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

(Last Modified: March 2023)

Indirect ("Contra") Proof Examples

Introduction: Here are three conjectures that have straightforward proofs using both proof by contraposition and proof by contradiction. The solutions can be found starting on the next page. But try to prove them yourself first, and only then look at the answers!

Review of the proof techniques:

- In a direct proof of a conjecture of the form $p \to q$, we assume that p is true, and show that q is true.
- In a proof by contraposition (a.k.a., a proof of the contrapositive), we perform a direct proof on the contrapositive of the conjecture. This works because $p \to q \equiv \neg q \to \neg p$. That is: To prove the truth of $p \to q$, we assume that $\neg q$ is true, and show that $\neg p$ is true.
- In a proof by contradiction, we assume that both p and $\neg q$ are true, and reason until we reach a contradiction. This method works because $\neg(p \to q) \equiv p \wedge \neg q$; if we assume that $p \wedge \neg q$ is true, and we use logically valid reasoning to reach a contradiction, then the logical error must be with the starting assumption. If $p \wedge \neg q$ is not true, then its negation, which is equivalent to $p \to q$, must be true.

The Conjectures

1. Consider this conjecture: If $(n-2)(n+1)$ is odd, then n is even.
   (a) Prove this conjecture using a proof by contraposition.
   (b) Prove this conjecture using a proof by contradiction.

2. Consider this conjecture: If $9 \nmid (a+b+c)$, then a, b, and c are not consecutive multiples of three.
   (a) Prove this conjecture using a proof by contraposition.
   (b) Prove this conjecture using a proof by contradiction.

   ("$a \nmid b$" means the same thing as "not $a \mid b$." If you don't remember what $a \mid b$ represents, see Appendix A in "Kneel Before Zodd" or page 252 in the 8th edition of Rosen.)

3. Consider this conjecture: Whenever r^3 is irrational, $\sqrt{r^3}$ is irrational, assuming that $r \in \mathbb{R}^+$.
   (a) Prove this conjecture using a proof by contraposition.
   (b) Prove this conjecture using a proof by contradiction.

   (Remember: A rational number can be expressed as the ratio of two integers.)

(Continued . . .)

The Proofs

1. Consider this conjecture: If $(n-2)(n+1)$ is odd, then n is even.

   (a) Prove this conjecture using a proof by contraposition.

> *Thinking Before Doing:* First, let's identify the pieces within the conjecture. The structure is a basic "if – then," which tells us that "$(n-2)(n+1)$ is odd" is the antecedent and that "n is even" is the consequent. To form the contrapositive, we need to negate both pieces and swap them. Thus, the new antecedent is "n is odd," and the new consequent is "$(n-2)(n+1)$ is even." All that remains is to assume the truth of the new antecedent and use it to show the true of the new consequent.
>
> –
>
> Proof (by contraposition):
>
> Assume that n is odd, and show that $(n-2)(n+1)$ is even.
>
> As n is odd, we know it to be one more than an even. Let $n = 2k+1$, where $k \in \mathbb{Z}$.
>
> To show that $(n-2)(n+1)$ is even, we start by replacing each n with $2k+1$: $(n-2)(n+1) = ((2k+1)-2)((2k+1)+1)$. Next, we simplify the expression: $((2k+1)-2)((2k+1)+1) = (2k-1)(2k+2)$. We can factor a 2 from $2k+2$: $(2k-1)(2k+2) = (2)(2k-1)(k+1)$. Because our expression is twice an integer, and our expression is equal to $(n-2)(n+1)$, we have shown that $(n-2)(n+1)$ is even.
>
> Therefore, if $(n-2)(n+1)$ is odd, then n is even.

   (b) Prove this conjecture using a proof by contradiction.

> *Thinking Before Doing:* For a proof by contradiction, we assume that the original antecedent is true and also that the original consequent is false. That is, we assume that $(n-2)(n+1)$ is odd, and that n is also odd. Our mission is "find a contradiction," so we start reasoning and hope that we find one! (We don't have to hope too hard; we know the conjecture is true, so we will find a contradiction if we keep our eyes open for it.)
>
> –
>
> Proof (by contradiction):
>
> Assume that both $(n-2)(n+1)$ and n are odd.
>
> As n is odd, it is one more than an even. Let $n = 2k+1$, where $k \in \mathbb{Z}$.
>
> Taking a cue from our assumptions, let's see where playing with $(n-2)(n+1)$ leads us. We start by replacing each n with $2k+1$: $(n-2)(n+1) = ((2k+1)-2)((2k+1)+1) = (2k-1)(2k+2)$. Factoring out a 2 from $2k+2$ shows that $(2k-1)(2k+2) = 2(2k-1)(k+1)$. Because this represents twice an integer, and is equal to $(n-2)(n+1)$, we have shown that $(n-2)(n+1)$ is even.
>
> But that cannot be true! We started by assuming that $(n-2)(n+1)$ is odd, but have now shown that it must be even. It cannot be both; this is a contradiction.
>
> Therefore, if $(n-2)(n+1)$ is odd, then n is even.

(Continued . . .)

2. Consider this conjecture: If $9 \nmid (a+b+c)$, then a, b, and c are not consecutive multiples of three.

   (a) Prove this conjecture using a proof by contraposition.

> *Thinking Before Doing:* Step 1: Understand the problem! The antecedent ($9 \nmid (a+b+c)$) says that 9 does does not divide the sum evenly. Put another way, the sum is not a multiple of 9. The consequent says that all three values are multiples of three (that is, members of the sequence …, -3, 0, 3, …) and they are consecutive, meaning that they are next to each other in that sequence. Two examples are -3, 0, 3 and 15, 18, 21.
>
> Because we are doing a proof by contraposition, we need to negate and swap the antecedent and consequent before starting the proof.
>
> –
>
> Proof (by contraposition):
>
> Assume that a, b, and c are consecutive multiples of three, and show that $9 \mid (a+b+c)$.
>
> Let $a = 3k$, where $k \in \mathbb{Z}$, be the smallest of the three consecutive multiples of three, and c be the largest. That makes b the next multiple of three after a, and so must be three more than a: $b = 3k+3$. It follows that $c = 3k+6$.
>
> $a+b+c = (3k)+(3k+3)+(3k+6) = 9k+9 = 9(k+1)$, showing that $a+b+c$ is evenly divisible by 9, or that $9 \mid (a+b+c)$.
>
> Therefore, if $9 \nmid (a+b+c)$, then a, b, and c are not consecutive multiples of three.

   (b) Prove this conjecture using a proof by contradiction.

> *Thinking Before Doing:* See the above proof for the explanations of the meanings of the parts of the conjecture. Because we are doing a proof by contradiction, we assume the original antecedent, plus the negation of the original consequent, and reason about them until we discover a contradiction.
>
> –
>
> Proof (by contradiction):
>
> Assume that a, b, and c are consecutive multiples of three, and assume that $9 \nmid (a+b+c)$.
>
> Let $a = 3k, b = 3k+3$, and $c = 3k+6$, where $k \in \mathbb{Z}$. $a+b+c = (3k)+(3k+3)+(3k+6) = 9k+9 = 9(k+1)$, showing that $a+b+c$ is evenly divisible by 9, or that $9 \mid (a+b+c)$.
>
> This contradicts the other half of our assumed information, that $9 \nmid (a+b+c)$. (No value is, and is not, evenly divisible by 9.)
>
> Therefore, if $9 \nmid (a+b+c)$, then a, b, and c are not consecutive multiples of three.

(Continued …)

3. Consider this conjecture:

(a) Prove this conjecture using a proof by contraposition. Whenever r^3 is irrational, $\sqrt{r^3}$ is irrational, assuming that $r \in \mathbb{R}^+$.

Thinking Before Doing: Reflexivity and irreflexivity are not opposites, but rational and irrational are! (Isn't English a fun language?) This fact makes proof by contraposition a good choice for this conjecture, because it's much easier to work with something rational than something irrational. Here, we'll get to assume that $\sqrt{r^3}$ is rational, and will need to show that r^3 is rational. The key will be to construct a representation for $\sqrt{r^3}$ that is a fraction, and stick with fractional representations from that point forward, because to show that r^3 is rational, we'll need to end up with a fractional representation for it, too. Looking ahead, we'll have to eliminate the square root, but that's not a problem: $\sqrt{x} \cdot \sqrt{x} = x$.

– –

Proof (by contraposition):

Assume that $\sqrt{r^3}$ is rational, show that r^3 is rational.

As $\sqrt{r^3}$ is rational, we can represent it as the ratio of two integers: $\sqrt{r^3} = \frac{n}{d}$, where $n, d \in \mathbb{Z}$, and $d \neq 0$. We can 'extract' r^3 from $\sqrt{r^3}$ by squaring $\sqrt{r^3}$: $(\sqrt{r^3})^2 = r^3$, but also $(\sqrt{r^3})^2 = (\frac{n}{d})^2$. By transitivity of equality, $r^3 = (\frac{n}{d})^2$.

Remembering how to multiply fractions, we learn that $r^3 = (\frac{n}{d})^2 = \frac{n}{d} \cdot \frac{n}{d} = \frac{n \cdot n}{d \cdot d} = \frac{n^2}{d^2}$. As r^3 can be expressed as a ratio of integers, it is rational.

Therefore, whenever r^3 is irrational, $\sqrt{r^3}$ is irrational.

(b) Prove this conjecture using a proof by contradiction.

Thinking Before Doing: As always when doing a proof by contradiction, we assume the truth of the antecedent (in this case, r^3 is irrational) and of the negation of the consequent (the negation of "$\sqrt{r^3}$ is irrational" is "$\sqrt{r^3}$ is rational"), and reason until we find a contradiction. As above, we'll reason using fractions, in hopes of finding a rational representation of r^3 to contradict our assumption of irrationality.

– –

Proof (by contradiction):

Assume that r^3 is irrational and that $\sqrt{r^3}$ is rational, and show a contradiction.

As $\sqrt{r^3}$ is rational, we can represent it as the ratio of two integers: $\sqrt{r^3} = \frac{n}{d}$, where $n, d \in \mathbb{Z}$, and $d \neq 0$. Squaring $\sqrt{r^3}$ gives us a useful representation of r^3: $(\sqrt{r^3})^2 = (\frac{n}{d})^2 = r^3$.

$r^3 = (\frac{n}{d})^2 = \frac{n}{d} \cdot \frac{n}{d} = \frac{n \cdot n}{d \cdot d} = \frac{n^2}{d^2}$. As r^3 can be expressed as the ratio of the integers n^2 and d^2, it is rational. This is a contradiction of our assumption that r^3 is irrational.

Therefore, whenever r^3 is irrational, $\sqrt{r^3}$ is irrational.