ for some integer ℓ. $= 2k^2+2k$.

Thus n^2 is odd

Prove: n odd $\Rightarrow n^2$ odd

Another approach: "follow your nose." Works when there's really only thing to do at any stage.

Pf: n odd $\Rightarrow n = 2k+1$, some k

$$\Rightarrow n^2 = (2k+1)^2$$
$$= \cdots$$
$$= 2(2k^2+2k)+1$$

$\Rightarrow n^2 = 2\ell+1$, some ℓ

$\Rightarrow n^2$ odd.

Generally, we write our final version in paragraph form.

No 2-column proofs in this course

<u>Prove</u>: If n is an odd integer, then n^2 is odd.

Ex: Write a direct proof of "for an integer n, n^2 even $\Rightarrow$ n even."

Pf: Let n^2 be even, so $n^2 = 2k$ for some k.

Then $n = \sqrt{2k} = \sqrt{2} \cdot \sqrt{k}$

STUCK!

How could I show $n = 2\ell$, some ℓ?

Proof by Contrapositive: prove $p \Rightarrow q$ indirectly via a direct proof of (logically equivalent) contrapositive statement.

$$\sim q \Rightarrow \sim p$$

<u>Prove:</u> n^2 even $\Rightarrow$ n even

<u>Pf</u>: I will prove the equivalent contrapositive stmt,

$$n \text{ odd} \Rightarrow n^2 \text{ odd}.$$

(Done in 3 lines)

or cite, if already done

"reduce to a previously solved problem."

Proof by Contradiction

A contradiction is stmt which is always false: $2=1$, 2 odd. We can use them to prove stmts. Let c be a contradiction

- $(\sim p \Rightarrow c) \Leftrightarrow p$

  Assume p is false, show it leads to nonsense. Hence our assumption was wrong, and p must be true.

- $[(p \wedge \sim q) \Rightarrow c] \Leftrightarrow p \Rightarrow q$

  Assume p and $\sim q$, i.e. assume $(p \Rightarrow q)$ is false, show that leads to nonsense. Hence assumption is wrong, and $(p \Rightarrow q)$ must be true.

Prove: There are infinitely many primes.

Let's use fact that if p divides evenly into n and m, then it also divides evenly into $n+m$, $n-m$, etc.

Ex 7 divides evenly into 28 and 42. Also into $42-28=14$.

Pf: Assume not, so there are finitely many primes,

$$p_1, p_2, p_3, \ldots, p_n.$$

Define $N = p_1 p_2 p_3 \cdots p_n - 1$. This is a number, so there is a p_i which divides into it. That p_i also divides evenly into $N+1 = p_1 p_2 \cdots p_i \cdots p_n$.

Thus p_i divides $(N+1)-N = +1$. $\lightning$, $\rightarrow\leftarrow$ This is a contr. (prime can't divide 1). Hence our ass'mptn was wrong.

Prove $\sqrt{2}$ is irrational

Prove If $\underbrace{f(x)=\frac{2x+3}{x+2}}_{p}$, then $\underbrace{\text{for all } x,\ f(x)\neq 2}_{q}$.

Pf: Assume not, so $f(x)=\frac{2x+3}{x+2}$ and there exists an x for which $f(x)=2$. ($\leftarrow$ $\sim(p\Rightarrow q)$ is p and $(\sim q)$)

Note that this x is not -2, which is not in domain of f.

Then for this x,
$$\frac{2x+3}{x+2}=2$$
$$2x+3=2x+4$$
$$3=4$$

This is a contradiction; hence our assumption was wrong and the stmt is true.

⚠ Don't overuse Pf by contradiction.

Prove: n odd $\Rightarrow n^2$ odd

Pf: Assume not, so n is odd but n^2 is even.

Then $n = 2k+1$ for some k, and

$$n^2 = (2k+1)^2$$
$$=$$
$$\vdots$$
$$= 2(\quad) + 1$$

unnecessary contradiction – just use direct pf in middle!

Thus n^2 is an odd number.

This contradicts assumption that n^2 is even, etc.

$\exists$ other methods...

Pf by induction – later this semester!

"Pf by Cases": <u>Prove</u> $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$ for $b \neq 0$.

<u>Recall</u>: $|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{else.} \end{cases}$

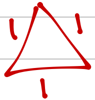
<u>Pf</u>: Go through each of 4 case (a, b +/–) and explain why formula is true.

Wrapup...

WATCH OUT: to prove a stmt is false it suffices to give one counterexample.

(negation of "always true" is "false at least once".)

Ex "$a^2+b^2=c^2$ for all Δ's". false:



BUT you can't prove a universal stmt by checking 1 (or 10, or 10,000,000...) examples.

Ex Can't prove Pyth. Thm just for 3-4-5 right Δ.

Also iff stmts require two proofs!! $p \Leftrightarrow q$: $p \Rightarrow q$
$q \Rightarrow p$

Deductive Reasoning

Showing a conclusion follows from certain premises

$$p \Rightarrow s_1 \Rightarrow s_2 \Rightarrow \cdots \Rightarrow q$$

Inductive Reasoning

pattern recognition.

Often we use INductive reasoning to figure out what to prove, DEductive to do it.

Proof techniques

Similar lists have been circulating around the net for decades. The original was written by Dan Angluin and publisted in SIGACT News, Winter-Spring 1983, Volume 15 #1.

Proof by example

The author gives only the case n = 2 and suggests that it contains most of the ideas of the general proof.

Proof by intimidation

``Trivial'' or ``obvious.''

Proof by exhaustion

An issue or two of a journal devoted to your proof is useful.

Proof by omission

``The reader may easily supply the details'', ``The other 253 cases are analogous''

Proof by obfuscation

A long plotless sequence of true and/or meaningless syntactically related statements.

Proof by wishful citation

The author cites the negation, converse, or generalization of a theorem from the literature to support his claims.

Proof by importance

A large body of useful consequences all follow from the proposition in question.

Proof by reference to inaccessible literature

The author cites a simple corollary of a theorem to be found in a privately circulated memoir of the Icelandic Philological Society, 1883. This works even better if the paper has never been translated from the original Icelandic.

Proof by ghost reference

Nothing even remotely resembling the cited theorem appears in the reference given. Works well in combination with proof by reference to inaccessible literature.

Proof by accumulated evidence

Long and diligent search has not revealed a counterexample.

Proof by mutual reference

In reference A, Theorem 5 is said to follow from Theorem 3 in reference B, which is shown to follow from Corollary 6.2 in reference C, which is an easy consequence of Theorem 5 in reference A.

Proof by picture

A more convincing form of proof by example. Combines well with proof by omission.

Proof by misleading or uninterpretable graphs

Almost any curve can be made to look like the desired result by suitable transformation of the variables and manipulation of the axis scales. Common in experimental work.

Proof by vehement assertion

It is useful to have some kind of authority relation to the audience, so this is particularly useful in classroom settings.

Proof by vigorous handwaving

Works well in a classroom, seminar, or workshop setting.

Proof by appeal to intuition

Cloud-shaped drawings frequently help here.

Proof by cumbersome notation

Best done with access to at least four alphabets, special symbols, and the newest release of LaTeX.

Proof by abstract nonsense

A version of proof by intimidation. The author uses terms or theorems from advanced mathematics which look impressive but are only tangentially related to the problem at hand. A few integrals here, a few exact sequences there, and who will know if you really had a proof?