CS 30: Discrete Math in CS (Winter 2020): Lecture 2 + 3

Date: 8th January, 2020 (Wednesday) + 9th January, 2020 (X-hour)
Topic: Functions, Propositional Logic
Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.
Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

---

1 Functions

1. **Definition.** A function is a *mapping* from one set to another. The first set is called the *domain* of the function, and the second set is called the *co-domain*. For *every* element in the domain, a function assigns a *unique* element in the co-domain.

   Notationally, this is represented as
   $$f : A \to B$$
   where A is the set indicating the domain $\mathrm{dom}(f)$, and B is the set indicating the co-domain $\mathrm{codom}(f)$. For every $a \in A$, the function maps the value of $a \mapsto f(a)$ where $f(a) \in B$.

   The *range* of the function is the subset of the co-domain which are *actually mapped to*. That is, $b \in B$ is in the range if and only if there is some element $a \in A$ such that $f(a) = b$. The range can also be written in the set-builder notation as
   $$\mathrm{range}(f) := \{f(a) : a \in A\}$$

   Remark: *For any function f with finite domains and ranges, we have* $|\mathrm{range}(f)| \le |\mathrm{dom}(f)|$

2. **An Example.** Suppose

   $A = \{1, 2, 3\}$, and $B = \{5, 6\}$, then the map $f(1) = 5, f(2) = 5, f(3) = 6$ is a valid function.

   A is the domain. B is the co-domain. In this example, B also happens to be the range.

3. **The Identity Function.** When the domain is the same as the co-domain, the *idenitity* function $\mathrm{id} : A \to A$ maps $a \in A$ to $a \mapsto a$.

4. **More Examples.**
   - Usually (say in calculus) a function is described as a formula like $f(x) = x^2$. Henceforth, whenever you see a function ask your self how does it map to the above definition. In this example, this is as follows.
     the domain is $\mathbb{R}$, the set of real numbers, and so is the co-domain. The map is $x \mapsto x^2$ – check both are real numbers. The range of the function is the set of non-negative real numbers (sometimes denoted as $\mathbb{R}_+$).
   - $f(x) = \sin x$ is a function whose domain is $\mathbb{R}$ and the range is the interval $[-1, 1]$.
   - A (deterministic) computer program/algorithm is also a function; its domain is the set of possible inputs and its range is the set of possible outputs.

Remark: *How about the function $f(x) = \sqrt{x}$? Is this a function? When you think about it, you see some issues if we don't define the domain and co-domain. For instance, if the domain contains* negative *numbers, then what is $\sqrt{-1}$? Ok, so perhaps the domain is all positive real numbers. However, we also have a problem with $\sqrt{4}$ – is it mapping to $+2$ or -2? Note it can only map to a* unique *number. This can be resolved by stating the domain and co-domain are both non-negative reals, and the $x \mapsto \sqrt{x}$ goes to the positive root.*

✍

Exercise: *Given a set $A = \{1,2,3\}$ and $B = \{4,5,6\}$, describe a function f whose range is $\{5\}$, and describe a function g whose range is $\{4,6\}$. Just to get a feel, how many functions can you describe of the first form (whose range is $\{5\}$), and how many functions can you describe of the second form?*

5. **Sur-, In-, Bi- jective functions.** A function $f : A \to B$ is

   - *surjective*, if the range is the same as the co-domain. That is, for every element $b \in B$ there exists some $a \in A$ such that $f(a) = b$. Such functions are also called *onto* functions.
     For example, if $A = \{1,2,3\}$ and $B = \{5,6\}$, and consider the function $f : A \to B$ with $f(1) = 5$, $f(2) = 5$, and $f(3) = 6$. Then, f is surjective. This is because for $5 \in B$ there is $1 \in A$ such that $f(1) = 5$ and for $6 \in B$ there is a $3 \in A$ such that $f(3) = 6$.

     Remark: *If A and B are* finite sets*, and $f : A \to B$ is a surjective function, then $|B| \le |A|$?*

   - *injective*, if there are no collisions. That is, for any two elements $a \neq a' \in A$, we have $f(a) \neq f(a')$. Such functions are also called *one-to-one* functions.
     For example, if $A = \{1,2,3\}$ and $B = \{5,6,7,8\}$, and consider the function $f : A \to B$ with $f(1) = 5$, $f(2) = 6$, and $f(3) = 8$. Then, f is injective. This is because $f(1), f(2), f(3)$ are all distinct numbers.

     Remark: *If A and B are* finite sets*, and $f : A \to B$ is an injective function, then $|A| = |\text{range}(f)|$. Thus, $|A| \le |B|$.*

     Injective functions have *inverses*. Formally, given any injective function $f : A \to B$, we can define a function $f^{-1} : \text{range}(f) \to A$ as follows

     $$f^{-1}(b) = a \quad \text{where } a \text{ is the } \textit{unique } a \in A \text{ with } f(a) = b.$$

   - *bijective*, if the function is both surjective and injective.
     For example, if $A = \{1,2,3,4\}$ and $B = \{2,4,6,8\}$, then the function $f(x) = 2x$ defined over the domain A and co-domain B is a bijective function. Can you see why?

     Remark: *If A and B are* finite sets*, and $f : A \to B$ is a bijective function, then $|B| = |A|$? We will see this useful fact many times in the combinatorics module.*

6. **Composition of Functions.** Given a function $f : A \to B$ and a function $g : B \to C$, one can define the composition of g and f, denoted as $g \circ f$ with domain A and co-domain C as follows:

$$(g \circ f)(a) = g(f(a)) \quad \text{that is} \quad a \mapsto g(f(a))$$

Note this is well defined since for every $a \in A$, $f(a) \in B$, and thus $g(f(a)) \in C$.

Examples

- Suppose $A = \{1,2,3\}$ and $B = \{5,6\}$ and $C = \{3,4\}$. Also suppose $f : A \to B$ is defined as $f(1) = 5$, $f(2) = 6$, and $f(3) = 5$; and $g : B \to C$ is defined as $g(5) = 3$ and $g(6) = 4$, then the composed function is $(g \circ f)(1) = 3$, $(g \circ f)(2) = 4$, and $(g \circ f)(3) = 3$.
- If $f : \mathbb{R} \to \mathbb{R}_+$ defined as $f(x) = x^2$ and $g : \mathbb{R}_+ \to \mathbb{R}_+$ defined as $g(x) = \sqrt{x}$ (as defined above), then (convince yourself) that $(g \circ f)(x)$ returns the *absolute* value of x.
- If $f : A \to B$ is a bijection, and $f^{-1} : B \to A$ is its inverse, convince yourself that $(f^{-1} \circ f) : A \to A$ is the $\mathrm{id} : A \to A$ identity function.

2 Propositional Logic

1. **Atomic Propositions/ Boolean Variables.** A *proposition* is a statement which takes one of the two *Boolean* values $\{\mathsf{true}, \mathsf{false}\}$. Here are a few examples.

   (a) $p : (2 + 2 = 4)$.

   (b) q : (Nairobi is the capital of the USA).

   (c) r : (It will rain sometime tomorrow.).

   Clearly, p is a proposition which takes value true, and q is a proposition which takes a value false. r is a proposition regarding the future, and its value will be determined tomorrow. As of now, it is a *Boolean variable*.

2. **Compound Propositions/ Boolean Formulas.** One can form compound propositions by taking atomic propositions and joining them together using operations. For instance, the following statement: "Either $2 + 2 = 4$, or Nairobi is the capital of the USA" contains a *either...or...* of two atomic statements. One of them is true, one of them is false, but since one is true it renders the compound statement, true.

   Compound Propositions are obtained by doing operations on Boolean Variables, and are often referred to as *Boolean Formulas*.

3. **Logic Operators.**

   - **Negation.** Given a proposition p, the proposition $q = \neg p$ is defined to take the value true if p takes the value false, and vice-versa, that is, q takes the value false if p takes the value true.

     For example, if $p : (2 + 2 = 4)$, then $q = \neg p$ is defined as $q : (2 + 2 \neq 4)$.
   - **OR and AND.** Given two atomic propositions p, q:

- The proposition $p \vee q$ is true if and only if *at least one (and possibly both) of* p and q take the value true.
- The proposition $p \wedge q$ takes the value true if and only if *both* p and q take the value true.

For example, if $p : (7 \text{ is even})$ and $q = (14 \text{ is even})$, then

- $p \vee q$ is true since q is true.
- $p \wedge q$ is false since p is false.

Exercise: *Suppose we had three atomic propositions p, q, r. When would $p \vee (q \vee r)$ be* true*? When would $p \wedge (q \wedge r)$ be true?*

- **Implications.** The final operation we look at is *implications.* The proposition $p \Rightarrow q$ is supposed to capture the proposition stating "if p is true, then q is true". The definition is that $p \Rightarrow q$ has truth value false *only if* p has truth value true and q has truth value false.

  For example, consider the statement "If it rains tomorrow, then I will not deliver mail tomorrow" Suppose p is the proposition "It will rain tomorrow" and q is the proposition "I will not deliver mail tomorrow.", then the above statement is captured by the proposition $(p \Rightarrow q)$.

  Both p and q are atomic propositions. "Tomorrow" will decide what the values p and q take. If it rains, p takes the value true, otherwise it takes the value false. If I do deliver mail tomorrow, q takes the value false, otherwise it takes the value true.

  What about the proposition $r = (p \Rightarrow q)$ though? Well, if it does rain tomorrow and I don't deliver mail, then r takes the value true. And, if it rains tomorrow but I do deliver mail, then r takes the value false. But the slightly interesting situation is if it *doesn't* rain tomorrow (that is, if p takes the value false). Suppose, furthermore, you did *not* deliver mail either (so q takes the value true.) What value do you think r takes? It takes the value true – the implication "still holds"; if the premise is false, then I can make *any* statement I want.

  Another example: The statement "If the sun rises in the West, then I am Batman" is *true*. It doesn't *matter* whether I am Batman or not; the sun doesn't rise in the West, and so I can say any garbage after "If the sun rises in the West,..." and the implication is still true. Useless, but true. To contrast this, consider the slightly different statement "If the sun rises in the East, then I am Batman". Well this, if I read it, is false. Sun does rise in the East, and I am not Batman; ergo, the implication is untrue. (Of course, if Batman reads it, he would think it is true.)

  Formally, $(p \Rightarrow q)$ is true *unless* p takes the value true and q takes the value false.

4. **Truth Tables.** This is perhaps the most important construct in this lecture. Given a compound proposition, one can completely understand it by looking at the *truth table*, that is, the value this compound proposition takes given the possible settings of the underlying atomic propositions.

   Below are the truth tables of the various operations above.

p	$q = \neg p$
true	false
false	true

p	q	$p \vee q$
true	true	true
true	false	true
false	true	true
false	false	false

p	q	$p \wedge q$
true	true	true
true	false	false
false	true	false
false	false	false

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

Exercise: *Write the truth tables of:*

- $p \vee (q \vee r)$ *and* $p \wedge (q \wedge r)$.
- $\neg p \vee q$
- $p \wedge (q \vee r)$, *and* $(p \vee q) \wedge (p \wedge r)$.

5. **Order of Operations.** Just as in arithmetic, with logical operations there is an order in which they are applied. If the parantheses are not provided, then the first precedence is given to $\neg$. Then comes the ORs and ANDs – these are always parenthesized. And the last in order are implications.

   For example, the compound proposition $p \Rightarrow p \vee q$ actually means $p \Rightarrow (p \vee q)$ instead of $(p \Rightarrow p) \vee q$. Similarly, $\neg p \vee q$ means $(\neg p) \vee q$ and not $\neg(p \vee q)$. Generally, when in doubt put parenthesis.

6. **Logical Equivalence.** Two compound propositions/formulas are *logically equivalent* if they have the same truth tables. Here is an important example which expresses the $\Rightarrow$ using OR and negations.

   $$p \Rightarrow q \quad \equiv \quad \neg p \vee q \tag{Implication as OR}$$

   The proof of the above equivalence is described by the following truth table.

7. **Important Equivalences.** There are many important equivalences which one should internalize. They are listed below. You should (a) first get a feeling of these using plain English, and (b) then formally check **all** of them by writing truth tables. Think of this as one big exercise.

   - (**Negation of Negation.**) $\neg(\neg p) \equiv p$.

p	q	$p \Rightarrow q$	$\neg p$	$\neg p \vee q$
true	true	true	false	true
true	false	false	false	false
false	true	true	true	true
false	false	true	true	true

- (**Operation with** true, false.) $p \wedge \text{true} \equiv p$; $p \vee \text{true} \equiv \text{true}$; $p \wedge \text{false} \equiv \text{false}$; $p \vee \text{false} \equiv p$.
- (**Idempotence.**) $p \wedge p \equiv p$; $p \vee p \equiv p$.
- (**Operation with Negation.**) $p \wedge \neg p \equiv \text{false}$; $p \vee \neg p \equiv \text{true}$.
- (**Irrelevance.**) $p \vee (p \wedge q) \equiv p$; $p \wedge (p \vee q) \equiv p$.
- (**Commutativity.**)
  - $p \vee q \equiv q \vee p$.
  - $p \wedge q \equiv q \wedge p$.
- (**Associativity.**)
  - $p \vee (q \vee r) \equiv (p \vee q) \vee r$.
  - $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$.
- (**Distributivity.**)
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.
- (**Implications as an OR.**) $p \Rightarrow q \equiv \neg p \vee q$.
- (**De Morgan's Law.**) $\neg(p \vee q) \equiv \neg p \wedge \neg q$; $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

Exercise: *Show* $(p \wedge q) \Rightarrow q$ *is* $\equiv \text{true}$.

8. **Tautologies, Contradictions, and Satisfiability.**

A formula ϕ is a *tautology* if it takes the truth value true *no matter* what values the underlying variables take. That is, ϕ is logically equivalent to true. We have already see one tautology: $p \vee \neg p$ in the operation with negation.

Here is another example

$$\phi := \quad p \wedge (p \Rightarrow q) \Rightarrow q$$

One way to check this the truth table.

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$p \wedge (p \Rightarrow q) \Rightarrow q$
true	true	true	true	true
true	false	false	false	true
false	true	true	false	true
false	false	true	false	true

Another way is to reduce the formula as follows to prove that the formula is equivalent to true.

$$
\begin{aligned}
p \wedge (p \Rightarrow q) \Rightarrow q \;&\equiv\; p \wedge (\neg p \vee q) \Rightarrow q && \text{Implication as OR} \\
&\equiv\; ((p \wedge \neg p) \vee (p \wedge q)) \Rightarrow q && \text{Distributivity} \\
&\equiv\; (\mathsf{false} \vee (p \wedge q)) \Rightarrow q && \text{Operation with Negation} \\
&\equiv\; (p \wedge q) \Rightarrow q && \text{Operation with } \mathsf{false} \\
&\equiv\; \mathsf{true} && \text{Exercise}
\end{aligned}
$$

A formula ϕ is a *contradiction* or *unsatisfiable* if it takes the truth value false *no matter* what values the underlying variables take. That is, ϕ is logically equivalent to false. ✍

Exercise: *Prove that the following formula is a contradiction*

$$\big((\neg p \wedge q) \vee (p \wedge \neg q)\big) \wedge (p \Rightarrow q) \wedge (q \Rightarrow p)$$

A formula ϕ is *satisfiable* if there is some setting of the underlying variables which makes it true. That is, it is *not* unsatisfiable.