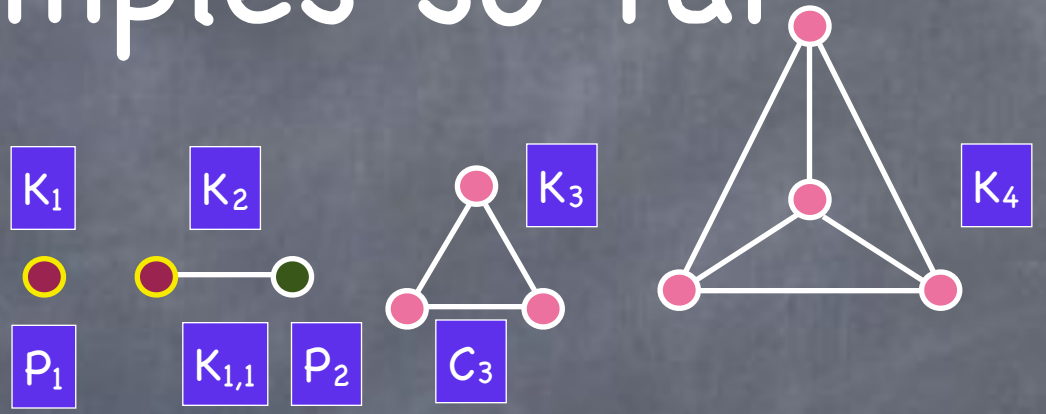
Graphs

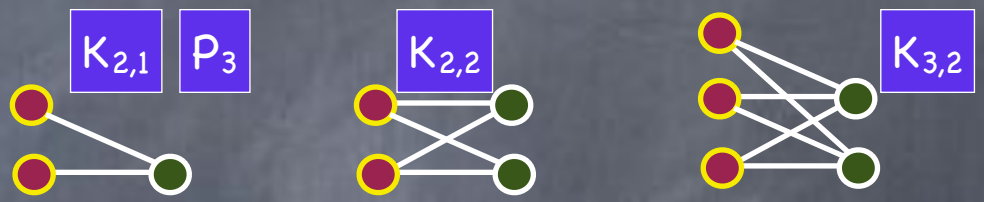
Lecture 13

Examples so far

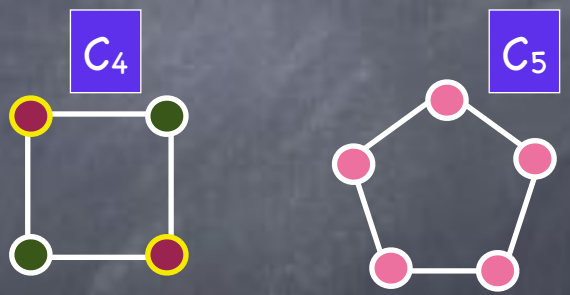
- Complete graph K_n



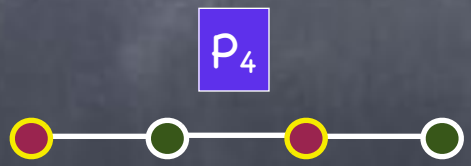
- Complete bi-partite graph $K_{m,n}$



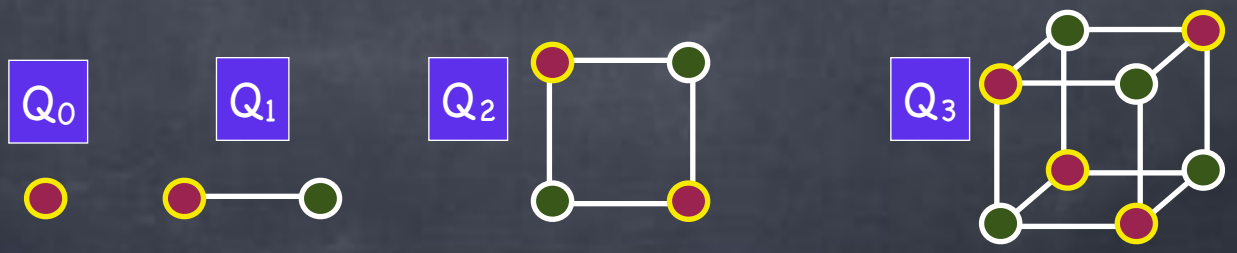
- Cycle graph C_n



- Path graph P_n

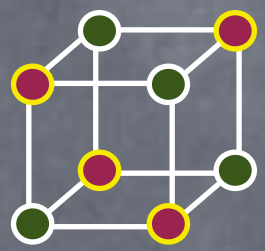


- Hypercube graph Q_n



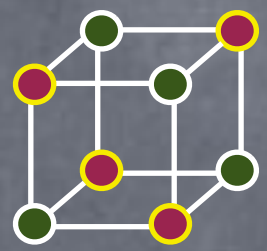
Graph Coloring

Graph Coloring



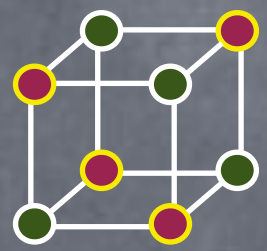
- Recall bi-partite graphs

Graph Coloring



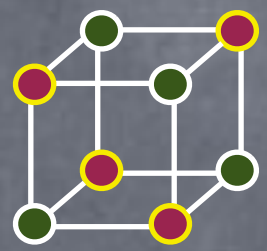
- Recall bi-partite graphs
  - We can "color" the nodes using 2 colors (which part they are in) so that no edge between nodes of the same color

Graph Coloring



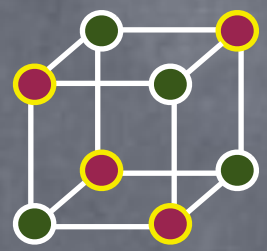
- Recall bi-partite graphs
  - We can "color" the nodes using 2 colors (which part they are in) so that no edge between nodes of the same color
- More generally, a coloring (using k colors) is valid if there is no edge between nodes of the same color

Graph Coloring



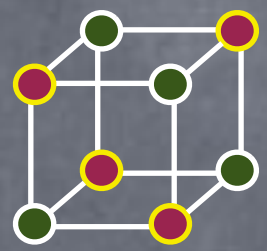
- Recall bi-partite graphs
  - We can "color" the nodes using 2 colors (which part they are in) so that no edge between nodes of the same color
- More generally, a coloring (using k colors) is valid if there is no edge between nodes of the same color
  - k-coloring: a function $c:V \rightarrow \{1,..,k\}$ s.t. $\forall x,y \in V \ \{x,y\} \in E \rightarrow c(x) \neq c(y)$

Graph Coloring



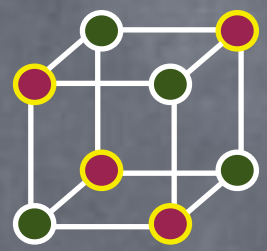
- Recall bi-partite graphs
  - We can "color" the nodes using 2 colors (which part they are in) so that no edge between nodes of the same color
- More generally, a coloring (using k colors) is valid if there is no edge between nodes of the same color
  - k-coloring: a function $c:V \rightarrow \{1,..,k\}$ s.t. $\forall x,y \in V \ \{x,y\} \in E \rightarrow c(x) \neq c(y)$
  - The least number of colors possible in a valid coloring of G is called the Chromatic number of G, $\chi(G)$

Graph Coloring



- Recall bi-partite graphs
  - We can "color" the nodes using 2 colors (which part they are in) so that no edge between nodes of the same color
- More generally, a coloring (using k colors) is valid if there is no edge between nodes of the same color
  - k-coloring: a function $c:V \to \{1,..,k\}$ s.t. $\forall x,y \in V \ \{x,y\} \in E \rightarrow c(x) \neq c(y)$
  - The least number of colors possible in a valid coloring of G is called the Chromatic number of G, $\chi(G)$
    - G has a k-coloring $\leftrightarrow$ $\chi(G) \leq k$

Graph Coloring



- Recall bi-partite graphs
  - We can "color" the nodes using 2 colors (which part they are in) so that no edge between nodes of the same color
- More generally, a coloring (using k colors) is valid if there is no edge between nodes of the same color
  - k-coloring: a function $c:V \to \{1,..,k\}$ s.t. $\forall x,y \in V \ \{x,y\} \in E \rightarrow c(x) \neq c(y)$
  - The least number of colors possible in a valid coloring of G is called the Chromatic number of G, $\chi(G)$
    - G has a k-coloring $\leftrightarrow$ $\chi(G) \leq k$

Upper-bounding $\chi(G)$

Graph Coloring

Graph Coloring

- Suppose H is a subgraph of G. Then:

Graph Coloring

- Suppose H is a subgraph of G. Then:
  - G has a k-coloring → H has a k-coloring

Graph Coloring

- Suppose H is a subgraph of G. Then:
  - G has a k-coloring → H has a k-coloring
    - i.e., $\chi(G) \geq \chi(H)$

Graph Coloring

- Suppose H is a subgraph of G. Then:
  - G has a k-coloring → H has a k-coloring
    - i.e., $\chi(G) \geq \chi(H)$

Lower-bounding $\chi(G)$

Graph Coloring

- Suppose H is a subgraph of G. Then:
  - G has a k-coloring → H has a k-coloring
    - i.e., $\chi(G) \geq \chi(H)$

Lower-bounding $\chi(G)$

- e.g., G has K_n as a subgraph → $\chi(G) > n-1$ (i.e., $\chi(G) \geq n$)

Graph Coloring

- Suppose H is a subgraph of G. Then:
  - G has a k-coloring → H has a k-coloring
    - i.e., $\chi(G) \geq \chi(H)$

Lower-bounding $\chi(G)$

- e.g., G has K_n as a subgraph → $\chi(G) > n-1$ (i.e., $\chi(G) \geq n$)
- e.g., G has C_n for odd n as a subgraph → $\chi(G) > 2$

Graph Coloring

- Suppose H is a subgraph of G. Then:
  - G has a k-coloring → H has a k-coloring
    - i.e., $\chi(G) \geq \chi(H)$

Lower-bounding $\chi(G)$

- e.g., G has K_n as a subgraph → $\chi(G) > n-1$ (i.e., $\chi(G) \geq n$)
- e.g., G has C_n for odd n as a subgraph → $\chi(G) > 2$
- Summary: One way to show $k_{lower} \leq \chi(G) \leq k_{upper}$
  Show a coloring $c:V \rightarrow \{1,\ldots,k_{upper}\}$
  And show a subgraph H with $k_{lower} \leq \chi(H)$

Complete Graph

Complete Graph

- $\chi(G)=|V| \leftrightarrow$ G is isomorphic to $K_{|V|}$

Complete Graph

- $\chi(G)=|V| \leftrightarrow$ G is isomorphic to $K_{|V|}$
  - $\leftarrow$: $\chi(K_n) = n$ and isomorphism preserves χ (exercise!)

Complete Graph

- $\chi(G)=|V| \leftrightarrow$ G is isomorphic to $K_{|V|}$
  - $\leftarrow$: $\chi(K_n) = n$ and isomorphism preserves χ (exercise!)
  - $\rightarrow$: We will prove the contrapositive: i.e., that if G not isomorphic to $K_{|V|}$, then $\chi(G) \neq |V|$.

Complete Graph

- $\chi(G)=|V| \leftrightarrow$ G is isomorphic to $K_{|V|}$
  - $\leftarrow$: $\chi(K_n) = n$ and isomorphism preserves χ (exercise!)
  - $\rightarrow$: We will prove the contrapositive: i.e., that if G not isomorphic to $K_{|V|}$, then $\chi(G) \neq |V|$.
    - Suppose G not isomorphic to $K_{|V|}$. So G should have at least two distinct nodes u, v s.t. $\{u,v\} \notin E$. Consider the coloring which assigns colors $\{1,..., |V|-2\}$ to the nodes in $V-\{u,v\}$ and the color $|V|-1$ to both u and v. This is a valid coloring (because $f(x)=f(y) \rightarrow \{x,y\} \notin E$). So $\chi(G) \leq |V|-1$

Graph Coloring

Graph Coloring

- The origins: map-making

Graph Coloring

- The origins: map-making
  - "Graph": one node for each country; an edge between countries which share a border

Graph Coloring

- The origins: map-making
  - "Graph": one node for each country; an edge between countries which share a border
  - Neighboring countries shouldn't have the same color. Use as few colors as possible.

Graph Coloring

- The origins: map-making
  - "Graph": one node for each country; an edge between countries which share a border
  - Neighboring countries shouldn't have the same color. Use as few colors as possible.
- Next time: $\chi(G) \leq$ Max-degree(G) + 1 (proof by "induction"!)

Graph Coloring

- The origins: map-making
  - "Graph": one node for each country; an edge between countries which share a border
  - Neighboring countries shouldn't have the same color. Use as few colors as possible.
- Next time: $\chi(G) \leq$ Max-degree(G) + 1 (proof by "induction"!)
- Efficient algorithms known for coloring many special kinds of graphs with as few colors as possible

Graph Coloring

- The origins: map-making
  - "Graph": one node for each country; an edge between countries which share a border
  - Neighboring countries shouldn't have the same color. Use as few colors as possible.
- Next time: $\chi(G) \leq$ Max-degree(G) + 1 (proof by "induction"!)
- Efficient algorithms known for coloring many special kinds of graphs with as few colors as possible
  - But computing chromatic number in general is believed to be "hard" (known to be in a class of problems called "NP-hard")

Graphs in action

Graph Coloring in Action

- Many problems can be modeled as a graph coloring problem
- Resource scheduling: allocate "**resources**" (e.g. time slots, radio frequencies) to "**demands**" (exams, radio stations). Use as few resources as possible. Same resource can be used to satisfy multiple demands, as long as they don't have a "**conflict**" (same student, inhabited area with signal overlap).
  - Create a "conflict graph": Demands are the nodes; connect them by an edge if they have a conflict
  - Color the graph with as few colors as possible
  - Allocate one resource per color

Shortest Paths in Action

- Obvious example: nodes correspond to locations on a map and edges are roads, optic fibers etc.
  - Weighted edges: each edge has its own "length" (instead of 1)
- But also over more abstract graphs
  - e.g., Graph-based models in AI/machine-learning for modeling probabilistic systems
    - e.g., a graph, modeling speech production: nodes correspond to various "states" the vocal chords/lips etc. could be in while producing a given a sound sequence. Edges show transitions (next state) over time. Shortest path in this graph gives the "most likely" word that was spoken.

Graphs in action

Network Flow

- Transporting (people, material, data) over a network of links with limited capacity, and possibly cost for bandwidth use
  - A central problem in "Operations Research"
- (Bipartite) Matching problem: pair up every node with one of its neighbors, so that no node is left alone or has more than one partner
- "Max-flow Min-cut" theorem: can route as much flow from one node to another, as the smallest "cut" permits
  - Efficient algorithms known
  - More challenging when there are multiple flows to be routed together on the same network

More graphs

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds
- Graphs used to design networks of processors in a super-computer

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds
- Graphs used to design networks of processors in a super-computer
- Design graphs with **low degree** (look at a few (neighboring) pieces of data at a time; reduce hardware cost), but **good "connectivity"** -- i.e., (possibly many) short paths between any two nodes (to reach the required piece of data quickly, by taking a path over the graph; to route data quickly)

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds
- Graphs used to design networks of processors in a super-computer
- Design graphs with **low degree** (look at a few (neighboring) pieces of data at a time; reduce hardware cost), but **good "connectivity"** -- i.e., (possibly many) short paths between any two nodes (to reach the required piece of data quickly, by taking a path over the graph; to route data quickly)
- Very efficient algorithms known for relevant graph problems

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds
- Graphs used to design networks of processors in a super-computer
- Design graphs with **low degree** (look at a few (neighboring) pieces of data at a time; reduce hardware cost), but **good "connectivity"** -- i.e., (possibly many) short paths between any two nodes (to reach the required piece of data quickly, by taking a path over the graph; to route data quickly)
- Very efficient algorithms known for relevant graph problems
  - e.g., breadth/depth-first search, shortest path algorithm...

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds
- Graphs used to design networks of processors in a super-computer
- Design graphs with **low degree** (look at a few (neighboring) pieces of data at a time; reduce hardware cost), but **good "connectivity"** -- i.e., (possibly many) short paths between any two nodes (to reach the required piece of data quickly, by taking a path over the graph; to route data quickly)
- Very efficient algorithms known for relevant graph problems
  - e.g., breadth/depth-first search, shortest path algorithm...
- But many other graph problems are known to be "NP-hard"

Graphs in action

More graphs

- Used to keep data in an easy-to-search/manipulate fashion
  - **Data structures**: mainly, (balanced) "trees" of various kinds
- Graphs used to design networks of processors in a super-computer
- Design graphs with **low degree** (look at a few (neighboring) pieces of data at a time; reduce hardware cost), but **good "connectivity"** -- i.e., (possibly many) short paths between any two nodes (to reach the required piece of data quickly, by taking a path over the graph; to route data quickly)
- Very efficient algorithms known for relevant graph problems
  - e.g., breadth/depth-first search, shortest path algorithm...
- But many other graph problems are known to be "NP-hard"
  - e.g., Traveling Salesperson Problem (TSP): visit all cities, by traveling the least distance

Mathematical Induction

Proof by Programming

Lecture 13

Programming a Proof

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔
  - $f(2) = 5$, $g(2) = 5$ ✔

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔
  - $f(2) = 5$, $g(2) = 5$ ✔
  - $f(3) = 14$, $g(3) = 14$ ✔

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔
  - $f(2) = 5$, $g(2) = 5$ ✔
  - $f(3) = 14$, $g(3) = 14$ ✔
  - But we need to check this for all n...

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔
  - $f(2) = 5$, $g(2) = 5$ ✔
  - $f(3) = 14$, $g(3) = 14$ ✔
  - But we need to check this for all n...
- To the rescue: mathematical induction

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔
  - $f(2) = 5$, $g(2) = 5$ ✔
  - $f(3) = 14$, $g(3) = 14$ ✔
  - But we need to check this for all n...
- To the rescue: mathematical induction
  - No need to explicitly write down such a proof. Enough to prove that an explicit proof exists!

Programming a Proof

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔
  - $f(2) = 5$, $g(2) = 5$ ✔
  - $f(3) = 14$, $g(3) = 14$ ✔
  - But we need to check this for all n...
- To the rescue: mathematical induction
  - No need to explicitly write down such a proof. Enough to prove that an explicit proof exists!
    - Describe a procedure that can generate the proof for each n

A Funny ATM

A Funny ATM

A Funny ATM

- Give it a $1 bill, it gives you a $2 bill (it is a funny ATM..)
  In fact, give it an $n bill, it gives you an $(n+1) bill ($n \geq 1$)

A Funny ATM

- Give it a $1 bill, it gives you a $2 bill (it is a funny ATM..)
  In fact, give it an $n bill, it gives you an $(n+1) bill ($n \geq 1$)
- How do you get a $100 bill out of this ATM?

A Funny ATM

- Give it a $1 bill, it gives you a $2 bill (it is a funny ATM..)
  In fact, give it an $n bill, it gives you an $(n+1) bill (n≥1)
- How do you get a $100 bill out of this ATM?
  - Give it a $99 bill.

A Funny ATM

- Give it a $1 bill, it gives you a $2 bill (it is a funny ATM..)
  In fact, give it an $n bill, it gives you an $(n+1) bill ($n \geq 1$)
- How do you get a $100 bill out of this ATM?
  - Give it a $99 bill.
  - But what if you don't have one?

A Funny ATM

- Give it a $1 bill, it gives you a $2 bill (it is a funny ATM..)
  In fact, give it an $n bill, it gives you an $(n+1) bill ($n \geq 1$)
- How do you get a $100 bill out of this ATM?
  - Give it a $99 bill.
  - But what if you don't have one?
  - Get it from the ATM by feeding it a $98 bill. And if you don't have a $98 bill, get that from the ATM... Enough to start with a $1 bill!

A Funny ATM

- Give it a $1 bill, it gives you a $2 bill (it is a funny ATM..)
  In fact, give it an $n bill, it gives you an $(n+1) bill ($n \geq 1$)
- How do you get a $100 bill out of this ATM?
  - Give it a $99 bill.
  - But what if you don't have one?
  - Get it from the ATM by feeding it a $98 bill. And if you don't have a $98 bill, get that from the ATM... Enough to start with a $1 bill!
- To get a $100 bill, you need two things: some smaller bill ($1 would do) and the funny ATM

A Proof in Two Acts

A Proof in Two Acts

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$

A Proof in Two Acts

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$

A Proof in Two Acts

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+$, $f(n) = g(n)$
  - $f(1) = 1$, $g(1) = 1$ ✔ (that is our $1 bill)

A Proof in Two Acts

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$
  - $f(1) = 1,\ \ g(1) = 1$ ✔ (that is our $1 bill)

Proving the Base Case

A Proof in Two Acts

Proving the Base Case

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$
  - $f(1) = 1,\ \ g(1) = 1$ ✔ (that is our $1 bill)
- What is the funny ATM?

A Proof in Two Acts

Proving the Base Case

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$
  - $f(1) = 1,\ \ g(1) = 1$ ✔ (that is our $1 bill)
- What is the funny ATM?
  - $\forall n \in \mathbb{Z}^+,\ \ (\underline{f(n) = g(n)}) \rightarrow (\underline{f(n+1) = g(n+1)})$

A Proof in Two Acts

Proving the Base Case

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$
  - $f(1) = 1,\ \ g(1) = 1$ ✔ (that is our $1 bill)
- What is the funny ATM?
  - $\forall n \in \mathbb{Z}^+,\ \ (\underline{f(n) = g(n)}) \rightarrow (\underline{f(n+1) = g(n+1)})$
    - We need to build this ATM: i.e., prove this statement

A Proof in Two Acts

Proving the Base Case

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ \ f(n) = g(n)$
  - $f(1) = 1,\ \ g(1) = 1$ ✔ (that is our $1 bill)
- What is the funny ATM?
  - $\forall n \in \mathbb{Z}^+,\ \ (\underline{f(n) = g(n)}) \rightarrow (\underline{f(n+1) = g(n+1)})$
    - We need to build this ATM: i.e., prove this statement
      - This is easier than proving the original statement

A Proof in Two Acts

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ f(n) = g(n)$
  - $f(1) = 1,\quad g(1) = 1$ ✔ (that is our \$1 bill)
- What is the funny ATM?
  - $\forall n \in \mathbb{Z}^+,\ (f(n) = g(n)) \rightarrow (f(n+1) = g(n+1))$
  - We need to build this ATM: i.e., prove this statement
    - This is easier than proving the original statement

Proving the Base Case

Proving original statement: setting up a press to print any \$n bill.

ATM needs to only change the value printed on the bill

A Proof in Two Acts

- Let $f(n) = \Sigma_{(i=1 \text{ to } n)}\ i^2$ and $g(n) = n(n+1)(2n+1)/6$
- $\forall n \in \mathbb{Z}^+,\ f(n) = g(n)$
  - $f(1) = 1,\ g(1) = 1$ ✔ (that is our \$1 bill)
- What is the funny ATM?
  - $\forall n \in \mathbb{Z}^+,\ (f(n) = g(n)) \rightarrow (f(n+1) = g(n+1))$
  - We need to build this ATM: i.e., prove this statement
    - This is easier than proving the original statement
  - We also need to procure a \$1 bill (we already did by proving f(1)=g(1))

Proving the Base Case

Proving original statement: setting up a press to print any \$n bill.

ATM needs to only change the value printed on the bill

Building the ATM

Building the ATM

The Induction Step

Building the ATM

- To prove: $\forall k \in \mathbb{Z}^+$, $(f(k) = g(k)) \rightarrow (f(k+1) = g(k+1))$

The Induction Step

Building the ATM

- To prove: $\forall k \in \mathbb{Z}^+$, $(f(k) = g(k)) \rightarrow (f(k+1) = g(k+1))$

The Induction Step

- Consider an arbitrary $k \in \mathbb{Z}^+$ s.t. $f(k)=g(k)$

Building the ATM

- To prove: $\forall k \in \mathbb{Z}^+$, $(f(k) = g(k)) \rightarrow (f(k+1) = g(k+1))$

The Induction Step

- Consider an arbitrary $k \in \mathbb{Z}^+$ s.t. $f(k)=g(k)$

- $f(k+1) = f(k) + (k+1)^2$
  $= g(k) + (k+1)^2$ By induction hypothesis
  $= k(k+1)(2n+1)/6 + (k+1)^2$

Building the ATM

- To prove: $\forall k \in \mathbb{Z}^+$, $(f(k) = g(k)) \rightarrow (f(k+1) = g(k+1))$

The Induction Step

- Consider an arbitrary $k \in \mathbb{Z}^+$ s.t. $f(k)=g(k)$

- $f(k+1) = f(k) + (k+1)^2$
  $= g(k) + (k+1)^2$ By induction hypothesis
  $= k(k+1)(2n+1)/6 + (k+1)^2$

- Now some algebraic manipulation:

  $f(k+1) = k(k+1)(2k+1)/6 + (k+1)^2 = (k+1)\,[\,2k^2 + k + 6k + 6\,]/6$

  $g(k+1) = (k+1)(k+2)(2(k+1)+1)/6 = (k+1)\,[\,(k+2)(2k+3)\,]/6$

Building the ATM

The Induction Step

- To prove: $\forall k \in \mathbb{Z}^+,\ (f(k) = g(k)) \rightarrow (f(k+1) = g(k+1))$
- Consider an arbitrary $k \in \mathbb{Z}^+$ s.t. $f(k)=g(k)$
- $f(k+1) = f(k) + (k+1)^2$
  $= g(k) + (k+1)^2$ By induction hypothesis
  $= k(k+1)(2n+1)/6 + (k+1)^2$
- Now some algebraic manipulation:

  $f(k+1) = k(k+1)(2k+1)/6 + (k+1)^2 = (k+1)\ [\ 2k^2 + k + 6k + 6\ ]/6$

  $g(k+1) = (k+1)(k+2)(2(k+1)+1)/6 = (k+1)\ [\ (k+2)(2k+3)\ ]/6$
- $f(k+1) = g(k+1)$

Completing the proof

Completing the proof

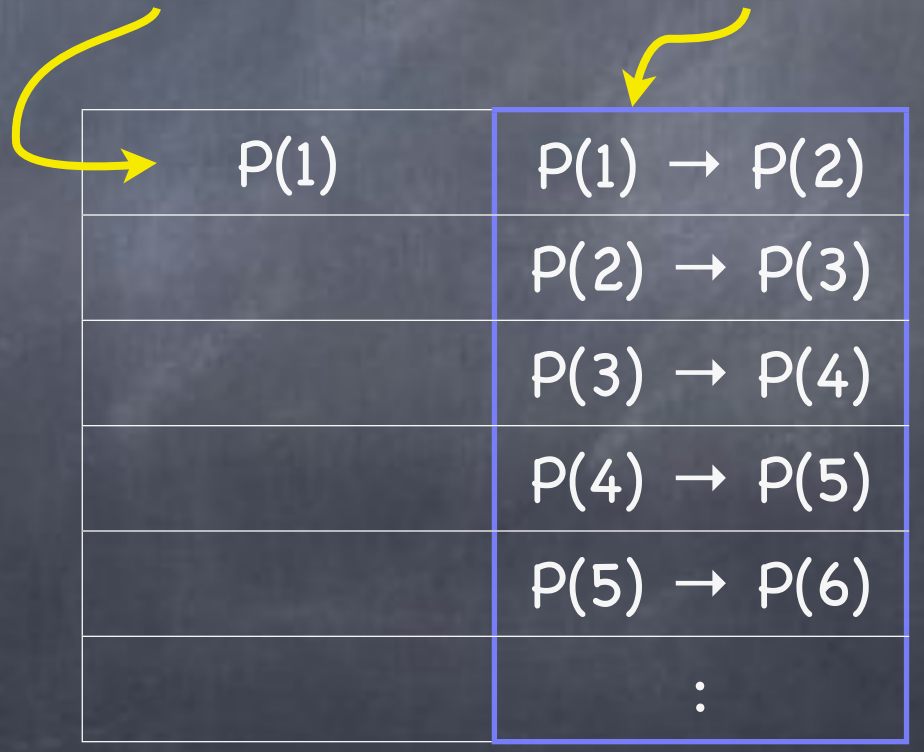
- To prove $\forall n \in \mathbb{Z}^+$ P(n):

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$

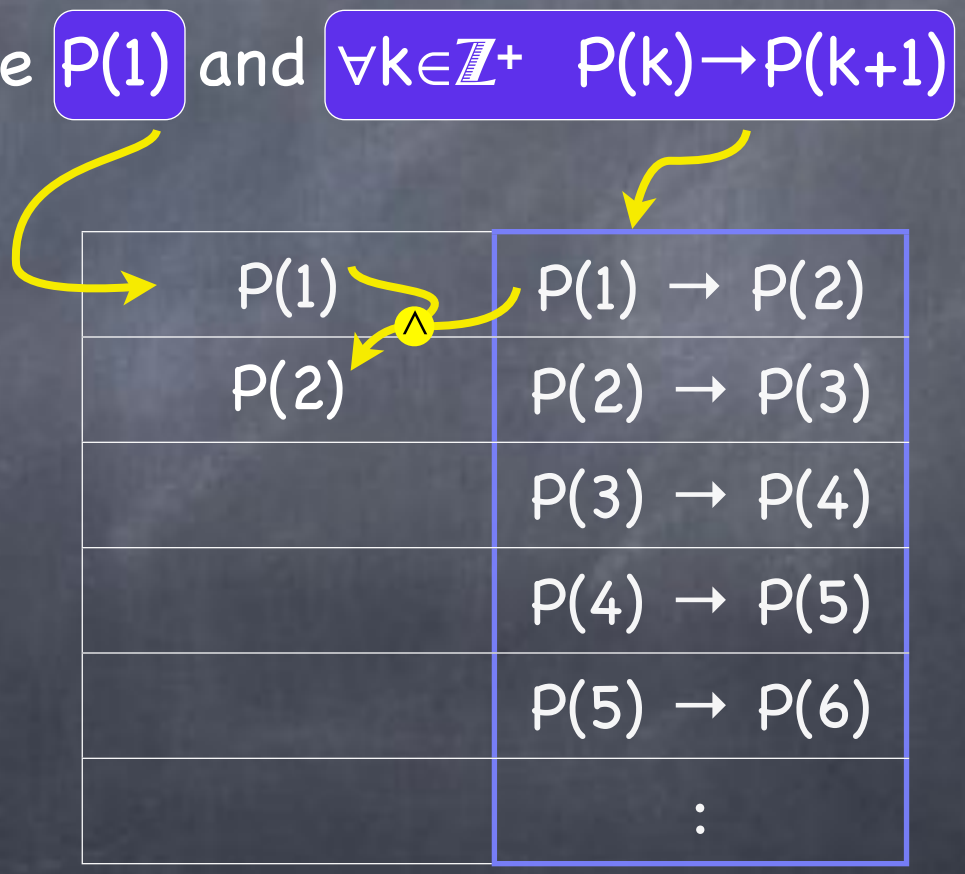
Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$



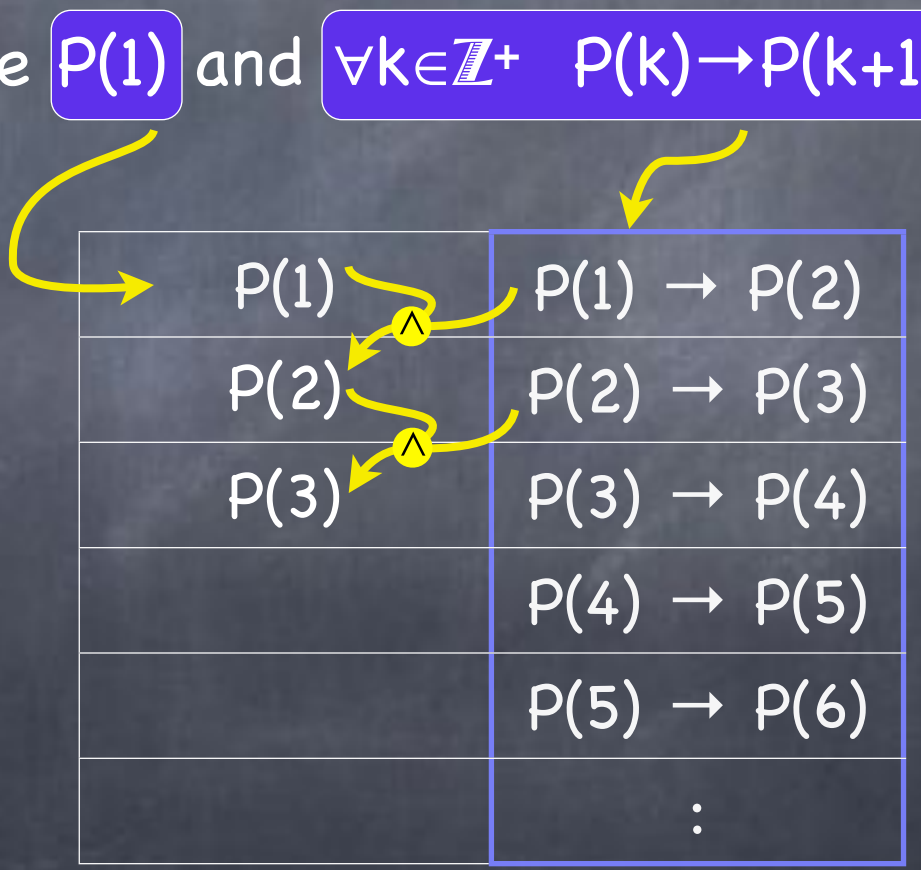
Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$



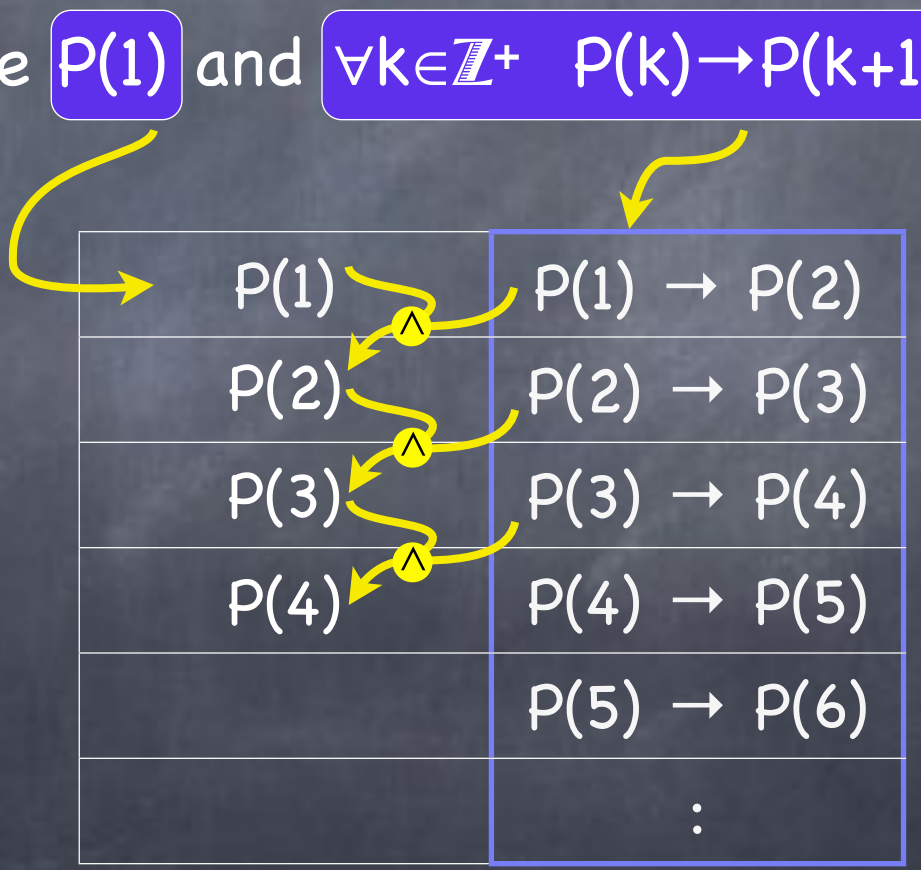
Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$



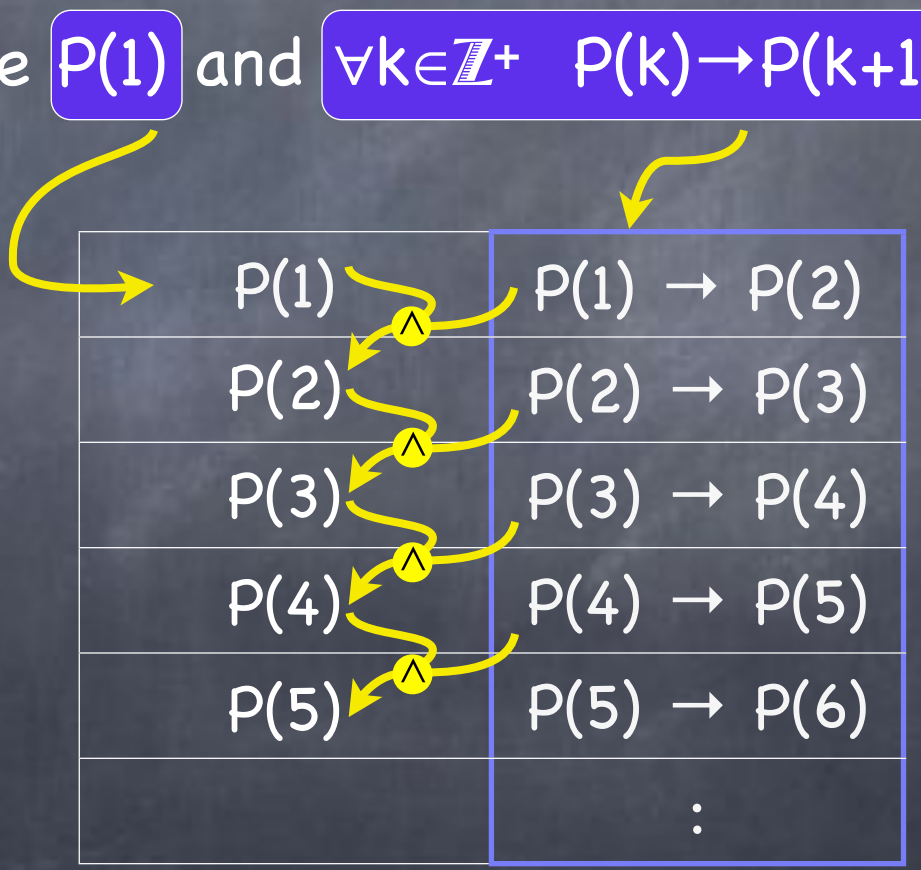
Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$



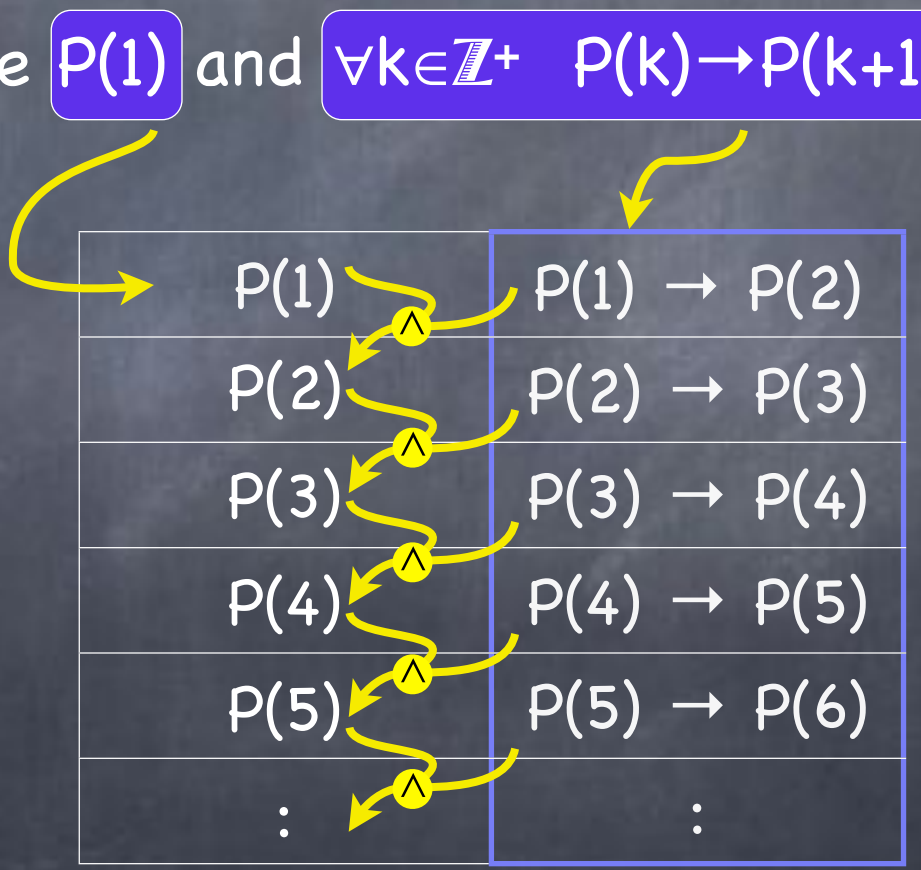
Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$



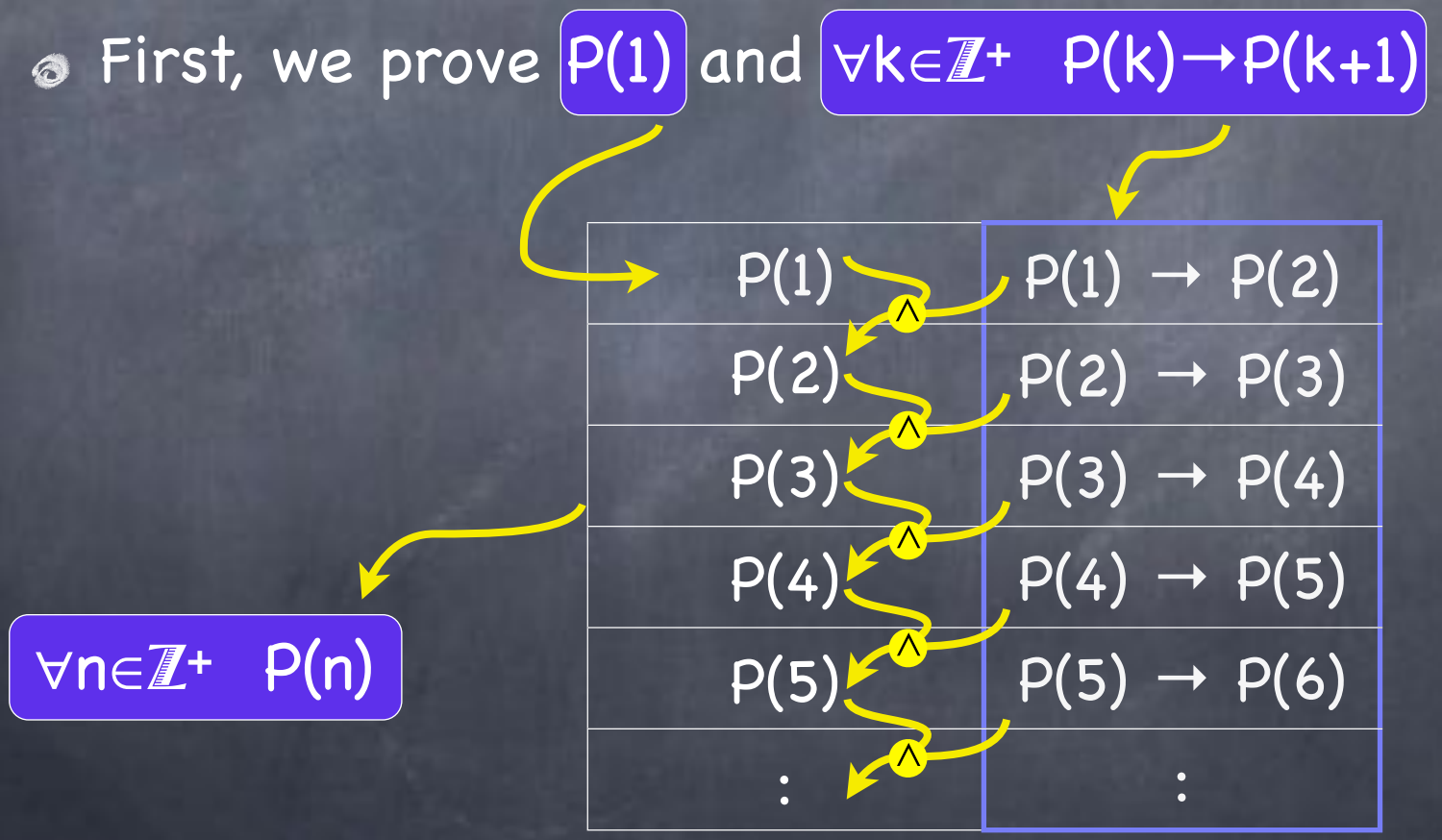
Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$



Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$

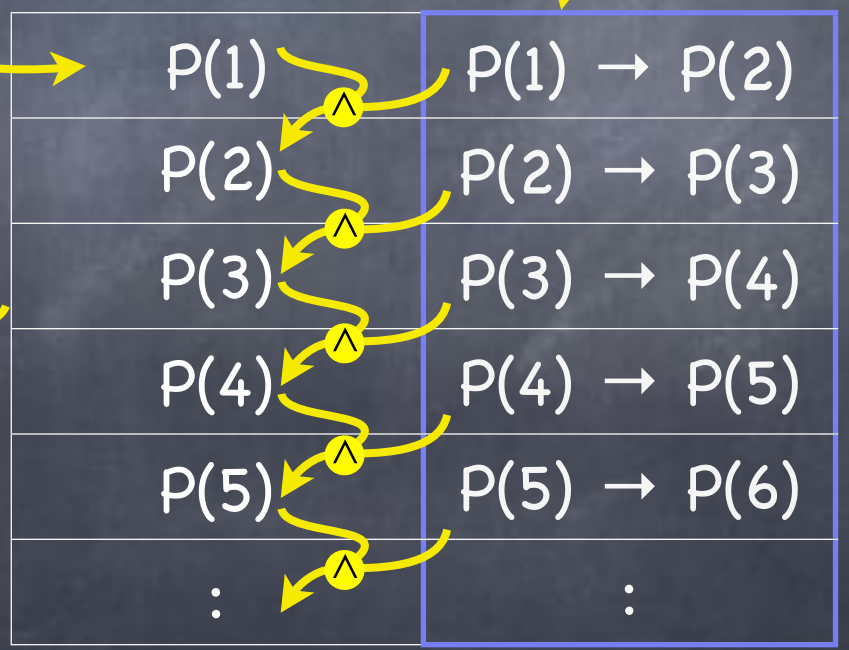


Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$

Mathematical Induction

The fact that for any n, we can run this procedure to generate a proof for P(n), and hence for any n, P(n) holds.



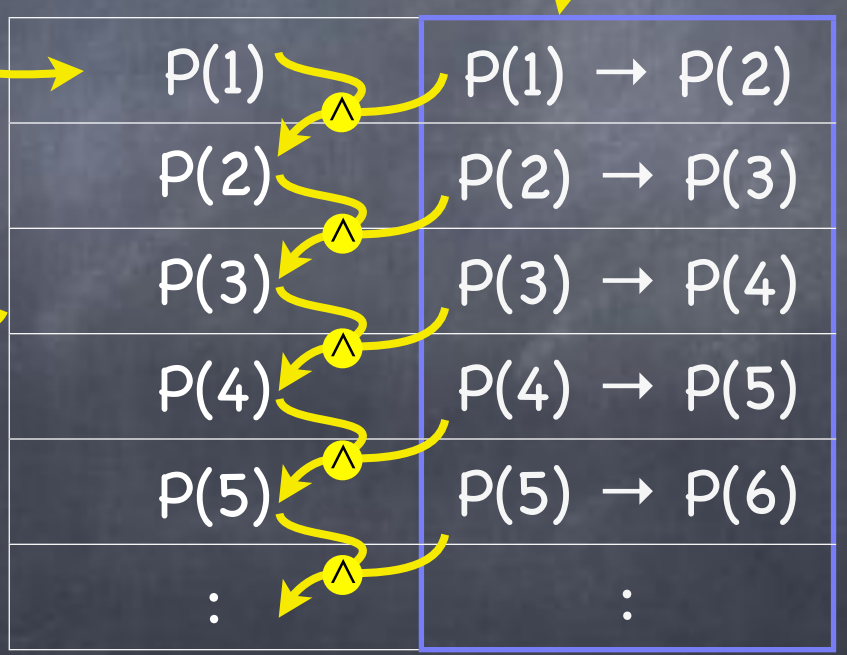
$\forall n \in \mathbb{Z}^+ \;\; P(n)$

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$

Weak Mathematical Induction

The fact that for any n, we can run this procedure to generate a proof for P(n), and hence for any n, P(n) holds.



$\forall n \in \mathbb{Z}^+ \;\; P(n)$

Completing the proof

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+$ P(n):

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$
  - Then by mathematical induction, $\forall n \in \mathbb{Z}^+ \;\; P(n)$

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$
  - Then by mathematical induction, $\forall n \in \mathbb{Z}^+ \;\; P(n)$
- Some other possibilities:

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$
  - Then by mathematical induction, $\forall n \in \mathbb{Z}^+ \; P(n)$
- Some other possibilities:
  - Suppose the ATM takes an $n bill and gives an $(n+2) bill

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$
  - Then by mathematical induction, $\forall n \in \mathbb{Z}^+ \; P(n)$
- Some other possibilities:
  - Suppose the ATM takes an $n bill and gives an $(n+2) bill
    - To get every possible bill, start with $1 and $2 bills

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)$
  - Then by mathematical induction, $\forall n \in \mathbb{Z}^+ \;\; P(n)$
- Some other possibilities:
  - Suppose the ATM takes an $n bill and gives an $(n+2) bill
    - To get every possible bill, start with $1 and $2 bills
  - Suppose the ATM doesn't take bills under $5

Completing the proof

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$
  - Then by mathematical induction, $\forall n \in \mathbb{Z}^+ \; P(n)$
- Some other possibilities:
  - Suppose the ATM takes an $n bill and gives an $(n+2) bill
    - To get every possible bill, start with $1 and $2 bills
  - Suppose the ATM doesn't take bills under $5
    - Print $1,…,$5 on your own. Use the ATM for the rest

Example

Example

- $\forall n \in \mathbb{Z}^+ \quad 3 \mid (2^{2n}-1)$

Example

- $\forall n \in \mathbb{Z}^+ \quad 3 \mid (2^{2n}-1)$
  - Base case: n=1. $2^{2 \cdot 1}-1 = 3$, so $3 \mid 2^{2 \cdot 1}-1$

Example

- $\forall n \in \mathbb{Z}^+ \;\; 3 \mid (2^{2n}-1)$
  - Base case: n=1. $2^{2 \cdot 1}-1 = 3$, so $3 \mid 2^{2 \cdot 1}-1$
  - Induction step: $\forall k \in \mathbb{Z}^+ \;\; \underline{3 \mid (2^{2k}-1)} \rightarrow \underline{3 \mid (2^{2(k+1)}-1)}$

Example

- $\forall n \in \mathbb{Z}^+ \;\; 3 \mid (2^{2n}-1)$
  - Base case: n=1. $2^{2 \cdot 1}-1 = 3$, so $3 \mid 2^{2 \cdot 1}-1$
  - Induction step: $\forall k \in \mathbb{Z}^+ \;\; \underline{3 \mid (2^{2k}-1)} \rightarrow \underline{3 \mid (2^{2(k+1)}-1)}$
    - $2^{2(k+1)}-1 = 4.2^{2k}-1 = 4(2^{2k}-1) + 3$
      By induction hypothesis, $3 \mid 4(2^{2k}-1)$.
      Hence, $3 \mid (2^{2(k+1)}-1)$.

Example

- $\forall n \in \mathbb{Z}^+ \;\; 3 \mid (2^{2n}-1)$
  - Base case: n=1. $2^{2 \cdot 1}-1 = 3$, so $3 \mid 2^{2 \cdot 1}-1$
  - Induction step: $\forall k \in \mathbb{Z}^+ \;\; \underline{3 \mid (2^{2k}-1)} \rightarrow \underline{3 \mid (2^{2(k+1)}-1)}$
    - $2^{2(k+1)}-1 = 4.2^{2k}-1 = 4(2^{2k}-1) + 3$
      By induction hypothesis, $3 \mid 4(2^{2k}-1)$.
      Hence, $3 \mid (2^{2(k+1)}-1)$.
  - Hence (by weak induction), $\forall n \in \mathbb{Z}^+ \;\; 3 \mid (2^{2n}-1)$