Lecture 3

“Laws” of computation

Common algebraic properties of basic operations

- operations? Think “addition” and “multiplication”

- laws: commutativity and associativity

- these laws applicable to union and intersection

“Laws” of computation

Common algebraic properties of basic operations

- **operations? Think “addition” and “multiplication”**
- **when you just multiply or add multiple numbers, it does not matter how you group them**
- **the order does not matter either**

- **Definition.** Operation $\Box$ ($x \Box y$, e.g. $x \cdot y$, *or* $x + y$) is ***<u>associative</u>*** if

$$x \Box y \Box z = (x \Box y) \Box z = x \Box (y \Box z)$$

"Laws" of computation

Common algebraic properties of basic operations

- **operations? Think "addition" and "multiplication"**
- **when you just multiply or add multiple numbers, it does not matter how you group them**
- **the order does not matter either**

- **Definition.** Operation $\square$ ($x \square y$, e.g. $x \cdot y$, *or* $x + y$) is ***associative*** if

$$x \square y \square z = (x \square y) \square z = x \square (y \square z)$$

- **Definition.** Operation $\square$ is ***commutative*** if

$$x \square y = y \square x \text{ (for all x,y)}$$

Examples

operation which is associative but not commutative?

operation which is not commutative but is associative?

Examples 1

- **commutative but not associative:**
  - ***averaging*: $a \diamond b := (a + b)/2$**
  - **NAND!**
- **associative but not commutative:**
  - ***matrix multiplication*,**
  - "last argument"
  - **function composition**

$$(1 \diamond 2) \diamond 3 = \frac{3/2 + 3}{2} = \frac{9}{4}$$

$$1 \diamond (2 \diamond 3) = 1 \diamond \frac{5}{2} = \frac{1 + \frac{5}{2}}{2} = \frac{7}{4}$$

Examples 2

- **commutative but not associative:**
  - ***averaging***: $a \diamond b := (a+b)/2$
  - **NAND!**
- **associative but not commutative:**
  - ***matrix multiplication***
  - "last argument" $:= \quad L(a,b) = b \iff a \llcorner b = b$
  - **function composition**

$$1 \llcorner 2 \llcorner 3 = (1 \llcorner 2) \llcorner 3 = 2 \llcorner 3 = 3$$
$$= 1 \llcorner (2 \llcorner 3) = 1 \llcorner 3 = 3$$
ASSOCIATIVE

$$2 \llcorner 3 = 3$$
$$3 \llcorner 2 = 2$$
NOT COMMUTATIVE

Question:

- **Union, intersection, set difference, symmetric difference**
- **Associative? Commutative?**

Union, intersection,

Yup

Question:

- **Union, intersection, set difference, symmetric difference**
- **Associative? Commutative?**

Set difference?

Nope

$A - B \neq B - A$ (choose $B = \emptyset$

$A - (B - C) \neq (A - B) - C$ (choose $B = C = A$

$A - \emptyset = A$

$\emptyset - C = \emptyset$

Question:

- **Union, intersection, set difference, symmetric difference**
- **Associative? Commutative?**

Symmetric difference

Yup.

Distributivity

- how two operations and groupings interact

  - $10 \cdot (5 + 7) = 10 \cdot 13 = 130$
  - $10 \cdot (5 + 7) = 10 \cdot 5 + 10 \cdot 7 = 50 + 70 = 130$

  "Multiplication is distributive over addition"

- **question: is addition distributive over multiplication?**

Distributivity

- **how two operations and groupings interact**

- $10 \cdot (5 + 7) = 10 \cdot 13 = 130$
- $10 \cdot (5 + 7) = 10 \cdot 5 + 10 \cdot 7 = 50 + 70 = 130$

“Multiplication is distributive over addition”

- **question: is addition distributive over multiplication?**

$$10 + (5 \cdot 7) = 350$$

$$10 + (5 \cdot 7) \neq (10 + 5) \cdot (10 + 7) = 15 \cdot 17 = 255$$

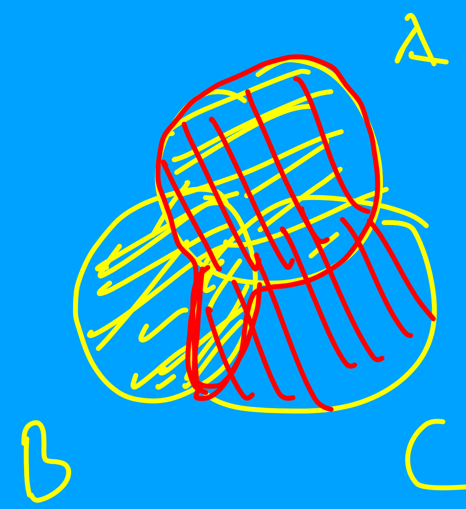
Distributivity of set operations

Theorem. Intersection (union) is distributive over the union (intersection), i.e,

for all sets A, B, C it holds that:

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Let's do one using Venn



= $A \cup B$

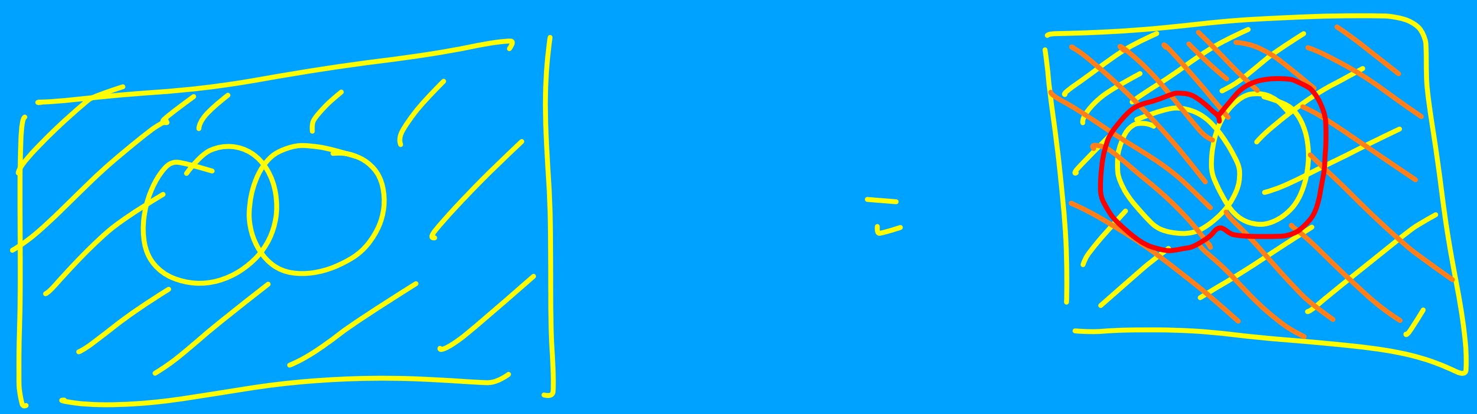
= $A \cup C$

De Morgan's law (theorem)

With respect to any universe U, for any two sets *A, B* it holds that:

- $(A \cup B)^c = A^c \cap B^c$

Venn…



Laws laws laws

With respect to any universe U, for any set *A*, it holds that

Identity laws:

- $A \cap \varnothing = \varnothing \qquad A \cup \varnothing = A$
  $A \cap U = A \qquad A \cup U = U$

Idempotent laws:

- $A \cap A = A \qquad A \cup A = A$

Complement laws:

- $(A^c)^c = A$
- $A \cap A^c = \varnothing \qquad A \cup A^c = U$
  $U^c = \varnothing \qquad \varnothing^c = U$

Laws laws laws

With respect to any universe U, for any set *A,B,C,* it holds that

Theorem 6.5

Commutativity:

$A\cap B = B\cap A$ $\quad$ $A\cup B = B\cup A$

Associativity

$(A\cap B)\cap C = A\cap (B\cap C)$ $\quad$ $(A\cup B)\cup C = A\cup (B\cup C)$

Distributivity:

$A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$ $\quad$ $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$

Idempotence

$A\cap A = A$ $\quad$ $A\cup A = A$

De Morgan

$(A\cup B)^c = A^c\cap B^c$ $\quad$ $(A\cap B)^c = A^c\cup B^c$

nul element (identity)

$A\cap\varnothing = \varnothing$ $\quad$ $A\cup\varnothing = A$

identity element

$A\cap U = A$ $\quad$ $A\cup U = U$

double complement (involution)

$(A^c)^c = A$

complementation rules

$A\cap A^c = \varnothing$ $\quad$ $A\cup A^c = U$

Each "law" is a theorem given the chosen operations.
Provably holds from definitions of the particular operations.

BUT, we can go the other way around.
We can treat them as *axioms*… *"algebra of sets"*

See Schaum 1.5 and 15.5

Digression!

Basic Identities of Boolean Algebra

Let X be a boolean variable and 0,1 constants

1. $X + 0 = X$ -- Zero Axiom
2. $X \cdot 1 = X$ -- Unit Axiom
3. $X + 1 = 1$ -- Unit Property
4. $X \cdot 0 = 0$ -- Zero Property

5. $X + X = X$ -- Idempotence
6. $X \cdot X = X$ -- Idempotence
7. $X + X' = 1$ -- Complement
8. $X \cdot X' = 0$ -- Complement
9. $(X')' = X$ -- Involution

Fall 2006 Digital Technique by Todor Stefanov, Leiden University

Fundamentals of Digital Systems Design

Other useful “laws” (equivalent axioms)

- **Absorption:**
  $A \cap (A \cup B) = A$ & $A \cup (A \cap B) = A$

Prove please: identity, distributivity…

See Schaum 15.5

What constitutes a proof?

Given a set of statements (axioms), and a schemata of rewrite rules, any statement we can reach is called a theorem.

Most theorems will be actually deriving *conditional statements!*
Mathematics establishes relations

Proofs in algebra of sets

Unecessarily long proofs:

$$
\begin{array}{cc}
A \cap A = & (nul - element) \\
(A \cap A) \cup \varnothing = & (complement) \\
(A \cap A) \cup (A \cap A^c) = & (distributivity) \\
A \cap (A \cup A^c) = & (complement) \\
A \cap U = & (unit\ element) \\
A &
\end{array}
$$

Duality of intersection and union

"Take any valid expression with intersections and unions.
Switch unions with intersections, and empty sets with U. It is still true."

Proofs in algebra of sets

Duality (set algebra)
Let Φ, Ψ be meaningful expressions involving sets, unions and intersections, then
if $\Phi = \Psi$ then $\Phi^* = \Psi^*$

where Φ^* denotes the expression obtained by exchaning unions and intersections and empty sets with U.

Proofs in algebra of sets

Duality of intersection and union
"take any valid expression, and switch unions with intersections, and empty sets with U. It is still true."

Why, how, what?

-the duality holds for the basic rules (axioms).