Discrete Structures, CSCI-150.

Information

Mon, Wed, 8:25 – 9:40pm. Hunter North C107.

Instructor: Alexey Nikolaev.

Website: http://a-nikolaev.github.io/ds/

Grading policy
No late homeworks accepted. Homeworks once a week (Monday usually). Due at the beginning of the class.

Final grade:
HWs: 25%
Two Midterms and Final: 37.5% + 37.5%

When computing the final grade, only two best exams out of three are counted, and the worst is dropped. The Final is cumulative.

Course content

Propositional Logic. Logical connectives. Truth tables. Logical equivalence. Rules of inference. Satisfiability. Predicates and quantifiers. Proofs.

Counting. Sum and product rules. Pigeonhole principle. Permutations, n! Binomial coefficients, n choose k. Selection with replacement.

Induction. Hanoi towers. Summation of series. Recurrence. Fibonacci numbers. Solving linear recurrences. Recursion.

Number theory. Divisibility and primes. Modulo-arithmetics. GCD and Euclid's algorithm. Cryptography. RSA.

Sets. Operations, empty set, singleton set, powerset. Natural, rational, real numbers. Diagonalization. Relations and Functions. Counting and Bijection. Partial orders.

Graphs. Bridges of Koenigsberg. Eulerian and Hamiltonian cycles. Trees, spanning trees. Huffman coding.

Probability. Bernoulli Trials. Random variables. Expected value.

Literature

Primary books:

- *Rosen*
  "Discrete Mathematics and its Applications" edition 6 or 7.
  (you can find a used or new 6th edition for less than $40).
- *Lehman and Leighton*
  Lecture notes "Mathematics for Computer Science" (2004).
  (free, but this is not a complete textbook)

Propositions

Def. *A proposition is a declarative sentence that is either true or false, but not both.*

A good test for a proposition is to ask *"Is it true that . . . ?"* If that makes sense, it is a proposition.

- "One plus two equals three."
- "Washington, D.C., is the capital of the US."
- "The Moon is a satellite of the Earth."

- "Albany is the capital of Canada."
- "All planets have satellites."

Propositions

Def. *A proposition is a declarative sentence that is either true or false, but not both.*

A good test for a proposition is to ask *"Is it true that . . . ?"* If that makes sense, it is a proposition.

- "One plus two equals three." *true* ✓
- "Washington, D.C., is the capital of the US." *true* ✓
- "The Moon is a satellite of the Earth." *true* ✓

- "Albany is the capital of Canada." *false* ✓
- "All planets have satellites." *false* ✓ all are propositions

Propositions

Def. *A proposition is a declarative sentence that is either true or false, but not both.*

A good test for a proposition is to ask *"Is it true that ...?"* If that makes sense, it is a proposition.

- "Please add one and two."
- "A cat."
- "Does anyone have any questions?"
- "The largest planet in the Solar System."
- "n in a prime number."

Propositions

Def. *A proposition is a declarative sentence that is either true or false, but not both.*

A good test for a proposition is to ask *"Is it true that . . . ?"* If that makes sense, it is a proposition.

- "Please add one and two." ✗
- "A cat." ✗
- "Does anyone have any questions?" ✗
- "The largest planet in the Solar System." ✗
- "n in a prime number". ✗ neither one is a proposition

Propositions

Is the following sentence a propositions?

- "Every even integer greater than 2 can be expressed as the sum of two primes."

Propositions

Instead of writing sentences, we will abbreviate them by using *propositional variables*.

It is standard practice to use the lower-case letters: $p, q, r, \ldots$

Then, if

$$\begin{aligned} p &: \quad \text{“It is raining”,} \\ q &: \quad \text{“I have an umbrella”,} \end{aligned}$$

we can construct *compound propositions* using logical operators:

$$\begin{aligned} p \textit{ and } q &: \quad \text{“It is raining, and I have an umbrella”.} \\ \textit{not } q &: \quad \text{“I don't have an umbrella”.} \end{aligned}$$

Logical Operators

And (called Conjunction)

p *and* q

$p \wedge q$ is true when both p and q are true, otherwise false.

Or (called Disjunction)

p *or* q

$p \vee q$ is true when p or q or both are true, otherwise false.

Negation

not p

$\neg\, p$ is true when p is false, otherwise false.

Truth tables

And (Conjunction)

p	q	$p \wedge q$
T	T	T
F	T	F
T	F	F
F	F	F

Or (Disjunction)

p	q	$p \vee q$
T	T	T
F	T	T
T	F	T
F	F	F

Negation

p	$\neg p$
T	F
F	T

Think of the truth tables as our ultimate definition of the logical connectives (operators).

More Operators. Implication

Consider a dietary advice
(proposition, can be true or false):

> "If you eat your breakfast, you will lose weight".

More Operators. Implication

Consider a dietary advice
(proposition, can be true or false):

> “If you eat your breakfast, you will lose weight”.

This logical connective is called *implication*:

$$\text{(eat breakfast)} \rightarrow \text{(lose weight)}$$

More Operators. Implication

Implication

if p *then* q

$p \to q$ is true if whenever p is true, so is q, otherwise false.

Truth table:

p	q	$p \to q$
T	T	T
F	T	T
T	F	F
F	F	T

An implication is true when
the if-part *is false or the* then-part *is true.*

So, $p \to q$ is equivalent to $(\neg p) \vee q$.

"I need an umbrella, if it's raining".

"If the Earth is flat, my brother is a physicist".

More Operators. Implication

1. *“If he is hungry, he is grumpy”.*
2. *“He is hungry”.*

Is he grumpy or not?

More Operators. Implication

h	g	$h \to g$
T	T	T
F	T	T
T	F	F
F	F	T

"If he is hungry, he is grumpy".

$$h \to g = T$$

If an implication is true, we can make conclusions about g, if we know h.

We know that *"he is hungry"*,

$$h = T,$$

it's only possible that he is grumpy

$$g = T.$$

More Operators. Implication

1. *"If he is hungry, he is grumpy".*
2. *"He is **not** hungry".*

Is he grumpy or not?

More Operators. Implication

h	g	$h \to g$
T	T	T
F	T	T
T	F	F
F	F	T

"If he is hungry, he is grumpy".

$$h \to g = T$$

If an implication is true, we can make conclusions about g, if we know h.

If we know that *"he is not hungry"*,

$$h = F,$$

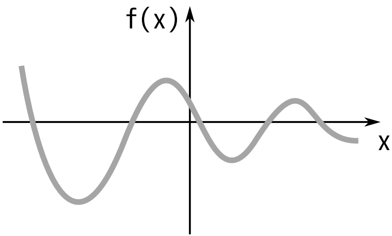
then

$$g \text{ can be } T \text{ or } F.$$

More Operators. Implication

p	q	$p \rightarrow q$
T	T	T
F	T	T
T	F	F
F	F	T

Mathematical theorems are often formulated as implications. For example:



Theorem. *If a continuous function defined on an interval is sometimes positive and sometimes negative, it must be 0 at some point.*

More Operators. Biconditional

Biconditional

p *if and only if* q
$p \leftrightarrow q$
is true when p and q have the same truth values, otherwise false.

p	q	$p \leftrightarrow q$
T	T	T
F	T	F
T	F	F
F	F	T

Often, "if and only if" is abbreviated to *iff*:

$$p \textit{ iff } q$$

"You can take the flight if and only if you buy a ticket."

Theorems are often formulated as implications or biconditionals.

Combined truth tables for connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	F	T	T	T	T
F	T	T	F	T	T	F
T	F	F	F	T	F	F
F	F	T	F	F	T	T

Complex compound propositions?

Let's take a complex compound proposition:

$$q \lor ((\neg q) \land r)$$

$$q \text{ or } ((\text{not } q) \text{ and } r)$$

q	r	$\cdots$
T	T	$\cdots$
F	T	$\cdots$
T	F	$\cdots$
F	F	$\cdots$

Complex compound propositions?

Let's take a complex compound proposition:

$$q \vee ((\neg q) \wedge r)$$

$$q \text{ or } ((\text{not } q) \text{ and } r)$$

q	r	$\neg q$	$\cdots$
T	T	F	$\cdots$
F	T	T	$\cdots$
T	F	F	$\cdots$
F	F	T	$\cdots$

Complex compound propositions?

Let's take a complex compound proposition:

$$q \vee ((\neg q) \wedge r)$$

$$q \text{ or } ((\text{not } q) \text{ and } r)$$

q	r	$\neg q$	$(\neg q) \wedge r$	$\cdots$
T	T	F	F	$\cdots$
F	T	T	T	$\cdots$
T	F	F	F	$\cdots$
F	F	T	F	$\cdots$

Complex compound propositions?

Let's take a complex compound proposition:

$$q \vee ((\neg q) \wedge r)$$

$$q \text{ or } ((\text{not } q) \text{ and } r)$$

q	r	$\neg q$	$(\neg q) \wedge r$	$q \vee ((\neg q) \wedge r)$
T	T	F	F	T
F	T	T	T	T
T	F	F	F	T
F	F	T	F	F

Complex compound propositions?

The number of rows in the truth table of a compound proposition is equal to 2^n, where n is the number of used propositional variables.

$$(\neg p) \vee ((q \rightarrow r) \wedge p)$$

p	q	r	$\cdots$
T	T	T	$\cdots$
F	T	T	$\cdots$
T	F	T	$\cdots$
F	F	T	$\cdots$
T	T	F	$\cdots$
F	T	F	$\cdots$
T	F	F	$\cdots$
F	F	F	$\cdots$

Each of the three variables can take two possible values, so the system has $2 \cdot 2 \cdot 2 = 8$ possible states.

Equivalence

Two compound propositions are equivalent if they have the same truth values for all possible cases (have the same truth tables).

q	r	$q \vee ((\neg q) \wedge r)$	$q \vee r$
T	T	T	T
F	T	T	T
T	F	T	T
F	F	F	F

Therefore, these two propositions are logically equivalent!

We write it as follows

$$q \vee ((\neg q) \wedge r) \quad \equiv \quad q \vee r$$

Note that the statement of the equivalence of two compound propositions, $a \equiv b$, is not a proposition itself.

Equivalent formulae

$$
\begin{aligned}
(A \wedge B) &\equiv (B \wedge A) && \text{commutativity of } \wedge \\
(A \vee B) &\equiv (B \vee A) && \text{commutativity of } \vee \\
((A \wedge B) \wedge C) &\equiv (A \wedge (B \wedge C)) && \text{associativity of } \wedge \\
((A \vee B) \vee C) &\equiv (A \vee (B \vee C)) && \text{associativity of } \vee \\
\neg(\neg A) &\equiv A && \text{double-negation elimination} \\
(A \rightarrow B) &\equiv (\neg B \rightarrow \neg A) && \text{contraposition} \\
(A \rightarrow B) &\equiv (\neg A \vee B) && \text{implication elimination} \\
(A \leftrightarrow B) &\equiv (A \rightarrow B) \wedge (B \rightarrow A) && \text{biconditional elimination} \\
\neg(A \wedge B) &\equiv (\neg A \vee \neg B) && \text{De Morgan's Law} \\
\neg(A \vee B) &\equiv (\neg A \wedge \neg B) && \text{De Morgan's Law} \\
(A \wedge (B \vee C)) &\equiv (A \wedge B) \vee (A \wedge C) && \text{distributivity of } \wedge \text{ over } \vee \\
(A \vee (B \wedge C)) &\equiv (A \vee B) \wedge (A \vee C) && \text{distributivity of } \vee \text{ over } \wedge
\end{aligned}
$$

Equivalent formulae

If **True** is a compound propositions that is always true, and **False** is a proposition that is always false:

$$A \wedge \textbf{True} \equiv A \qquad \text{identity}$$
$$A \vee \textbf{False} \equiv A \qquad \text{identity}$$
$$A \vee \textbf{True} \equiv \textbf{True} \qquad \text{domination}$$
$$A \wedge \textbf{False} \equiv \textbf{False} \qquad \text{domination}$$
$$A \vee \neg A \equiv \textbf{True} \qquad \text{complementation (excluded middle)}$$
$$A \wedge \neg A \equiv \textbf{False} \qquad \text{complementation (non-contradiction)}$$

Examples of such always true compound propositions:
True : $p \vee \neg p, \quad p \leftrightarrow p, \quad p \rightarrow (p \vee q), \quad$ etc.
False : . . . find a few examples of always false propositions.

Proving logical equivalences without truth tables

We can prove a logical equivalence using a sequence of known equivalences. The goal is to show that the left-hand-side is equivalent to the right-hand-side.

For example, prove that

$$q \vee ((\neg q) \wedge r) \quad \equiv \quad q \vee r$$

$$\begin{aligned} q \vee ((\neg q) \wedge r) \quad &\equiv \quad (q \vee \neg q) \wedge (q \vee r) \\ &\equiv \quad \textbf{True} \wedge (q \vee r) \\ &\equiv \quad q \vee r \end{aligned}$$

We used the distributivity of $\vee$ over $\wedge$, then the complementation equivalence, then the identity equivalence.