COMP S264F Unit 2: Methods of Proof

Dr. Keith Lee

School of Science and Technology

The Open University of Hong Kong

Overview

- Proof by inference rules
- Direct proof
- Indirect proof / Proof by contraposition
- Non-proof
- Proof by cases
  - Exhaustive proof / Proof by exhaustion
- Proof by contradiction
- Mathematical induction

Theroem

- A *theorem (lemma)* is a statement that can be shown to be true.
- A theorem often takes the following form:
  - p ~~is true~~.
    - e.g., $\sqrt{2}$ is an irrational number.
  - p $\rightarrow$ q ~~is true~~.
    - e.g., For any integer x, if x is a prime number and x > 3, then $\exists$ n (x = 6n - 1 or 6n + 1).
  - p $\leftrightarrow$ q ~~is true~~.
    - e.g., $\forall$x (x is a prime number and x > 3 if and only if $\exists$ n (x = 6n - 1 or 6n + 1)).

- A *lemma* is a theorem for helping prove another theorem. It is a step in the direction of proof of another theorem.

Proof

- A *proof* is a sequence of statements demonstrating a theorem is true.
  - We want to a proof to be correct, precise, concise.

- Some of these statements are assumed to be true (*axioms, known fact, definitions*), while the truth of other statements is established based on logical deduction.

Proof: Example

Prove: If $\exists x \, \forall y \, P(x, y)$, then $\forall y \, \exists x \, P(x, y)$.

1. Assume $\exists x \, \forall y \, P(x, y)$.
2. $\forall y \, P(x_0, y)$, for some x_0 .
3. $\forall y \, \exists x \, P(x, y)$.

Prove: If $\forall x \, \exists y \, P(x, y)$, then $\exists y \, \forall x \, P(x, y)$.

- Counterexample: Consider P(x, y) as x = y.

Deduction / Inference Rules

Given: $P \Rightarrow Q$ and $\neg P \Rightarrow Q$
Conclude: Q

Why?
$[(P \Rightarrow Q) \wedge (\neg P \Rightarrow Q)] \Rightarrow Q$ is a tautology.

Given: $P \Rightarrow Q$ and $Q \Rightarrow R$
Conclude: $P \Rightarrow R$

Modus ponens
Given: P and $P \Rightarrow Q$
Conclude: Q

Modus tollens
Given: $P \Rightarrow Q$ and $\neg Q$
Conclude: $\neg P$

Quiz:
Given: $\neg P \Rightarrow$ false
Conclude: _______

Given: $\neg P \Rightarrow P$
Conclude: _______

Given: $P \Rightarrow \neg P$
Conclude: _______

Recall that **$p \Rightarrow q$ *is false*** only when **p is true** but **q is false**.

More Inference Rules

Given: $\forall x\, P(x)$.

Conclude: $\exists\, x\, P(x)$.

Given: $\exists\, x\, P(x)$.

Conclude: $P(x_0)$, where x_0 is a particular element (an element, some element) in the domain.

Given: Let x_0 be a particular element in the domain. $P(x_0)$.

Conclude: $\exists\, x\, P(x)$.

Proof by Inference Rules: Example 1

To prove a proposition ***p*** (to be true),

we can start with some proposition ***p'*** that is known to be true and show that ***p'*** $\Rightarrow$ ***p*** (is true).

Then it follows that ***p*** is true. (***Modus ponens***)

This is equivalent to the tautology

$$[\, p' \wedge (p' \Rightarrow p)\,] \Rightarrow p$$

Given:

- If you study in OUHK, you have a student card.
- You study in OUHK.

Conclude: You have a student card.

Proof by Inference Rules: Example 2

Modus tollens

Given: $p \Rightarrow q$ and $\neg q$

Conclude: $\neg p$

This is equivalent to the tautology

$$[(p \Rightarrow q) \land \neg q] \Rightarrow \neg p$$

Given:

- If Tom studies in OUHK, Tom has a student card.
- Tom does not have a student card.

Conclude: Tom does not study in OUHK.

Proof by Inference Rules: Example 3

Hypothetical Syllogism

Given: $p \Rightarrow q$ and $q \Rightarrow r$

Conclude: $p \Rightarrow r$

This is equivalent to the tautology

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$$

Given:

- If you pass the course, then you pass the exam.
- If you pass the exam, then you have attended the exam.

Conclude: If you pass the course, then you have attended the exam.

Proof by Inference Rules: Example 4

Disjunctive Syllogism

Given: $\boldsymbol{p} \vee \boldsymbol{q}$ and $\neg \boldsymbol{p}$

Conclude: $\boldsymbol{q}$

This is equivalent to the tautology

$$[(\boldsymbol{p} \vee \boldsymbol{q}) \wedge \neg \boldsymbol{p}] \Rightarrow \boldsymbol{q}$$

Given:

- I study before exam **or** I fail the course.
- I do not study before exam.

Conclude: I fail the course.

Proving a theorem in the form of $p \Rightarrow q$

<u>Direct proof</u>: To prove $p \Rightarrow q$, we assume that p is true, then show that q is true.

Example: For any integer n, if n is odd, then n^2 is odd.

Proof.

- Suppose that n is odd.
- Then, $n = 2k + 1$ for some integer k.
- It follows that

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

- Therefore, n^2 is odd.

Indirect Proof / Proof by Contraposition

- Note that $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$ (*contrapositive*).
- To prove "$p \Rightarrow q$", we can prove "$\neg q \Rightarrow \neg p$".

Example 1: For any integer n, if 3n + 2 is odd, then n is odd.

Proof. Assume that n is even (i.e., not odd).
Then 3n, as well as 3n+2, is even (i.e., not odd).
Therefore, 3n + 2 is odd $\Rightarrow$ n is odd.

Example 2: For any integer n, if n^2 is even, then n is even.

Proof. We proved its contrapositive in the previous slide:
If n is odd, then n^2 is odd.
Therefore, if n^2 is even, then n is even.

Non-proof

- Failure to note the justification for each step can lead easily to non-proofs.

Theorem. *(not!)* 1 = -1

Proof. $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \sqrt{-1}^2 = -1$.

- At least one of the above steps is false, but each looks reasonable to the author of the proof.
- Writing out the full justifying axioms for each step reveals: it is not incorrect that for any *x* and *y*, $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Proof by Cases

- To prove "$p_1 \vee p_2 \vee \ldots \vee p_n \Rightarrow q$" is true, we note that

$$p_1 \vee p_2 \vee \ldots \vee p_n \Rightarrow q$$
$$\equiv \neg (p_1 \vee p_2 \vee \ldots \vee p_n) \vee q$$
$$\equiv (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \quad \text{[by De Morgan's law]}$$
$$\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \quad \text{[by distributive law]}$$
$$\equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \ldots \wedge (p_n \Rightarrow q)$$

- That means, we should prove each $(p_i \Rightarrow q)$ one by one.

Proof by Cases: Example

(more commonly written as "$n^2 \equiv 1 \bmod 3$").

If n is an integer not divisible by 3, then $\underline{n^2 \bmod 3 = 1}$.

$\equiv$ If ($n \bmod 3 = 1$ **or** $n \bmod 3 = 2$), then $n^2 \bmod 3 = 1$.

$\equiv$ If ($n \bmod 3 = 1$), then $n^2 \bmod 3 = 1$, **and** if ($n \bmod 3 = 2$), then $n^2 \bmod 3 = 1$.

Case 1: If $n \bmod 3 = 1$, $n = 3k + 1$ for some integer k.

It follows that $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$.

Therefore, $n^2 \bmod 3 = 1$.

Case 2: If $n \bmod 3 = 2$, $n = 3k + 2$ for some integer k.

It follows that $n^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$.

Therefore, $n^2 \bmod 3 = 1$.

Exhaustive proof / Proof by Exhaustion

- Exhaustive proof is a special type of proof by cases, where each case involves checking a single example.

Example: All integers between 10 and 15 exclusive are not square of another integer.

Proof.

- The numbers between 10 and 15 exclusive 11, 12, 13,14.
- We can check each of these numbers and show that
-

$$\sqrt{11} \approx 3.316$$
$$\sqrt{12} \approx 3.464$$
$$\sqrt{13} \approx 3.605$$
$$\sqrt{14} \approx 3.741$$

Proof by contradiction

- A popular way to prove a proposition.

> To prove $\boldsymbol{p}$, we show that "$\neg \boldsymbol{p} \Rightarrow$ *false*" is true.
> Note that "$\neg \boldsymbol{p} \Rightarrow$ *false*" is equivalent to $\boldsymbol{p}$.
> Thus, it follows that $\boldsymbol{p}$ is true.

- More specifically, we show that for some proposition $\boldsymbol{r}$,

$$\neg \boldsymbol{p} \Rightarrow (\boldsymbol{r} \text{ and } \neg \boldsymbol{r}) \quad \text{(is true).}$$

- Note that ($\boldsymbol{r}$ and $\neg \boldsymbol{r}$) $\Leftrightarrow$ *false.*
- Therefore, $\neg \boldsymbol{p} \Rightarrow$ *false* (is true).

- NB. We say that *<u>a contradiction occurs</u>* when both $\boldsymbol{r}$ and $\neg \boldsymbol{r}$ can be deduced.

Proof by contradiction: Example

Definition. A real number is **rational** if and only if it can be expressed as a quotient of two integers with a non-zero denominator. More formally, if ***r*** is a real number, then

$$r \text{ is rational} \Leftrightarrow \exists \text{ integers } a, b \text{ such that } r = \frac{a}{b} \text{ and } b > 0$$

Theorem. $\sqrt{2}$ is irrational (i.e., not a rational number).

Proof plan:

Assume $\sqrt{2}$ is rational.

$\sqrt{2} = a/b$ for some integers a, b >0
such that

- a, b are *relatively prime* (i.e., don't have a common factor except 1).
- a, b are **not** *relatively prime*.

false

Proof by contradiction: Example (cont')

Theorem. $\sqrt{2}$ is irrational (i.e., not a rational number).

Proof.

Suppose, for the sake of contradiction, $\sqrt{2}$ is rational.

$\exists$ integers *a*, *b* > 0 such that $\sqrt{2} = \frac{a}{b}$ and *a, b are relatively prime.*

Thus, $\sqrt{2}b = a \;\Rightarrow\; 2b^2 = a^2 \;\Rightarrow\;$ a^2 is even.

In slide 12, we have shown that: If a^2 is even, then *a* is even.

Therefore, *a* is even. (*modus ponens*)

$\Rightarrow$ $a = 2c$ for some integer *c*.

$\Rightarrow b^2 = a^2/2 = (4c^2)/2 = 2c^2$

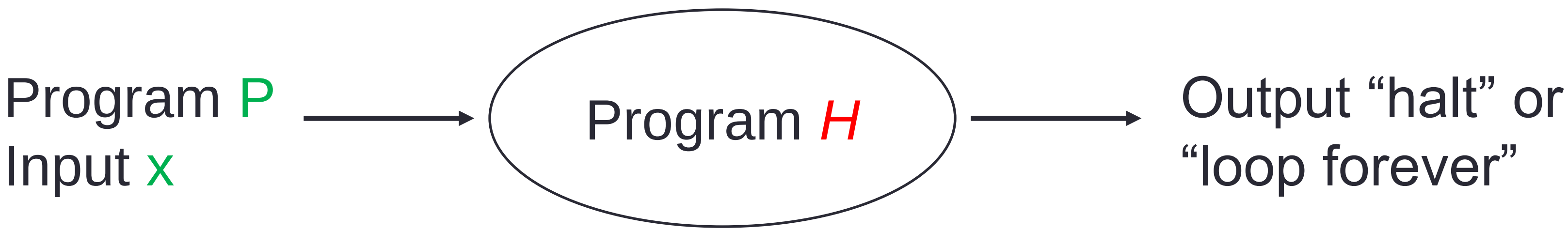
$\Rightarrow$ *b is also even.*

As both *a* and *b* are even, they have a common factor of 2 and are not relatively prime. A contradiction occurs.

Puzzle: Halting problem

Is it possible to write a Python function *H* that

- takes two inputs (arguments): a Python function (binary string) P and an input (binary string) x;
- and reports "loop forever" if P loops forever with input x, and "halt" if P halts eventually ?



Theorem. There doesn't exist such a function *H*.

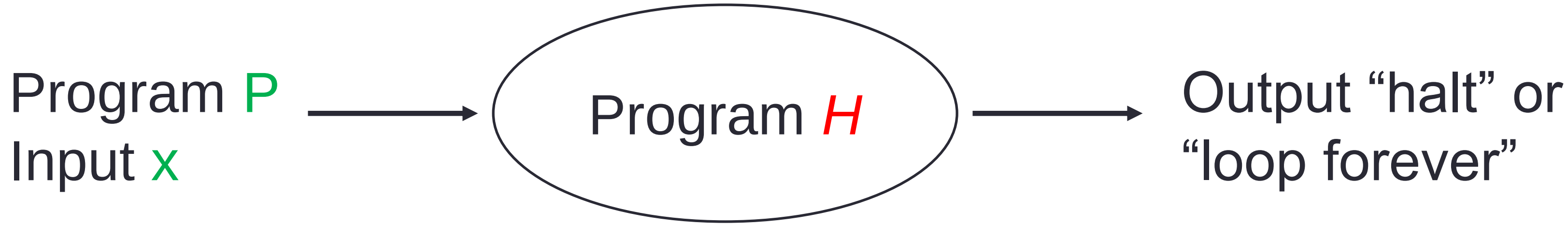
Program P
Input x → Program *H* → Output "halt" or "loop forever"

Proof. Suppose, for the sake of contradiction, that *H* exists.

We construct another function ***K*** that takes only one input, which is a Python function P, and works as follows:

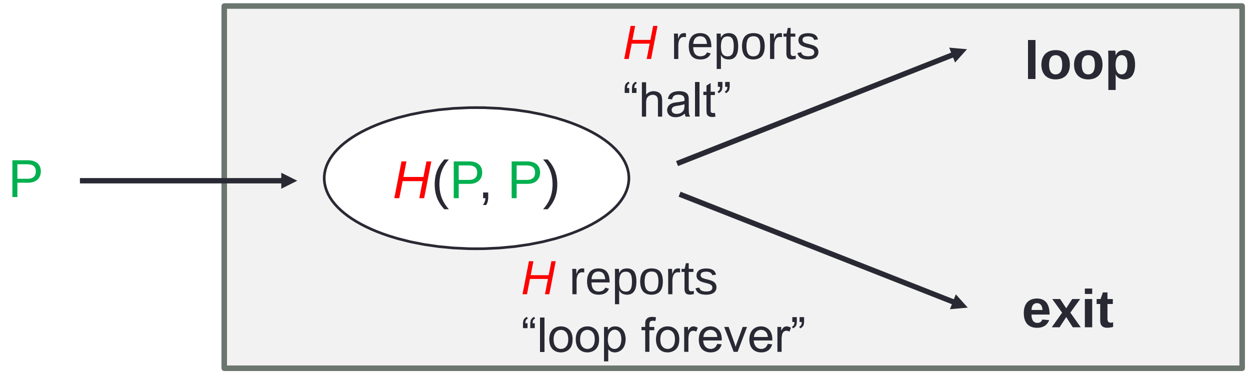
1. Call *H*(P, P)
2. Then, do the following based on the output of *H*(P, P):
   - if *H*(P, P) returns "halt", ***K*** executes a simple loop forever; (e.g.,
     ```
     b = 2
     while b <= 2:
         a = 1
     ```
)
   - if *H*(P, P) returns "loop forever", ***K*** halts immediately.

PS. *H* takes two inputs, and ***K*** takes one input only.



Proof. Suppose, for the sake of contradiction, that *H* exists.

Program ***K***



Fact. ***K***(P) does not loop forever.

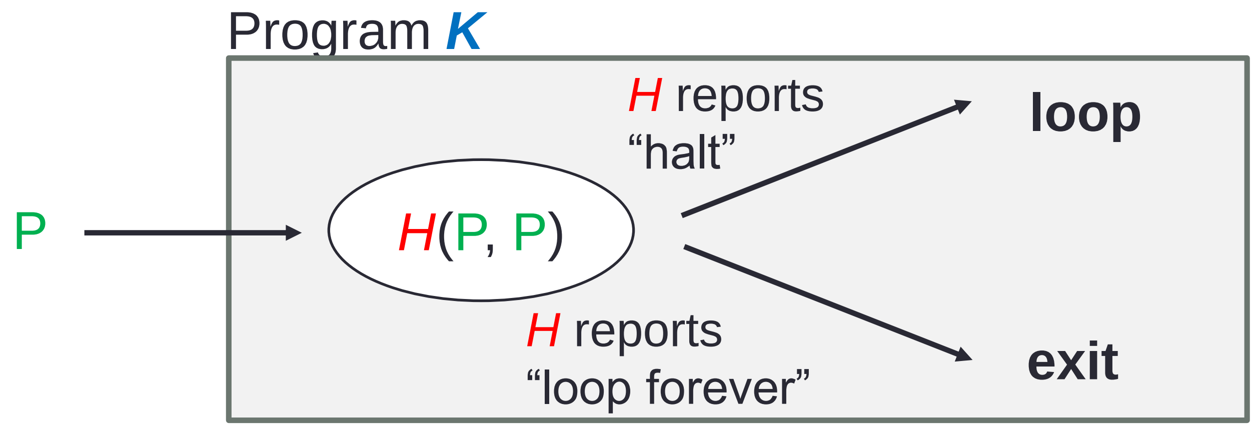
<u>if and only if</u>

H(P, P) reports “loop forever” (by definition of ***K***)

<u>if and only if</u>

P, when given P as input, loops forever (by definition of *H*)

Puzzle: Halting problem - Contradiction



Consider running the function ***K*** with K as input.

K(K) either loops forever or halts.

- <u>***K***(K) loops forever</u>: This happens only when *H*(K, K) reports "halt"; i.e., <u>K(K) does not loop forever</u>.

- <u>***K***(K) halts</u>: This happens only when *H*(K, K) reports "loop forever", i.e., <u>K(K) does not halt</u>.

In both cases, contradiction occurs. Therefore, *H* cannot exist.

Example: Barber paradox

A town has only 1 male barber. A man in the town is shaved by the barber if an only if he does not shave himself.

Theorem. Such a barber does not exist.

Assume, for the sake of contradiction, that such a barber exists. Denote this barber by *B*.

Does *B* shave himself?

- *Yes*: *B* doesn't shave himself.
- *No*: *B* shaves himself.

Proving a theorem in the form of $p \Rightarrow q$ (revisited)

- We can also use proof by contradiction.
- $p \Rightarrow q$ is false $\Leftrightarrow$ p is true and q is false.
- We can show that

$$(p \wedge \neg q) \Rightarrow (\boldsymbol{r} \text{ and } \neg \boldsymbol{r}) \text{ for some } \boldsymbol{r}.$$

- N.B. "$\boldsymbol{r}$ and $\neg \boldsymbol{r}$" is a contradiction (i.e., always false).

Example 2: For any integer n, if n^2 is even, then n is even.

Proof. Assume that $\underline{n^2 \text{ is even}}$ and $\underline{n \text{ is odd}}$.

Thus, $n = 2k + 1$ for some k.

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

Thus, $\underline{n^2 \text{ is odd}}$, which contradicts that $\underline{n^2 \text{ is even}}$.

Proving a theorem in the form of $p \Rightarrow q$ (Summary)

In summary, three possible ways to prove $\mathbf{p} \Rightarrow \mathbf{q}$:

- Assume **p**. … **q**.
- Assume $\neg$**q**. … $\neg$**p**.
- Assume **p** and $\neg$**q**. … **r** and $\neg$**r**. A contradiction occurs.

Proving a theorem in the form of $p \Leftrightarrow q$

To prove $\mathbf{p} \Leftrightarrow \mathbf{q}$, there are many possible ways.

- First assume **p**. … **q**. That is, $\mathbf{p} \Rightarrow \mathbf{q}$.
  And then assume **q**. … **p**. That is, $\mathbf{q} \Rightarrow \mathbf{p}$.

- First assume **p**. … **q**. That is, $\mathbf{p} \Rightarrow \mathbf{q}$.
  And then assume $\neg\mathbf{p}$. … $\neg\mathbf{q}$. That is, $\neg\mathbf{p} \Rightarrow \neg\mathbf{q}$.

- $\mathbf{p} \Leftrightarrow \mathbf{r}_1 \Leftrightarrow \mathbf{r}_2 \Leftrightarrow \ldots \Leftrightarrow \mathbf{q}$.

- …

Recap: Negation

Is $\neg(\forall x\, P(x))$ equivalent to $\exists x\, \neg P(x)$?
I.e., $\neg(\forall x\, P(x)) \Leftrightarrow \exists x\, \neg P(x)$ is true or false?

- YES.
- Suppose "$\neg(\forall x\, P(x))$" is true.
  $\forall x\, P(x)$ is false.
  There exists x such that P(x) is false.
  "$\exists x\, \neg P(x)$" is true.

- Suppose "$\neg(\forall x\, P(x))$" is false.
  $\forall x\, P(x)$ is true.
  "$\exists x\, \neg P(x)$" is false.

Mathematical Induction

- Many theorems have the form P(n) for all positive integers.

- A proof by mathematical induction consists of two steps:
- Basis step (base case): P (1) is true.
- Induction step: for any positive integer i, if P (i) is true,
  then P (i+1) is true.

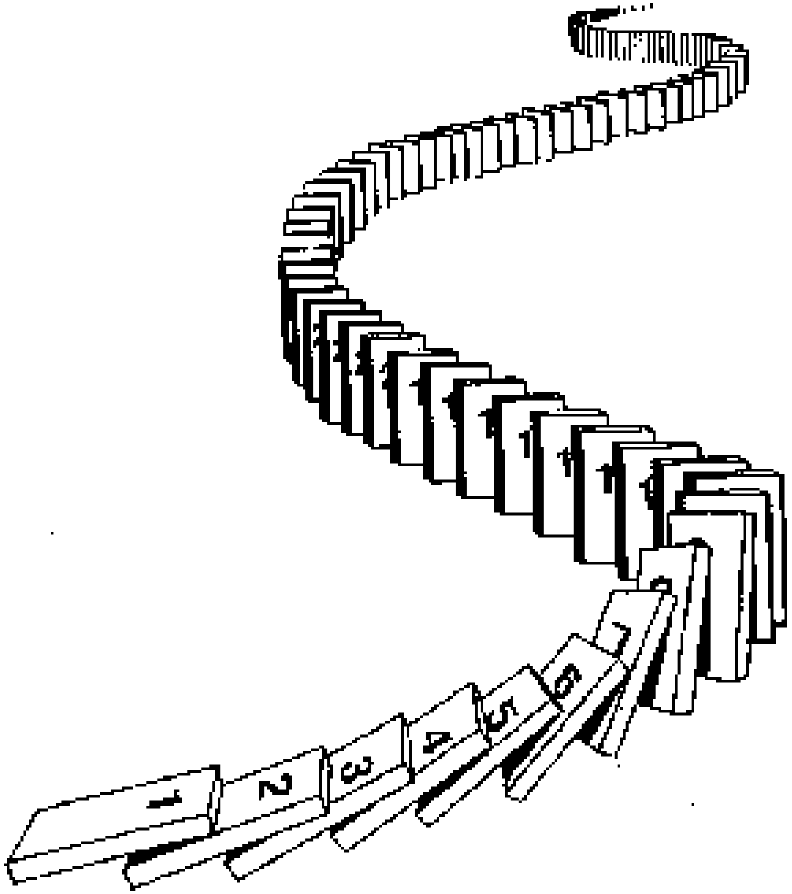
Induction hypothesis

- When we complete both steps, we have proved that
  P(n) is true for all positive integers n.
- Why?

Why Mathematical Induction works?

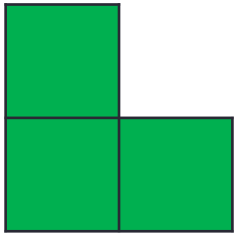
Let k be any integer. Is P(k) true?

- P(1) (is true).
- P(1) $\Rightarrow$ P(2).
- Thus, P(2).
- P(2) $\Rightarrow$ P(3).
- Thus, P(3).
- P(3) $\Rightarrow$ P(4).
- Thus, P(4).
- …
- Thus, P(k).

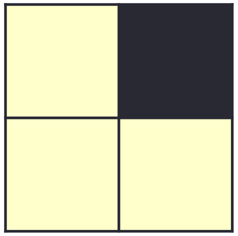


Mathematical Induction: Example

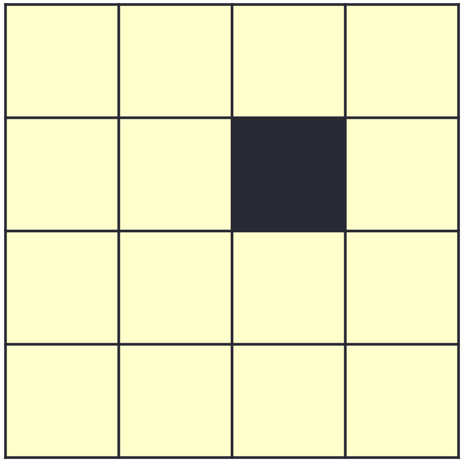
Show that any $2^n \times 2^n$ chessboard with one square removed can be covered using L-shaped pieces (each occupying 3 squares) only.



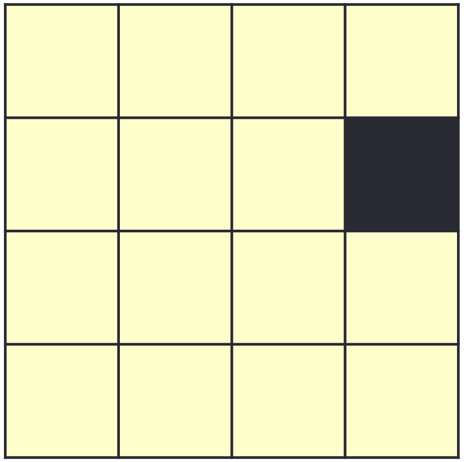
n = 1



n = 2



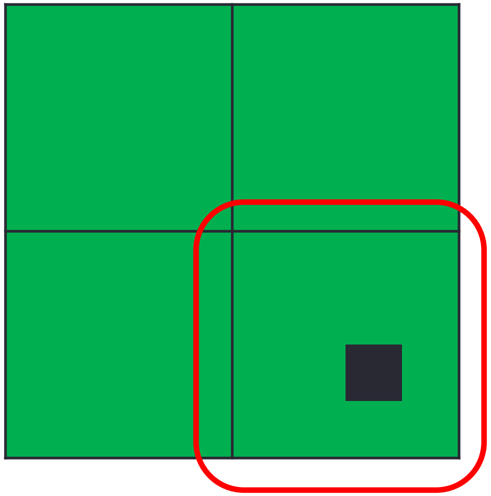
n = 2



Mathematical Induction: Proof

- Basis step, $n = 1$: No matter where the missing square is, the remaining three squares can be covered by one L-shaped piece.

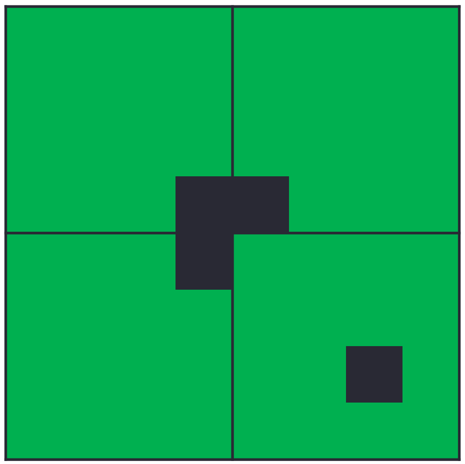
- Inductive step: Assume the claim is true for some $n \geq 1$. Consider a chessboard of size $2^{n+1} \times 2^{n+1}$.
  - Divide the board into 4 quadrants, each containing $2^n \times 2^n$ squares.



By the induction hypothesis, the quadrant containing the missing square can be covered using L-shaped pieces.

What about the remaining three?

Mathematical Induction: Proof (cont’)



Cover the center using one L-shaped piece.

Then apply the induction hypothesis to cover each individual quadrant using L-shaped pieces.

Inductive Step

Inductive step: for any positive integer i, if P(i) is true, then P(i+1) is true.

Another form of inductive step: for any positive integer i, if $P(1) \wedge P(2) \wedge \ldots \wedge P(i)$ is true, then P(i+1) is true.

Both forms of inductive step can lead to the same conclusion (i.e., P(n) is true for all n). However in some cases, the second form is easier to prove.

Example: Big O Notation

- Consider an algorithm A.
- Let f(n) be the number of steps required by an algorithm A when the input is of size n.
- When we way f(n) = O(n), what does it mean?

- What is O(n)? E.g., 66 n, 23n+1234, 100n, log n, …
- Roughly speaking, f(*n*) = O(*n*) if f(*n*) is at most *n* multiplied by a constant.

- Example: MergeSort takes O(n log n) steps to sort n numbers.

Induction

- The following mathematical induction shows that $n^2 = O(n)$
- Basis step: $n = 1$, $1 = O(1)$
- Induction step:

  If $n^2 = O(n)$, then

  $(n+1)^2 = n^2 + 2n + 1 = O(n) + 2n + 1 = O(n)$

Big O Notation: Definition

In general, if a function f(n) = O(n log n), what does it mean?

- Asymptotically, f(n) is at most n log n multiplied by a constant. (E.g., f(n) = 3 n log n + 1000).

- There exists a constant c such that for all n, f(n) ≤ c n log n.
  ∃ c ∀ *n* f(n) ≤ c n log n. (Too restricted!)

- There exists a constant c such that for all sufficiently large n, f(n) ≤ c n log n.
  ∃ c ∃ n_o ∀ *n* if $n > n_o$ **then** f(n) ≤ c n log n.