Recap :

Propositional Logic

- Boolean formulae : satisfiable / tautology
- Tautologies $\rightsquigarrow$ Proof strategy

$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$

Proof by contraposition

$$(p \wedge (p \Rightarrow q)) \Rightarrow q$$

$$\left((p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \cdots \wedge (p_{i-1} \Rightarrow p_i)\right) \Rightarrow (p_1 \Rightarrow p_i)$$

To prove $p_1 \Rightarrow p_i$, construct a sequence of implications, $(p_1 \Rightarrow p_2), (p_2 \Rightarrow p_3), \cdots, (p_{i-1} \Rightarrow p_i)$

Predicate Logic $\quad P : S \rightarrow \{T, F\}$

$\forall x \in S : P(x) \qquad \exists x \in S : P(x)$

Rules for simplifying predicate logic expressions

$\neg(\forall x \in S : P(x)) \Leftrightarrow \exists x \in S : \neg P(x)$

$\neg(\exists x \in S : P(x)) \Leftrightarrow \forall x \in S : \neg P(x)$

used often, when proving by contradiction

See last lecture for other such rules.

Exercise : $P : \mathbb{N} \to \{T, F\}$

$Q : \mathbb{N} \to \{T, F\}$

$$S = \left(\forall n \in \mathbb{N} . \ (n \geq 5) \Rightarrow P(n) \right)$$

$$U = \left(\forall n \in \mathbb{N} . \ (n \geq 6) \Rightarrow Q(n) \right)$$

$$V = \left(\exists n . \ P(n) \wedge \neg Q(n) \right)$$

$$S \wedge U \implies V \ ?$$

No. Consider Q s.t. $Q(n) = T$ for all n.

P s.t. $P(n) = T$ for all n.

$S = U = T$ but $V = F$.

Exercise 2: Consider the stmt:

$$\forall n \geq 50 . \ \exists x \geq 0 . \ \exists y \geq 0 . \ \exists z \geq 0 . \ n = 6x + 14y + 21z .$$

Negation of this statement ?

$$\exists n \geq 50 . \ \forall x \geq 0 . \ \forall y \geq 0 . \ \forall z \geq 0 . \ n \neq 6x + 14y + 21z .$$

Lecture 5 : Mathematical Induction

$\mathbb{N}$: every natural number $n > 1$ is either prime or can be expressed as product of two or more primes. Is this decomposition unique?

We will prove this (and other facts about natural numbers) using Principle of Math. Induction (PMI).

Axiom: Principle of Math. Induction.

Let $P : \mathbb{N} \to \{T, F\}$ be a predicate s.t.

Base case • $P(1) = T$

Induction step • $\forall i \in \mathbb{N}$, $P(i) \Rightarrow P(i+1)$

Then, $\forall n \in \mathbb{N}$, $P(n)$ holds.

There is also a stronger version of PMI, called Strong Principle of Math. Induction (strong PMI) (which is actually equivalent to PMI, although makes our proofs slightly cleaner)

Axiom: Strong Principle of Math. Induction.

Let $P: \mathbb{N} \to \{T, F\}$ be a predicate s.t.

Base case • $P(1) = T$

Induction step • $\forall i \in \mathbb{N}, (P(1) \wedge P(2) \wedge \dots \wedge P(i)) \Rightarrow P(i+1)$

Then, $\forall n \in \mathbb{N}$, $P(n)$ holds.

PMI and strong PMI are two new 'proof strategies'. To prove something using PMI / strong PMI, you need to prove both the 'base case' and the 'induction step'.

PMI / strong PMI are often useful when you have to prove something for all $n \in \mathbb{N}$, given the 'base case' and 'induction step'.

Note that induction is not needed if you have to prove $P(c)$ (where c is some finite number) and you are given $P(1)$, and also given that for all $i \in \mathbb{N}$, $P(i) \Rightarrow P(i+1)$.

Template for proofs using PMI / Strong PMI.

1. State whether you're using PMI or Strong PMI.

2. Clearly state the induction hypothesis: the predicate $P : \mathbb{N} \to \{T, F\}$ used for induction

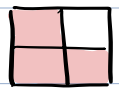
3. Prove the base case.

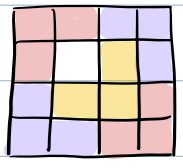
4. Prove the induction step.

Example 1: [Thm 5.1.2 of [LLM]]

Given a square board of dimension $2^n \times 2^n$. Need to cover this grid with non-overlapping  trominoes. Can't cover the whole grid since there are 4^n squares and 3 does not divide 4^n. Can we cover all-but-one square?

$n = 0$ ✓

$n = 1$  ✓

$n = 2$  ✓

Claim 5.1: $\forall n \geq 1$, $\exists\ (x, y) \in [2^n] \times [2^n]$ s.t. $2^n \times 2^n$ square board with (x, y) square removed can be covered by non-overlapping trominoes.

Informal statement: For any n, there exists some square that can be removed, and the remaining can be covered using non overlapping ⊞

Proof: PROOF BY (WEAK) INDUCTION

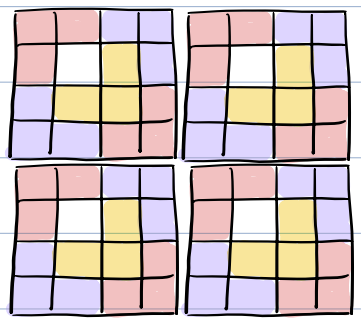
$P(n) :=$ $\exists\ (x, y) \in [2^n] \times [2^n]$ s.t. $2^n \times 2^n$ square board with (x, y) removed can be covered by non-overlapping trominoes

BASE CASE: Holds true for $n = 1$. Pick $(1, 1)$, and the remaining can be covered using  .

INDUCTION STEP: To prove: $\forall i \in \mathbb{N}$, $P(i) \Rightarrow P(i+1)$

How to proceed?

A natural idea is to split the $2^{i+1} \times 2^{i+1}$ board into 4 boards of dimensions $2^i \times 2^i$ each. However, it is not clear how to proceed from here. For example, suppose $i = 2$.



How to convert this to a covering where exactly one square is left uncovered?

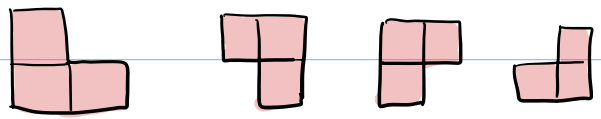
KEY IDEA: STRENGTHEN THE INDUCTION HYPOTHESIS!

Proof: PROOF BY (WEAK) INDUCTION

$Q(n)$:= For all $(x,y) \in [2^n] \times [2^n]$, $2^n \times 2^n$ square board with (x,y) removed can be covered by non-overlapping trominoes.

NOTE: If we prove $\forall n\ Q(n)$, then this proves our claim 5.1.

Base case: $Q(1)$ holds.



removed cell: (2,2) (1,1) (2,1) (1,2)

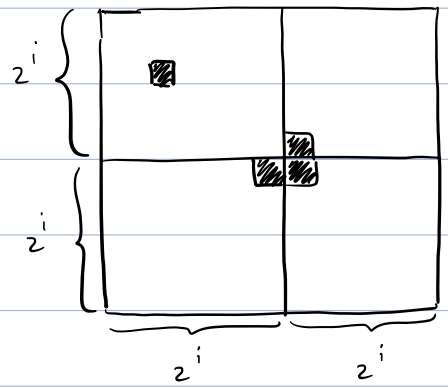
Induction step: To prove: $\forall i \in \mathbb{N},\ Q(i) \Rightarrow Q(i+1)$

$Q(i+1)$: Given any (x,y), the $2^{i+1} \times 2^{i+1}$ square board with (x,y) removed can be covered by non-overlapping trominoes

Case 1: Given (x,y) cell is in top left square.
Case 2: Given (x,y) cell is in bottom left square
Case 3: Given (x,y) cell is in bottom right square.
Case 4: Given (x,y) cell is in bottom right square.

All four cases are symmetric, therefore it suffices

to consider only case 1.



Q(i) states that for any square removed, the $2^i \times 2^i$ board can be covered using trominoes.

For the top left quadrant, invoke Q(i) by removing $(x, y-2^i)$ cell

For the bottom left quadrant, invoke Q(i) by removing top right corner square.

For the bottom right quadrant, invoke Q(i) by removing top left corner square.

For the top right quadrant, invoke Q(i) by removing

Cover the missing part in middle using tromino.

Hence, by induction, we conclude that for all $n \geq 1$, Q(n) holds. Therefore, Claim 5-1 holds.

Example 2 : The (Un) Stacking Game [Sec 5.2.5]

Given : a stack with n boxes.

During the game, at any point, there will be i stacks, $i \in \{1, 2, \ldots, n\}$

You can pick any stack, and convert it into two stacks. Suppose you convert a stack of height h into two stacks of heights a, b where $h = a+b$. Then you get $a \cdot b$ points.

Game ends when there are n stacks, each of height 1.

What should be the strategy to maximize points ?

Claim 5.2 [Thm 5.2.1 of [LLM]] Every way of unstacking n boxes gives $\frac{n \cdot (n-1)}{2}$ points.

Proof : PROOF BY STRONG INDUCTION

Predicate $P(n)$: Every way of unstacking n boxes gives $\frac{n(n-1)}{2}$ pts.

Base case: $n = 1$

There is no unstacking. Hence 0 points possible: $1 \cdot (1-1)/2 = 0$.

Induction Step: Since we are using strong induction, we are assuming $P(1)$, $P(2)$, ..., $P(i)$, and we will prove $P(i+1)$.

Suppose you remove 'a' boxes in first step. Then total pts. is

$a(i+1-a)$ + pts for unstacking ht. 'a'
+ pts for unstacking ht. '$i+1-a$'.

From $P(a)$, we get that second term is $a \cdot \frac{(a-1)}{2}$. From $P(i+1-a)$, we get that third term is $\frac{(i+1-a)(i-a)}{2}$.

Adding them, we get $\frac{(i+1)\,i}{2}$.

Therefore, by strong induction, $P(n)$ holds; the strategy doesn't matter, final score is always $n \cdot (n-1)/2$

BASIC NUMBER THEORY USING (STRONG) MATHEMATICAL INDUCTION

We have seen that every natural number $n > 1$ is either a prime, or can be expressed as product of primes. We will now prove that this decomposition is unique.

A key lemma that's needed for this proof is the following:

Lemma 5.1 For any prime p, and natural numbers $x_1, x_2, \ldots, x_n$ p divides $x_1 \cdot x_2 \cdot \ldots \cdot x_n$, then $\exists i$ s.t. p divides x_i

We will attempt to prove this using strong induction. However, there will be a flaw in the proof. First identify the flaw, then think about how to fix it.

"**Proof**": By STRONG INDUCTION

$\forall x_1, x_2, \ldots, x_n \in \mathbb{N}$, if

Predicate $Q_p(n) :=$ p divides $\underbrace{x_1 \cdot x_2 \cdot \ldots \cdot x_n}_{\text{prod. of } x_1 \ldots x_n}$, then $\exists i \in [n]$ s.t. p divides x_i.

Base case : $n = 1$. ✓

$\forall x_1 \in \mathbb{N}$, if p divides x_1, then $\exists i \in [1]$ s.t. p divides x_i.

Induction step : To prove :

$$\forall n \in \mathbb{N}, \left(Q_p(1) \wedge Q_p(2) \wedge \dots \wedge Q_p(n)\right) \Rightarrow Q_p(n+1)$$

Suppose $Q_p(1)$, $Q_p(2)$, ..., $Q_p(n)$ hold.

Consider any $x_1, \dots, x_n, x_{n+1}$ s.t. p div. $x_1 \cdots x_{n+1}$ (prod. of $x_1, \dots, x_{n+1}$)

Let $y_1 = x_1$ $y_2 = x_2$ ... $y_{n-1} = x_{n-1}$, $y_n = x_n \cdot x_{n+1}$.

Note that p divides $y_1 \cdot y_2 \cdot \dots \cdot y_n$.

Using $Q_p(n)$, we can conclude that $\exists i \in [n]$ s.t. p divides y_i.

If $i < n$, then p divides $y_i = x_i$. We are done.

If $i = n$, then p divides $y_n = x_n \cdot x_{n+1}$.

Using $Q_p(2)$, we conclude that p divides either x_n or x_{n+1}.

Hence $Q_p(2) \wedge Q_p(n) \Rightarrow Q_p(n+1)$.

Using induction, we conclude that $\forall n$, $Q_p(n)$ holds.

Flaw: In the induction step, we need to prove

FOR ALL $n \in \mathbb{N}$, $(Q_p(1) \wedge \dots \wedge Q_p(n)) \Rightarrow Q_p(n+1)$

For $n = 1$, we need to show $Q_p(1) \Rightarrow Q_p(2)$

We proved that $\forall n, (Q_p(2) \wedge Q_p(n) \Rightarrow Q_p(n+1))$

But we have not proven $Q_p(2)$!