CS 320

Applied Discrete Mathematics
Fall 2015 Colin Godfrey

Course info

The course web page will be www.cs.umb.edu/cs320, I hope.

I can be reached by email at colin.godfrey@umb.edu.

I'll have office hours Tu after class, M-3-607

The Powerpoint slides are originally descended from ones from Marc Pomplun, from CS 320, Spring 2003, with much subsequent modification.

Slides will be available on the course web page. The pdf version will be handouts, 6 slides per page.

Why Care about Discrete Math?

"Discrete" means separate things, as opposed to continuous things, as in calculus.

"Discrete" is quite different from "discreet".

• Digital computers are based on discrete "atoms"(bits).

Both a computer's
- structure (circuits) and
- operations (execution of algorithms)

can be described by discrete math.

What we shall cover

- Logic and Set Theory
- Functions and Sequences
- Algorithms
- Applications of Number Theory
- Mathematical Reasoning
- Counting
- Probability Theory
- Relations and Equivalence Relations
- Graphs and Trees
- Boolean Algebra

Mathematical Appetizers

Useful tools for discrete mathematics:

Logic

Set Theory

Functions

Sequences

Logic

- Crucial for reasoning in mathematics and in writing software.
- Used for designing electronic circuitry
- Logic is a system based on propositions.
- A **proposition** is a **statement**: something that is either true or false (not both).
- We say that the truth value of a proposition is either true (T) or false (F).
- T and F correspond to 1 and 0 in digital circuits

Different Kinds of Logic

There are various kinds of multiple-valued logics, where you can have True, False, and some other things, perhaps representing “unknown” or “maybe”.

In this course we shall stick to classical logic, where we have only T and F values.

Let’s Talk About Logic

Logic is a system based on propositions.

A proposition is a statement that is either true or false (not both).

We say that the truth value of a proposition is either true (T) or false (F).

T and F correspond to 1 and 0 in digital circuits

The Statement/Proposition Game

“Elephants are bigger than mice.”

Is this a proposition?

yes

What is the truth value of the proposition?

true

The Statement/Proposition Game

“520 < 111”

Is this a proposition?

yes

What is the truth value of the proposition?

false

The Statement/Proposition Game

“y > 5”

Is this a proposition?

no

Its truth value depends on the value of y, but this value is not specified.

We call this type of statement a propositional function or open sentence.

The Statement/Proposition Game

“Today is September 8 and 99 < 5.”

Is this a proposition?

yes

What is the truth value of the proposition?

false

The Statement/Proposition Game

"Please do not fall asleep."

Is this a proposition?

no

It's a request.

The Statement/Proposition Game

"If all elephants are red, they can hide in cherry trees."

Is this a proposition?

yes

What is the truth value of the proposition?

This is a tough question, and may have a different meaning in ordinary life than it would have in logic.

The Statement/Proposition Game

"x < y if and only if y > x."

Is this a proposition?

yes

What is the truth value of the proposition?

true

… because its truth value does not depend on specific values of x and y.

It depends on our understanding of the context – that x and y are numbers, for example

Combining Propositions

As we have seen in the previous examples, one or more propositions can be combined to form a single compound proposition.

We formalize this by denoting propositions by letters such as p, q, r, s, and introducing several logical operators.

The reason we do this is to abstract from the particular to a general pattern, true for all propositions.

We want to understand the general pattern.

Logical Operators (Connectives)

We will examine the following logical operators:

- Negation (NOT)
- Conjunction (AND)
- Disjunction (OR)
- Exclusive or (XOR)
- Implication (if – then)
- Biconditional (if and only if)

Truth tables can be used to show how these operators can combine propositions to form compound propositions.

These operations can be performed bitwise on bit strings, for example in C, C++, or java.

Negation (NOT)

Negation

Unary Operator, Symbol: $\neg$

P	$\neg$P
True	False
False	True

Conjunction (AND)

Binary Operator, Symbol: ∧

P	Q	P∧Q
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction (OR)

Binary Operator, Symbol: ∨

P	Q	P∨Q
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive Or (XOR)

Binary Operator, Symbol: ⊕

P	Q	P ⊕ Q
T	T	F
T	F	T
F	T	T
F	F	F

Implication (if – then)

Binary Operator, Symbol: →

If it is raining then the ground is wet.

P	Q	P → Q
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional (if and only if)

Binary Operator, Symbol:↔

P	Q	P ↔ Q
T	T	T
T	F	F
F	T	F
F	F	T

Statements and Operations

Statements and operators can be combined in any way to form new statements.

P	Q	P∧Q	¬(P∧Q)	(¬P) ∨(¬Q)
T	T	T	F	F
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

Equivalent Statements

P	Q	$\neg(P\wedge Q)$	$(\neg P)\vee(\neg Q)$	$(\neg(P\wedge Q))\leftrightarrow((\neg P)\vee(\neg Q))$
T	T	F	F	T
T	F	T	T	T
F	T	T	T	T
F	F	T	T	T

The statements $\neg(P\wedge Q)$ and $(\neg P)\vee(\neg Q)$ are logically equivalent, because $\neg(P\wedge Q) \leftrightarrow (\neg P)\vee(\neg Q)$ is always true.

Tautologies and Contradictions

A *tautology* is a statement that is always true.

Examples:

- $R\vee(\neg R)$
- $\neg(P\wedge Q) \rightarrow (\neg P)\vee(\neg Q)$

If $S \rightarrow T$ is a tautology, we write $S \Rightarrow T$.

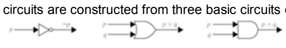
If $S \leftrightarrow T$ is a tautology, we write $S \Leftrightarrow T$.

Logic Circuits (Studied in depth in Chapter 12)

Electronic circuits; each input/output signal can be viewed as a 0 or 1.

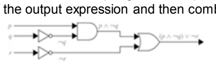
- 0 represents **False**
- 1 represents **True**

Complicated circuits are constructed from three basic circuits called gates.



- The inverter (**NOT gate**) takes an input bit and produces the negation of that bit.
- The **OR gate** takes two input bits and produces the value equivalent to the disjunction of the two bits.
- The **AND gate** takes two input bits and produces the value equivalent to the conjunction of the two bits.

More complicated digital circuits can be constructed by combining these basic circuits to produce the desired output given the input signals by building a circuit for each piece of the output expression and then combining them. For example:



Tautologies and Contradictions

A *contradiction* is a statement that is always false.

Examples:

- $R\wedge(\neg R)$
- $\neg(\neg(P\wedge Q) \leftrightarrow (\neg P)\vee(\neg Q))$

The negation of any tautology is a contradiction, and

the negation of any contradiction is a tautology.

Exercises

We already know the following tautology:
$\neg(P\wedge Q) \Leftrightarrow (\neg P)\vee(\neg Q)$

Nice home exercise: Show that
$\neg(P\vee Q) \Leftrightarrow (\neg P)\wedge(\neg Q)$.

These two tautologies are known as De Morgan's laws.

Table 6 in Section 1.3 shows many useful laws.

The first thirty or so exercises in Section 1.3 may help you get used to propositions and operators.

Equivalences

When an iff statement is a tautology:
$\neg(P\wedge Q) \Leftrightarrow (\neg P)\vee(\neg Q)$

we can write it as an *equivalence*, meaning the two statements are logically equivalent:
For any truth values of the variables the statements are both true or both false

$\neg(P\wedge Q) \equiv (\neg P)\vee(\neg Q)$

Important Equivalences

An equivalence that is important for you to think about and understand is:

$P \rightarrow Q \equiv \neg P \vee Q$

It follows from this that:

$\neg(P \rightarrow Q) \equiv P \wedge \neg Q$

There are many other good ones on page 28 that you should try to understand intuitively. e.g.

$(P \rightarrow Q) \wedge (P \rightarrow R) \equiv P \rightarrow (Q \wedge R)$

8 Sept 2015 31

Propositional Functions

Propositional function (open sentence):
statement involving one or more variables,

e.g.: x-3 > 5.

Let us call this propositional function P(x), where P is the *predicate* and x is the *variable*.

What is the truth value of P(2) ? false

What is the truth value of P(8) ? false

What is the truth value of P(9) ? true

8 Sept 2015 32

Propositional Functions

Let us consider the propositional function Q(x, y, z) defined as:

x + y = z.

Here, Q is the predicate and x, y, and z are the variables.

What is the truth value of Q(2, 3, 5) ? true

What is the truth value of Q(0, 1, 2) ? false

What is the truth value of Q(9, -9, 0) ? true

8 Sept 2015 33

Universal Quantification

Let P(x) be a propositional function.

Universally quantified sentence:
For all x in the universe of discourse P(x) is true.

Using the universal quantifier ∀:
∀x P(x) "for all x P(x)" or "for every x P(x)"

(Note: ∀x P(x) is either true or false, so it is a proposition, not a propositional function.)

8 Sept 2015 34

Universal Quantification

Example:

S(x): x is a UMB student.

G(x): x is a genius.

What does ∀x (S(x) → G(x)) mean ?

"If x is a UMB student, then x is a genius."
or
"All UMB students are geniuses."

8 Sept 2015 35

Existential Quantification

***Existentially quantified* sentence**:
There exists an x in the universe of discourse for which P(x) is true.

Using the existential quantifier ∃:
∃x P(x) "There is an x such that P(x)."
"There is at least one x such that P(x)."

(Note: ∃x P(x) is either true or false, so it is a proposition, but not a propositional function.)

8 Sept 2015 36

Existential Quantification

Example:
G(x): x is a genius.
P(x): x is a UMB professor.

What does $\exists x\ (P(x) \wedge G(x))$ mean ?

"There is an x such that x is a UMB professor and x is a genius."
or
"At least one UMB professor is a genius."

8 Sept 2015 37

Quantification

Another example:
Let the universe of discourse be the real numbers.

What does $\forall x \exists y\ (x + y = 320)$ mean ?

"For every x there exists a y such that x + y = 320."

Is it true? yes

Is it true for the natural numbers? no

8 Sept 2015 38

Disproof by Counterexample

A counterexample to $\forall x\ P(x)$ is an object c so that P(c) is false.

Statements such as $\forall x\ (P(x) \rightarrow Q(x))$ can be disproved by simply providing a counterexample.

Statement: "All birds can fly."
Disproved by counterexample: Penguin.

8 Sept 2015 39

Negation

$\neg(\forall x\ P(x))$ is logically equivalent to $\exists x\ (\neg P(x))$.

$\neg(\exists x\ P(x))$ is logically equivalent to $\forall x\ (\neg P(x))$.

See Table 2 in Section 1.4.

I recommend exercises 5, 7, 9 in Section 1.4, for starters.

8 Sept 2015 40

Precedence of Logical Operators

Operator	precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

8 Sept 2015 41

Operator Precedence

$p \vee q \wedge r$ means
$p \vee (q \wedge r)$

$p \rightarrow q \vee r$ means
$p \rightarrow (q \vee r)$

$p \rightarrow q \leftrightarrow q \rightarrow p$ means
$(p \rightarrow q) \leftrightarrow (q \rightarrow p)$

8 Sept 2015 42

Let's proceed to…

Mathematical Reasoning

Sections 1.6, 1.7

Mathematical Reasoning

We need **mathematical reasoning** to

- determine whether a mathematical argument is correct or incorrect and
- construct mathematical arguments.

Mathematical reasoning is not only important for conducting **proofs** and **program verification**, but also for **artificial intelligence** systems (drawing inferences).

Terminology

An ***axiom*** is a basic assumption about mathematical structures that needs no proof.

We can use a ***proof*** to demonstrate that a particular statement is true. A proof consists of a sequence of statements that form an argument.

The steps that connect the statements in such a sequence are the ***rules of inference***.

Cases of incorrect reasoning are called ***fallacies***.

A ***theorem*** is a statement that can be shown to be true.

Terminology

A ***lemma*** is a simple theorem used as an intermediate result in the proof of another theorem.

A ***corollary*** is a proposition that follows directly from a theorem that has been proved.

A ***conjecture*** is a statement whose truth value is unknown. Once it is proven, it becomes a theorem.

Rules of Inference

Rules of inference provide the justification of the steps used in a proof.

One important rule is called ***modus ponens*** or the ***law of detachment***. It is based on the tautology $(p \wedge (p \rightarrow q)) \rightarrow q$. We write it in the following way:

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

The two ***hypotheses*** p and $p \rightarrow q$ are written in a column, and the ***conclusion*** below a bar, where $\therefore$ means "therefore".

Rules of Inference

The general form of a rule of inference is:

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline \therefore q \end{array}$$

The rule states that if p_1 **and** p_2 **and** … **and** p_n are all true, then q is true as well.

The following rules of inference can be used in any mathematical argument and do not require any proof.

Rules of Inference

$$\frac{p}{\therefore\ p \lor q}$$ Addition

$$\frac{p \land q}{\therefore\ p}$$ Simplification

$$\frac{\begin{array}{l} p \\ q \end{array}}{\therefore\ p \land q}$$ Conjunction

$$\frac{\begin{array}{l} \neg q \\ p \rightarrow q \end{array}}{\therefore\ \neg p}$$ Modus tollens

$$\frac{\begin{array}{l} p \rightarrow q \\ q \rightarrow r \end{array}}{\therefore\ p \rightarrow r}$$ Hypothetical syllogism

$$\frac{\begin{array}{l} p \lor q \\ \neg p \end{array}}{\therefore\ q}$$ Disjunctive syllogism

Arguments

Just like a rule of inference, an ***argument*** consists of one or more hypotheses and a conclusion.

We say that an argument is ***valid***, if whenever all its hypotheses are true, its conclusion is also true.

However, if any hypothesis is false, even a valid argument can lead to an incorrect conclusion.

Arguments

Example:

"If 101 is divisible by 3, then 101^2 is divisible by 9. 101 is divisible by 3. Consequently, 101^2 is divisible by 9."

Although the argument is **valid**, its conclusion is **incorrect**, because one of the hypotheses is false ("101 is divisible by 3.").

If in the above argument we replace 101 with 102, we could correctly conclude that 102^2 is divisible by 9.

Arguments

Which rule of inference was used in the last argument?

p: "101 is divisible by 3."

q: "101^2 is divisible by 9."

$$\frac{\begin{array}{l} p \\ p \rightarrow q \end{array}}{\therefore\ q}$$ Modus ponens

Unfortunately, one of the hypotheses (p) is false. Therefore, the conclusion q is incorrect.

Arguments

Another example:

"If it rains today, then we will not have a barbeque today. If we do not have a barbeque today, then we will have a barbeque tomorrow.
Therefore, if it rains today, then we will have a barbeque tomorrow."

This is a **valid** argument: If its hypotheses are true, then its conclusion is also true.

Arguments

Let us formalize the previous argument:

p: "It is raining today."

q: "We will not have a barbecue today."

r: "We will have a barbecue tomorrow."

So the argument is of the following form:

$$\frac{\begin{array}{l} p \rightarrow q \\ q \rightarrow r \end{array}}{\therefore\ p \rightarrow r}$$ Hypothetical syllogism

Arguments

Another example:

Gary is either intelligent or a good actor.
If Gary is intelligent, then he can count from 1 to 10.
Gary can only count from 1 to 2.
Therefore, Gary is a good actor.

i: “Gary is intelligent.”
a: “Gary is a good actor.”
c: “Gary can count from 1 to 10.”

Arguments

i: “Gary is intelligent.”
a: “Gary is a good actor.”
c: “Gary can count from 1 to 10.”

Step 1:	$\neg c$	Hypothesis
Step 2:	$i \to c$	Hypothesis
Step 3:	$\neg i$	Modus Tollens Steps 1 & 2
Step 4:	$a \lor i$	Hypothesis
Step 5:	a	Disjunctive Syllogism Steps 3 & 4

Conclusion: **a** (“Gary is a good actor.”)

Arguments

Yet another example:

If you listened to me, you will have passed CS 320.
You passed CS 320.
Therefore, you have listened to me.

Is this argument valid?

No, it assumes $((p \to q) \land q) \to p$.

This statement is not a tautology. It is false if p is false and q is true.

Rules of Inference for Quantified Statements

$$\frac{\forall x\, P(x)}{\therefore P(c) \text{ if } c \in U}$$ *Universal instantiation*

$$\frac{P(c) \text{ for an arbitrary } c \in U}{\therefore \forall x\, P(x)}$$ *Universal generalization*

$$\frac{\exists x\, P(x)}{\therefore P(c) \text{ for some element } c \in U}$$ *Existential instantiation*

$$\frac{P(c) \text{ for some element } c \in U}{\therefore \exists x\, P(x)}$$ *Existential generalization*

Rules of Inference for Quantified Statements

Example:

Every UMB student is a genius.
George is a UMB student.
Therefore, George is a genius.

U(x): “x is a UMB student.”
G(x): “x is a genius.”

Rules of Inference for Quantified Statements

The following steps are used in the argument:

Step 1: $\forall x\, (U(x) \to G(x))$	Hypothesis
Step 2: $U(George) \to G(George)$	Univ. instantiation using Step 1
Step 3: U(George)	Hypothesis
Step 4: G(George)	Modus ponens using Steps 2 & 3

$$\frac{\forall x\, P(x)}{\therefore P(c) \text{ if } c \in U}$$ Universal instantiation