Today's topics

- Induction

- Reading: Sections 3.3
- Upcoming
  - More Induction

§3.3: Mathematical Induction

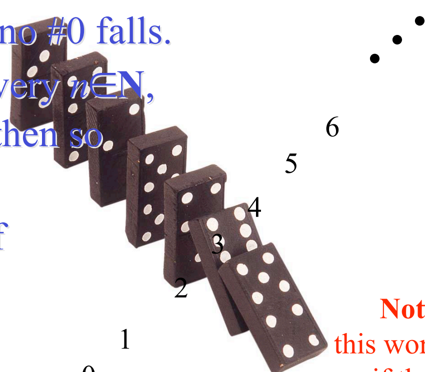
- A powerful, rigorous technique for proving that a predicate $P(n)$ is true for *every* natural number n, no matter how large.
- Essentially a "domino effect" principle.
- Based on a predicate-logic inference rule:

$$\begin{array}{l} P(0) \\ \forall n \geq 0\ (P(n) \rightarrow P(n+1)) \\ \hline \therefore \forall n \geq 0\ P(n) \end{array}$$

"The First Principle of Mathematical Induction"

The "Domino Effect"

- **Premise #1:** Domino #0 falls.
- **Premise #2:** For every $n \in \mathbb{N}$, if domino #n falls, then so does domino #$n+1$.
- **Conclusion:** All of the dominoes fall down!



Note: this works even if there are infinitely many dominoes!

Validity of Induction

Proof that $\forall k \geq 0\ P(k)$ is a valid consequent:
Given any $k \geq 0$, the 2nd antecedent $\forall n \geq 0\ (P(n) \rightarrow P(n+1))$ trivially implies that $\forall n \geq 0\ (n<k) \rightarrow (P(n) \rightarrow P(n+1))$, *i.e.*, that $(P(0) \rightarrow P(1)) \wedge (P(1) \rightarrow P(2)) \wedge \ldots \wedge (P(k-1) \rightarrow P(k))$. Repeatedly applying the hypothetical syllogism rule to adjacent implications in this list $k-1$ times then gives us $P(0) \rightarrow P(k)$; which together with $P(0)$ (antecedent #1) and *modus ponens* gives us $P(k)$. Thus $\forall k \geq 0\ P(k)$. ■

The Well-Ordering Property

- Another way to prove the validity of the inductive inference rule is by using the *well-ordering property*, which says that:
  - Every non-empty set of non-negative integers has a minimum (smallest) element.
  - $\forall\ \emptyset \subset S \subseteq \mathbf{N} : \exists m \in S : \forall n \in S : m \leq n$
- This implies that $\{n | \neg P(n)\}$ (if non-empty) has a min. element m, but then the assumption that $P(m-1) \rightarrow P((m-1)+1)$ would be contradicted.

Outline of an Inductive Proof

- Let us say we want to prove $\forall n\ P(n)$…
  - Do the *base case* (or *basis step*): Prove $P(0)$.
  - Do the *inductive step*: Prove $\forall n\ P(n) \rightarrow P(n+1)$.
    - *E.g.* you could use a direct proof, as follows:
    - Let $n \in \mathbf{N}$, assume $P(n)$. (*inductive hypothesis*)
    - Now, under this assumption, prove $P(n+1)$.
  - The inductive inference rule then gives us $\forall n\ P(n)$.

Generalizing Induction

- Rule can also be used to prove $\forall n \geq c\ P(n)$ for a given constant $c \in \mathbf{Z}$, where maybe $c \neq 0$.
  - In this circumstance, the base case is to prove $P(c)$ rather than $P(0)$, and the inductive step is to prove $\forall n \geq c\ (P(n) \rightarrow P(n+1))$.
- Induction can also be used to prove $\forall n \geq c\ P(a_n)$ for any arbitrary series $\{a_n\}$.
- Can reduce these to the form already shown.

Second Principle of Induction

A.k.a. "Strong Induction"

- Characterized by another inference rule:

  $P(0)$

  $\forall n \geq 0: (\underbrace{\forall 0 \leq k \leq n\ P(k)}_{P \text{ is true in } all \text{ previous cases}}) \rightarrow P(n+1)$

  $\therefore \forall n \geq 0: P(n)$
- The only difference between this and the 1st principle is that:
  - the inductive step here makes use of the stronger hypothesis that $P(k)$ is true for *all* smaller numbers $k<n+1$, not just for $k=n$.

Induction Example (1st princ.)

- Prove that the sum of the first n odd positive integers is n^2. That is, prove:

$$\forall n \geq 1: \underbrace{\sum_{i=1}^{n} (2i-1) = n^2}_{P(n)}$$

- Proof by induction.
  - Base case: Let n=1. The sum of the first 1 odd positive integer is 1 which equals 1^2. (Cont…)

Example cont.

- Inductive step: Prove $\forall n \geq 1: P(n) \rightarrow P(n+1)$.
  - Let $n \geq 1$, assume $P(n)$, and prove $P(n+1)$.

$$\sum_{i=1}^{n+1} (2i-1) = \left(\sum_{i=1}^{n} (2i-1) \right) + (2(n+1)-1)$$
$$= n^2 + 2n + 1$$
$$= (n+1)^2$$

By inductive hypothesis P(n)

Problem

- Show for all natural numbers n
  - $(n^3 - n)$ is divisible by 3

Another Induction Example

- Prove that $\forall n>0, n<2^n$. Let $P(n)=(n<2^n)$
  - Base case: $P(1)=(1<2^1)=(1<2)=\mathbf{T}$.
  - Inductive step: For $n>0$, prove $P(n)\rightarrow P(n+1)$.
    - Assuming $n<2^n$, prove $n+1 < 2^{n+1}$.
    - Note $n + 1 < 2^n + 1$ (by inductive hypothesis)
      $< 2^n + 2^n$ (because $1<2=2\cdot 2^0 \leq 2\cdot 2^{n-1}= 2^n$)
      $= 2^{n+1}$
    - So $n + 1 < 2^{n+1}$, and we're done.

Example of Second Principle

- Show that every $n>1$ can be written as a product $\prod p_i = p_1 p_2 \ldots p_s$ of some series of s prime numbers.
  - Let $P(n)$="n has that property"
- **Base case:** $n=2$, let $s=1$, $p_1=2$.
- **Inductive step:** Let $n\geq 2$. Assume $\forall 2\leq k\leq n$: $P(k)$. Consider $n+1$. If it's prime, let $s=1$, $p_1=n+1$. Else $n+1=ab$, where $1<a\leq n$ and $1<b\leq n$. Then $a=p_1p_2\ldots p_t$ and $b=q_1q_2\ldots q_u$. Then we have that $n+1 = p_1p_2\ldots p_t\, q_1q_2\ldots q_u$, a product of $s=t+u$ primes.

Another 2nd Principle Example

- Prove that every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps. $P(n)$="n can be…"
- **Base case:** $12=3(4)$, $13=2(4)+1(5)$, $14=1(4)+2(5)$, $15=3(5)$, so $\forall 12\leq n\leq 15$, $P(n)$.
- **Inductive step:** Let $n\geq 15$, assume $\forall 12\leq k\leq n\ P(k)$. Note $12\leq n-3\leq n$, so $P(n-3)$, so add a 4-cent stamp to get postage for $n+1$.

The Method of Infinite Descent

- A way to prove that $P(n)$ is false for all $n\in\mathbf{N}$.
- Sort of a converse to the principle of induction.
- Prove first that $\forall P(n)$: $\exists k<n$: $P(k)$.
  - Basically, "For every P there is a smaller P."
- But by the well-ordering property of **N**, we know that $\exists P(m) \rightarrow \exists P(n)$: $\forall P(k)$: $n\leq k$.
  - Basically, "If there is a P, there is a smallest P."
- Note that these are contradictory unless $\neg\exists P(m)$,
  - that is, $\forall m\in\mathbf{N}$: $\neg P(m)$. There is no P.

Infinite Descent Example

- **Theorem:** $2^{1/2}$ is irrational.
- **Proof:** Suppose $2^{1/2}$ is rational, then $\exists m,n\in\mathbf{Z}^+$: $2^{1/2}=m/n$. Let M,N be the m,n with the least n.

$$\sqrt{2} = \frac{M}{N} \therefore 2 = \frac{M^2}{N^2} \therefore 2N^2 = M^2.$$

$$\frac{2N-M}{M-N} = \frac{(2N-M)N}{(M-N)N} = \frac{2N^2-MN}{(M-N)N} = \frac{M^2-MN}{(M-N)N} = \frac{(M-N)M}{(M-N)N} = \frac{M}{N}$$

$$1<\sqrt{2}<2 \therefore 1<\frac{M}{N}<2 \therefore N<M<2N \therefore 0<M-N<N$$

So $\exists k<N, j$: $2^{1/2} = j/k$ (let $j=2N-M$, $k=M-N$). ■