# Introduction to Logic and Computer Science
# Foundation of Computer Science
# Logic in Computer Science

## Lecture #5: properties of truth functions

Tamás Mihálydeák, László Aszalós

This work was supported by the construction EFOP-3.4.3-16-2016-00021.
The project was supported by the European Union, co-financed by the European Social Fund.

# Precedence and associativity

We define precedence and associativity conventions among the operators to write less parentheses without ambiguity.

- the resulting strings are not formulae by definition
    - but they can be used to uniquely reconstruct the original formula
- for the sake of simplicity we call these strings as formula
    - but in each case, we refer to the original formula instead

# Our conventions

- The outermost parentheses can be discarded
- The precedence of binary operators from the strongest to the weakest is: $\wedge$, $\vee$, $\supset$ and $\equiv$
- Negation is stronger than the others
- The operators are right-associative, so $A \supset B \supset C$ means $A \supset (B \supset C)$

# Boole function

- $f : \{0,\ 1\}^n \to \{0,\ 1\}$
- number of Boole functions with $n$ variables: $2^{2^n}$

# Boole functions with arity 1

| x | a | b | c | d |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 |

a: $\perp$ (falsity)
b: identity
c: **negation**
d: $\top$ (truth)

# Boole functions with arity 2

| x | y | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

f: conjunction
k: XOR (exclusive or, $\oplus$)
l: disjunction
m: NOR (Pierce's arrow)
n: equivalence
r: implication s: NAND (Sheffer stroke)

# Properties of negation

- The law of double negation: $\neg\neg A \Leftrightarrow A$

# Properties of conjunction

- Commutative: $(A \wedge B) \Leftrightarrow (B \wedge A)$ for all $A, B \in Form$.
- Associative: $(A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C)$ for all $A, B, C \in Form$.
- Idempotent: $(A \wedge A) \Leftrightarrow A$ for all $A \in Form$.
- $(A \wedge B) \models A$, $(A \wedge B) \models B$
- The law of contradiction: $\models \neg(A \wedge \neg A)$
- If $A, A_1, A_2, \ldots, A_n \in Form$, then
  - the set $\{A_1, A_2, \ldots, A_n\}$ is satisfiable, iff the formula $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ is satisfiable
  - the set $\{A_1, A_2, \ldots, A_n\}$ is unsatisfiable, iff the formula $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ is unsatisfiable
  - $\{A_1, A_2, \ldots, A_n\} \models A$ iff $A_1 \wedge A_2 \wedge \cdots \wedge A_n \models A$,
  - $\{A_1, A_2, \ldots, A_n\} \models A$ iff $A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge \neg A$ is unsatisfiable.

# Properties of disjunction:

- Commutative: $(A \vee B) \Leftrightarrow (B \vee A)$ for all $A$ ,$B \in Form$.
- Associative: $(A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C)$ for all $A$ ,$B$, $C \in Form$.
- Idempotent: $(A \vee A) \Leftrightarrow A$ for all $A \in Form$.
- $A \models (A \vee B)$ for all $A, B \in Form$.
- $\{(A \vee B), \neg A\} \models B$
- The law of excluded middle: $\models (A \vee \neg A)$
- Conjunction and disjunction are dual truth functors.
  - replacing disjunction-conjunction, true-false
- Two laws of distributivity:
  - $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$
  - $(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$
- Properties of absorption
  - $(A \wedge (B \vee A)) \Leftrightarrow A$
  - $(A \vee (B \wedge A)) \Leftrightarrow A$

# De Morgan's laws

- What do we say when we deny a conjunction?
- What do we say when we deny a disjunction?
- $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$
- $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$
- The proofs of De Morgan's laws.

# Properties of implication:

- $\models (A \supset A)$
- Modus ponens: $\{(A \supset B), A\} \models B$
- Modus tollens: $\{(A \supset B), \neg B\} \models \neg A$
- Chain rule: $\{(A \supset B), (B \supset C)\} \models (A \supset C)$
- Reduction to absurdity: $\{(A \supset B), (A \supset \neg B)\} \models \neg A$
- $\neg A \models (A \supset B)$
- $B \models (A \supset B)$
- $((A \wedge B) \supset C) \Leftrightarrow (A \supset (B \supset C))$
- Contraposition: $(A \supset B) \Leftrightarrow (\neg B \supset \neg A)$
- $(A \supset \neg A) \models \neg A$
- $(\neg A \supset A) \models A$
- $(A \supset (B \supset C)) \Leftrightarrow ((A \supset B) \supset (A \supset C))$
- $\models (A \supset (\neg A \supset B))$
- $((A \vee B) \supset C) \Leftrightarrow ((A \supset C) \wedge (B \supset C))$
- If $A, A_1, A_2, \ldots, A_n \in Form$, then
  - $\{A_1, A_2, \ldots, A_n\} \models A$ iff the formula $((A_1 \wedge A_2 \wedge \cdots \wedge A_n) \supset A)$ is valid.

# Properties of (material) equivalence:

- $\models (A \equiv A)$
- $\neg(A \equiv \neg A)$
- $A \equiv B \Leftrightarrow B \equiv A$
- $A \equiv (B \equiv C) \Leftrightarrow (A \equiv B) \equiv C$
- $(\neg A \equiv B) \Leftrightarrow \neg(A \equiv B)$

# Expressibility

- $(A \supset B) \Leftrightarrow \neg(A \wedge \neg B)$
- $(A \supset B) \Leftrightarrow (\neg A \vee B)$
- $(A \wedge B) \Leftrightarrow \neg(A \supset \neg B)$
- $(A \vee B) \Leftrightarrow (\neg A \supset B)$
- $(A \vee B) \Leftrightarrow \neg(\neg A \wedge \neg B)$
- $(A \wedge B) \Leftrightarrow \neg(\neg A \vee \neg B)$
- $(A \equiv B) \Leftrightarrow ((A \supset B) \wedge (B \supset A))$

# Theory of truth functors: base

A base is a set of truth functors whose members can express all truth functors.

- For example: $\{\neg, \supset\}$, $\{\neg, \wedge\}$, $\{\neg, \vee\}$
  1. $(p \wedge q) \Leftrightarrow \neg(p \supset \neg q)$
  2. $(p \vee q) \Leftrightarrow (\neg p \supset q)$
- Truth functor Sheffer: $(p|q) \Leftrightarrow_{def} \neg(p \wedge q)$
- Truth functor neither-nor: $(p \parallel q) \Leftrightarrow_{def} (\neg p \wedge \neg q)$
- Remark: Singleton bases: $(p|q)$, $(p \parallel q)$

# Normal forms

**Definition**

If $p \in Con$, then formulae $p$, $\neg p$ are literals ($p$ is the base of the literals).

**Definition**

If the formula $A$ is a literal or a conjunction of literals with different bases, then $A$ is an elementary conjunction.

**Definition**

If the formula $A$ is a literal or a disjunction of literals with different bases, the $A$ is an elementary disjunction.

# Normal forms

**Definition**

A disjunction of elementary conjunctions is a disjunctive normal form.

**Definition**

A conjunction of elementary disjunctions is a conjunctive normal form.

**Theorem**

Any formula of proposition logic can be transformed to normal form, i. e. if $A \in Form$, then there is a formula $B$ such that $B$ is a normal form and $A \Leftrightarrow B$

# Karnaugh-maps for minimising formula

- Graphic method (for few variables)
  - Bell Labs, 1952-1954; Edward Veitch, Maurice Karnaugh
- We write the values of the formula in a rectangle
- In the case of DNF, cover the ones with rectangles of size 1, 2, 4, ...
  - overlapping is allowed
  - describe the common properties of the rectangles
- In the case of CNF, cover the zeros
  - reverse description

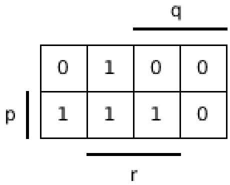
# Interpretations

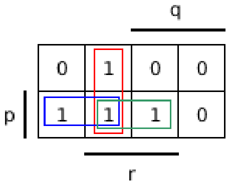
| | |
|---|---|
| $\neg p,\ \neg q$ | $\neg p,\ q$ |
| $p,\ \neg q$ | $p,\ q$ |

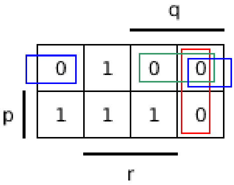
| | | | |
|---|---|---|---|
| $\neg p,\ \neg q,\ \neg r$ | $\neg p,\ \neg q,\ r$ | $\neg p,\ q,\ r$ | $\neg p,\ q,\ \neg r$ |
| $p,\ \neg q,\ \neg r$ | $p,\ \neg q,\ r$ | $p,\ q,\ r$ | $p,\ q,\ \neg r$ |

| | | | |
|---|---|---|---|
| $\neg p,\ \neg q,\ \neg r,\ \neg s$ | $\neg p,\ \neg q,\ \neg r,\ s$ | $\neg p,\ \neg q,\ r,\ s$ | $\neg p,\ \neg q,\ r,\ \neg s$ |
| $\neg p,\ q,\ \neg r,\ \neg s$ | $\neg p,\ q,\ \neg r,\ s$ | $\neg p,\ q,\ r,\ s$ | $\neg p,\ q,\ r,\ \neg s$ |
| $p,\ q,\ \neg r,\ \neg s$ | $p,\ q,\ \neg r,\ s$ | $p,\ q,\ r,\ s$ | $p,\ q,\ r,\ \neg s$ |
| $p,\ \neg q,\ \neg r,\ \neg s$ | $p,\ \neg q,\ \neg r,\ s$ | $p,\ \neg q,\ r,\ s$ | $p,\ \neg q,\ r,\ \neg s$ |

# Example




DNF: $(\neg q \wedge r) \vee (p \wedge \neg q) \vee (p \wedge r)$
CNF: $(\neg q \vee r) \wedge (p \vee r) \wedge (p \vee \neg q)$

# Solving by rewriting

Simplify the formula $p \vee q \supset r \equiv (p \supset q) \supset (p \supset r)$!

- $(\neg(p \vee q) \vee r) \equiv (\neg(\neg p \vee q) \vee (\neg p \vee r))$
- $(\neg(p \vee q) \vee r) \equiv ((p \wedge \neg q) \vee \neg p \vee r))$
- $(\neg(p \vee q) \vee r) \equiv (p \vee \neg p \vee r) \wedge (\neg q \vee \neg p \vee r)$
- $(\neg(p \vee q) \vee r) \equiv (\neg q \vee \neg p \vee r)$
- $((\neg(p \vee q) \vee r) \supset (\neg q \vee \neg p \vee r)) \wedge ((\neg q \vee \neg p \vee r) \supset (\neg(p \vee q) \vee r))$
- $(\neg(\neg(p \vee q) \vee r) \vee \neg q \vee \neg p \vee r) \wedge (\neg(\neg q \vee \neg p \vee r) \vee \neg(p \vee q) \vee r)$
- $(((p \vee q) \wedge \neg r) \vee \neg q \vee \neg p \vee r) \wedge ((q \wedge p \wedge \neg r) \vee \neg(p \vee q) \vee r)$
- $((p \vee q \vee \neg q \vee \neg p \vee r) \wedge (\neg r \vee \neg q \vee \neg p \vee r)) \wedge ((q \wedge p \wedge \neg r) \vee \neg(p \vee q) \vee r)$
- $((q \wedge p \wedge \neg r) \vee \neg(p \vee q) \vee r)$
- $(q \vee \neg(p \vee q) \vee r) \wedge (p \vee \neg(p \vee q) \vee r) \wedge (\neg r \vee \neg(p \vee q) \vee r)$
- $(q \vee (\neg p \wedge \neg q) \vee r) \wedge (p \vee (\neg p \wedge \neg q) \vee r)$
- $(q \vee r \vee \neg p) \wedge (\neg q \vee q \vee r) \wedge (p \vee r \vee \neg p) \wedge (\neg q \vee p \vee r)$
- $(q \vee r \vee \neg p) \wedge (\neg q \vee p \vee r) \Leftrightarrow r \vee (p \wedge q) \vee (\neg p \wedge \neg q)$

# Example: Karnaugh-map

Simplify the formula $p \vee q \supset r \equiv (p \supset q) \supset (p \supset r)$!

| | | | |
|---|---|---|---|
| 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 |

$r \vee \neg p \wedge \neg q \vee p \wedge q$