CS 2742 (Logic in Computer Science) – Fall 2008
Lecture 17

Antonina Kolokolova

November 10, 2008

Definition 1. *A Boolean algebra is a set B together with two operations, generally denoted $+$ and $\cdot$, such taht for all a and b in B both $a + b$ and $a \cdot b$ are in B and the following properties hold:*

- *Commutative laws:* $a + b = b + a$ *and* $a \cdot b = b \cdot a$.
- *Associative laws:* $(a + b) + c = a + (b + c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *Distributive laws:* $(a + b) \cdot c = a \cdot c + b \cdot c$ *and* $a \cdot b + c = (a + b) \cdot (a + c)$ *(recall that the second one does not hold for the normal arithmetic $+$ and $\cdot$).*
- *Identity laws:* $a + 0 = a$ *and* $a \cdot 1 = a$
- *Complement laws: for each a there exists an element called negation of a and denoted $\bar{a}$ such that* $a + \bar{a} = 1$, $a \cdot \bar{a} = 0$.

Proofs in Boolean algebra:

Example 1 (Idempotent identity)**.** Show that $a + a = a$.

$$\begin{aligned}
a &= a + 0 && \text{because 0 is the identity for } + \\
&= a + (a \cdot \bar{a}) && \text{by the complement law for } \cdot \\
&= (a + a) \cdot (a + \bar{a}) && \text{by the distributive law} \\
&= (a + a) \cdot 1 && \text{by the complement law for } + \\
&= a + a && \text{because 1 is the identity for } +
\end{aligned}$$

5.1 Power set and diagonalization

A *power set* of a set A, denoted 2^A, is a set of all subsets of A. For example, if $A = \{1, 2, 3\}$ then $2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$.

Let $|A|$ denote the number of elements of A (also called *cardinality*, especially when talking about infinite sets.) The size of the power set, as notation suggests, is $2^|A|$.

Theorem 1. *Let A be a finite set. Then the cardinality of 2^A is $2^|A|$.*

Proof. Suppose A has n elements. Now, every subset S of A can be represented by a binary string of length n, which would have a 1 in the positions corresponding to an element in S, and a 0 in places corresponding to elements not in S. For example, if $A = \{1, 2, 3\}$ as above, then $S\{1, 3\}$ is represented by a string 101, and $\emptyset$ is represented by a string 000. Now, the number of binary strings of length n is 2^n. Therefore, the number of possible subsets of A (and thus the elements of 2^A) is also 2^n. $\square$

What if A is infinite? Still the size of the powerset (called *cardinality* in this context) will be larger. The proof is by diagonalization argument.

Halting problem for Java programs. Remember Russell's paradox:

$A = \{x \mid x \notin A\}$.

Let CheckHalt be an algorithm such that CheckHalt(M,x) prints "halts" if M terminates on input x, and "loops" if M does not terminate. Let $Diag(X) = \neg CheckHalt(X, X)$. Such a $Diag(X)$ gives a paradox.

Another way of proving it is using a technique called Diagonalization, due to Cantor. But to present this we need some more definitions first.