Induction and recursion

Principle 8.1.1 Let $m \in \mathbb{Z}$. To prove that $\forall n \in \mathbb{Z}_{\geq m}\ P(n)$ is true, where $P(n)$ is a proposition, then it suffices to:

(base step) show that $P(m)$ is true; and

(induction step) show that $\forall k \in \mathbb{Z}_{\geq m}, P(k) \Rightarrow P(k+1)$.

Principle 8.2.1 Let $m \in \mathbb{Z}$. To prove that $\forall n \in \mathbb{Z}_{\geq m}\ P(n)$ is true, where $P(n)$ is a proposition, then it suffices to choos some $l \in \mathbb{Z}_{\geq 0}$ and:

(base step) show that $P(m), P(m+1), \cdots, P(m+l-1)$ is true; and

(induction step) show that $\forall k \in \mathbb{Z}_{\geq 0}$,

$$P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+l-1+k) \Rightarrow P(m+l+k)$$

is true.

Theorem 8.2.10 (Well-Ordering Principle). Every non-empty subset of $\mathbb{Z}_{\geq m}$, where $m \in \mathbb{Z}$, has a smallest element.

Rough idea 8.4.5 A recursive definition of a set S consists of three types of clauses.

(base clause) Specify that certain elements, called founders, are in S: if c is a founder, then $c \in S$.

(recursion clause) Specify certain functions, called constructors, under which the set S is closed: if f is a constructor and $x \in S$, then $f(x) \in S$.

(minimality clause) Membership for S can always be demonstrated by (finitely many) successive applications of the clauses above.

Rough idea 8.4.6 (structural induction). Let S be a recursively defined set. To prove that $\forall x \in S \quad P(x)$ is true, where $P(x)$ is a proposition, it suffices to:

(base step) show that $P(c)$ is true for every founder c; and

(induction step) show that $\forall x \in S, P(x) \Rightarrow P(f(x))$ is true for every constructor f.

Functions

Definition 7.2.1 Let A, B be sets. A function from A to B is an assignment to each element of A exactly one element of B. Suppose $f : A \to B$.

1. Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to. $f(x)$ is the image of x under f.
2. A is the domain of f, and B is the codomain of f.

Definition 9.1.3 Let A be a set. A string or word over A is an expression of the form

$$a_0 a_1 \cdots a_{l-1}$$

where $l \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \cdots, a_{l-1} \in A$. l is the length of the string. A^* is the set of all strings over A. The empty string, denoted ε is the string of length 0.

Definition 9.1.6 Two functions $f : A \to B$ and $g : C \to D$ are equal if

1. $A = C$ and $B = D$; and
2. $f(x) = g(x)$ for all $x \in A$.

Definition 9.3.1 Let $f : A \to B$.

1. If $X \subseteq A$, then $f(X) = \{f(x) : x \in X\}$
2. If $Y \subseteq B$, then $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$

$f(X)$ is the setwise image of X. $f^{-1}(Y)$ is the setwise preimage of Y under f.

Definition 9.3.6 Let $f : A \to B$.

1. f is surjective or onto if
$$\forall y \in B \quad \exists x \in A \quad (y = f(x))$$
2. f is injective or one-to-one if
$$\forall x_1, x_2 \in A \quad (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$$
3. f is bijective if it is both surjective and injective, i.e.,
$$\forall y \in B \quad \exists! x \in A \quad (y = f(x))$$

Proposition 9.3.17 (uniqueness of inverses). If g_1, g_2 are inverses of $f : A \to B$, then $g_1 = g_2$.

Theorem 9.3.19 A function $f : A \to B$ is bijective if and only if it has an inverse.

Remark $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$

Cardinality

Theorem 10.1.1 (Pigeonhole Principle). Let A and B be finite sets. If there is an injection $f : A \to B$, then $|A| \leq |B|$.

Theorem 10.1.2 (Dual Pigeonhole Principle). Let A and B be finite sets. If there is a surjection $f : A \to B$, then $|A| \geq |B|$.

Theorem 10.1.3 Let A and B be finite sets. Then there is a bijection $A \to B$ if and only if $|A| = |B|$.

Definition 10.2.1 (Cantor). A set A is said to have the same cardinality as a set B is there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

Countability

Definition 10.3.1 (Cantor). A set is countable if it is finite, or it has the same cardinality as $\mathbb{Z}_{\geq 0}$.

Note 10.3.4 An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots \in B$ in which every element of B appears exactly once.

Lemma 10.3.5 An infinite set B is countable if and only if there is a sequence $c_0, c_1, c_2, \cdots$ in which every element of B appears. There could be repeats, there could be elements not in B.

Proposition 10.3.6 Any subset A of a countable set B is countable.

Proposition 10.3.7 Every infinite set B has a countable infinite subset.

Propoisition 10.4.1 Let A, B be countable infinite sets. Then $A \cup B$ is countable.

Theorem 10.4.2 $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is countable.

Theorem 10.4.3 (Cantor 1891). Let A be a countable infinite set. Then $\mathcal{P}(A)$ is not countable.

Remark Removing finitely many elements from an infinite set still leaves an infinite set.

Counting

Theorem 9.1.1 If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

Theorem 9.2.3 If n and r are integers and $1 \leq r \leq n$, then the number of r-permutations of a set with n elements is given by

$$P(n, r) = n(n-1) \cdots (n-r+1) = \frac{n!}{(n-r)!}$$

Theorem 9.3.1 Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \cdots, A_k$. Then

$$|A| = |A_1| + |A_2| + \cdots + |A_k|$$

Theorem 9.3.2 If A is a finite set and $B \subseteq A$, then

$$|A \setminus B| = |A| - |B|$$

Theorem 9.3.3 If A, B, C are finite sets, then

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

and

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

Pigeonhole Principle A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.

Generalized Pigeonhole Principle For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $k < n/m$, then there is some $y \in Y$ such that y is the image of at least $k+1$ distinct elements of X.

Generalized Pigeonhole Principle (Contrapositive) For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(y)$ has at most k elements, then X has at most km elements; in other words, $n \leq km$.

Theorem 9.5.1 The number of subsets of size r (or r-combinations) that can be chosen from a set of n elements is given by

$$\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$$

Theorem 9.5.2 Suppose a collection consists of n objects of which n_i are of type i, and are indistinguishable from each other, for integers $1 \leq i \leq k$. Then the number of distinguishable permutations of the n objects is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}$$

Theorem 9.6.1 The number of r-combination with repetition allowed (multisets of size r) that can be selected from a set of n elements is:

$$\binom{r+n-1}{r}$$

Theorem 9.7.1 Let n and r be positive integers, $r \leq n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Theorem 9.7.2 Given any real numbers a and b and any non-negative integer n,

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

Probability

Probability Axioms Let S be a sample space. A probability function P from the set of all events in S to the set of real numbers satisfies the following axioms: For all events A and B in S,

1. $0 \leq P(A) \leq 1$
2. $P(\varnothing) = 0$ and $P(S) = 1$
3. If A and B are disjoint, then $P(A \cup B) = P(A) + P(B)$

Probability of Complement If A is any event in a sample space S, then $P(A') = 1 - P(A)$.

Probability of Union If A and B are any events in a sample space S, then $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Expected Value Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, \cdots, a_n$, which occur with probabilities $p_1, p_2, \cdots, p_n$. The expected value of the process is

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + \cdots + a_n p_n$$

Linearity For random variables X and Y, and for scalars a, b,

$$E[aX + bY] = aE[X] + bE[Y]$$

Conditional Prob. Let A and B be events in a sample space S. If $P(A) \neq 0$, then the conditional probability of B given A is

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)}$$

Theorem 9.9.1 (Bayes' Theorem). Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, \cdots, B_n$. Suppose A is an event in S, and suppose $P(A), P(B_1), P(B_2), \cdots, P(B_n)$ are all non-zero. If k is an integer with $1 \leq k \leq n$, then

$$P(B_k \mid A) = \frac{P(A \mid B_k) \cdot P(B_k)}{P(A \mid B_1) \cdot P(B_1) + \cdots + P(A \mid B_n) \cdot P(B_n)}$$

Independent Events If A and B are events in a sample space S, then A and B are independent, if and only if,

$$P(A \cap B) = P(A) \cdot P(B)$$

Pairwise and Mutual Independence Let A, B and C be events in a sample space S. A, B and C are pairwise independent if and only if conditions 1-3 are fulfilled. A, B and C are mutually independent if and only if all conditions are fulfilled.

1. $P(A \cap B) = P(A) \cdot P(B)$
2. $P(A \cap C) = P(A) \cdot P(C)$
3. $P(B \cap C) = P(B) \cdot P(C)$
4. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

Graphs (additional)

Adjacency Matrix

1. Sum along row of adjacency matrix is the number of outgoing edges.
2. Sum along column of adjacency matrix is the number of incoming edges.

Eulerian circuit In the Eulerian circuit, each edge in the graph is taken once, but can revisit vertices.

Hamiltonian circuit In the Hamiltonian circuit, each vertex in the graph is visited once. Any complete graph with at least 2 vertices has a Hamiltonian circuit.

Pre- and in-order

1. The leftmost element in the pre-order is the root, let it be V.
2. Find V in the in-order. Everything to the left of V will be in the left subtree of V, and vice versa for the right.

In- and post-order

1. The rightmost element in the post-order is the root, let it be V.
2. Find V in the in-order. Everything to the left of V will be in the left subtree of V, and vice versa for the right.

Pre- and post-order (Full Binary Tree only)

1. The leftmost element in the pre-order is the root, let it be V.
2. The second element is the left child of the root, let it be C.
3. Find C in the post-order. Everything to the left of C will be in the left subtree of V. Everything to the right of C is in the right subtree of V.

Misc (unproved)

Inverse Relation R^{-1} is an equivalence relation if and only if R is an equivalence relation.

Distributivity of $\times$ Set $\times$ is distributive over $\cap$ and $\cup$.

Subset of partial order A subset of a partial order is also anti-symmetric.