Today:

- Example of an axiom system
- Proof methods
- Purposes of proof
- Many proofs example

HW #1

Textbook problems I: 11, 16

Also, write an inductive proof (using the formula $\binom{n}{i} = \frac{n!}{i!(n-i)!}$), and a direct proof using the definitions, of Pascal's identity:

$$\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$$

Assume the following statements are true about

- some things we will call numbers (which will be denoted by letters like $a, b, c \ldots$)
- distinguished numbers called 1 and 0
- operations $+, -, \cdot$, and $/$

Axiom 1 Commutativity

$$a+b = b+a \quad \text{and} \quad a \cdot b = b \cdot a$$

Axiom 2 Associativity

$$(a+b)+c = a+(b+c) \quad \text{and} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Axiom 3 Distributivity

$a(b+c) = a \cdot b + a \cdot c$ and

$(a+b) \cdot c = a \cdot c + b \cdot c$

Axiom 4 **Zero**

$a + 0 = a$ and

$0 + a = a$

Axiom 5 **One**

$a \cdot 1 = a$

$1 \cdot a = a$

Axiom 6 **Subtraction**

If $a + x = 0$, there is a number called

$-a$

such that $x = -a$

Axiom 7 **Division**

If $ax = b$ (and $a \neq 0$), then there is a number called

a^{-1}

such that $x = a^{-1} \cdot b$ (and $x = b \cdot a^{-1}$)

Assume the following statements are true about some numbers and a relation called $<$ (or $>$) between them:

Inequality axioms

Axiom 1 **Trichotomy**

Either $a < b$, or

$a = b$, or

$b < a$,

and for given a and b only 1 of these is true.

Axiom 2 **Addition**

If $a < b$, then $a + c < b + c$ for any c.

Axiom 3 **Multiplication**

If $a < b$ (and $c > 0$), $a \cdot c < b \cdot c$

If $a < b$ (and $c < 0$), $a \cdot c > b \cdot c$

Axiom 4 **Transitivity**

If $a < b$ and $b < c$, then $a < c$

---

https://www.youtube.com/watch?v=ixsXkrBV80A

Proof methods

- cases (exhaustion)
- reconstruction (backwards)
- contradiction
- ~~intimidation, authority~~
- induction

Examples

Proposition. If $a < b$ and $a > 0$ then $a^2 < b^2$.

Proof. Assume $a < b$.

Since $a > 0$,

$a \cdot a < a \cdot b$ (mult. axiom)

Also, $0 < a$ and $a < b \Rightarrow 0 < b$ (transitivity axiom). Th

$a \cdot b < b \cdot b$ (mult. axiom)

Then

$a^2 < a \cdot b$ and $a \cdot b < b^2 \Rightarrow a^2 < b^2$ (trans. axiom)

Lemma $a^2 > 0$ unless $a = 0$. Proof: If $a > 0$, $a \cdot a > 0$.
If $a < 0$, $a \cdot a > 0$.

Proposition If $a < b$ then $4ab < (a+b)^2$

Proof.

#1

The technically correct "I already magically know the answer" proof:

#2

The explanatory backwards proof

$(a+b)^2 = a^2 + 2ab + b^2$, so the conclusion is equivalent to

$(a-b)^2 > 0$ (see lemma)

$\Rightarrow a^2+b^2-2ab > 0$

$\Rightarrow a^2+b^2+2ab > 4ab$ (addition)

$\Rightarrow (a+b)^2 > 4ab$

$$4ab < a^2 + 2ab + b^2$$

which is equivalent, by the addition law, to

$$0 < a^2 - 2ab + b^2$$

The right-side expression we recognize from experience with algebra:

$$a^2 - 2ab + b^2 = (a-b)^2$$

Then the statement is equivalent to

$$0 < (a-b)^2,$$

which follows from the lemma.

Definition For integers a and b,

$$a \mid b \qquad (\text{"}a \text{ divides } b\text{"})$$

means that there is an integer c such that

$$b = a \cdot c$$

Proposition If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof:

$$b = a \cdot k, \; c = b \cdot l \implies c = (a \cdot k) \cdot l$$

$$\implies c = a \cdot (k \cdot l) \iff a \mid c.$$

Proposition There do not exist integers m and n such that

$$14m + 20n = 101$$

Proof. Suppose there were such integers.

Then

$$2 \cdot (7m + 10n) = 101 \quad \text{[distributivity]}$$

Now: Either $(7m+10n) \geq 51$ or $(7m+10n) \leq 50$. [AND this is all the possibilities]

In the first case,

$$2 \cdot (7m + 10n) \geq 102, \text{ and}$$

in the second case

$$2 \cdot (7m+10n) \leq 100$$

Since in all cases $2 \cdot (7m+10n) \neq 101$, and yet

$$2 \cdot (7m + 10n) = 101,$$

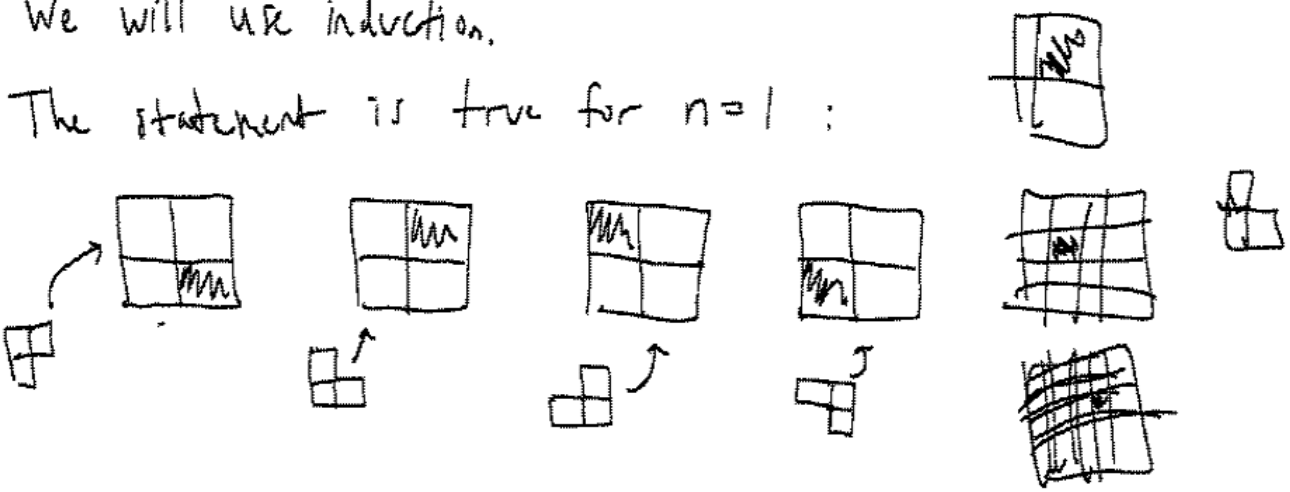
we have reached a contradiction by assuming that m and n exist with the stated property.

Therefore no such m, n exist.

Proposition. Every square made of a 2^n by 2^n grid of squares can be covered by tiles in the shape  , provided that 1 square is removed from the grid.

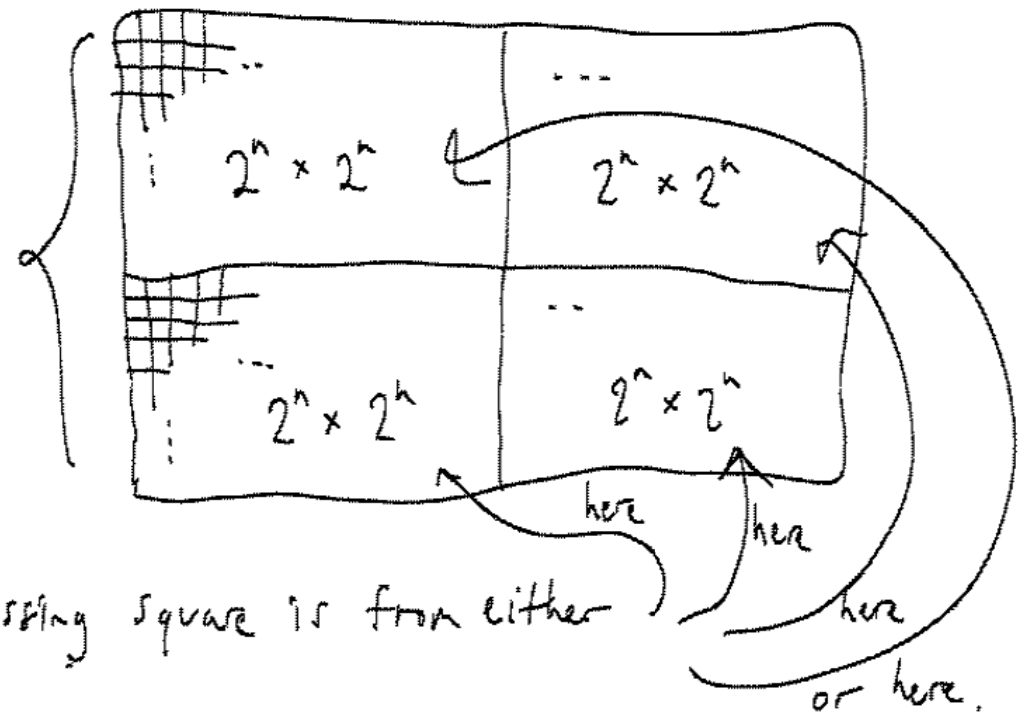
Proof. We will use induction.

The statement is true for $n=1$:



Now, suppose the statement is true for some given value of n, and consider a 2^{n+1} by 2^{n+1} grid with 1 square removed.

$2 \cdot 2^n$

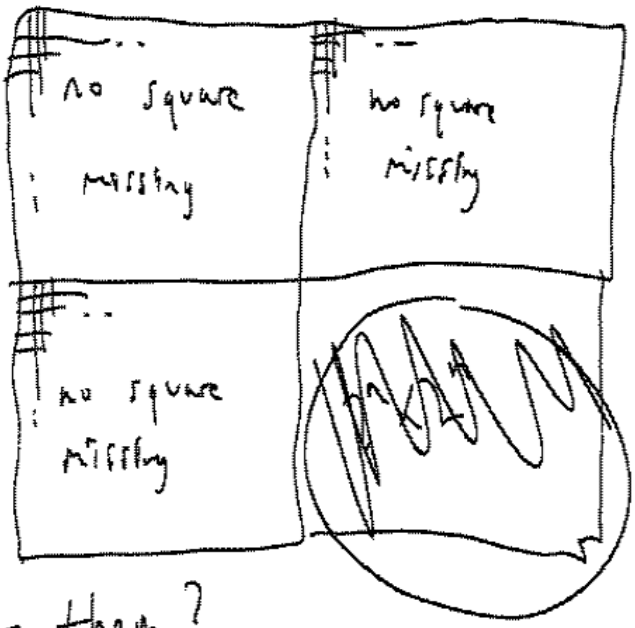


The missing square is from either

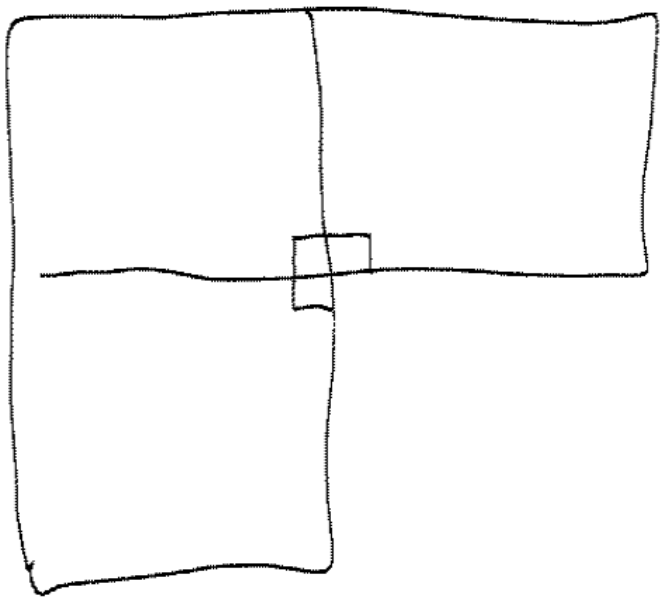
By induction, the $2^n \times 2^n$ quadrant with a missing square

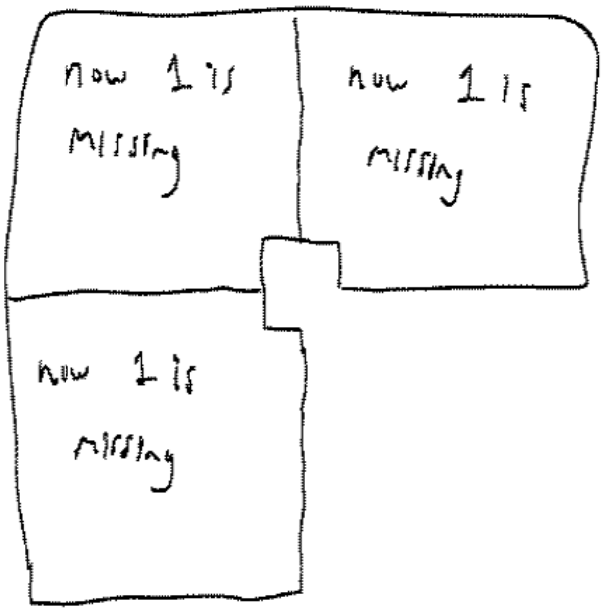
can be covered.

What about the remaining 3 full quadrants???



How to cover them?





So the 2^{n+1} by 2^{n+1} grid with 1 missing can also be covered.

Therefore all 2^n by 2^n grids with 1 square missing can be covered by the ⅃ tiles.

Induction principle (Axiom)

Let P_n be a sequence of statements:

$$P_1, P_2, P_3, \ldots$$

If P_1 is true, and P_n implies P_{n+1} for each n, then all P_n are true.

Strong induction

Let P_n be a sequence of statements.

If, for each n, all previous statements

$$P_1, P_2, \ldots, P_{n-1}$$

imply P_n, then all P_n are true.

Exercise

(1) Prove that 7 does not divide 100. $(7 \nmid 100)$

(2) Let P = "I ride the train"
Q = "I drive"
R = "I will be late"

Write correct English versions of the following statements:

a) $P \Rightarrow R$ [implication]

b) $R \Rightarrow P$ [converse]

c) not $R \Rightarrow$ not P [contrapositive]

d) $(P \text{ or } Q) \Rightarrow R$

e) not $R \Rightarrow$ (not P) and (not Q)

Are (d) and (e) equivalent?