Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Module 4: Proof Methods
Fall 2021

This module corresponds to the following sections from your textbook:

4. Theorem
5. Proof
6. Counterexample
20. Contradiction
21. Smallest Counterexample

1 Introduction

In 1175, Alain de Lille wrote "*mīlle viae dūcunt hominēs per saecula Rōmam*", or "a thousand roads lead men forever to Rome". You might know this phrase better by its modern formulation, "all roads lead to Rome". This proverb asserts that one can take many different routes and still end up at the same destination.

"All roads lead to Rome" encompasses the spirit of mathematical discovery; not in the sense that the Romans were mathematical prodigies, but in the sense that there is often not just one correct way to arrive at a desired result. For centuries, mathematicians have discovered and rediscovered various results by attacking the problem from various directions.

In this module, we will look at a number of techniques to prove mathematical statements. You have likely seen most of these techniques put to use in some of your previous mathematics or computing courses, possibly without even realizing it.

In the examples throughout these notes, we will prove some statements using the proof techniques we learn in each section. In our example proofs, the steps you should perform when using a given technique will be labelled in bold-italics (***like this***). When you write your proofs for the assigned problem sets, you may use this method (or another method of your choice, which equally gets the job done) to explain your work if that is asked of you.

Finally, we will use two special terms in our examples, so we define those terms here:

Definition 1 (Odd and even numbers)**.** A number $n \in \mathbb{Z}$ is odd if it can be written in the form $n = 2k + 1$ for some $k \in \mathbb{Z}$. A number n is even if it can be written in the form $n = 2k$ for some $k \in \mathbb{Z}$.

2 Direct Proof

Direct proof is, as the name suggests, the most direct way to prove a statement. A direct proof consists of using a series of known results, axioms, or other facts to establish the truth of a statement. Although the method seems straightforward, every other proof technique we will see builds off of direct proof in some way, so it's good to establish the fundamentals first!

2.1 If-Then (Conditional)

To begin, we will use the direct proof technique on statements of a certain form: "if x, then y". We call such statements **conditionals**, **implications**, or "if-then" statements.

Definition 2 (Direct proof)**.** To prove that a statement y is true given a statement x that is assumed to be true, prove that the statement "if x, then y" is true.

Since we assume x is true, showing that the statement "if x, then y" is true demonstrates that the truth of y must follow from the truth of x. Within an implication, we call x the **antecedent** and we call y the **consequent**.

Remark. The technique of direct proof is related to the *modus ponens* rule of inference. In this rule, if we know that the statements "if x, then y" and "x" are both true, then we conclude that "y" must also be true.

Example 3. Let us prove the following claim using a direct proof.

Claim. If n is an odd integer, then n^2 is an odd integer.

Proof. (***Assume the antecedent is true***) Suppose n is an odd integer.

(***State known facts***) Then $n = 2k + 1$ for some integer k. Squaring both sides, we get

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

(***Conclude the consequent is true***) Let $j = 2k^2 + 2k$. Then $n^2 = 2j + 1$, so n^2 is an odd integer. □

2.2 If and Only If (Biconditional)

Sometimes, we would like to show that two statements x and y are **logically equivalent**; that is, whenever x is true, then y is also true, and vice versa. Showing the logical equivalence of two statements can make the art of proof writing easier; if we need a result x, but we find that proving x directly is difficult, then we can find a statement y that is both logically equivalent to x and easier to prove and continue from there. A statement asserting logical equivalence is called a **biconditional** or, more colloquially, an "if and only if" statement.

At its core, showing logical equivalence is no different from writing two direct proofs and combining them.

Definition 4 (Logical equivalence)**.** To show that two statements x and y are logically equivalent, show that the statements "if x, then y" and "if y, then x" are both true.

We call the statement "if y, then x" the **converse** of the statement "if x, then y".

Claim. An integer x is even if and only if $x + 1$ is odd.

Proof. (***Suppose*** x ***is even.***) This means that $x = 2k$ for some integer k. Adding 1 to both sides gives

$$x + 1 = 2k + 1.$$

By the definition of odd, $x + 1$ is odd.

(***Suppose*** $x + 1$ ***is odd.***) This means that $x + 1 = 2k + 1$ for some integer k. Subtracting 1 from both sides gives

$$x = 2k.$$

By the definition of even, x is even. □

2.3 Trivial and Vacuous Proofs

There are two special cases of direct proof that depend on the truth values of x and y in the statement "if x, then y".

- If we can prove that y is always true regardless of the truth value of x, then the statement "if x, then y" is always true. This is called a **trivial proof**.
- If we can prove that x is always false regardless of the truth value of y, then the statement "if x, then y" is always true. This is called a **vacuous proof**. Statement 4.2 from your textbook is an example of a vacuous proof.

3 Proof by Counterexample

A **proof by counterexample** is different from a direct proof in that, instead of proving the truth of a statement, we are proving the falsehood of a statement. The name "proof by counterexample" is a bit misleading, since we are in fact *dis*proving a statement when we use this method.

Definition 5 (Proof by counterexample)**.** To prove that a statement z is false, find a counterexample that invalidates the assumed truth of z.

In the case where our statement z is an implication (if x, then y), then a proof by counterexample involves us finding a particular instance where x is true but y is false. We know what happens when this occurs:

x	y	"if x, then y"
T	T	T
T	F	F
F	T	T
F	F	T

When x is true and y is false, the implication is false. Indeed, this is the only scenario where we get this outcome! Therefore, finding a single instance where both x is true and y is false is enough to invalidate the entire statement.

Example 6. Let us disprove the following claim using a proof by counterexample.

Claim. If n is an even integer, then n^2 is an odd integer.

Proof. (***Assume the statement is true***) Let n be an even integer. Then n^2 must be an odd integer.

(***Find an instance where the antecedent is true***) Suppose $n = 2$.

(***Show that, in this instance, the consequent is false***) Then $n^2 = 4$, which is not an odd integer.

(***Conclude the assumption is false***) Therefore, the claim is false because we presented a counterexample, i.e., an even integer n for which n^2 is not odd. □

Finding counterexamples can often be difficult, so a proof by counterexample shouldn't be your first approach to a problem. Instead, try solving the problem using another strategy, and then exploit any possible weaknesses in your approach where a counterexample might arise.

As an illustration of how difficult finding a counterexample can be, consider the following claim:

Claim. For all natural numbers $n \in \mathbb{N}$,

$$\left\lceil \frac{2}{2^{1/n} - 1} \right\rceil = \left\lfloor \frac{2n}{\log_{\mathrm{e}}(2)} \right\rfloor .$$

Here, $\lceil \cdot \rceil$ denotes the ceiling function (round up to the nearest integer) and $\lfloor \cdot \rfloor$ denotes the floor function (round down to the nearest integer). If you test small values of n such as 1, 2, or 10 as a sanity check, you will see that the claimed equality holds. Even testing larger values, like 1 000 or 1 million, results in the equality still holding. Surely the equality is always true, then? Not so: the smallest value of n for which the equality does not hold is $n = 777\,451\,915\,729\,368$.

4 Proof by Contrapositive

In certain cases, it may be difficult to attack a problem by starting with a known result and deriving the conclusion. Such cases render the technique of direct proof nearly impossible. Fortunately, we don't always have to work in the forward direction, so to speak. We could instead take the desired conclusion and negate it, then show that the negated conclusion requires our known result to be negated in order for the statement to be valid. For instance, if all students in CISC 203 are fuelled by caffeine, then students who are not fuelled by caffeine are not in CISC 203. Manipulating a statement in this way is called **contraposition**, and a proof that uses this technique is called a **proof by contrapositive** or an **indirect proof**.

Definition 7 (Proof by contrapositive)**.** To prove that a statement "if x, then y" is true, prove that the contrapositive statement "if not-y, then not-x" is true.

To see that a statement and its contrapositive are logically equivalent, let's draw a truth table:

x	y	"if x, then y"	"not-x"	"not-y"	"if not-y, then not-x"
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

In our truth table, the original statement is the third column and the contrapositive is the sixth column. Since these columns contain exactly the same logical values, the two statements are logically equivalent.

Remark. The technique of proof by contrapositive is related to the *modus tollens* rule of inference, also known as denying the consequent. In this rule, if we know that the statements "if x, then y" and "not-y" are both true, then we conclude that "not-x" must also be true.

Be careful not to confuse taking the contrapositive with the logical fallacy of affirming the consequent; given the statement "if x, then y", you cannot always conclude that its converse form "if y, then x" is true.

Example 8. Let us prove the following claim using a proof by contrapositive.

Claim. If n is an odd integer, then n^2 is an odd integer.

Proof. (***Assume the negation of the consequent is true***) Suppose n^2 is not an odd integer.

(***State known facts***) Then n^2 must be even. Add n to n^2 to get

$$n^2 + n = n(n + 1).$$

Since n and $(n + 1)$ differ by one, exactly one of these terms must be even and the other odd. From this, we know that $n^2 + n = n(n + 1)$ is even, since the product of an even integer and an odd integer is even.

(***Conclude the negation of the antecedent is true***) Since the sum $n^2 + n$ is even, and since n^2 is an even integer, n is an even integer. □

Note that, as done above, it is okay to use some elementary facts without proof, such as "the sum of two even integers is even." However, be careful to not use non-obvious statements without proof.

Exercise

The above proof can be done more easily as a direct proof. Do this as an exercise.

In contrast, there is no easy method to write a direct proof for the following proposition. In this case, a proof by contrapositive is the clear choice.

Proposition 9. *Let R be an equivalence relation on a set A and let $a, b \in A$. If $a \not R\, b$, then $[a] \cap [b] = \emptyset$.*

Proof. We prove the contrapositive: Suppose $[a] \cap [b] \neq \emptyset$. So, there is an $x \in [a] \cap [b]$; that means $x \in [a]$ and $x \in [b]$. Hence, $x \mathrel{R} a$ and $x \mathrel{R} b$. By symmetry, $a \mathrel{R} x$. Since $x \mathrel{R} b$, by transitivity we have $a \mathrel{R} b$. Thus, we have proven the contrapositive, so the proposition is true. □

5 Proof by Contradiction

While proofs by counterexample are useful when we wish to prove statements false, a **proof by contradiction** allows us to prove the truth of a statement using the same "false assumption" idea. To write a proof by contradiction, we assume that the statement we are given (that we wish to prove is true) is false, and we show that such an assumption leads to an impossible outcome. Since our assumption that the statement was false led to nonsense, we conclude that our assumption was wrong; the statement must have been true.

Definition 10 (Proof by contradiction)**.** To prove that a statement "if x, then y" is true:

1. Assume that x is true.
2. Suppose, for the sake of contradiction, that y is false.
3. Argue until a contradiction is reached. This means that the supposition of y being false must have been incorrect. Hence, y is true and we have shown "if x, then y".

Refer also to Proof Template 12 (p. 121) in your textbook. Also refer to Proposition 20.2 and the truth table (p. 121) to see that $x \to y$ (which is what we show in a direct proof) is logically equivalent to $(x \wedge \neg y) \to \textsc{false}$ (which is what we show in a proof by contradiction).

We can think of a proof by contradiction as reducing an argument to an absurd (that is, impossible) conclusion. Along this line of thought, we get the Latin phrase for this proof technique: *reductio ad absurdum.*

Example 11. Let us prove the following claim using a proof by contradiction.

Claim. If n is an odd integer, then n^2 is an odd integer.

Proof. (***Assume the antecedent is true***) Suppose n is an odd integer.

(***Suppose the consequent is false***) Further suppose that n^2 is not an odd integer. Then n^2 must be an even integer.

(***State known facts and lay out a logical argument until you reach a contradition***)

Since n is an odd integer, we have $n = 2k + 1$ for some integer k. Squaring both sides, we get

$$n^2 = 2(2k^2 + 2k) + 1.$$

Let $j = 2k^2 + 2k$. Then $n^2 = 2j + 1$, so n^2 is an odd integer.

(***Reach a contradiction***) We found n^2 to be odd, but our starting supposition was that n^2 was not an odd integer. $\Rightarrow\Leftarrow$

(***Conclude the proof***) If n is an odd integer, n^2 must also be an odd integer, and the claim is proved. □

Like your textbook, we use the symbol $\Rightarrow\Leftarrow$ as an abbreviation for: "Thus, we have reached a contradiction. Therefore the supposition that B (the consequent) is false is incorrect. Hence, B is true."

Exercise

Note that the above example assumed the antecedent (A) to be true and supposed the consequent (B) to be false. However, it reached the contradiction that B is true, despite originally supposing B to be false. So, what we really have is a direct proof with some unnecessary extra statements. As an exercise, convert the above proof into a direct proof.

Note that similarly, if we (after assuming that A is true) start with the supposition that B is false to reach the conclusion that A is false, then what we actually have is a proof by contrapositive with some unnecessary extra statements. You would then be able to rewrite your proof as a proof by contrapositive.

In contrast, the following example illustrates a more fitting use of a proof by contradiction.

Example 12. Let us prove the following claim by using a proof by contradiction.

Claim. No integer is both even and odd.

Proof. (***Reword the claim as an if-then statement***) If x is an integer, then x is not both even and odd.

(***Assume the antecedent is true***) Let x be an integer.

(***Suppose the consequent is false***) Suppose that x is both even and odd.

(***State known facts and lay out a logical argument until you reach a contradiction***)

Since x is even, we know that there is an integer a such that $x = 2a$.

Since x is odd, we know that there is an integer b such that $x = 2b + 1$.

Therefore, we have $2a = 2b + 1$. So, $a = b - \frac{1}{2}$.

(***Reach a contradition***) a and b are both integers, but we also have $a = b - \frac{1}{2}$, which cannot be an integer since $\frac{1}{2}$ is not an integer. $\Rightarrow\Leftarrow$

(***Conclude the proof***) Therefore, x cannot be both even and odd, and the claim is proved.

□

5.1 Common Uses for Proof by Contradiction

Your textbook mentions two noteworthy scenarios where proof by contradiction is commonly used:

1. To prove that a set is empty, you may suppose that the set is nonempty and lay out a logical argument until you reach a contradiction (see Proof Template 13, p. 122).
2. To prove that there is at most one object x that satisfies a set of conditions, you may suppose that there are two different objects x and y that satisfy the conditions, and lay out a logical argument until you reach a contradiction (see Proof Template 14, p. 123).

The table below summarizes the underlying logic for each method of proving an $A \to B$ proposition (i.e., in the form of "if A is true, then B is true") discussed thus far in this module.

Proof type	Logical mechanism	Textbook ref.
Direct proof	Show that $A \to B$	Proof Template 1 (p. 17)
Proof by contrapositive	Show that $\neg B \to \neg A$	Proof Template 11 (p. 120)
Proof by contradiction	Assume A is true, but assume B is not true. Lay out a logical argument until you reach a contradiction (i.e., a false statement) that leaves no other possible conclusion than for B to be true.	Proof Template 12, 13, and 14 (p. 121, 122, and 123)

Note that proving an $A \iff B$ (i.e., in the form of "A is true if-and-only-if B is true") requires proving both (i) $A \to B$ proposition (if A is true, then B is true), and (ii) $B \to A$ proposition (if B is true, then A is true). Refer to Proof template 2 (p. 21) in your textbook.

6 Smallest Counterexample

This proof technique, sometimes also known as Proof by Minimal Counterexample, is a bit misleadingly named. It is actually a Proof By Contradiction That Involves Showing That There Cannot Exist a Minimal Counterexample, but that is far too wordy. The assumption is that there exists some counterexamples to the statement, and that they are ordered in some way such that one of the counterexamples is the smallest.

Definition 13 (Proof by smallest counterexample)**.** We have a claim that P is true. We will prove it by contradiction, by assuming P to be false.

1. Let x be a smallest counterexample to a claim P. It must be clear that there can be such an x.
2. Find the smallest instance for a for which the statement P is true. So we know that $x > a$. This is called the basis step.
3. Consider another instance x' that has a value smaller than x.
4. Use the fact that P is true for x' but not true for x to reach a contradiction.
5. Conclude that the result is true.

Refer also to Proof Template 15 (p. 128) in your textbook.

We illustrate this with the following example.

Example 14. Let us prove the following claim using a proof by smallest counterexample.

Claim. Let n be a positive integer. The sum of the first n odd natural numbers is n^2.

The first n odd natural numbers are $1, 3, 5, \ldots, 2n - 1$. The proposition claims that the summation of these numbers is n^2. Let $P(n)$ be the statement that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Proof. (***Assume the statement is false***) Let x be the smallest positive integer for which the statement is false. That is,

$$1 + 3 + 5 + \cdots + (2x - 1) \neq x^2.$$

(***Show that the statement holds for the basis step***) We know that $x > 1$ because the statement $P(1)$ is true, since $1 = 1^2$.

(***Consider** $x - 1$**.***) $P(x - 1)$ must be true, since the smallest counterexample is x. So,

$$1 + 3 + 5 + \cdots + [2(x - 1) - 1)] = (x - 1)^2.$$

(***Reach a contradiction by showing that*** $P(x)$ ***is true***) Let us add the term $(2x-1)$ to both sides of the equation, which gives

$$1+3+5+\cdots+[2(x-1)-1)]+(2x-1)=(x-1)^2+(2x-1).$$

The left-hand side of the equality is the sum of the first x odd natural numbers, and the right-hand side can be simplified as follows:

$$\begin{aligned}(x-1)^2+(2x-1)&=(x^2-2x+1)+(2x-1)\\&=x^2\end{aligned}$$

This means that the sum of the first x odd natural numbers is x^2, and therefore $P(x)$ is true. But this is a contradiction, since we defined x as the smallest counterexample to the statement P.

(***Conclude the statement is true***) We have shown that there can not exist a minimal counterexample, and therefore the statement P is true. □

Note that to prove that there is no smallest counterexample is equivalent to proving that there is no counterexample at all. Furthermore, proof by smallest counterexample can only be done for a statement over a set of numbers for which there exists a smallest element. This is not the case, for example, with the integers $\mathbb{Z}$, because any element $a \in \mathbb{Z}$ has infinitely many numbers that are less than it.

Exercise

Prove, using the same technique, that $1+2+3+\cdots+n=\frac{n(n+1)}{2}$ for every positive integer n.

6.1 Well-Ordering Principle

Proof by smallest counterexample uses what is formally known as the Well-Ordering Principle.

Definition 15 (Well-Ordering Principle)**.** Every nonempty subset of the set of natural numbers $\mathbb{N}$ contains a smallest element.

We do not prove this, because the set of natural numbers $\mathbb{N}$ is actually defined as a set of numbers that meets certain conditions, and the Well-Ordering Principle is one of them.

We can reformulate the technique of proof by smallest counterexample as a proof by the Well-Ordering Principle, as follows.

Definition 16 (Proof by well-ordering)**.** Let P be a statement over the set of natural numbers $\mathbb{N}$. To prove that P is true:

1. Suppose that P is false, then take $X \subseteq \mathbb{N}$ to be the set of counterexamples for P. By the well-ordering principle, X contains a smallest element x.
2. Find an integer a that satisfies the statement P. Now, we know that $x \neq a$ and therefore $x > a$. Usually, we pick $a = 0$ or $a = 1$, but sometimes we may need to pick another positive integer. This is called the basis step.
3. Consider $x - 1$, for which P must be true, since we know that x is the smallest natural number for which P is false.
4. Then, show that P is also true for x, which is a contradiction (since x was a counterexample).

Refer also to Proof Template 16 (p. 131) in your textbook.

We illustrate this proof technique as follows.

Example 17. Let us prove the following claim using a proof by well-ordering.

Claim. For all integers $n \geq 5$, we have $2^n > n^2$.

Proof. (***Assume the statement is false***) Let $P(n)$ be the statement $2^n > n^2$. Suppose P is false, and let $X = \{n \in \mathbb{N} \mid 2^n \not> n^2\}$. Since we have assumed P is false, we know that $X \neq \emptyset$. Moreover, by the well-ordering principle, X contains a smallest element x.

(***Show that the statement holds for the basis step***) $P(5)$ is true, since $2^5 > 5^2$. So, $x \geq 6$.

(***Consider*** $x - 1$**.**) $P(x-1)$ is true. That is, $2^{x-1} > (x-1)^2$ is true.

(***Reach a contradiction by showing that*** $P(x)$ ***is true***) By the previous step, we know that $2^{x-1} > (x-1)^2$. So, we have

$$2^{x-1} > x^2 - 2x + 1.$$

So,

$$\frac{1}{2}2^x > x^2 - 2x + 1.$$

Multiplying both sides by 2 gives

$$2^x > 2x^2 - 4x + 2.$$

So, to show that $2^x > x^2$, we will show that $2x^2 - 4x + 2 > x^2$, or equivalently $x^2 - 4x + 2 > 0$. Adding 2 to both sides gives $x^2 - 4x + 4 > 2$, and factoring the left-hand side gives $(x-2)^2 > 2$. We know that this is true since $x \geq 6$.

Therefore, we have shown that $2^x > x^2$. Thus, $P(x)$ is true, but this contradicts $x \in X$.

(***Conclude the statement is true***) We have shown that there can not exist a minimal counterexample, and therefore the statement P is true. □

Exercise

Prove, using the same technique, that for all $n \in \mathbb{N}$,

$$n < 2^n.$$

We will now give another example using the sequence of Fibonacci numbers, defined as follows.

Definition 18 (Fibonacci numbers)**.** The sequence of Fibonacci numbers F_n is the infinite sequence of integers satisfying the following conditions:

$$\begin{aligned} &F_0 = 1, \\ &F_1 = 1, \text{ and} \\ &F_n = F_{n-1} + F_{n-2}, \text{ for } n \geq 2. \end{aligned}$$

The first ten Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, 21, 34, and 55. It doesn't seem too obvious how each term F_n grows as n increases, so with the following example we show an upper bound for F_n.

Example 19. Let us prove the following claim using a proof by well-ordering.

Claim. For all $n \in \mathbb{N}$ where $n \geq 1$, $F_n \leq 1.7^{n-1}$.

Proof. (***Assume the statement is false***) Let $P(n)$ be the statement $F_n \leq 1.7^{n-1}$. Suppose P is false, and let $X = \{n \in \mathbb{N} \mid F_n \not\leq 1.7^{n-1}\}$. Since we have assumed P is false, we know that $X \neq \emptyset$. Moreover, by the well-ordering principle, X contains a smallest element x.

(***Show that the statement holds for the basis step***) Since F_n is defined in terms of F_{n-1} and F_{n-2}, we require at least two basis steps. The smallest possible values of n are 1 and 2, so we take our basis steps to be $P(1)$ and $P(2)$. When $n = 1$, we have $F_1 = 1 \leq 1.7^0$. When $n = 2$, we have $F_2 = 1 \leq 1.7^1$. Therefore, both $P(1)$ and $P(2)$ are true. So, $x \geq 3$.

(***Consider*** $x-1$ ***and*** $x-2$***.***) $P(x-1)$ and $P(x-2)$ are true. That is, both $F_{x-1} \leq 1.7^{x-2}$ and $F_{x-2} \leq 1.7^{x-3}$.

(***Reach a contradiction by showing that*** $P(x)$ ***is true***) We know that $F_x = F_{x-1} + F_{x-2}$. So, we have

$$\begin{aligned} F_x &= F_{x-1} + F_{x-2} \\ &\leq 1.7^{x-2} + 1.7^{x-3} = 1.7^{x-3}(1.7+1) = 1.7^{x-3}(2.7) \\ &< 1.7^{x-3}(1.7^2) = 1.7^{x-1}, \end{aligned}$$

so $F_x < 1.7^{x-1}$. We have shown that $P(x)$ is true, but this contradicts $x \in X$.

(***Conclude the statement is true***) We have shown that there can not exist a minimal counterexample, and therefore the statement P is true. □

Exercise

Prove, using the same technique, that for all $n \in \mathbb{N}$,

$$F_0 + F_1 + \cdots + F_n = F_{n+2} - 1.$$