Proof

1.1 Propositional Logic

Step 0. Proof.

Step 1. Convert program into mathematical formula.

Step 2. Ask the computer to solve the formula.

1.2 First Order Logic

Step 1. Convert program into first order logic formula.

Step 2. Ask the computer to solve the formula.

1.3 Interactive Proof

Step 1. Axiom system

Step 2. Ask the computer to check the invariants

Adapted From:

Stanford CS 103, Lecture 1, 2
Berkeley CS 70, Lecture 2, 3
CMU CDM, Lecture 10

Instructor:

Zhaoguo Wang

Proof

1.1 Propositional Logic

Step 0. Proof.

Step 1. Convert progr
mathematical formula

Step 2. Ask the comp
to solve the formula.

WHAT IS YOUR FIRST QUESTION?

1.2 First Order Logic

am
rmula.

uter
to solve the formula.

1.3 Interactive Proof

Step 1. Axiom system

Step 2. Ask the computer
to check the invariants

Proof

1.1 Propositional Logic

Step 0. Proof.

Step 1. Convert program into mathematical formula.

Step 2. Ask the computer to solve the formula.

1.2 First Order Logic

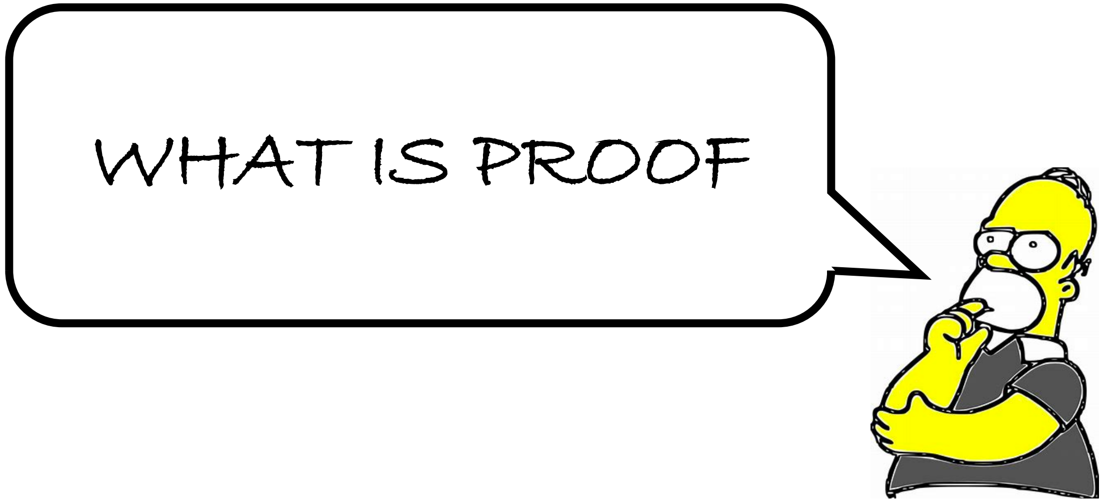
Step 1. Convert program into first order logic formula.

Step 2. Ask the computer to solve the formula.

1.3 Interactive Proof

Step 1. Axiom system

Step 2. Ask the computer to check the invariants



Proof

1.1 Propositional Logic

Step 0. Proof.

Step 1. Convert program into mathematical formula.

Step 2. Ask the computer to solve the formula.

1.2 First Order Logic

Step 1. Convert program into first order logic formula.

Step 2. Ask the computer to solve the formula.

1.3 Interactive Proof

Step 1. Axiom system

Step 2. Ask the computer to check the invariants

A ***proof*** is an argument that demonstrates why a conclusion is true, subject to certain standards of truth. (CS103)

Proof

1.1 Propositional Logic

Step 0. Proof.

Step 1. Convert program into mathematical formula.

Step 2. Ask the computer to solve the formula.

1.2 First Order Logic

Step 1. Convert program into first order logic formula.

Step 2. Ask the computer to solve the formula.

1.3 Interactive Proof

Step 1. Axiom system

Step 2. Ask the computer to check the invariants

A ***mathematical proof*** is an argument that demonstrates why a mathematical statement is true, following the rules of mathematics. (CS103)

Proof

1.1 Propositional Logic

Step 0. Proof.

Step 1. Convert program into mathematical formula.

Step 2. Ask the computer to solve the formula.

1.2 First Order Logic

Step 1. Convert program into first order logic formula.

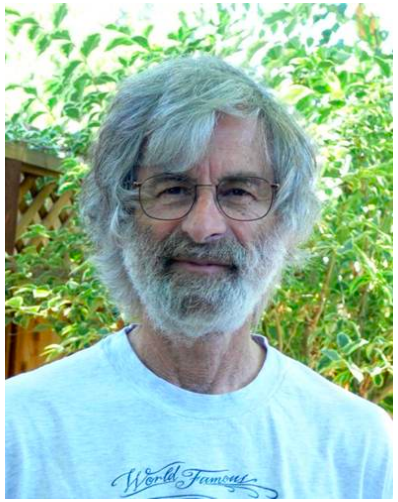
Step 2. Ask the computer to solve the formula.

1.3 Interactive Proof

Step 1. Axiom system

Step 2. Ask the computer to check the invariants

Modern Proofs



Some 20 years ago, I published an article titled *How to Write a Proof* in a festschrift in honor of the 60^{th} birthday of Richard Palais [5]. In celebration of his 80^{th} birthday, I am describing here what I have learned since then about writing proofs and explaining how to write them.

How to Write a Proof

Leslie Lamport

February 14, 1993

revised December 1, 1993

How to Write a 21^{st} Century Proof

Leslie Lamport

23 November 2011

Minor change on 15 January 2012

Examples – Modern Proofs

1. Direct Proof.

2. Proof By Contradiction.

3. Proof By Induction.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

DEFINITION

An integer n is ***even*** if there is an integer k such that $n = 2k$.

An integer n is ***odd*** if there is an integer k such that $n = 2k + 1$.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

ASSUMPTIONS FOR NOW

Every integer is either even or odd.

No integer is both even and odd.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that n = 2k.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that n = 2k.

This means that n2 = $(2k)^2 = 4k^2 = 2(2k^2)$.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

This symbol means "end of proof".

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that n = 2k.

This means that n2 = $(2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since … 2k.

This …

From … k^2)

where …

Therefore, n^2 is even. ■

To prove a statement of the form "If P, then Q".

Assume that P is true, then show that Q must be true as well.

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that n = 2k.

This means that n2 = $(2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that n = 2k.

This means

From this,

where n^2 =

Therefore,

This is the definition of an even integer. When writing a mathematical proof, it's common to call back the definitions,

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

Theor

Notice how we use the value of k that we obtained above. Giving names to quantities, even if we aren't fully sure what they are, allows us to manipulate them. This is similar to variables in programs.

Let n b

Since n is even, there is some integer k such that n = 2k.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

The

Our ultimate goal is to prove that n is even. This means that we need to find some m such that $n^2 = 2m$. Here, we're explicitly showing how we can do that.

Le

Si

Thi

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Direct Proof

Theorem: If n is an even integer, then n^2 is even.

PROOF

Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

DEFINITION

An integer n is ***even*** if there is an integer k such that $n = 2k$.

An integer n is ***odd*** if there is an integer k such that $n = 2k + 1$.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

ASSUMPTIONS FOR NOW

Every integer is either even or odd.

No integer is both even and odd.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Squaring both sides of this equality and simplifying gives the following:

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Squaring both sides of this equality and simplifying gives the following:

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Squaring both sides of this equality and simplifying gives the following:

$n^2 = (2k+1)^2 = 4k^2 + 4k+1 = 2(2k^2 + 2k)+1.$

From this, we see that there is an integer m (namely, $2k2 + 2k$) such that $n2 = 2m + 1$.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Squaring both sides of this equality and simplifying gives the following:

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

From this, we see that there is an integer m (namely, $2k2 + 2k$) such that $n2 = 2m + 1$.

Therefore, $n2$ is odd. ■

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that **if *n* is odd, then n^2 is odd.**

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Squaring both sides of this equality and simplifying gives the following:

$n^2 = (2k+1)^2 = 4k^2 + 4k+1 = 2(2k^2 + 2k)+1$.

From this, we see that there is an integer m (namely, $2k2 + 2k$) such that $n2 = 2m + 1$.

Therefore, $n2$ is odd. ■

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that **if *n* is odd, then n^2 is odd.**

The general pattern here is the following:

1. Start by announcing that we're going to use a proof by contrapositive so that the reader knows what to expect.
2. Explicitly state the contrapositive of what we want to prove.
3. Go prove the contrapositive.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that **if *n* is odd, then *n*^{2} is odd.**

Let n be ... ger

k such th...

Squaring ... ng:

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

From this ... n that

$n2 = 2m + 1$.

Therefore, $n2$ is odd. ■

The contrapositive of the statement.

If P, then Q.

If NOT Q, then NOT P.

Modern Proofs – Proof By Contradiction

Theorem: If n^2 is an even integer, then n is even.

PROOF

We will prove this by contrapositive by showing that if n is odd, then n^2 is odd.

Let n be an arbitrary odd integer. Since n is odd, there is some integer k such that $n = 2k + 1$.

Squaring both sides of this equality and simplifying gives the following:

$n^2 = (2k+1)^2 = 4k^2 +4k+1 = 2(2k^2 +2k)+1$.

From this, we see that there is an integer m (namely, $2k2 + 2k$) such that $n2 = 2m + 1$.

Therefore, $n2$ is odd. ■

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$,

Then $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$. ■

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$,

Then $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$. ■

REALLY??? Tiger, I do not trust you. ☺

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$,

Then $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$. ■

It shows that we can always move to the next step, but we need to start somewhere.

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ **and** if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ **and** if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

First, since $\sum_{i=1}^{1} i = 1, and\ \frac{1(1+1)}{2} = 1$, then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$.

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ **and** if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

First, since $\sum_{i=1}^{1} i = 1, and\ \frac{1(1+1)}{2} = 1$, then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$.

Second, since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ **and** if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

First, since $\sum_{i=1}^{1} i = 1, and\ \frac{1(1+1)}{2} = 1$, then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$.

Second, since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Therefore, the theorem is true. ■

Modern Proofs – Proof By Induction

Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ **and** if $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

The general pattern here is the following:

1. Start by announcing that we're going to use a proof by induction.
2. Explicitly state the base case and the inductive case.
3. Go prove both cases.

Modern Proofs – Proof By Induction

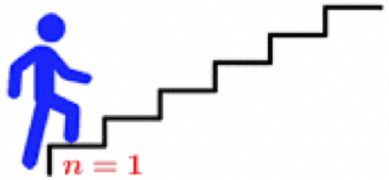
Theorem: If n is an integer and n > 0, then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

PROOF

We will prove this by induction by showing that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ **and if** $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

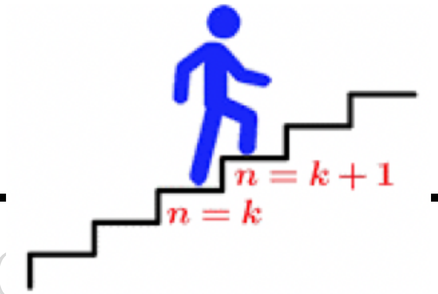
First, since $\sum_{i=1}^{1} i = 1, and\ \frac{1(1+1)}{2} = 1$, then $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$.

Base Case : prove the property holds for base elements.



Modern Proofs – Proof By Induction

inductive case : prove the property holds for elements built by elements-building operations according to induction hypothesis.



First, since $\sum_{i=1}^{1} i = 1, and\ \frac{1(1+1)}{2} = 1$, then $\sum_{i=1}^{1} i = \frac{1(}{2}$.

Second, since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, then $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Therefore, the theorem is true. ■

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

DEFINITION

N queens problem: placing N chess queens on an N×N chessboard so that no two queens threaten each other.

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

DEFINITION

N queens problem: placing N chess queens on an N×N chessboard so that no two queens threaten each other.

Two queens threaten each other: two queens share the same row, column or diagonal.

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

DEFINITION

2 queens problem: placing 2 chess queens on an 2×2 chessboard so that no two queens share the same row, column or diagonal.

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

REPHRASE

If placing 2 chess queens on an 2×2 chessboard, then they must share the same row, column or diagonal.

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

INTUITION

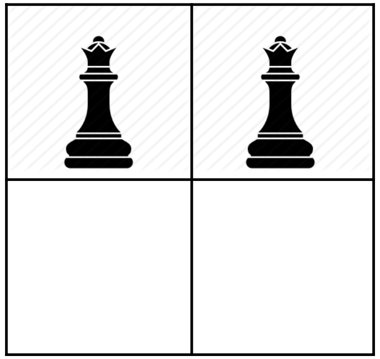
P1	P2
P3	P4

Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

INTUITION

P1	P2
P3	P4

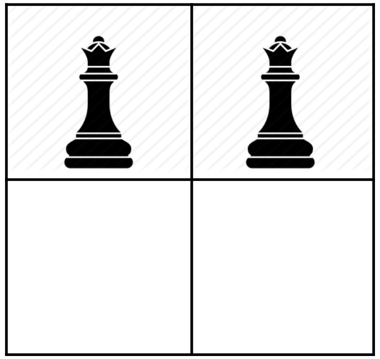


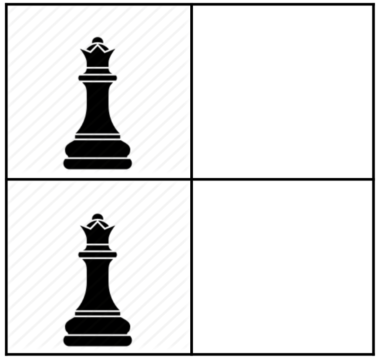
Modern Proofs – Proof By Cases

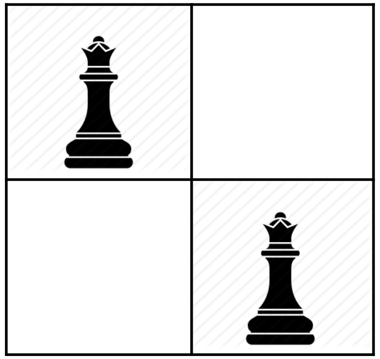
Theorem: Two queens problem has no solution.

INTUITION

P1	P2
P3	P4



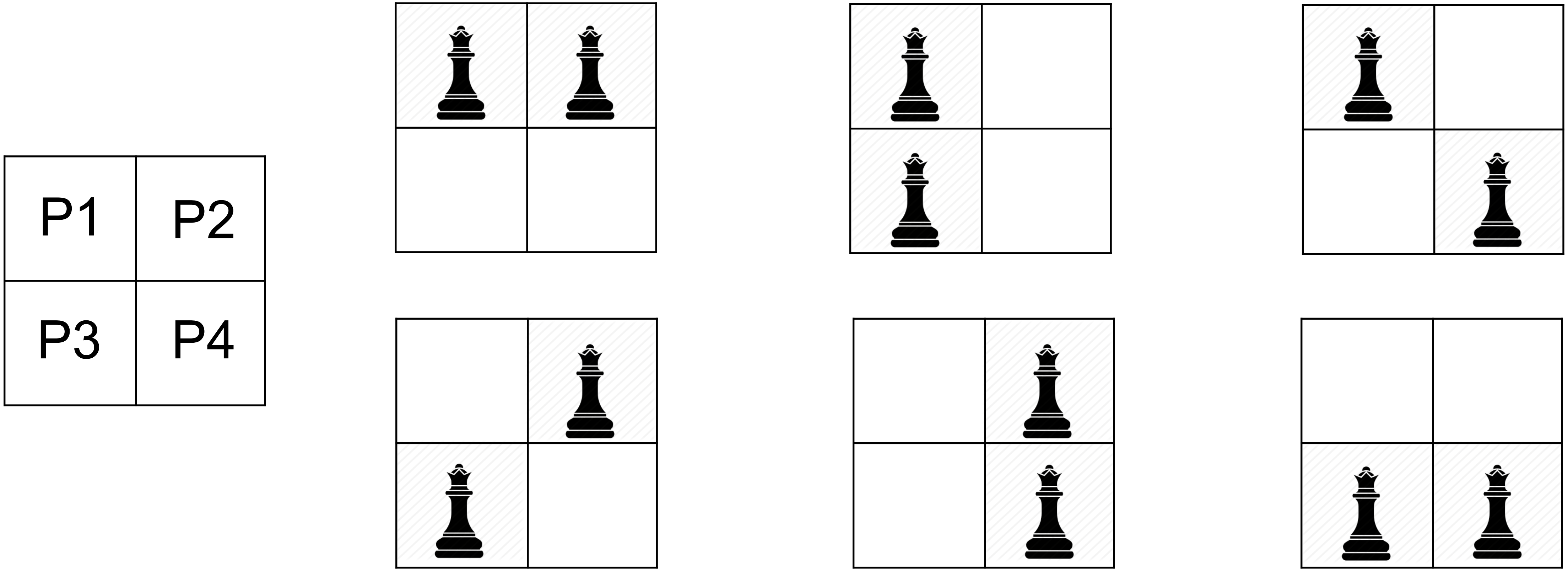




Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

INTUITION



Modern Proofs – Proof By Cases

Theorem: Two queens problem has no solution.

PROOF

Let's pick two positions P_A and P_B to places these two queens. We will prove that two queens threaten each other by cases (by exhaustion).

Case 1: P_A is P1, and P_B is P2, so two queens share the same row.

Case 2: P_A is P1, and P_B is P3, so two queens share the same column.

Case 3: P_A is P1, and P_B is P4, so two queens share the same diagonal.

Case 4: P_A is P2, and P_B is P3, so two queens share the same diagonal.

Case 5: P_A is P2, and P_B is P4, so two queens share the same column.

Case 6: P_A is P3, and P_B is P4, so two queens share the same row.

Since P_A and P_B are symmetric, above list all cases. In any case, we find two queens threaten each other by definition. ■