APPENDIX

I

Common Errors In Proofs

The following list describes some common errors made by students while creating proofs. The list is intended to help you avoid making the same errors.

1. **An example does not constitute a valid proof.**

   Suppose you want to prove the claim:

Let $a, b, c \in \mathbb{Z}$. If $a\|(bc)$ then either $a\|b$ or $a\|c$.

   Incorrect Proof: Let $a = 5$, $b = 3$, and $c = 10$. Then $a|(bc)$ because $5|30$. Also, since $5|10$ it is true that $a|c$, so the claim is true.

   The error in the proof: In this case it is easy to see that the attempted proof is not valid, because the claim is not true. Consider the case where $a = 6, b = 3$, and $c = 8$. Then $a|(bc)$ because $6|24$, but $6 \nmid 3$ and $6 \nmid 8$, so a divides neither b nor c.

   The moral: An example does not prove a universally quantified claim (such as $\forall a, b, c \in \mathbb{Z}$, $a|(bc) \rightarrow (a|b) \vee (a|c)$). However, a single counter example does *disprove* such a claim.

2. **Introducing the same variable for two different values is an error.**

   Suppose you want to prove the assertion:

Let $a, b, \in \mathbb{Z}$ where $a = 1 \bmod 3$ and $b = 2 \bmod 3$. Then $(a + b) = 0 \bmod 3$.

   Incorrect Proof: Since $a = 1 \bmod 3$ there is an integer k in $\mathbb{Z}$ such that $a = 3k + 1$. Since $b = 2 \bmod 3$, we can write $b = 3k + 2$. Thus $a + b = (3k + 1) + (3k + 2) = 6k + 3 = 3(2k + 1)$, so $(a + b) = 0 \bmod 3$.

   The error in the proof: The attempted proof assumes that $b = a + 1$ since $b - a = (3k + 2) - (3k + 1) = 1$. So the proof is only valid for that limited set of choices for a and b.

   A correct proof: Since $a = 1 \bmod 3$ there is an integer k in $\mathbb{Z}$ such that $a = 3k+1$. Since $b = 2 \bmod 3$, there is an integer n in $\mathbb{Z}$ such that $b = 3n + 2$. Therefore $a + b = (3k + 1) + (3n + 2) = 3k + 3n + 3 = 3(k + n + 1)$, so $(a + b) = 0 \bmod 3$.

3. **A proof by contradiction starts with an assumption that you eventually want to reject. The rejection isn't because you provide a proof that the opposite of the assumption is true. The rejection is due to the assumption leading to a conclusion that we know is impossible.**

   Suppose you want to use a proof by contradiction to prove the claim:

If $a \in \mathbb{R}$ and $a > 1$, then $0 < \frac{1}{a} < 1$.

   ⟨Since $a \cdot \frac{1}{a} = 1 > 0$ and $a > 1 > 0$, we know that $\frac{1}{a}$ must also be positive, so I will drop the $0 < \frac{1}{a}$ part of the claim for the rest of this discussion.⟩

   Not really a "proof by contradiction": Assume that $1 \leq \frac{1}{a}$. Since $a > 1$, we can divide both sides by a (without reversing the inequality) to get $\frac{a}{a} > \frac{1}{a}$ so $1 > \frac{1}{a}$. This contradicts the assumption that $1 \leq \frac{1}{a}$. Thus it must be that $a > \frac{1}{a}$.

   Why the proof is inadequate: The proof above is really a direct proof. We could shorten it to:

   Since $a > 1$, we can divide both sides by a (without reversing the inequality) to get $\frac{a}{a} > \frac{1}{a}$ so $1 > \frac{1}{a}$.

   The assumption was never really used in an important way.

   A real proof by contradiction: Assume that $1 \leq \frac{1}{a}$. Since $a > 0$, we can multiply both sides of the assumed inequality by a without reversing the inequality sign to get $a \cdot 1 \leq a \cdot \frac{1}{a}$ which is the same as $a \leq 1$. But this contradicts the hypothesis $a > 1$. This contradiction was caused by assuming that $1 \leq \frac{1}{a}$, so to remove the contradiction it must be the case that $1 > \frac{1}{a}$.

   ⟨This contradiction proof used the tautology $[P \to Q] \Leftrightarrow [(P \wedge (\neg Q)) \to (\neg P)]$. It also actually used the assumption as a key element in deriving the contradiction.⟩

4. **Declaring a proof to be trivial is not in and of itself a complete proof.** Especially when it doesn't meet the requirements to be an actual trivial proof (namely, if the right hand side of the implication is not always true, then a trivial proof is not possible). Don't use the word "trivial" to mean "too easy to bother writing the details". The word has a technical meaning when discussing proofs.

5. **Even if the conclusion in an implication is false, the implication is not necessarily false.**

   Suppose you want to prove the claim:

Let $k \geq 1$ with $k \in \mathbb{Z}$. If $2^k \equiv 0 \bmod 3$ then $8 \equiv 1 \bmod 3$.

   Incorrect Proof: The claim is false. Here are two counter-examples: if $k = 1$ then $8^1 \not\equiv 1 \bmod 3$ ($8 = 2 \cdot 3 + 2$ so $8 \equiv 2 \bmod 3$). If $k = 3$ then $8^3 = 512 \not\equiv 1 \bmod 3$ ($512 = 170 \cdot 3 + 2$). In fact, whenever k is odd, $8^k \equiv 2 \bmod 3$.

   The Error: The claim is actually true.

   Correct Proof: Since $k \geq 1$, $2^k = 2 \cdot 2 \cdots 2$ is **not** divisible by 3. Thus 2^k is never congruent to 0 mod 3 for $k \geq 1$. That means the hypothesis of the claim is false, so the implication is true. (This is a vacuous proof.)