Proof By Induction

$D := \mathbb{N} := \{0, 1, 2, 3, \ldots\}$ (domain)

$P(x) :=$ "x has property P" (predicate w/ domain D)

Prove: $\forall n\, P(n)$ (P holds for all natural numbers)

Rule of inference: (a new valid argument one may use in such a proof)

$$\frac{\begin{array}{ll} P(0) & \text{base case} \\ \forall k\ P(k) \rightarrow P(k+1) & \text{Inductive Step} \end{array}}{\therefore\ \forall n\, P(n) \quad \text{conclusion}}$$

Remark: $P(k)$ is called the "Inductive Hypothesis" we assume it to be true in order to prove $P(k+1)$

tautology:

$$P(0) \wedge \forall k\ P(k) \rightarrow P(k+1) \rightarrow \forall n\, P(n)$$

proof: Well ordering of $\mathbb{N}$ $\Leftrightarrow$ Induction is Valid

Axiom: $(\mathbb{N}, \leq)$ is **well-ordered**

(i.e. $\emptyset \neq S \subseteq \mathbb{N} \Rightarrow \exists$ smallest element in S)

Axiom $\Rightarrow$ Induction is Valid proof by contradiction

proof: Suppose $P(0) \wedge \forall k\, P(k) \to P(k+1) \wedge \neg \forall n\, P(n)$

$$\neg \forall n\, P(n) \equiv \exists n\, \neg P(n)$$

$S := \{n \in \mathbb{N} \mid \neg P(n)\} \neq \emptyset$ the set of all natural #s failing to have property P

Well-ordering $\Rightarrow \exists x \in S$ s.t. $x \leq y\ \forall y \in S$

i.e. x is the smallest element of S

$\Rightarrow x-1 \notin S \overset{\text{def of } S}{\Longrightarrow} P(x-1)$ is true

$P(x-1) \wedge \forall k\, P(k) \to P(k+1) \Rightarrow P(x)$ true

but $x \in S \overset{\text{def}}{\Longrightarrow} \neg P(x)$ true

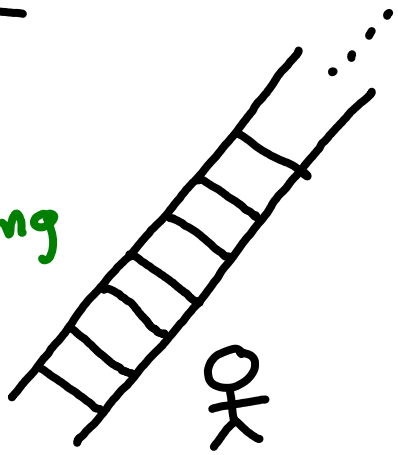
$P(x) \wedge \neg P(x) \equiv F$

we have deduced a contradiction

the other direction (induction $\Rightarrow$ well-ordering) is left as an exercise. we give a hint/potential strategy below. □

2 Truths & 1 Lie

(I) The infinite ladder



We can reach the bottom rung

&

From any given rung we can reach the next rung

$\therefore$ We can reach any rung

(II) Infinite String of Dominos

We can push the first domino over

&

When a domino falls it pushes the next domino over

$\therefore$ Every domino will fall

(III) Every Horse is the Same Color

$P(n) :=$ Every horse in a collection of n horses must be the same color.

$P(1)$ is obviously true. (Base Case)

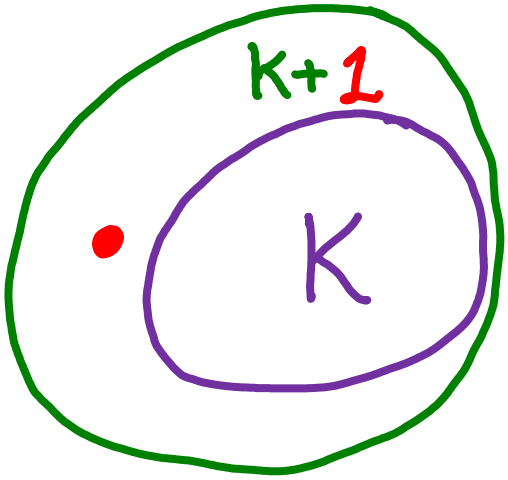
We now provide a "spoof" (invalid proof) that

$\forall k \; P(k) \rightarrow P(k+1)$

Spoof: Suppose $P(k)$ (inductive hypothesis)

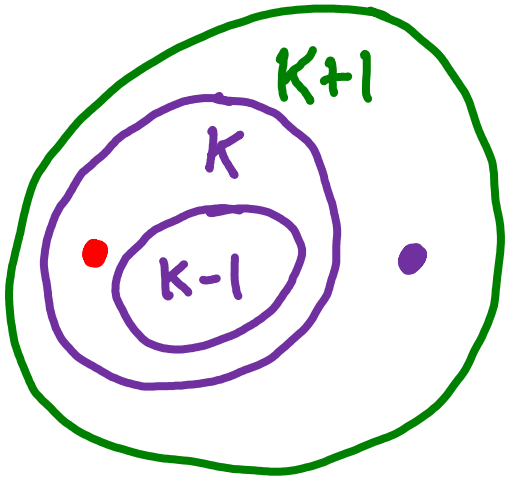
(i.e. Every horse in a collection of k horses must be the same color)

Consider a collection of $k+1$ horses

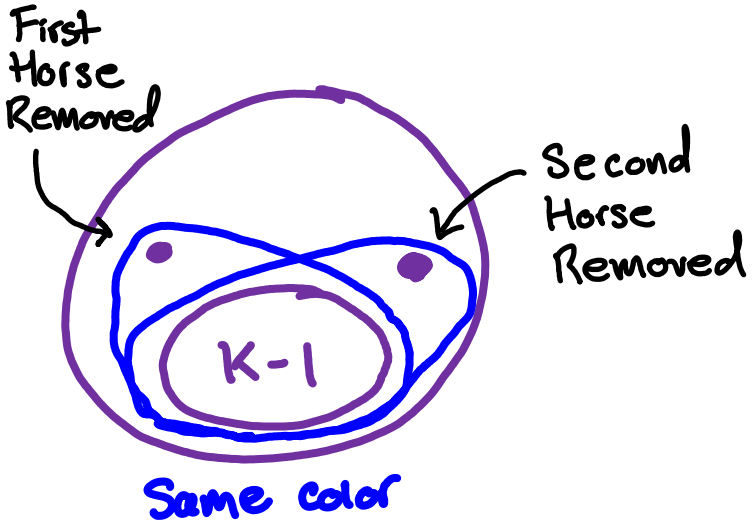


remove 1 horse. The remaining k are all the same color

put this horse back into the collection & remove a different one.



Each of the horses in the collection share the same color by IH



"being the same color" is an equivalence relation on horses. Thus we conclude $\forall k\ P(k) \rightarrow P(k+1)$ by the transitive property.

What's the Problem?

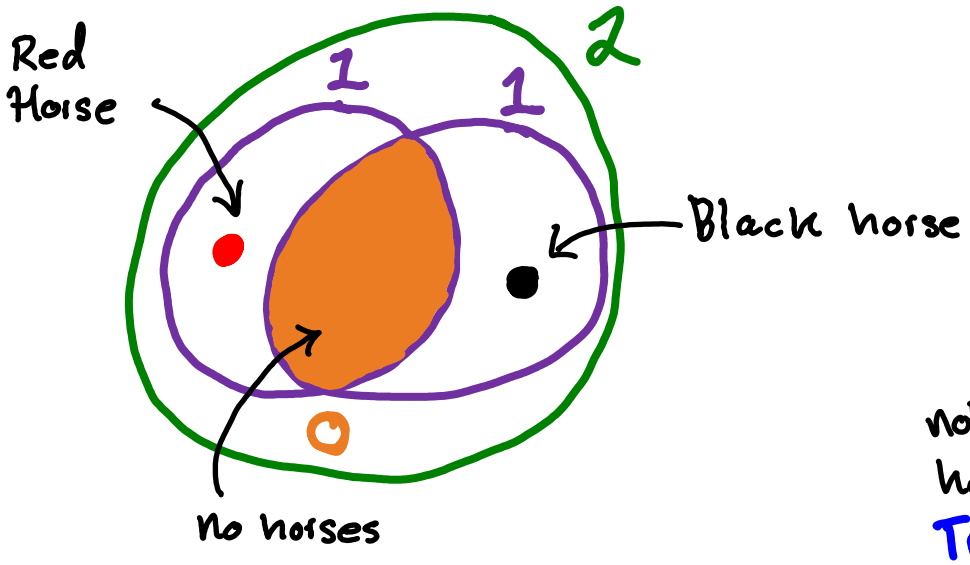
Try Small Examples

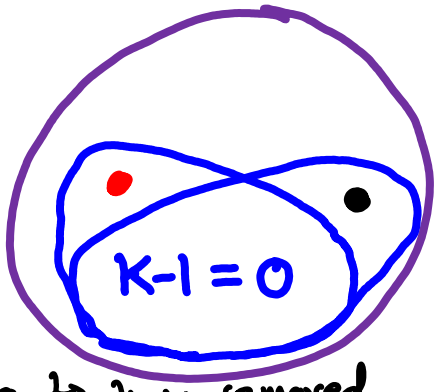
$P(1)$ is indeed definitely true because the relation of "being the same color" is reflexive.

$P(2)$ there are collections of 2 different colored horses.

Our proof above must fail for $P(1) \to P(2)$

(i.e. $K=1$)





nothing to link removed horses w/. Our use of Transitivity requires at least 3 horses!

Remark: The above argument has nothing to do with horses. We could modify it to prove everything is the same color if it were valid.

it can be useful to think about what else you can prove w/ a given argument. If the argument leads to absurd results it is likely invalid.

Induction Cannot Help You Discover New Facts You Must Already Have The Correct Answer Before Writing A (valid) Proof By Induction.

Q: Find A Formula In Terms of n for

$$\sum_{i=1}^{n} i$$

Induction is no help in answering this question

A: To answer this question we actually have to figure out what's going on (unfortunately).

A Very General Problem Solving Strategy

Try Small Examples &
Look For A Pattern

$$\sum_{i=1}^{1} i \quad \sum_{i=1}^{2} i \quad \sum_{i=1}^{3} i \quad \sum_{i=1}^{4} i \quad \cdots \quad \sum_{i=1}^{n-1} i \quad \sum_{i=1}^{n} i \quad \cdots$$

$$1 \quad 1+2 \quad 1+2+3 \quad 1+2+3+4 \quad \cdots \quad a_{n-1} \quad a_n \quad \cdots$$

$+2 \quad +3 \quad +4 \quad +n$

Claim 1: $a_n := \sum_{i=1}^{n} i \Rightarrow a_1 = 1 \;\&\; a_n = a_{n-1} + n$

proof: $a_1 := \sum_{i=1}^{1} i = 1$

$$a_n := \sum_{i=1}^{n} i = \underbrace{1+2+3+\ldots+n-1}_{} + n = \left(\sum_{i=1}^{n-1} i\right) + n$$

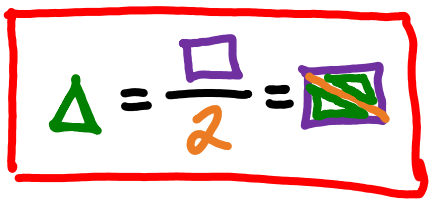
$$=: a_{n-1} + n \qquad \square$$

Claim 2: $a_1 = 1 \;\&\; a_n = a_{n-1} + n \Rightarrow a_n = \frac{n(n+1)}{2}$

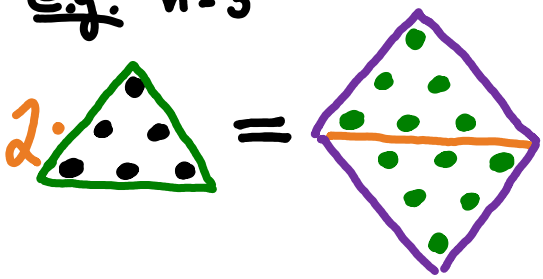
proof: we should be able to provide many proofs of this claim by now, but just in case ...

Recall.

$$\underbrace{\sum_{i=1}^{n} i}_{\text{triangle of dots}} = \frac{\overbrace{n(n+1)}^{\text{rectangle of dots}}}{2}$$



e.g. $n=3$



Q: Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{Z}_{>0}$

Induction is a really useful tool for questions like this

↳ It is of the form $\forall n \; P(n)$

↳ The Correct Formula is Provided

proof: Proof by induction

Let $P(n) := "\sum_{i=1}^{n} i = \frac{n(n+1)}{2}"$

Base Case: We need to show $P(1)$ is true

$$P(1) := "\sum_{i=1}^{1} i = \frac{1(1+1)}{2}"$$

proof: $\sum_{i=1}^{1} i = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1 \cdot (1+1)}{2}$ □

Induction Step: We need to show

$$\forall k \; P(k) \longrightarrow P(k+1)$$

Choose an arbitrary $k \in \mathbb{Z}_{>0}$

prove the conditional $P(k) \rightarrow P(k+1)$ by assuming the **Inductive Hypothesis** (IH) $P(k)$ then deducing $P(k+1)$

★ (Always State Exactly Where You Use The Inductive Hypothesis in a proof (If your proof does not use IH then it is not correct))

proof: $P(k) := "\sum_{i=1}^{k} i = \frac{k(k+1)}{2}"$ (IH)

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + k+1 = \frac{k(k+1)}{2} + (k+1)\frac{2}{2} = \frac{(k+1)(k+2)}{2}$$

$$\overset{\text{def}}{=} P(k+1)$$ □

The Claim $\forall n \; P(n)$ Follows by induction □

Necessary Elements of an Inductive Proof

(i) State the variable you will "induct" on

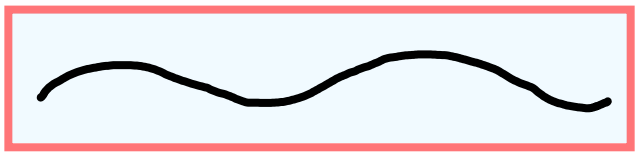
↳ "We prove this claim by induction on x"

(ii) Prove a base case

(iii) State the inductive hypothesis

(iv) Provide a proof of the inductive step & cite the use of the inductive hypothesis

Proof by Induction Template

Theorem: 

Proof: We prove the theorem by induction on _____ (i)

base case: _____ $= 0$ (or _____ $= 1, \ldots$) (ii)

whatever the smallest value of _____ is

Inductive Hypothesis:  (iii)

inductive step:

(iv)

↑ use IH somewhere here

□

Strong Induction

Typical Goal: Prove $\forall n \in \mathbb{N}\ P(n)$

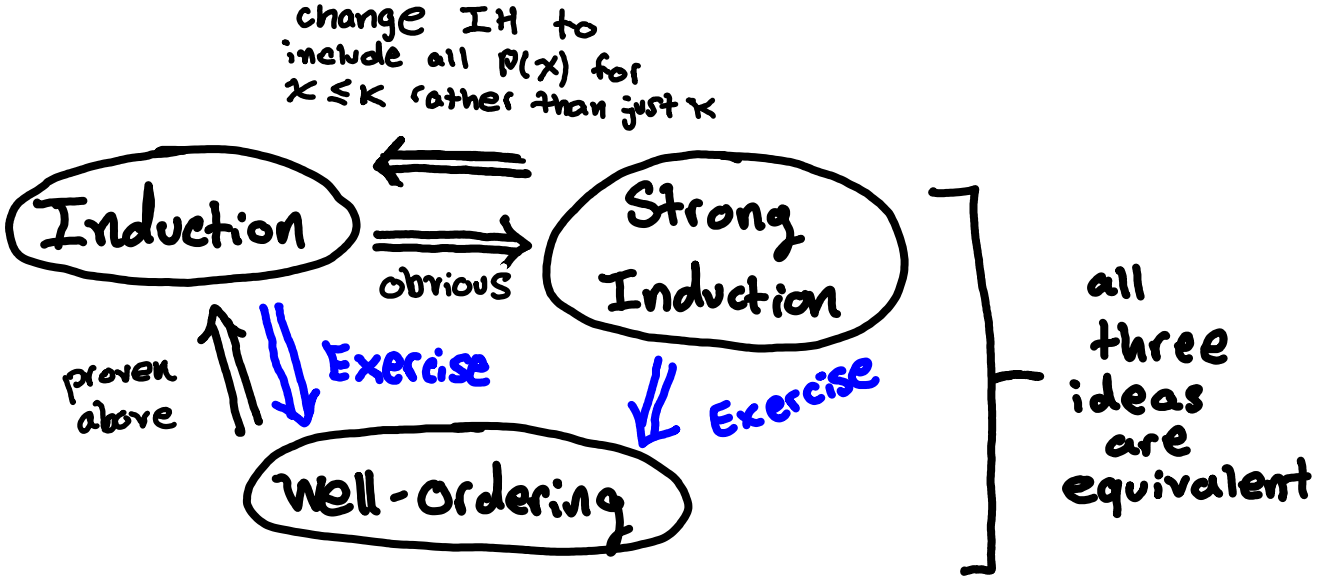
Rule of inference:

$P(0)$ — Same base case as normal induction

$\forall k\ [P(0) \wedge P(1) \wedge \ldots \wedge P(k)] \rightarrow P(k+1)$ — but we give ourselves a stronger assumption (IH) for the inductive step

$\therefore\ \forall n\ P(n)$ — Conclusion

Rather than just leveraging the fact that $P(k)$ is true in order to prove $P(k+1)$ we may use the fact that $P(1), P(2), \ldots, P(k)$ are all true in order to prove $P(k+1)$ This may make it seem as though we might be able to use this form of induction to prove more facts than what induction alone can prove however...



Hence, any proof by Strong induction can be rewritten as a proof by induction & vice versa.

Filling in Some Details

Generalized Addition Rule:

$\{A_i\}_{i=1}^n$ collection of pairwise disjoint, nonempty, finite sets. ($A_i \cap A_j = \emptyset$ for any $i, j \in \{1, \ldots, n\}$)

$$\Rightarrow \left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$$

Generalized Product Rule:

$\{A_i\}_{i=1}^n$ collection of nonempty, finite sets

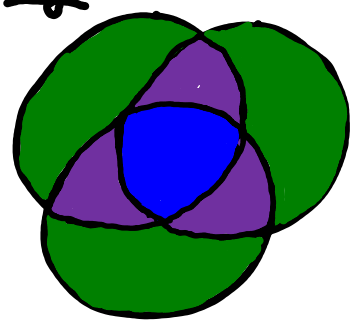
$$\Rightarrow |A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$$

Generalized Inclusion-Exclusion Principle:

$\{A_i\}_{i \in I}$ Collection of nonempty, finite sets indexed by the set $I (\neq \emptyset)$

$$\Rightarrow \left|\bigcup_{i \in I} A_i\right| = \sum_{i \in I} |A_i| + \sum_{\substack{X \in \mathcal{P}(I) \\ |X|>1}} (-1)^{|X|+1} \left|\bigcap_{i \in X} A_i\right|$$

eg.



Counts ■ exactly once

Counts ■ exactly twice

Counts ■ exactly three times

takes out redundant ■ which removes ■ IU

■ gets removed 3 times just need to add $(-1)^4 = 1$ ■ back

Power Rule: $|P(X)| = 2^{|X|}$

Generalized Demorgan: $\forall n \in \mathbb{Z}_{>0}$

$$\neg \bigwedge_{i=1}^{n} P_i \equiv \bigvee_{i=1}^{n} \neg P_i \qquad \left(\bigcap_{i=1}^{n} A_i\right)^c = \bigcup_{i=1}^{n} A_i^c$$

$$\neg \bigvee_{i=1}^{n} P_i \equiv \bigwedge_{i=1}^{n} \neg P_i \qquad \left(\bigcup_{i=1}^{n} A_i\right)^c = \bigcap_{i=1}^{n} A_i^c$$

Correctness of Algorithms:

Checking Truth of "For All Statements"

Input: Finite Domain D, Function $P(-)$ taking $x \in D$
Return Value of P: True xor False

Output: Truth value of $\forall_x P(x)$

```
i = 1
for i ≤ |D|
    if ! P(i) == T
        return F
    i += 1
return T
```

Note: we are implicitly assuming $D \neq \emptyset$

Multiplication is Repeated Addition:

$$a_0 := 0,\ a_n := a_{n-1} + c \implies a_n = n \cdot c$$

Exponents are Repeated Multiplication:

$$a_0 := 1,\ a_n := c\,a_{n-1} \implies a_n = c^n$$

Sum of a Geometric Series: $r \neq 1$

$$\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r-1}$$

Explicit Formula For The N^{th} Fibonacci Number:

$$F_0 := 0,\ F_1 := 1,\ F_N = F_{N-1} + F_{N-2}$$

$$\implies F_N = \frac{\eta^N - (1-\eta)^N}{\sqrt{5}},\quad \eta := \frac{1+\sqrt{5}}{2}$$

Exercise - Prove this by induction & state what kind of induction you used.

Counting & Algorithms

Another example of induction being used to prove something about pseudocode

```
total := 0
For i ≤ N
    For j ≤ M
        total += 1
        j += 1
    i += 1
Return total
```

prove: Value of "total" after the code runs is
= # loop iterations
= $N \cdot M$

Linear/Power Inequality: $\forall n \in \mathbb{N}, \; n < 2^n$

Sum of Binomial Coefficients: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

 # Leaves in Rooted Binary Tree $= 2^{\#\text{ rows}}$

Binomial Theorem: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Power/Factorial Inequality: $2^n < n!, \; n \geq 4$

Factorial/n^n Inequality: $n! < n^n, \; n \geq 2$

Generalized Addition Rule:

$\{A_i\}_{i=1}^n$ collection of pairwise disjoint, nonempty, finite sets. $(A_i \cap A_j = \emptyset$ for any $i, j \in \{1, \ldots, n\})$

$$\Rightarrow \left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$$

proof: induction on n

base case: $n=1$ $\quad \{A_i\}_{i=1}^{1} = \{A_1\}$

in this case, $\bigcup_{i=1}^{1} A_i = A_1$ so the formula degenerates to

$|A_1| = |A_1|$ which is clearly true.

IH: $\{A_i\}_{i=1}^{k}$ collection of pairwise disjoint, nonempty finite sets $\Rightarrow \left|\bigcup_{i=1}^{k} A_i\right| = \sum_{i=1}^{k} |A_i|$

Induction Step: $n = k+1$

note $\quad A_{k+1} \cap \left(\bigcup_{i=1}^{k} A_i\right) = \emptyset$ $\quad$ so

$$\left|\bigcup_{i=1}^{k+1} A_i\right| = |A_{k+1}| + \left|\bigcup_{i=1}^{k} A_i\right| \overset{IH}{=} |A_{k+1}| + \sum_{i=1}^{k} |A_i|$$

$$= \sum_{i=1}^{k+1} |A_{k+1}| \quad \square$$

Recall: $\forall$ finite sets A, B we have

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Generalized Product Rule:

$\{A_i\}_{i=1}^n$ collection of nonempty, finite sets

$$\Rightarrow |A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$$

proof: Exercise □

Generalized Inclusion-Exclusion Principle:

$\{A_i\}_{i \in I}$ Collection of nonempty, finite sets indexed by the set $I (\neq \emptyset)$

$$\Rightarrow \left| \bigcup_{i \in I} A_i \right| = \sum_{\substack{X \in P(I) \\ X \neq \emptyset}} (-1)^{|X|+1} \left| \bigcap_{i \in X} A_i \right|$$

proof: We induct on $|I|$

base case: $|I| = 1$ $\quad |A_1| = |A_1|$ ✓

IH: the formula from the statement above is true for any collection $\{A_i\}_{i \in I}$ where $|I| = K$

Induction Step: $J := I \cup \{j\}$ where $|I| = K$

$$\left| \bigcup_{i \in J} A_i \right| = |A_j \cup (\bigcup_{i \in I} A_i)| = |A_j| + \left| \bigcup_{i \in I} A_i \right| - |A_j \cap (\bigcup_{i \in I} A_i)|$$

$$= |A_j| + \sum_{\substack{X \in P(I) \\ \emptyset \neq X}} (-1)^{|X|+1} \left| \bigcap_{i \in I} A_i \right| - \underbrace{\left| \bigcup_{i \in I} (A_j \cap A_i) \right|}_{|I| = K \text{ so we can use IH again}}$$

$$= |A_j| + \sum_{\substack{X \in P(I) \\ \emptyset \neq X}} (-1)^{|X|+1} \left| \bigcap_{i \in I} A_i \right| - \sum_{\substack{X \in P(I) \\ \emptyset \neq X}} (-1)^{|X|+1} \left| \bigcap_{i \in X} (A_j \cap A_i) \right|$$

all intersections involving indices from I

all intersections involving the index j (with an extra negative so the signs are correct)

$$= \sum_{\substack{X \in P(J) \\ \emptyset \neq X}} (-1)^{|X|+1} \left| \bigcap_{i \in X} A_i \right| \quad \square$$

power Rule: $|P(X)| = 2^{|X|}$

proof: induct on $|X|$

base case: $|X| = 0 \Rightarrow X = \emptyset \quad P(\emptyset) = \{\emptyset\}$

So $|P(X)| = 1 = 2^0 = 2^{|X|}$

Inductive Hypothesis: $|X| = k \Rightarrow |P(X)| = 2^{|X|}$

inductive step: $Y := X \cup \{y\}$

$|P(Y)| = |P(X)| + |\{Z \subseteq Y \mid y \in Z\}|$ ← Subsets containing the new element

$= 2^{|X|} + |\{Z \subseteq Y \mid Z = \{y\} \cup W, W \in P(X)\}|$

the new element together w/ a subset of the old set

$= 2^{|X|} + 2^{|X|} = 2 \cdot 2^{|X|} = 2^{|X|+1} = 2^{|Y|}$ $\square$

Generalized Demorgan: $\forall n \in \mathbb{Z}_{>0}$

(I) $\neg \bigwedge_{i=1}^{n} P_i \equiv \bigvee_{i=1}^{n} \neg P_i$

(II) $\left(\bigcup_{i=1}^{n} A_i \right)^c = \bigcap_{i=1}^{n} A_i^c$

proof of (I): induct on n

base case. $n=1$ $\quad \neg P_1 \equiv \neg P_1$ ✓

Inductive Hypothesis: $\neg \bigwedge_{i=1}^{k} P_i \equiv \bigvee_{i=1}^{k} \neg P$

inductive step: $\neg \bigwedge_{i=1}^{k+1} P_i \equiv \neg \left(P_{k+1} \wedge \left(\bigwedge_{i=1}^{k} P_i \right) \right)$

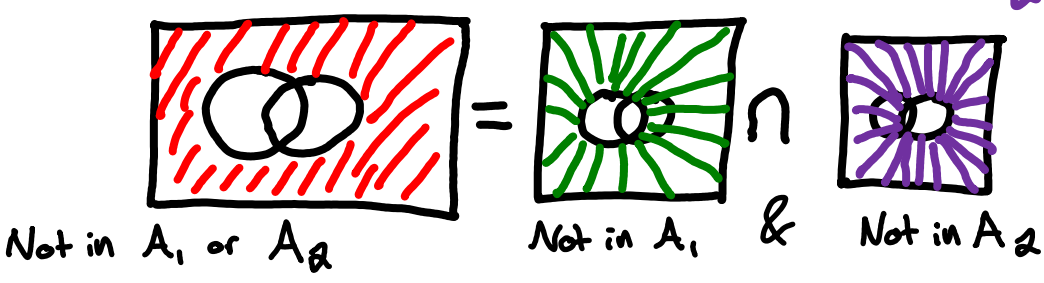
$\equiv$ (De Morgan's Law) $\neg P_{k+1} \vee \neg \bigwedge_{i=1}^{k} P_i \equiv \neg P_{k+1} \vee \left(\bigvee_{i=1}^{k} \neg P_i \right)$

$\equiv \bigvee_{i=1}^{k+1} \neg P_i$ $\quad \square$

proof of (II): induct on n

base case: $n=1$ obvious

$n=2$ $\quad (A_1 \cup A_2)^c = A_1^c \cap A_2^c$



Inductive Hypothesis: $\left(\bigcup_{i=1}^{k} A_i\right)^c = \bigcap_{i=1}^{k} A_i^c$

inductive step:

$$\left(\bigcup_{i=1}^{k+1} A_i\right)^c = \left(A_{k+1} \cup \left(\bigcup_{i=1}^{k} A_i\right)\right)^c \overset{n=2 \text{ case above}}{=} A_{k+1}^c \cap \left(\bigcup_{i=1}^{k} A_i\right)^c$$

$$= A_{k+1}^c \cap \left(\bigcap_{i=1}^{k} A_i^c\right) = \bigcap_{i=1}^{k+1} A_i^c \qquad \square$$

Multiplication is Repeated Addition:

$$a_0 := 0,\ a_n := a_{n-1} + c \implies a_n = n \cdot c$$

proof: induct on n

base case: $n = 0$ $\quad a_0 = 0 = 0 \cdot c$ ✓

IH: $a_k = kc$

inductive step: $a_{k+1} = a_k + c = kc + c = c(k+1)$ $\square$

Exponents are Repeated Multiplication:

$$a_0 := 1,\ a_n := c\,a_{n-1} \implies a_n = c^n$$

proof: **base case:** $n = 0$ $\quad a_0 = 1 = c^0$

IH: $a_k = c^k$

inductive step: $a_{k+1} = c a_k = c\,c^k = c^{k+1}$ $\square$

Sum of a Geometric Series: $r \neq 1$

$$\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r-1}$$

proof: induct on n

base case: $n=0$ $\quad a = \frac{ar-a}{r-1} = \frac{a(r-1)}{r-1} = a$ ✓

IH: $\sum_{j=0}^{k} ar^j = \frac{ar^{k+1}-a}{r-1}$

inductive step:

$$\sum_{j=0}^{k+1} ar^j = ar^{k+1} + \sum_{j=0}^{k} ar^j = ar^{k+1} + \frac{ar^{k+1}-a}{r-1}$$

$$= \frac{ar^{k+1}(r-1)}{r-1} + \frac{ar^{k+1}-a}{r-1} = \frac{ar^{k+2} - ar^{k+1} + ar^{k+1} - a}{r-1}$$

$$= \frac{ar^{k+2}-a}{r-1}$$

□

Sum of Binomial Coefficients: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

proof: induct on n

base case: $n=0$ $\quad \binom{0}{0} = \frac{0!}{0!(0-0)!} = \frac{1}{1 \cdot 1} = 1 = 2^0$ ✓

IH: $\sum_{k=0}^{m} \binom{m}{k} = 2^m$,

inductive step: $\sum_{k=0}^{m+1} \binom{m+1}{k} = \sum_{k=0}^{m} \binom{m}{k} + \sum_{k=1}^{m+1} \binom{m}{k-1}$

$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ Pascal's Identity

change of variables: let $j = k-1$

$= \sum_{k=0}^{m} \binom{m}{k} + \sum_{j=0}^{m} \binom{m}{j} = 2\sum_{k=0}^{m} \binom{m}{k} = 2 \cdot 2^m = 2^{m+1}$ □

j is just a dummy variable

Binomial Theorem: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

proof:

base case: $n = 0$

$(x+y)^0 = 1 = 1 \cdot 1 \cdot 1 = \binom{n}{0} \cdot x^0 \cdot y^{0-0} = \sum_{k=0}^{0} \binom{n}{k} x^k y^{n-k}$

IH: $(x+y)^m = \sum_{k=0}^{m} \binom{m}{k} x^k y^{m-k}$

Inductive Step: $(x+y)^{m+1} = (x+y)(x+y)^m$

$$= (x+y)\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k}$$

$$= x\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} + y\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k}$$

$$= \underbrace{\sum_{k=0}^{m}\binom{m}{k}x^{k+1} y^{m-k}} + \underbrace{\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k+1}}$$

We need to combine like terms

Consider the term $x^k y^{m-(k-1)}$ from the first sum

it has coefficient $\binom{m}{k-1}$

looking @ the same term $x^k y^{m-k+1}$ from the second sum we see a coefficient of $\binom{m}{k}$

$\Rightarrow$ Coeff of $x^k y^{m-k+1}$ after combining is

$$\binom{m}{k-1}+\binom{m}{k} = \binom{m+1}{k}$$

↑ Pascal's Identity

Hence, first sum + Second sum $= \sum_{k=0}^{m+1}\binom{m+1}{k}x^k y^{m+1-k}$

□

Linear/Power Inequality: $\forall n \in \mathbb{N},\ n < 2^n$

proof:

base case: $n=0$ $\quad 0 < 1 = 2^0$ ✓

IH: $k < 2^k$

inductive step:

$$k+1 < 2^k + 1 < 2 \cdot 2^k = 2^{k+1}$$

↑ because $2^k \geq 1$ thus $2^k + 2^k = 2 \cdot 2^k \geq 1+1 = 2$ □

Power/Factorial Inequality: $2^n < n!,\ n \geq 4$

proof:

base case: $n=4$

$$2^4 = 16 < 24 = 4!$$ ✓

IH: $2^k < k!$

inductive step:

$$2^{k+1} = 2\,2^k < 2 \cdot k! < (k+1) \cdot k! = (k+1)!$$

↑ because $2 < k+1$ $(k \geq 4)$ □

Factorial / n^n Inequality: $n! < n^n, \quad n \geq 2$

proof:

base case. $n=2$

$$2! = 2 < 4 = 2^2 \quad \checkmark$$

IH: $k! < k^k$

inductive step:

$$(k+1)! = (k+1)k! < (k+1)k^k < (k+1)^{k+1}$$ □

An Example of Strong Induction

Fundamental Theorem of Arithmetic:

$\forall n \in \mathbb{N} \setminus \{0,1\}$ $\exists!$ factorization of n into ≥ 1 prime(s)

proof: base case: $n=2$ Since 2 is prime & all other primes are strictly larger than 2 it follows that it is uniquely expressed as a product of 1 prime.

IH: We assume the claim is true for all $2 \leq k \leq m$

inductive step: Now consider the natural number $m+1$

Case: $m+1$ is prime $m+1$ is then a product of 1 prime & (by def) has no divisors other than 1 & itself $\Rightarrow$ this factorization is unique

Case: $m+1$ is composite

$\Leftrightarrow$ $m+1 = ab$ $\Rightarrow$ $2 \leq a \leq b < m+1$ (no loss in generality assuming this)

Each of a & b are $< m+1$ so by **IH** they factor uniquely into a product of ≥ 1 prime(s). Let p be the smallest prime factor appearing in either factorization.

$p \mid m+1 \Rightarrow m+1 = pM$ where $2 \leq M < m+1$

IH Since M factors uniquely into ≥ 1 prime(s) & p is the smallest prime dividing $m+1$ we know the prime factorization for $m+1$ is unique. □

Notice the subtlety in this argument. It would not suffice to appeal to the uniqueness of the prime factorizations of a & b since $m+1$ may admit a factorization of the form $m+1 = c \cdot d$ for some pair of natural numbers c & d such that both $a \neq c \neq b$ & $a \neq d \neq b$. Of course, by the inductive hypothesis, these numbers have unique factorizations too, and what guarantee do we have that the prime factors of a & b bear any relation to those of c & d? Indeed, this is exactly what makes the fact that any factor tree of a ⁂ terminates in the same set of primes @ their leaves so surprising.

Conclusion

Induction is a powerful tool for proving (even complicated) statements that have a very particular form. Indeed, many of the facts we established before now (avoiding the use of induction) have much simpler/shorter proofs with this method, but it is not entirely void of drawbacks, for instance, it does not always provide the most enlightening proof & it cannot be used to discover facts it can only be used to prove them or verify a "lucky" guess.