Proof Techniques

CSCI 1951k/2951z

Topics

1. Direct Proof
2. Proof by Induction
3. Proof by Contradiction

Direct Proof

Usage: Given a set of *rules* (axioms), can you prove a particular statement?

Direct Proof

Usage: Given a set of *rules* (axioms), can you prove a particular statement?

Idea: At a high level, direct proofs consist of repeated ‘massaging’ of an expression followed by the application of one of these rules.

Direct Proof

Usage: Given a set of *rules* (axioms), can you prove a particular statement?

Idea: At a high level, direct proofs consist of repeated ‘massaging’ of an expression followed by the application of one of these rules.

Expr 1 $\xrightarrow{\text{Algebra}}$ Expr 2 $\xrightarrow{\text{Rule 1}}$ Expr 3 $\xrightarrow{\text{Algebra}}$ Expr 4 $\xrightarrow{\text{Rule 2}}$ Desired

Direct Proof

Example: *Rule 1*: Let k be an integer. Then, $n = 2k + 1$ is odd.

Direct Proof

Example: *Rule 1*: Let k be an integer. Then, $n = 2k + 1$ is odd.

Rule 2: If a and b are of opposite parity, then $a + b$ is odd.

Direct Proof

Example: *Rule 1*: Let k be an integer. Then, $n = 2k + 1$ is odd.

Rule 2: If a and b are of opposite parity, then $a + b$ is odd.

Desired: The square of the sum of two consecutive integers is odd.

Direct Proof

Solution: We wish to show $(x + [x + 1])^2$ is odd.

Direct Proof

Solution: We wish to show $(x + [x + 1])^2$ is odd.

By rule 2: x and $x + 1$ are opposite parity, hence $x + [x + 1]$ must be odd.

Direct Proof

Solution: We wish to show $(x + [x + 1])^2$ is odd.

By rule 2: x and $x + 1$ are opposite parity, hence $x + [x + 1]$ must be odd.

Algebra: $(x + [x + 1])^2 = 4x^2 + 4x + 1 = 2(2x^2 + 2x) + 1$

Direct Proof

Solution: We wish to show $(x + [x + 1])^2$ is odd.

By rule 2: x and $x + 1$ are opposite parity, hence $x + [x + 1]$ must be odd.

Algebra: $(x + [x + 1])^2 = 4x^2 + 4x + 1 = 2(2x^2 + 2x) + 1$

By rule 1: Since $2x^2 + 2x$ is an integer, then the above expression must be odd.

Proof by Induction

Usage: You want to show that some sequence of objects has some property P.

Proof by Induction

Usage: You want to show that some sequence of objects has some property *P*.

Idea: Show that the first of these objects has this property *P*. Then prove that if the *i*th object has property *P*, then the *i*+1st object also has property *P*.

Proof by Induction

Example: Show that the sum of the first n positive integers is $n(n + 1)/2$.

Proof by Induction

Example: Show that the sum of the first n positive integers is $n(n + 1)/2$.

Solution:

First, show that this holds for $n = 1$. Using the formula, the sum of the first 1 integers is: $1(1 + 1)/2 = 1$. Hence, the property holds for $n = 1$.

Proof by Induction

Example: Show that the sum of the first n positive integers is $n(n + 1)/2$.

Solution:

First, show that this holds for $n = 1$. Using the formula, the sum of the first 1 integers is: $1(1 + 1)/2 = 1$. Hence, the property holds for $n = 1$.

Now, given that this property holds for n, show that it holds for $n + 1$. We have: $1 + 2 + \ldots + n + [n + 1] = n(n + 1)/2 + [n + 1] = (n + 1)(n + 2)/2$. Hence, this holds for all n and we are finished.

Proof by Contradiction

Usage: Is a given statement true? Useful almost everywhere.

Proof by Contradiction

Usage: Is a given statement true? Useful almost everywhere.

Idea: Assume that the desired statement holds. Use this assumption to derive a mathematical or logical contradiction. This shows that our assumption is false.

Proof by Contradiction

Example: Is rt(2) rational?

Proof by Contradiction

Example: Is rt(2) rational?

Solution: Assume that rt(2) is rational. Then rt(2) can be represented as the fraction *a* / *b* in lowest terms for integers *a*, *b*, where one of *a* and *b* is odd.

Proof by Contradiction

Example: Is rt(2) rational?

Solution: Assume that rt(2) is rational. Then rt(2) can be represented as the fraction *a* / *b* in lowest terms for integers *a*, *b*, where one of *a* and *b* is odd.

If *a* / *b* = rt(2) $\rightarrow a^2 = 2b^2$, hence *a* must be even, which implies that *b* is odd.

Proof by Contradiction

Example: Is rt(2) rational?

Solution: Assume that rt(2) is rational. Then rt(2) can be represented as the fraction *a* / *b* in lowest terms for integers *a*, *b*, where one of *a* and *b* is odd.

If a / b = rt(2) $\rightarrow a^2 = 2b^2$, hence *a* must be even, which implies that *b* is odd.

Since *a* is even, it can be written as $2k$ and $a^2 = 4k^2 = 2b^2 \rightarrow 2k^2 = b^2$. Hence, *b* must be even.

Proof by Contradiction

Example: Is rt(2) rational?

Solution: Assume that rt(2) is rational. Then rt(2) can be represented as the fraction *a* / *b* in lowest terms for integers *a*, *b*, where one of *a* and *b* is odd.

If *a* / *b* = rt(2) $\rightarrow a^2 = 2b^2$, hence *a* must be even, which implies that *b* is odd.

Since *a* is even, it can be written as $2k$ and $a^2 = 4k^2 = 2b^2 \rightarrow 2k^2 = b^2$. Hence, *b* must be even.

From above, *b* is both even and odd, which is a contradiction.

Other Proof Techniques

1. Upper/Lower Bounding
2. Existence/Uniqueness Proofs
3. Proof by Casework/Exhaustion

Upper/Lower Bounding Proofs

Usage: We wish to compare two values, a and b.

Upper/Lower Bounding Proofs

Usage: We wish to compare two values, a and b.

Idea: Say we wish to prove $a < b$. In some cases, these quantities are difficult to compare directly. There are two things we can do:

1. We can find some *upper* bound on a, call it a', and show $a' < b$.
2. Alternatively, we can find some *lower* bound on b, call it b', and show $a < b'$.

Upper/Lower Bounding Proofs

Usage: We wish to compare two values, a and b.

Idea: Say we wish to prove $a < b$. In some cases, these quantities are difficult to compare directly. There are two things we can do:

1. We can find some *upper* bound on a, call it a', and show $a' < b$.
2. Alternatively, we can find some *lower* bound on b, call it b', and show $a < b'$.

Applications: Prophet-Inequality and Bulow-Klemperer, both of which we will see soon in class!

Existence and Uniqueness Proofs

Usage: We wish to show that there exists some object *a* with a particular property. Furthermore, we wish to show that it is the *only* object with this property.

Existence and Uniqueness Proofs

Usage: We wish to show that there exists some object *a* with a particular property. Furthermore, we wish to show that it is the *only* object with this property.

Idea: For the existence part of the proof, either one can directly find this object with the desired property, or use a proof by contradiction to show one exists.

Existence and Uniqueness Proofs

Usage: We wish to show that there exists some object *a* with a particular property. Furthermore, we wish to show that it is the *only* object with this property.

Idea: For the existence part of the proof, either one can directly find this object with the desired property, or use a proof by contradiction to show one exists.

For uniqueness, let *a*’ be an alternate object with this property that holds. We will then try and prove that *a* = *a*’.

Existence and Uniqueness Proofs

Usage: We wish to show that there exists some object *a* with a particular property. Furthermore, we wish to show that it is the *only* object with this property.

Idea: For the existence part of the proof, either one can directly find this object with the desired property, or use a proof by contradiction to show one exists.

For uniqueness, let *a'* be an alternate object with this property that holds. We will then try and prove that $a = a'$.

Applications: Banach fixed point theorem. Game of four.

Proof by Casework/Exhaustion

Usage: We wish to show that a particular statement is true in some context that is naturally ‘partitionable’.

Proof by Casework/Exhaustion

Usage: We wish to show that a particular statement is true in some context that is naturally ‘partitionable’.

Idea: We have a statement P that we wish to prove true in some context C. We partition C into events $C_1 \ldots C_n$ and show that P holds in each of $C_1 \ldots C_n$.

Proof by Casework/Exhaustion

Usage: We wish to show that a particular statement is true in some context that is naturally 'partitionable'.

Idea: We have a statement P that we wish to prove true in some context C. We partition C into events $C_1 \ldots C_n$ and show that P holds in each of $C_1 \ldots C_n$.

Applications: The four color theorem that you might have heard of in other courses was proven using this technique!