Thm (NOT!): All horses are the same color

pf: by induction

P(n): in any set of $n(\geq 1)$ horses, the horses in the set are all the same color.

Basecase: P(1) is true since just one horse.

Inductive step: Assume P(n) to prove P(n+1)   * P(1) ⇒ P(2)?

H_1, H_2

Consider any set of (n+1) horses $H_1, H_2, \cdots, H_n, H_{n+1}$.

H_1 H_2

Then $H_1, \cdots, H_n$ are the same color & $H_2, \cdots, H_{n+1}$ are the same color because they are set of n horses.

becomes empty set H_2

Since color(H_1) = color($H_2, \cdots, H_n$) = color(H_{n+1}) ⇒ all (n+1) are same color. ⇒ P(n+1) □.

⇒ therefore does not work

P(1), P(2) ⇒ P(3), P(3) ⇒ P(4) ⋯ , $\forall n \geq 2$, P(n) ⇒ P(n+1)

P(1) ⇒ P(2) is not true. Let the Basecase be P(2) is true ⇒ Basecase fails.

Thm $\forall n, \exists$ a way to tile a $2^n \times 2^n$ region with a center square missing (for a statue of wealthy donor) using L-shaped tile.

pf. by induction

2. any

P(n): $\exists$ a way to tile a $2^n \times 2^n$ region with a center square missing (for a statue of wealthy donor Bill)

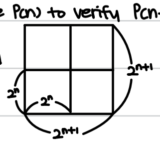
Basecase: P(0), the $2^0 \times 2^0$ region is for Bill.

(stronger)

Inductive Step: For $n \geq 0$, assume P(n) to verify P(n+1) ⇒ hard to proof ⇒ 1. What if we make P(n) harder to proof?

3. P(n) ⇒ P(n+1) because P(n) gives a stronger assumption.

Consider a $2^{n+1} \times 2^{n+1}$ courtyard



Strong Induction

Good proofs are

- correct
- complete
- clear
- brief
- "elegant"
- well-organized
- in-order

Tom Leighton and Marten van Dijk

Top 10 Proof Techniques NOT Allowed in 6.042

10. Proof by throwing in the kitchen sink: The author writes down every theorem or result known to mankind and then adds a few more just for good measure. When questioned later, the author correctly observes that the proof contains all the key facts needed to actually prove the result. Very popular strategy on 6.042 exams. Known to result in extra credit with sufficient whining.

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

8. Proof by vigorous 원기왕성한 **handwaving:** A faculty favorite. Works well in any classroom or seminar setting.

7. Proof by cumbersome 성가신 **notation:** Best done with access to at least four alphabets and special symbols. Helps to speak several foreign languages.

6. Proof by exhaustion: An issue or two of a journal devoted to your proof is useful. Works well in combination with proof by throwing in the kitchen sink and proof by cumbersome notation.

5. Proof by omission 생략**:**

"The reader may easily supply the details."
"The other 253 cases are analogous."
"..."

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

3. Proof by vehement 열정적인 **assertion** 표명**:** It is useful to have some kind of authority in relation to the audience.

2. Proof by appeal to intuition: Cloud-shaped drawings frequently help here. Can be seen on 6.042 exams when there was not time to include a complete proof by throwing in the kitchen sink.

1. Proof by reference to eminent 저명한 **authority:**

"I saw Fermat in the elevator and he said he had a proof . . ."

Here are some other common proof techniques that can be very useful, but which are not recommended for this class.

- **Proof by intimidation:** Can involve phrases such as: "Any moron knows that..." or "You know the Zorac Theorem of Hyperbolic Manifold Theory, right?" Sometimes seen in 6.042 tutorials.
- **Proof by intimidation (alternate form):** Consists of a single word: "Trivial." Often used by faculty who don't know the proof.
- **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. It helps if the issue has not been translated.
- **Proof by semantic shift:** Some standard but inconvenient definitions are changed for the statement of the result.
- **Proof by cosmology:** The negation of the proposition is unimaginable or meaningless. Popular for proofs of the existence of God.
- **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 personal communication:**
  "$x^n + y^n \neq z^n$ for $n > 2$" [Fermat, personal communication].
- **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 mutual reference:** In reference A, Theorem 5 is said to follow from Theorem 3 in reference B, which is shown from Corollary 6.2 in reference C, which is an easy consequence of Theorem 5 in reference A.
- **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 the first.
- **Proof by metaproof:** A method is given to construct the desired proof. The correctness of the method is proved by any of the above techniques.

6.042J / 18.062J Mathematics for Computer Science
Fall 2010

Fermat's last thm

$\forall n \geq 2, \neg\exists\, x, y, z \in \mathbb{N}^+$ (positive natural number) $x^n + y^n = z^n$

Problem: Find a sequence of moves to go from

A	B	C
D	E	F
H	G	

to

A	B	C
D	E	F
H	G	

Legal move: Slide a letter into adjacent blank square

Thm: There is no sequence of legal moves to invert G & H and return all other letters to their original position

Row moves: ex)

A^1	B^2	C^3
D^4	G^5	
E^6	F^7	H^8

⇒

A^1	B^2	C^3
D^4		G^5
E^6	F^7	H^8

Column Moves: ex)

A^1	B^2	C^3
D^4	F^5	
H^6	E^7	G^8

⇒

A^1	B^2	C^3
D^4	F^5	G^6
H^7	E^8	

A^1	B^2	C^3
D^4		G^5
H^6	E^7	F^8

⇒

A^1		C^2
D^3	B^4	G^5
H^6	E^7	F^8

Lemma 1: A row move does not change the order of the items

pf. In a row move, we move an item from some cell i into an adjacent cell $i-1$ or $i+1$. Nothing else moves. Hence the order of item is preserved. □

Lemma 2. A column move changes the relative order of precisely two pairs of items.

pf. In a column move, we move an item in cell i to a blank spot in cell $i-3$ or $i+3$. When an item moves 3 positions, it changes order with 2 items. ($i-1, i-2$ or $i+1, i+2$) □

Def. A pair of letters L_1 & L_2 is an inversion (a.k.a inverted pair) if L_1 precedes L_2 in alphabet but L_1 is after L_2 in puzzle

ex)

A	B	C
F	D	G
E	H	

3 inversions (D, F), (E, F), (E, G)

A	B	C
D	E	F
H	G	

1 inversion

to

A	B	C
D	E	F
H	G	

0 inversion

Lemma 3. During the moves, the # of inversions can only increase by two, decrease by two or stay the same.

pf. Row move: no changes by Lemma 1.

Column move: 2 pairs change order by Lemma 2.

A. Both of pairs were in order → # inversions ↑2

B. Both of pairs were inverted → # inversions ↓2

C. One pair inverted → # inversions stay the same

Corollary 1: During a move, the parity (even or odd) of # inversions does not change.

pf. adding or subtracting 2 does not change parity. □

Lemma 4. In every state reachable from

A	B	C
D	E	F
H	G	

, the parity of # inversions is odd.

pf. By induction.

one inversion: (H, G)

P(n): After any sequence of n moves from

A	B	C
D	E	F
H	G	

, the parity of # inversions is odd.

Basecase: $n=0$, # inversions$=1 \Rightarrow$ parity is odd: $P(0)$

Inductive step: For $n \geq 0$, show $P(n) \Rightarrow P(n+1)$.

Consider any sequence of $n+1$ moves, $M_1, \dots, M_{n+1}$

By I.H $P(n)$ we know that that parity after $M_1, \cdots, M_n$ is odd. By corollary 1, we know parity of # inversions does not change during $M_{n+1} \Rightarrow$ The parity after $M_1, M_2, \cdots, M_n, M_{n+1}$ is odd $\Rightarrow P(n+1)$ □

Pf of thm: The parity of # inversions in desired state is even(0). By Lemma 4, the desired state cannot be reached by legal moves from

A	B	C
D	E	F
H	G	

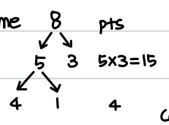
. □

Strong Induction

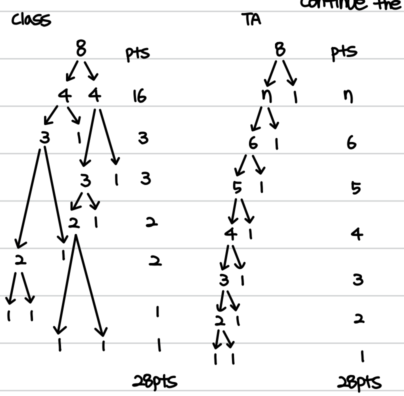
Let $P(n)$ be any predicate. If $P(0)$ is true & $\forall n\ (P(0) \wedge P(1) \wedge \cdots P(n)) \Rightarrow P(n+1)$ is true, then $\forall n\ P(n)$ is true

difference with original induction

ex) Unstacking Game



Continue the procedure and when you reach an end, add up all the points and its your score



Thm: All strategies for the n-block games produce the same score $S(n)$. $= \frac{n(n-1)}{2}$

ex) $S(8) = 28$

pf. By strong induction

I.H: $P(n)$ = All strategies for the n-block games produce the same score $S(n)$.

Basecase: $n=1$, $S(1)=0$ ✓ $S(1) = \frac{1\cdot 0}{2} = 0$

Inductive step: Assume $P(1), P(2) \cdots P(n)$ to prove $P(n+1)$. Look at $n+1$ blocks $n+1$, $1 \le k \le n$

$k \quad n+1-k$

$S(n+1)$

Score $= k(n+1-k) + P(k) + P(n+1-k)$ → depends on k. Need a stronger induction hypothesis.

$$= k(n+1-k) + \frac{k(k-1)}{2} + \frac{(n+1-k)(n+1-k-1)}{2} = \frac{\cancel{2kn} + \cancel{2k} - \cancel{2k^2} + \cancel{k^2} - \cancel{k} + (n+1)n - \cancel{kn} - \cancel{k} - \cancel{kn} + \cancel{k^2}}{2} = \frac{n(n+1)}{2} = S(n). \ \square$$