COMS W3261 : Discrete Math review

Anum Ahmad, William Pires

These notes are based on from Cyrus Illick and Walt McKelvie (2022).

1 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. We're here to help you!

2 Boolean Logic

We use 1 for TRUE and 0 for FALSE. We use letters such as (P, Q) to denote variables (a variable takes value 0 or 1). The three basic Boolean logic rules are $(\neg)$ = NOT, $(\wedge)$ = AND, $(\vee)$ = OR,

Example 1. The following are examples of boolean operations:

1. $0 \wedge 0 = 0$
2. $0 \wedge 1 = 0$
3. $1 \wedge 0 = 0$
4. $1 \wedge 1 = 1$
5. $0 \vee 0 = 0$
6. $0 \vee 1 = 1$
7. $1 \vee 0 = 1$
8. $1 \vee 1 = 1$
9. $\neg 1 = 0$
10. $\neg 0 = 1$

A **proposition** is a declarative statement that is either true or false. ($1 + 1 = 2$ and $4 < 3$ are both propositions). This leads us to $(\rightarrow)$ = Implies, and $(\leftrightarrow)$= Equivalent.

- $A \rightarrow B$ is read as "If A, then B". For instance, "If it rains, then the grass is wet".

  $A \rightarrow B$ is the same to $\not{A} \vee B$.

  So, $A \rightarrow B$ is true whenever B is true or A is false. In particular, if A is true B must be true. But if B is true and A is false, that's ok.

  For instance: "If $1 + 1 = 3$, then $1 + 1 = 2$" is a true statement. Even if both A and B are false, the statement is true. So, "If $\sqrt{1} = 2$, then $1 + 1 = 3$" is also a true statement.

- $A \leftrightarrow B$ is read as "A if and only if B". For instance, "A triangle is a right triangle if and only if it has a 90° angle".

  $A \leftrightarrow B$ is true whenever both A and B are true, or both they are both false.

  $A \leftrightarrow B$ is the same as: $(A \rightarrow B)$ AND $(B \rightarrow A)$.

- **Converse:** The converse of $A \rightarrow B$ is $B \rightarrow A$. Note that they are not the same thing ! For instance "If a quadrilateral is a square, all its angles are 90° angle" (this is a true statement).

The converse is "If all the angles of a quadrilateral are 90° degrees, then it's a square" (this is false!).

In this class, you will see a lot of theorems of the form "If A then B". Make sure that you don't use "If B then A" as it might not always be true.

- **Contrapositive:** The contrapositive of $A \to B$ is $\neg B \to \neg A$. In particular, these two statements have the same truth value. That is:

$$(A \to B) \leftrightarrow (\neg B \to \neg A).$$

For instance "If a language L is regular, then there is a DFA for L". The contrapositive is "If there is no DFA for L, then L isn't regular".

If in class you learnt "If A then B", you can always use "If $\neg B$, then $\neg A$".

A small note. Sometimes in a **definition** we will a "if A then B", instead of "A if and ony if B".

For instance "If L is a regular language, then there's a DFA that recognizes L". Since this is the definition of a regular language, we really mean to say "L is a regular language *if and only if* there's a DFA that recognizes L".

In this case, the converse of the statement "If there's a DFA that recognizes L, then L is regular" is true, because that's just the other direction of the iff.

If you're ever unsure if a statement in class is supposed to be an if and only if, please ask us!

3 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 2. The following are examples of sets:

1. $\{1, 5, 6\}$.
2. {cat,dog,wolf}.
3. $\{1, 2, \{\}, \{1, 2\}\}$ is a set that contains 2 integers, and two sets! A set can contain elements of different "types".
4. $\mathbb{N}$ is the set $\{0, 1, 2, 3, 4, \ldots\}$, of all natural numbers.
5. $\mathbb{Z}$ is the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of integers.
6. $\mathbb{R}$ is the set of real numbers.

From the above you can see some sets are *finite* (you can count the number of elements), and some are *infinite*. We will define and discuss infinitely countable sets a bit later in the class.

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

Sometimes we will a specific notation for sets. For instance we'll write as set like this :

$$\{x \mid \text{some condition applies to x}\}$$

The above is read as "the set of all x such that some condition applies to x.". Sometimes, we write : instead of |. So we'd write:

$$\{x \ : \ \text{some condition applies to x}\}$$

There is no difference between the two! It's up to you to pick whatever notation you prefer.

Example 3. Here are some examples of sets constructed using set-builder notation:

1. The set of integers greater than 5 can be written as $\{x \in \mathbb{Z} \mid x > 5\}$ or $\{x \in \mathbb{Z} \ : \ x > 5\}$ (pronounced "all x in $\mathbb{Z}$ such that x is greater than 5").
2. The prime numbers can be formally defined by

   $$\{x \in \mathbb{N} \ : \ \text{there doesn't exists } y \in \mathbb{N} \text{ with } 1 < y < x \text{ and } y \text{ divides } x\}.$$

   In particular this is read as "The set of x in $\mathbb{N}$ such that there doesn't exist a natural number y, with $1 < y < x$ and y divides x.

Example 4. The following are true statements about sets using the $\in$ operation:

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

3.1 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.

For instance if $A = \{1, 2, 3\}$, then $|A| = 3$ and if $B = \{1, 3, 1, 2, \{\}\}$ then $|B| = 4$. If $C = \emptyset$, then $|C| = 0$.

We will discuss the cardinality of infinite sets later in class.

3.2 Operations on Sets

Definition 2. 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, $A \cup B = \{x \mid x \in A \vee x \in B\}$.

For example : $\{1, 2, 3\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$.

Definition 3. 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, $A \cap B = \{x \mid x \in A \wedge x \in B\}$.

For example : $\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$.

Definition 4. 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, $A \times B = \{(p, q) : p \in A \text{ and } q \in B\}$.

For example: $\{1, 2, 3\} \times \{4, 5\} = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$.

Definition 5. The **set difference** of two sets A and B, denoted $A \setminus B$ is the set of elements in A but not in B. That is, $A \setminus B = \{x : x \in A \wedge x \notin B\}$.

For instance : $\{1, 2, 3\} \setminus \{2, 4, 5, 6\} = \{1, 3\}$. And $\{2, 4, 5, 6\} \setminus \{1, 2, 3\} = \{4, 5, 6\}$.

3.3 Subsets and Powersets

Definition 6. For two sets A, B, we say $A \subseteq B$ (or "A is a subset of B") if :

$$\text{For all } x \in A, \text{ we have that } x \in B$$

. For such sets, we can also say $B \supseteq A$ ("B is a superset of A").

Example 5.

1. $\{0\} \subseteq \{0, 1\}$.
2. $\mathbb{N} \subseteq \mathbb{Z}$.
3. For any set S, we have $\emptyset \subseteq S$.

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").

Often a problem will require to look at all the subsets of size k of some set.

If you have a set with n elements, the number of subsets of size k is denoted $\binom{n}{k}$. We have

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Definition 7. The **powerset** of a set A, or $\mathcal{P}(A)$, is the set of all subsets of A.

For example: $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

The following will be probably be useful at some point : If $|A| = k$, then $|\mathcal{P}(A)| = 2^k$.

4 Predicates, Quantified expressions, and De Morgan's Law

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 8. Universal quantification is quantifying a predicate such that for any value, the predicate will be true. The symbol $\forall$ is read "for all". The proposition $(\forall x \in S, P(x))$ is true if **for all** values $x \in S$, the predicate $P(x)$ is true.

Definition 9. Existential Quantification is quantifying a predicate such that there exists a value in a set S where the predicate is true. The symbol $\exists$ is read "exists". The proposition $(\exists x \in SP(x))$ is true if there exists **at least one** value $x \in S$, such that the predicate $P(x)$ is true.

Example 6. The following are examples of quantified statements:

1. $(\forall x \in \mathbb{R})(x + 0 = x)$. "For all real numbers x, $x + 0 = x$".
2. $(\exists x \in \mathbb{N})(x + 5 = 20)$. "There exists a natural number x such that $x + 5 = 20$".
3. $(\forall x \in \{1,2\}\ \exists y \in \{1,2,-1,-2\})(x + y = 0)$. "For all $x \in \{1,2\}$, there exists a $y \in \{1,2,-1,-2\}$ such that $x + y = 0$."

4. $(\exists x \in \{-1, 0, 1, 2\}\ \forall y \in \mathbb{R})(x + y > y)$. "There exists $x \in \{-1, 0, 1, 2\}$ such that for all real number y, $x + y > y$."

In the last two examples, the quantifiers are nested.

In particular in the statement : $(\forall x \in \{1, 2\}\ \exists y \in \{1, 2, -1, -2\})(x + y = 0)$ given x one picks y to be $-x$. In particular, y is allowed to depend on x.

The order of quantifier matters ! For instance $(\forall x \in \mathbb{R}\ \exists y \in \mathbb{R})(x + y = 0)$ is true, but $(\exists y \in \mathbb{R}\ \forall x \in \mathbb{R})(x + y = 0)$ is false. You can't swap the order as it changes the meaning of statements.

Theorem 1. [De Morgan's Law for Quantifier] For any predicate P(x) :

$$\neg\left(\forall x \in S : P(x)\right) \leftrightarrow \left(\exists x \in S : \neg P(x)\right)$$

and similarly

$$\neg\left(\exists x \in S : P(x)\right) \leftrightarrow \left(\forall x \in S : \neg P(x)\right)$$

.

So, when negating a quantified statement, you flip $\forall$ to $\exists$ and vice versa. And then negate $P(x)$.

For instance:

- The negation of $(\forall x \in \mathbb{N})(x + 0 = x)$ is $(\exists x \in \mathbb{N})(x + 0 \neq x)$.
- When dealing with nested quantifiers, you flip all of them, and then negate the predicate. For instance the negation of

  $$(\exists x \in \{-1, 0, 1, 2\}\ \forall y \in \mathbb{R})(x + y > y)$$

  is

  $$(\forall x \in \{-1, 0, 1, 2\}\ \exists y \in \mathbb{R})(x + y \leq y)\,.$$

5 Strings and languages

Definition 10. An alphabet Σ is a *finite* set of symbols.

For instance: $\Sigma = \{0, 1\}$ or $\Sigma = \{a, b, c\}$ are alphabets.

Definition 11. A string s over Σ is a **finite** sequence of symbols from Σ. The length of a string $|s|$ is denoted $|s|$, this is the number of symbols in it.

For instance: If $\Sigma = \{0, 1\}$, then 00 (which has length 2) and 111001 (length 6) are strings. But $000\ldots$ isn't a string since this isn't finite.

A special string is the empty string ϵ. This is the (only) string of length 0 [1].

If s has length n, we can write $s = s_1 s_2 \ldots s_n$ where each $s_i \in \Sigma$.

Given a string s its reverse s^R is s in the reverse order. So $s^R = s_n \ldots s_2 s_1$.

Given two strings s, t we denote by $s \circ t$ their concatenation. Sometimes, we omit the $\circ$ and just write st.

For instance: $11 \circ 010 = 11010$ and $\epsilon \circ 00 = 00$

Given an alphabet Σ, we denote by Σ^k the set of all strings of length k over Σ. And we denote :

$$\Sigma^* = \cup_{i=0}^{\infty} \Sigma^i = \{ \text{ all strings over } \Sigma\}$$

For instance: If $\Sigma = \{0, 1\}$, we have $\Sigma^0 = \{\epsilon\}$,$\Sigma^1 = \{0, 1\}$, $\Sigma^2 = \{00, 01, 10, 11\}$.

Definition 12. A language L over alphabet Σ is a set of string $L \subseteq \Sigma^*$

In particular, a language is just a set. It can be finite, infinite. We can take the union of two language $L \cup L' := \{s \ : \ s \text{ is a string in } L \text{ or in } L'\}$, or their intersection etc...

Definition 13. The complement of language L over alphabet Σ denoted L^c (or also $\overline{L}$) is the set all strings over Σ that are not in L. That is:

$$L^c = \Sigma^* \setminus L = \{s \in \Sigma^* \ : \ s \notin L\}$$

Here are some examples

[1] ϵ would correspond to the string "" in Python.

1. $L = \{0, 1, 000111\}$ is a *finite* language. We have $0 \in L$, but $\epsilon \notin L$.

2. $L = \{0, 00, 000, \ldots\}$ is an *infinite* language. But note that every string in L is finite, so for any $s \in L$, we have $|s| = k$ for some integer k.

3. $\{\}$ is the empty language, it also denoted $\emptyset$. For any string s, we have $s \notin \emptyset$ (in particular $\epsilon \notin \emptyset$).

6 Proof Techniques

If you're not sure how to start proving a statement, you can always refer to these templates for inspiration.

Proof Template 1 (Proving "For all $x \in S$, P(x) is true"). To prove a statement of this form, where P(x) is a predicate. You need to proceed as follow:

- Let x be an arbitrary element of S.
- Prove that for x the statement is true.

Make sure you don't pick a specific x to work with.

Here's an example.

Example 7. For all odd integers x, x^2 is odd.

Proof. Let x be an odd integer. Then $x = 2k + 1$ for some integer k. So $x^2 = 4k^2 + 4k + 1$. In particular, $x^2 = 2(2k^2 + 2k) + 1$. So x^2 is odd. □

In particular, in the above you can't say "Let $x = 5$, then $x^2 = 25$ which is odd". This is bad since you're proving the statement for a specific number x, not all odd integers.

Similarly, if you learn a statement of the form "If A, then there exists x such that...". Make sure you don't pick a specific x, as this is a very common mistake. For instance consider the following:

Theorem 2. "If L is regular, then there exists $k \geq 1$, such that L has a DFA with k states".

Now, if you want to use theorem in a proof, you can't say "By Theorem 2, since $L = \{0, 00, 000, \ldots, \}$ is regular it has a DFA with $k = 2$ states". The theorem doesn't say anything about what value k has, so you can't pick $k = 2$.

Proof Template 2 (Proving "The exists an $x \in S$, with P(x) true"). To prove a statement of this form, where P(x) is a predicate. You need to proceed as follow:

- Pick a specific $x \in S$.
- Prove that for the x you picked $P(x)$ is true.

Here it's ok to pick a specific value for x.

Here's an example.

Example 8. There is a language L over $\{0, 1\}$ such that L has a DFA with one state.

Proof. Let $L = \Sigma^*$. Then the DFA for L has one state q_0, such that q_0 is the start state and an accept state.

The transitions function is just $\delta(q_0, 0) = \delta(q_0, 1) = q_0$. □

Proof Template 3 (Proving "If P then Q")**.** To prove a statement of this form, the easiest way to is to say "Assume P is true". And then derive that Q has to be true.

Example 9. If n is even, then n^2 is even.

Proof. Assume that n is even. Then we can write $n = 2m$ for some integer m. So $n^2 = 4m^2 = 2 \times (2m^2)$. So 2 divides n^2, which means n^2 as to be even. □

However when having to prove $P \to B$, there are other ways to do. Here are the two most common ones.

Important to remember: The negation of $P \to B$ is $P \wedge \neg P$.

Proof Template 4 (Proof by **Contradiction**)**.** A proof by **Contradiction** starts by assuming 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 $P \Rightarrow Q$.

Example 10. 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. □

Another option, is a proof by contraposition. Do not confuse this with a proof by contradiction.

Proof Template 5 (Proof by **Contraposition**)**.** In a proof by **Contraposition**, instead of proving $P \Rightarrow Q$ directly, we prove its contrapositive: $\neg Q \Rightarrow \neg P$.
A prove of $P \Rightarrow Q$ by contraposition, goes like this: Say "Assume $\neg Q$ is true" and derive that this $\neg P$ is true.

Example:

Example 11. If x^2 is even, then x is even.

Proof. The contrapositive of this statement, is "If x is odd, then x^2 is odd". Hence the proof goes like this:

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. □

A lot of times, we'll ask you to prove $P \leftrightarrow Q$. This is how you should proceed.

Proof Template 6 (Proving "P if and only if Q")**.** To prove $P \leftrightarrow Q$ you must prove :

- $P \to Q$,
- and $Q \to P$.

Do not forget to prove **both** statements. Also, you can use different techniques for each.

For example, to prove $P \leftrightarrow Q$ you can prove $P \to Q$, and $\neg P \to \neg Q$ (the contrapositive of $Q \to P$).

Induction is another common proof technique.

Proof Template 7 (Proof by **Induction**)**.** To prove that $P(n)$ is true for all positive integers n 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.

- You can do a proof by induction for all integers ≥ 0, simply by adjusting the basis case to prove $P(0)$.
- Another concept is "strong induction". The Basis Step stays the same. But in the Inductive Step, we want to show:

$$(\forall i \in \{1, \ldots, k\},\, P(k)) \to P(k+1)\,.$$

So we assume $P(i)$ is true for $1 \leq i \leq k$, and then prove that $P(k+1)$ is also true.

Example 12. $1 + 2 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1$ 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, $1 + 2 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1$ □