Mathematical Reasoning

Presentation · April 2017

DOI: 10.13140/RG.2.2.33874.15041

1 author:

Gede Pramudya
Technical University of Malaysia Malacca

Foundation 2: MATHEMATICAL REASONING

Gede Pramudya[1]

[1]Senior Lecturer in Department of Intelligent Computing and Analytics
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka with LaTeX

February 20, 2017

Outline

Outline

Introduction

- Proofs in mathematics are *valid arguments* that establish the truth of mathematical statements.
- By an **argument**, we mean a sequence of *statements* that end with a *conclusion*.
- By **valid**, we mean the conclusion must follow from the truth of the preceding statements, or **premises**, of the argument. That is, an argument is valid if and only if it is *impossible* for all premises to be true and the conclusion to be false.
- To deduce new statements from statements we already have, we use *rules of inference* which are templates for constructing valid arguments. Rules of inference are basic tools for establishing the truth of statements.

Introduction

- Proofs in mathematics are *valid arguments* that establish the truth of mathematical statements.
- By an **argument**, we mean a sequence of *statements* that end with a *conclusion*.
- By **valid**, we mean the conclusion must follow from the truth of the preceding statements, or **premises**, of the argument. That is, an argument is valid if and only if it is *impossible* for all premises to be true and the conclusion to be false.
- To deduce new statements from statements we already have, we use *rules of inference* which are templates for constructing valid arguments. Rules of inference are basic tools for establishing the truth of statements.

Introduction

- Proofs in mathematics are *valid arguments* that establish the truth of mathematical statements.
- By an **argument**, we mean a sequence of *statements* that end with a *conclusion*.
- By **valid**, we mean the conclusion must follow from the truth of the preceding statements, or **premises**, of the argument. That is, an argument is valid if and only if it is *impossible* for all premises to be true and the conclusion to be false.
- To deduce new statements from statements we already have, we use *rules of inference* which are templates for constructing valid arguments. Rules of inference are basic tools for establishing the truth of statements.

Introduction

- Proofs in mathematics are *valid arguments* that establish the truth of mathematical statements.
- By an **argument**, we mean a sequence of *statements* that end with a *conclusion*.
- By **valid**, we mean the conclusion must follow from the truth of the preceding statements, or **premises**, of the argument. That is, an argument is valid if and only if it is *impossible* for all premises to be true and the conclusion to be false.
- To deduce new statements from statements we already have, we use *rules of inference* which are templates for constructing valid arguments. Rules of inference are basic tools for establishing the truth of statements.

Outline

Valid Arguments

Consider the following argument involving propositions:

- "If you have a current password, then you can log onto the network." "You have a current password." Therefore, "You can log onto the network."
- You would like to determine whether this is a valid argument. That is, we we would like to determine whether the conclusion "You can log onto the network" must be true when the premises "If you have a current password, then you can log onto the network" and "You have a current password" are both true.
- Before we discuss the validity of this argument, we will look at its form first. Use p to represent "You have a current password" and q to represent "You can log onto the network."

Valid Arguments

Consider the following argument involving propositions:

- "If you have a current password, then you can log onto the network." "You have a current password." Therefore, "You can log onto the network."
- You would like to determine whether this is a valid argument. That is, we we would like to determine whether the conclusion "You can log onto the network" must be true when the premises "If you have a current password, then you can log onto the network" and "You have a current password" are both true.
- Before we discuss the validity of this argument, we will look at its form first. Use p to represent "You have a current password" and q to represent "You can log onto the network."

Valid Arguments

Consider the following argument involving propositions:

- "If you have a current password, then you can log onto the network." "You have a current password." Therefore, "You can log onto the network."
- You would like to determine whether this is a valid argument. That is, we we would like to determine whether the conclusion "You can log onto the network" must be true when the premises "If you have a current password, then you can log onto the network" and "You have a current password" are both true.
- Before we discuss the validity of this argument, we will look at its form first. Use p to represent "You have a current password" and q to represent "You can log onto the network."

Valid Arguments contd.

- Then the argument has the form

$$\frac{(p \rightarrow q) \quad p}{\therefore q}$$

- where $\therefore$ is the symbol that denotes "therefore." We know that when p and q are propositional variables, the statement $((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology. In particular, when both $p \rightarrow q$ and p are true.
- We say this form of argument is valid because whenever all its premises are true, the conclusion must also be true.

Valid Arguments contd.

- Then the argument has the form

$$\frac{(p \rightarrow q) \quad p}{\therefore q}$$

- where $\therefore$ is the symbol that denotes "therefore." We know that when p and q are propositional variables, the statement $((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology. In particular, when both $p \rightarrow q$ and p are true.
- We say this form of argument is valid because whenever all its premises are true, the conclusion must also be true.

Valid Arguments contd.

- Then the argument has the form

$$\frac{(p \rightarrow q) \quad p}{\therefore q}$$

- where $\therefore$ is the symbol that denotes "therefore." We know that when p and q are propositional variables, the statement $((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology. In particular, when both $p \rightarrow q$ and p are true.
- We say this form of argument is valid because whenever all its premises are true, the conclusion must also be true.

Outline

Rules of Inference for Proposition Logic

- Since using truth table is a tedious approach, we can establish the validity of some relative simple argument forms by using rules of inference. These rule of inference can be used as building blocks to construct more complicated valid argument forms.
- The tautology $(p \wedge (p \to q)) \to q)$ is the basis of the rule of inference called **modus ponens**, or the **law of detachment**. This tautology leads to the following argument form.

$$\begin{array}{r} p \\ \underline{p \to q} \\ \therefore q \end{array}$$

Rules of Inference for Proposition Logic

- Since using truth table is a tedious approach, we can establish the validity of some relative simple argument forms by using rules of inference. These rule of inference can be used as building blocks to construct more complicated valid argument forms.
- The tautology $(p \wedge (p \to q)) \to q)$ is the basis of the rule of inference called **modus ponens**, or the **law of detachment**. This tautology leads to the following argument form.

$$\begin{array}{r} p \\ p \to q \\ \hline \therefore q \end{array}$$

Rules contd.

In particular, modus ponens tells us that if a conditional statement and the hypothesis of this conditional statement are both true, the conclusion must also be true.

Example

Consider the two following arguments.

1. If it rains today, then we will go fishing. It is raining today. Therefore, we will go fishing. (A valid argument and true conclusion).
2. If $\sqrt{2} > \frac{3}{2}$, then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Consequently, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$. (a valid argument, but false conclusion).

Some Rules of Inference

There are some other rules of inference can be mentioned here. They are (not limited to)

- **Modus Tollens**: $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$;
- **Hypothetical Syllogism**: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$;
- **Addition**: $p \rightarrow (p \vee r)$;
- **Simplification**: $(p \wedge q) \rightarrow p$;
- **Resolution**: $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$.

Examples

- Consider the following argument. *If it rains today, then we will not have jogging today. If we do not have jogging today, then we will have it tomorrow. Therefore, if it rains today, then we will have jogging tomorrow*. Which rule is used?
- Consider also this argument. *If you do every problem in this book, then you will pass discrete mathematics. You passed discrete mathematics. Therefore, you did every problem in this book*. Is it valid? This is called **fallacy of affirming the conclusion** since the compound proposition $((p \to q) \wedge q) \to p$ is contingency.
- Another example is $((p \to q) \wedge \neg p) \to \neg q$,which is called as the **fallacy of denying the hypothesis**.

Examples

- Consider the following argument. *If it rains today, then we will not have jogging today. If we do not have jogging today, then we will have it tomorrow. Therefore, if it rains today, then we will have jogging tomorrow*. Which rule is used?
- Consider also this argument. *If you do every problem in this book, then you will pass discrete mathematics. You passed discrete mathematics. Therefore, you did every problem in this book.* Is it valid? This is called **fallacy of affirming the conclusion** since the compound proposition $((p \rightarrow q) \wedge q) \rightarrow p$ is contingency.
- Another example is $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$,which is called as the **fallacy of denying the hypothesis**.

Examples

- Consider the following argument. *If it rains today, then we will not have jogging today. If we do not have jogging today, then we will have it tomorrow. Therefore, if it rains today, then we will have jogging tomorrow*. Which rule is used?
- Consider also this argument. *If you do every problem in this book, then you will pass discrete mathematics. You passed discrete mathematics. Therefore, you did every problem in this book.* Is it valid? This is called **fallacy of affirming the conclusion** since the compound proposition $((p \to q) \wedge q) \to p$ is contingency.
- Another example is $((p \to q) \wedge \neg p) \to \neg q$,which is called as the **fallacy of denying the hypothesis**.

Outline

1. Rules of Inference
   - Introduction
   - Valid Arguments
   - Rules of Inference for Proposition Logic
   - Rules of Inference for Quantified Statements
   - Combining Rules of Inference
2. Introduction to Proofs
   - Introduction
   - Proving Theorems

Rules of Inference for Quantified Statements

These are the rules:

- **Universal instantiation**: $(\forall x P(x)) \rightarrow P(c)$, for a particular member c of the domain;
- **Universal generalization**: $(P(c)$for an arbitrary $c) \rightarrow \forall x P(x)$;
- **Existential instantiation**: $(\exists x P(x)) \rightarrow P(c)$, for some element c of the domain;
- **Existential generalization**: $(P(c)$for some element c of the domain$) \rightarrow \exists x P(x)$.

Rules of Inference for Quantified Statements

These are the rules:

- **Universal instantiation**: $(\forall x P(x)) \to P(c)$, for a particular member c of the domain;
- **Universal generalization**: $(P(c)$for an arbitrary $c) \to \forall x P(x)$;
- **Existential instantiation**: $(\exists x P(x)) \to P(c)$, for some element c of the domain;
- **Existential generalization**: $(P(c)$for some element c of the domain$) \to \exists x P(x)$.

Rules of Inference for Quantified Statements

These are the rules:

- **Universal instantiation**: $(\forall x P(x)) \rightarrow P(c)$, for a particular member c of the domain;
- **Universal generalization**: $(P(c)$for an arbitrary $c) \rightarrow \forall x P(x)$;
- **Existential instantiation**: $(\exists x P(x)) \rightarrow P(c)$, for some element c of the domain;
- **Existential generalization**: $(P(c)$for some element c of the domain$) \rightarrow \exists x P(x)$.

Rules of Inference for Quantified Statements

These are the rules:

- **Universal instantiation**: $(\forall x P(x)) \rightarrow P(c)$, for a particular member c of the domain;
- **Universal generalization**: $(P(c)\text{for an arbitrary } c) \rightarrow \forall x P(x)$;
- **Existential instantiation**: $(\exists x P(x)) \rightarrow P(c)$, for some element c of the domain;
- **Existential generalization**: $(P(c)\text{for some element c of the domain}) \rightarrow \exists x P(x)$.

Example

Let we have an example.

- **Problem**: Show that the argument "Everyone in this discrete mathematics class has taken a course in computer science. Marla is a student in this class. Therefore, Marla has taken a course in computer science." is valid.
- **Solution**: Let *D(x)* denotes "*x* is in this discrete mathematics class", and *C(x)* denote "*x* has taken a course in computer science." Then the premises are $\forall x D(x) \rightarrow C(x)$ and $D(Marla)$. The conclusion is $C(Marla)$. The following steps can be used to establish the conclusion from the premises.
  1. $\forall x(D(x) \rightarrow C(x))$: Premise;
  2. $D(Marla) \rightarrow C(Marla)$: Universal instantiation from (1);
  3. $D(Marla)$: Premise;
  4. $C(Marla)$: Modus ponens from (2) and (3).

Example

Let we have an example.

- **Problem**: Show that the argument "Everyone in this discrete mathematics class has taken a course in computer science. Marla is a student in this class. Therefore, Marla has taken a course in computer science." is valid.
- **Solution**: Let *D(x)* denotes "*x* is in this discrete mathematics class", and *C(x)* denote "*x* has taken a course in computer science." Then the premises are $\forall x D(x) \rightarrow C(x)$ and $D(Marla)$. The conclusion is $C(Marla)$. The following steps can be used to establish the conclusion from the premises.
  1. $\forall x(D(x) \rightarrow C(x)$: Premise;
  2. $D(Marla) \rightarrow C(Marla)$: Universal instantiation from (1);
  3. $D(Marla)$: Premise;
  4. $C(Marla)$: Modus ponens from (2) and (3).

Outline

Combining Rules of Inference for Propositions and Quantified Statements

We have developed rules of inference both for propositions and quantified statements. Note in the previous example we used both universal instantiation, a rule of inference for quantified statements, and modus ponens, a rule of inference for propositional logic. We will often need to use this combination of rules of inference.

Combining contd.

Because universal instantiation and modus ponens are used so often together, this combination of rules is sometimes called universal modus ponens. The form is

$$\frac{\begin{array}{r}\forall[P(x) \rightarrow Q(x)] \\ P(a), \text{where } a \text{ as a particular element in the domain}\end{array}}{\therefore Q(a)}$$

Example

- **Problem**: Show that the premises "A student in this class has not read the note," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has nor read the note."
- **Solution**: Let $C(x)$ be "x is in the class," $B(x)$ be "x has read the note," and $P(x)$ be "x passed the first exam." The premises are $\exists x[C(x) \wedge \neg B(x)]$ and $\forall x[C(x) \rightarrow P(x)]$. The conclusion is $\exists x[P(x) \wedge \neg B(x)]$.

Example

- **Problem**: Show that the premises "A student in this class has not read the note," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has nor read the note."
- **Solution**: Let $C(x)$ be "x is in the class," $B(x)$ be "x has read the note," and $P(x)$ be "x passed the first exam." The premises are $\exists x[C(x) \wedge \neg B(x)]$ and $\forall x[C(x) \rightarrow P(x)]$. The conclusion is $\exists x[P(x) \wedge \neg B(x)]$.

Example contd.

The following steps can be used to establish the conclusion from the premise.

1. $\exists x[C(x) \land \neg B(x)]$: Premise
2. $C(a) \land \neg B(a)$: Existential instantiation from (1)
3. $C(a)$: Simplification from (2)
4. $\forall x[C(x) \to P(x)]$: Premise
5. $C(a) \to P(a)$: Universal instantiation from (4)
6. $P(a)$: Modus ponens from (3) and (5)
7. $\neg B(a)$: Simplification from (2)
8. $P(a) \land \neg B(a)$: Conjunction from (6) and (7)
9. $\exists x[P(x) \land B(x)]$: Existential generalization from (8)

Example

- **Problem**: Assume that "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" is true. Use universal modus ponens to show that $100^2 < 2^{100}$.
- **Solution**: Let $P(n)$ denote "$n > 4$" and $Q(n)$ denote "$n^2 < 2^n$." The statement "For all positive integers n, if n greater than 4, then n^2 is less than 2^n" can be represented by $\forall n[P(n) \to Q(n)]$, where the domain contains all positive integers. We are assuming that $\forall n[P(n) \to Q(n)]$ is true. Note $P(100)$ is true because $100 > 4$. It follows by universal modus ponens that $Q(n)$ is true, namely that $100^2 < 2^{100}$.

Example

- **Problem**: Assume that "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" is true. Use universal modus ponens to show that $100^2 < 2^{100}$.
- **Solution**: Let $P(n)$ denote "$n > 4$" and $Q(n)$ denote "$n^2 < 2^n$." The statement "For all positive integers n, if n greater than 4, then n^2 is less than 2^n" can be represented by $\forall n[P(n) \rightarrow Q(n)]$, where the domain contains all positive integers. We are assuming that $\forall n[P(n) \rightarrow Q(n)]$ is true. Note $P(100)$ is true because $100 > 4$. It follows by universal modus ponens that $Q(n)$ is true, namely that $100^2 < 2^{100}$.

Outline

Introduction

- In this part we will discuss the notion of proof and describe methods of constructing *proofs*.
- A proof is a valid argument that establishes the truth of a mathematical statement. A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems. Using these ingredients and the *rules of inference*, the final step of the proof establishes the truth of the statement being proved.
- In this discussion we move from formal proofs of theorems toward more informal proofs since formal proofs can extremely long and hard to follow.

Introduction

- In this part we will discuss the notion of proof and describe methods of constructing *proofs*.
- A proof is a valid argument that establishes the truth of a mathematical statement. A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems. Using these ingredients and the *rules of inference*, the final step of the proof establishes the truth of the statement being proved.
- In this discussion we move from formal proofs of theorems toward more informal proofs since formal proofs can extremely long and hard to follow.

Introduction

- In this part we will discuss the notion of proof and describe methods of constructing *proofs*.
- A proof is a valid argument that establishes the truth of a mathematical statement. A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems. Using these ingredients and the *rules of inference*, the final step of the proof establishes the truth of the statement being proved.
- In this discussion we move from formal proofs of theorems toward more informal proofs since formal proofs can extremely long and hard to follow.

Introduction contd.

- In practice, proofs of theorems designed for human consumption are almost always informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated.
- The methods of proof discussed are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science.

Introduction contd.

- In practice, proofs of theorems designed for human consumption are almost always informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated.
- The methods of proof discussed are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science.

Outline

Proving Theorems

Formally, a **theorem** is a statement that can be shown to be true. Less important theorems sometimes are called **propositions**. A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion. However, it may be some other types of logical statement. We demonstrate that a theorem is true with a **proof**. A proof is a valid argument that establishes the truth of a theorem. The statements used in a proof can include **axioms** (or **postulates**), which are statements we assume to be true, the premises, if any, of the theorem, and previously proven theorems.

Proving contd.

A less important theorem that is helpful in the proof of other results is called **lemma**. A **corollary** is a theorem that can be established directly from a theorem that has been proved. A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or intuition of an expert. When a proof of conjecture is found, the conjecture becomes a theorem.

With Quantifiers

Many theorems assert that a property holds for all elements in a domain, as as the integers or the real numbers. Although the precise statement of such theorems needs to include a universal quantifier, the standard convention in mathematics is to omit it. For example, the statement "If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$" really means "For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$." Furthermore, when theorems of this type are proved, the law of universal instantiation is often used without explicit mention. The first step of the proof usually involves selecting a general element of the domain. Subsequent steps show that this element has the property in the question. Finally, universal generalization implies that the theorem holds for all members of the domain. These are some of the methods.

Direct Proofs

A direct proof of conditional statement $p \to q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inferences, with the final step showing that q must also be true. A direct proof shows that a conditional statement $p \to q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs. In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Example

- **Problem**: Give a direct proof of the theorem "If n is odd, then n^2 is also odd."
- **Solution**: Note this theorem states $\forall n P(n) \to Q(n)$, where $P(n)$ is "n is odd", and $Q(n)$ is "n^2 is odd." We will follow the usual convention in mathematical proof by showing that $P(n)$ implies $Q(n)$. To begin with, we assume that the hypothesis of this conditional is true, namely, we assume that n is odd. By the definition of odd integer, it follows that $n = 2k + 1$ for an integer k. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2. When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, by the definition of an odd integer, we can conclude that n^2 is odd. Consequently, we have prove that if n is odd, then n^2 is odd too.

Example

- **Problem**: Give a direct proof of the theorem "If n is odd, then n^2 is also odd."
- **Solution**: Note this theorem states $\forall n P(n) \rightarrow Q(n)$, where $P(n)$ is "n is odd", and $Q(n)$ is "n^2 is odd." We will follow the usual convention in mathematical proof by showing that $P(n)$ implies $Q(n)$. To begin with, we assume that the hypothesis of this conditional is true, namely, we assume that n is odd. By the definition of odd integer, it follows that $n = 2k + 1$ for an integer k. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2. When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, by the definition of an odd integer, we can conclude that n^2 is odd. Consequently, we have prove that if n is odd, then n^2 is odd too.

Proof by Contraposition

Sometimes, attempts at direct proof often reach dead ends. We need other methods of proving theorems in the form of $\forall x(P(x) \to Q(x))$. An extremely useful type of indirect proof is known as proof by contraposition. Proofs by contraposition make use of the fact that the conditional statement $p \to q$ is logically equivalent to its contrapositive $\neg q \to \neg p$

Example

- **Problem**: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
- **Solution**: The first step of proof is to assume that the conclusion is false, namely, assume that n is even. Then by the definition of even integer, $n = 2k$ for some integer k. Substituting $2k$ for n we find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. This tells us that $3n + 2$ is even This is the negation of the premise of the theorem. Since the negation of the conclusion of the conditional statement implies that the hypothesis is false, then the conditional statement is true. We have proved the theorem.

Example

- **Problem**: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
- **Solution**: The first step of proof is to assume that the conclusion is false, namely, assume that n is even. Then by the definition of even integer, $n = 2k$ for some integer k. Substituting $2k$ for n we find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. This tells us that $3n + 2$ is even This is the negation of the premise of the theorem. Since the negation of the conclusion of the conditional statement implies that the hypothesis is false, then the conditional statement is true. We have proved the theorem.

Proofs by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

Example

- **Problem**: Prove that $\sqrt{2}$ is irrational.
- **Solution**: Let p be the proposition "$\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that $\neg p$, which says that $\sqrt{2}$ is rational. If $\sqrt{2}$ is rational, then there exists integer a and $b \neq 0$ such that $\sqrt{2} = a/b$ and a and b have no common factors (so that the fraction a/b is in the lowest term). Because $\sqrt{2} = a/b$, then $2 = \frac{a^2}{b^2}$. Hence, $2b^2 = a^2$. It follows that a^2 is even. We use the fact that if a^2 is even, then a must also be even. Furthermore, since a is even, there exists integer c such that $a = 2c$. Thus $2b^2 = 4c^2$. Dividing both sides of this equation by 2 gives $b^2 = 2c^2$. By the definition of even, this means b^2 is even. We conclude that b must be even as well.

Example

- **Problem**: Prove that $\sqrt{2}$ is irrational.
- **Solution**: Let p be the proposition " $\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that $\neg p$, which says that $\sqrt{2}$ is rational. If $\sqrt{2}$ is rational, then there exists integer a and $b \neq 0$ such that $\sqrt{2} = a/b$ and a and b have no common factors (so that the fraction a/b is in the lowest term). Because $\sqrt{2} = a/b$, then $2 = \frac{a^2}{b^2}$. Hence, $2b^2 = a^2$. It follows that a^2 is even. We use the fact that if a^2 is even, then a must also be even. Furthermore, since a is even, there exists integer c such that $a = 2c$. Thus $2b^2 = 4c^2$. Dividing both sides of this equation by 2 gives $b^2 = 2c^2$. By the definition of even, this means b^2 is even. We conclude that b must be even as well.

Example contd.

We have now shown that the assumption of $\neg p$ leads to the equation $\sqrt{2} = a/b$, where a and b have no common factor, but both a and b are even. Because our assumption of $\neg p$ lead to the contradiction that 2 divides both a and b and 2 does not divide both a and b, $\neg p$ must be false. That is, p is true. We have proved that $\sqrt{2}$ is irrational.