Study Guide

ECS 20: Discrete Math for CS

Computer Science Tutoring Club
Fall 2017

December 19, 2018

Contents

How to Use This Study Guide

This study guide is meant to help you review topics before the midterms and the final. Please do not use this study guide as your main source of preparation for exams.

This study guide goes over each and every topic in ECS 20. I have previously taken ECS 20 with Professor Koehl, so I have a pretty good idea about exams and the material covered. Hence this study guide is tailor made for students in Professor Patrice Koehl's ECS 20. If you are not in Professor Koehl's ECS 20 and still wish to use this study guide, please go ahead and do so. Please be forewarned that some topics might not covered in this study guide that other professors might cover (for example: Graph Theory is not covered in this study guide).

Each chapter in the study guide reviews important concepts and theorems. Furthermore, I have gone ahead and solved some questions that have been asked on previous midterms. Additionally, I have added a few questions for you to try out on your own (**No solutions have been provided**).

I sincerely hope that this study guide helps you better prepare for the midterms and the final! Good luck on this challenging course.

Aakash Prabhu (Class of 2019)
President, *Computer Science Tutoring Club*

Chapter 1

Math Symbols, Notations, and Identities

1.1 Symbols and Notations

Here are the symbols and notations that you must absolutely know!

1.1.1 Sets of Numbers

$\mathbb{N}$ = Set of all Natural Numbers.
$\mathbb{Z}$ = Set of all Integers.
$\mathbb{Q}$ = Set of all Rational Numbers.
$\mathbb{R}$ = Set of all Real Numbers.
$\mathbb{C}$ = Set of all Complex Numbers.

1.1.2 Propositional Logic

$\neg P$ = Negation of the proposition, P.
$P \wedge Q$ = Conjunction of the propositions P *and* Q.
$P \vee Q$ = Disjunction of the propositions P *and* Q.
$P \oplus Q$ = P XOR Q (Exclusive Or).
$P \rightarrow Q$ = "If P, then Q" (Conditional).
$P \leftrightarrow Q$ = "P if and only if Q" (Biconditional).
$P \Leftrightarrow Q$ = P is equivalent to Q.

1.1.3 Set Theory

$\emptyset$ = Empty Set.
$x \in \mathbb{Q}$ = x belongs to a rational number.
$A \subset B$ = Set A is a subset of set B.
$S = \{1, 2, 3, 4\}$ = An example of a set in roster form.
$S = \{x \mid 1 \leq x \leq 4, x \in \mathbb{Z}\}$ = An example of a set in set-builder form.
$A \cup B$ = A union B.
$A \cap B$ = A intersection B.
$A - B$ = A minus B (Set difference).
$\overline{A}$ = Complement of A.
$\mid A \mid$ = Number of elements in A (Cardinality).

1.1.4 Functions

$\lceil x \rceil$ = Ceiling of x.
$\lfloor x \rfloor$ = Floor of x.
$O(f(x))$ = Big-O of the function *f*.
$\Omega(f(x))$ = Big-Omega of the function *f*.
$\Theta(f(x))$ = Big-Theta of the function *f*.

1.1.5 Number Theory

a/b = a divides b.
$a \equiv b[m]$ = a is congruent to b modulo m.

1.1.6 Miscellaneous

$\sum_{i=1}^{n} i$ = Sum of first n terms.
$\prod_{i=1}^{n} i$ = Product of first n terms. $n!$ = n factorial.
$\forall x \in \mathbb{Z}, P(x)$ = For all x in the set of integers, P(x) is true.
$\exists x \in \mathbb{Z}, P(x)$ = There exists an x such that P(x) is true.

1.2 Important Identities

I have compiled a bunch of identities that are going to prove to be very useful for proofs or problem solving. Again, I have broken them down into chapters for better reference [1].

1.2.1 Simple Mathematical Identities

$(a+b)^2 = a^2 + 2ab + b^2$
$(a-b)^2 = a^2 - 2ab + b^2$
$a^2 - b^2 = (a+b) \times (a-b)$
$a^m \times a^n = a^{m+n}$
$(a^m)^n = a^{mn}$
$\log(a \times b) = \log(a) + \log(b)$
$\log(a^b) = b \times \log(a)$

1.2.2 Propositional Logic

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

1.2.3 Functions

$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
$\lfloor -x \rfloor = -\lceil x \rceil$
$\lceil -x \rceil = -\lfloor x \rfloor$
$\lfloor x + n \rfloor = \lfloor x \rfloor + n$, for some $n \in \mathbb{Z}$
$\lceil x + n \rceil = \lceil x \rceil + n$, for some $n \in \mathbb{Z}$
$(\exists n \in \mathbb{Z})(\exists \epsilon \in \mathbb{R}) \lfloor x \rfloor = n + \epsilon$, where $0 \leq \epsilon \leq 1$
$f(x) = O(g(x)) \rightarrow (\exists k \in \mathbb{Z})(\exists c \in \mathbb{R}^+)(\forall x > k)[f(x) \leq c \times g(x)]$
$f(x) = \Omega(g(x)) \rightarrow (\exists k \in \mathbb{Z})(\exists c \in \mathbb{R}^+)(\forall x > k)[f(x) \geq c \times g(x)]$
$f(x) = \Theta(g(x)) \rightarrow [f(x) = O(g(x))] \wedge [f(x) = \Omega(g(x))]$

[1] I haven't included basic conjunctions and disjunctions of propositions because you should be knowing them by now!

1.2.4 Number Theory

$a/b \rightarrow (\exists c \in \mathbb{Z})[a = b \times c]$
$a/b \wedge a/c \rightarrow a/(b + c)$
$a/b \wedge b/c \rightarrow a/c$
$\gcd(a, b) = am + bn$, for some $m, n \in \mathbb{Z}$ (**Bezout's Identity**)
$\gcd(a, b) \times \mathrm{lcm}(a, b) = a \times b$
$a \equiv b[m] \wedge c \equiv d[m] \rightarrow (a + b) \equiv (c + d)[m]$
$a \equiv b[m] \wedge c \equiv d[m] \rightarrow (ab) \equiv (cd)[m]$
If p is a prime number, then $a^p \equiv a[p]$ (**Fermat's Little Theorem**)
If p is a prime number and p/ab, then $p/a \vee p/b$ (**Euclid's Identity**)

1.2.5 Counting

$| A \cup B | = | A | + | B | - | A \cap B |$
$P(n, r) \frac{n!}{(n-r)!}$ (**Permutations**)
$C(n, r)$ or $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ (**Combinations**)

Chapter 2

Propositional Logic

Definition. A **proposition** is a statement with exactly one truth value.
Definition. Two propositions are said to be **equivalent** if they have the same truth table.
Definition. A **tautology** is a statement that is always true.
Definition. A **contradiction** is a statement that is always false.

2.1 Truth Tables and Logical Equivalences

If you are given a proposition and asked to check if it is a tautology or a contradiction, here are two different ways to proceed:

1. Construct a truth table for the given proposition.
2. Use logical equivalences.

Question. Is this a tautology or a contradiction?

$$[p \wedge (q \wedge r)] \rightarrow [(((r \wedge p) \wedge q) \vee q)]$$

Solution. 1 - Truth Table: For readability, let us define $\alpha = p \wedge (q \wedge r)$ and let us define $\beta = (((r \wedge p) \wedge q) \vee q)$

Table 2.1: Truth Table

p	q	r	$q \wedge r$	α	$(r \wedge p)$	$((r \wedge p) \wedge q)$	β	$\alpha \rightarrow \beta$
T	T	T	T	T	T	T	T	**T**
T	T	F	F	F	F	F	T	**T**
T	F	T	F	F	T	F	F	**T**
T	F	F	F	F	F	F	F	**T**
F	T	T	T	F	F	F	T	**T**
F	T	F	F	F	F	F	T	**T**
F	F	T	F	F	F	F	F	**T**
F	F	F	F	F	F	F	F	**T**

Since $\alpha \rightarrow \beta$ is always true, this is an example of a tautology!

Solution. 2 - Logical Equivalences:

$$
\begin{aligned}
& [p \wedge (q \wedge r)] \rightarrow [(((r \wedge p) \wedge q) \vee q)] \\
\iff & \neg[p \wedge q \wedge r] \vee [((r \wedge p \wedge q) \vee q)] \ \textbf{(Definition)} \\
\iff & \neg(p \wedge q \wedge r) \vee [(p \wedge q \wedge r) \vee q] \ \textbf{(Commutative law)} \\
\iff & [\neg(p \wedge q \wedge r) \vee (p \wedge q \wedge r)] \vee q \ \textbf{(Associative Law)} \\
\iff & T \vee q \ \textbf{(Complement Law)} \\
\iff & T(\textbf{Identity Law})
\end{aligned}
$$

Since the result is always true, the given proposition is a tautology!

Remark. As you can see, solving problems through logical equivalences is quicker, but require you to manipulate the given propositions. If you are uncomfortable doing this, please feel free to resort to Truth Tables. The same question showed up on my midterm, and I used logical equivalences to solve the problem.

2.2 Knights and Knaves

You can always expect a question on logic puzzles on the midterms and the finals. These questions are actually fun to do and are not too difficult.

You will be given a situation and you are required to use truth tables to solve the problem. Here is a sample problem (From a past midterm):

A very special island is inhabited only by Knights and Knaves. Knights always tell the truth,while Knaves always lie. You meet three inhabitants: Alex, John and Sally.Alex says, “John is a Knight if and only if Sally is a Knave”. John says, “If Sally is a Knight, then Alex is a Knight”.

Question. Can you find what Alex, John, and Sally are? Explain your answer.

Solution. Let us break down the problem:

You have three people: Alex (A), John (J), and Sally (S). Each of them are either a Knight or a Knave. Hence, we have 8 possible rows in our truth table.

Let us also break down what the people have to say:

1. Alex says, “John is a Knight if and only if Sally is a Knave," which basically means: **John is a Knight $\iff$ Sally is a Knave.**

2. John says, “If Sally is a Knight, then Alex is a Knight," which basically means: **Sally is a Knight $\implies$ Alex is a Knight.**

With this information, let us construct our truth table:

Table 2.2: Truth Table

A	J	S	Alex Says	John Says	Does This Work?
Knight	Knight	Knight	F	T	**No** - Alex is a Knight who is lying
Knight	Knight	Knave	T	T	**YES**
Knight	Knave	Knight	T	T	**No** - John is a Knave who is telling the truth
Knight	Knave	Knave	F	T	**No** -John is a Knave who is telling the truth
Knave	Knight	Knight	F	F	**No** - John is a Knight who is lying
Knave	Knight	Knave	T	T	**No** - Alex is a Knave who is telling the truth
Knave	Knave	Knight	T	F	**No** - Alex is a Knave who is telling the truth
Knave	Knave	Knave	F	T	**No** - John is a Knave who is telling the truth

From this, we can see that there is only one possible combination, that Alex and John are Knights and Sally is a Knave.

Remark. Sometimes there may be more than one possible combination that works out, in that case it is not possible to correctly determine who is who, but it is one of those correct combinations.

Remark. There’s almost always a Knights and Knaves (or a variation) question on the exams.

Remark. If you are interested in these problems, These problems are called *Smullyan’s Island Puzzles.*

2.3 Additional Exercises

Please note that there are no solutions for the following questions.

2.3.1 Logic

Question. Construct the truth table for the following proposition:

$$[p \wedge (p \to q)] \to q$$

This rule of inference is commonly referred to as *Modus Ponens*.

Question. Prove or disprove:

$$(p \to q) \Leftrightarrow (q \to p)$$

Question. Is this a tautology or a contradiction?

$$(((P \to Q) \wedge (R \to S) \wedge (P \vee R))) \to (Q \vee S)$$

You may use either Truth Tables or Logical Equivalences for this question.

This proposition is usually referred to as the *Constructive Dilemma*.

Question. Prove or disprove:

$$(p \oplus q) \Leftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$$

2.3.2 Logic Puzzles

Question. A very special island is inhabited only by Knights and Knaves. Knights always tell the truth, while Knaves always lie. You meet three inhabitants: Alex, John and Sally. Alex says, "John is a Knight, if and only if Sally is a Knave". John says, "If Sally is a Knight, then Alex is a Knight". What can you conclude from the given information?

Question. A very special island is inhabited only by knights and knaves. Knights always tell the truth, and knaves always lie. You meet three inhabitants: Alex, John and Sally. Alex says, "At least one of the following is true: that Sally is a knave or that I am a knight." John says, "Alex could claim that I am a knave." Sally claims, "Neither Alex nor John are knights." What can you conclude from the given information?

Chapter 3

Proofs and Proof Methods

Writing proofs deepens your knowledge of the subject at hand. ECS 20 is a proof heavy course and prepares you to write extensive proofs in upper division CS and Math classes. Almost 60% of your exam will be based on proofs and will test your ability to write a flawless proof. Here are three important proof methods that this chapter will cover:

- Direct Proof
- Indirect Proof (Proof by Contraposition)
- Proof by Contradiction
- Proof by Cases
- Constructive and Non-Constructive Proofs

3.1 Direct Proof

This is the most basic proof method. Here, we will be given a statement of the form $P \to Q$ and you will be asked to prove this propositional form. Here is how you could prove something directly:

Step 1 Given $P \to Q$, assume P is true.

Step 2 Using P, try to use the given information of P to arrive at Q.

Here is a simple example:

Theorem. *If a is an even integer, then $a^3 - 6a$ is even.*

Proof. Let us use a direct proof.
Assume a is an even integer.

Then,

$$\begin{aligned}
&\exists k \in \mathbb{Z}, a = 2k \\
&a^3 - 6a = (2k)^3 - 6(2k) \\
&\qquad = 8k^3 - 12k \\
&\qquad = 2(4k^3 - 6k) \\
&\qquad = 2m, \text{ where } m = 4k^3 - 6k
\end{aligned}$$

Thus, $a^3 - 6a$ is even. Therefore, if a is even, then $a^3 - 6a$ is even □

3.2 Indirect Proof (Proof by Contraposition)

Suppose we are given a statement of the form $P \to Q$. Sometimes, a direct proof might be very hard (sometimes impossible) to go about. Therefore we resort to another proof method that simplifies things. In this proof, we will try to show $\neg Q \to \neg P$ is true. By drawing out a simple truth table you can show that $P \to Q \Leftrightarrow \neg Q \to \neg P$.

Here is how you can prove something by contraposition:

Step 1 Given $P \to Q$, Assume $\neg Q$ is true.

Step 2 Using $\neg Q$, try to arrive at $\neg P$.

Here is a simple example:

Theorem. *If a^2 is even, then a is even*

Proof. Let us use an indirect proof.

Assume a is odd (Assume $\neg Q$).

Then,

$$\begin{aligned}
&\exists k \in \mathbb{Z}, a = 2k + 1 \\
&\qquad a^2 = (2k+1)^2 = 4k^2 + 4k + 1 \\
&\Leftrightarrow a^2 = 2(2k^2 + 2k) + 1 \\
&\qquad \Leftrightarrow = 2m + 1, \text{ where } m = 2k^2 + 2k
\end{aligned}$$

Therefore, a^2 is odd. Thus, we have shown that if a is odd, then a^2 is odd.

Therefore by contraposition, If a^2 is even then, a is even. □

3.3 Proof By Contradiction

Suppose we are given asked to prove a given statement, Q, a direct proof might not be feasible. Hence we resort to our last proof method to prove

statements that might look difficult to prove directly. In this proof method, we assume $\neg Q$ to be true. Suppose you are given a statement of the form $P \to Q$, then you assume $\neg(P \to Q)$, which is basically $P \wedge \neg Q$.

Here is a simple example:

Theorem. *If* $(a, b) \in \mathbb{Z}^2$*, then* $a^2 - 4b \neq 2$

Proof. Let us use a proof by contradiction. Assume $P \wedge \neg Q$ is true. Then $(a, b) \in \mathbb{Z}^2 \wedge (a^2 - 4b = 2)$ is true.

$$
\begin{aligned}
&\text{If } a^2 - 4b = 2, \text{ then} \\
&\quad a^2 = 2 + 4b \\
\iff &a^2 \text{ is even} \\
\iff &a \text{ is even } ^1 \\
\iff &\exists k \in \mathbb{Z} a = 2k \\
\iff &(2k)^2 - 4b = 2 \\
\iff &4k^2 - 4b = 2 \\
\iff &2k^2 - 2b = 1 \\
\iff &2 \times (k^2 - 2b) = 1
\end{aligned}
$$

$\Leftrightarrow$ An even integer is equal to the odd integer 1, which is a contradiction.

This contradiction arises due to our incorrect assumption that $\neg(P \to Q)$ was true.

Therefore, $P \to Q$ is true.

Thus, If $(a, b) \in \mathbb{Z}^2$, then $a^2 - 4b \neq 2$ □

3.4 Proof by Cases

This is a proof method that is always used when you do not know the constraints to a problem. Let us illustrate this with a very simple example:

Theorem. *If* a *is an integer, then* $2a + 1$ *is odd.*

Proof. Here, we do not know if a is an even or odd integer. Thus, we consider both cases and try to prove our hypothesis:

Case 1: a is even.

Then, $(\exists k \in \mathbb{Z})[a = 2k]$.

Then, $2a + 1 = 2(2k) + 1$, which is odd!

Case 2: a is odd.

Then, $(\exists k \in \mathbb{Z})[a = 2k + 1]$.

Then, $2a + 1 = 2(2k + 1) + 1$, which is also odd! □

3.5 Constructive and Non-Constructive Proofs

3.5.1 Constructive Proofs

Constructive proofs are proof methods in which a specific example is provided. These proofs are generally referred to as "*Existence Proofs*".
Let us take two separate examples to illustrate this proof method.

Example 1: Show that there exist two integers a and b such that $a+b$ and $a-b$ are both prime numbers.

Proof. We only need to show a single pair (a, b) for which $a+b$ and $a-b$ are both prime numbers.

Let us take $a = 5$ and $b = 2$.
Then, $a + b = 7$ and $a - b = 3$.
Both, 7 and 3 are prime numbers.
Thus, we found a particular pair of numbers for which the hypothesis holds. □

Example 2: Prove or disprove the following:

For all $k \in \mathbb{Z}$ greater than 2, $2k + 7$ is a prime number.

Proof. Let us try out a few numbers and see what we get:
Try $k = 2$
Then, $2k + 7 = (2 \times 2) + 7 = 4 + 7 = 11$ which is a prime number.
Try $k = 3$
Then, $2k + 7 = (2 \times 3) + 7 = 6 + 7 = 13$ which is a prime number.
Try $k = 4$
Then, $2k + 7 = (2 \times 4) + 7 = 8 + 7 = 15$ **which is NOT prime**.

Thus, we have found one example which violates the hypothesis.
Thus, the given statement is **FALSE**! □

3.5.2 Non-Constructive Proofs

This is another kind of an existence proof. In this method, we do not explicitly find a value of 'x' such that $P(x)$ is true. Instead, we show that there must exist some x for which $P(x)$ is true. This might seem like a confusing definition, so let us use this in an example:

Question. Show that there exists a pair of irrational numbers a and b such that $c = a^b$ is rational.

Remark. This is a very famous and interesting problem in the field of proofs and discrete mathematics. Let us look at the solution:

Proof. We know that $\sqrt{2}$ is irrational. Let us define $c = (\sqrt{2})^{\sqrt{2}}$.

Additionally, let us define $d = c^{\sqrt{2}}$.

Then, $d = (\sqrt{2})^{\sqrt{2}\times\sqrt{2}} = (\sqrt{2})^2 = 2$ which is rational. □

Note that we did not explicitly find the values of a and b in the above example. We simply showed that there could exist a pair of irrational numbers in which a^b could be rational.

Trivia: Did you know that there is a constructive proof for the above mentioned example? It is quite hard to find the right examples for a and b, but it is possible. I haven't included the answers, but do think about it!

Chapter 4

Set Theory

Set Theory is one of the most fundamental topics in Abstract/Discrete Mathematics. If you have ever heard about Relations, Equivalence Classes, Groups, Rings, and Fields, they are all based off Set Theory! This chapter covers the following and it is essential that you know all of it:

4.1 Definitions

Definition. Set A is said to be a **subset** of the set B if $(\forall x \in A)[x \in B]$.
Definition. The **union** of set A and set B is the set: $\{x \mid x \in A \vee x \in B\}$.
Definition. The **intersection** of A and B is the set: $\{x \mid x \in A \wedge x \in B\}$.
Definition. The **difference** of A and B is the set: $\{x \mid x \in A \wedge x \notin B\}$.
Definition. Sets A and B are said to be **equal** if $(A \subset B) \wedge (B \subset A)$.
Definition. The **complement** of A is the set: $\{x \mid x \in D \wedge x \notin A\}$, where D is the domain or universal set.
Definition. The **cardinality** of A is the number of elements in A.

4.2 Proofs

This class in particular will not test too many hard proofs in Set Theory. In fact, most proofs in this chapter will require you to construct simple direct proofs. So, let us show you an example of how proofs in set theory might look like:

Question. If A and B are two sets, show that $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof. We need to show that $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$ and $\overline{A} \cup \overline{B} \subset \overline{A \cap B}$

Let x be an arbitrary element $\in \overline{A \cap B}$

$$\begin{aligned}
&\implies x \notin A \cap B \\
&\implies \neg(x \in A \wedge x \in B) \\
&\implies x \notin A \vee x \notin B \\
&\implies x \in \overline{A} \cup \overline{B} \\
&\implies \overline{A \cap B} \subset \overline{A} \cup \overline{B}
\end{aligned}$$

Let $x \in \overline{A} \cup \overline{B}$

$$\begin{aligned}
&\implies x \in \overline{A} \vee x \in \overline{B} \\
&\implies \neg x \in A \vee \neg x \in B \\
&\implies \neg(x \in A \wedge x \in B) \\
&\implies \neg(x \in A \cap B) \\
&\implies x \in \overline{A \cap B} \\
&\implies \overline{A} \cup \overline{B} \subset \overline{A \cap B}
\end{aligned}$$

Thus, $\overline{A \cap B} = \overline{A} \cup \overline{B}$. □

You also need to know set identities but they are the same as the basic identities of propositional logic, so I haven't included them in this section.

I have also skipped the section of Generalized Unions and Intersections as they are based on the basic definition of union and intersection of sets. Otherwise, that is pretty much it with regards to set theory!

Chapter 5

Functions

5.1 Basics

A function f, from A to B is an assignment of exactly one element of B to each element in A.

Example. Let f be a function such that $\forall x \in \mathbb{R}$, $f(x) = x^2$. You can observe that for any desired value of x, there is only one unique mapping to $f(x)$. The reverse is not always true!

Definition. A function is considered **one-to-one or injective** if $f(x) = f(y) \Leftrightarrow x = y$
Definition. A function from A to B is **onto or surjective** if $\forall y \in B$ $\exists x \in A$ such that $f(x) = y$.
Definition. A function that is both one-to-one and onto is called a **bijection**. A function that is bijective implies that an inverse for the function exists!

Example. Consider the function $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = 12x + 5$. Show that f has an inverse and find its inverse.

Solution. First we have to show that f is injective.

Let us assume that $f(x_1) = f(x_2)$.

Then, $12x_1 + 5 = 12x_2 + 5 \Leftrightarrow 12x_1 = 12x2 \Leftrightarrow x_1 = x_2$. Thus, f is injective!

Next, we have to show that f is surjective.

Let $f(x) = y$. Then, $y = 12x + 5$.

Then, $x = \frac{y-5}{12}$. One can observe that for any real number y, there exists a real number x such that $x = \frac{y-5}{12}$. Thus, f is surjective!

Since f is a bijection, the inverse of f $f^{-1}(x) = \frac{x-5}{12}$

5.2 Floor and Ceiling Functions

Definition. The **floor** of any real number returns the greatest integer that is less than or equal to the real number.

Definition. The **ceiling** of any real number returns the smallest integer that is greater than or equal to the real number.

Example.

$$\lfloor 2.5 \rfloor = 2, \lfloor -3.4 \rfloor = -4, \lfloor 7 \rfloor = 7$$
$$\lceil 2.5 \rceil = 3, \lceil -3.4 \rceil = -3, \lceil \pi \rceil = 4$$

5.2.1 Proofs regarding Floor and ceiling functions

I think it would be quite redundant to show proofs regarding floor and ceiling functions. Questions that are similar to the ones shown in the *lecture notes* generally show up on the midterms/final. Thus, I have omitted this one topic as you can just read it up from the notes.

5.3 Growth of Functions

Often times, your task would be to determine the running time of an algorithm that you just developed. These running times are represented as $O()$ (Big Oh), $\Omega()$ (Big Omega), and $\Theta()$ (Big Theta) respectively.

5.3.1 Big-O Notation

The Big-O Notation is often used to represent the worst case analysis. Think of Big-O as an upper bound for functions. The function f(x) is O(g(x)) if $[f(x) \leq c \times g(x)]$ for all x > k, where c is a positive constant.

Example. Show that $x^2 + 5x + 3$ is $O(x^2)$

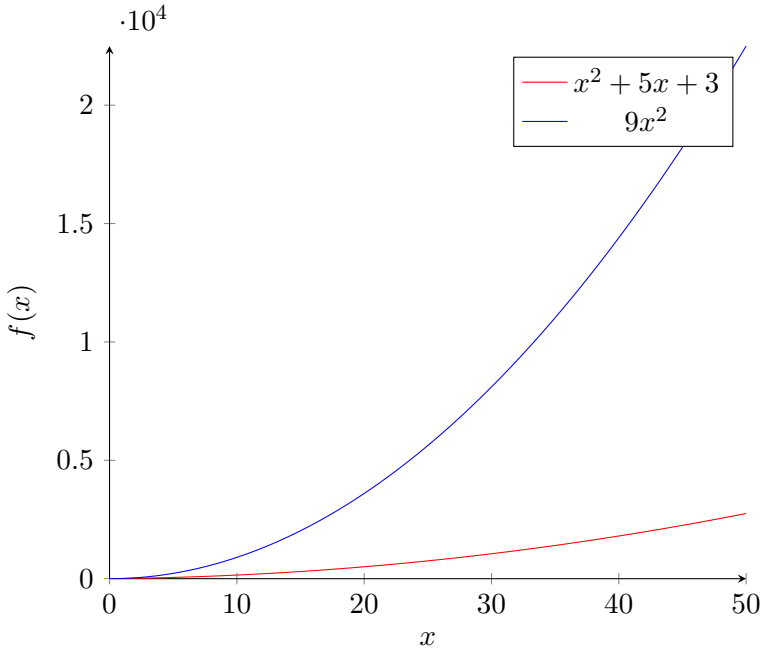
Solution. In order for $x^2 + 5x + 3$ to be $O(x^2)$, $x^2 + 5x + 3 \leq cx^2$.

We know that if $x > 1$ then, $5x \leq 5x^2$ and $3 \leq 3x^2$.

Adding these up we get: $x^2 + 5x + 3 \leq x^2 + 5x^2 + 3x^2 \leq 9x^2$.

Thus by selectively choosing $k = 1$ and $c = 9$, we can show that x^2+5x+3 is $O(x^2)$.

For further verification and understanding, let us graph the functions $x^2 + 5x + 3$ and $9x^2$.



As you can see, $x^2 + 5x + 3$ is never greater than $9x^2$.

5.3.2 Big-Omega Notation

The Big-Omega Notation is often used to represent the best case analysis. Think of Big-Omega as an lower bound for functions. The function f(x) is $\Omega(g(x))$ if $[f(x) \geq c \times g(x)]$ for all x > k, where c is a positive constant.

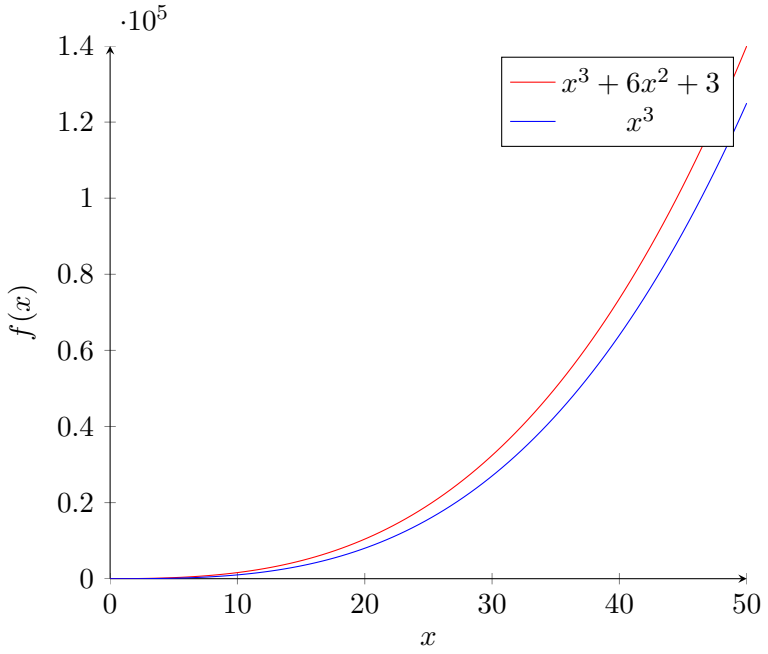
Example. Show that $x^3 + 6x^2 + 3$ is $\Omega(x^3)$

Solution. In order for $x^3 + 6x^2 + 3$ to be $\Omega(x^3)$, $x^3 + 6x^2 + 3 \geq cx^3$.

We know that if $x > 1$ then, $x^3 + 6x^2 + 3 \geq x^3$.

Thus by selectively choosing $k = 1$ and $c = 1$, we can show that $x^3 + 6x^2 + 3$ is $\Omega(x^3)$.

For further verification and understanding, let us graph the functions $x^3 + 6x^2 + 3$ and x^3.



As you can see, $x^3 + 6x^2 + 3$ is always greater than x^3.

5.3.3 Big-Theta Notation

The Big-Theta Notation is often used to represent the average case analysis. Think of Big-Theta as a tight bound for functions. The function f(x) is $\Theta(g(x))$ if f(x) is $O(g(x))$ and if f(x) is $\Omega(g(x))$

Example. Show that $x^2 + 4x + 7$ is $\Theta(x^2)$

Solution. First, we have to show that $x^2 + 4x + 7$ is $O(x^2)$.

Then, $x^2 + 4x + 7 \leq cx^2$.

We know that for all $x > 1$, $4x \leq 4x^2$ and $7 \leq 7x^2$. Adding these up, we can say that $x^2 + 4x + 7 \leq 12x^2$. Thus by selectively choosing $k = 1$ and $c = 12$ we can conclude that $x^2 + 4x + 7$ is $O(x^2)$.

Next, we have to show the Big-Omega relation between these two functions.

We know that for all $x > 1$ $x^2 + 4x + 7 \geq x^2$

Thus by selectively choosing $k = 1$ and $c = 1$ we can conclude that $x > 1$ $x^2 + 4x + 7$ is $\Omega(x^2)$.

Thus $\forall x > 1$ we can infer that:

$$x^2 \leq x^2 + 4x + 7 \leq 12x^2$$

Thus, $x^2 + 4x + 7$ is $\Theta(x^2)$

5.3.4 Why do we need all this?

Often times in algorithm analysis, you deal with large chunks of data. If, for example, $n = 10$ where n is the number of elements, then it doesn't really matter how good or bad our Big-Oh is. What if $n = 1,000,000$? Then n^2 and n^3 would be significantly different. This is why we study the growth of these functions. These notations are also sometimes referred to as time complexities. You will learn about time complexities extensively in ECS 60 and ECS 122A.

Chapter 6

Number Theory