Handout 01: Discrete Math Review Sheet

CS Theory Fall 2022

Cyrus Illick and Walt McKelvie *September 19, 2022*

Intro

This document is a review of Discrete Math. The following list of definitions, theorems, and examples **do not encompass all of Discrete**. These are just some aspects we consider to be helpful for our CS Theory class (the class webpage has pointers to some other resources as well). Discrete Math is a prerequisite for this course: if you are feeling shaky with the content, we suggest you look back and review your notes, and come to office hours if you have any questions!

Boolean Logic

We use letters such as (P,Q,R) to denote variables, and use 1 for TRUE and 0 for FALSE. Important operations in Boolean logic include: ($\neg$) = NOT, ($\wedge$) = AND, ($\vee$) = OR, ($\oplus$) = XOR, ($\rightarrow$) = IMPLIES, ($\leftrightarrow$) = EQiVALENT.

Example. The following are examples of boolean operations:

- $0 \wedge 0 = 0$
- $0 \vee 0 = 0$
- $0 \oplus 0 = 0$
- $0 \leftrightarrow 0 = 1$
- $0 \rightarrow 0 = 1$
- $\neg 0 = 1$
- $0 \wedge 1 = 0$
- $0 \vee 1 = 1$
- $0 \oplus 1 = 1$
- $0 \leftrightarrow 1 = 0$
- $0 \rightarrow 1 = 1$
- $\neg 1 = 0$
- $1 \wedge 0 = 0$
- $1 \vee 0 = 1$
- $1 \oplus 0 = 1$
- $1 \leftrightarrow 0 = 0$
- $1 \rightarrow 0 = 0$
- $1 \wedge 1 = 1$
- $1 \vee 1 = 1$
- $1 \oplus 1 = 0$
- $1 \leftrightarrow 1 = 1$
- $1 \rightarrow 1 = 1$
- $P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$
- $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
- $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
- $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
- $P \oplus Q \Leftrightarrow \neg(P \leftrightarrow Q)$
- $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

Predicates, Quantified expressions, and De Morgan's Law

A **proposition** is a declarative statement that is either true or false. ($1 + 1 = 2$ and $4 < 3$ are both propositions). A **predicate** is a statement that is based on variables that when assigned will make the statement true or false. P(x) = "x is even" is a predicate where P(x) is true for all even numbers. Predicates can also be quantified, there are two types of quantification: *universal quantification*, *existential quantification*.

Definition 0.1. Universal quantification is quanitifying a predicate such that for any value, the predicate will be true. The symbol $\forall$ is read "for all". The proposition $(\forall x P(x))$ is true if for all values of x, the predicate P(x) is true.

Definition 0.2. Existential Quantification is quantifying a predicate such that there exists a value where the predicate is true. The symbol $\exists$ is read "exists". The proposition $(\exists x P(x))$ is true if there exists a value of x, such that the predicate P(x) is ture.

Example. The following are examples of quantified statements:

- $(\forall x)(x + 0 = x)$
- $(\forall x \exists y)(x + y = 0)$
- $(\exists x)(x + 5 = 20)$
- $(\exists x \forall y)(x + y > y)$

Theorem 0.3. De Morgan's Law for Quantifiers: for any predicate P(x), $\neg \forall x : P(x) \iff \exists x : \neg P(x)$, and similarly $\neg \exists x : P(x) \iff \forall x : \neg P(x)$.

What is a Set?

Sets are, informally, a collection of elements. They are characterized by the elements they contain; for a set A and any x, we can say $x \in A$ (x is in A), or $x \notin A$ (x is not in A). Sets can be defined both explicitly (by listing all elements), or implicitly (as we will see below).

Example. The following are examples of sets:

- $\{1, 5, 6\}$.
- {cat,dog,wolf}.
- The prime numbers.
- The real numbers.

Note that the ordering in a set does not matter: {cat,dog,wolf} and {dog,cat,wolf} are the same set, just written two different ways. This is in contrast to a sequence, where order does matter – the sequence (cat,dog,wolf) is not the same as (dog,cat,wolf). Also note that a set consists only of distinct elements – each element is either in the set or not – it can't be in the set twice (so the set $\{a, b, b, c, d\}$ is just the set $\{a, b, c, d\}$).

Definition 0.4. The set with no elements is called the **empty set**, and is written as $\emptyset$ or $\{\}$.

Sets that are not explicitly defined can be described verbally or written in **set-builder notation**. Set-builder notation follows the format { x | some condition applies to x }, pronounced "the set of all x such that some condition applies to x." (| can also be replaced with a colon (:), with the same meaning).

Example. Here are some examples of sets constructed using set-builder notation:

- The set of integers greater than 5 can be written as $\{x \in \mathbb{Z} | x > 5\}$ or $\{x \in \mathbb{Z} : x > 5\}$ (pronounced "all x in $\mathbb{Z}$ such that x is greater than 5").
- The prime numbers can be formally defined by $\{x \in \mathbb{N} : \nexists y \in \mathbb{N} : 1 < y < x, y|x\}$, where $y|x$ means "y divides x," or "x is divisible by y."
- $\{x + y | x, y \in \mathbb{Z}, x > 2, y < 1\}$. This can actually be proved to be the same set as $\{n | n \in \mathbb{Z}\} = \mathbb{Z}$.

Example. The following are true statements about sets using the $\in$ operation:

- $0 \in \{0, 1, 2, 3, 4\}$
- $dog \notin \{cat, bird, tiger\}$
- $3 \in \{x | x < 5\}$

Set Cardinality

The **cardinality** of a set A, written as $|A|$, can be thought of as a measure of "how big" a set is. For finite sets, this is simply the number of elements in the set.

Example. If $A = \{1, 2, 3\}$, then $|A| = 3$. If $B = \emptyset$, then $|B| = 0$.

Operations on Sets

Definition 0.5. The **union** of two sets A and B, written $A \cup B$, is the set of all x that is in either A or B. Using set-builder notation, $A \cup B = \{x | x \in A \vee x \in B\}$.

Example. $\{1, 2, 3\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$.

Definition 0.6. The **intersection** of two sets A and B, written $A \cap B$, is the set of all x that is in both A and B. Using set-builder notation, $A \cap B = \{x | x \in A \wedge x \in B\}$.

Example. $\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$.

Definition 0.7. The **Cartesian product** of two sets A and B, written as $A \times B$, is the set of pairs (p, q) such that $p \in A$ and $q \in B$. Using set-builder notation, $A \times B = \{(p, q) : p \in A, q \in B\}$.

Example. $\{1, 2, 3\} \times \{4, 5\} = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$.

Subsets and Powersets

Definition 0.8. For two sets A, B, we say $A \subseteq B$ (or "A is a subset of B") if, for all $x \in A$, $x \in B$. For such sets, we can also say $B \supseteq A$ ("B is a superset of A").

Example. $\{0\} \subseteq \{0, 1\}$.
Note that $A \subseteq A$ for any set A. If we want to convey that $A \subseteq B$ and $A \neq B$, then we can write $A \subsetneq B$ ("A is a proper subset of B"). Authors vary in their usage of the symbol $\subset$ (which could mean either a subset or a proper subset), so this symbol should usually be avoided for clarity.

Definition 0.9. The **powerset** of a set A, or $\mathcal{P}(A)$, is the set of all subsets of A.

Example. $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Functions

A function $f : A \to B$ (pronounced "f taking A to B" or "f from A to B") is a subset of $A \times B$ satisfying the following. $f : A \to B$ is a function precisely when each element $x \in A$ is matched to one value $f(x) \in B$.

Injections, Surjections, and Bijections

Definition 0.10. A function is called **injective** if f maps distinct elements of its domain to distinct elements. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

Definition 0.11. A function is called **surjective** if f maps an element x to every element y. For every y, there is an x such that $f(x) = y$.

Definition 0.12. A function is called **bijective** if it is both injective and surjective.

Theorem 0.13. The composition of injective functions is also injective.

Theorem 0.14. The composition of surjective functions is injective.

Corollary 0.15. The composition of bijective functions is bijective.

Proof Techniques

Proof by **Contradiction** assumes that the statement to be proved is false, and arrives at a contradiction, thus concluding the statement was true. It is often applied to statements of the form $P \Rightarrow Q$. Here's an example.

Theorem 0.16. If $3n + 2$ is odd, then n is odd.

Proof. Assume for sake of contradiction that $3n + 2$ is odd, and n is even.
Because n is even, there is an integer k such that $n = 2k$.
This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. We can define $t = 3k + 1$ and thus $3n + 2 = 2t$ which implies that $3n + 2$ is even. Thus we have arrived at a contradiction becuase $3n + 2$ cannot be both odd and even.
So it must be true that if $3n + 2$ is odd, then n is odd. ■

Proof by **Contraposition** is often confused with proof by contradiction. To prove $P \Rightarrow Q$ by contraposition, assume $\neg Q$ and derive that this must mean $\neg P$. This proves that $\neg Q \Rightarrow \neg P$ which is equivalent to $P \Rightarrow Q$. Example:

Theorem 0.17. if x^2 is even, then x is even.

Proof. Assume that x is odd. The product of two odd numbers is odd, thus $x \cdot x = x^2$ is odd. So x^2 is not even.
Therefore, if x^2 is even, then x is even. ■

Induction is another common proof technique. To prove that P(n) is true for all positive integers n, where P(n) is a propositional function, we complete two steps:

(1) Basis Step: We verifiy that P(1) is true.

(2) Inductive Step: We show that the conditional statement $P(k) \to P(k+1)$ is true for all postive integers k. That is, we assume $P(k)$ is true (called "the inductive hypothesis"), and prove that $P(k + 1)$ is also true.

Definition 0.18. The principle of mathematical induction: $(P(1) \wedge \forall k(P(k) \Rightarrow P(k + 1))) \Rightarrow \forall n \geq 1, P(n)$.

The above can be generalized to proofs for all nonnegative integers ≥ 0 (or any other starting point), simply by adjusting the basis case to prove $P(0)$. Here is an example.

Theorem 0.19. $1 + 2 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1$ for all $n \geq 0$.

Proof. Let $P(n)$ be the proposition that $1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$ for the integer n
Basis Step: $P(0)$ is true because $2^0 = 1 = 2^1 - 1$. This completes the basis step.
Inductive Step: We assume that $P(k)$ is true for an arbitrary nonnegative integer k.
$1 + 2 + 2^2 + ... + 2^k = 2^{k+1} - 1$
We add 2^{k+1} to both sides of the above equation.
$1 + 2 + 2^2 + ... + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1}$
$1 + 2 + 2^2 + ... + 2^k + 2^{k+1} = 2 \cdot 2^{k+1} - 1$
$1 + 2 + 2^2 + ... + 2^k + 2^{k+1} = 2^{(k+1)+1} - 1$
Thus if $P(k)$ is true then $P(k + 1)$ is true.
By mathematical induction we know that $P(n)$ is true for all n.
Thus, $1 + 2 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1$ ■

Strong induction strengthens the inductive hypothesis to assume $P(1) \dots P(k)$ (rather than just $P(k)$), and uses it to prove $P(k+1)$. This is very useful when $P(k+1)$ depends on some combination of $P(1), P(2), ..., P(k)$

Definition 0.20. The principle of strong mathematical induction: $(P(1) \wedge \forall k([P(1) \wedge P(2) \wedge ... \wedge (P(k))] \Rightarrow P(k+1))) \Rightarrow \forall n P(n)$