1 Proof Writing Guidelines

In this worksheet we have several different exercises to get you used to the CMSC250 styled format of step-by-step proofs.

Here are some guidelines you should take when writing proofs in the 250 style:

- When starting the proof, be sure to give all the objects you are working with variable names.
- It helps to number your steps, because you might want to refer to a previous step. If this reminds you too much of geometry two column proofs you can label specific steps with a marker like $(*)$ or $(**)$, for example

  we have the equation $e^{\pi i} = -1$ $(*)$.

  then by $(*)$ and algebra, $e^{\pi i} + 1 = 0$.
- If you are in doubt whether or not to skip a step, I recommend that you do not skip a step.

Here are some other guidelines:

- Suppose I have a number $n = 2r + 1$. Have I shown that n is odd yet? No! I still need to check that the expression r is an integer. This justification should be one of its own lines in the proof. The lesson here is make sure you have verified **all parts** of a definition *in writing* before claiming something is of that specific definition type.
- What does it mean for an integer n to not be divisible by 3? It means that there is some integer q where either

  $$n = 3q + 1 \text{ or } n = 3q + 2.$$

  This follows from something called the **remainder theorem** for integers. What if we replace 3 with some other number?
- In discussion I will show how to structure a proof by cases.

1. Suppose $x \in \mathbb{N}^{\leq 4}$ (That is, the set of natural numbers less than or equal to 4). Then, prove that $n^3 \leq 3^n$.
2. Prove (by cases) that 100 is not the perfect cube of a natural number. (Hint: there are two cases to consider. The first problem might help.)
3. Answer each question, and prove your answer is correct.
   (a) For any $m, n \in \mathbb{Z}$ is $6m + 8n$ even?
   (b) For any $m, n \in \mathbb{Z}$ is $10mn + 7$ odd?
   (c) For any $c \in \mathbb{Z}$ what can we say about $(c + 1)^2 - (c - 1)^2$?

4. Suppose $a \in \mathbb{Z}$ is an odd number. Prove that $a^2 = 8m + 1$ for some $m \in \mathbb{Z}$ (that is, a^2 is n more than a multiple of 8). There are many ways to do this problem.

5. Suppose m is an even integer. Prove that $m(m + 2)$ is a multiple of 8.

6. (Challenge Problem) Suppose p is a prime number greater than 3. (A prime number p is a positive integer which has no positive integer divisors other than 1 and itself. For example, 2, 3, and 101 are prime, but 15 is not (since 3 divides 15). Prove that p^2 is 1 more than a multiple of 24, that is there exists some integer k such that $p^2 = 24k + 1$. (Hint: at some point you will have to use the result of the previous problem.)

2 Indirect Proof

In this document we will outline some typical examples of where indirect proofs will be used.

1. This problem gives you some more practice with the divides $|$ notation.

   (a) Prove by use of the contrapositive method that if $a \nmid b$ and $a \mid c$, then $a \nmid (b + c)$.

   (b) Prove the result in the first part, but using contradiction instead. (Try doing this part if you're having trouble with the first part)

2. Prove that if $2 \mid a^2$, then $2 \mid a$. Which proof method should we use, contradiction or contrapositive?

3. Prove by contradiction that there are no integers a and b such that $a^2 - 4b = 2$. (You will need to use the previous problem at some point in your argument.)

4. Prove that u is an irrational number if and only if $1 + 3u$ is an irrational number. If you are feeling particularly saucy today, prove one direction using contradiction and another direction using contrapositive. (Reminder that proving an if and only if implication $P \iff Q$ requires proving both $P \implies Q$ and $Q \implies P$.)

5. Prove that for all positive real numbers r and s that $\sqrt{r + s} \neq \sqrt{r} + \sqrt{s}$. So the non-identity called the "freshman dream" is not true.

6. (a) Suppose a, b, and c are odd integers. Prove that the polynomial $p(x) = ax^2+bx+c$ only has irrational roots.

   (b) After you have proved this, look up the Rational Root Theorem on your own time. Try to find a proof of this statement. Is the proof direct or indirect? Does it depend on facts which you don't know? Is the approach the same as this exercise (This is a judgement which depends on your taste).

   (c) Think about this part after tomorrow's lecture. How similar is this proof to the proof that $\sqrt{2}$ is irrational? In some sense this part is even more subjective than the previous part.

3 Why do we need proofs?

Colloquially, when people say that some evidence "proves" something, they refer to some object or conversation which demonstrates that a given claim is true. Proof is supposed to be the evidence in favor or demonstrating the claim. In computer science and mathematics, the use of the word "proof" is similarly used. In computer science and mathematics, the general thought process is on various ideas and their consequences. A big focus is on why certain claims are true or false. The reason why there is a big focus on why things are true is that these explanations give some motivation for why other claims are true as well.

In my experience, for very simple claims involving very basic objects, the majority of people can give a reasonable explanation for why such a claim is true or false. For example, take the following claim:

The sum of two even numbers is even.

Most people understand an even number to be a number $2n$, where n is an integer. If we have two such even numbers $2n$, and $2m$, then their sum is $2n + 2m = 2(n + m)$. Since $n + m$ is an integer the claim follows. In its most basic form, this is an example of a proof. For our purposes, a proof is nothing more than a logical explanation about why a claim is true. The word "logical" is important, because it means that proofs can be either be correct or incorrect. Either all the steps in the explanation logically follow from the previous few, or there is a mistake somewhere, rendering the proof incorrect. Since our definition of "proof" is a logical explanation about why a claim is true, then a proof is the best way, in fact the only way, to demonstrate the truth of any given claim.

Since in this book we will introduce several kinds of objects and present some of their properties. Often, showing an object has a property is also a claim, and will require proof. So it makes sense to first introduce the concept of proofs themselves before diving into the math.

In many classes which teach students how to write proofs, a lot of emphasis is given on certain structure and grammatical conventions and tone of language when writing a proof. In reality this sort of emphasis is superfluous. The advantage it gives the instructors is that it makes homework and exams easier to grade. However, that is not to say you can get away with poor writing in proofs, especially if you are presenting proofs for other people to read.

4 Direct Proofs

Here are two examples of direct proofs.

Proposition 1. 5 *is an odd number.*

Proof. Since we can write $5 = 2(2) + 1$, it follows that 5 is odd. □

Proposition 2. *The sum of two odd numbers is even.*

Proof. Suppose m and n are odd numbers. Then we may write

$$m = 2k + 1$$
$$n = 2j + 1$$

where k and j are integers. Then

$$m + n = 2k + 2j + 2 = 2(k + j + 1)$$

is even, since $k + j + 1$ is an integer. □

The claims were kept simple to better indicate their structure. Notice that the first claim has the "object has property" form. The second claim has the "hypothesis implies conclusion" form, once we rewrite the claim in the following form:

Proposition 3. *If m and n are odd numbers, then their sum $m + n$ is an even number.*

Notice how the proof of this claim takes two unspecified odd numbers and verifies that their sum is even. This is the general strategy for showing that a combination of objects with various properties will satisfy some conclusion.

5 Structure of Logical Claims

In general, there are three kinds of claim "structures" which encompass the vast majority of claims that people want to prove. These are the "object has property" structure, the "hypothesis implies conclusion" structure, and the "situations are equivalent" structure. We expand more on these below.

An "object has property" structure concerns some specific object or collection of objects, with certain properties known beforehand. The nature of the claim is that the object has some other property, which is usually not totally obvious from the properties that are known beforehand. Here is an example of such a claim:

Proposition 4. *The set of natural numbers $\mathbb{N}$ are countable.*

Here the object in question is specific, being the set of natural numbers $\mathbb{N}$ and the property is the property of countability of a set. However, based on the definition of countability, this claim is trivially true based on the definition of countability. Is there anything we might glean from it? Here is another similar claim, but instead with a collection of objects.

Proposition 5. *Any subset of the natural numbers $\mathbb{N}$ is countable.*

Here, the property remains the same, but we have expanded to a collection of objects, namely the subset of natural numbers. However, this claim is still trivially true based on the definition of countability. Maybe there is a more general claim which is not immediately obvious? There is, once we replace $\mathbb{N}$ with any countable set.

Proposition 6. *Any subset of a countable set is countable.*

We use this set of examples to indicate that a claim involving a very specific object (the natural numbers) can be made into a claim that is much more general (and not immediately obvious). In this way, a lot of mathematics is built from the "ground up" from small examples which get more general.

5.1 Hypothesis implies Conclusion

The other type of claim usually investigated has a "hypothesis implies conclusion" structure. With these claims, the hypothesis usually involves one or several objects with various properties, and the claim is that some given conclusion will follow. That is, these types of claims usually go the following way: "Suppose A, B, ... satisfy the following properties or relations. Then a certain conclusion follows." Here is a more specific example:

Proposition 7. *Suppose A, B, and C are sets with $A \subset B$ and $B \subset C$. Then $A \subset C$.*

Here, the objects are A, B, and C with some properties involving subset relations. The conclusion is another property involving subset relations.

5.2 Situations are Equivalent

Similarly to the "hypothesis implies conclusion" proof structure, the "situations are equivalent" structure involves a set of two or more hypotheses. The claim is that each of these hypotheses implies the other. Usually these claims will have the following form:

Proposition 8. *The following are equivalent:*

- *Situation A*
- *Situation B*

To prove this proposition is true is the same as showing both the claims "Situation A implies Situation B" and "Situation B implies Situation A".

For the situation with 3 or more hypotheses, one might imagine that one needs to show a lot more than two claims, and the situation may get out of hand quickly. However, this is not the case, since it turns out implication is transitive. That is, if "Situation A implies Situation B" and "Situation B implies Situation C", then it follows that "Situation A implies Situation C". So if we are to show situations A, B, and C are equivalent, one possible way to show this is to show the following claims to be true:

- Situation A implies Situation B
- Situation B implies Situation C
- Situation C implies Situation A.