Discrete Structures, CSCI-150.

Information

Tuesday and Friday 9:45 – 11:00 am.

Instructor: Alexey Nikolaev.

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

Grading policy
No late homeworks accepted.
Expect to have homeworks every week.

Final grade:
HWs: 25%
Exams: 75%

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

Information
Propositions
Operators
Fighting Complexity
Equivalence

Course content

Propositional Logic. Operators. 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. Catalan numbers. Solving linear recurrence.

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 used or new 6th edition for $30–50)
- *Lehman and Leighton*
  Lecture notes "Mathematics for Computer Science" (2004).
  (free, but this is not a complete textbook)

Our first object

Information

Propositions

Operators

Fighting Complexity

Equivalence

Something that is either

true or *false*

Propositions

Information
Propositions
Operators
Fighting Complexity
Equivalence

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.
- The Sun is a planet.

Propositions

Information
Propositions
Operators
Fighting Complexity
Equivalence

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* ✓
- The Sun is a planet. *false* ✓ all are propositions

Propositions

Information

Propositions

Operators

Fighting Complexity

Equivalence

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.

- Three plus four.
- Consider these sentences.
- Does anyone have any questions?
- The largest planet in the Solar System.
- n in a prime number.

Propositions

Information
Propositions
Operators
Fighting Complexity
Equivalence

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.

- Three plus four. ✗ neither one is a proposition
- Consider these sentences. ✗
- Does anyone have any questions? ✗
- The largest planet in the Solar System. ✗
- n in a prime number. ✗

Propositions

Information
Propositions
Operators
Fighting Complexity
Equivalence

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

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

we can construct *compound propositions* using logical operators:

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

Logical Operators

Information

Propositions

Operators

Fighting Complexity

Equivalence

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

Information
Propositions
Operators
Fighting Complexity
Equivalence

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

Information

Propositions

Operators

Fighting Complexity

Equivalence

Implication

if p *then* q

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

Truth table:

p	q	$p \rightarrow q$
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, $p \rightarrow q$ 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

Information

Propositions

Operators

Fighting Complexity

Equivalence

h	g	$h \rightarrow g$
T	T	T
F	T	T
T	F	F
F	F	T

"If he is hungry, he is grumpy".

$$h \rightarrow g = T$$

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

If we know that he is indeed hungry,

$$h = T,$$

then

$$g = T.$$

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

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

Information

Propositions

Operators

Fighting Complexity

Equivalence

More Operators. Implication

Information

Propositions

Operators

Fighting Complexity

Equivalence

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

Big Al told us that dogs can't look up.

Our thought was that:
$p \to q =$ "If dogs can look up, Big Al is a liar".

$p =$ "Dogs can look up"
$q =$ "Big Al is a liar"

$(\neg p) \vee q =$ "Dogs can't look up, or Big Al is a liar".

More Operators. Biconditional

Information
Propositions
Operators
Fighting Complexity
Equivalence

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?

Information
Propositions
Operators
Fighting Complexity
Equivalence

Let's take a complex compound proposition:

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

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

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:

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

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

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

Complex compound propositions?

Information

Propositions

Operators

Fighting Complexity

Equivalence

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?

Information
Propositions
Operators
Fighting Complexity
Equivalence

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

Information
Propositions
Operators
Fighting Complexity
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

Information
Propositions
Operators
Fighting Complexity
Equivalence

$(a \land b) \equiv (b \land a)$	commutativity of $\land$
$(a \lor b) \equiv (b \lor a)$	commutativity of $\lor$
$((a \land b) \land c) \equiv (a \land (b \land c))$	associativity of $\land$
$((a \lor b) \lor c) \equiv (a \lor (b \lor c))$	associativity of $\lor$
$\neg(\neg a) \equiv a$	double-negation elimination
$(a \rightarrow b) \equiv (\neg b \rightarrow \neg a)$	contraposition
$(a \rightarrow b) \equiv (\neg a \lor b)$	implication elimination
$(a \leftrightarrow b) \equiv (a \rightarrow b) \land (b \rightarrow a)$	biconditional elimination
$\neg(a \land b) \equiv (\neg a \lor \neg b)$	De Morgan's Law
$\neg(a \lor b) \equiv (\neg a \land \neg b)$	De Morgan's Law
$(a \land (b \lor c)) \equiv (a \land b) \lor (a \land c)$	distributivity of $\land$ over $\lor$
$(a \lor (b \land c)) \equiv (a \lor b) \land (a \lor c)$	distributivity of $\lor$ over $\land$