Mathematical Proofs
A Transition to Advanced Mathematics

Chapter 5
Existence and Proof by Contradiction

Gary Chartrand Albert D. Polimeni Ping Zhang

Counterexamples

We have now seen two proof techniques that can be used to verify statements of the type:

$$\forall x \in S, R(x)\text{: For every } x \in S,\ R(x).\ \text{If } x \in S, \text{ then } R(x).$$

Of course, sometimes a statement of the type $\forall x \in S, R(x)$ is false. Then its negation is true:

$$\sim (\forall x \in S, R(x)) \equiv \exists x \in S,\ \sim R(x).$$

Definition

So, there exists some element x in the set S for which $R(x)$ is false. Such an element x is called a **counterexample** of the false statement $\forall x \in S, R(x)$.

Finding a counterexample verifies that $\forall x \in S, R(x)$ is false.

Counterexamples

Example 1

Consider the statement:

$$\text{If } x \in \mathbf{R}, \text{ then } (x^2 - 1)^2 > 0. \tag{1}$$

or, equivalently,

$$\text{For every real number } x, (x^2 - 1)^2 > 0.$$

Show that the statement (1) is false by exhibiting a counterexample.

Solution. For $x = 1$,

$$(x^2 - 1)^2 = (1^2 - 1)^2 = 0.$$

Thus, $x = 1$ is a counterexample. ♦

Counterexamples

Definition

If a statement P is shown to be false in some manner, then P is said to be **disproved**.

The counterexample $x = 1$ therefore disproves the statement

$$\text{If } x \in \mathbf{R}, \text{ then } (x^2 - 1)^2 > 0.$$

Example 2

Disprove the statement:

$$\text{If } x \in \mathbf{Z}, \text{ then } \frac{x^2+x}{x^2-x} = \frac{x+1}{x-1}. \tag{2}$$

Solution. If $x = 0$, then $x^2 - x = 0$ and so $\dfrac{x^2+x}{x^2-x}$ is not defined. On the other hand, if $x = 0$, then $\dfrac{x+1}{x-1} = -1$; so the expressions $\dfrac{x^2+x}{x^2-x}$ and $\dfrac{x+1}{x-1}$ are certainly not equal when $x = 0$. Thus, $x = 0$ is a counterexample to the statement (2). ♦

Example 3

Show that the statement:

$$\text{Let } n \in \mathbf{Z}. \text{ If } 4 \mid (n^2 - 1), \text{ then } 4 \mid (n - 1).$$

is false.

Solution. Since $4 \mid (3^2 - 1)$ but $4 \nmid (3 - 1)$, it follows that $n = 3$ is a counterexample. ♦

Example 4

Show that the statement

$$\text{For positive integers } a, b, c,\ a^{bc} = \left(a^b\right)^c.$$

is false.

Solution. Let $a = 2$, $b = 2$ and $c = 3$. Then

$$a^{bc} = 2^{2^3} = 2^8 = 256,$$

while

$$\left(a^b\right)^c = \left(2^2\right)^3 = 4^3 = 64.$$

Since $256 \neq 64$, the positive integers $a = 2$, $b = 2$ and $c = 3$ constitute a counterexample. ♦

Proof by Contradiction

As we mentioned, we have now seen two proof techniques that can be used to verify statements of the type:

$$\forall x \in S, R(x).$$

These two proof techniques are (1) direct proof and (2) proof by contrapositive. We now introduce a third proof technique.

Suppose that we are interested in showing a certain mathematical statement is true. Often the statements R we encountered are expressed as

$$R\text{: } \forall\ x \in S,\ P(x) \Rightarrow Q(x)\text{: Let } x \in S.\ \text{If } P(x), \text{ then } Q(x).$$

Suppose, by assuming that R is a false statement, we are able to arrive at a statement that contradicts something we know to be true (which might be some assumption, an axiom or a theorem).

Proof by Contradiction

Let's denote this assumption or known fact by P. That is, what we have deduced is $\sim P$ and have thus produced the contradiction

$$C : P \wedge (\sim P).$$

Both P and $\sim P$ are true, which is impossible. So, what we have proved is the implication

$$(\sim R) \Rightarrow C.$$

Therefore, $(\sim R) \Rightarrow C$ is true and C is false. The only way this can occur is for $\sim R$ to be false and so R is true.

Definition

Showing R is true by this technique is called **proof by contradiction**.

Proof by Contradiction

If R is the quantified statement $\forall\ x \in S,\ P(x) \Rightarrow Q(x)$, then a proof by contradiction of this statement consists of verifying the implication

$$\sim (\forall\ x \in S,\ P(x) \Rightarrow Q(x)) \ \Rightarrow\ C$$

for some contradiction C. However, since

$$\begin{aligned} \sim (\forall\ x \in S,\ P(x) \Rightarrow Q(x)) &\equiv \exists x \in S,\ \sim (P(x) \Rightarrow Q(x)) \\ &\equiv \exists x \in S,\ (P(x) \wedge (\sim Q(x))), \end{aligned}$$

it follows that a proof by contradiction of $\forall\ x \in S,\ P(x) \Rightarrow Q(x)$ would begin by assuming the existence of some element $x \in S$ such that $P(x)$ is true and $Q(x)$ is false.

Proof by Contradiction

Often the reader is alerted that a proof by contradiction is being used by saying (or writing)

Suppose that R is false.

or

Assume, to the contrary, that R is false.

Therefore, if R is the quantified statement $\forall\, x \in S,\ P(x) \Rightarrow Q(x)$, then a proof by contradiction might begin with:

> *Assume, to the contrary, that there exists some element $x \in S$ for which $P(x)$ is true and $Q(x)$ is false.*

(or something along these lines). The remainder of the proof then consists of showing that this assumption leads to a contradiction.

Proof by Contradiction

Example 5

Result There is no smallest positive real number.

Proof. Assume, to the contrary, that there is a smallest positive real number, say r. Since $0 < r/2 < r$, it follows that $r/2$ is a positive real number that is smaller than r. This, however, is a contradiction. □

Example 6

Result No odd integer can be expressed as the sum of three even integers.

Proof. Assume, to the contrary, that there exists an odd integer n which can be expressed as the sum of three even integers x, y and z. Then

$$x = 2a,\ y = 2b \text{ and } z = 2c$$

with $a, b, c \in \mathbf{Z}$. Therefore,

$$n = x + y + z = 2a + 2b + 2c = 2(a + b + c).$$

Since $a+b+c$ is an integer, n is even. This is a contradiction. □

Example 7

Result If a is an even integer and b is an odd integer, then

$$4 \nmid (a^2 + 2b^2).$$

Proof. Assume, to the contrary, that there exist an even integer a and an odd integer b such that $4 \mid (a^2 + 2b^2)$. Thus,

$$a = 2x,\ b = 2y + 1 \text{ and } a^2 + 2b^2 = 4z$$

for some integers x, y and z. Hence,

$$a^2 + 2b^2 = (2x)^2 + 2(2y + 1)^2 = 4z.$$

Example 7 (continued)

Simplifying, we obtain $4x^2 + 8y^2 + 8y + 2 = 4z$ or, equivalently,

$$2 = 4z - 4x^2 - 8y^2 - 8y = 4(z - x^2 - 2y^2 - 2y).$$

Since $z - x^2 - 2y^2 - 2y$ is an integer, $4 \mid 2$, which is impossible. □

Proof by Contradiction

One of the most famous results in mathematics using a proof by contradiction is showing that the number $\sqrt{2}$ is irrational.

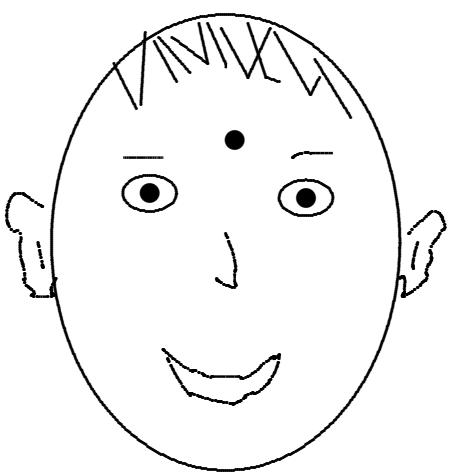
Theorem

The real number $\sqrt{2}$ is irrational.

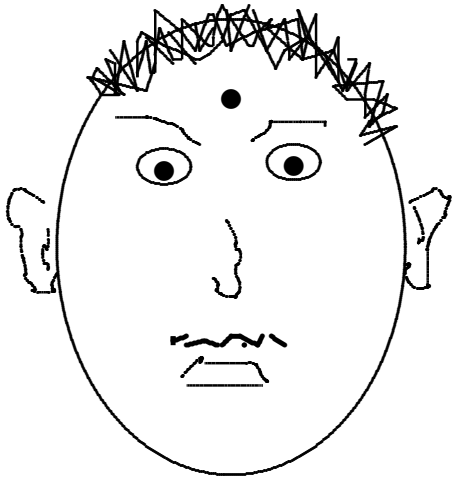
Proof. Assume, to the contrary, that $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$, where $a, b \in \mathbf{Z}$ and $b \neq 0$. We may further assume that a/b has been expressed in (or reduced to) lowest terms. Then $2 = a^2/b^2$; so $a^2 = 2b^2$. Since b^2 is an integer, a^2 is even. Then a is even. So, $a = 2c$, where $c \in \mathbf{Z}$. Thus, $(2c)^2 = 2b^2$ and so $4c^2 = 2b^2$. Therefore, $b^2 = 2c^2$. Because c^2 is an integer, b^2 is even, which implies that b is even. Since a and b are even, each has 2 as a divisor, which is a contradiction since a/b has been reduced to lowest terms. □

The Three Prisoners Problems

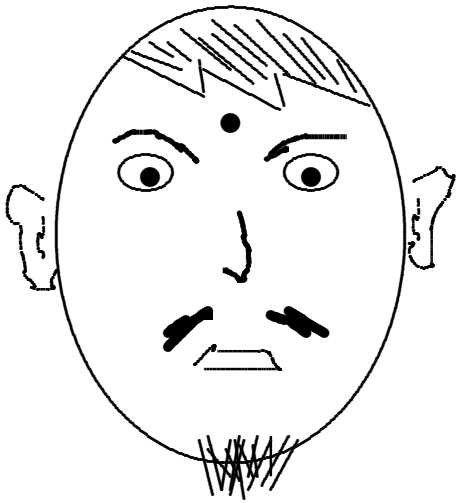
Three prisoners in the figure have been sentenced to long terms in prison, but due to overcrowded conditions, one prisoner must be released. The warden devises a scheme to determine which prisoner is to be released. He tells the prisoners that he will blindfold them and then paint a red dot or a blue dot on each forehead.



#1



#2



#3

The Three Prisoners Problems

After he paints the dots, he will remove the blindfolds and a prisoner should raise his hand if he sees a red dot on at least one of the other two prisoners. The first prisoner to identify the color of the dot on his own forehead will be released. Of course, the prisoners agree to this. (What do they have to lose?)

The warden blindfolds the prisoners, as promised, and then paints a dot on the foreheads of *all three prisoners*. In fact, he paints a red dot on the foreheads of all three prisoners. He removes the blindfolds and, since each prisoner sees a red dot (indeed two red dots), each prisoner raises his hand. Some time passes when one of the prisoners exclaims, "I know what color my dot is! It's red!" This prisoner is then released. Although the story of the three prisoners is over, there is a lingering question: How did this prisoner correctly identify the color of the dot painted on his forehead?

Existence Proofs

Definitions

An **existence theorem** asserts the existence of an object (or objects) possessing some specified property or properties. Typically, an existence theorem is expressed as a quantified statement

$$\exists x \in S, R(x): \text{ There exists } x \in S \text{ such that } R(x).$$

Such a statement is true if $R(x)$ is true for some $x \in S$. A proof of an existence theorem is called an **existence proof**.

Example 8

Result There exists an integer whose cube equals its square.

Proof. Since $1^3 = 1^2 = 1$, the integer 1 has the desired property. □

Example 9

Result There exist real numbers a and b such that

$$(a+b)^2 = a^2 + b^2.$$

Proof. Let $a, b \in \mathbf{Z}$ such that $(a+b)^2 = a^2 + b^2$. Then

$$a^2 + 2ab + b^2 = a^2 + b^2,$$

so $2ab = 0$. Since $a = 1$, $b = 0$ is a solution to this equation, we have

$$(a+b)^2 = (1+0)^2 = 1^2 = 1^2 + 0^2 = a^2 + b^2.$$

Example 10

Result There exist irrational numbers a and b such that a^b is rational.

Proof. Consider the number $\sqrt{2}^{\sqrt{2}}$. Of course, this number is either rational or irrational. We consider these possibilities separately.

Case 1. $\sqrt{2}^{\sqrt{2}}$ *is rational.* Then we can take

$$a = b = \sqrt{2}$$

and we have the desired result.

Example 10 (continued)

Case 2. $\sqrt{2}^{\sqrt{2}}$ *is irrational.* In this case, consider the number obtained by raising the (irrational) number $\sqrt{2}^{\sqrt{2}}$ to the (irrational) power $\sqrt{2}$; that is, consider a^b, where

$$a = \sqrt{2}^{\sqrt{2}} \text{ and } b = \sqrt{2}.$$

Observe that

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

which is rational. □

Existence Proofs

While an existence theorem can be proved by giving a single example of a desired type, it may be the case that we can't find such an example.

Nevertheless, the existence theorem can still be verified without exhibiting a single example of a desired type.

For example, there are theorems in mathematics that tell us that every polynomial of odd degree with real coefficients has at least one real number as a solution but we don't necessarily know how to find a solution.

Existence Proofs

The following is a well-known theorem from calculus.

The Intermediate Value Theorem of Calculus:

If f is a function that is continuous on the closed interval $[a, b]$ and k is a number between $f(a)$ and $f(b)$, then there exists a number $c \in (a, b)$ such that $f(c) = k$.

We now give an example to show how this theorem can be used.

Example 11

Result The equation $x^5 + 2x - 5 = 0$ has a real number solution between $x = 1$ and $x = 2$.

Proof. Let $f(x) = x^5 + 2x - 5$. Since f is a polynomial function, it is continuous on the set of all real numbers and so f is continuous on the interval $[1, 2]$. Now,

$$f(1) = -2 \text{ and } f(2) = 31.$$

Since 0 is between $f(1)$ and $f(2)$, it follows by the Intermediate Value Theorem of Calculus that there is a number c between 1 and 2 such that

$$f(c) = c^5 + 2c - 5 = 0.$$

Hence, c is a solution. □

Example 12

Result The equation $x^5 + 2x - 5 = 0$ has a unique real number solution between $x = 1$ and $x = 2$.

Proof. Assume, to the contrary, that the equation $x^5 + 2x - 5 = 0$ has two distinct real number solutions a and b between $x = 1$ and $x = 2$. We may assume that $a < b$. Since $1 < a < b < 2$, it follows that

$$a^5 + 2a - 5 < b^5 + 2b - 5.$$

On the other hand,

$$a^5 + 2a - 5 = 0 \text{ and } b^5 + 2b - 5 = 0.$$

Thus,

$$0 = a^5 + 2a - 5 < b^5 + 2b - 5 = 0,$$

which produces a contradiction. □

Disproving Existence Statements

We have already seen that to disprove a quantified statement of the type $\forall\ x \in S, R(x)$, it suffices to produce a counterexample (that is, an element x in S for which $R(x)$ is false).

However, disproving a quantified statement of the type $\exists x \in S, R(x)$ requires a totally different approach. Since

$$\sim (\exists x \in S, R(x)) \equiv \forall x \in S,\ \sim R(x),$$

it follows that the statement $\exists x \in S, R(x)$ is false if $R(x)$ is false for *every* $x \in S$.

Example 13

Disprove the statement: There exists an odd integer n such that $n^2 + 2n + 3$ is odd.

Solution. We show that if n is an odd integer, then $n^2 + 2n + 3$ is even. Let n be an odd integer. Then $n = 2k + 1$ for some integer k. Thus,

$$\begin{aligned} n^2 + 2n + 3 &= (2k+1)^2 + 2(2k+1) + 3 \\ &= 4k^2 + 4k + 1 + 4k + 2 + 3 \\ &= 4k^2 + 8k + 6 = 2(2k^2 + 4k + 3). \end{aligned}$$

Since $2k^2 + 4k + 3$ is an integer, $n^2 + 2n + 3$ is even. ⧫

Example 14

Disprove the statement: There is a real number x such that

$$x^6 + 2x^4 + x^2 + 2 = 0.$$

Solution. Let $x \in \mathbf{R}$. Since x^6, x^4 and x^2 are all even powers of the real number x, it follows that $x^6 \geq 0$, $x^4 \geq 0$ and $x^2 \geq 0$. Therefore,

$$x^6 + 2x^4 + x^2 + 2 \geq 0 + 0 + 0 + 2 = 2$$

and so

$$x^6 + 2x^4 + x^2 + 2 \neq 0.$$

Hence, the equation $x^6 + 2x^4 + x^2 + 2 = 0$ has no real number solution. ♦

Disproving Existence Statements

Example 15

Disprove the statement: There exists an integer n such that $n^3 - n + 1$ is even.

Solution. Let $n \in \mathbf{Z}$. We consider two cases.

Case 1. *n is even.* Then $n = 2a$, where $a \in \mathbf{Z}$. So

$$\begin{aligned} n^3 - n + 1 &= (2a)^3 - (2a) + 1 = 8a^3 - 2a + 1 \\ &= 2(4a^3 - a) + 1. \end{aligned}$$

Since $4a^3 - a$ is an integer, $n^3 - n + 1$ is odd and so it is not even.

Example 15 (continued)

Case 2. n is odd. Then $n = 2b + 1$, where $b \in \mathbf{Z}$. Hence,

$$\begin{aligned} n^3 - n + 1 &= (2b+1)^3 - (2b+1) + 1 \\ &= 8b^3 + 12b^2 + 6b + 1 - 2b - 1 + 1 \\ &= 8b^3 + 12b^2 + 4b + 1 = 2(4b^3 + 6b^2 + 2b) + 1. \end{aligned}$$

Since $4b^3 + 6b^2 + 2b$ is an integer, $n^3 - n + 1$ is odd and so it is not even. ⧫