# Introduction to Decision Sciences

## Lecture 9

Andrew Nobel

October 10, 2017

# Consequences of Bezout's Theorem

**Corollary:** Suppose $a, b, c \in \mathbb{N}_+$. If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$

**Proposition:** If $p$ is prime and $p \mid a_1 \cdots a_n$ then $p$ divides some $a_i$.

**Fact:** If $p$ is prime and $0 < k < p$ then $p \mid \binom{p}{k}$

**FTA (Uniqueness):** Suppose that $n \geq 1$ and $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are primes such that

$$n \; = \; p_1 \cdots p_r \; = \; q_1 \cdots q_s.$$

Then $r = s$ and $q_1, \ldots, q_r$ is just a rearrangement of $p_1, \ldots, p_r$.

# Mathematical Induction

# Overview of Mathematical Induction

**Given:** Propositional function $P(n)$ with domain $\mathbb{N}_+ = \{1, 2, \ldots\}$

**Induction:** Proof strategy to establish that $P(n)$ is true for every $n$

Mathematical basis of induction is the *well ordering property*, an axiom of the natural numbers $\mathbb{N}_+$ that states

- Every non-empty set $S \subseteq \mathbb{N}_+$ has a smallest element

# Mathematical Induction

**Given:** Propositional function $P(n)$ with domain $\mathbb{N}_+$

**Basis step:** Show that $P(1)$ is true

**Inductive step:** Show that $P(k) \to P(k+1)$ is true for every $k \geq 1$

- assume that $P(k)$ is true "inductive hypothesis"
- establish that $P(k+1)$ is true

**Conclusion:** $P(n)$ is true for every $n \in \mathbb{N}_+$

We can view induction as a (new) rule of inference, namely,

$$[P(1) \land \forall k \, (P(k) \to P(k+1))] \; \to \; \forall n \, P(n)$$

# Validity of Induction

**Informal:** Ladder/Dominos

- $P(1)$ is true by Basis step
- $P(1) \rightarrow P(2)$ is true by Inductive step, so $P(2)$ is true
- $P(2) \rightarrow P(3)$ is true by Inductive step, so $P(3)$ is true
- $P(3) \rightarrow P(4)$ is true by Inductive step, so $P(4)$ is true
- and so on...

**Conclude:** $P(n)$ is true for every $n$

# Validity of Induction

**Formal:** Suppose that basis and inductive steps hold but $\forall n\, P(n)$ is F

- Then $S = \{n : P(n)$ is F$\}$ is non-empty
- By well-ordering, $S$ has smallest element $m$
- By Basis step, $P(1)$ is true so $m \geq 2$
- Definition of $S$ implies $P(m-1)$ is T and we know $m - 1 \geq 1$
- Inductive step then implies $P(m)$ is T, a contradiction
- Conclude that $\forall n\, P(n)$ is T

# Examples

**Example 1:** Sum of first $n$ odd integers is $n^2$. To show: $\forall n\, P(n)$, where

$$P(n) \text{ is } 1 + 3 + \cdots + (2n-1) = n^2$$

**Example 2:** Sum of first $n$ perfect squares. To show $\forall n\, P(n)$, where

$$P(n) \text{ is } 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

**Example 3:** If $n \geq 1$ is odd then $8 \mid n^2 - 1$. To show: $\forall m \geq 0\ P(m)$, where

$$P(m) \text{ is } 8 \mid (2m+1)^2 - 1$$

# Fermat's Little Theorem

**Theorem:** If $p$ is prime and $r \geq 0$ then $p \mid r^p - r \quad (*)$

**Binomial Theorem:** For all $a, b \in \mathbb{R}$ and $n \geq 0$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

# Harmonic Numbers

**Definition:** The $n$th harmonic number is the sum

$$H_m = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m}$$

**Fact:** For each $n \geq 0$, $H_{2^n} \geq 1 + n/2$

**Corollaries:**

- $H_n$ tends to infinity as $n$ tends to infinity
- $H_n \geq 1 + \lfloor \log_2 n \rfloor / 2$ for each $n \geq 1$

**Theorem:** $H_n - \ln n \to \gamma = .577...$ (Euler's constant) as $n \to \infty$

# Induction with a Stronger Inductive Hypothesis.

**Given:** Propositional function $P(n)$ with domain $\mathbb{N}_+$.

**Basis step:** Show that $P(1)$ is T

**Inductive step:** Show that $P(1) \wedge \cdots \wedge P(k) \rightarrow P(k+1)$ is T for each $k \geq 1$.

- assume that $P(1) \wedge \cdots \wedge P(k)$ is T "strong inductive hypothesis"
- establish that $P(k+1)$ is true

**Conclusion:** $P(n)$ is true for every $n \in \mathbb{N}_+$

We can view strong induction as a (new) rule of inference

$$[P(1) \wedge \forall k\, (P(1) \wedge \cdots \wedge P(k) \rightarrow P(k+1))] \rightarrow \forall n\, P(n)$$

Formal validity of strong induction follows from well-ordering principle.

# Ex. Prime Factorization

**Thm:** Every integer $n \geq 2$ can be written as a product of primes.

**Proof:** Strong induction. Propositional function: for $n \geq 2$ let

$$P(n) = n \text{ can be written as a product of primes}$$

**Basis:** $P(2)$ is true as $2$ is prime.

**Induction:** Suppose that $P(2), P(3), \ldots, P(k)$ are true.

- *Case 1:* Suppose $k+1$ is prime
- *Case 2:* Suppose $k+1$ is composite.

# Ex. Piles of Stones

**Given:** Pile of $n \geq 2$ stones

- split pile into two piles of size $r, s \geq 1$ with $r + s = n$
- compute product $rs$ of pile sizes
- continue splitting piles into smaller ones until every pile has one stone

**Claim:** No matter how piles split, sum of products $rs$ over splits is $n(n-1)/2$

**Proof:** Strong induction. Propositional function: for $n \geq 2$ let

$$P(n) = \text{ starting with } n \text{ stones, sum of products is } n(n-1)/2$$

**Basis:** Consider $P(2)$

**Induction:** Suppose that $P(2), P(3), \ldots, P(k)$ are T.

# Basics of Counting

# Product Rule

**Product Rule:** Suppose that the elements of a collection $S$ can be specified by a sequence of $k$ steps such that

- There are $n_j$ possibilities at step $j$
- The selections made at steps $1, \ldots, j$ do not affect the *number* of possibilities at step $j+1$

Then $S$ has $n_1 \cdot n_2 \cdots n_k$ elements.

**Example:** Cartesian product of sets $A_1, \ldots, A_k$ is

$$A_1 \times \cdots \times A_k \;=\; \{(a_1, \ldots, a_k) : a_1 \in A_1, \ldots, a_k \in A_k\}$$

By product rule $|A_1 \times \cdots \times A_k| \;=\; |A_1| \cdots |A_k|$

# Example: Counting Functions

**Given:** Finite sets $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$.

**Qu 1:** What is the number of functions $f : A \to B$?

**Qu 2:** What is the number of one-to-one functions $f : A \to B$?

**Qu 3:** What is the number of onto functions $f : A \to B$?

# Indicator Functions

**Definition:** The indicator function of a proposition $q$ is given by

$$I(q) = \begin{cases} 1 & \text{if } q \text{ is true} \\ 0 & \text{if } q \text{ is false} \end{cases}$$

**Example:** Find $|2^S|$ for $S = \{s_1, \ldots, s_n\}$ finite

Define function $f : 2^S \to \{0,1\}^n$ from subsets of $S$ to binary $n$-tuples by

$$f(A) \ = \ (I(s_1 \in A), I(s_2 \in A), \ldots, I(s_n \in A))$$

Can check that $f()$ is one-to-one and onto, so

$$|2^S| \ = \ |\{0,1\}^n| \ = \ 2^n \ = \ 2^{|S|}$$

# Sum Rule

**Sum Rule:** S'pose that each element of a collection $S$ is one of $k$ types, and

- There are $n_j$ elements of type $j$
- No element can be of more than one type.

Then $|S| = n_1 + \cdots + n_k$.

**Equivalent Form:** If $S = A_1 \cup \cdots \cup A_k$ where $A_i \cap A_j$ for $i \neq j$ then $|S| = |A_1| + \cdots + |A_k|$.

**Example:** How many binary sequences $b$ of length $6$ begin with $01$ or $001$?