CS 38/138: An Introduction to Algorithms

Spring 2016

Notes

Chinmay Nirkhe

Contents

1 Preface

I took this course in the spring of 2015 and was a TA for the course in 2016. I wrote these notes as an extension of most of the recitations I gave during the year and in particular tried to emphasize how to write proofs effectively and concisely. The first couple chapters will have plenty of examples of fully written proofs for algorithms and you should use these as templates for writing your solution sets. The later chapters will relax this slightly; I will be more succinct and might omit certain parts of the proof as exercises for you the reader. There is a lot of additional information that I have included in the footnotes; I highly encourage you to read them as some of them are tangential musings while others actual carry rather pertinent information to the subject.

A word of warning, however. I go into a lot of detail about the mathematics (as it interests me). I've tried to make it as accessible as possible by adding definitions for mathematical concepts as well as the intuition behind some of these definitions. However, if you are lost, Wikipedia is a good source for these definitions.

I hope you enjoy this course as much as I did and feel free to ask me or any of the TAs questions. If you spot errors in these notes please let me know right away as I guarantee you that there will be plenty. I had a great time writing these notes and as I wrote them, I realized there was so much I hadn't understood the first and second times looking at this course. Please also take your own notes, but hopefully these will help you through this course.

Lastly, a word about the structure of the course. When these notes were written, the course was 40% homework, 20% midterm, 40% final. That meant over the 7-8 sets, each problem on a set was worth about 1% of your grade. This is not something worth losing sleep over! Its far more important to get a deep conceptual understanding of the material. Most importantly, this was noticeable in the two exams. The exams will test you on slightly different things than the sets. While each set will generally introduce 1-2 new algorithm topics and test you on them, the exams will test you on all the topics till that date and in particular will test you on your ability to look at a problem and quickly figure out what type of algorithm it is looking for. More often that not, students spend too long on a problem on the exam trying to find an algorithm of the wrong type.

–Chinmay

2 Designing an Algorithm

Designing an algorithm is an art and something which this course will help you perfect. At the fundamental level, an algorithm is a set of instructions that manipulate an input to produce an output. For those of you with experience programming, you have often written a program to compute some function $f(x)$ only to find yourself riddled with (a) syntax errors and (b) algorithmic errors. In this class, we won't worry about the former, and instead focus on the latter. In this course, you will not be asked to construct any implementations of algorithms. Meaning we don't expect you to write any 'pseudocode' or code for the problems at hand. Instead, give an explanation of what the algorithm is intending to do and then provide an argument (i.e. proof) as to why the algorithm is correct.

A general problem you will find on your sets will ask you to *design* an algorithm X to solve a certain problem with a runtime Y[1]. Your solution should contain three parts:

1. An algorithm description.
2. A proof of correctness.
3. A statement of the complexity.

I strongly suggest that your solutions keep these three sections separate (see the examples). This will make it much easier for you to keep your thoughts organized (and the grader to understand what you are saying).

2.1 Algorithm Description

When specifying an algorithm, you have to provide the right amount of detail. I often express that this is similar to how you would right a lab report in a chemistry or physics lab today compared to what you would write in grade school. The level of precision is different because you are writing to a different audience. Identically, the audience to whom you are writing you should assume has a fair experience with algorithms and programming. If written correctly, your specification should provide the reader with an exercise in programming (i.e. actually implementing the algorithm in a programming language). You should be focusing on the exercise of designing the algorithm. In general, I suggest you follow these guidelines:

(a) You are writing for a *human* audience. Don't write C code, Java code, Python code, or any code for that matter. Write plain, technical English. Its highly recommended that you use LaTeX to write your solutions. The examples provided should give you a good idea of how to weave in the technical statements and English. For example, if you want to set m as the max of an array a of values, **don't** write a for loop iterating over a to find the maximizing element. Instead the following technical statement is sufficient.[2]

$$m \leftarrow \max_{x \in a}\{x\} \tag{2.1}$$

[1] If no runtime is given, find the best runtime possible.

[2] It is notational practice to set a variable using the $\leftarrow$ symbol. This avoids the confusing abusive notation of the $=$ symbol.

(b) Don't spend an inordinate time trying to find 'off-by-one' errors in your code. This doesn't really weigh in much on the design of the algorithm or its correctness and is more an exercise in programming. Notice in the example in (2.1), if written nicely, you won't even have to deal with indexing! Focus on making sure the algorithm is clear, not the implementation.

(c) On the other hand, you can't generalize too much. There should still be a step-by-step feel to the algorithm description. However, there are some simplifications you can make. if we have in class already considered an algorithm X that you want to use as a subroutine to then by all means, make a statement like 'apply X here' or 'modify X by doing $(\dots)$ and then apply here'. Please don't spend time writing out an algorithm that is already well known.

(d) If you are using a new data structure, explain how it works. Remember that data structures don't magically whisk away complexity. For example a min heap is $O(1)$ time to find the minimum, but $O(\log n)$ time to add an element. Don't forget these when you create your own data structures. However, if you are using a common data structure like a stack, you can take these complexities as given without proof. Make a statement like 'Let S be a stack' and say nothing more.

2.2 Proof of Correctness

A proof of correctness should explain how the nontrivial elements of your algorithm works. Your proof will often rely on the correctness of other algorithms it uses as subroutines. Don't go around reproving them. Assume their correctness as a lemma and use it to build a strong succinct proof. In general you will be provided with two different types of problems: Decision Problems and Optimization Problems. You will see examples of these types of problems throughout the class, although you should be familiar with Decision Problems from CS 21.

Definition 2.1 (Decision Problem)**.** A decision problem is a function $f : \Sigma \to \{\text{TRUE}, \text{FALSE}\}$.[3] Given an input x, an algorithm solving the decision problem efficiently finds if $f(x)$ is TRUE or FALSE.[4]

Definition 2.2 (Optimization Problem)**.** An optimization problem is a function $f : \Sigma \to \mathbb{R}$[5] along with a subset $\Gamma \subseteq \Sigma$. The goal of the problem is to find the $x \in \Gamma$ such that for all $y \in \Gamma$, $f(x) \leq f(y)$.

Recognize that as stated, this is a minimization problem. Any maximization problem can be written as a minimization problem by considering the function $-f$. We we call x the arg min of f and could efficiently write this problem as finding

$$x \leftarrow \arg\min_{y \in \Gamma} \{f(y)\} \tag{2.2}$$

When proving the correctness of a decision problem there are two parts. Colloquially these are called $yes \to yes$ and $no \to no$, although because of contrapositives its acceptable to prove $yes \to yes$

[3] Here Σ notes the domain on which the problem is set. This could be the integers, reals, set of tuples, set of connected graphs, etc.

[4] Often a decision problem f is phrased as follows: Given input (x, k) with $x \in \Sigma, k \in \mathbb{R}$ calculate if $g(x) \leq k$ for some function $g : \Sigma^* \to \mathbb{R}$.

[5] For the mathematicians out there reading this, you only need $f : \Sigma \to T$, where T is a set with a total ordering.

and $yes \leftarrow yes$. This means that you have to show that if your algorithm return TRUE on input x then indeed $f(x) =$ TRUE and if your algorithm returns FALSE then $f(x) =$ FALSE.

When proving the correctness of an optimization problem there are also two parts. First you have to show that the algorithm returns a feasible solution. This means that you return an $x \in \Gamma$. Second you have to show optimality. This means that there is no $y \neq x \in \Gamma$ such that $f(y) < f(x)$. This is the tricky part and the majority of what this course focuses on.

Many of the problem in this class involve combinatorics. These proofs are easy if you understand them and tricky if you don't. To make things easier on yourself, I suggest that you break your proof down into lemmas that are easy to solve and finally put them together in a legible simple proof.

2.3 Algorithm Complexity

This is the only section of your proof where you should mention runtimes. This is generally the easiest and shortest part of the solution. Explain where your complexity comes from. This can be rather simple such as: 'The outer loop goes through n iterations, and the inner loop goes through $O(n^2)$ iterations, since a substring of the input is specified by the start and end points. Each iteration of the inner loop takes constant time, so overall, the runtime is $O(n^3)$.' Don't bother mentioning steps that *obviously* don't contribute to the asymptotic runtime. However, be sure to include runtimes for all subroutines you use. For more information on calculating runtimes, read the next section.

2.4 Example Solution

The following is an example solution. I've riddled it with footnotes explaining why each statement is important. Note the problem, I have solved here is a dynamic programming problem. It might be better to read that chapter first so that you understand how the algorithm works before reading this.

Exercise 2.3 (Longest Increasing Subsequence)**.** Given an array of integers $x_1, \ldots, x_n$, find the *longest increasing subsequence* i.e. the longest sequence of indices $i_1 < i_2 < \cdots < i_k$ such that $x_{i_1} \leq x_{i_2} \leq \cdots \leq x_{i_k}$. Design an algorithm that runs in $O(n^2)$.

Algorithm Description. This is a dynamic programming algorithm.[6] We will construct tables ℓ and p where $\ell[j]$ will is the length of the longest increasing subsequence that ends with x_j and $p[j]$ is the index of the penultimate element in the longest subsequence.[7]

1. For $j = 1$ to n:[8]

[6] A sentence like this is a great way to start. It immediately tells the reader what type of algorithm to expect and can help you get some easy partial credit.

[7] We've told the reader all the initializations we want to make that aren't computationally trivial. Furthermore, we've explained what the ideal values of the tables we want to propagate are. This way when it comes to showing the correctness, we only have to assert that their tables are filled correctly.

[8] Its perfectly reasonable to use bullet points or numbers lists to organize your thinking. Just make sure you know that the result shouldn't be code.

(a) Initialize $\ell[j] \leftarrow 1$ and $p[j] \leftarrow$ NULL (soon to be changed).

(b) For every $k < j$ such that $x_k < x_j$: If $\ell[k]+1 > \ell[j]$, then set $\ell[j] \leftarrow \ell[k]+1$ and $p[j] \leftarrow k$.

2. Let j be the arg max of ℓ. Follow p backwards to construct the subsequence. That is, return the reverse of the sequence $j, p[j], p[p[j]], \ldots$ until some term has $p[j] =$ NULL.[9]

Proof of Correctness. First, we'll argue that the two arrays are filled correctly. Its trivial to see that the case of $j = 1$ is filled correctly. By induction on k, when $\ell[j]$ is updated, there is some increasing subsequence which ends at x_j and has length $\ell[j]$. This sequence is precisely the longest subsequence ending at x_k followed by x_j. The appropriate definition for $p[j]$ is immediate.[10] This update method is exhaustive as the longest increasing subsequence ending at x_j has a penultimate element at some x_k and this case is considered by the inductive step.

By finding the arg max of ℓ, we find the length of the longest subsequence as the subsequence must necessarily end at some x_j. By the update rules stated above, for $k = p[j]$, we see that $\ell[k] = \ell[j]-1$ and $x_k < x_j$. Therefore, *a* longest subsequence is the solution to the subproblem k and x_j. The backtracking algorithm stated above, recursively finds the solution to the subproblme.[11] Reversing the subsequence produces it in the appropriate order.

Complexity. The outer loop runs n iterations and the inner loop runs at most n iterations, with each iteration taking constant time. Backtracking takes at most $O(n)$ time as the longest subsequence is at most length n. The total complexity is therefore: $O(n^2)$.[12]

[9] Resist the urge to write a while loop here. As stated is perfectly clear.

[10] We've so far argued that the updating is occuring only if a sequence of that length exists. We now only need to show that all longest sequences are considered.

[11] Backtracking is as complicated as you make it to be. All one needs to do is argue that the solution to the backtracked problem will help build recursively the solution to the problem at hand.

[12] Don't bother writing out tedious arithmetic that both of us know how to do.

3 Runtime Complexity and Asymptotic Analysis

3.1 Asymptotic Analysis

I'm sure all of you have read about Big O Notation in the past so the basic definition should be of no surprise to you. That definition you will find is sometimes a bit simplistic and in this class we are going to require more formalism to effectively describe the efficiency of our algorithms.

Bear with me for a bit, as I'm going to delve into a lot of mathematical intuition but I promise you that it will be helpful!

Let's form a *partial* ordering on the set of function $\mathbb{N} \to \mathbb{R}^+$ (functions from natural numbers to positive reals). Let's say for $f, g : \mathbb{N} \to \mathbb{R}^+$, that $f \leq g$ if for all but finitely many n, $f(n) \leq g(n)$.[13] Formally this means the following:

(a) (reflexivity) $f \leq f$ for all f.

(b) (antisymmetry) If $f \leq g$ and $g \leq f$ then $f = g$.[14]

(c) (transitivity) If $f \leq g$ and $g \leq h$ then $f \leq h$

What differentiates a partial ordering from a *total* ordering is that there is no idea that f and g are comparable. It might be that $f \leq g$, $f \geq g$ or perhaps neither. In a total ordering, we guarantee that $f \leq g$, or $f \geq g$, perhaps both.

Why is this important, you may rightfully ask. By defining this partial ordering, we've given ourselves the ability to define *complexity equivalence classes*.

Definition 3.1 (Big O Notation)**.** Let $f, g : \mathbb{N} \to \mathbb{R}^+$. We say $f \in O(g)$ and (equivalently) $g \in \Omega(f)$ if $f \leq cg$ for some $c > 0$. Here we use '$\leq$' as described previously.

First recognize that $O(g)$ and $\Omega(f)$ are *sets* of functions. Let's discuss equivalence classes and relations for a bit.

Definition 3.2 (Equivalence Relation)**.** We say $\sim$ is an equivalence relation on a set X if for any $x, y, z \in X$, $x \sim x$ (reflexivity), $x \sim y$ iff $y \sim x$ (symmetry), and if $x \sim y$ and $y \sim z$ then $x \sim z$.

Our general definition for '=' fits very nicely into this definition for equivalence relations. But equivalence relations are more general than that. In fact they work with the definition of equality in a partial ordering above as well. Check this if you are unsure about it. Now, we can bring up the notation of an equivalence class.

[13] You might see this in the notation $\exists\, n_0 \in \mathbb{N}$ such that for all $n > n_0$, $f(n) \leq g(n)$. These are in fact equivalent. If $f(n) \leq g(n)$ for all but finitely many n (call them $n_1 \leq \cdots \leq n_m$) then for all $n > n_m$, $f(n) \leq g(n)$. Setting $n_0 = n_m$ completes this proof. For the other direction, let the set of finitely many n for which it doesn't satisfy be the subset of $\{1, \ldots, n_0\}$ where $f(n) > g(n)$.

[14] Careful here! When we say $f = g$ we don't mean that f and g are equal in the traditional sense. We mean they are equal in the asymptotic sense. Formally this means that for all but finitely many n, $f(n) = g(n)$. For example, the functions $f(x) = x$ and $g(x) = \lceil \frac{x^2}{x+10} \rceil$ are asymptotically equal.

Definition 3.3 (Equivalence Class)**.** We call the set $\{y \in X \text{ s.t. } x \sim y\}$, the equivalence class of x in X and notate it by $[x]$.

You might be asking yourself what does any of this have to do with runtime complexity? I'm getting to that. The point of all of these definitions about partial ordering and equivalence classes is that $f \in O(g)$ is a partial ordering as well! Go through the process of checking this as an exercise.

Definition 3.4. We say $f \in \Theta(g)$ and (equivalently) $g \in \Theta(f)$ if $f \in O(g)$ and $g \in O(f)$.

This means that $f \in \Theta(g)$ is an equivalence relation and in particular $\Theta(g)$ is an equivalence class. By now, perhaps you've gotten an intuition as to what this equivalence class means. It is the set of functions that have the same *asymptotic computational complexity*. This means that asymptotically, their values only deviate from each by a linear factor.

This is an incredibly powerful idea! We're now defined ourselves with the idea of equality that is suitable for this course. We are interested in asymptotic equivalence. If we're looking for a quadratic function, we're happy with finding any function in $\Theta(n^2)$. This doesn't mean per se that we don't care about linear factors, its just that its not the concern of this course. A lot of work in other areas of computer science focus on the linear factor. What we're interested in this course is how to design algorithms for problems that look exponentially hard but in reality might have polynomial time algorithms. That jump is far more important than a linear factor.

We can also define o, ω notation. These are stronger relations. We used to require the existence of some $c > 0$. Now we require it to be true for all $c > 0$.

Definition 3.5 (Little O Notation)**.** Let $f, g : \mathbb{N} \to \mathbb{R}^+$. We say $f \in o(g)$ and (equivalently) $g \in \omega(f)$ if $f \leq cg$ for all $c > 0$. Here we use '$\leq$' as described previously.

We can also discuss asymptotic analysis for functions of more than one variable. I'll provide the definition here for Big O Notation but its pretty easy to see how the other definitions translate.

Definition 3.6 (Multivariate Big O Notation)**.** Let $f, g : \mathbb{N}^k \to \mathbb{R}^+$. We say $f \in O(g)$ and (equivalently) $g \in \Omega(f)$ if $f(x_1, \ldots, x_k) \leq cg(x_1, \ldots, x_k)$ for some $c > 0$ for all but finitely many tuples $(x_1, \ldots, x_k)$.[15]

A word of warning. Asymptotic notation can be used incredibly abusively. For example you might see something written like $3n^2 + 18n = O(n^2)$. In reality, $3n^2 + 18n \in O(n^2)$. But the abusive notation can be helpful if we want to 'add' or 'multiply' big O notation terms. You might find this difficult at first so stick to more correct notations until you feel comfortable using more abusive notation.

3.2 Random Access Machines and the Word Model

Okay, so we've gotten through defining Big O Notation so now we need to go about understanding how to calculate runtime complexity. A perfectly reasonable question to ask is 'what computer are we thinking about when calculating runtime complexity?'. A lot of you have taken courses on

[15] It really helps me to think of this graphically. Essentially, this definition is saying that the region for which $f \not\leq cg$ is bounded.

parallelization, for example. Are we allowed to use a parallel computing system here? These are all good questions and certainly things to be thinking about. However, for the intents of our class, we are not going to be looking at parallelization. We are going to assume a single threaded machine. [16] Is this a quantum machine? Also, interesting but in this case outside the scope of this course.

The most general model we could use would be a single headed one tape Turing machine. Although equivalent in computation power, we know that this is not an efficient model particularly because the head will move around too much and this was incredibly inefficient. It was a perfectly reasonable model for us to use in CS 21 because the movement of the head can be argued to not cause more than a polynomial deviation in the complexity which was perfectly fine with us as we were really only concerned about the distinction of P and NP.

To define a model for computation, we need to define the costs of each of the operations. We can start from the ground up and define the time to flip a bit, the time to move the head to a new bit to flip, etc. and build up our basic operations of addition, multiplication from there and then move on to more complicated operations and so forth. This we will quickly find becomes incredibly complicated and tedious. However, this is the only actual method of calculating the time of an algorithm. What we will end up using is a simplification, but one that we are content with. When you think about an algorithm's complexity, you must always remember what model you are thinking in. For example, I could define a model where sorting is a $O(1)$ operation. This wouldn't be a very good model but now you could solve the problem of finding the mode of a set in $O(n)$ time with $O(1)$ additional space. Luckily, the models we're going to use have some logical intuition behind them and you wouldn't have any such silly pitfalls.

We are going to be using two different models in this class. The most common model we will be working in is the *Random-Access Machine (RAM) model*. In this model, instructions are operated on sequentially with no concurrency. Furthermore, we can write as much as we want to the memory and the access of any part of the memory is done in constant time.[17] We further assume that reading and writing a single bit takes constant time.

Recall that a n-bit integer can be stored using $O(\log n)$ bits. So addition, subtraction, and multiplication of n-bit integers naïvely takes $O(\log n)$ time.[18] This model is the most accurate because it most closely reflects how a computer works.

However, as I said before this can get really messy. We will also make a simplification which we call the *word model*. In the word model, we assume that all the words can be stored in $O(1)$ space. There are numerous intuitions behind the word model but the most obvious is how most programming languages allocate memory. When you allocate memory for an integer, languages

[16] If you consider a multi threaded machine with k threads, then any computation that takes time t to run on the multithreaded machine takes at most kt time to run on the single threaded machine. And conversely, any computation that takes time t to run on the single threaded machine takes at most t time to run on the multithreaded machine. If k is a constant, this doesn't affect asymptotic runtime.

[17] This is the motivation of the name Random-Access. A random bit of memory can be accessed in constant time. In a Turing machine only the adjacent bits of the tape can be accessed in constant time.

[18] You can also think about this as adding m bit integers takes $O(m)$ time. And you can store numbers as large as 2^m using m bits.

usually allocate 32 bits (this varies language to language). These 32 bits allow you to store integers between -2^{31} and $2^{31}-1$. This is done irrespective of the size the integer. So, operations on these integers are irrespective of the length.

This model is particularly useful if we want to consider the complexity of higher order operations. A good example is matrix multiplication. A naïve algorithm for matrix multiplication runs in $O(n^3)$ for the multiplication of two $n \times n$ matrices. By this we mean that the number of multiplication and addition operations applied on the elements of the matrices is $O(n^3)$.[19] The complexity of the multiplication of the elements isn't directly relevant to the matrix multiplication algorithm itself and can be factored in later.

For the most part, you will be able to pick up on whether the RAM model or the Word model should be used. In the example in the previous chapter, we used the Word model. Why? Because, the problem gave no specification as to the size of the elements $x_1, \ldots, x_n$. If specified, then it implies the RAM model. In situations where this is confusing, we will do the best to clarify which model the problem should be solved in. If in doubt, ask a TA.

[19] Later we will show how to get this down to $O(n^{\log_2 7})$.

4 The GCD Algorithm

4.1 Recursion

Definition 4.1 (Recursive Algorithm)**.** A recursive algorithm is any algorithm whose answer is dependent on running the algorithm with 'simpler' values, except for the 'simplest' values for which the value is known trivially.[20]

The idea of a recursive algorithm probably isn't foreign to you. In this class, we will be looking at two different 'styles' of recursive algorithms: Dynamic Programming and Divide-and-Conquer algorithms. Let's take a look a look at a more basic recursive algorithm to start off. We will also introduce the notion of *duality* along the way.

Definition 4.2 (Greatest Common Divisor)**.** For integers a, b not both 0, let $\text{DIVS}(a, b)$ be the set of positive integers dividing both a and b. The greatest common divisor of a and b noted $\gcd(a, b) = \max\{\text{DIVS}(a, b)\}$.

Let's start by creating a naïve algorithm for the gcd problem.[21] We know that trivially $\gcd(a, b) \leq a$ and $\gcd(a, b) \leq b$ or equivalently $\gcd(a, b) \leq \min(a, b)$. A naïve algorithm could be to check all values $1, \ldots, \min(a, b)$ to see if they divide both a and b. This will have runtime $O(\min(a, b))$ assuming the word model.

We checked a lot of cases here, but under closer observation a lot of the checks were redundant. For example, if we showed that 5 didn't divide either a or b, then we know that none of $10, 15, 20, \ldots$ divide them either. Let's explore how we can exploit this observation.

Lemma 4.3. *For integers a, b, not both 0,* $\text{DIVS}(a, b) = \text{DIVS}(b, a)$ *(reflexivity), and* $\text{DIVS}(a, b) = \text{DIVS}(a + b, b)$.

Proof. Reflexivity is trivial by definition. If $x \in \text{DIVS}(a, b)$ then $\exists\ y, z$ integers such that $xy = a, xz = b$. Therefore, $x(y+z) = a+b$, proving $x \in \text{DIVS}(a+b, b)$. Conversely, if $x' \in \text{DIVS}(a+b, b)$ then $\exists\ y', z'$ integers such that $x'y' = a + b, x'z' = b$. Therefore, $x'(y' - z') = a$ proving $x' \in \text{DIVS}(a, b)$. Therefore, $\text{DIVS}(a, b) = \text{DIVS}(a + b, b)$. □

Corollary 4.4. *For integers a, b, not both 0,* $\text{DIVS}(a, b) = \text{DIVS}(a+kb, b)$ *for $k \in \mathbb{Z}$, and therefore* $\gcd(a, b) = \gcd(a + kb, b)$.

Proof. Apply induction. The gcd argument follows at is the max element of the same set. □

Let's make a stronger statement. Recall that one way to think about $a \pmod b$ is the unique number in $\{0, \ldots, b\}$ that is equal to $a + kb$ for some $k \in \mathbb{Z}$.[22] Therefore, the following corollary also holds.

[20] By simpler, I don't necessarily mean smaller. It could very well be that $f(t)$ is dependent on $f(t + 1)$ but $f(T)$ for some large T is a known base case.

[21] This is generally a good practice to follow especially in interview questions at companies. Start by stating a naïve algorithm, state its faults and how you could go about improving it.

[22] The more 'mathy' way of thinking about $a \pmod b$ is as the conjugacy class of a when we consider the equivalence relation $x \sim y$ if $x - y$ is a multiple of b. This forms a group known as $\mathbb{Z}/b\mathbb{Z}$. Addition is defined on the conjugacy classes as a consequence of addition on any pair of elements in the conjugacy classes permuting the classes. Read any Abstract Algebra textbook for more information.

Corollary 4.5. *For integers a, b, not both 0, $\gcd(a, b) = \gcd(a \pmod b, b)$.*

This simple fact is going to take us home. We've found a way to recursively reduce the larger of the two inputs (wlog [23] assume a) to strictly less than b. Because it's strictly less than b, we know that this repetitive recursion will actually terminate. By terminate, we mean that we will reach a base case that we know the solution of. In this case, let's assume our base case is naïvely that $\gcd(a, 0) = a \ \forall \ a$. Just for the sake of formality, I've stated this as an algorithm below:

Algorithm 4.6 (Euclid-Lamé)**.** Given integer inputs inputs a, b with $a \geq b$, if $b = 0$ then return a. Otherwise, return the $\gcd(b, a \pmod b)$ calculated recursively.[24]

To state correctness, its easiest to just cite the previous corollary and argue that as the input's strictly decrease we will eventually reach a base case. A truly great proof would also say something about negative inputs and why this case isn't to be worried about (hint $\gcd(a, b) = \gcd(a, -b)$).

How do you go about arguing complexity? In most cases its pretty simple but this problem is a little bit trickier. Recall the Fibonacci numbers $F_1 = 1, F_2 = 1$ and $F_k = F_{k-1} + F_{k-2}$ for $k > 2$. I'm going to assume that you have remembered the proof from Ma/CS 6a (using generating functions) that:

$$F_k = \frac{1}{\sqrt{5}}\phi^k - \frac{1}{\sqrt{5}}\phi'^k \tag{4.1}$$

where ϕ, ϕ' are the two roots of $x^2 = x + 1$ (ϕ is the larger root, a.k.a the golden ratio). Note that $|\phi'| < 1$ so F_k tends to $\phi^k/\sqrt{5}$. More importantly, it grows exponentially.

Most times, you're complexity argument will be the smallest argument. Let's make the following Theorem about the complexity:

Theorem 4.7. *If $0 < b \leq a$, and $b < F_{k+2}$ then the Euclid-Lamé algorithm makes at most k recursive calls.*

Proof. This is a proof by induction. Check for $k < 2$ by hand. Now, if $k \geq 2$ then recall that the recursive call is for $\gcd(b, c)$ where we define $c := a \pmod b$. Now there are two cases to consider. The first is easy: If $c < F_{k+1}$ then by induction at most $k - 1$ recursive calls from here so total at most k calls. ✓In the second case: $c \geq F_{k+1}$. One more function call gives us $\gcd(c, b \pmod c)$. First, recall that there's a strict inequality among the terms in a recursive gcd call (proven previously). So $b > c$. Therefore, $b > b \pmod c$ as $c > b \pmod c$. In particular we have strict inequality, so $b \geq (b \pmod c) + c$ or equivalently $b \pmod c \leq b - c$. Then apply the bounds on b, c to get

$$b \pmod c \leq b - c \leq b - F_{k+1} < F_{k+2} - F_{k+1} = F_k \tag{4.2}$$

So in two calls, we get to a position from where inductively we make at most $k - 2$ calls, so total at most k calls as well. □

The theorem tells us that Euclid-Lamé for $\gcd(a, b)$ makes $O(\log(\min(a, b)))$ recursive calls in the word model. I'll leave it as a nice exercise to finish this last bit.

[23] without loss of generality.

[24] I write it as $\gcd(b, a \pmod b)$ instead of $\gcd(a \pmod b, b)$ here to insure that the first argument is strictly larger than the second.

4.2 Duality

Incidentally, this isn't the only problem that benefits from this recursive structure of looking at modular terms. We're going to look at a *dual* problem that shares the same structure. Formally for optimization problems,

Definition 4.8 (Duality)**.** A minimization problem $\mathcal{D}$ is considered the *dual* of a maximization problem $\mathcal{P}$ is the solution of $\mathcal{D}$ provides an upper bound for the solution of $\mathcal{D}$. This is referred to as *weak duality*. If the solutions of the two problems are equal, this is called *strong duality*.

Define $\text{SUMS}(a, b)$ as the set of positive integers of the form $xa + yb$ for $x, y \in \mathbb{Z}$. With a little effort one can prove that like DIVS, the following properties hold for SUMS.

Lemma 4.9. *For integers a, b, not both 0, $\text{SUMS}(a, b) = \text{SUMS}(a + kb, b)$ for any $k \in \mathbb{Z}$, and therefore $\text{SUMS}(a, b) = \text{SUMS}(a \pmod b, b)$.*

It shouldn't be surprising then in fact there is a duality structure here. I formalize it below:

Theorem 4.10 (Strong Dual of GCD)**.** *For integers a, b, not both 0,* $\min\{\text{SUMS}(a, b)\} = \max\{\text{DIVS}(a, b)\} = \gcd(a, b)$.

Proof. Its easy to see as $\gcd(a, b)$ divides a and b then it divides any $ax + yb$ proving weak duality. For strong duality, assume for contradiction, that there exists (a, b) such that $a+b$ is the smallest.[25] But then the pair $(b, a - b)$ yields the same set of SUMS however, $b + (a - b) = b < a + b$, a contradiction. □

[25] This is a very common proof style and one we will see again in greedy algorithms. We assume that we have a smallest instance of a contradiction and argue a smaller instance of contraction. Here we define smallest by the magnitude of $a + b$.

5 Dynamic Programming

Before you get some alternate idea, let me state it that *Dynamic Programming is a form of recursion.* In Computer Science, you have probably heard the tradeoff between Time and Space. This has nothing to do with General relativity, but has to do with the trade off between the space complexity on the memory and the time complexity of the algorithm[26]. The way I like to think about Dynamic Programming is that we're going to exploit the tradeoff by utilizing the memory to give us a speed advantage when looking at recursion problems.

Not all recursion problems have such a structure. For example the GCD problem from the previous chapter does not. We will see more examples that don't have a Dynamic Programming structure. Here are the properties, you should be looking for when seeing if a problem can be solved with Dynamic Programming.

5.1 Principal Properties

Principal Properties of Dynamic Programming. Almost all Dynamic Programming problems have these two properties:

1. Optimal substructure: The optimal value of the problem can easily be obtained given the optimal values of subproblems. In other words, there is a recursive algorithm for the problem, which would be fast if we could just skip the recursive steps.
2. Overlapping subproblems: The subproblems share sub-subproblems. In other words, if you actually ran that naïve recursive algorithm, it would waste a lot of time solving the same problems over and over again.

In other words, your algorithm trying to calculate $f(x)$ might recursively call $f(y)$ many times. It will be therefore, more efficient to store the value of $f(y)$ and recall it rather than calculating it again and again. I know that's confusing, so lets look at a couple examples to clear it up.

5.2 Tribonacci Numbers, an example

I'll introduce computing 'tribonacci' numbers as a preliminary example[27] The tribonacci numbers are defined by $T_0 = 1, T_1 = 1, T_2 = 1$ and $T_k = T_{k_1} + T_{k-2} + T_{k-3}$ for $k \geq 3$.

[26] I actual prefer to think about this as a 3-way tradeoff between time complexity, space complexity, and correctness. This has lead to the introduction of the vast field of randomized and probabilistic algorithms, which are correct in expectation and have small variance. But that is for other classes particularly CS 139 and CS 150

[27] The easiest example is Fibonacci numbers but as I've given you the explicit formula in the previous chapter, it seems moot. Although this problem is also rather easily solvable with recurrence relations, but bear with me.

6 Greedy Algorithms

7 Graph Algorithms

8 Branch and Bound

9 Divide and Conquer

10 Multiplicative Weights Algorithm

11 Max-Flow Min-Cut

12 Dynamic Programming