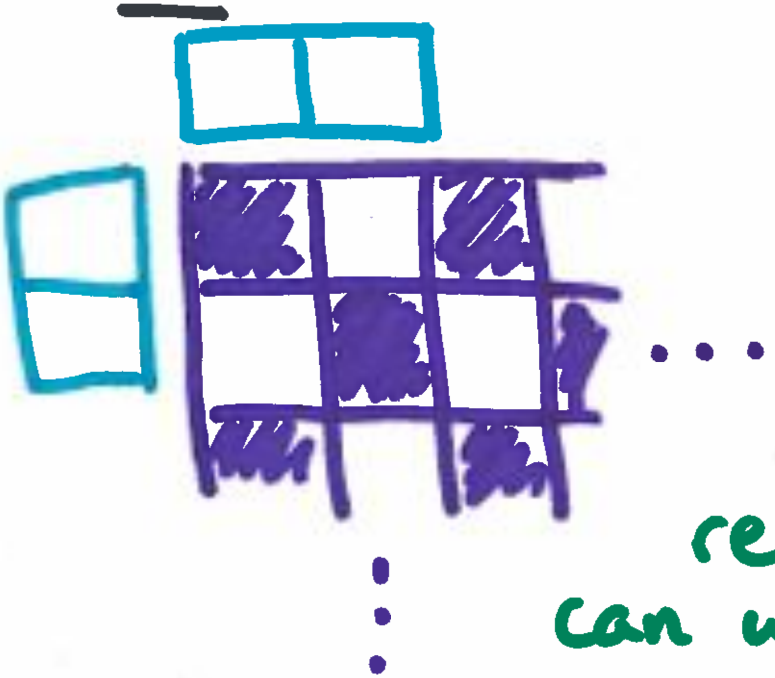
§1.3-1.4 Techniques of Proof

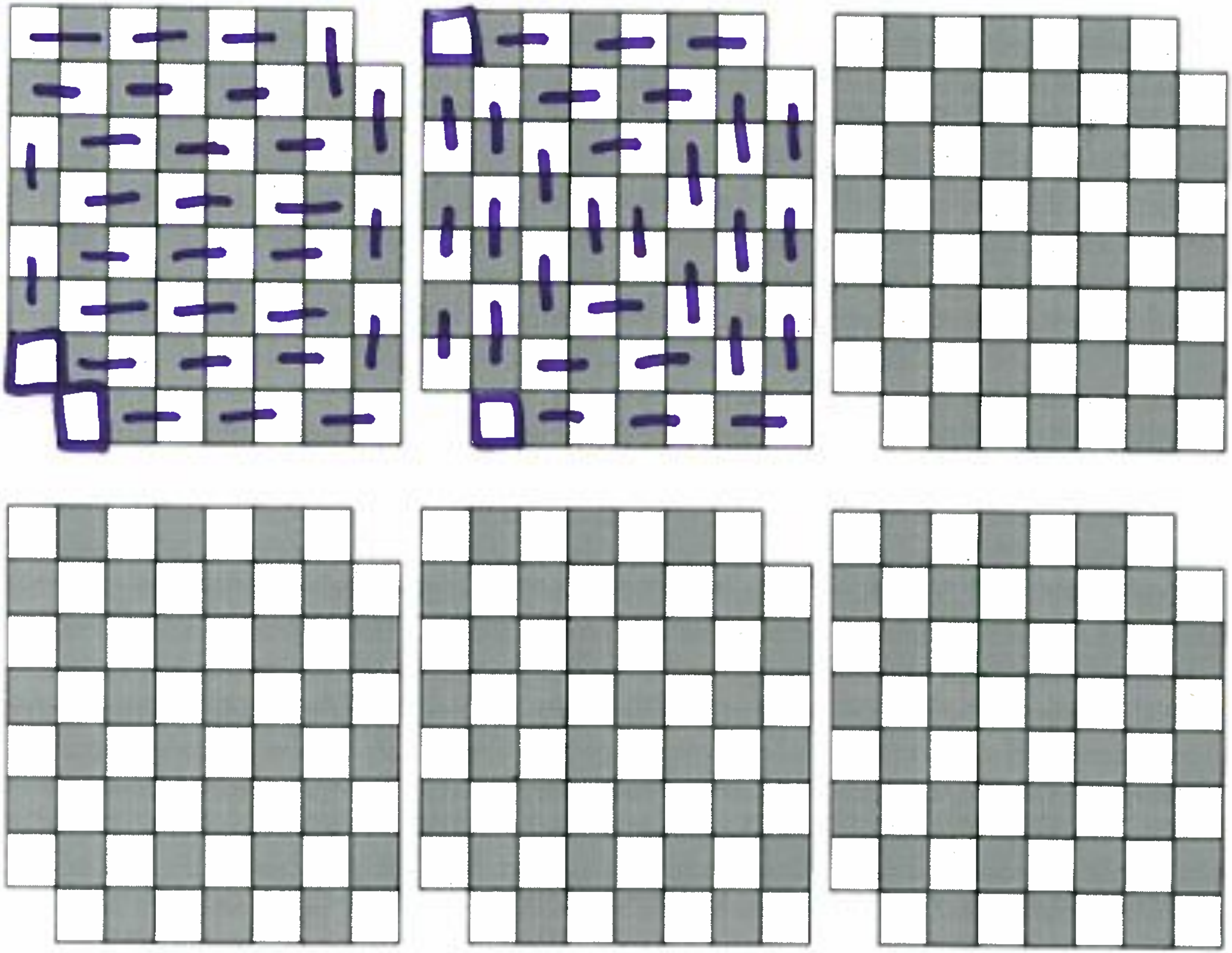
Words like "proof" and "theorem/theory" have very different meanings in math than in other fields.

Ex Mutilated Checkerboard Problem (MCP



Take dominos which can be laid vertically or horizontally over two squares on board. If we remove opposite corners of board, can we cover it completely w/ dominos?

Mutilated Checkerboard Problem



"Scientific" Approach

After 5 (50, 500, ...) failed attempts we suspect it can't be done. Might eventually be called "theory." BUT eventually may be replaced by more accurate explanation.

Math approach - we want an airtight logical argument. A correct mathematical proof is true for all eternity. (!!)

In symbols, to prove if p, then q ($p \Rightarrow q$) we want to construct a series of implications w/ stmts: $p \Rightarrow s_1 \Rightarrow s_2 \Rightarrow s_3 \Rightarrow \cdots \Rightarrow s_n \Rightarrow q$.

<u>KEY</u>: If p is true and each implication is true, then q is true as well!

⚠ Before we start, what can you assume in this section? algebra, arithmetic

- n even integer $\Leftrightarrow$ $n = 2k$, some intgr k
  n odd $\Leftrightarrow$ $n = 2k+1$ ———— " ————
- x rational $\Leftrightarrow$ $x = \frac{a}{b}$ ← integers, $b \neq 0$.

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

One approach: start at beginning and end, and work to connect them in the middle.

Pf Suppose n is odd.

$\Rightarrow n = 2k+1$, some integer k.

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

$\Rightarrow n^2 = 4k^2 + 4k + 1$

$$\Rightarrow n^2 = 2\underbrace{(2k^2 + 2k)}_{\text{integer.}} + 1$$

$\Rightarrow n^2 = 2 \cdot \ell + 1$, integer ℓ

$\Rightarrow$ Thus n^2 is odd.

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

Another approach: "follow your nose" – works when there's really only one thing to do at each step.

Let n be odd integer.

$\Rightarrow n = 2k+1$, some k

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

$\Rightarrow n^2 = 4k^2 + 4k + 1$

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

$\Rightarrow n^2$ odd.

Generally, we write our final version in paragraph form.

→ No two column proofs in this course! ←

Prove If n is an odd integer, then n^2 is odd.

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

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

which has the form of an odd integer. Thus n^2 is odd.

Direct Proof is just one method

Today/Friday: Pf by contrapositive, pf by contradiction, (pf by cases)

induction - to come later!

Def The contrapositive of $p \Rightarrow q$ is $\sim q \Rightarrow \sim p$

Ex Write contrapositive of:

If $x>1$, then $x^2>1$.

If $x^2 \leq 1$ then $x \leq 1$.

If it's raining, the sidewalk is wet.

dry sidewalk $\Rightarrow$ not raining.

Contrapos. is useful b/c of this tautology:

$$(p \Rightarrow q) \Longleftrightarrow (\sim q \Rightarrow \sim p)$$

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

Ex Prove: for an integer n, n^2 even $\Rightarrow$ n even

Pf: Let n^2 be even

$\Rightarrow n^2 = 2k$, some k.

Now what?! $n = \sqrt{2k} = \sqrt{2}\sqrt{k}$??!

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

Pf: We prove the equivalent contrapositive stmt,

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

(in 3 lines we're done)

Proof by Contradiction A contradiction is a stmt which is always false: 2 is odd, $0=1$

We can use contradictions to prove things:

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

  If I assume p is false and ~~the~~ it leads to total nonsense (a contradiction), the our assumption was wrong, and thus p must be true.

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

  If we assume $p \Rightarrow q$ is false (i.e $p \wedge \sim q$) and it leads to a contradiction, then $p \Rightarrow q$ must be true.

Prove There are infinitely many primes.

My favorite version uses the fact that if p divides evenly into n and m, then it divides evenly into $n+m$, $n-m$, etc.

Ex 5 divides 20, 30

5 divides -10, 50

Pf Assume there are only finitely many primes, $p_1, p_2, \dots, p_n$. let $N = p_1 p_2 \cdots p_n - 1$.

Since N is an integer, it is divisible by some prime p_i. Thus p_i divides both N, $N+1$, hence divides $(N+1)-N = 1$. $\lightning$

Thus our assumption was wrong, etc....

Last "Method": Proof by cases

Prove $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$

Pf

Case 1 $a \le 0,\ b < 0$ $\qquad \frac{|a|}{|b|} = \frac{-a}{-b} = \cdots = \left|\frac{a}{b}\right|$

Case 2 $a \le 0,\ b > 0$

Case 3 $a \ge 0,\ b < 0$

Case 4 $a \ge 0,\ b > 0$

__WATCH OUT__: to prove a stmt is false it suffices to give __one__ counterexample.
(negation of "always true" is "fails at least once.")

__Ex__ give ctr-ex to $a^2+b^2=c^2$ for all Δ's.

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

To prove Pyth. Thm, can't just check 3-4-5 Δ.

Summary of terms

Given

$p \Rightarrow q$ implication

$\sim q \Rightarrow \sim p$ contrapositive

} log. eq.

$q \Rightarrow p$ converse

$\sim p \Rightarrow \sim q$ inverse

} log. eq.

⚠ In general $\exists$ no connection b/w truth values of $p \Rightarrow q$ and its converse

Ex n^2 even $\Leftrightarrow$ n even (T)

[redacted] (T)

converse: n even $\Rightarrow$ n^2 even

$f(x)$ diff'ble $\Rightarrow$ $f(x)$ continuous. (T)

converse: cont $\Rightarrow$ diff'ble False

__Deductive Reasoning__ showing a conclusion follows from certain premises.

$$p \Rightarrow s_1 \Rightarrow \cdots \Rightarrow s_n \Rightarrow q$$

__Inductive Reasoning__ pattern recognition.

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

How to prove it (floating around online for 20+ years?)

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'.

Proof by vigorous handwaving:
Works well in a classroom or seminar setting.

Proof by cumbersome notation:
Best done with access to at least four alphabets and special symbols.

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 funding:
How could three different government agencies be wrong?

Proof by eminent authority:
'I saw Karp in the elevator and he said it was probably NP- complete.'

Proof by personal communication:
'Eight-dimensional colored cycle stripping is NP-complete [Karp, personal communication].'

Proof by reduction to the wrong problem:

'To see that infinite-dimensional colored cycle stripping is decidable, we reduce it to the halting problem.'

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 Slovenian Philological Society, 1883.

Proof by importance:
A large body of useful consequences all follow from the proposition in question.

Proof by accumulated evidence:
Long and diligent search has not revealed a counterexample.

Proof by cosmology:
The negation of the proposition is unimaginable or meaningless. Popular for proofs of the existence of God.

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 metaproof:
A method is given to construct the desired proof. The correctness of the method is proved by any of these techniques.

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

Proof by vehement assertion:
It is useful to have some kind of authority relation to the audience.

Proof by ghost reference:
Nothing even remotely resembling the cited theorem appears in the reference given.

Proof by forward reference:
Reference is usually to a forthcoming paper of the author, which is often not as forthcoming as at first.

Proof by semantic shift:
Some of the standard but inconvenient definitions are changed for the statement of the result.

Proof by appeal to intuition:
Cloud-shaped drawings frequently help here.