CSc 144 — Discrete Structures for Computer Science I
(McCann)

(Last Modified: March 2023)

Direct Proof Examples

1. **Conjecture:** $n^2 - 3$ is even if n is odd, $n \in \mathbb{Z}$.

   Discussion: The first thing to do is identify the hypothesis and the conclusion. Why? Because in a direct proof, we are allowed to assume the hypothesis, giving us a piece of information that we can use as a starting point for our argument. Knowing the conclusion gives us a goal to work toward.

   In this conjecture, the "if" is placed in the middle. We know that the hypothesis follows the "if" (unless the form is "only if"), and so:

   - The Hypothesis: n is odd.
   - The Conclusion: $n^2 - 3$ is even.

   As is usually the case in a conjecture for which the direct proof method is suitable, we have a basic piece of information to start from, and a more complex destination. In this case, we need to build from n to $n^2 - 3$ and see if the resulting expression tells us anything about evenness.

   One convenient way to think about the relationship between odd and even numbers is that every odd number is one more than an even number. Thus, we can say that $n = 2k + 1$, where k is an integer. Why $2k$? Because we can keep the domain general (integers) and still capture the idea that we have a value that's one more than an even integer (because twice any integer is even).

   To build toward $n^2 - 3$, we first need to square our new expression for n: $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$.

   Almost there: After subtracting three, we see that $n^2 - 3 = 4k^2 + 4k - 2$. But what does that tell us about the evenness of $n^2 - 3$? Perhaps not much in that form, but what if we factor a '2' out of each term? $4k^2 + 4k - 2 = 2(2k^2 + 2k - 1)$. Just above, we used the idea that doubling an integer produces an even number. Here we see that $n^2 - 3$ is also the doubling of an integer. This means that $n^2 - 3$ must be even, completing our argument.

   Of course, this sort of multi-paragraph description isn't the form we want to use to write our proof; it is far too wordy. Instead, write your proofs as I've demonstrated in class. Here's the proof in that form:

   > **Proof (Direct):** Assume that n is odd.
   > Let $n = 2k+1,\ k \in \mathbb{Z}$. $n^2-3 = (2k+1)^2-3 = (4k^2+4k+1)-3 = 4k^2+4k-2 = 2(2k^2+2k-1)$.
   > As $2(2k^2 + 2k - 1)$ is of the form $2j$ where $j \in \mathbb{Z}$, we know that $n^2 - 3$ is even.
   > Therefore, $n^2 - 3$ is even if n is odd.

   The following would be even better, as it makes the math much easier to follow:

   > **Proof (Direct):** Assume that n is odd. Let $n = 2k + 1,\ k \in \mathbb{Z}$.
   >
   > $$\begin{aligned} n^2 - 3 &= (2k+1)^2 - 3 \\ &= (4k^2 + 4k + 1) - 3 \\ &= 4k^2 + 4k - 2 \\ &= 2(2k^2 + 2k - 1) \end{aligned}$$
   >
   > As $2(2k^2 + 2k - 1)$ is of the form $2j$ where $j \in \mathbb{Z}$, we know that $n^2 - 3$ is even.
   >
   > Therefore, $n^2 - 3$ is even if n is odd.

   Remember, stating the assumption(s) at the start is something we think is a good idea, but stating them is not required. The "Proof (Direct)" at the start, the correct and easy-to-follow argument in the middle, and the "Therefore" followed by a restatement of the conjecture at the end are all required.

2. **Conjecture:** $c^2 + c > 2c,\ \forall c \geq 6$

   Discussion: Inequalities such as this are also candidates for direct proofs, though other proof techniques (e.g., induction) are also appropriate.

   At first glance, the conjecture appears to have two problems: It is not in an "if – then" form, and c has no stated domain. Neither is a problem in practice. Because this is an algebraic problem without a domain, the assumption is that the domain is all real numbers. We make this assumption because it is the most reasonable one to use; if the author of the conjecture had wanted a more restrictive domain, s/he would have stated it. Similarly, when conjectures involve odds and evens, we often don't state that the domain is $\mathbb{Z}$, because that is the most reasonable general assumption in that situation.

   To adjust the form, we observe that we can restate the conjecture as "if $c \geq 6$, then $c^2 + c > 2c$" without changing the problem. Now the hypothesis and conclusion are clear:

   - The Hypothesis: $c \geq 6$.
   - The Conclusion: $c^2 + c > 2c$.

   In the previous example, we started with the given information and built toward the conclusion. In this case it will be easier to start by simplifying the conclusion. Specifically, we can subtract c from both sides to produce the equivalent inequality $c^2 > c$.

   We can then divide both sides by c, but first remember that dividing both sizes of an inequality by a negative value would change the direction of the inequality. In this case, we are given that c will be no less than 6; thus, c will always be positive, and dividing by c won't change the direction. After division, the resulting inequality is $c > 1$.

   What does that mean? It means that $c^2 + c > 2c$ is true when $c > 1$, because they are equivalent expressions. We already know that $c \geq 6$, which means that the conjecture must be true.

   Here's the final argument:

   > **Proof (Direct):** Assume that $c \geq 6$.
   >
   > Subtracting c from both sides of $c^2 + c > 2c$ gives $c^2 > c$. Because c is always positive, dividing both sides of $c^2 > c$ by c produces $c > 1$. We are given that $c \geq 6$, which tells us that c will always be greater than one.
   >
   > Therefore, $c^2 + c > 2c,\ \forall c \geq 6$.

   As this example shows, direct proofs do not need to begin with the assumptions; they can start in other ways, such as with finding equivalent expressions for the conclusion and working to a point at which the assumptions are useful for continuing the argument or concluding it – both are demonstrated in this proof.