Reading #1

Review of Proofs and Mathematical Induction

Mathematical Proofs

What is a Mathematical 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.

Examples of Axioms

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.

  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*.

Theorems and Proof Techniques

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!
So, you will see one more theorem that you may use, later on, by the end of this set of notes.
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

Theorem.

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

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. □

Why This is Not a Proof: 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.

Why are Mathematical Proofs Important?

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

How You Can Tell Whether Something* is *a Mathematical Proof:
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!

More About 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 claims that are not actually *true*)... but
Writing a mathematical proof down, once you have discovered it is a ***skill*** that can be taught and learned... but requires *practice*.

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 me 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.

Mathematical Induction

Mathematical induction is a *proof technique* (or pair of related ones) that you already learned about in MATH 271 and that is *extremely* useful for proving the correctness and efficiency of algorithms and data structures.
In CPSC 331 you would initially have seen the instructor present proofs that use mathematical induction for this.
You would then (occasionally) have been required to write your own proofs in that course.
You ***will*** be required to do much more of this in CPSC 413 and later theory courses that you choose to take.

Principle of Mathematical Induction: Standard Form

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 $n \geq \alpha$.

How To Apply This

One way to prove that $P(n)$ is true for every integer $n \geq \alpha$ is to do the following.

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: A *Correct* Proof of the Previous Theorem

Once again, consider the problem of proving that

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

for every integer $n \geq 0$.
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.

A *correct* proof of the previous theorem, using this proof technique, as follows.

Proof. The claim will be proved using mathematical induction on n. The standard form of mathematical induction will be used.

Basis: If $k = 0$ then

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

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

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

when $k = 0$.

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

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

(and nothing more) to prove the following

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

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 complete the inductive step. It now follows that

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

for every integer $n \geq 0$. □

A Tedious (But Somewhat Important) Exercise

Perhaps you are wondering whether this is a mathematical proof at all!
Tedious Exercise: Go to your MATH 271 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.

Principle of Mathematical Induction: Strong Form

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 $n \geq \alpha$.

How To Apply This

Another way to prove that $P(n)$ is true for every integer $n \geq \alpha$ is to do the following.

1. ***Choice of Breakpoint:*** Choose an integer β such that $\beta \geq \alpha$.
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 Proof

Theorem. *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 $n \geq 0$.

How To Prove This: One can apply the above method by setting...

- $P(k)$ to be the property that if $k \geq 0$ then $g_k = 5 \cdot 3^k + 7 \cdot 2^k$,
- setting α to be 0,
- and setting β to be 1, so that the cases $k = 0$ and $k = 1$ will both be considered in the basis.

Proof. The result will be proved using mathematical induction on k. The strong form of mathematical induction will be used, and the cases $k = 0$ and $k = 1$ will both be considered in the basis.

Basis: If $k = 0$ then $g_k = g_0 = 12$ as defined above, and

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

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

If $k = 1$ then $g_k = g_1 = 29$ as defined above, and

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

as well, so that $g_k = 5 \cdot 3^k + 7 \cdot 2^k$ 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 $0 \leq i \leq k$

(and nothing more) to prove the following

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

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

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

as required to complete the inductive step.

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

Which Form of "Induction" Should I Use?

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 more complicated than necessary if you did this.

Choice of Breakpoint

- ***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 $k = 0$ (and $k+1 = 1$) then needs to be handled as a special case — 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 longer and more repetitious than it needs to be.

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

What is (Not) Important Here?

- ***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 Watch For: 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.

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. 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 $g_i \leq 5 \cdot 3^i + 7 \cdot 2^i$ when $i = 0$ and $i = 1$.
- 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: $g_{k+1} \geq 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$.

Question: So, what is the problem here? Why has practically *nothing* actually been proved?
Answer: 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!

Recommendation: Write down

- Precisely what you need to prove in the ***basis*** for your proof,
- Precisely what you can assume as the *inductive hypothesis* for your ***inductive step,*** and
- Precisely what the *inductive claim* is that you need to establish in the ***inductive step***

as soon as you can! Check that they are consistent and refer back to them, as needed, as you continue to develop your proof.

Yet Another Mistake: Avoiding Mathematical Induction When You 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 a single mark (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 CPSC 413 and you will, occasionally, be required to understand and use *both*.

Another 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 has probably happened if you never actually ***use*** the *inductive hypothesis,* in the ***inductive step,*** when you are proving the *inductive claim.*

More Mistakes To Avoid in Theory Courses

Please ***try not to do the following*** on assignments or tests in a theory course:

- *Leave Half The Answer Out:* This happens **a lot**. Markers cannot read minds and will (or should) not give you credit for information that you failed to include. Sometimes so much information is missing that it is impossible to make sense of the information that *has* been given.
- *Use Technical Terms (or Notation), Meaning Different Things, Interchangeably:* For example (related to CPSC 313), **functions**, **strings** and **languages** are very different things. So are **languages** and **Turing machines**. I recently finished marking a CPSC 313 exam and read many, many answers that made no sense at all, because these technical terms were being mixed up.
- *Give me an Example when a Proof of a General Result is Required.*
- *Give me an Essay, like Something You would Give in an English Course — Probably Describing Intuition or an Opinion — when a Mathematical Proof is Required.*

As a "theory proof" I take a **very dim view** of these things and rarely give more than one or two marks (if the question is out of ten or twenty) for them — if I give any marks, at all.
No, I do not care how long this kind of answer is, or how much time you apparently spent providing it.
By giving this kind of answer you are telling me that *you do not know the proof that is required* and, furthermore are unwilling or unable to try to provide it.
Finally, please do not. . .

- *Give Me a Picture, and Almost Nothing More, When a Proof is Required.*
- *Give Me An Answer That Does Not Include Any Written Words at All:* Sequences of apparently unrelated equations or other mathematical expressions are generally, unclear, difficult to understand, and are always unacceptable.
- *Make Up Your Own Notation or Technical Terms and Use Them without Defining Them.*
- *Find Other Ways to Tell Me That You Do Not Know How to Write.*

I try to be polite — and refer students to Writing Services, on campus — when I discover problems like these. Once again, I generally do not give very many marks for answers with these mistakes, if I give any marks for them at all.

Conclusion, and a Final Bit of Advice

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.