CPSC 313 — Supplemental Material for Lecture #1
Mathematics Review

What is a Proof?

In mathematics, and computer science, a ***proof*** is formal argument, establishing a ***claim***. This kind of argument proceeds line-by-line (or, from one ***deduction*** to another) using

- ***Axioms***: Properties that are understood — and universally agreed — to be correct.
- ***Theorems:*** Other results that have been proved already.
- ***Proof Techniques:*** Formal methods that can be used, with results that have been proved already, to prove new ones.

These do not necessarily need to be *written* in a formal way — but it should always be possible to identify the *axioms*, *theorems*, and *proof techniques* that have been used *in* a proof.

Axioms that you should already know about, and that can be used when writing proofs, include the following.

- Properties of integers, and other sets and structures, that you learned about in MATH 271[1].

  Example: *Commutativity of Integer Addition:* For all integers a and b, $a + b = b + a$.

- Properties of statements in programming languages that you learned about in the programming prerequisites for this course.

  Example: If `x` is an integer variable and *exprn* is an integer expression, then (in **Java**) the *assignment statement*

  `x = exprn`

  sets the value of the variable `x` to be the current value of *exprn*.

You almost certainly learned about some ***theorems*** in MATH 271. The list of theorems you may use grows every time you see a valid mathematical proof!

[1] or MATH 273, if this was the prerequisite in discrete mathematics that you completed before this course

Examples of ***proof techniques*** that you should already know about include

- Proof by contradiction
- Proof of an *existential* claim by giving an example
- Mathematical induction

Negative Example — This is *not* a proof. Consider the following.

Claim:

$$\sum_{i=0}^{n}(2i+1) = (n+1)^2$$

for every integer $n \geq 0$.

Proof: (Which is Actually *Not* One, at All): If $n = 0$ then

$$\sum_{i=0}^{n}(2i+1) = (2 \times 0 + 1) = 1 = 1^2 = (n+1)^2.$$

If $n = 1$ then

$$\sum_{i=0}^{n}(2i+1) = (2 \times 0 + 1) = (2 \times 1 + 1) = 1 + 3 = 4 = 2^2 = (n+1)^2.$$

Similarly, if $n = 2$ then

$$\sum_{i=0}^{n}(2i+1) = 1 + 3 + 5 = 9 = 3^2 = (n+1)^2,$$

and so on. □

This is *not* a valid proof because it is not using a valid ***proof technique:*** When you are proving a property that is supposed to hold for all the elements of an infinite set, you can *never* do that just by checking whether the property holds for a finite subset of it.

Mathematical proofs are important because they are **reliable:** They can be *understood* and *trusted* — when other kinds of arguments cannot be.

Even though it might be tedious, you should be able to **identify** the *axioms, theorems* and *proof techniques* that were used to establish all the claims in the argument. If you **cannot** do that then there is a pretty good chance that the argument is *not* a mathematical proof at all.

Discovering — and Writing — Mathematical Proofs

Finding mathematical proofs is something of an ***art***: Professional mathematicians and computer scientists work for years to discover proofs of claims (sometimes including proofs of claims that are not actually *true*).

On the other hand, ***writing*** a mathematical proof down, once you have discovered it is a ***skill*** that can be taught and learned... but requires *practice*.[2]

When writing a proof to solve a problem on an assignment you should remember

whom you should be writing for.

You should actually be writing for someone who ***does not*** know why the claim is true, and might not even believe it (even though the marker does) — but you should also be writing for someone who understands enough basic mathematics and logic to understand and accept a well-written proof.

What To Do if You Get Stuck. Suppose you are asked to write a proof on a test and do not know how to do it or get stuck in the middle...

- *A Good Thing To Do:* Tell the marker what you ***do*** know about how to prove it: Mention the *proof technique* that you believe should be used, *theorems* and *axioms* you know that seem to be relevant, and tell the marker how far you *did* get when you tried to use these.
- *What **NOT** To Do:* Forget or ignore everything you have learned about mathematical proofs (and the material introduced in this course) and give the marker an argument like the "negative example" from earlier in those notes.

Review of Mathematical Induction

Mathematical induction is a **proof technique** (or set of related ones) that you already learned about in MATH 271 and that is *extremely* useful for proving properties of automata and grammars.

[2] This is also a reason for some of the readings and why proofs for problems on tutorial exercises are being provided: Teaching assistants ***do not*** have the time to provide well-written proofs during time-limited tutorials.

In CPSC 313 lectures or supplemental material, mathematical induction will be used to prove the correctness of several of the constructions that are being described.

You might also be asked to use mathematical induction to prove things in this course — and you will *definitely* be required to do this in one or more CPSC courses that you take.

Standard Form of Mathematical Induction. Let $P(n)$ be a property that is defined for all integers n, and let α be a fixed integer. Suppose the following two statements are true:

1. $P(\alpha)$ is true.
2. For all integers $k \geq \alpha$, if $P(k)$ is true then $P(k+1)$ is true.

Then $P(n)$ is true for every integer $n \geq \alpha$.

One way to prove that $P(n)$ is true for every integer $n \geq \alpha$ is to use the following ***proof outline*** — after stating what it is that you are proving, and naming the proof technique that is being used:[3]

1. ***Basis:*** Show that $P(\alpha)$ is true.
2. ***Inductive Step:*** Let k be an arbitrarily chosen integer such that $k \geq \alpha$. Assuming only the

   Inductive Hypothesis: $P(k)$ is true,

   prove the

   Inductive Claim: $P(k+1)$ is true.
3. Conclude that $P(n)$ is true for every integer $n \geq \alpha$.

Example Proof. Consider the problem of proving that

$$\sum_{i=0}^{n}(2i+1) = (n+1)^2$$

for every integer $n \geq 0$.

[3] Students often forget to do these things — leaving readers, including markers, confused about what is going on.

One can apply the above method to prove this by setting...

- $P(k)$ to be the property that

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2$$

- and setting α to be 0.

The resulting proof looks like the following.

Claim:

$$\sum_{i=0}^{n}(2i+1) = (n+1)^2$$

for every integer $n \geq 0$.

Proof: This will be proved by induction on n. The standard form of mathematical induction will be used.

Basis: If $n = 0$ then

$$\sum_{i=0}^{n}(2i+1) = \sum_{i=0}^{0}(2i+1) = 1.$$

Since $(n+1)^2 = 1^2 = 1$ in this case, as well, it follows that

$$\sum_{i=0}^{n}(2i+1) = (n+1)^2$$

when $n = 0$.

Inductive Step: Let k be an arbitrarily chosen integer such that $k \geq 0$. It is necessary and sufficient to use the following

$$\underline{\text{Inductive Hypothesis:}}\ \sum_{i=0}^{k}(2i+1) = (k+1)^2.$$

to prove the following

$$\underline{\text{Inductive Claim:}}\ \sum_{i=0}^{k+1}(2i+1) = (k+2)^2.$$

Note that

$$\begin{aligned}\sum_{i=0}^{k+1}(2i+1) &= \sum_{i=0}^{k}(2i+1) + (2k+3) \\ &= (k+1)^2 + 2k + 3 && \text{(by the inductive hypothesis)} \\ &= k^2 + 2k + 1 + 2k + 3 \\ &= k^2 + 4k + 4 \\ &= (k+2)^2 = ((k+1)+1)^2\end{aligned}$$

as required to establish the inductive claim and complete the inductive step. It now follows that

$$\sum_{i=0}^{n}(2i+1) = (n+1)^2$$

for every integer $n \geq 0$. □

Perhaps you are wondering whether this is a mathematical proof at all.

Tedious Exercise: Go to your MATH 271 notes or textbook and identify all of the properties of integers, introduced in that course, that are **axioms** that were used in the above proof — along with any **theorems** proved in that course that have been used here too.

Indeed, this really *would* be tedious.... but it is what you would need to do to be convinced that this really *is* a mathematical proof, if you did not already see this.

Strong Form of Mathematical Induction. Once again, let $P(n)$ be a property that is defined for all integers n. Let α and β be fixed integers such that $\alpha \leq \beta$. Suppose that the following two statements are true.

1. $P(\alpha), P(\alpha+1), P(\alpha+2), \ldots, P(\beta)$ are all true.
2. For every integer $k \geq \beta$, if $P(i)$ is true for every integer i such that $\alpha \leq i \leq k$, then $P(k+1)$ is true as well.

Then $P(n)$ is true for every integer $n \geq \alpha$.

Another way to prove that $P(n)$ is true for every integer $n \geq \alpha$ is to applying the corresponding ***proof technique*** — once again, after saying what you will prove and identifying the proof technique to be used.

1. ***Choice of Breakpoint:*** Choose an integer β such that $\beta \geq \alpha$.[4]
2. ***Basis:*** Prove that $P(\alpha), P(\alpha+1), P(\alpha+2), \ldots, P(\beta)$ are all true.
3. ***Inductive Step:*** Let k be an arbitrarily chosen integer such that $k \geq \beta$. Assuming only the

   Inductive Hypothesis: $P(i)$ is true for every integer i such that $\alpha \leq i \leq k$.

   prove the

   Inductive Claim: $P(k+1)$ is true.
4. Conclude that $P(n)$ is true for every integer $n \geq \alpha$.

Example. Suppose that $g_0, g_1, g_2, \ldots$ are integers such that (for a nonnegative integer i)

$$g_i = \begin{cases} 12 & \text{if } i = 0, \\ 29 & \text{if } i = 1, \\ 5 \cdot g_{i-1} - 6 \cdot g_{i-2} & \text{if } i \geq 2. \end{cases}$$

Consider the problem of proving that $g_n = 5 \cdot 3^n + 7 \cdot 2^n$ for every integer $n \geq 0$.

One can apply the above method...

- by setting $P(k)$ to be the property that if $k \geq 0$ then $g_k = 5 \cdot 3^k + 7 \cdot 2^k$
- and by setting α to be 0.

The resulting proof will look something like the following.

Claim: Suppose that $g_0, g_1, g_2, \ldots$ are integers such that (for a nonnegative integer i)

$$g_i = \begin{cases} 12 & \text{if } i = 0, \\ 29 & \text{if } i = 1, \\ 5 \cdot g_{i-1} - 6 \cdot g_{i-2} & \text{if } i \geq 2. \end{cases}$$

Then $g_n = 5 \cdot 3^n + 7 \cdot 2^n$ for every integer $n \geq 0$.

Proof: This will be proved by induction on n. The strong form of mathematical induction will be used, and the cases that $n = 0$ and $n = 1$ will be considered in the basis.

[4] Breakpoints will not be called this very much later on. Instead, something like the phrase "The cases that $\alpha \leq i \leq \beta$ will be considered in the basis." will appear near the beginning of the proof.

Basis: If $n = 0$ then $g_n = g_0 = 12$ as defined above, and

$$5 \cdot 3^n + 7 \cdot 2^n = 5 \cdot 1 + 7 \cdot 1 = 12$$

as well, so that $g_n = 5 \cdot 3^n + 7 \cdot 2^n$ in this case.

If $n = 1$ then $g_n = g_1 = 29$ as defined above, and

$$5 \cdot 3^n + 7 \cdot 2^n = 5 \cdot 3 + 7 \cdot 2 = 15 + 14 = 29$$

as well, so that $g_n = 5 \cdot 3^n + 7 \cdot 2^n$ once again.

Inductive Step: Let k be an arbitrarily chosen integer such that $k \geq 1$. It is necessary and sufficient to use the following

> Inductive Hypothesis: $g_i = 5 \cdot 3^i + 7 \cdot 2^i$ for every integer i such that $0 \leq i \leq k$.

to prove the following

> Inductive Claim: $g_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$.

Since $k \geq 1$, $k + 1 \geq 2$, so that $k - 1$ and k are both integers between 0 and k, and

$$\begin{aligned}
g_{k+1} &= 5 \cdot g_k - 6 \cdot g_{k-1} && \text{(since } k+1 \geq 2\text{)} \\
&= 5 \cdot (5 \cdot 3^k + 7 \cdot 2^k) - 6 \cdot (5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}) && \text{(by the inductive hypothesis)} \\
&= 5 \cdot (5 \cdot 3 - 6) \cdot 3^{k-1} + 7 \cdot (5 \cdot 2 - 6) \cdot 2^{k-1} && \text{(reordering terms)} \\
&= 5 \cdot 3^2 \cdot 3^{k-1} + 7 \cdot 2^2 \cdot 2^{k-1} \\
&= 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}
\end{aligned}$$

as required to complete the inductive step.

It now follows that $g_n = 5 \cdot 3^n + 7 \cdot 2^n$ for every integer $n \geq 0$. □

A Few Questions. You might be wondering about a few things by now...

- **Question:** Why did I use "standard" induction for the first example, but "strong" induction for the second?
- **Answer:** I use standard induction whenever I can, because it is a simpler proof technique. The second proof would break down if standard induction was used instead of strong induction, because you would need to assume something that is not part of the "inductive hypothesis," during the inductive step (and this is not allowed). Try it and see!

Note: It would **not** be a "mistake" to use strong induction for the first example too! You certainly *could* prove the claim by doing this! However, your proof would probably be a bit more complicated than necessary if you did this.

- **Question:** Can other values be chosen for the "breakpoint" β in the example proof (for strong induction)?
- **Answer:** Yes, other values can be used. You *can* choose β to be 0 instead of 1.

  However, this complicates the inductive step because the case that $k = 0$ (so that $k+1 = 1$) then needs to be handled as a special case in the inductive step: The argument needed here is different from the one that can be used when $k \geq 1$.

  This might make it a bit harder to make the proof simple and easy to read and understand.

  One can choose β to be 2 (or larger) as well... but, since the argument needed to establish the result is the same, whenever, $k \geq 1$, this will probably result in a proof that is a bit longer and more repetitious than it needs to be.

Sometimes you will only discover the "best" choice for β after you have picked a different value and have started to write a proof.

This is one of the reasons why you should ***allow lots of time to write proofs***, especially if you are not used to doing this — you might find that you can improve your proof by starting over again and organizing it differently.

- **Question:** Do *my* proofs need to look like this?
- **Answer:** Yes... and no.

  Yes, you *must* be using mathematical induction correctly. Your proofs must be based on the "principles" of induction (and descriptions of how to apply these) that are in these notes.

  No, you *do not* have to follow the instructor's writing style, or anyone else's. *Everybody* writes differently. That's OK, as long as your writing is clear and correct.

A Mistake To Avoid: Not Writing Enough. While *your* proofs do not need to be as long as the instructor's, you should always make sure to write down the following things — as clearly, carefully, and *completely* as you can:

- the ***claim*** that you are trying to prove
- the ***proof technique*** that you are using to prove this

- whatever it is that you are "inducting on," if you are using mathematical induction
- what you are proving in the ***basis***, if you are using mathematical induction
- what the ***inductive hypothesis*** is, if you are using mathematical induction
- what the ***inductive claim*** is, if you are using mathematical induction

You also need to include enough *detail* to allow somebody else who ***does not*** know a proof of the claim to know one, after reading what you have written.

Finally, you should make sure that your proof is a ***written document:*** Your proof should be a sequence of paragraphs, including complete and grammatically correct sentences — with a little bit of mathematical notation included.

It is a mistake ***not*** to do this, because

- markers do not read minds, and
- markers are not supposed to "assume" that you know how to prove something: You have to *show* them that you can.

A Mistake To Avoid: Missed Cases. It is easy to "miss a case" in a proof by induction — especially when strong induction is being used. For example, one might forget that the case "$k = 1$" has to be handled separately in the example proof (for strong induction) that is given above.

Your proof is incomplete (and you have certainly *not* established the desired result) if this happens.

Indeed, this is — probably — the mistake that students make, most often, when they are trying to prove something using mathematical induction — after "not writing enough," and leaving out half of the proof.

Recommendation: Take the time to work through the first few examples by hand. If you are proving that some property $P(n)$ is satisfied whenever $n \geq \alpha$, take the time to check that your proof really does explain why $P(\alpha)$, $P(\alpha+1)$, $P(\alpha+2)$ and $P(\alpha+3)$ are all true — doing this slowly and carefully, and checking as much as you can.

If you've missed a case then — more often than not — this is all that you will need to do in order to discover that!

Another Mistake: Forgetting What You are Proving. Here is an extreme (and somewhat silly) example of this: Suppose that you modified the second "example proof" in the following way:

- In the basis, you proved that $g_n \leq 5 \cdot 3^n + 7 \cdot 2^n$ when $n = 0$ and $n = 1$.
- For the inductive step you assumed the

  Inductive Hypothesis: $g_i = 5 \cdot 3^i + 7 \cdot 2^i$ for every integer i such that $0 \leq i \leq k$

  in order to try to establish an

  Inductive Claim: $g_{k+1} \geq 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$

Something to think about before you continue: So, what is the problem here? Why has practically *nothing* actually been proved?

The **mistake** is that there is no single property, "$P(n)$," that is considered in the basis, used to produce the inductive hypothesis, *and* used to form the inductive claim too. Three different properties got considered instead... so that the "proof" would not, really, establish any of them!

Students make this mistake more often than you might think — especially on tests! In particular, it is *very* easy to make this mistake if you have not "written enough down."

Yet Another Mistake: Avoiding Mathematical Induction When You Actually Need It. Let's consider the second problem, once again, and suppose you were asked to give a proof of the claim on a test.

It is possible (even likely) that quite a few students would give an answer that confirms that $g_n = 5 \cdot 3^n + 7 \cdot 2^n$ when $0 \leq n \leq 4$ and then write something like "dot, dot, dot... the same argument holds for larger n."

If the question is worth ten marks then I would probably award at most one or two marks (or, maybe, no marks at all!) for this kind of answer.

Sometimes, properties hold for small (nonnegative) integers — even for lots of them — but do not hold for larger ones.

And... sometimes... the reason why I am choosing a problem is to try to make sure that you know how to use a specific *proof technique,* namely, mathematical induction. Giving me an answer that *avoids* this technique will not, in any way at all, show me that you know how to do this.

A Related Problem: I have noticed, in the past, that students who "avoid mathematical induction like the plague" tend to "avoid recursive algorithms and programs like the plague" as well. Mathematical induction and recursion are both important for this course and you will, occasionally, be required to understand and use *both*.

Final Mistake: Using Mathematical Induction When it is *not* Needed. On the other hand, students sometimes use mathematical induction when it is not needed at all: Sometimes it is possible to prove that a property "$P(n)$" holds for all integers $n \geq \alpha$ by giving a much simpler argument (possibly, just by checking and repeating a definition or applying another result that you already know).

This is probably happening, when you are writing a proof, if you never actually *use* the "inductive hypothesis," in the inductive step, when you are proving the inductive claim.

Conclusion

I apologize if you are disillusioned or discouraged after reading the above!

That said: In my experience, writing proofs *can* be tricky when you start out, but this *does* often get easier with practice.

Showing your proofs to somebody else can often be very helpful too: We are ***all*** our own worst editors, and somebody else can often spot a mistake that we have made and missed, even though we have checked our own work over and over again.

When the rules allow it, please *do* ask other students to comment on your proofs, and please *do* agree to this when other students ask you to do the same. Make sure that you are constructive and polite, though, if there are errors that you've spotted!

References

- Susanna Epp
  Discrete Mathematics with Applications (Fourth Edition)
  Brooks/Cole, 2004

  This book has often been used as the textbook for MATH 271. Apart from some minor changes in wording, the "principles" of mathematical induction and descriptions of how to apply these have been taken from this reference.

- My personal experience... I have been marking students' proofs that use mathematical induction, in one course or another, for quite a while now! This is the basis for the discussion of common mistakes (and some recommendations about how to avoid them) found in these notes.