Mistakes in Proofs

Topics

- Review of the Proof Techniques
- Fallacies
- Conjectures

Mistakes in Proofs: examples

What is wrong with this famous supposed “proof” that 1 = 2?

Proof: We use these steps, where a and b are two equal positive integers.

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Mistakes in Proofs: incorrect conclusion

- A common error of reasoning is to draw incorrect conclusions from examples.
- No matter how many separate examples are considered, a theorem is not proved by considering examples unless every possible case is covered.
- The problem of proving a theorem is analogous to showing that a computer program always produces the output desired.
- No matter how many input values are tested, unless all input values are tested, we cannot conclude that the program always produces the correct output.

Mistakes in Proofs: incorrect conclusion examples

Is it true that every positive integer is the sum of 18 fourth powers of integers?

Solution: To determine whether a positive integer n can be written as the sum of 18 fourth powers of integers, we might begin by examining whether n is the sum of 18 fourth powers of integers for the smallest positive integers. Because the fourth powers of integers are 0, 1, 16, 81, … , if we can select 18 terms from these numbers that add up to n, then n is the sum of 18 fourth powers.

We can show that all positive integers up to 78 can be written as the sum of 18 fourth powers. (The details are left to the reader.) However, if we decided this was enough checking, we would come to the wrong conclusion. It is not true that every positive integer is the sum of 18 fourth powers because 79 is not the sum of 18 fourth powers (as the reader can verify).

Existence Proofs

- Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition of the form $\exists x P(x)$, where P is a predicate.
- A proof of a proposition of the form $\exists x P(x)$ is called an **existence proof**. There are several ways to prove a theorem of this type.
- Sometimes an existence proof of $\exists x P(x)$ can be given by finding an element a, called a witness, such that $P(a)$ is true. This type of existence proof is called constructive.
- It is also possible to give an existence proof that is non-constructive; that is, we do not find an element a such that $P(a)$ is true, but rather prove that $\exists x P(x)$ is true in some other way.
- One common method of giving a non-constructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

Constructive and non-constructive Proofs: examples

Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Solution: After considerable computation (such as a computer search) we can find that $1729 = 10^3 + 9^3 = 12^3 + 1^3$.

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

Constructive and non-constructive Proofs: examples

Show that there exist irrational numbers x and y such that x^y is rational.

Solution: We know that $\sqrt{2}$ is irrational. Consider the number $(\sqrt{2})^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely, $x = \sqrt{2}$ and $y = \sqrt{2}$. On the other hand if $(\sqrt{2})^{\sqrt{2}}$ is irrational, then we can let $x = (\sqrt{2})^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{(\sqrt{2}\cdot\sqrt{2})} = (\sqrt{2})^2 = 2$.

This proof is an example of a non-constructive existence proof because we have not found irrational numbers x and y such that x^y is rational. Rather, we have shown that either the pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = (\sqrt{2})^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, but we do not know which of these two pairs works!

Open problems

- **FERMAT'S LAST THEOREM**: The equation $x^n + y^n = z^n$ has no solutions in integers x, y, and z with $xyz \neq 0$ whenever n is an integer with $n > 2$.
- **The 3x + 1 Conjecture**: Let T be the transformation that sends an even integer x to $x/2$ and an odd integer x to $3x + 1$. A famous conjecture, sometimes known as the $3x + 1$ conjecture, states that for all positive integers x, when we repeatedly apply the transformation T, we will eventually reach the integer 1. For example, starting with x = 13, we find $T(13) = 3 \cdot 13 + 1 = 40$, $T(40) = 40/2 = 20$, $T(20) = 20/2 = 10$, $T(10) = 10/2 = 5$, $T(5) = 3 \cdot 5 + 1 = 16$, $T(16) = 8$, $T(8) = 4$, $T(4) = 2$, and $T(2) = 1$. The 3x + 1 conjecture has been verified using computers for all integers x up to $5.48 \cdot 10^{18}$.
- **Twin Prime Conjecture**: There are infinitely many pairs of twin primes.

Rules of Inference

- By an argument, we mean a sequence of statements that end with a conclusion.
- By valid, we mean that the conclusion, or final statement of the argument, 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 the 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 our basic tools for establishing the truth of statements of Inference.
- After we illustrate how rules of inference are used to produce valid arguments, we will describe some common forms of incorrect reasoning, called fallacies, which lead to invalid arguments.

Rules of Inference

- An **argument** in propositional logic is a sequence of propositions.
- All but the final proposition in the argument are called **premises** and the final proposition is called the **conclusion**.
- An argument is **valid** if the truth of all its premises implies that the conclusion is true.
- An **argument form** in propositional logic is a sequence of compound propositions involving propositional variables.
- An argument form is **valid** if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Rules of Inference

Determine whether the argument given here is valid and determine whether its conclusion must be true because of the validity of the argument.

> "If $\sqrt{2} > 3/2$, then $(\sqrt{2})^2 > (3/2)^2$.
> We know that $\sqrt{2} > 3/2$. Consequently, $(\sqrt{2})^2 = 2 > (3/2)^2 = 9/4$."

Solution: Let p be the proposition "$\sqrt{2} > 3/2$" and q the proposition "$2 > (3/2)^2$." The premises of the argument are $p \rightarrow q$ and p, and q is its conclusion. This argument is valid because it is constructed by using *modus ponens*, a valid argument form. However, one of its premises, $2 > 3/2$, is false. Consequently, we cannot conclude that the conclusion is true. Furthermore, note that the conclusion of this argument is false, because $2 < 9/4$.

Rules of Inference: Modus Ponens

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

where $\therefore$ is the symbol that denotes “therefore.”

Rules of Inference: Modus Tollens

$\neg q$

$p \to q$

$\therefore \neg p$ where $\therefore$ is the symbol that denotes "therefore."

Rules of Inference: Addition

$$\frac{p}{\therefore p \vee q}$$

where ∴ is the symbol that denotes "therefore."

Rules of Inference: Simplification

$$\frac{p \land q}{\therefore p}$$

where $\therefore$ is the symbol that denotes “therefore.”

Fallacies: fallacy of affirming the conclusion

Is the following argument valid?

> If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics.
> Therefore, you did every problem in this book.

Solution: Let p be the proposition "You did every problem in this book." Let q be the proposition "You learned discrete mathematics."
Then this argument is of the form: if $(p \rightarrow q)$ and q, then p.
This is an example of an incorrect argument using the fallacy of affirming the conclusion. Indeed, it is possible for you to learn discrete mathematics in some way other than by doing every problem in this book. (You may learn discrete mathematics by reading, listening to lectures, doing some, but not all, the problems in this book, and so on.)