Mathematical Induction

Part Two

Let P be some property. The ***principle of mathematical induction*** states that if

P is true for 0

If it starts true…

and

…and it stays true…

For any $k \in \mathbb{N}$, if P is true for k, then P is true for $k + 1$

then

P is true for every $n \in \mathbb{N}$.

…then it's always true.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero powers of two is $2^0 - 1$. Since the sum of the first zero powers of two is zero and $2^0 - 1$ is zero as well, we see that $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k - 1. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is $2^{k+1} - 1$. To see this, notice that

$$\begin{aligned} 2^0 + 2^1 + \ldots + 2^{k-1} + 2^k &= (2^0 + 2^1 + \ldots + 2^{k-1}) + 2^k \\ &= 2^k - 1 + 2^k \qquad \textit{(via (1))} \\ &= 2(2^k) - 1 \\ &= 2^{k+1} - 1. \end{aligned}$$

Therefore, $P(k + 1)$ is true, completing the induction. ■

Induction in Practice

- Typically, a proof by induction will not explicitly state $P(n)$.
- Rather, the proof will describe $P(n)$ implicitly and leave it to the reader to fill in the details.
- Provided that there is sufficient detail to determine
  - what $P(n)$ is;
  - that $P(0)$ is true; and that
  - whenever $P(k)$ is true, $P(k+1)$ is true,

  the proof is usually valid.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: By induction.

For our base case, we'll prove the theorem is true when $n = 0$. The sum of the first zero powers of two is zero, and $2^0 - 1 = 0$, so the theorem is true in this case.

For the inductive step, assume the theorem holds when $n = k$ for some arbitrary $k \in \mathbb{N}$. Then

$$\begin{aligned} 2^0 + 2^1 + \ldots + 2^{k-1} + 2^k &= (2^0 + 2^1 + \ldots + 2^{k-1}) + 2^k \\ &= 2^k - 1 + 2^k \\ &= 2(2^k) - 1 \\ &= 2^{k+1} - 1. \end{aligned}$$

So the theorem is true when $n = k+1$, completing the induction. ■

Variations on Induction: **Starting Later**

Induction Starting at 0

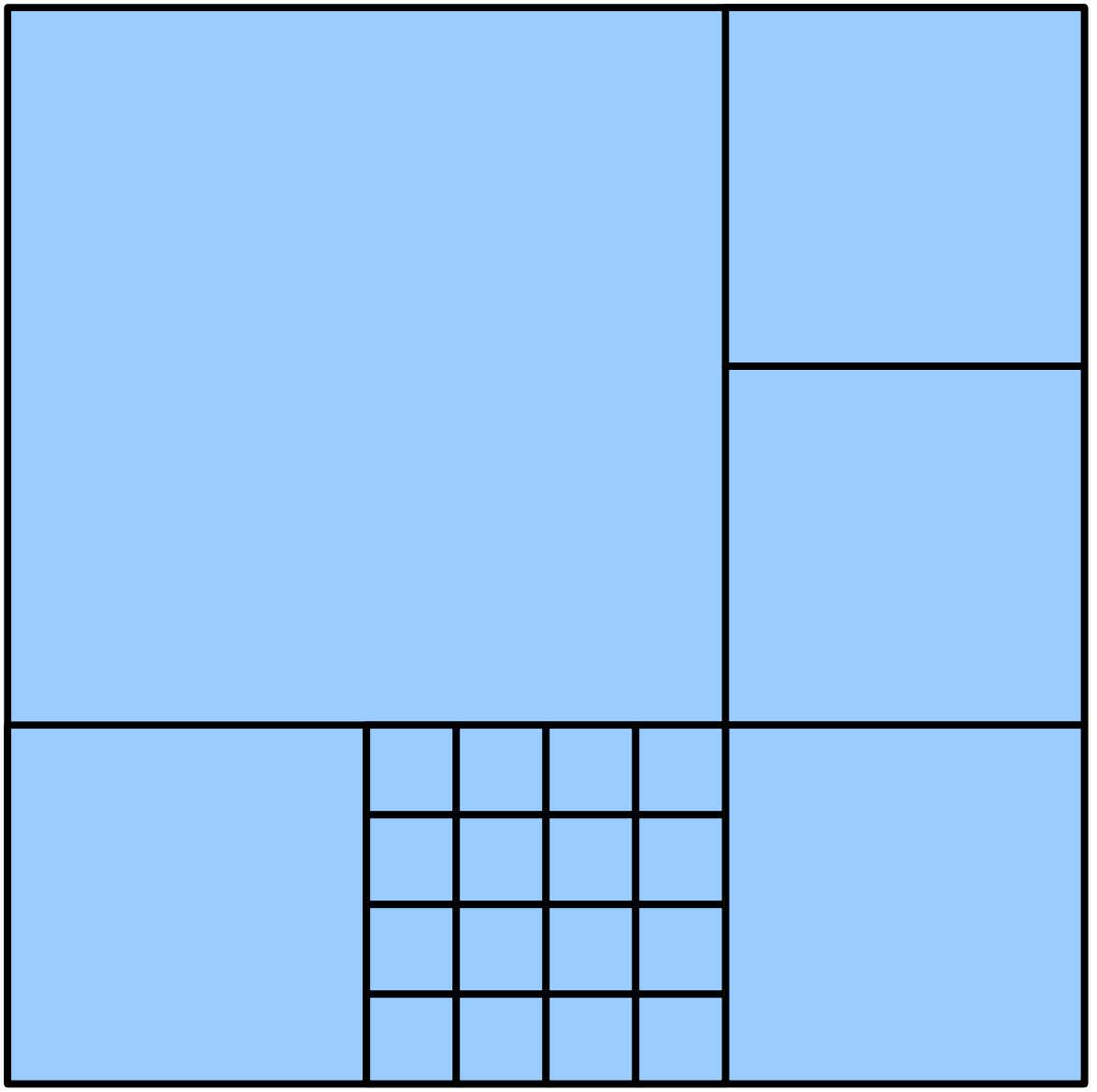
- To prove that $P(n)$ is true for all natural numbers greater than or equal to 0:
  - Show that $P(0)$ is true.
  - Show that for any $k \geq 0$, that if $P(k)$ is true, then $P(k+1)$ is true.
  - Conclude $P(n)$ holds for all natural numbers greater than or equal to 0.

Induction Starting at ***m***

- To prove that $P(n)$ is true for all natural numbers greater than or equal to ***m***:
  - Show that $P($***m***$)$ is true.
  - Show that for any $k \geq$ ***m***, that if $P(k)$ is true, then $P(k+1)$ is true.
  - Conclude $P(n)$ holds for all natural numbers greater than or equal to ***m***.

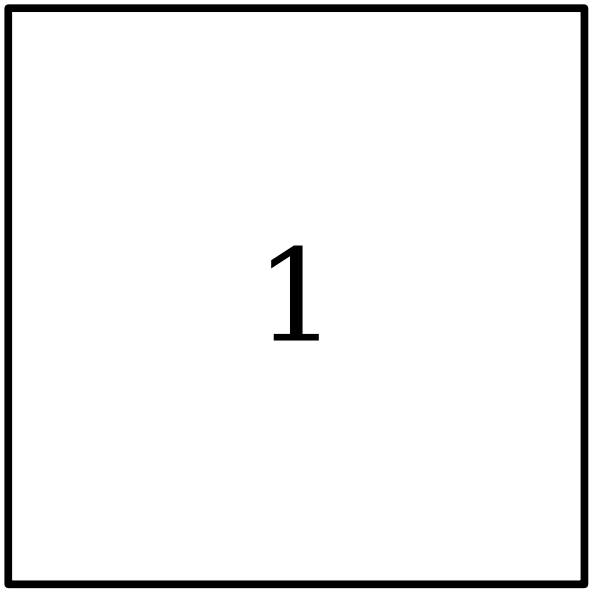
Variations on Induction: **Bigger Steps**

Subdividing a Square

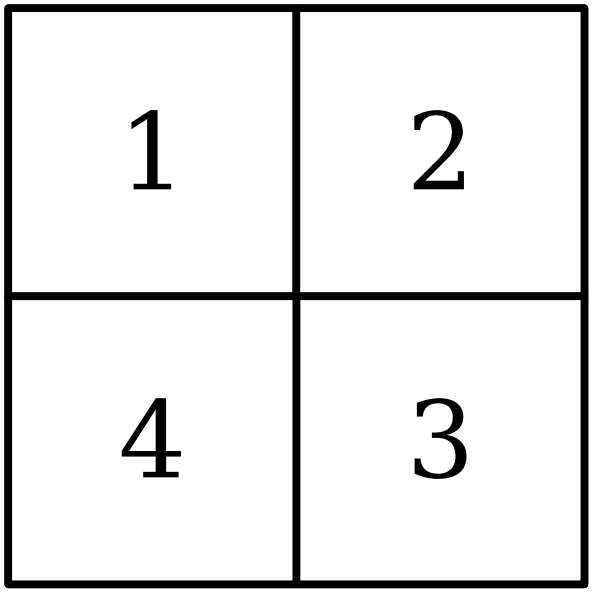


For what values of n can a square be subdivided into n squares?

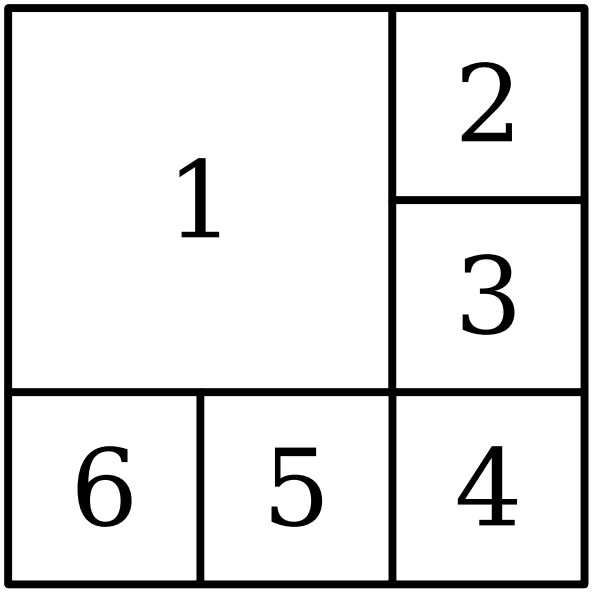
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



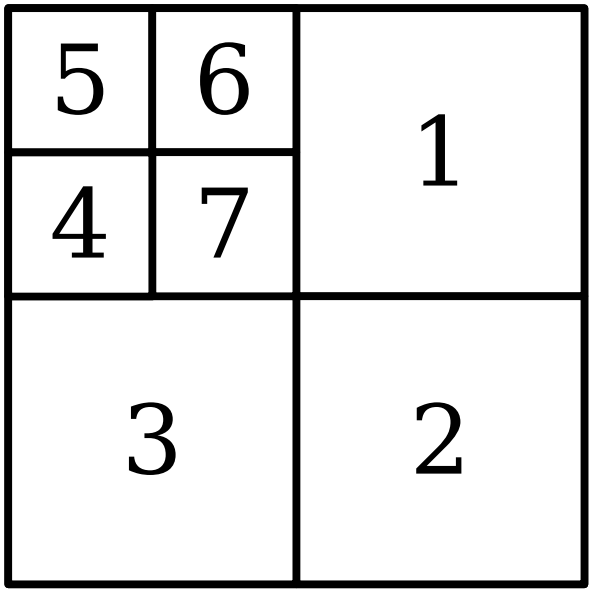
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



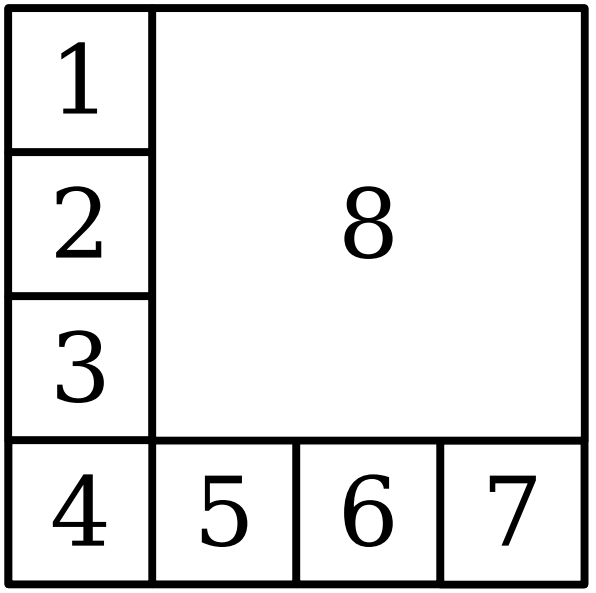
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



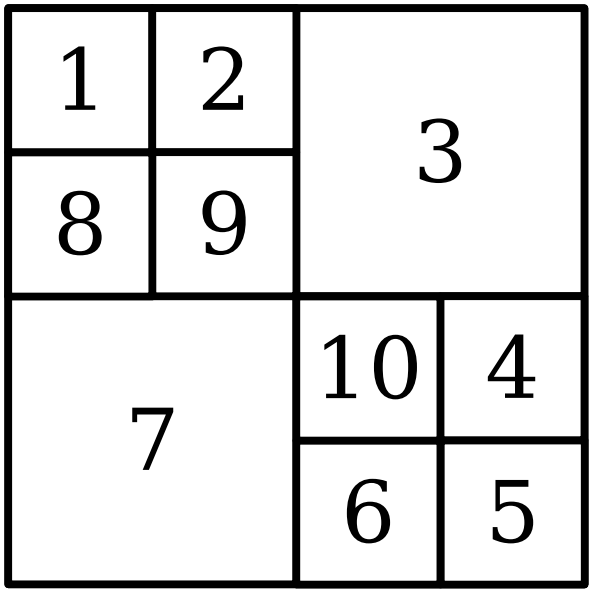
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



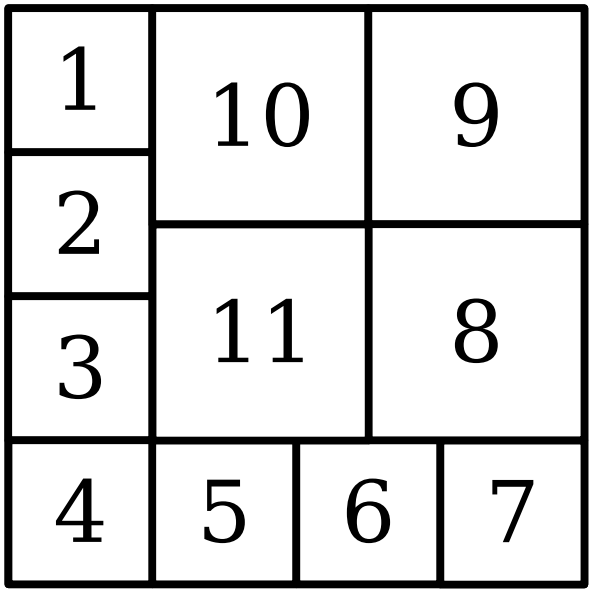
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12

1	2	3
8	9	4
7	6	5

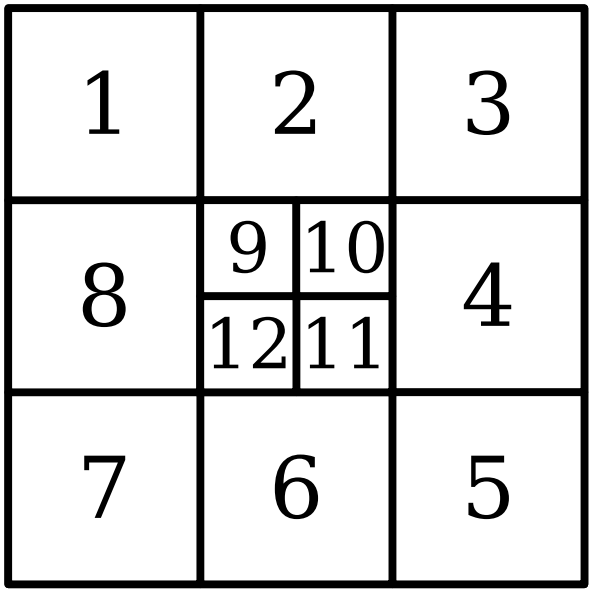
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



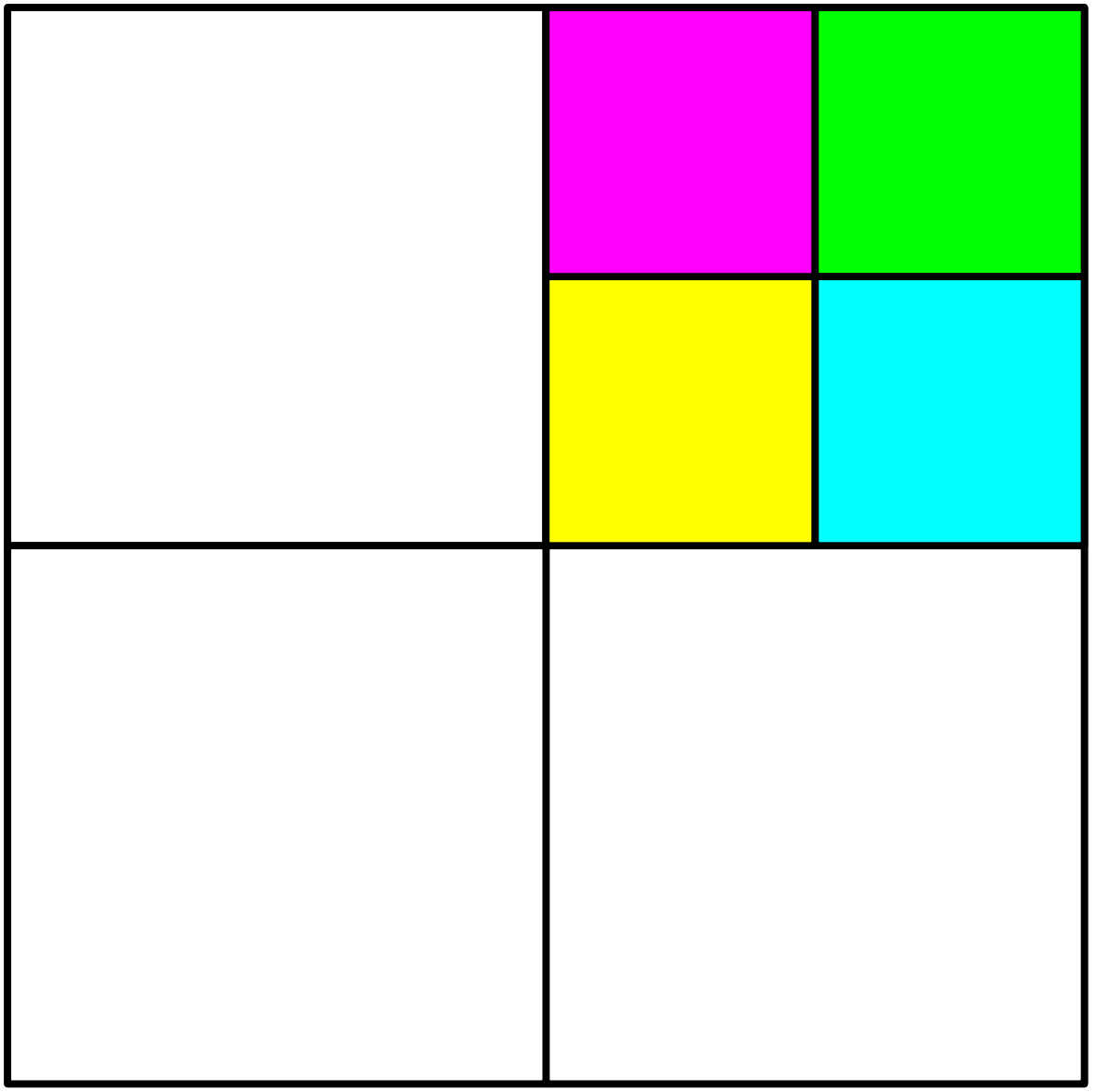
1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



1 ~~2~~ ~~3~~ 4 ~~5~~ 6 7 8 9 10 11 12



The Key Insight



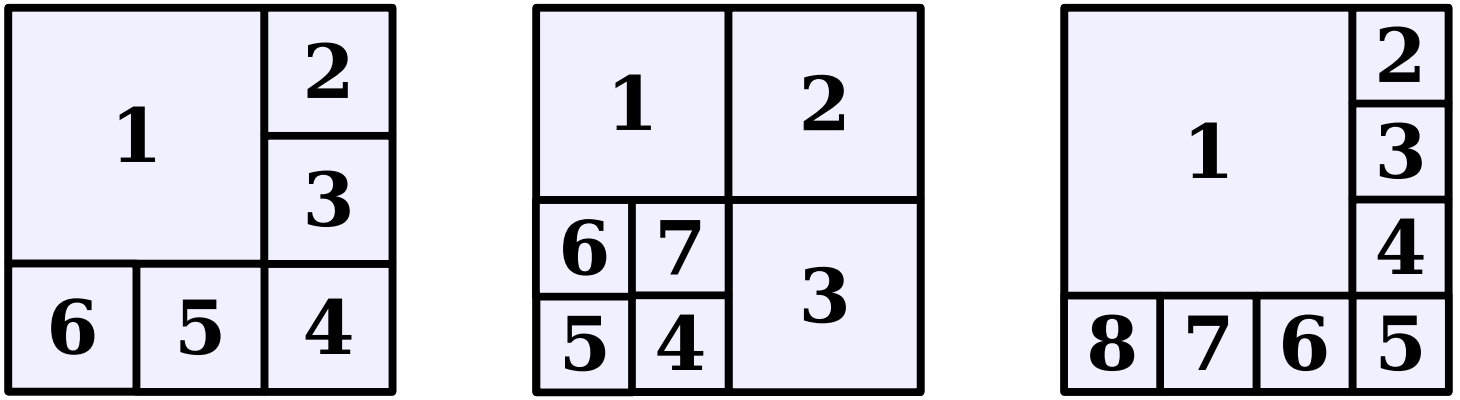
The Key Insight

- If we can subdivide a square into n squares, we can also subdivide it into $n + 3$ squares.
- Since we can subdivide a bigger square into 6, 7, and 8 squares, we can subdivide a square into n squares for any $n \geq 6$:
  - For multiples of three, start with 6 and keep adding three squares until n is reached.
  - For numbers congruent to one modulo three, start with 7 and keep adding three squares until n is reached.
  - For numbers congruent to two modulo three, start with 8 and keep adding three squares until n is reached.

Theorem: For any $n \geq 6$, it is possible to subdivide a square into n smaller squares.

Proof: Let $P(n)$ be the statement "a square can be subdivided into n smaller squares." We will prove by induction that $P(n)$ holds for all $n \geq 6$, from which the theorem follows.

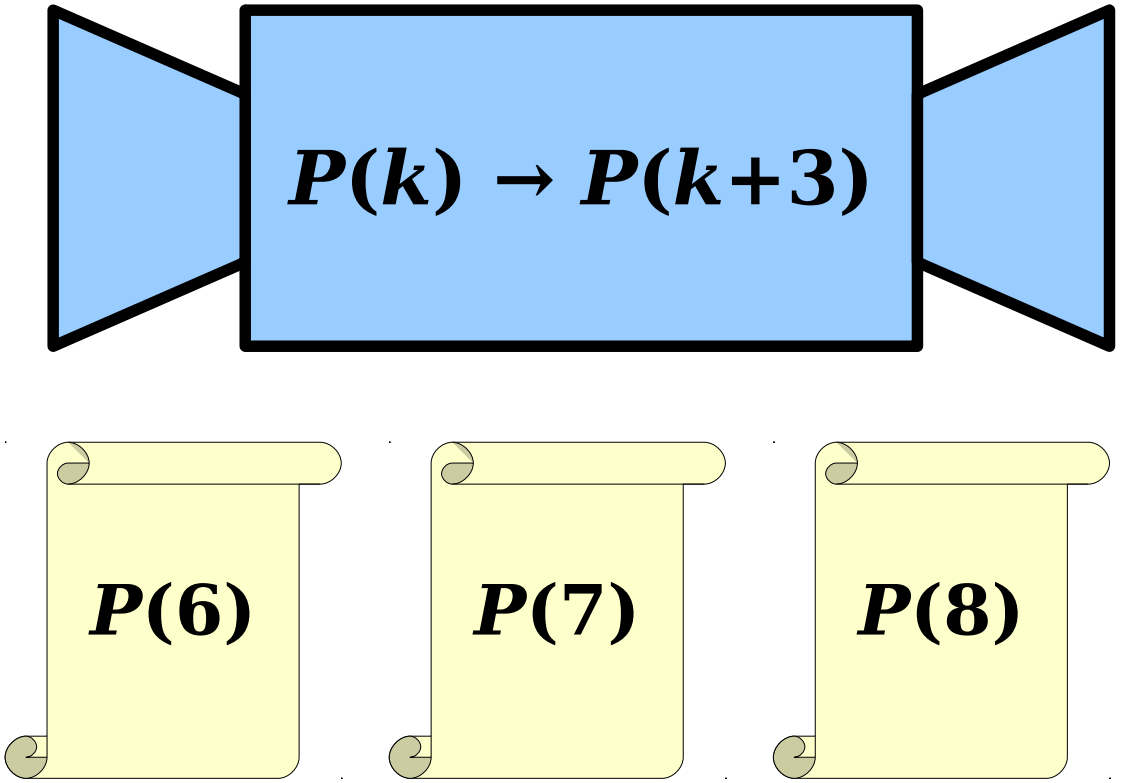
As our base cases, we prove $P(6)$, $P(7)$, and $P(8)$, that a square can be subdivided into 6, 7, and 8 squares. This is shown here:



For the inductive step, assume that for some $k \geq 6$ that $P(k)$ is true and a square can be subdivided into k squares. We prove $P(k+3)$, that a square can be subdivided into $k+3$ squares. To see this, start by obtaining (via the inductive hypothesis) a subdivision of a square into k squares. Then, choose any of the squares and split it into four equal squares. This removes one of the k squares and adds four more, so there will be a net total of $k+3$ squares. Thus $P(k+3)$ holds, completing the induction. ■

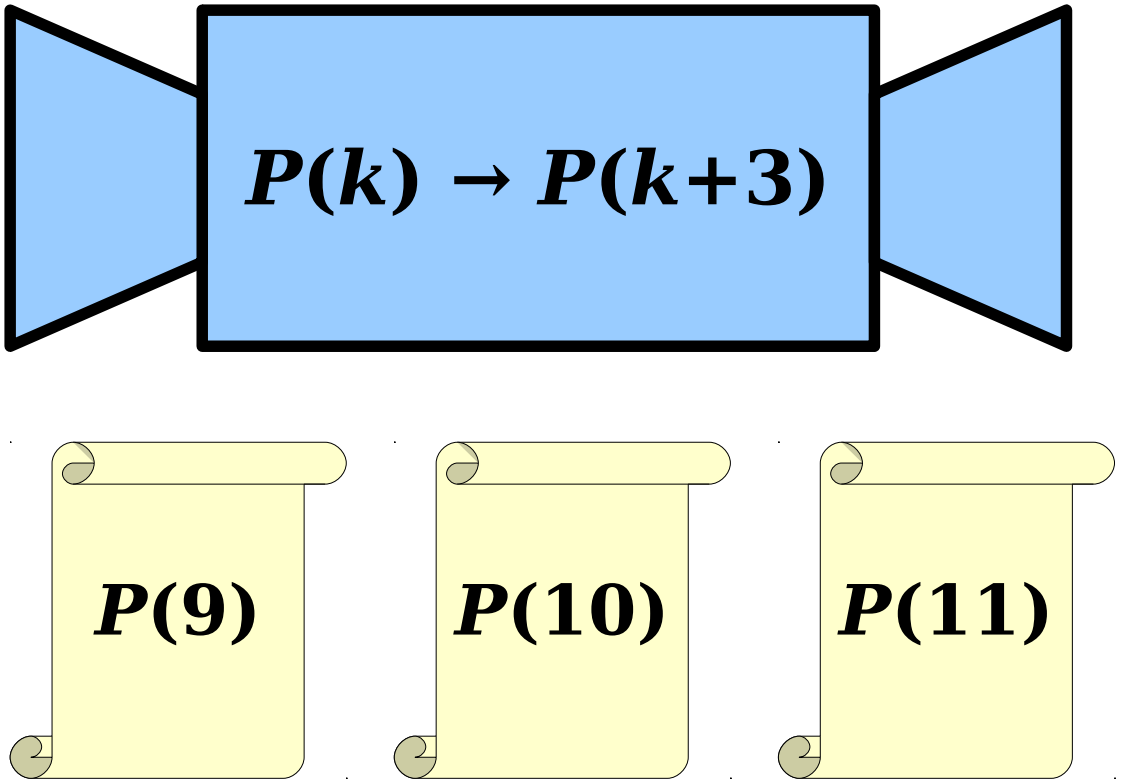
Why This Works

- This induction has three consecutive base cases and takes steps of size three.
- Thinking back to our “induction machine” analogy:



Why This Works

- This induction has three consecutive base cases and takes steps of size three.
- Thinking back to our “induction machine” analogy:



Generalizing Induction

- When doing a proof by induction:
  - Feel free to use multiple base cases.
  - Feel free to take steps of sizes other than one.
- Just be careful to make sure you cover all the numbers you think that you're covering!

Time-Out for Announcements!

Problem Set One

- Problem Set 1 due Friday, April 10 at the start of class.
  - Stop by office hours with questions!
  - Ask questions on Piazza!
  - Email the staff list (cs103-spr1415-staff@lists.stanford.edu) with questions!

Checkpoint Problems

- Problem Set 1 Checkpoints graded; feedback available online at Scoryst.
  - Please review this feedback before submitting the rest of the problems – the point of the checkpoint is to get useful feedback!
- When submitting the rest of Problem Set One, be sure to submit in the right category. You don't need to include the checkpoint question in your submission.
  - A note – a small number of you (single digits) submitted the entire problem set along with the checkpoint. Make sure you explicitly resubmit the later problems as your PS1 submission, since otherwise it won't get graded!

Your Questions

"To what extent is there still 'stuff to be discovered' in the field of mathematical foundations of computing/computer theory? What are some examples of research in these areas or problems students can think about?"

There is ***definitely*** a lot left to be discovered! Here are some questions we don't know the answers to:

1. What's the fastest algorithm to align two DNA strands?
2. Exactly how much computing power is required to compute optimal delivery routes?
3. Are the cryptographic systems we use online secure?

"If a proof is possible by one method (direct, contradiction, etc.), is it necessarily possible by another method?"

Not necessarily!

Certain results can only be proved indirectly; in fact, we can prove that you can't prove them otherwise!

Some proofs are called **nonconstructive proofs** and argue that something must exist without saying what it is. Some nonconstructive proofs **cannot** be converted into constructive proofs!

“What are some of your all-time favorite books? Or better yet, what are some books that you read as a college student and were significantly formative and influential?”

My favorite novel is *Slaughterhouse Five* by Kurt Vonnegut. For nonfiction, I strongly recommend “Guns, Germs, and Steel” by Jared Diamond and “Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety” by Eric Schlosser. If you want a good longform read, do a Google search for “Scott and Scurvey.”

“Is there a larger classroom for lecture at this time? There are still around 20 students sitting on the floor in the 2nd week.”

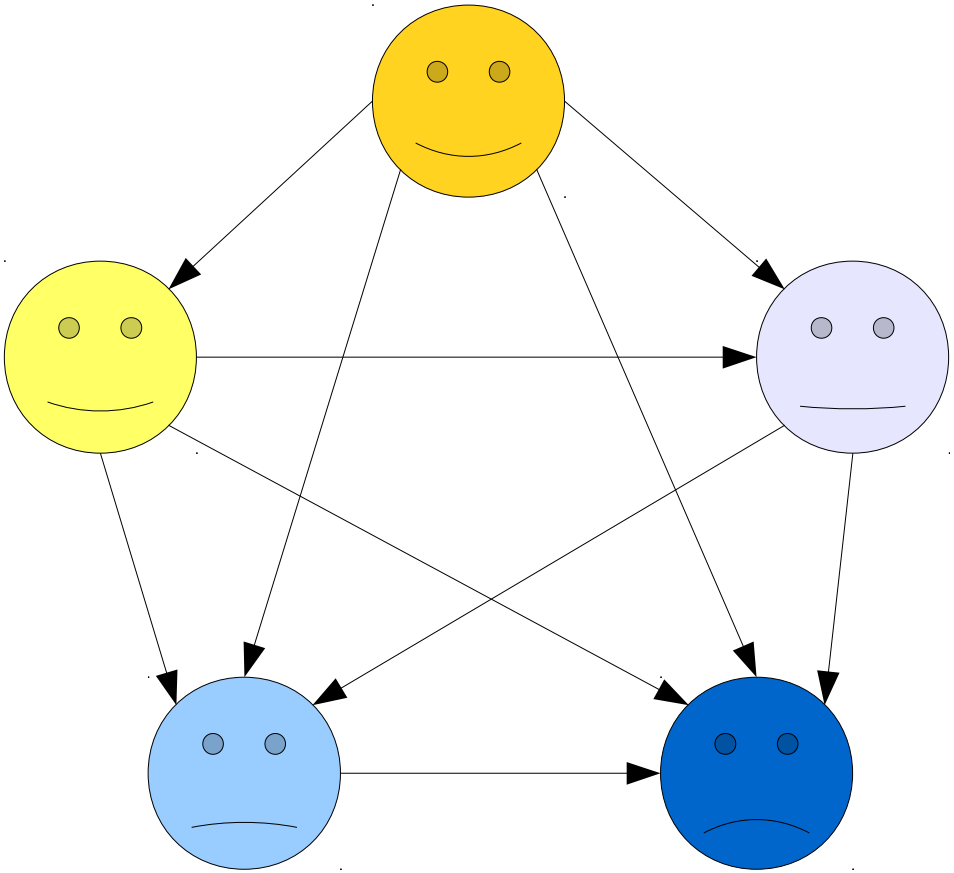
Working on it. ☺

Back to CS103!

Example: ***Tournaments***

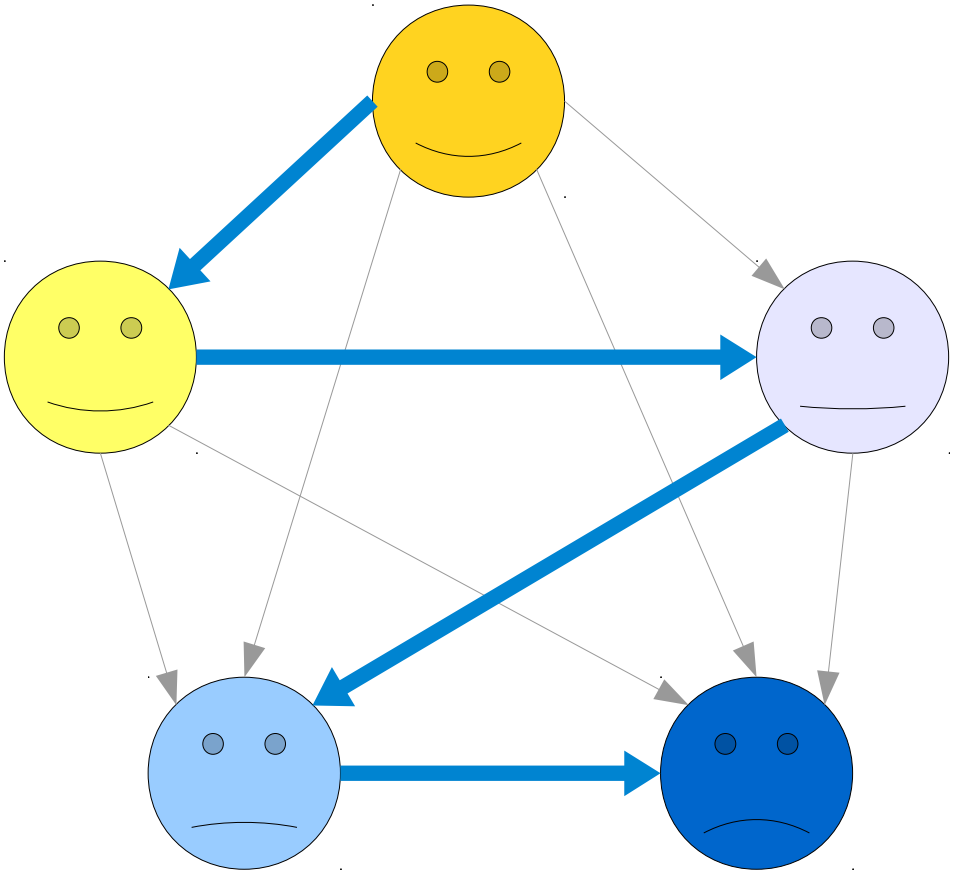
Tournaments

- A ***tournament*** is a contest for $n \geq 0$ people.
- Each person plays exactly one game against each other person, and there are no ties.
- The result can be visualized in a picture like this one, which is called a ***tournament graph***.



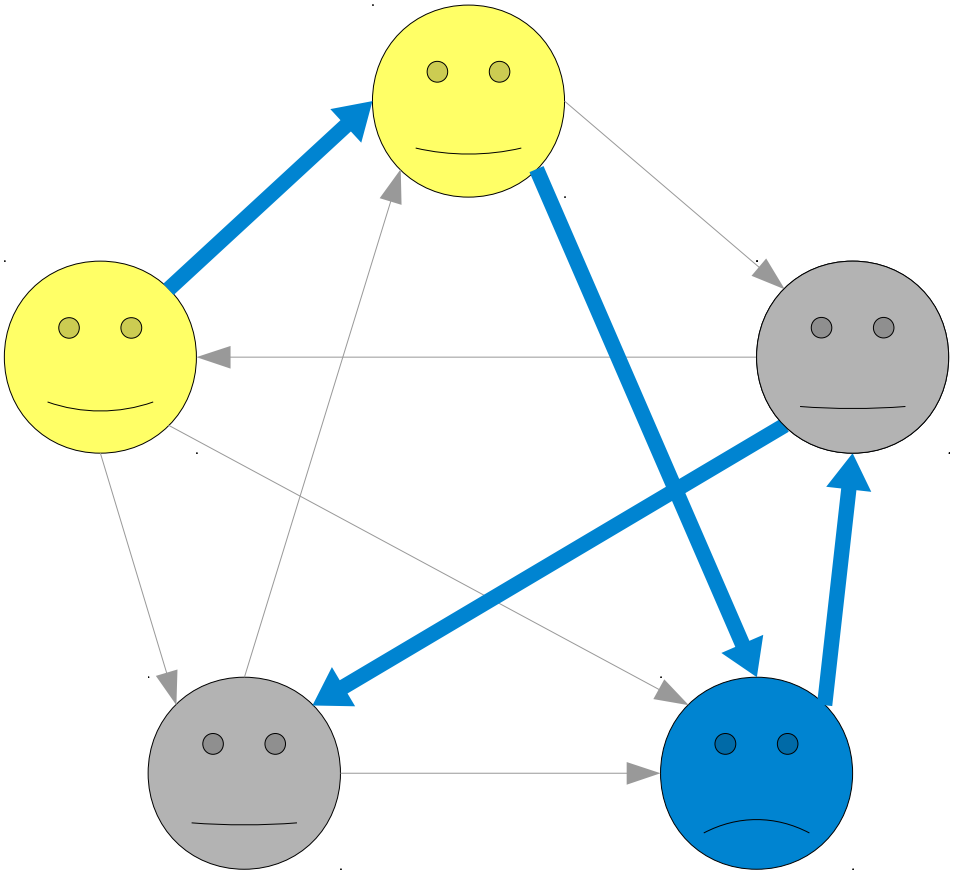
Victory Chains

- A ***victory chain*** in a tournament is a way of lining up the players so that every player beat the player that comes after them.



Victory Chains

- A ***victory chain*** in a tournament is a way of lining up the players so that every player beat the player that comes after them.



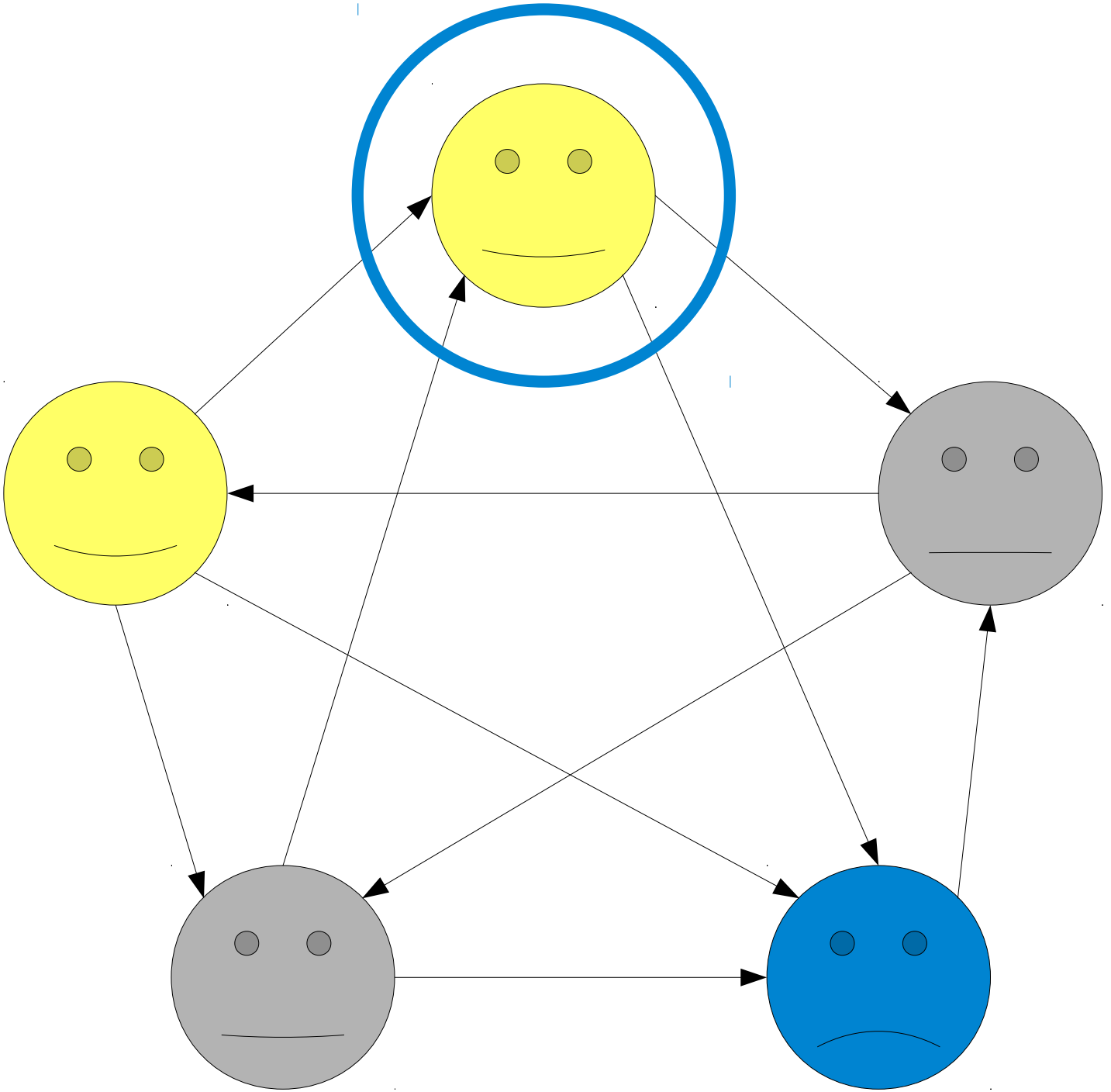
Theorem: Every tournament, regardless of the outcome, has a victory chain.

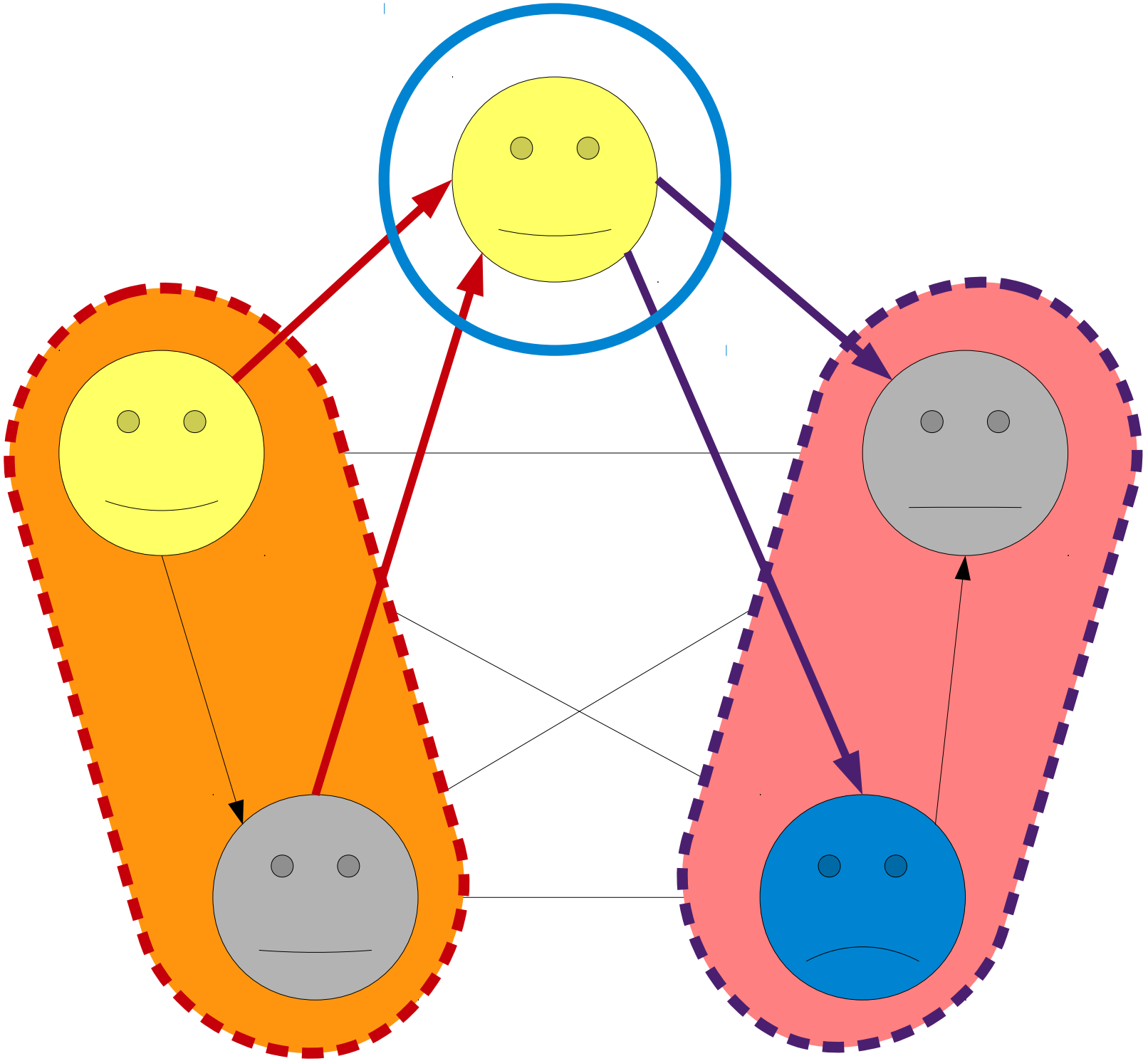
Thinking Inductively

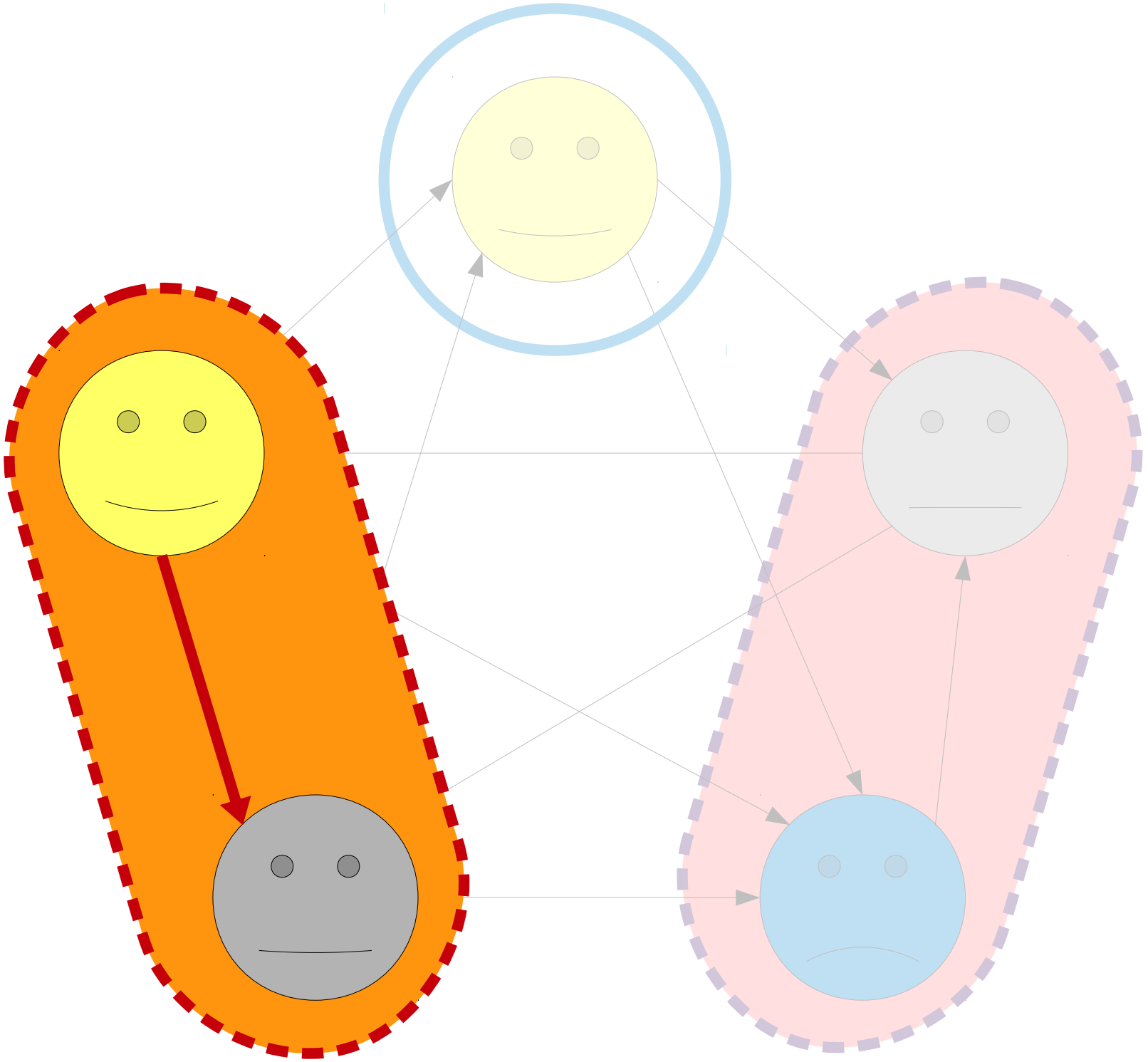
- The inductive step in an inductive proof uses the fact that the result is true for a smaller number (k) to prove that the result is true for a larger number ($k+1$).
- In most inductive proofs, the proof that the result is true for $k+1$ explicitly tries to simplify the $k+1$ case into the k case.
  - Counterfeit coins: Turn $k+1$ weighings into k weighings.
  - `MU` puzzle: Turn a sequence of $k+1$ events into a sequence of k events.
  - Square subdivision: Use a subdivision into k to get one for $k+3$.

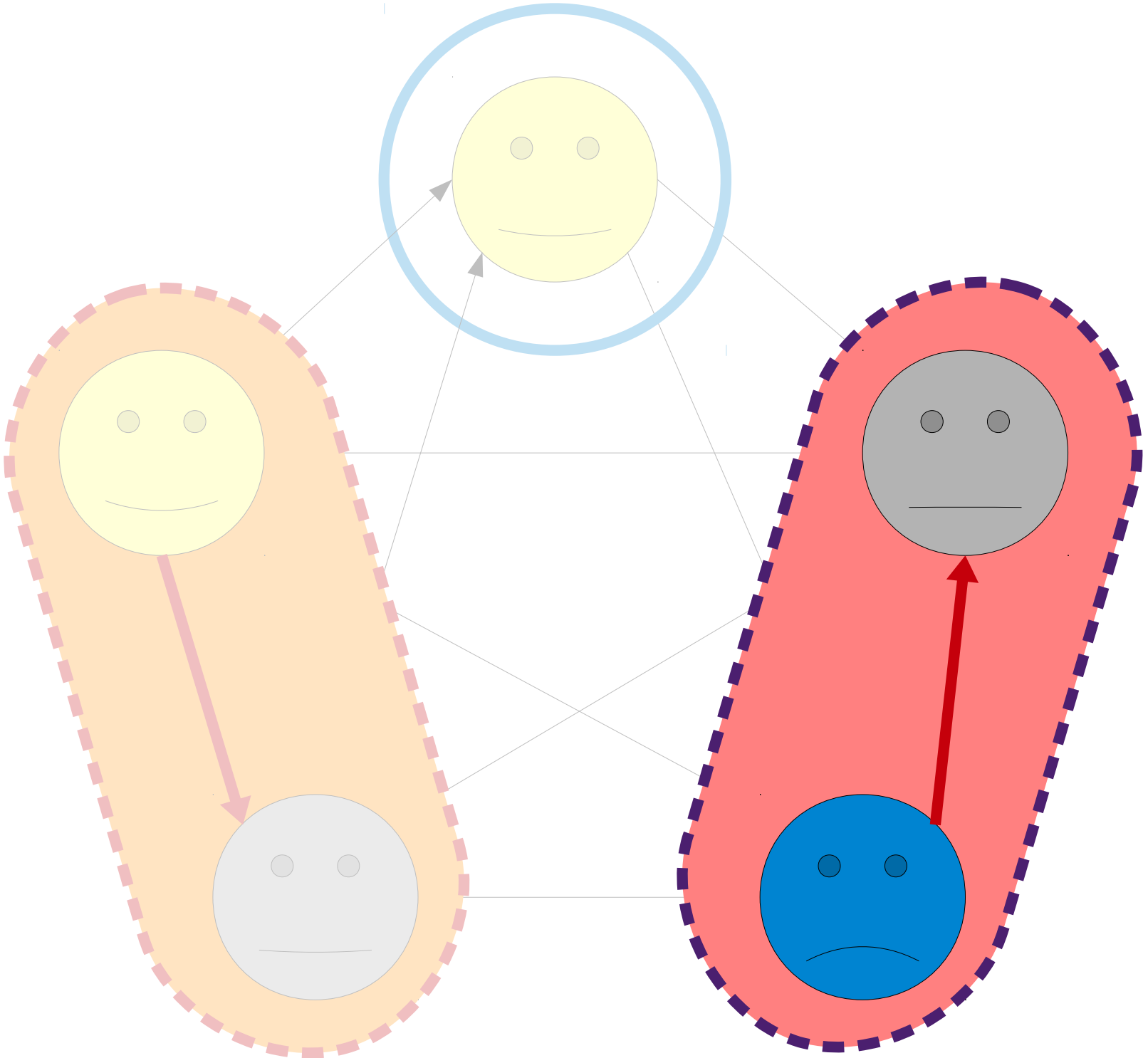
Thinking Inductively

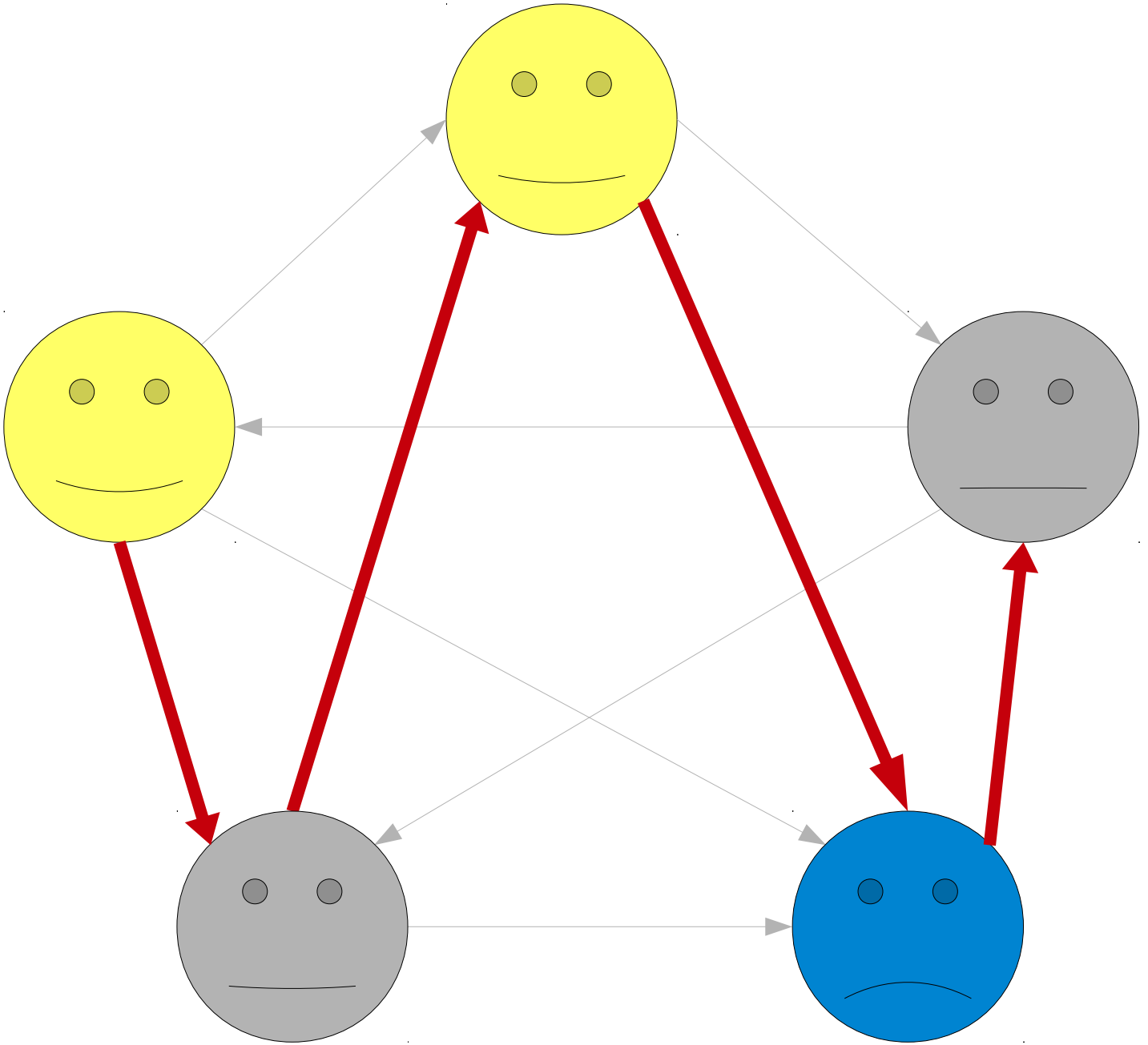
- For our victory chain proof, we will simplify the problem by turning the larger tournament into two smaller tournaments.
- We'll inductively argue that, since those smaller tournaments each have victory chains, the larger tournament must have a victory chain.



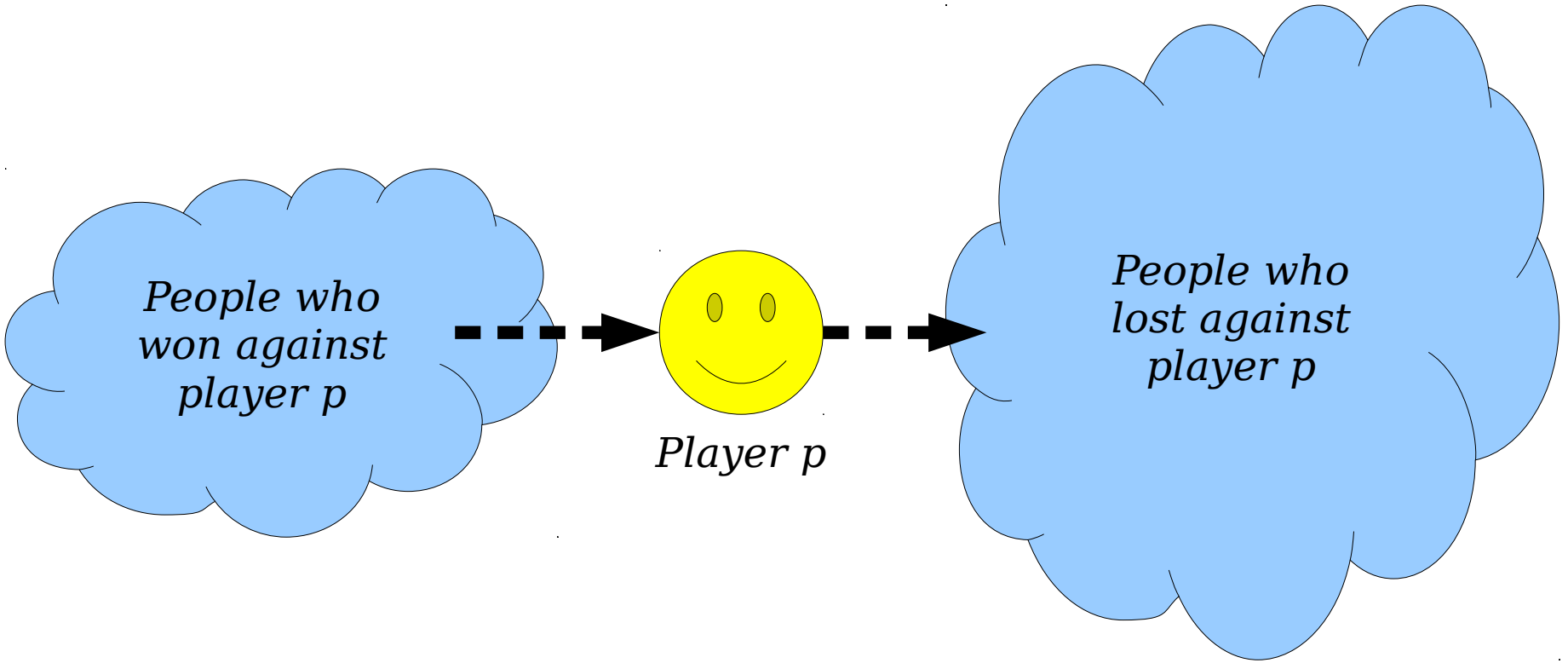








The Proof, Schematically



The Idea

- Suppose that every tournament with at most k players has a victory chain.
- Take a tournament T with $k+1$ players.
- Choose any one player p.
- Form the subtournaments T_0 and T_1 of all players who beat p and lost to p, respectively.
- Get victory chains from T_0 and T_1.
- Splice those chains together through p.

The Idea

Suppose that every tou
k players has a victory

Take a tournament T w

Choose any one player p.

This is the key idea behind an inductive proof – we're reducing the problem to smaller copies of itself.

- Form the subtournaments T_0 and T_1 of all players who beat p and lost to p, respectively.
- Get victory chains from T_0 and T_1.

Splice those chains together through p.

Writing the Proof: A First Attempt

We're going to run into trouble in the middle of this proof. Don't worry – we'll see how to fix it.

Theorem: Every

Proof: Let $P(n)$ l ayers has a victory chai true for all $n \in \mathbb{N}$, from

As a base ca no players has a victory t of all 0 of the players er beat the next player i

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ is true. In other words, we assume that any tournament with k players has a victory chain. We'll prove $P(k+1)$, that any tournament with $k+1$ players has a victory chain.

Consider any tournament T with $k+1$ players. Choose any one player p and form two subtournaments, a subtournament T_0 of all the players who beat p and a subtournament T_1 of all the players who lost to p. Both of these tournaments have between 0 and k players.

At this point, we're stuck. We know that tournaments with *exactly* k players must have a victory chain, but we're not assuming anything about tournaments with 0, 1, 2, …, $k-1$ players. Therefore, we can't necessarily say anything about these subtournaments.

Theorem: Every tournament has a victory chain.

Proof: Let $P(n)$ be the statement "every tournament with n players has a victory chain." We will prove by induction that $P(n)$ is true for all $n \in \mathbb{N}$, from

What if we made some additional assumptions so that we *can* say something about these smaller tournaments?

As a base ca no players has a victory t of all 0 of the players vacuously satisfies the claim that every player beat the next player in the list. Therefore, $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ is true. In other words, we assume that any tournament with k players has a victory chain. We'll prove $P(k+1)$, that any tournament with $k+1$ players has a victory chain.

Consider any tournament T with $k+1$ players. Choose any one player p and form two subtournaments, a subtournament T_0 of all the players who beat p and a subtournament T_1 of all the players who lost to p. Both of these tournaments have between 0 and k players.

Theorem: Every tournament has a victory chain.

Proof: Let $P(n)$ be the statement "every tournament with n players has a victory chain." We will prove by induction that $P(n)$ is true for all $n \in \mathbb{N}$, from v

We're now assuming that the result is true for 0, 1, 2, 3, …, k. Now, we can continue to make progress!

As a base ca no players has a victory of all 0 of the players vacuously satisfies the claim that every player beat the next player in the list. Therefore, $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(0)$, $P(1)$, $P(2)$, …, and $P(k)$ are all true. In other words, we assume that any tournament with at most k players has a victory chain. We'll prove $P(k+1)$, that any tournament with $k+1$ players has a victory chain.

Consider any tournament T with $k+1$ players. Choose any one player p and form two subtournaments, a subtournament T_0 of all the players who beat p and a subtournament T_1 of all the players who lost to p. Both of these tournaments have between 0 and k players.

Theorem: Every tournament has a victory chain.

Proof: Let $P(n)$ be the statement "every tournament with n players has a victory chain." We will prove by induction that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

As a base case, we prove $P(0)$, that any tournament with no players has a victory chain. In a tournament with no players, a list of all 0 of the players vacuously satisfies the claim that every player beat the next player in the list. Therefore, $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(0)$, $P(1)$, $P(2)$, ..., and $P(k)$ are all true. In other words, we assume that any tournament with at most k players has a victory chain. We'll prove $P(k+1)$, that any tournament with $k+1$ players has a victory chain.

Consider any tournament T with $k+1$ players. Choose any one player p and form two subtournaments, a subtournament T_0 of all the players who beat p and a subtournament T_1 of all the players who lost to p. Both of these tournaments have between 0 and k players. Therefore, by our inductive hypothesis, these two subtournaments have victory chains, call them V_0 and V_1. If we then splice together these chains to form the chain V_0, p, V_1, then we have a victory chain for T: every player is present, and every player beat the player immediately after them. Therefore, this arbitrary tournament of $k+1$ players has a victory chain, so $P(k+1)$ is true, completing the induction. ■

What We Just Did

- In a normal inductive step, we assume that $P(k)$ is true and prove $P(k+1)$.
- In this type of inductive step, we assume $P(0)$, $P(1)$, …, and $P(k)$ are true before we prove $P(k+1)$.
- That way, when we found *any* kind of smaller tournament, we knew something about its structure.
- This type of proof has a name!

Complete Induction

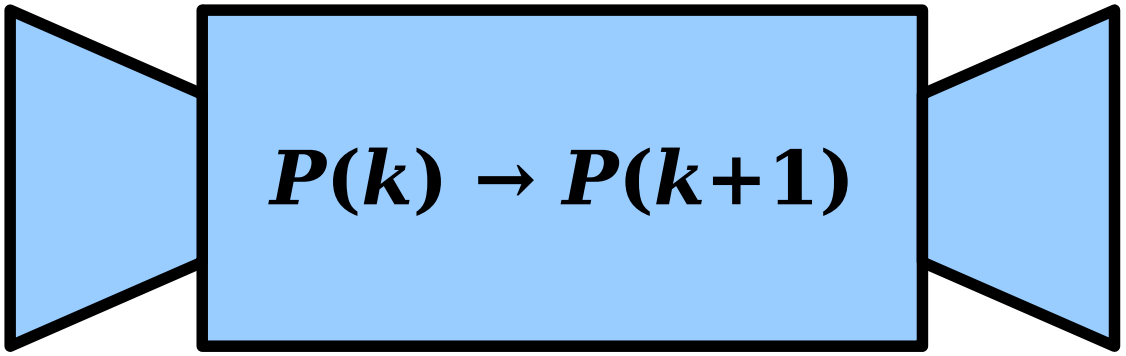
- If the following are true:
  - $P(0)$ is true, and
  - If $P(0)$, $P(1)$, $P(2)$, …, $P(k)$ are true, then $P(k+1)$ is true as well.

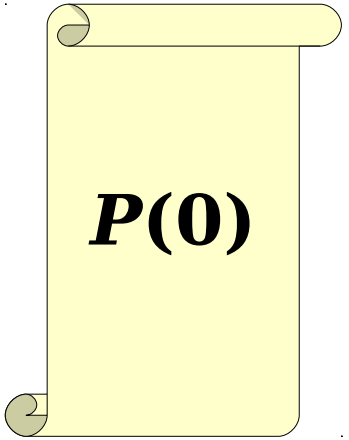
  then $P(n)$ is true for all $n \in \mathbb{N}$.
- This is called the ***principle of complete induction*** or the ***principle of strong induction***.
  - (A note: this also works starting from a number other than 0; just modify what you're assuming appropriately.)

That's a *lot* of assumptions to make!

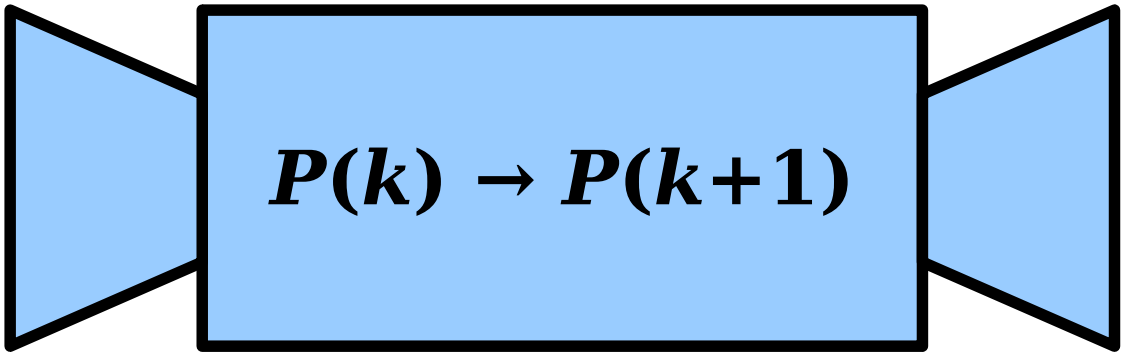
Why is this legal?

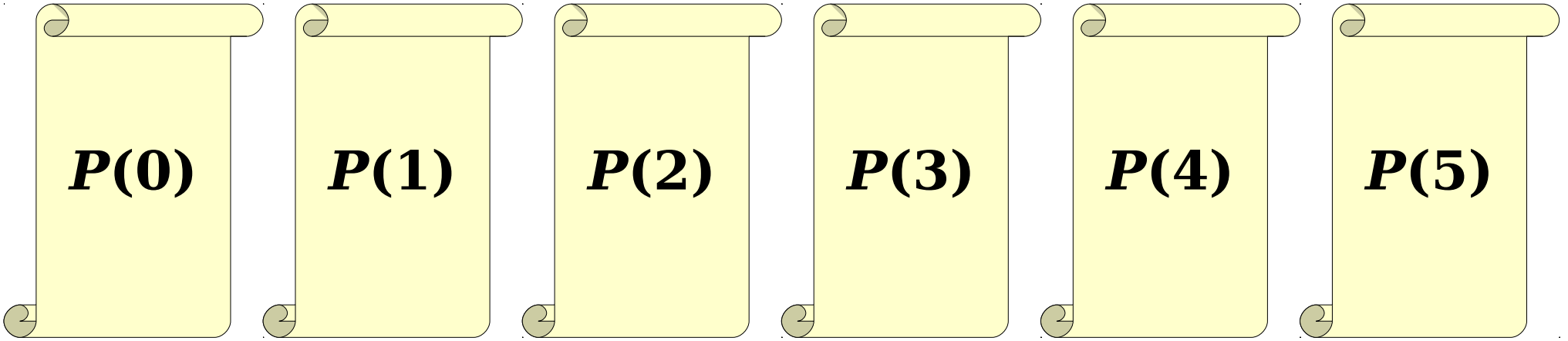
Review: Induction as a Machine



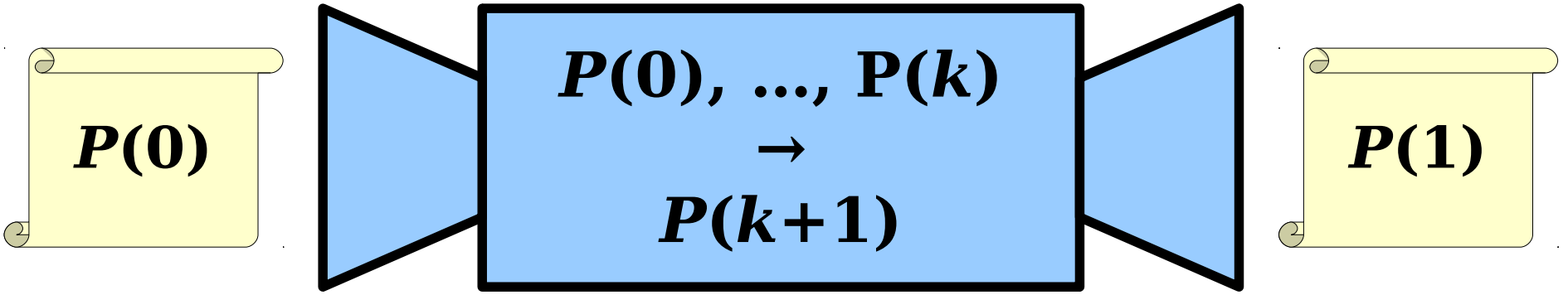


An Observation

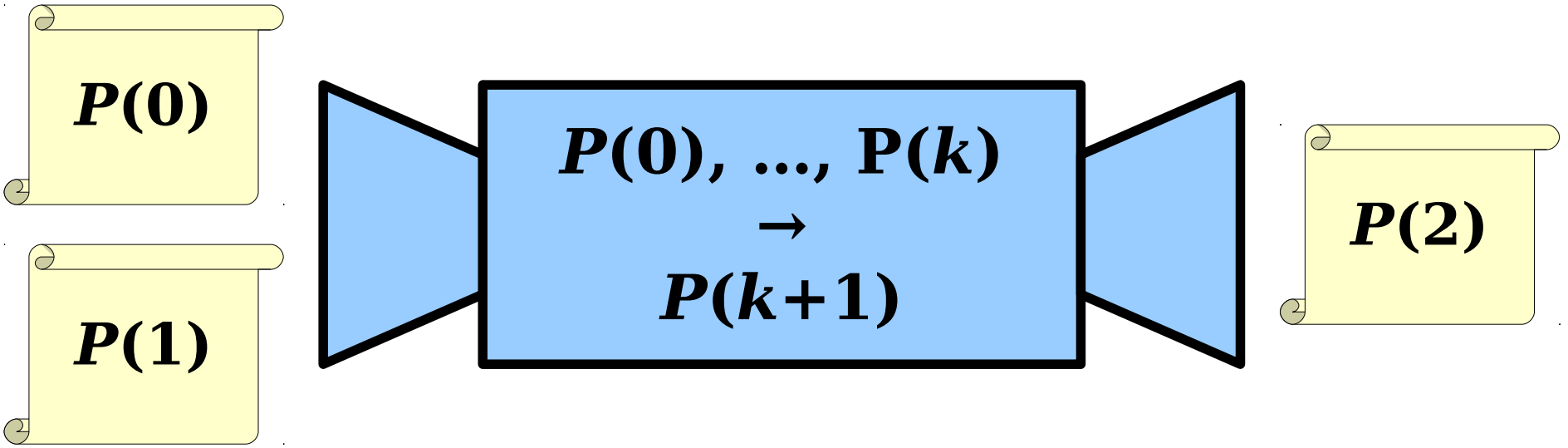




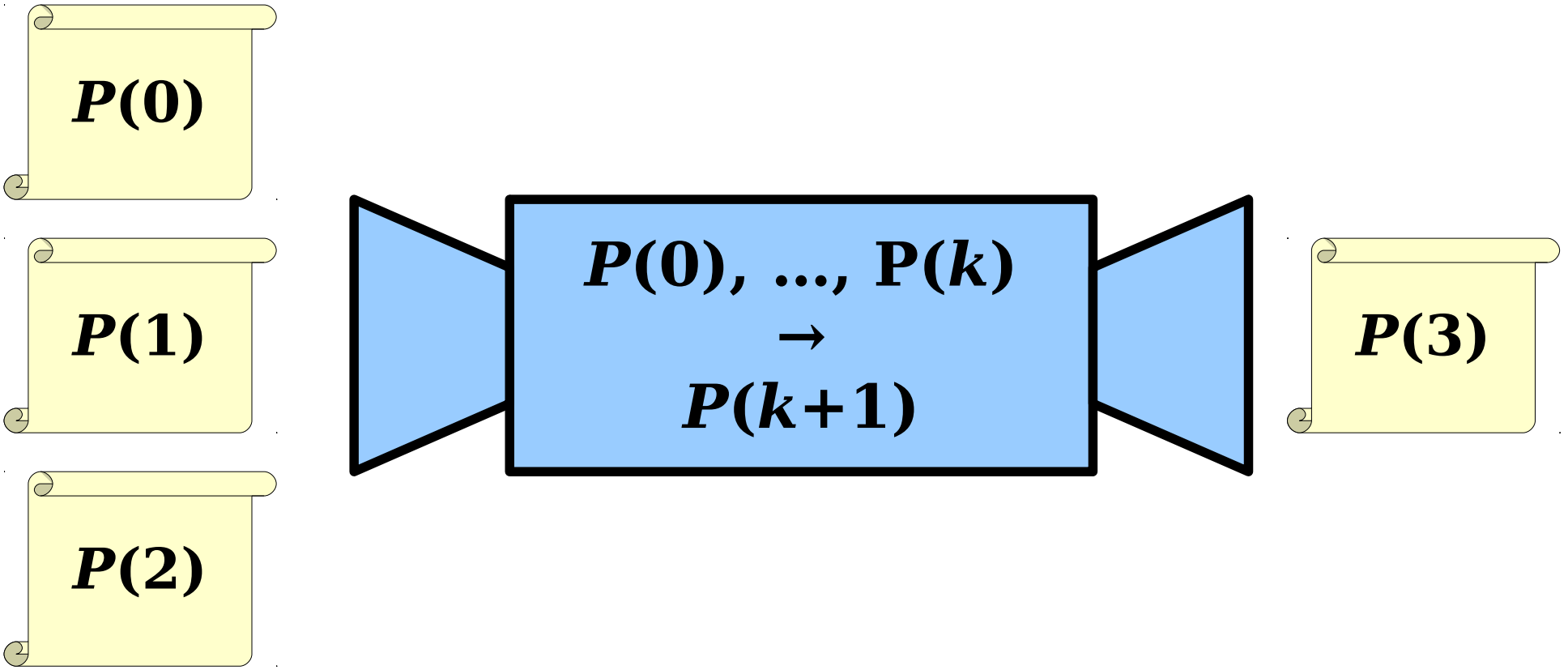
Intuiting Complete Induction



Intuiting Complete Induction



Intuiting Complete Induction



A Helpful Intuition

- If you see something of the form

  “keep repeating *X* until...”

  try proving it by induction.
- Use the inductive hypothesis to “assume away” future steps.
- Example: Counterfeit coins.
  - Process: “Keep splitting the coins into thirds and throwing away coins until only one's left.”
  - Proof: “Assume that it works for 3^k coins and prove that it works for 3^{k+1} coins.”