Discrete Structures

Class: CSCI 2824

Boolean algebra

Boolean Identity's

DeMorgan Laws	$\neg(a \vee b) \equiv \neg a \wedge \neg b$
	$\neg(a \wedge b) \equiv \neg a \vee \neg b$
	$\neg \forall x\ \beta(x) \equiv \exists x\ \neg \beta(x)$
	$\neg \exists x\ \beta(x) \equiv \forall x\ \neg \beta(x)$
Distributivity	$a \wedge (b \vee c) \equiv (a \wedge b) \vee (a \wedge c)$
	$a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$
Elimination	$a \wedge T \equiv a$
	$a \wedge F \equiv F$
	$a \vee F \equiv a$
	$a \vee T \equiv T$

Implications and equivalence Identity

Proof

Naive Set's Theory

Definitions

Union	$a \cup b = \{x \in U \mid x \in a \vee x \in b\}$
Intersection	$a \cap b = \{x \in U \mid x \in a \wedge x \in b\}$
Difference	$A - B = A \cap \overline{B} = \{x \mid x \in A \wedge x \notin B\}$
Cartesian Product	$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$
	$A_1 \times ... \times A_n$
	$= \{(a_1 \times ... \times a_n) \mid a_i \in A_i \text{ for } i = 1, ..., n\}$
	$\{a, b\} \times \{0, 1\} = \{(a, 0), (a, 1), (b, 0), (b, 1)\}$
Power Set	The power set $\wp(E)$ is the set of all sub sets of E.
Intervals	$[a, b] = \{x \mid a \leq x \leq b\}$
	$(a, b) = \{x \mid a < x < b\}$
Proper subset	$A \subset B$
	$= \forall x(x \in A \to x \in B) \wedge \exists x(x \in B \wedge x \notin A)$
Subsets	$A \subseteq B = \forall x(x \in A \to x \in B)$
A disjoint B.	$A \cap B = \emptyset$

The sets A and B are equal if $A \subseteq B$ and $B \subseteq A$.

Let S be a set. If there are exactly n distinct elements in S where n is a non negative integer, we say that S is a *finite* set and that n is the cardinality($|S|$) of S.

Identities

Identity	$A \cap U = A$
	$A \cup \emptyset = A$
Domination laws	$A \cup U = U$
	$A \cap \emptyset = \emptyset$
Idempotent laws	$A \cap A = A$
	$A \cup A = A$
Complementation law	$\overline{(\overline{A})} = A$
Commutative law	$A \cap B = B \cap A$
	$A \cup B = B \cup A$

Modular Arithmetic

a is divisebla by b	$a \mid b$
a congruent to b	$b \equiv a (\text{mod } N)$
a congruent to b	$a \equiv b (\text{mod } N)$

Counting

Discrete Probability's

Definition

S is the a finite nonempty sample space of equally likely outcomes, and $E \subseteq S$, the the probabilitie of E is $p(E) = \frac{|E|}{|S|}$.

Some Probability Theorems

$p(\overline{E}) = 1 - p(E)$

$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$

Theorems

Theorem 1 *For every set S, $\emptyset \subseteq S$ and $S \subseteq S$.*

Theorem 2 *Consider $f : \mathbb{Z} \to \mathbb{R}$ and $g : \mathbb{Z} \to \mathbb{R}$*
We say $f(x)$ is $\mathcal{O}(g(x))$ if there exist constants C and k such that $|f(x)| \leq C|g(x)|$ whenever $x > k$.

Theorem 3 (Def modulo) *Let $m \in \mathbb{Z}^+$. $a \equiv b (mod\, m)$ if and only if $\exists k(a = b + km)$. Where a and b are $\mathbb{Z}$*

Theorem 4 (Fermat little thm) $a^{p-1} \equiv 1 (mod\, p)$

Theorem 5 *Let m be a positive integer. If $a \equiv b (mod\, m)$ and $c \equiv d (mod\, m)$, then $b + d \equiv b + d (mod\, m)$ and $bd \equiv bd (mod\, m)$.*