CS280, Spring 2001	Handout 37
April 27, 2001	

1. Reading: K. Rosen *Discrete Mathematics and Its Applications*, 9.1, 9.2
2. The main message of this lecture:

> **Truth values 0(*FALSE*) and 1(*TRUE*) together with the Boolean operations on them constitute a mathematical structure, called "Boolean algebra".**

Definition 37.1. A **Boolean algebra** is a set B containing at least two distinct elements 0 and 1, and having one unary operation $\overline{}$ (complement) and two binary operations $\vee$ (called: disjunction, **sup**, the least upper bound *lub*, Boolean addition) and $\wedge$ (called: conjunction, **inf**, the greatest lower bound *glb*, Boolean multiplication) satisfying the following properties

$x \vee 0 = x$ $x \wedge 1 = x$	Identity Laws	$x \vee \overline{x} = 1$ $x \wedge \overline{x} = 0$	Domination Laws
$(x \vee y) \vee z = x \vee (y \vee z)$ $(x \wedge y) \wedge z = x \wedge (y \wedge z)$	Associative Laws	$x \vee y = y \vee x$ $x \wedge y = y \wedge x$	Commutative Laws

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$
Distributive Laws

The distributivity property for the usual algebraic expressions is $a \cdot (b + c) = a \cdot b + a \cdot c$. Note that for Boolean algebras not only multiplication distributes through addition, but also vice versa.

Example 37.2. The minimal Boolean algebra is the 2-element Boolean algebra: $B = \{0, 1\}$ with operations: Boolean complement $\overline{0} = 1$, $\overline{1} = 0$

Boolean addition (as $\vee$) $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1 + 1 = 1$

Boolean multiplication (as $\wedge$) $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$.

Example 37.3. The 4-element Boolean algebra: $B = P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Here $0 = \emptyset$, $1 = \{a, b\}$, $x \vee y = x \cup y$ (union), $x \wedge y = x \cap y$ (intersection), $\overline{x} = \{a, b\} - x$ (complement).

Theorem 37.4. *For any Boolean algebra and any elements x,y in it:*

1. $x \vee x = x$, $x \wedge x = x$
2. *if* $x \vee y = 1$ *and* $x \wedge y = 0$, *then* $y = \overline{x}$
3. $\overline{0} = 1$, $\overline{1} = 0$
4. $\overline{\overline{x}} = x$
5. *de Morgan Laws: a)* $\overline{(x \vee y)} = \overline{x} \wedge \overline{y}$, *b)* $\overline{(x \wedge y)} = \overline{x} \vee \overline{y}$.

Proof. 1. $x \vee x = (x \vee x) \wedge 1 = (x \vee x) \wedge (x \vee \overline{x}) =$ (by distributivity) $= x \vee (x \wedge \overline{x}) = x \vee 0 = x$, $x \wedge x = (x \wedge x) \vee 0 = (x \wedge x) \vee (x \wedge \overline{x}) =$ (by distributivity) $= x \wedge (x \vee \overline{x}) = x \wedge 1 = x$

2. Suppose $x \vee y = 1$ and $x \wedge y = 0$. Multiply $\overline{x}$ by both parts of the former and add $\overline{x}$ to both parts of the latter: $\overline{x} \wedge (x \vee y) = \overline{x} \wedge 1 = \overline{x}$, $\overline{x} \vee (x \wedge y) = \overline{x} \vee 0 = \overline{x}$. By distributivity, $(\overline{x} \wedge x) \vee (\overline{x} \wedge y) = 0 \vee (\overline{x} \wedge y) = \overline{x} \wedge y$, $(\overline{x} \vee x) \wedge (\overline{x} \vee y) = 1 \wedge (\overline{x} \vee y) = \overline{x} \vee y$, thus $\overline{x} \wedge y = \overline{x}$ and $\overline{x} \vee y = \overline{x}$. Plug this expression for $\overline{x}$ to $\overline{x} \vee y = \overline{x}$: $(\overline{x} \vee y) \wedge y = \overline{x}$. Therefore $(y \vee \overline{x}) \wedge (y \vee 0) = \overline{x}$. By distributivity, $y \vee (\overline{x} \wedge 0) = \overline{x}$, thus $y \vee 0 = \overline{x}$ and $y = \overline{x}$.

3. By identity and commutativity, $0 \vee 1 = 1$ and $0 \wedge 1 = 0$. By 2, $1 = \overline{0}$. Likewise, $0 = \overline{1}$.

4. By domination, $x \vee \overline{x} = 1$ and $x \wedge \overline{x} = 0$. By commutativity, $\overline{x} \vee x = 1$ and $\overline{x} \wedge x = 0$. By 2 (with x as y), $x = \overline{\overline{x}}$.

5a. Let $u = \overline{x} \wedge \overline{y}$. By 2, it suffices to show that $(x \vee y) \vee u = 1$ and $(x \vee y) \wedge u = 0$. Indeed, $(x \vee y) \vee u = (x \vee y) \vee (\overline{x} \wedge \overline{y}) = x \vee [y \vee (\overline{x} \wedge \overline{y})] = x \vee [(y \vee \overline{x}) \wedge (y \vee \overline{y})] = x \vee [(y \vee \overline{x}) \wedge 1] = x \vee (y \vee \overline{x}) = x \vee (\overline{x} \vee y) = (x \vee \overline{x}) \vee y = 1 \vee y = 1$. 5b is similar to 5a.

Example 37.5. There is no 3-element boolean algebra. Indeed, suppose $B = \{0, 1, \alpha\}$. Take $\overline{\alpha}$. Then there are three possibilities $\overline{\alpha} = 0$, $\overline{\alpha} = 1$, or $\overline{\alpha} = \alpha$. In the first case $\alpha = \overline{\overline{\alpha}} = \overline{0} = 1$. In the second case $\alpha = \overline{\overline{\alpha}} = \overline{1} = 0$. In the third case $\alpha = \alpha \vee \alpha = \alpha \vee \overline{\alpha} = 1$ (Likewise, one can show that $\alpha = 0$. This consideration demonstrates that no boolean algebra has self-dual elements, i.e. such x's that $x = \overline{x}$).

Theorem 37.6. *Each finite Boolean algebra is isomorphic to the power set $P(X)$ with set theoretical operations for an appropriate finite set X.*
Proof. Yet another bonus problem.

Definition 37.7. A **Boolean function of degree** n is a function from $\{0,1\}^n$ to $\{0,1\}$.

As we know, there are 2^{2^n} Boolean functions of degree n.

Definition 37.8. **Boolean expressions** in the variables $x_1, x_2, \ldots, x_n$ are defined recursively as follows:

$0, 1, x_1, x_2, \ldots, x_n$ are Boolean expressions

if U and V are Boolean expressions, then $\overline{U}$, $(U \cdot V)$ and $(U + V)$ are Boolean expressions. As usual, we will freely use variables other then $x_1, x_2, \ldots, x_n$, and omit "$\cdot$" and excessive parentheses whenever unambiguous. Examples of Boolean expressions: $1 + x\overline{y}$, $xyz + \overline{x}$.

Definition 37.9. The **dual** of a Boolean expression is obtained by interchanging sums and products and interchanging 0 and 1. For example, the dual of $x\overline{y} + 1$ is $(x + \overline{y}) \cdot 0$ Duality principle: the Boolean identity remains valid when both sides are replaced by their duals.

Each Boolean expression in the variables $x_1, x_2, \ldots, x_n$ represents a Boolean function of degree n. The converse is also true.

Theorem 37.10. (Functional completeness of Boolean expressions) *Every Boolean function can be represented as a Boolean expression*
Proof. Good old Disjunctive Normal Forms (a.k.a. **sum-of-products expansion** and Conjunctive Normal Form (a.k.a. **product-of-sums expansion**) from lecture 1.

Example 37.11. Let $f(1,0,1) = f(0,0,1) = 1$ and $f(x,y,z) = 0$ for all other triples (x,y,z). To find a Boolean expression for f we first build **minterms**, i.e. products of variables or their complements for the triples of arguments where f is equal to 1: $x\overline{y}z$ and $\overline{x}\overline{y}z$. Each of those midterms is 1 only on the corresponding triple of arguments. Finally, the desired expression is the sum of midterms: $f(x,y,z) = x\overline{y}z + \overline{x}\overline{y}z$.

Example 37.12. Let now $f(1,0,1) = f(0,0,1) = 0$ and $f(x,y,z) = 1$ for all other triples (x,y,z). Since there are less 0's then 1's among the values of f, we'd better use the product-of-sums expansion. We build **maxterms** for each row that gives value 0: $\overline{x} + y + \overline{z}$ and $x + y + \overline{z}$. Maxterms give 0's only in those rows. Then we take the product of the maxterms: $f(x,y,z) = (\overline{x} + y + \overline{z})(x + y + \overline{z})$.

Homework assignments. (The second installment due Friday 05/04) 37A:Rosen9.1-6; 37B:Rosen9.1-20cd; 37C:Rosen9.2-4cd(sum-of-products and product-of-sums).