Mathematical Induction

Part Two

Outline for Today

- ***Variations on Induction***
  - Starting later, taking different step sizes, and more!
- ***"Build Up" versus "Build Down"***
  - An inductive nuance that follows from our general proofwriting principles.
- ***Complete Induction***
  - When one assumption isn't enough!

Recap from Last Time

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

If it starts true…

$$\boldsymbol{P(0) \text{ is true}}$$

…and it stays true…

and

$$\forall k \in \mathbb{N}.\ (P(k) \to P(k+1))$$

then

$$\forall n \in \mathbb{N}.\ P(n)$$

…then it's always true.

Try It!

Starting with `MI`, apply these operations to make `MU`:

(a) Double the string after an `M`.

(b) Replace `III` with `U`.

(c) Append `U`, if the string ends in `I`.

(d) Delete `UU` from the string.

Not a single person in this room
was able to solve this puzzle.

Are we even sure that there is a solution?

Counting **I**'s


MI
1
MII
2
MIIII
4
MIIIIU
4
MIIIIUIIIIU
8
MIIIIUUIU
5
MIIIIUUIUIIIIUUIU
10
MUIUUIUIIIIUUIU
7

The Key Insight

- Initially, the number of `I`'s is *not* a multiple of three.
- To make `MU`, the number of `I`'s must end up as a multiple of three.
- Can we *ever* make the number of `I`'s a multiple of three?

Lemma 1: If n is an integer that is not a multiple of three, then $n - 3$ is not a multiple of three.

Proof: By contrapositive; we'll prove that if $n - 3$ is a multiple of three, then n is also a multiple of three. Because $n - 3$ is a multiple of three, we can write $n - 3 = 3k$ for some integer k. Then $n = 3(k+1)$, so n is also a multiple of three, as required. ■

Lemma 2: If n is an integer that is not a multiple of three, then $2n$ is not a multiple of three.

Proof: Let n be a number that isn't a multiple of three. If n is congruent to one modulo three, then $n = 3k + 1$ for some integer k. This means $2n = 2(3k+1) = 6k + 2 = 3(3k) + 2$, so $2n$ is not a multiple of three. Otherwise, n must be congruent to two modulo three, so $n = 3k + 2$ for some integer k. Then $2n = 2(3k+2) = 6k+4 = 3(2k+1) + 1$, and so $2n$ is not a multiple of three. ■

Lemma: No matter which moves are made, the number of **`I`**'s in the string never becomes multiple of three.

Proof: Let $P(n)$ be the statement "after any n moves, the number of **`I`**'s in the string will not be multiple of three." 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'll prove $P(0)$, that the number of **`I`**'s after 0 moves is not a multiple of three. After no moves, the string is **`MI`**, which has one **`I`** in it. Since one isn't a multiple of three, $P(0)$ is true.

For our inductive step, suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$. We'll prove $P(k+1)$ is also true. Consider any sequence of $k+1$ moves. Let r be the number of **`I`**'s in the string after the kth move. By our inductive hypothesis (that is, $P(k)$), we know that r is not a multiple of three. Now, consider the four possible choices for the $k+1^{\text{st}}$ move:

Case 1: Double the string after the **`M`**. After this, we will have $2r$ **`I`**'s in the string, and from our lemma $2r$ isn't a multiple of three.

Case 2: Replace **`III`** with **`U`**. After this, we will have $r - 3$ **`I`**'s in the string, and by our lemma $r - 3$ is not a multiple of three.

Case 3: Either append **`U`** or delete **`UU`**. This preserves the number of **`I`**'s in the string, so we don't have a multiple of three **`I`**'s at this point.

Therefore, no sequence of $k+1$ moves ends with a multiple of three **`I`**'s. Thus $P(k+1)$ is true, completing the induction. ■

Theorem: The `MU` puzzle has no solution.

Proof: Assume for the sake of contradiction that the `MU` puzzle has a solution and that we can convert `MI` to `MU`. This would mean that at the very end, the number of `I`'s in the string must be zero, which is a multiple of three. However, we've just proven that the number of `I`'s in the string can never be a multiple of three.

We have reached a contradiction, so our assumption must have been wrong. Thus the `MU` puzzle has no solution. ■

Algorithms and Loop Invariants

- The proof we just made had the form
  - "If P is true before we perform an action, it is true after we perform an action."
- We could therefore conclude that after any series of actions of any length, if P was true beforehand, it is true now.
- In algorithmic analysis, this is called a ***loop invariant***.
- Proofs on algorithms often use loop invariants to reason about the behavior of algorithms.
  - Take CS161 for more details!

New Stuff!

Variations on Induction: ***Starting Later***

Induction Starting at 0

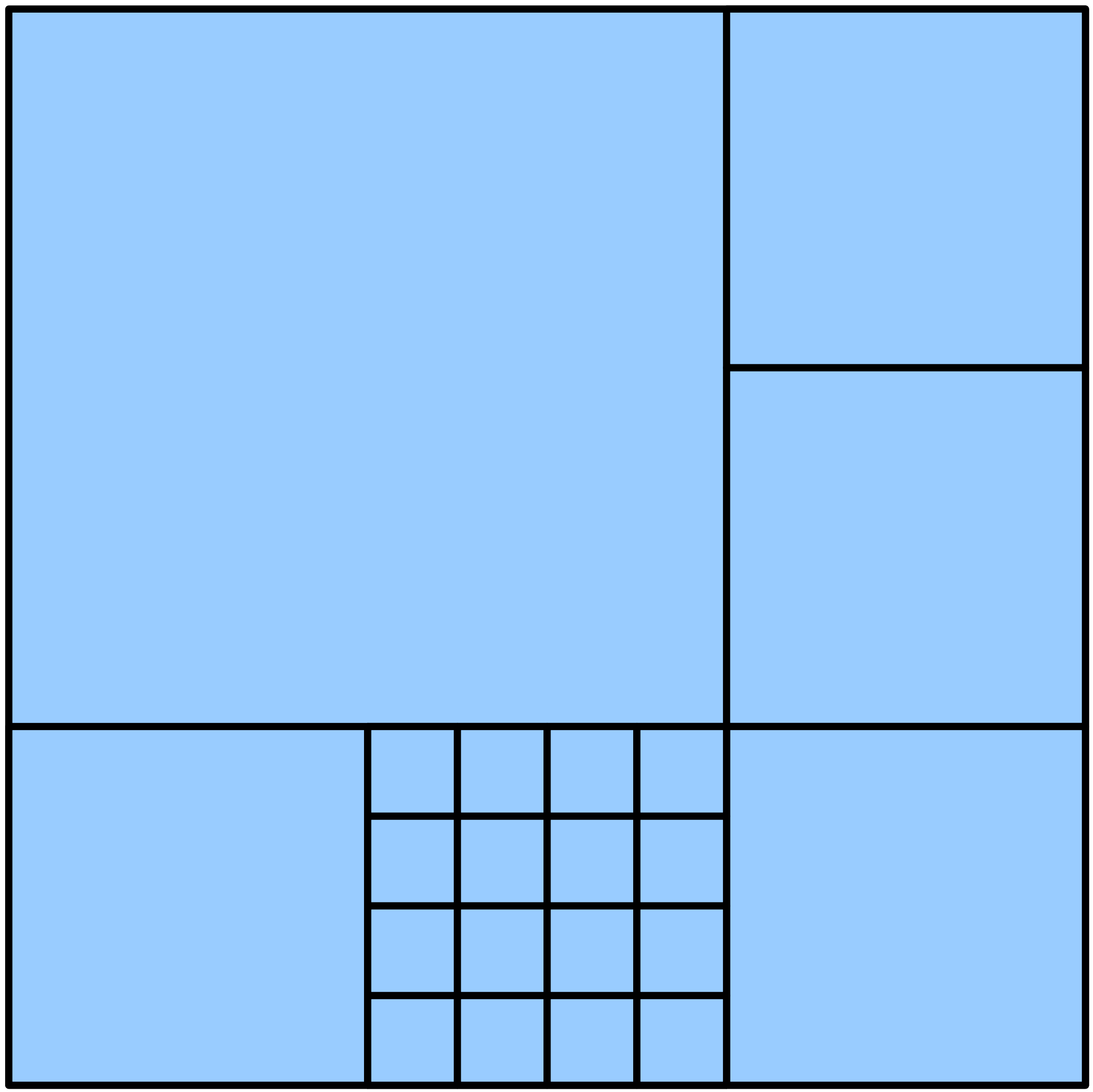
- To prove that $P(n)$ is true for all natural numbers greater than or equal to 0:
  - Show that $P(0)$ is true.
  - Show that for any $k \geq 0$, that if $P(k)$ is true, then $P(k+1)$ is true.
  - Conclude $P(n)$ holds for all natural numbers greater than or equal to 0.

Induction Starting at $\boldsymbol{m}$

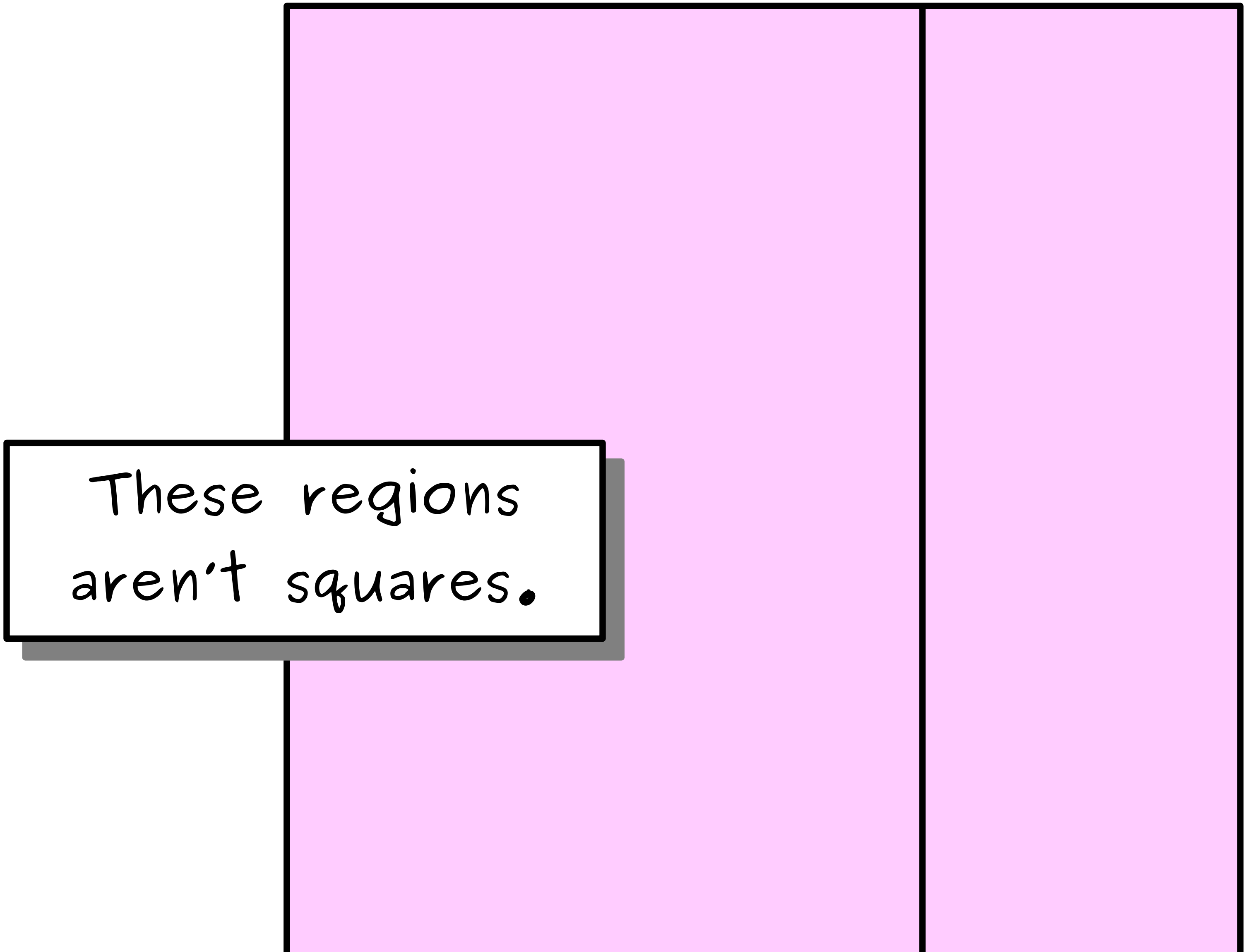
- To prove that $P(n)$ is true for all natural numbers greater than or equal to $\boldsymbol{m}$:
  - Show that $P(\boldsymbol{m})$ is true.
  - Show that for any $k \geq \boldsymbol{m}$, that if $P(k)$ is true, then $P(k+1)$ is true.
  - Conclude $P(n)$ holds for all natural numbers greater than or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

Variations on Induction: ***Bigger Steps***

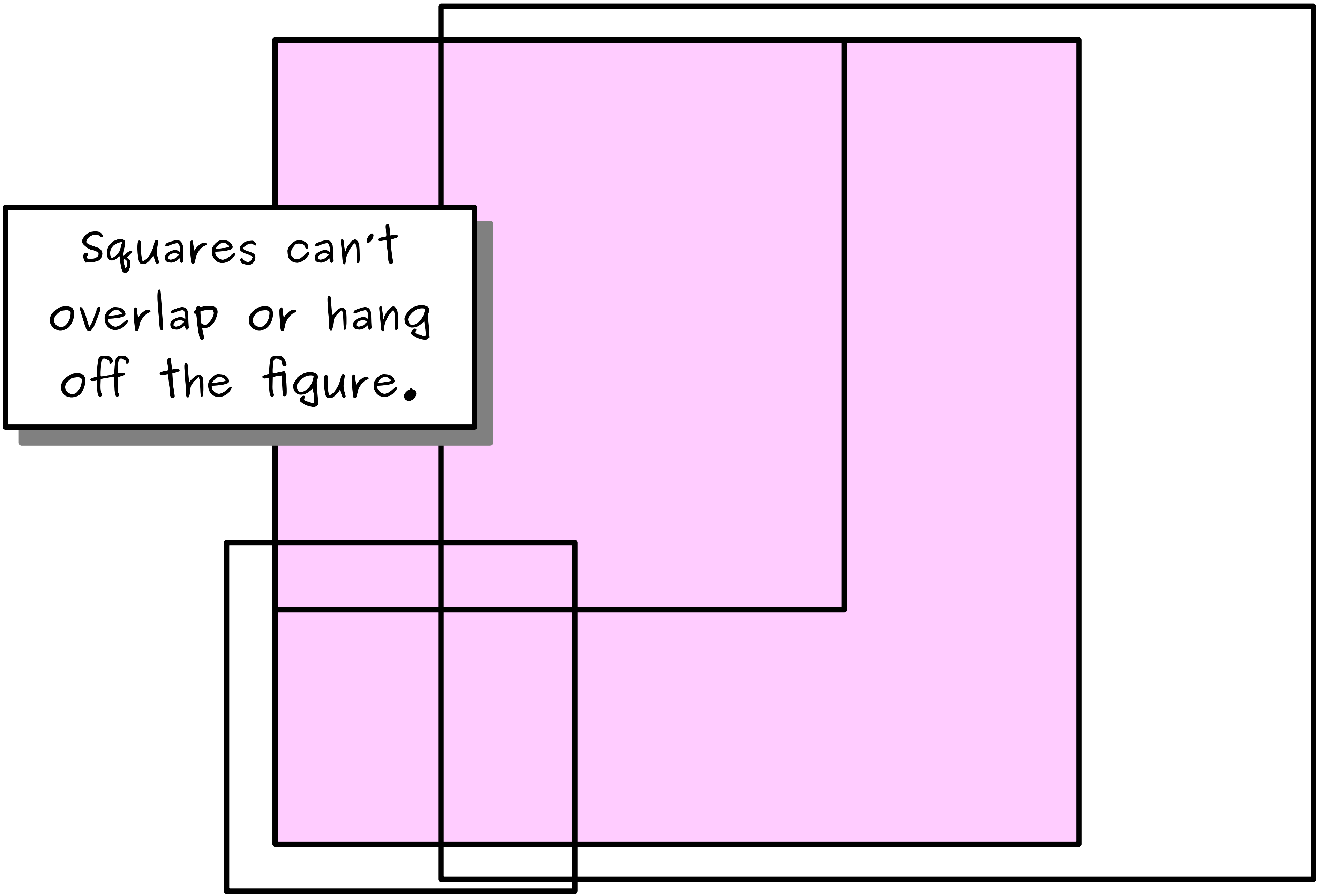
Subdividing a Square



Subdividing a Square

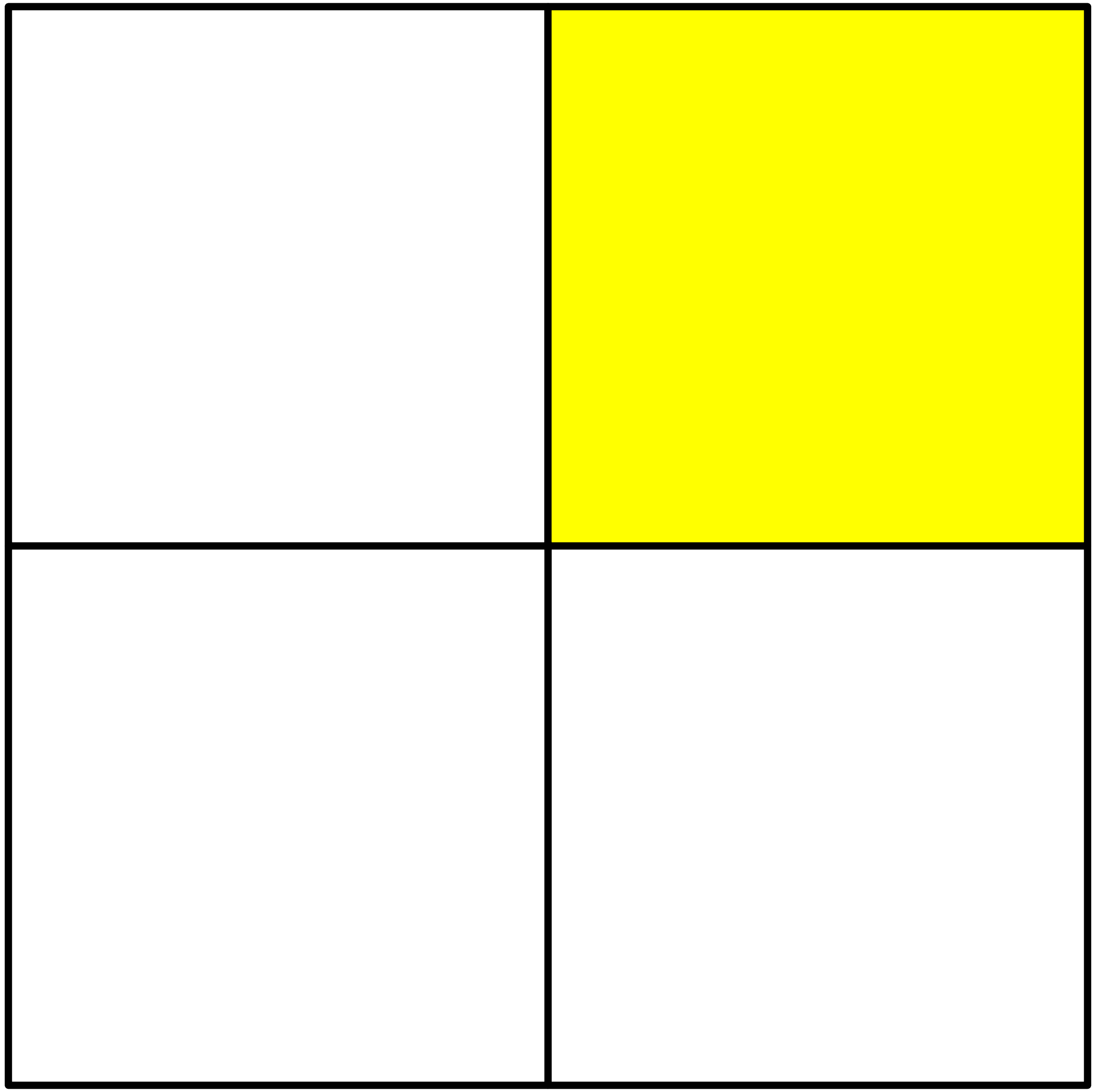


Subdividing a Square

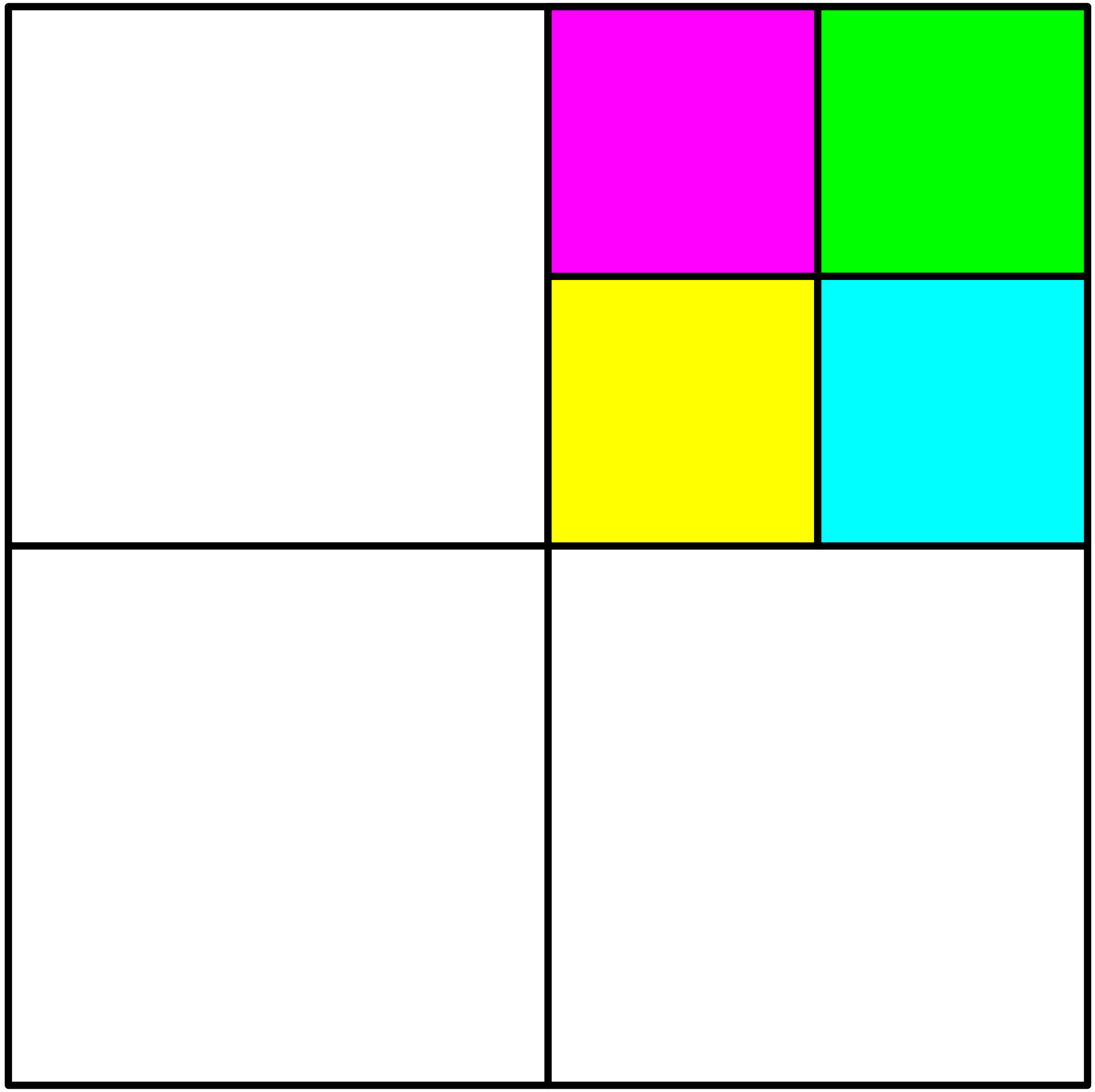


For what values of n can a square be subdivided into n squares?

An Insight



An Insight



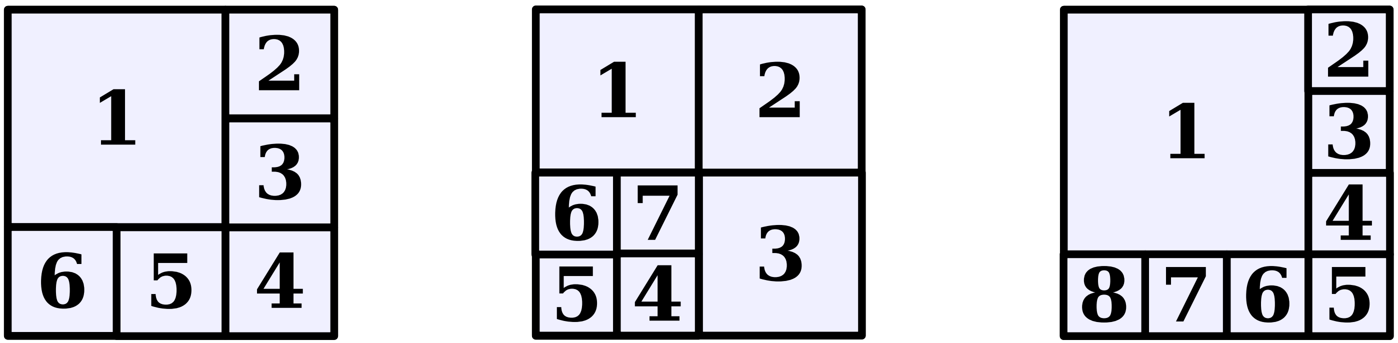
An Insight

- 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 $n \geq 6$, there is a way to subdivide a square into n smaller squares.

Proof: Let $P(n)$ be the statement "there is a way to subdivide a square 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 arbitrary $k \geq 6$ that $P(k)$ is true and that there is a way to subdivide a square into k squares. We prove $P(k+3)$, that there is a way to subdivide a square 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. ■

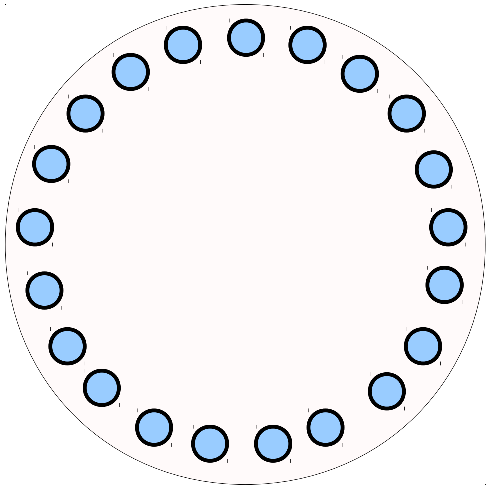
Generalizing Induction

- When doing a proof by induction,
  - feel free to use multiple base cases, and
  - feel free to take steps of sizes other than one.
- If you do, make sure that…
  - … you actually need all your base cases. Avoid redundant base cases that are already covered by a mix of other base cases and your inductive step.
  - … you cover all the numbers you need to cover. Trace out your reasoning and make sure all the numbers you need to cover really are covered.
- As with a proof by cases, you don't need to separately prove you've covered all the options. We trust you.

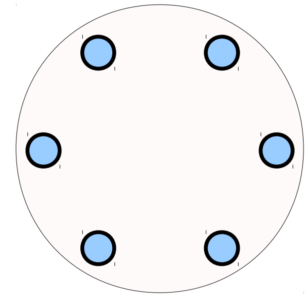
More on Square Subdivisions

- There are a ton of interesting questions that come up when trying to subdivide a rectangle or square into smaller squares.
- In fact, one of the major players in early graph theory (William Tutte) got his start playing around with these problems.
- Good starting resource: this Numberphile video on ***Squaring the Square***.

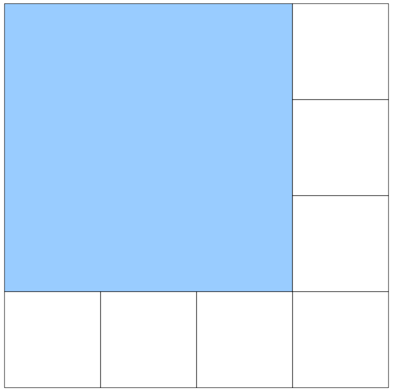
An Observation



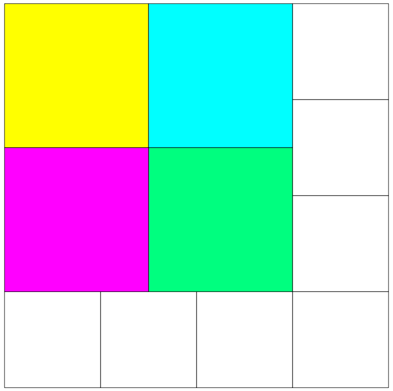
Start with larger graph



Get to smaller graph



Start with fewer squares



Get to more squares

Following the Rules

- When working with square subdivisions, our predicate looked like this:

$P(n)$ is "***there exists*** a way to subdivide a square into n squares."

- When working with Ramsey theory, our predicate looked like this:

$P(n)$ is "***for any*** coloring of a $K_{3n!}$, there is a monochrome K_3."

- With squares, the quantifier is ∃. With graphs, the first quantifier is ∀.
- This fundamentally changes the "feel" of induction.

Build Up with ∃

- In the case of squares, in our inductive step, we prove

  If

  there exists a subdivision into k squares,

  then

  there exists a subdivision into k+3 squares.

- Assuming the antecedent gives us a concrete subdivision into k squares.
- Proving the consequent means finding some way to subdivide in to k+3 squares.
- The inductive step goal is to "***build up***:" start with a smaller number of squares, and somehow work out what to do to get a larger number of squares.

Build Down with ∀

- In the Ramsey case, in our inductive step, we prove

  If

  for all colorings of $K_{3r!}$, there's a monochrome K_3.

  then

  for all colorings of $K_{3(r+1)!}$, there's a monochrome K_3.

- Assuming the antecedent means once we find an r-colored $K_{3r!}$, we get a monochrome K_3.
- Proving the consequent means picking an arbitrary coloring of $K_{3(r+1)!}$, then trying to find a monochrome K_3 in it.
- The inductive step goal is to "***build down***:" start with a larger graph, then find a way to turn it into a smaller graph.

Some Notes

- Not all predicates P(n) will have the form outlined here.
  - That's okay! Just use the normal rules for assuming and proving things.
  - Think of these as quick shorthands rather than fundamentally new strategies.
- In all cases, assume $P(k)$ and prove $P(k+1)$.
  - All that changes is what you do to assume $P(k)$ and what you do to prove $P(k+1)$.

Time-Out for Announcements!

Problem Set Five

- Problem Set Four was due at 4:00PM today.
  - You can use a late day to extend the deadline to Saturday at 4:00PM. Remember that you can use at most one late day per problem set.
- Problem Set Five goes out today. It’s due next Friday at 4:00PM.
  - Play around with everything we’ve covered so far, plus a healthy dose of induction and inductive problem-solving.
- Before starting, read our “Guide to Induction” and “Induction Proofwriting Checklist,” which cover common and important cases to look for.
- As always, ping us if you have any questions! That’s what we’re here for.

Back to CS103!

Complete Induction

This is kinda like $P(0)$.

If you are the ***leftmost*** person in your row, stand up right now.

Everyone else: stand up as soon as the person to your left in your row stands up.

This is kinda like $P(k) \to P(k+1)$.

This is kinda like P(0).

If you are the ***leftmost*** person in your row, stand up right now.

Everyone else: stand up as soon as ***everyone*** left of you in your row stands up.

What sort of sorcery is this?

Let P be some predicate. The ***principle of complete induction*** states that if

If it starts true…

$P(0)$ is true

…and it stays true…

and

for all $k \in \mathbb{N}$, if $P(0)$, …, and $P(k)$ are true, then $P(k+1)$ is true

then

$\forall n \in \mathbb{N}.\ P(n)$

…then it's always true.

Mathematical Induction

- You can write proofs using the principle of mathematical induction as follows:
  - Define some predicate $P(n)$ to prove by induction on n.
  - Choose and prove a base case (probably, but not always, $P(0)$).
  - Pick an arbitrary $k \in \mathbb{N}$ and assume that $P(k)$ is true.
  - Prove $P(k+1)$.
  - Conclude that $P(n)$ holds for all $n \in \mathbb{N}$.

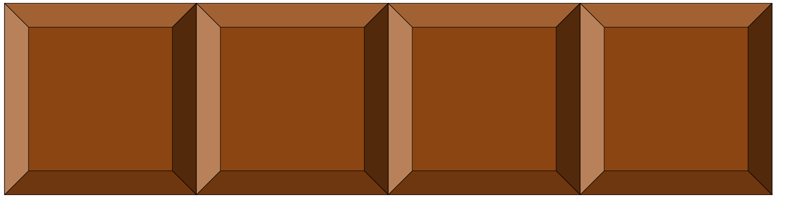
Complete Induction

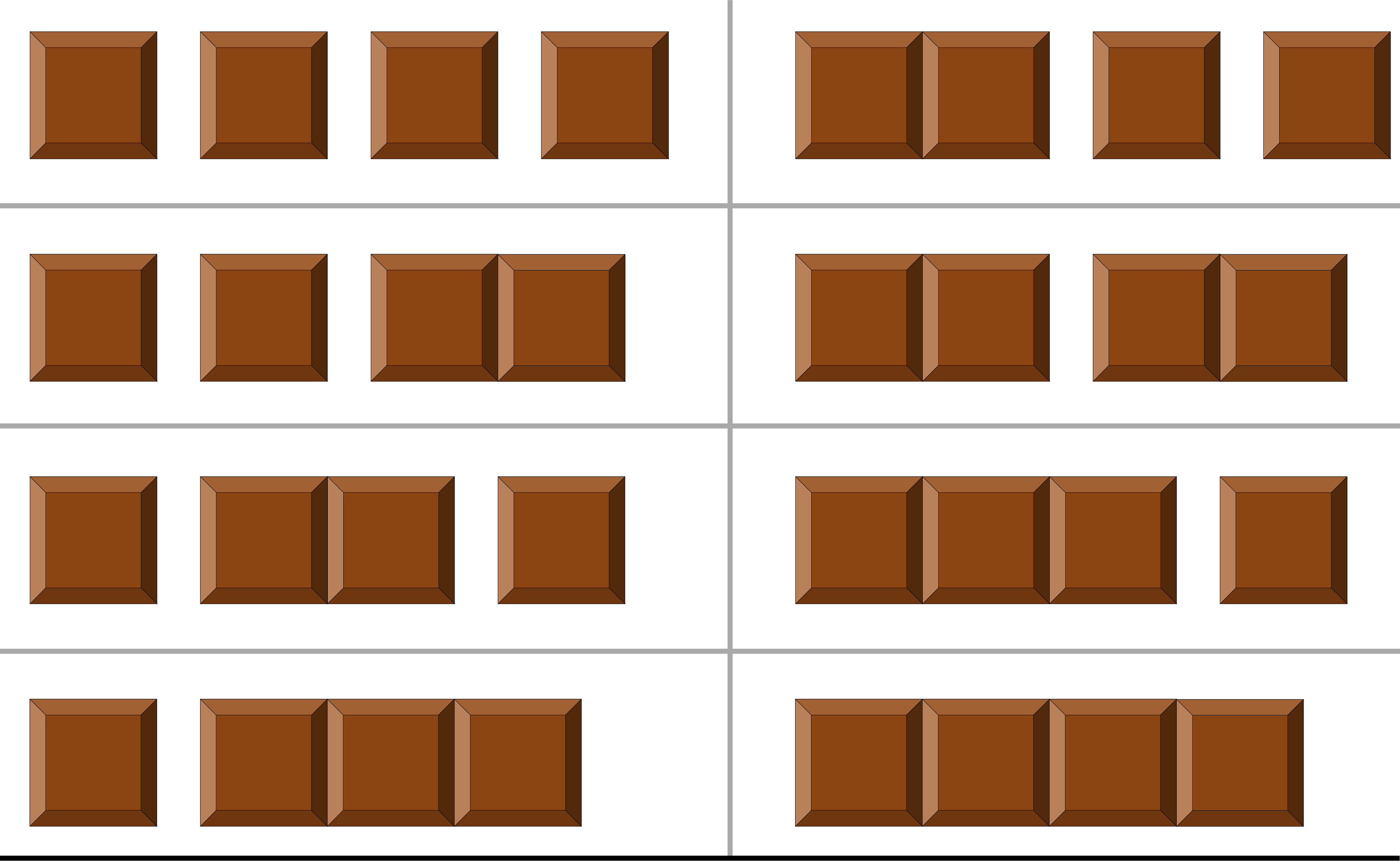
- You can write proofs using the principle of ***complete*** induction as follows:
  - Define some predicate $P(n)$ to prove by induction on n.
  - Choose and prove a base case (probably, but not always, $P(0)$).
  - Pick an arbitrary $k \in \mathbb{N}$ and assume that $\boldsymbol{P(0), P(1), P(2), \ldots,}$ **and** $\boldsymbol{P(k)}$ are all true.
  - Prove $P(k+1)$.
  - Conclude that $P(n)$ holds for all $n \in \mathbb{N}$.

An Example: ***Eating a Chocolate Bar***

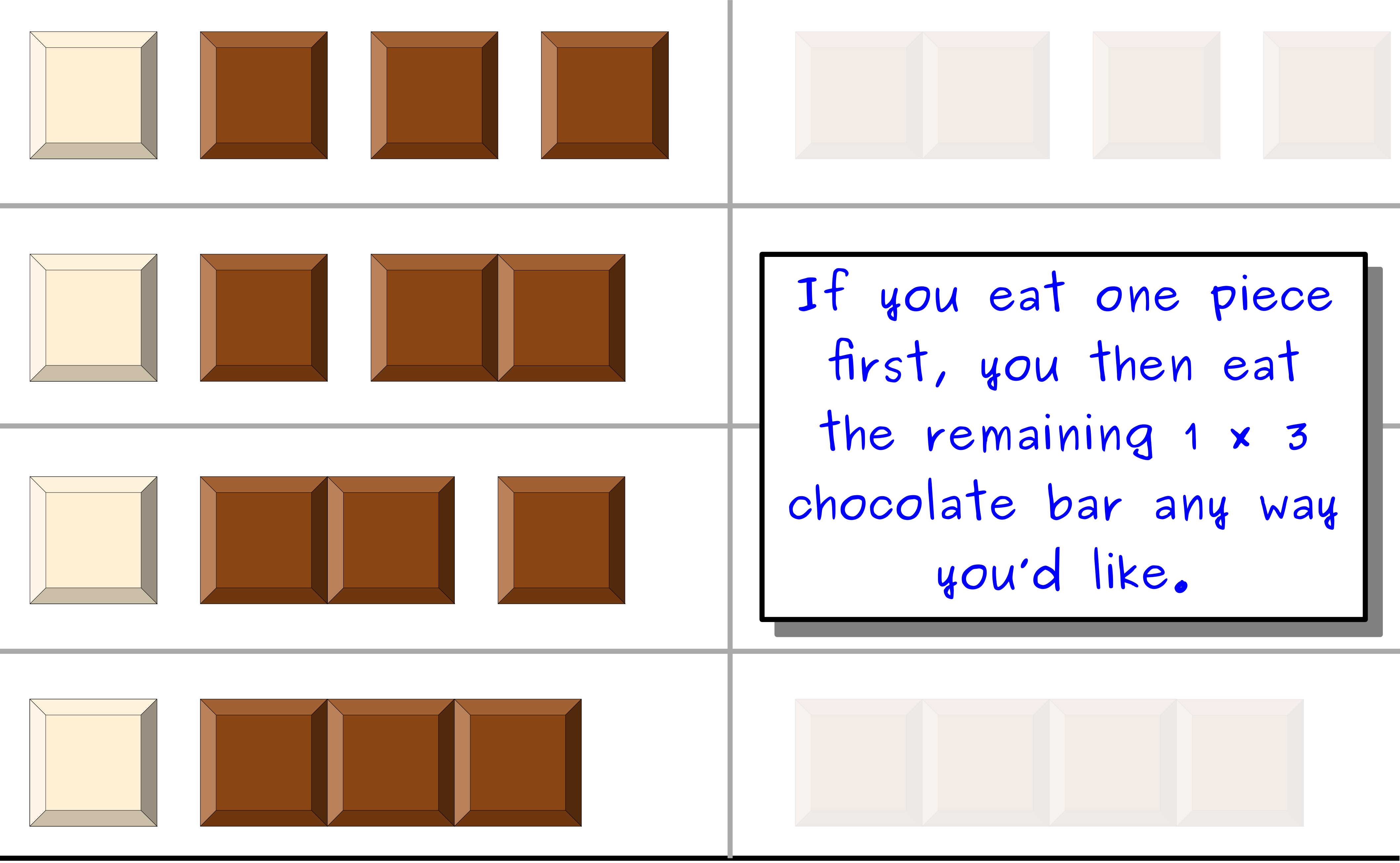
Eating a Chocolate Bar

- You have a $1 \times n$ chocolate bar subdivided into 1×1 squares.
- You eat the chocolate bar from left to right by breaking off one or more squares and eating them in one (possibly enormous) bite.
- How many ways can you eat a…
  - 1×1 chocolate bar?
  - 1×2 chocolate bar?
  - 1×3 chocolate bar?
  - 1×4 chocolate bar?

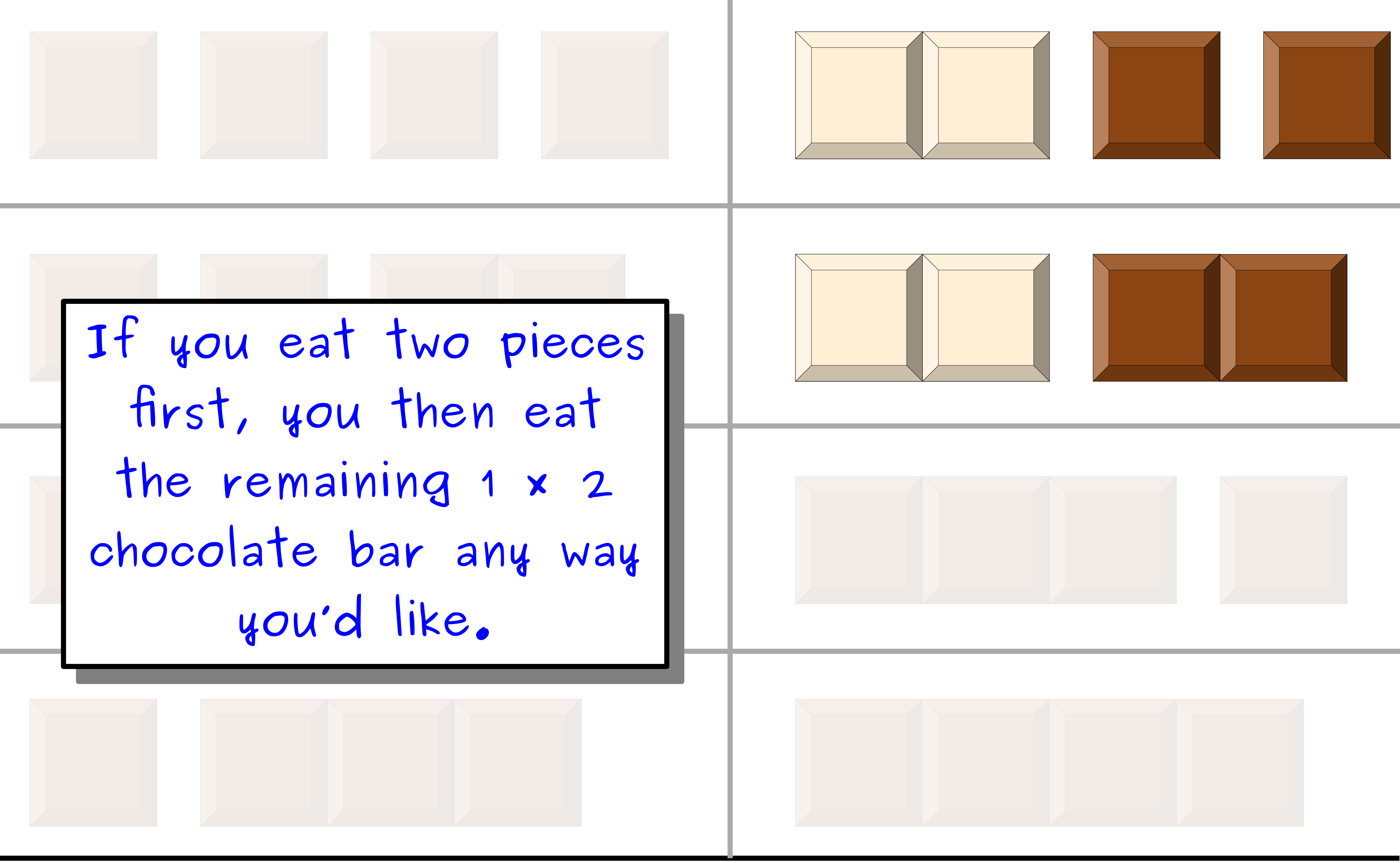




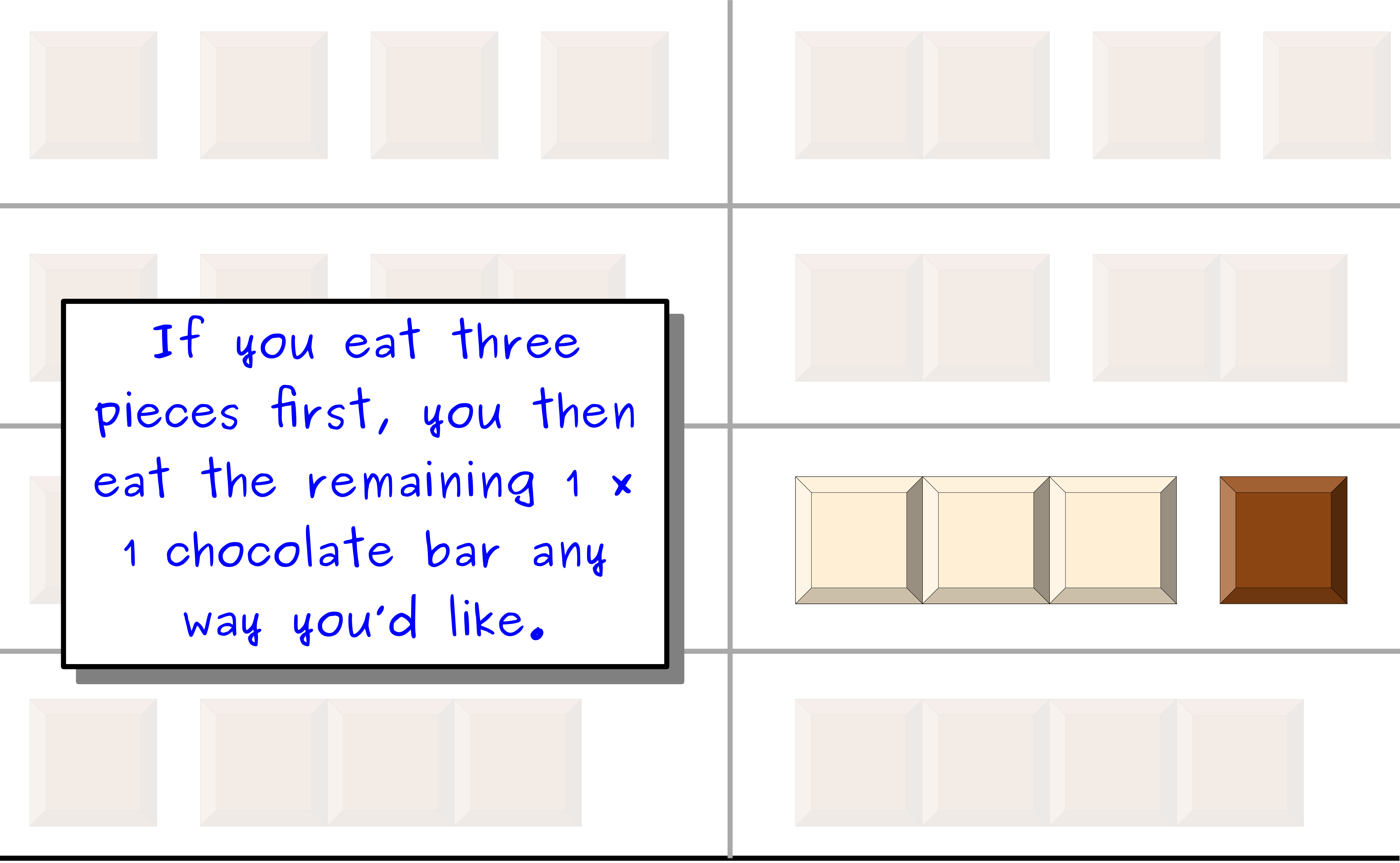
There are eight ways to eat a 1×4 chocolate bar.



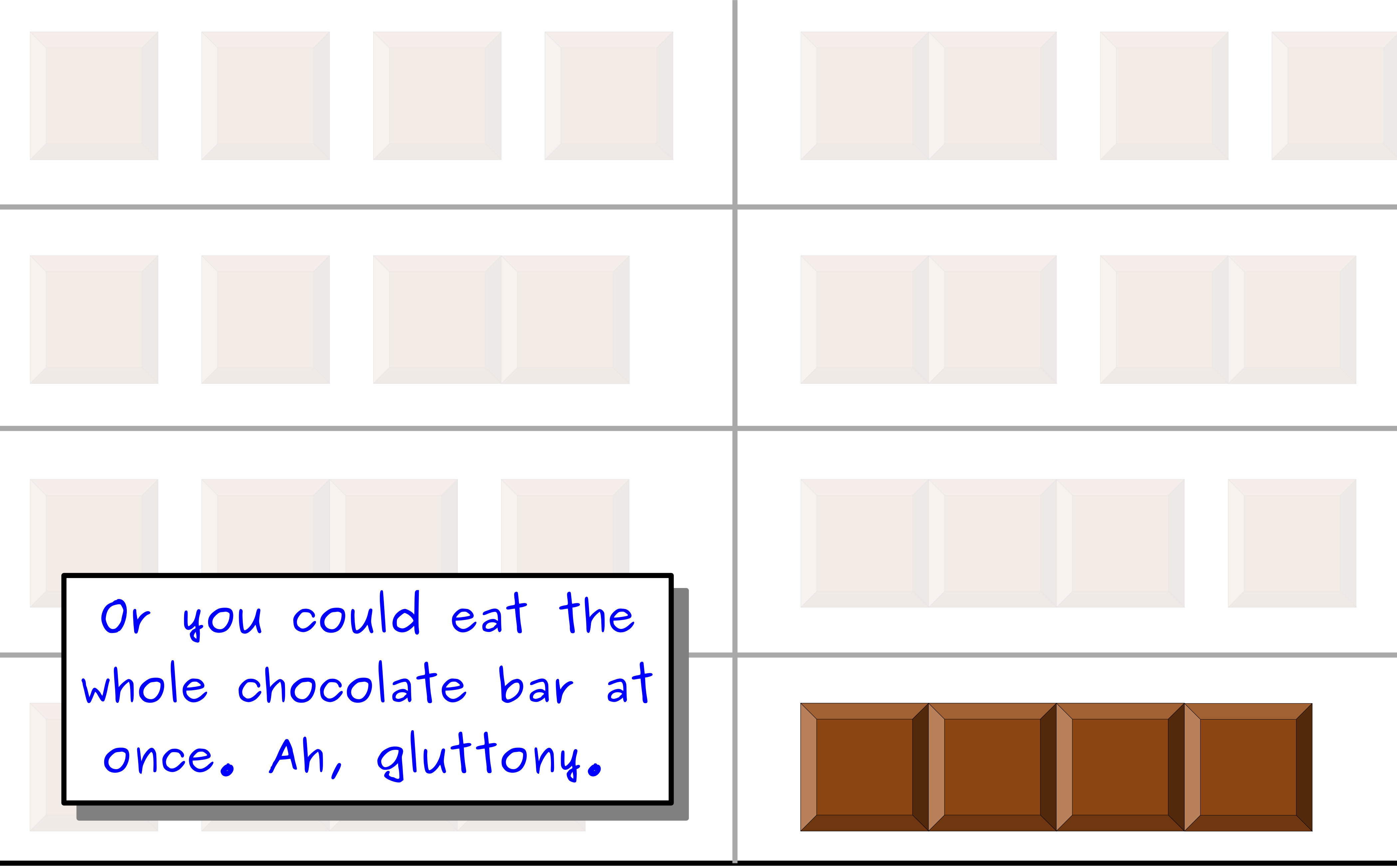
There are eight ways to eat a 1 × 4 chocolate bar.



There are eight ways to eat a 1×4 chocolate bar.



There are eight ways to eat a 1 × 4 chocolate bar.



There are eight ways to eat a 1 × 4 chocolate bar.

Eating a Chocolate Bar

- There's…
  - 1 way to eat a 1×1 chocolate bar,
  - 2 ways to eat a 1×2 chocolate bar,
  - 4 ways to eat a 1×3 chocolate bar, and
  - 8 ways to eat a 1×4 chocolate bar.
- ***Our guess:*** There are 2^{n-1} ways to eat a $1 \times n$ chocolate bar for any natural number $n \geq 1$.
- And we think it has something to do with this insight: we eat the bar either by
  - eating the whole thing in one bite, or
  - eating some piece of size k, then eating the remaining $n - k$ pieces however we'd like.
- Let's formalize this!

Theorem: For any natural number $n \geq 1$, the number of ways to eat a $1 \times n$ chocolate bar from left to right is 2^{n-1}.

Proof: Let $P(n)$ be "the number of ways to eat a $1 \times n$ chocolate bar from left to right is 2^{n-1}." We will prove by induction that $P(n)$ holds for all natural numbers $n \geq 1$, from which the theorem follows.

As our base case, we prove $P(1)$, that the number of ways to eat a 1×1 chocolate bar from left to right is $2^{1-1} = 1$. The only option here is to eat the entire chocolate bar at once, so there's just one way to eat it, as needed.

For our inductive step, assume for some arbitrary natural number $k \geq 1$ that $P(1)$, …, and $P(k)$ are true. We need to show $P(k+1)$ is true, that the number of ways to eat a $1 \times (k+1)$ chocolate bar is 2^k.

There are two options for how to eat the bar. First, we can eat the whole chocolate bar in one bite. Second, we could eat a piece of size r for some $1 \leq r \leq k$, leaving a chocolate bar of size $k+1-r$, then eat that chocolate bar from left to right. Since $1 \leq r \leq k$, we know that $1 \leq k+1-r \leq k$, so by our inductive hypothesis there are 2^{k-r} ways to eat the remainder.

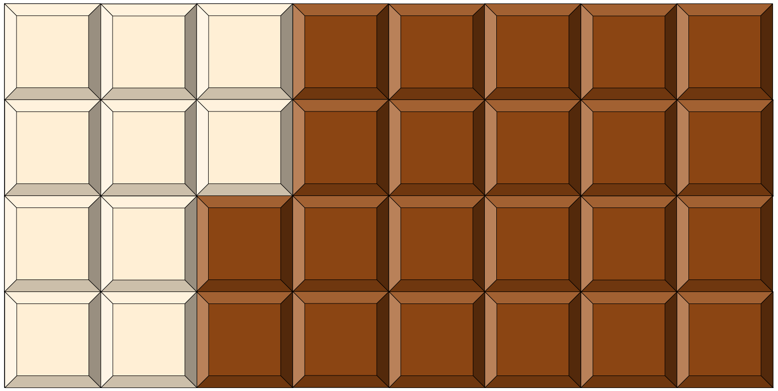
Summing up this first option, plus all choices of r for the second option, we see that the number of ways to eat the chocolate bar is

$$1 + 2^0 + 2^1 + \ldots + 2^{k-1} \quad = \quad 1 + 2^k - 1 \quad = \quad 2^k.$$

Thus $P(k+1)$ holds, completing the induction. ■

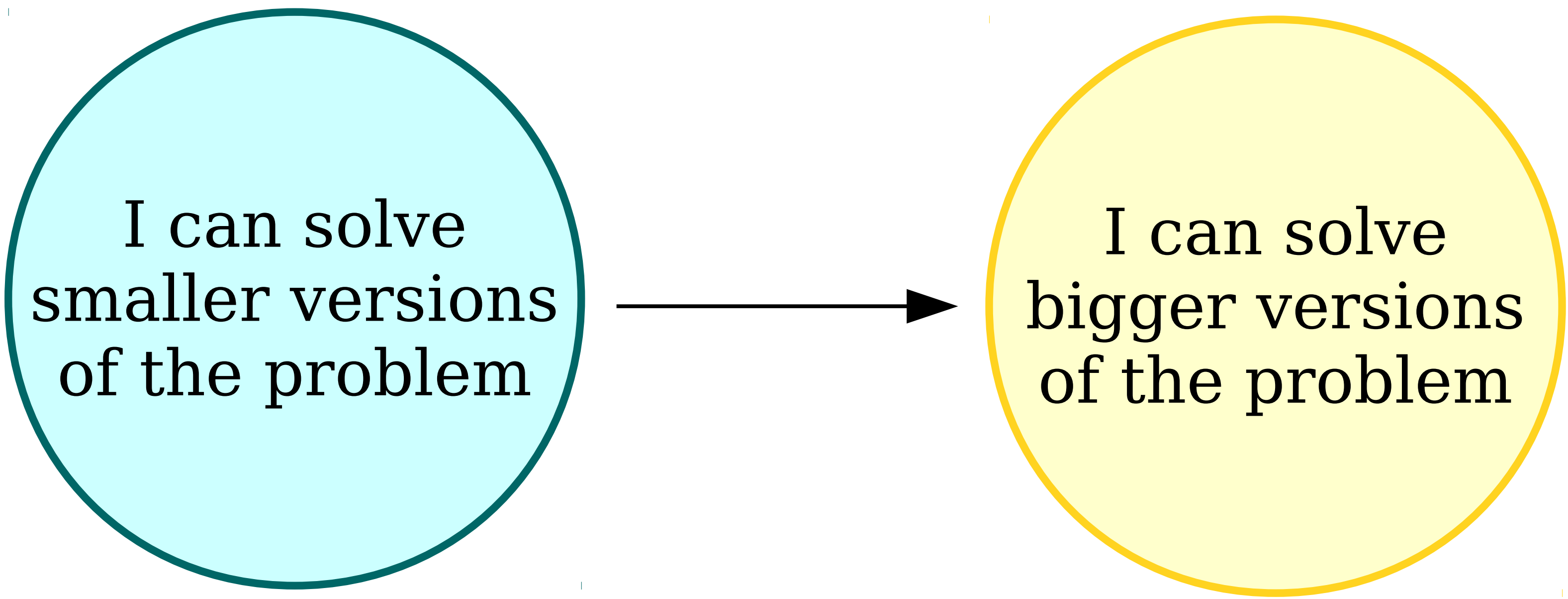
More on Chocolate Bars

- Imagine you have an $m \times n$ chocolate bar. Whenever you eat a square, you have to eat all squares above it and to the left.
- How many ways are there to eat the chocolate bar?

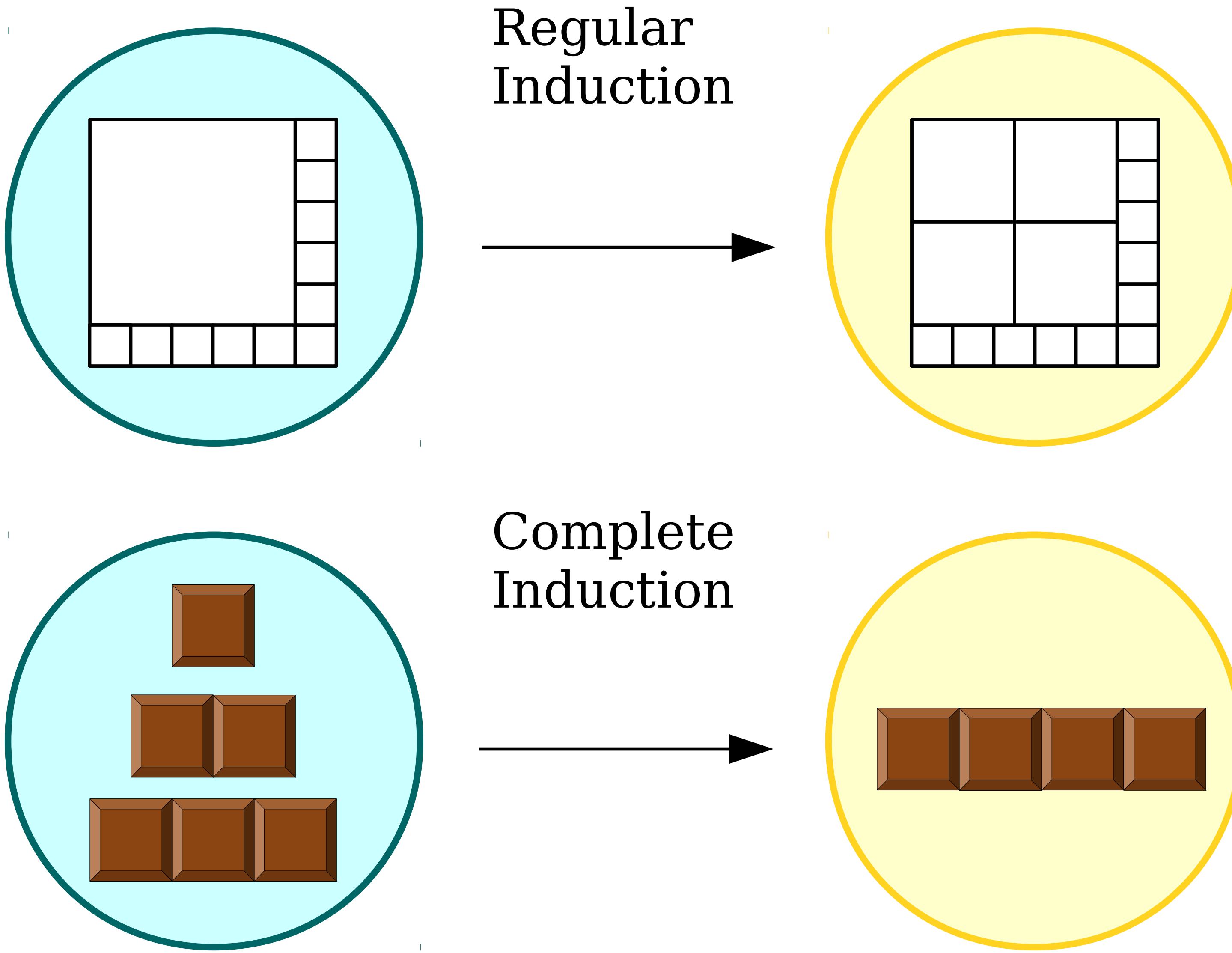


- ***Open Problem:*** Find a non-recursive exact formula for this number, or give an approximation whose error drops to zero as m and n tend toward infinity.

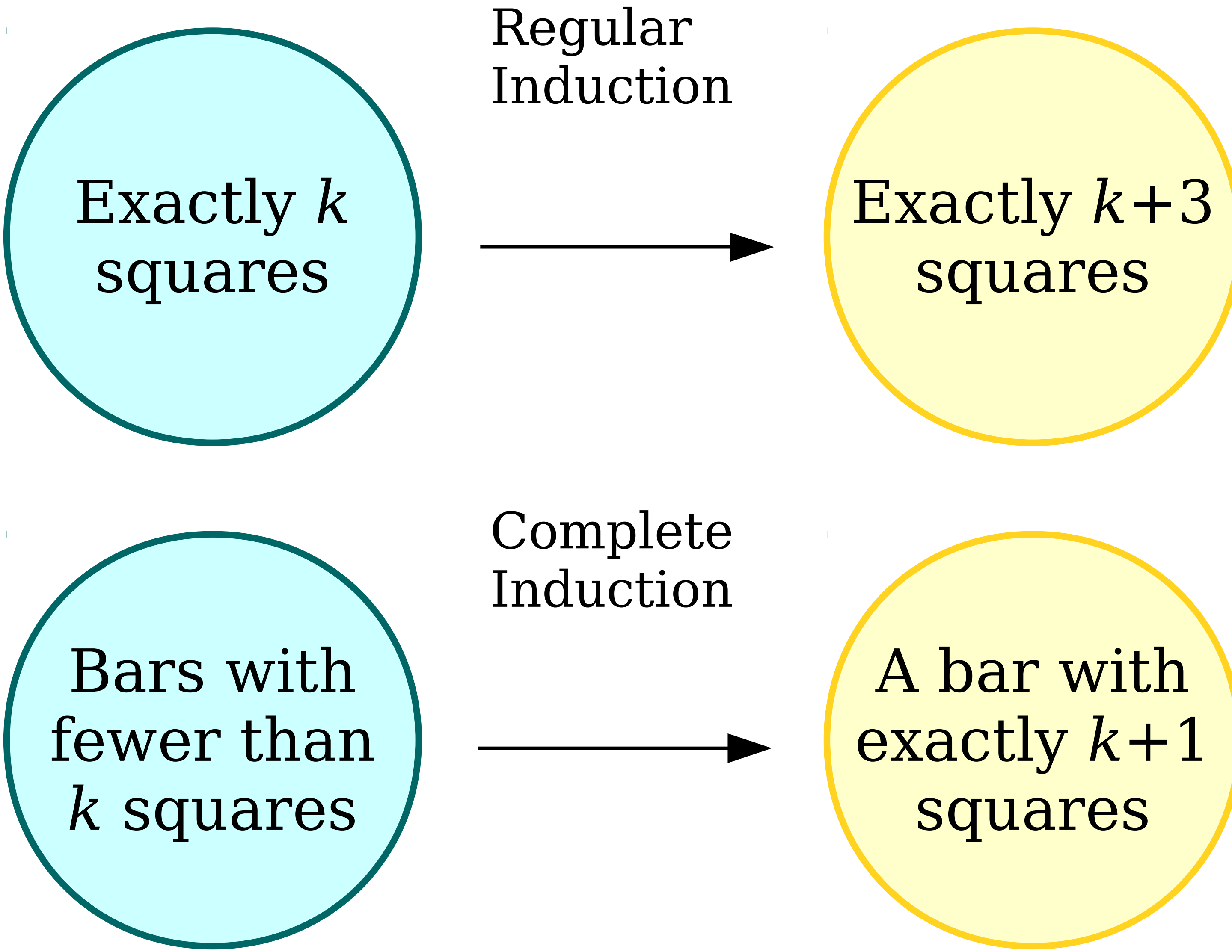
Induction vs. Complete Induction



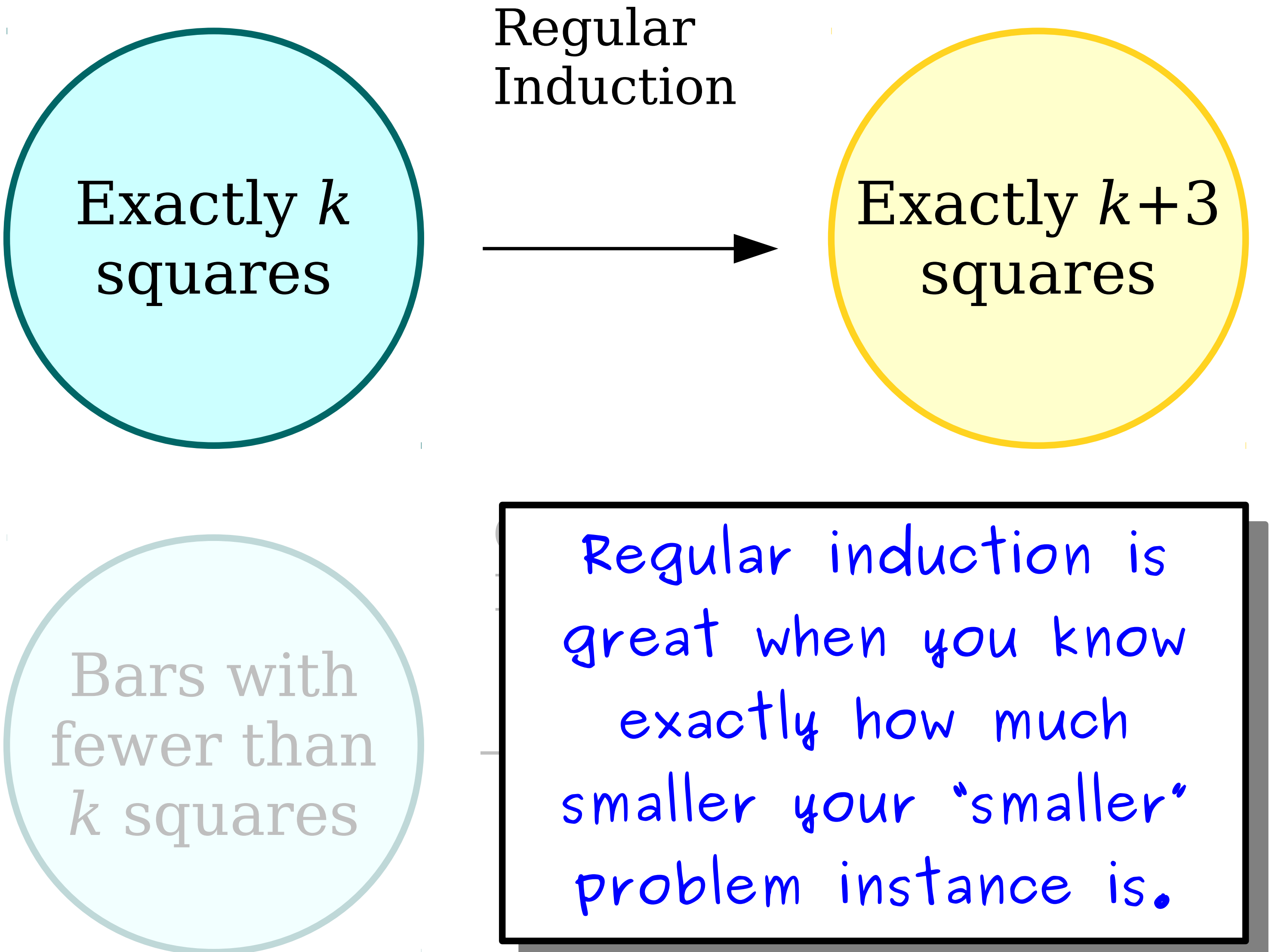
Induction vs. Complete Induction



Induction vs. Complete Induction

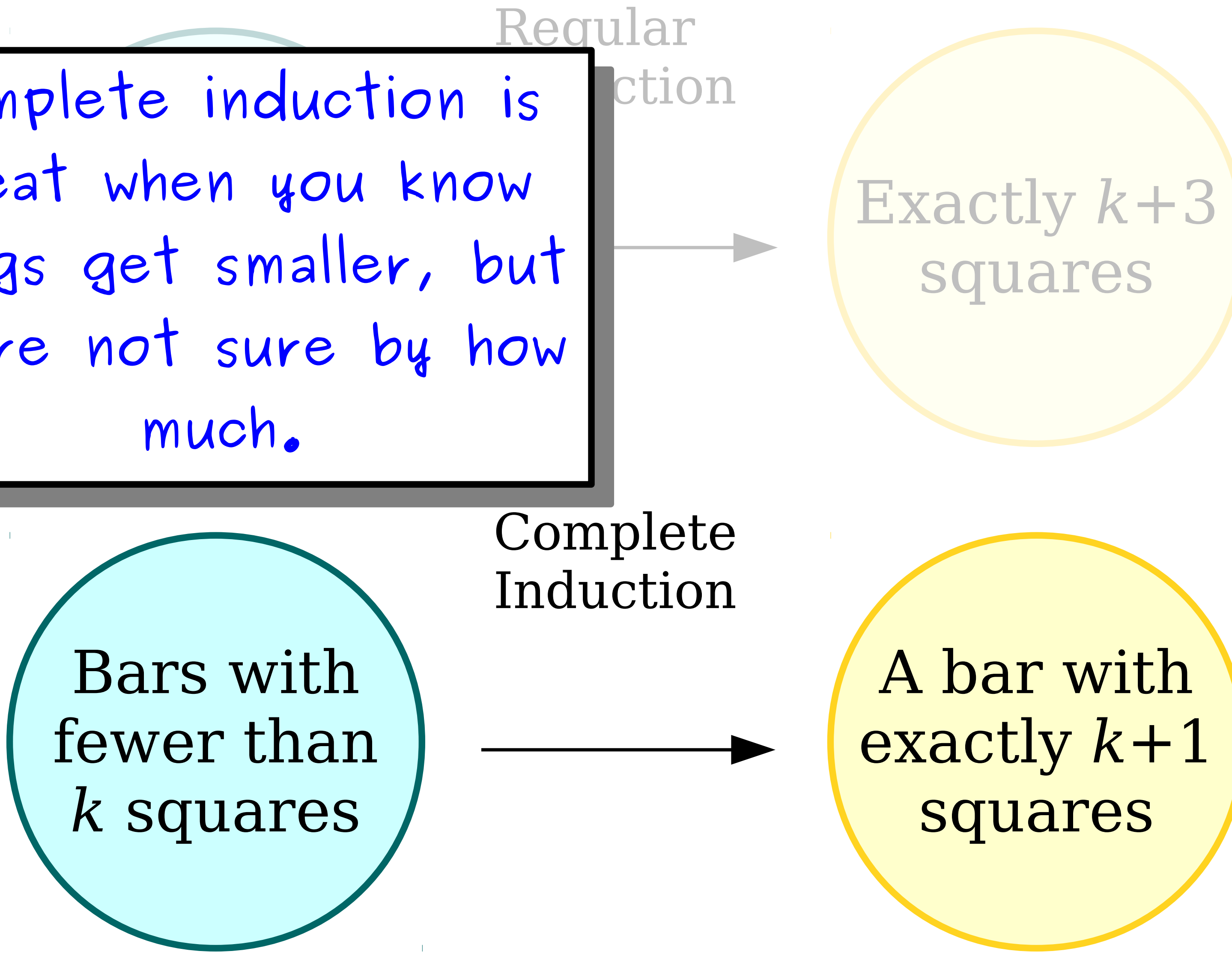


Induction vs. Complete Induction



Induction vs. Complete Induction

Complete induction is great when you know things get smaller, but you're not sure by how much.



How Not To Induct, Part 2

⚠ ***Incorrect!*** ⚠ ***Proof:*** Let $P(n)$ be the statement "all groups of n horses are the same color." We will prove by induction that $P(n)$ holds for all natural numbers n, from which the theorem follows.

As our base case, we prove $P(0)$, that all groups of 0 horses are the same color. This statement is vacuously true because there are no horses.

For the inductive step, assume that for an arbitrary natural number k that $P(k)$ is true and that all groups of k horses are the same color. Now consider a group of $k+1$ horses. Exclude the last horse and look only at the first k horses. By the inductive hypothesis, these horses are the same color. Next, exclude the first horse and look only at the last k horses. Again we see by the inductive hypothesis that these horses are the same color.

Therefore, the first horse is the same color as the non-excluded horses, who in turn are the same color as the last horse. Hence the first horse excluded, the non-excluded horses, and last horse excluded are all of the same color. Thus $P(k+1)$ holds, completing the induction. ■

What's wrong with this proof?

⚠ ***Incorrect!*** ⚠ ***Proof:*** Let $P(n)$ be the statement "all groups of n horses are the same color." We will prove by induction that $P(n)$ holds for all natural numbers n, from which the theorem follows.

As our base case, we prove $P(0)$, that all groups of 0 horses are the same color. This statement is vacuously true because there are no horses.

For the inducti … al number k
that $P(k)$ is true … me color. Now
consider a grou … nd look only at
the first k horse … es are the
same color. Nex … the last k
horses. Again w … se horses are
the same color.

The logic in our inductive step does not allow us to get from P(1) to P(2). Specifically, there are no non-excluded horses that were in both sets.

Therefore, the first horse is the same color as the non-excluded horses, who in turn are the same color as the last horse. Hence the first horse excluded, the non-excluded horses, and last horse excluded are all of the same color. Thus $P(k+1)$ holds, completing the induction. ■

Non-Issues with this Proof

- *“We should have proven additional base cases”*
  - A proof by induction only needs a single base case, so the fact that we only have one here is not in itself an issue.
- *“We should have used complete induction”*
  - Complete induction wouldn’t have helped us here either, since our inductive step would still need to use $P(0)$ and $P(1)$ to prove $P(2)$.

Induction Debugging Tips

- Remember that induction requires two parts: the base case and the inductive step.
- If you see an induction proof of a false statement, one of these pieces must be broken.
- Recommendation: try playing the induction out one step at a time (Is the base case true? From the base case, does the reasoning in your inductive step allow you to conclude the next statement? What about the following statement? etc…)

An Important Milestone

Recap: ***Discrete Mathematics***

- The past five weeks have focused exclusively on discrete mathematics:

Induction	Functions
Graphs	The Pigeonhole Principle
Formal Proofs	Mathematical Logic
Set Theory	

- These are building blocks we will use throughout the rest of the quarter.
- These are building blocks you will use throughout the rest of your CS career.

Three Questions

- What is something you know now that, at the start of the quarter, you knew you didn’t know?
- What is something you know now that, at the start of the quarter, you didn’t know that you didn’t know?
- What is something you don’t know that, at the start of the quarter, you didn’t know that you didn’t know?

Next Up: ***Computability Theory***

- It's time to switch gears and address the limits of what can be computed.
- We'll explore these questions:
  - How do we model computation itself?
  - What exactly is a computing device?
  - What problems can be solved by computers?
  - What problems *can't* be solved by computers?
- ***Get ready to explore the boundaries of what computers could ever be made to do.***

Next Time

- ***Formal Language Theory***
  - How are we going to formally model computation?
- ***Finite Automata***
  - A simple but powerful computing device made entirely of math!
- ***DFAs***
  - A fundamental building block in computing.