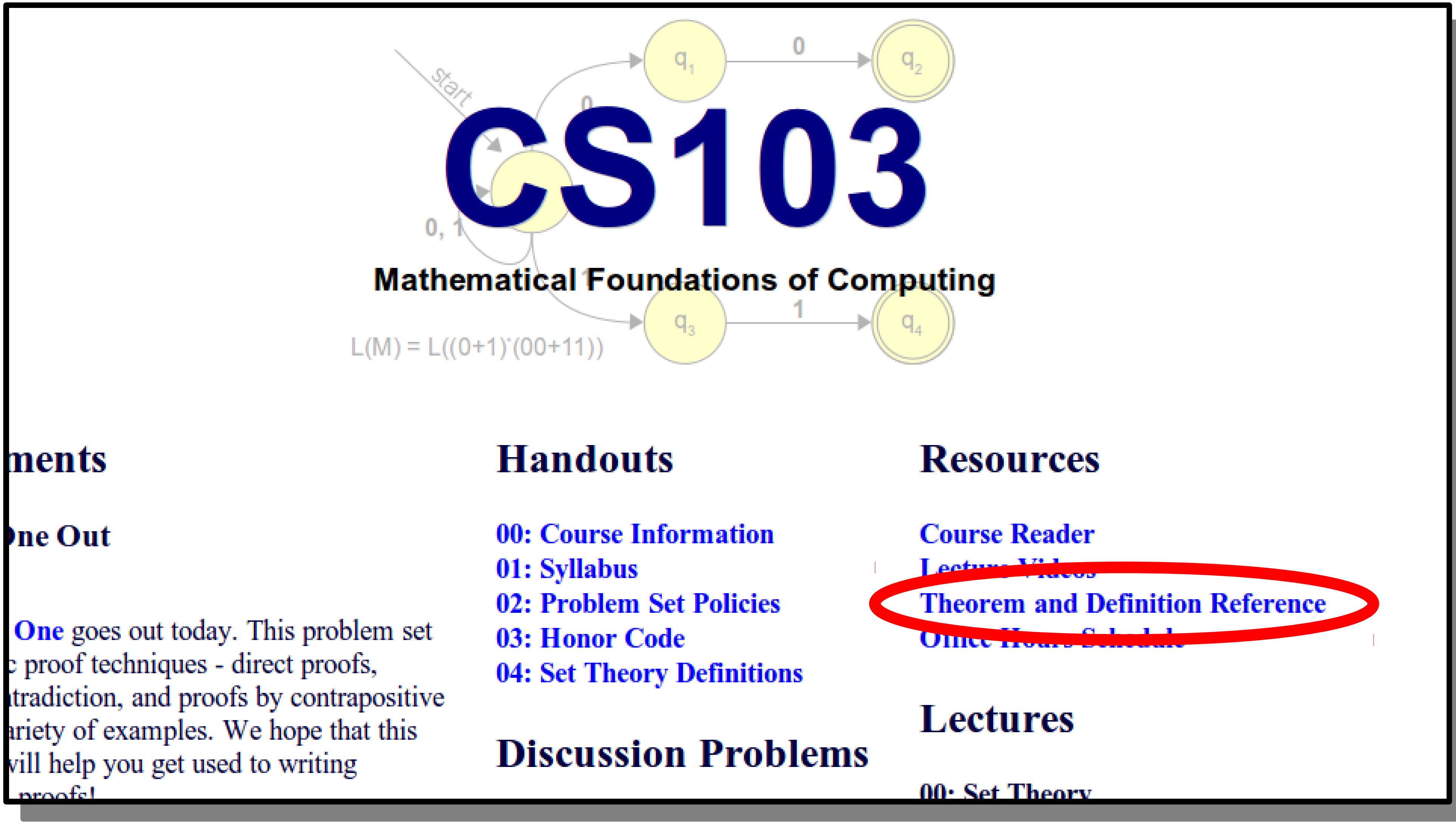
Indirect Proofs

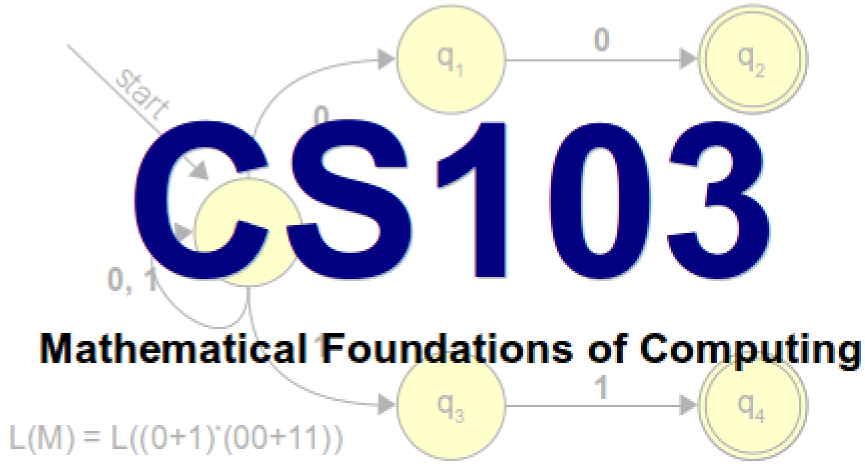
Announcements

- Problem Set 1 out.
- **Checkpoint** due Monday, September 30.
  - Grade determined by attempt rather than accuracy. It's okay to make mistakes – we want you to give it your best effort, even if you're not completely sure what you have is correct.
  - We will get feedback back to you with comments on your proof technique and style.
  - The more an effort you put in, the more you'll get out.
- **Remaining problems** due Friday, October 4.
  - Feel free to email us with questions!

Submitting Assignments

- You can submit assignments by
  - handing them in at the start of class,
  - dropping it off in the filing cabinet near Keith's office (details on the assignment handouts), or
  - emailing the submissions mailing list at **cs103-aut1314-submissions@lists.stanford.edu** and attaching your solution as a PDF. (Please don't email the staff list directly with submissions) See Handout #02 for more details.
- Late policy:
  - Three “late periods:” extend due date by one class period.
  - Can use at most one per assignment.
  - No work accepted more than one class period after the due date.


start
0
0
q1
q2
q3
q4
0, 1
1
1
CS103
Mathematical Foundations of Computing
L(M) = L((0+1)*(00+11))
ments
ne Out
One goes out today. This problem set
proof techniques - direct proofs,
tradiction, and proofs by contrapositive
riety of examples. We hope that this
vill help you get used to writing
proofs!
Handouts
00: Course Information
01: Syllabus
02: Problem Set Policies
03: Honor Code
04: Set Theory Definitions
Discussion Problems
Resources
Course Reader
Lecture Videos
Theorem and Definition Reference
Office Hours Schedule
Lectures
00: Set Theory



ments

ne Out

One goes out today. This problem set
proof techniques - direct proofs,
tradiction, and proofs by contrapositive
riety of examples. We hope that this
vill help you get used to writing
proofs!

Handouts

00: Course Information
01: Syllabus
02: Problem Set Policies
03: Honor Code
04: Set Theory Definitions

Discussion Problems

Resources

Course Reader
Lecture Videos
Theorem and Definition Reference
Office Hours Schedule

Lectures

00: Set Theory

Office hours start tomorrow.

Schedule available on the course website.

Friday Four Square

- Good snacks!
- Good company!
- Good game!
- Good fun!
- **Today at 4:15 in front of Gates.**

Outline for Today

- **Logical Implication**
  - What does "If P, then Q" mean?
- **Proof by Contrapositive**
  - The basic method.
  - An interesting application.
- **Proof by Contradiction**
  - The basic method.
  - Contradictions and implication.
  - Contradictions and quantifiers.

Logical Implication

Implications

- An **implication** is a statement of the form

  If *P*, then *Q*.

- When discussing implications in the abstract, we denote that P implies Q by writing $\boldsymbol{P \to Q}$.
- When $P \to Q$, we call P the **antecedent** and Q the **consequent**.

What Implication Means

- The statement $P \to Q$ means exactly the following:

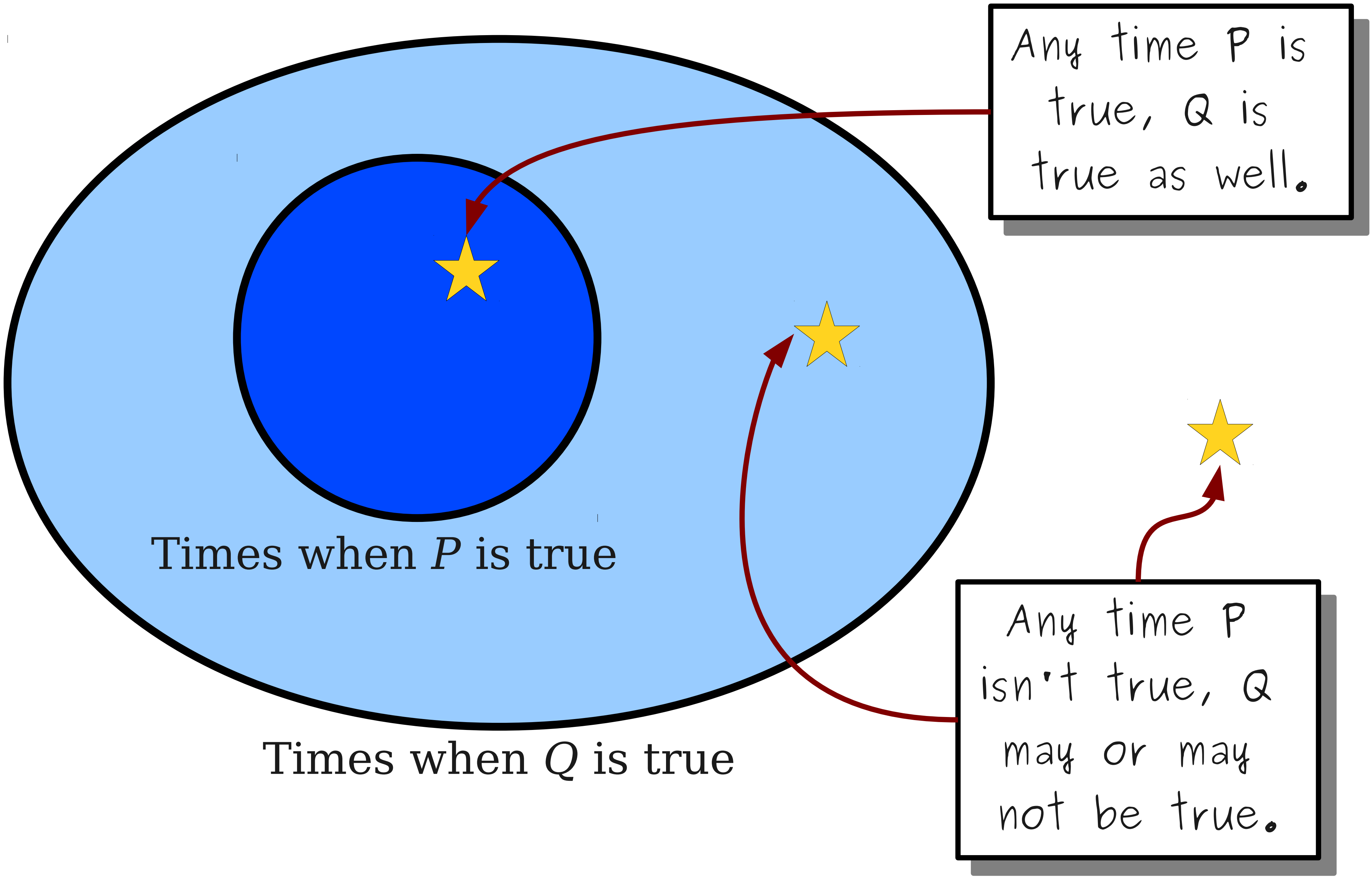
If P is true, then
Q must be true as well.

- For example:
  - n is an even integer $\to$ n^2 is an even integer.
  - $(A \subseteq B \text{ and } B \subseteq A) \to A = B$

What Implication Doesn't Mean

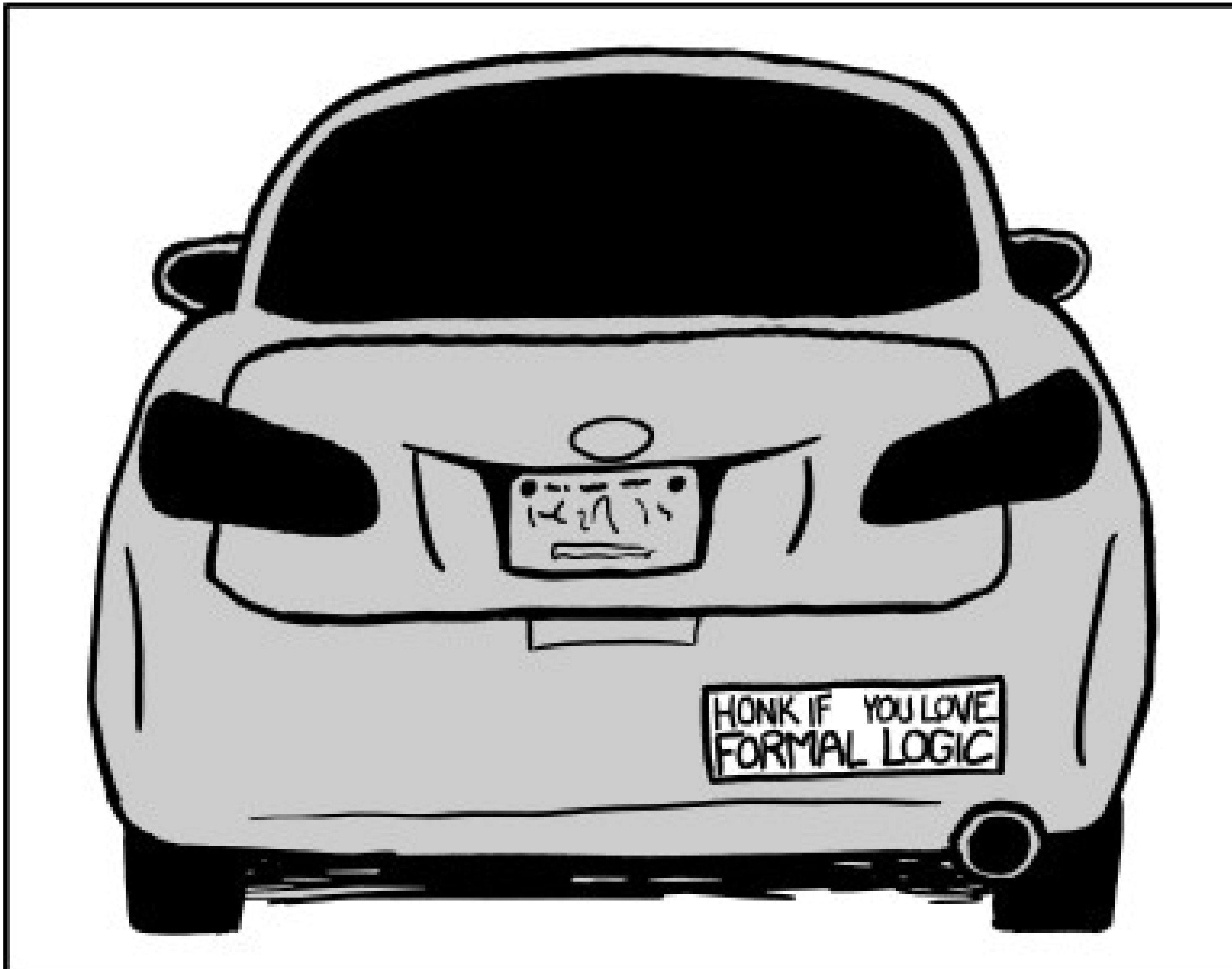
- $P \to Q$ ***doesn't*** mean that whenever Q is true, P is true.
  - "If you die in Canada, you die in real life" doesn't mean that if you die in real life, you die in Canada.
- $P \to Q$ ***doesn't*** say anything about what happens if P is false.
  - "If an animal is a puppy, you should hug it" doesn't mean that if that animal isn't a puppy, you shouldn't hug it.
  - **Vacuous truth:** If P is never true, then $P \to Q$ is always true.
- $P \to Q$ ***doesn't*** say anything about causality.
  - "If I like math, then $2 + 2 = 4$" is true because any time that I like make, $2 + 2 = 4$ is true.
  - "If I don't like math, then $2 + 2 = 4$" is also true, since whenever I don't like math, $2 + 2 = 4$ is true.

Implication, Diagrammatically



Proof by Contrapositive

Honk **If** You Love Formal Logic



Honk **If** You Love Formal Logic

Suppose that you're driving this car and you *don't* get honked at.

What can you say about the people driving behind you?

The Contrapositive

- The **contrapositive** of "If P, then Q" is the statement "If **not** Q, then **not** P."
- Example:
  - "If I stored the cat food inside, then the raccoons wouldn't have stolen my cat food."
  - Contrapositive: "If the raccoons stole my cat food, then I didn't store it inside."
- Another example:
  - "If you liked it, then you should have put a ring on it."
  - Contrapositive: "If you shouldn't have put a ring on it, then you didn't like it."

An Important Proof Strategy

To show that $P \rightarrow Q$, you may instead show that **not** $Q \rightarrow$ **not** P.

This is called a ***proof by contrapositive***.

An Important Proof Strategy

To show that $P \to Q$, you may instead show that $\neg Q \to \neg P$.

This is called a ***proof by contrapositive***.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; ???

If

n^2 is even

then

n is even

If

n is odd

then

n^2 is odd

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; **???**

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Therefore, there exists an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Therefore, there exists an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Thus n^2 is odd, as required.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Therefore, there exists an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Thus n^2 is odd, as required. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

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

Therefore, there exists an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Thus n^2 is odd, as required. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, $n = 2k + 1$ for some integer k. Then

$n^2 =$

$n^2 =$

$n^2 =$

There… m

(nam… $2m + 1$.

Thus n^2 is odd, as required. ■

Notice the structure of the proof. We begin by announcing that it's a proof by contrapositive, then state the contrapositive, and finally prove it.

Biconditionals

- Combined with what we saw on Wednesday, we have proven that, if n is an integer:

If n is even, then n^2 is even.

If n^2 is even, then n is even.

- Therefore, if n is an integer:

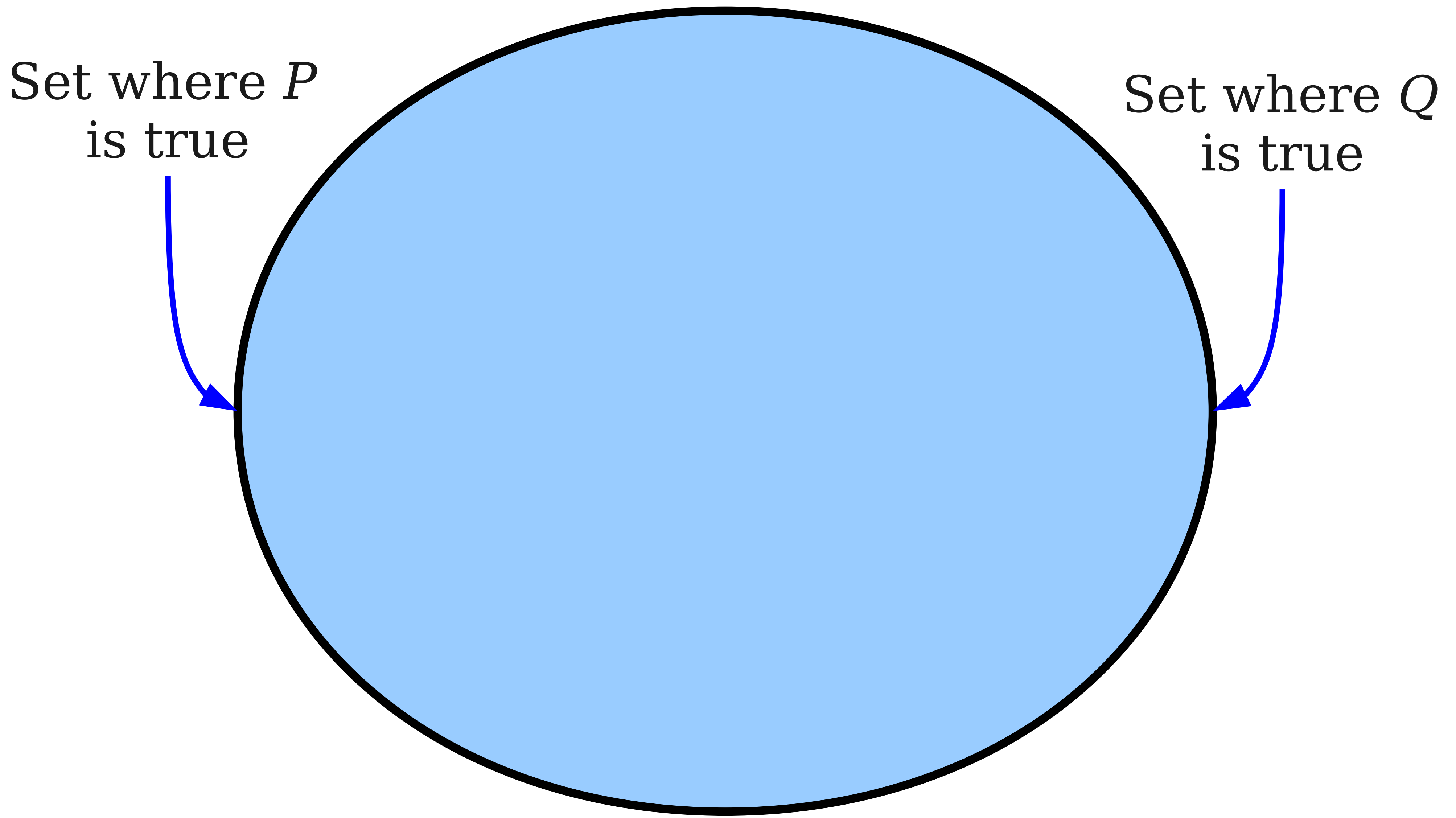
n is even if and only if n^2 is even.

- "If and only if" is often abbreviated **iff**:

n is even iff n^2 is even.

- This is called a **biconditional**.

P iff Q



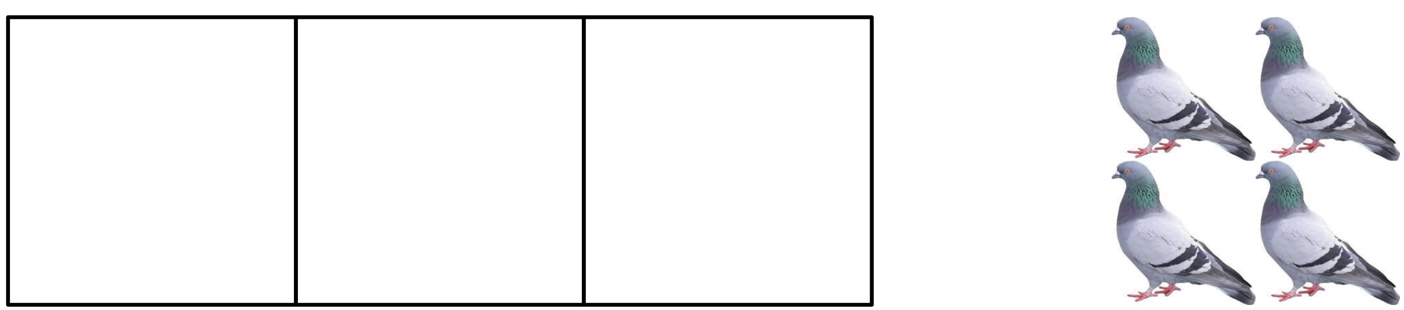
Proving Biconditionals

- To prove ***P* iff *Q***, you need to prove that *P* implies *Q* and that *Q* implies *P*.
- You can any proof techniques you'd like to show each of these statements.
  - In our case, we used a direct proof and a proof by contrapositive.

The Pigeonhole Principle

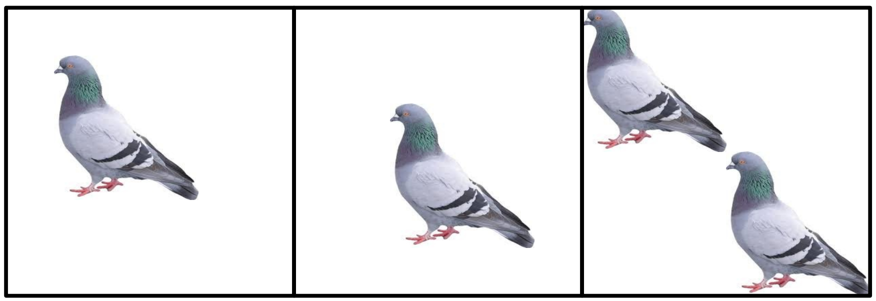
The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have $m > n$ pigeons.
- If you put the pigeons into the pigeonholes, some pigeonhole will have more than one pigeon in it.



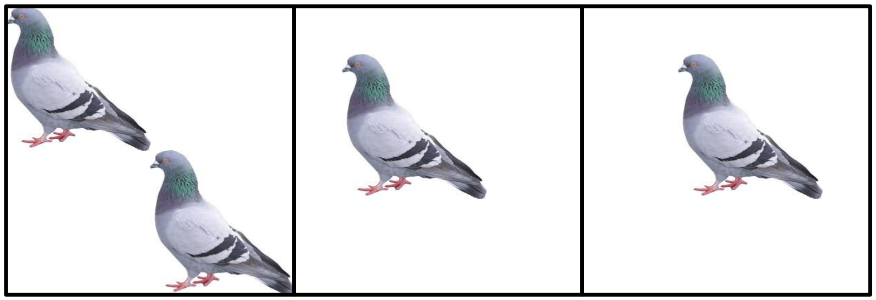
The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have $m > n$ pigeons.
- If you put the pigeons into the pigeonholes, some pigeonhole will have more than one pigeon in it.



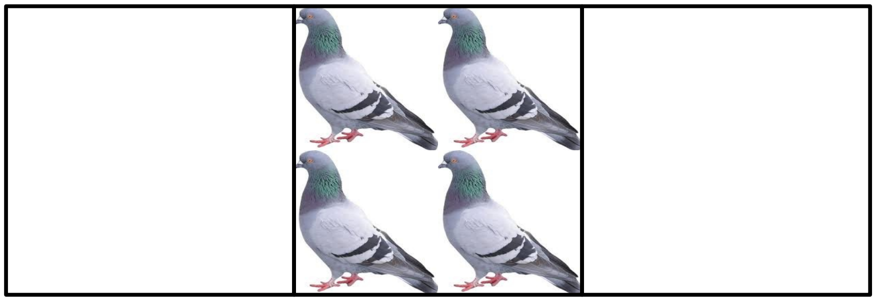
The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have $m > n$ pigeons.
- If you put the pigeons into the pigeonholes, some pigeonhole will have more than one pigeon in it.



The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have $m > n$ pigeons.
- If you put the pigeons into the pigeonholes, some pigeonhole will have more than one pigeon in it.



Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains at least two objects.

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains at least two objects.

Proof: By contrapositive;

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains at least two objects.

Proof: By contrapositive; **???**

If

$m > n$

then

there is some bin containing at least two objects

If

$m > n$

then

there is some bin containing at least two objects

If

$m > n$

then

there is some bin containing at least two objects

If

If

$m > n$

then

there is some bin containing at least two objects

If

every bin contains at most one object

If

$m > n$

then

there is some bin containing at least two objects

If

every bin contains at most one object

then

If

$m > n$

then

there is some bin containing at least two objects

If

every bin contains at most one object

then

$m \leq n$

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains at least two objects.

Proof: By contrapositive; we prove that if every bin contains at most one object, then $m \leq n$.

Let x_i be the number of objects in bin i. Since m is the number of total objects, we have that

$$m = x_1 + x_2 + \ldots + x_n$$

Since every bin has at most one object, $x_i \leq 1$ for all i. Thus

$$\begin{aligned} m &= x_1 + x_2 + \ldots + x_n \\ &\leq 1 + 1 + \ldots + 1 \qquad (n \text{ times}) \\ &= n \end{aligned}$$

So $m \leq n$, as required. ■

Using the Pigeonhole Principle

- The pigeonhole principle is an enormously useful lemma in many proofs.
  - We'll spend a full lecture on it in a few weeks.
- General structure of a pigeonhole proof:
  - Find m objects to distribute into n buckets, with $m > n$.
  - Using the pigeonhole principle, conclude that some bucket has at least two objects in it.
  - Use this conclusion to show the desired result.

Some Simple Applications

- Any group of 367 people must have a pair of people that share a birthday.
  - 366 possible birthdays (pigeonholes)
  - 367 people (pigeons)
- Two people in San Francisco have the exact same number of hairs on their head.
  - Maximum number of hairs ever found on a human head is no greater than 500,000.
  - There are over 800,000 people in San Francisco.
- Each day, two people in New York City drink the same amount of water, to the thousandth of a fluid ounce.
  - No one can drink more than 50 gallons of water each day.
  - That's 6,400 fluid ounces. This gives 6,400,000 possible numbers of thousands of fluid ounces.
  - There are about 8,000,000 people in New York City proper.

Some Words of Caution

An Incorrect Proof

Theorem: For any sets A and B, if $x \notin A \cap B$, then $x \notin A$.

An Incorrect Proof

Theorem: For any sets A and B,
if $x \notin A \cap B$, then $x \notin A$.

Proof: By contrapositive; we show that
if $x \in A \cap B$, then $x \in A$.

Since $x \in A \cap B$, $x \in A$ and $x \in B$.
Consequently, $x \in A$ as required. ■

An Incorrect Proof

Theorem: For any sets A and B,
if $x \notin A \cap B$, then $x \notin A$.

Proof: By contrapositive; we show that
if $x \in A \cap B$, then $x \in A$.

Since $x \in A \cap B$, $x \in A$ and $x \in B$.
Consequently, $x \in A$ as required. ■

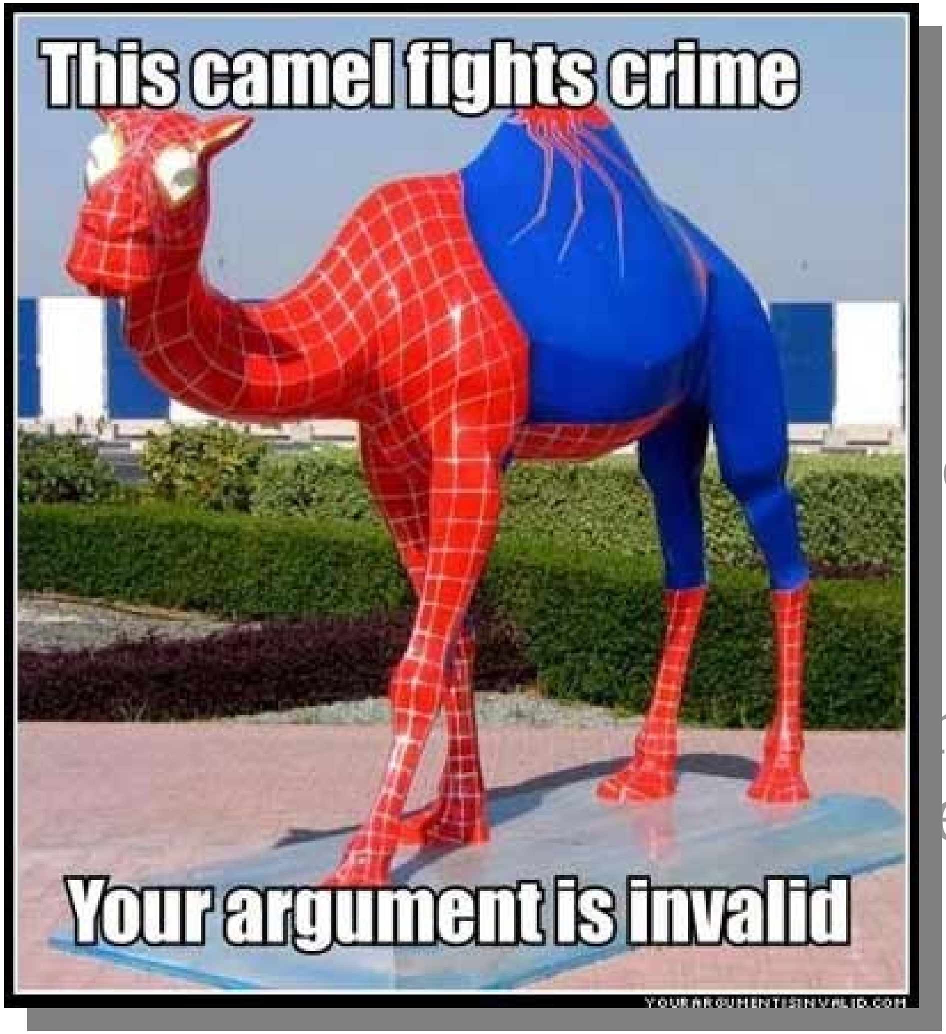
An Incorrect Proof

Theorem:

Proof: ow that

nd $x \in B$.

equired. ■



Common Pitfalls

To prove $P \to Q$ by contrapositive, prove

$$\boldsymbol{\neg Q \to \neg P}$$

Be careful not to prove

$$\boldsymbol{\neg P \to \neg Q}$$

Common Pitfalls

To prove $P \to Q$ by contrapositive, prove

$$\neg Q \to \neg P$$

Be careful not to prove

$$\neg P \to \neg Q$$

(Proving $\neg P \to \neg Q$ proves $Q \to P$, which isn't what you want!)

More Generally

- When doing a proof by contrapositive, your proof is only valid if you actually prove the contrapositive of the statement you want to prove.
- Make sure to set up the proof correctly; double- and triple-check you have taken the contrapositive correctly!
- This is true in general of most indirect proofs.

Proof by Contradiction

“When you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth.”

- Sir Arthur Conan Doyle, *The Adventure of the Blanched Soldier*

Proof by Contradiction

- A **proof by contradiction** is a proof that works as follows:
  - To prove that P is true, assume that P is not true.
  - Based on the assumption that P is not true, conclude something impossible.
  - Assuming the logic is sound, the only valid explanation is that the assumption that P is not true is incorrect.
  - Conclude, therefore, that P is true.

Theorem: There is no integer that is both even and odd.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; **??**

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = \frac{1}{2}$.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = \frac{1}{2}$. Since r and s are integers, their difference is an integer.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = ½$. Since r and s are integers, their difference is an integer. But this is impossible, since ½ is not an integer.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = ½$. Since r and s are integers, their difference is an integer. But this is impossible, since ½ is not an integer.

We have reached a contradiction, so our assumption must have been wrong.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = ½$. Since r and s are integers, their difference is an integer. But this is impossible, since ½ is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd.

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = \frac{1}{2}$. Since r and s are integers, their difference is an integer. But this is impossible, since ½ is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. Since k is odd, there is some $s \in \mathbb{Z}$ such that $k = 2s + 1$.

Therefore, $2r = 2s + 1$, so $2r - 2s = 1$ and therefore $r - s = ½$. Since r and s are integers, their difference is an integer. But this is impossible, since ½ is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Theorem: There is no integer that is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

The three key pieces:

1. State that the proof is by contradiction.
2. State what you are assuming is the negation of the statement to prove.
3. State you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Rational and Irrational Numbers

Rational and Irrational Numbers

- A **rational number** is a number r that can be written as

$$r = \frac{p}{q}$$

  where p and q are integers and $q \neq 0$.

- A number that is not rational is called **irrational**.
- Useful theorem: If r is rational, r can be written as p / q where $q \neq 0$ and where p and q have no common factors other than ± 1.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.
Proof: By contradiction;

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.
Proof: By contradiction; **???**

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.
Proof: By contradiction; assume $\sqrt{2}$ is rational.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\,q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\,q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2$

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2$

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.
Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\,q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even. But this means that both p and q have 2 as a common divisor.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even. But this means that both p and q have 2 as a common divisor. This contradicts our earlier assertion that their only common divisors are 1 and -1.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even. But this means that both p and q have 2 as a common divisor. This contradicts our earlier assertion that their only common divisors are 1 and -1.

We have reached a contradiction, so our assumption was incorrect.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\,q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even. But this means that both p and q have 2 as a common divisor. This contradicts our earlier assertion that their only common divisors are 1 and -1.

We have reached a contradiction, so our assumption was incorrect. Consequently, $\sqrt{2}$ is irrational.

A Famous and Beautiful Proof

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction; assume $\sqrt{2}$ is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{2}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}\, q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even. But this means that both p and q have 2 as a common divisor. This contradicts our earlier assertion that their only common divisors are 1 and -1.

We have reached a contradiction, so our assumption was incorrect. Consequently, $\sqrt{2}$ is irrational. ■

A Famous and Beautiful Proof

Theorem: √2 is irrational.

Proof: By contradiction; assume √2is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{}$, and p and q have no common divisors other than 1 and -1.

Since $p / q = \sqrt{2}$ and $q \neq 0$, we have $p = \sqrt{2}q$, so $p^2 = 2q^2$.

Since q^2 is an integer and $p^2 = 2q^2$, we have that p^2 is even. By our earlier result, since p^2 is even, we know p is even. Thus there is an integer k such that $p = 2k$.

Therefore, $2q^2 = p^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$.

Since k^2 is an integer and $q^2 = 2k^2$, we know q^2 is even. By our earlier result, since q^2 is even, we have that q is even. But this means that both p and q have 2 as a common divisor. This contradicts our earlier assertion that their only common divisors are 1 and -1.

We have reached a contradiction, so our assumption was incorrect. Consequently, √2 is irrational. ■

A Famous and Beautiful Proof

Theorem: √2 is irrational.

Proof: By contradiction; assume √2is rational. Then there exists integers p and q such that $q \neq 0$, $p / q = \sqrt{}$, and p and q have no common divisors other than 1 and -1.

The three key pieces:

1. State that the proof is by contradiction.
2. State what you are assuming is the negation of the statement to prove.
3. State you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

divisors are 1 and -1.

We have reached a contradiction, so our assumption was incorrect. Consequently, √2 is irrational. ■

Vi Hart on Pythagoras and the Square Root of Two:

http://www.youtube.com/watch?v=X1E7I7_r3Cw

A Word of Warning

- To attempt a proof by contradiction, make sure that what you're assuming actually is the opposite of what you want to prove.
- Otherwise, the core logic of your proof will be incorrect.
- Also true in proofs by contrapositive, but can be a lot more subtle in proofs by contradiction.

Negations of Standard Statements

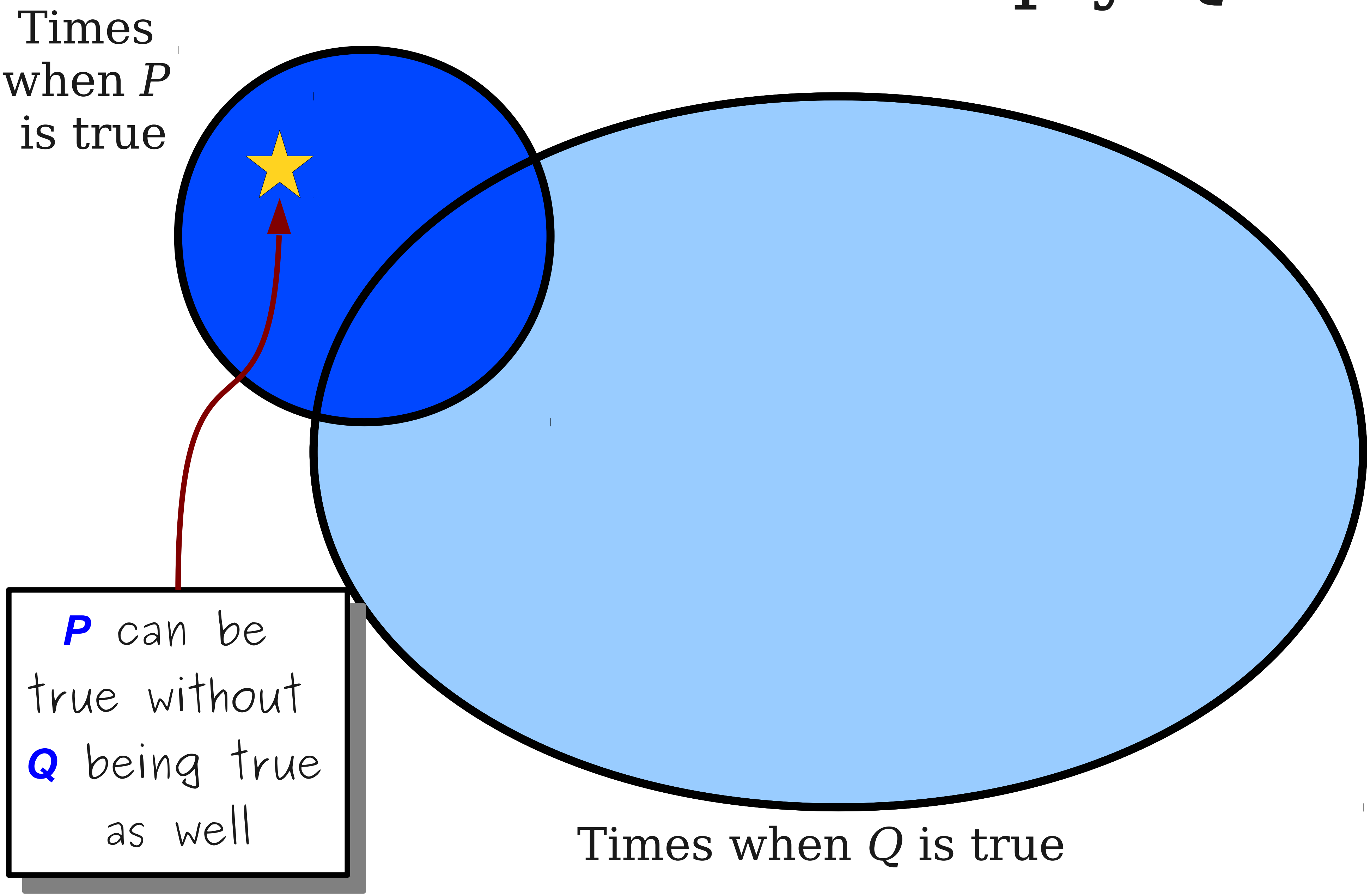
- It's good to know how to negate three general types of statements:
  - **Implications:** "If P, then Q."
  - **Universal statements:** "For all x, P(x) is true."
  - **Existential statements:** "There exists an x where P(x) is true."
- Let's quickly go over how to prove these statements by contradiction.

Negating Implications

When P Doesn't Imply Q

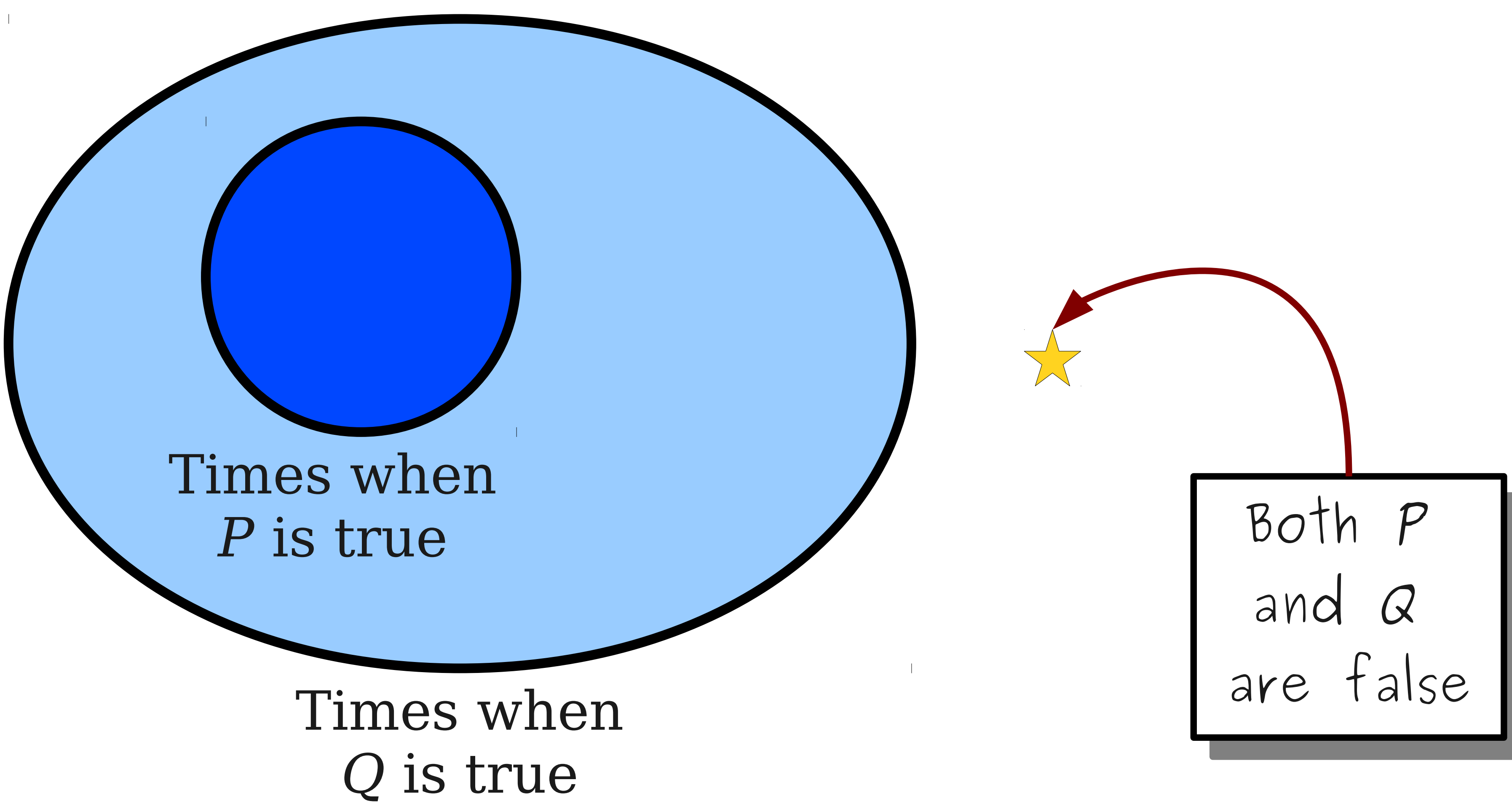
- Recall: What does “If P, then Q” mean?
  - **Answer**: If P is true, then Q is true as well.
- When will “If P, then Q” be false?
  - **Answer**: P is true, but Q is false.
- The only way to disprove that P implies Q is to show that there is some way for P to be true and Q to be false.

When P Doesn't Imply Q



A Common Mistake

- To show that $P \to Q$ is false, it is not sufficient to find a case where P is false and Q is false.



Contradictions and Implications

- Suppose we want to prove that $P \to Q$ is true by contradiction.
- The proof will look something like this:
  - Assume that $P \to Q$ is false.
  - Using this assumption, derive a contradiction.
  - Conclude that $P \to Q$ must be true.

Contradictions and Implications

Suppose we want to prove that $P \to Q$ is true by contradiction.

The proof will look something like this:

- Assume that $P \to Q$ is false.

  Using this assumption, derive a contradiction.

  Conclude that $P \to Q$ must be true.

Contradictions and Implications

Suppose we want to prove that $P \to Q$ is true by contradiction.

The proof will look something like this:

- Assume that P is true and Q is false.

  Using this assumption, derive a contradiction.

  Conclude that $P \to Q$ must be true.

Contradictions and Implications

- Suppose we want to prove that $P \to Q$ is true by contradiction.
- The proof will look something like this:
  - Assume that P is true and Q is false.
  - Using this assumption, derive a contradiction.
  - Conclude that $P \to Q$ must be true.

A Simple Proof by Contradiction

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

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction;

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; **???**

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

A Simple Proof by Contradiction

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

Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Then $n^2 = (2k + 1)^2$

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

A Simple Proof by Contradiction

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

Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is impossible, since n^2 is even.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false. Thus if n is an integer and n^2 is even, n is even as well.

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false. Thus if n is an integer and n^2 is even, n is even as well. ■

A Simple Proof by Contradiction

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

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

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false. Thus if n is an integer and n^2 is even, n is even as well. ■

A Simple Proof by Contradiction

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

Proof: By contradiction; assume n is an integer and n^2 is even, but that n is odd.

The three key pieces:

1. State that the proof is by contradiction.
2. State what the negation of the original statement is.
3. State you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

We have reached a contradiction, so our assumption was false. Thus if n is an integer and n^2 is even, n is even as well. ■

Negating Existential and Universal Statements

An Incorrect Proof

Theorem: For any natural number n, the sum of all natural numbers less than n is not equal to n.

Proof: By contradiction; assume that for any natural number n, the sum of all smaller natural numbers is equal to n. But this is clearly false, because $5 \neq 1 + 2 + 3 + 4 = 10$. We have reached a contradiction, so our assumption was false and the theorem must be true. ■

An Incorrect Proof

Theorem: For any natural number n, the sum of all natural numbers less than n is not equal to n.

Proof: By contradiction; assume that for any natural number n, the sum of all smaller natural numbers is equal to n. But this is clearly false, because $5 \neq 1 + 2 + 3 + 4 = 10$. We have reached a contradiction, so our assumption was false and the theorem must be true. ■

An Incorrect Proof

Theorem: For any natural number *n*, the sum of all natural numbers less than *n* is not equal to *n*.

Proof: By contradiction; assume that for any natural number *n*, the sum of all smaller natural numbers is equal to *n*. But this is clearly false, because $5 \neq 1 + 2 + 3 + 4 = 10$. … contradiction, so our ass… the theorem must be true. ■

Is this *really* the negation of the original statement?

The negation of the universal statement

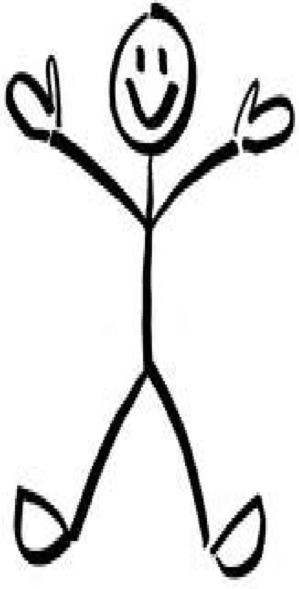
For all *x*, P(*x*) is true.

is **not**

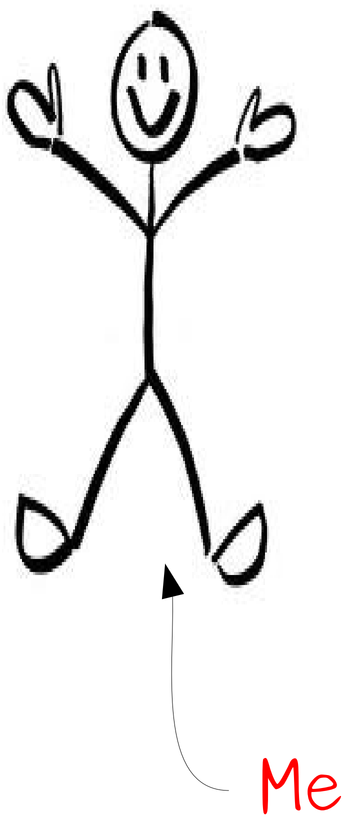
For all *x*, P(*x*) is false.

“All My Friends Are Taller Than Me”

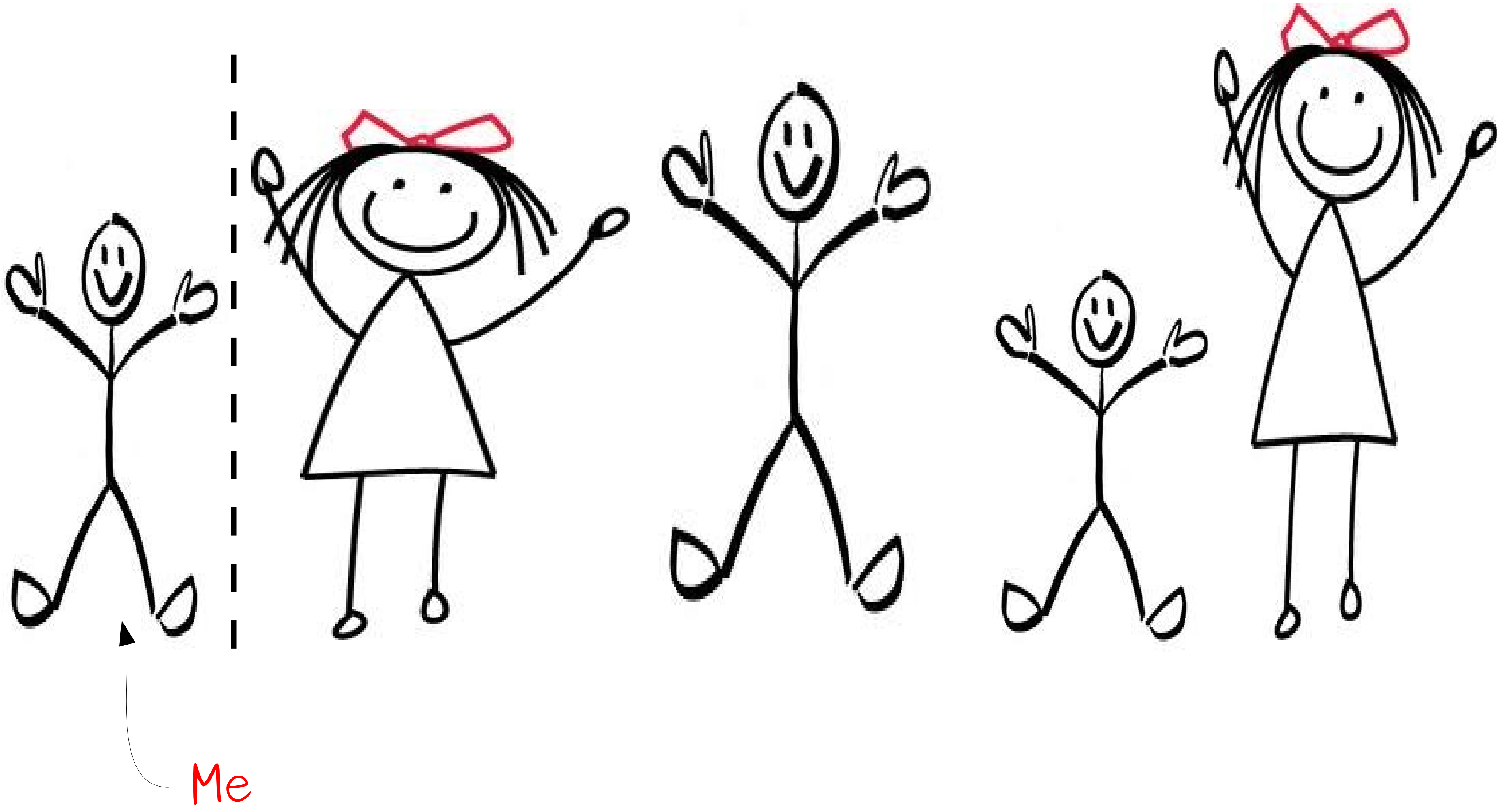
“All My Friends Are Taller Than Me”



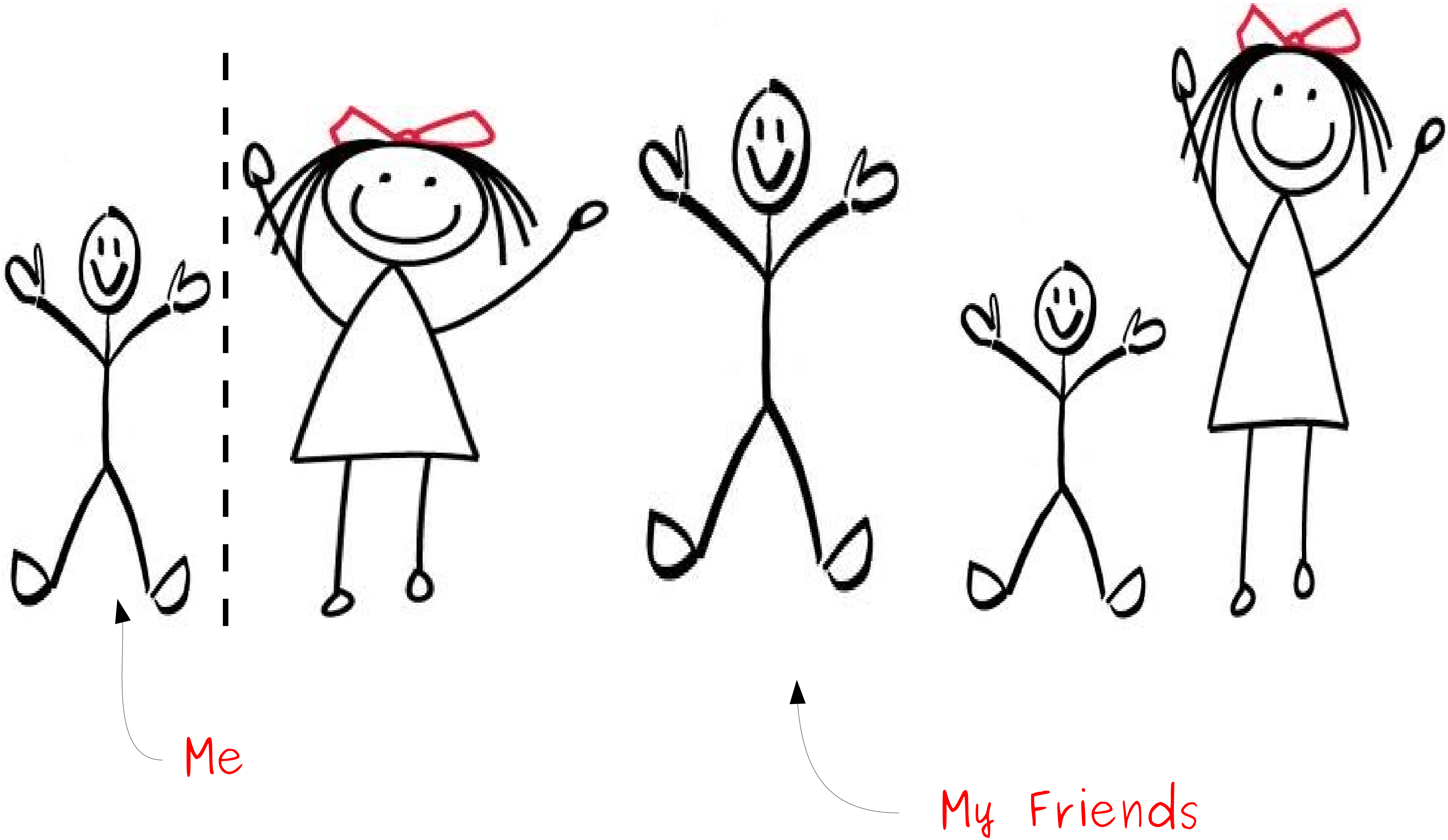
“All My Friends Are Taller Than Me”



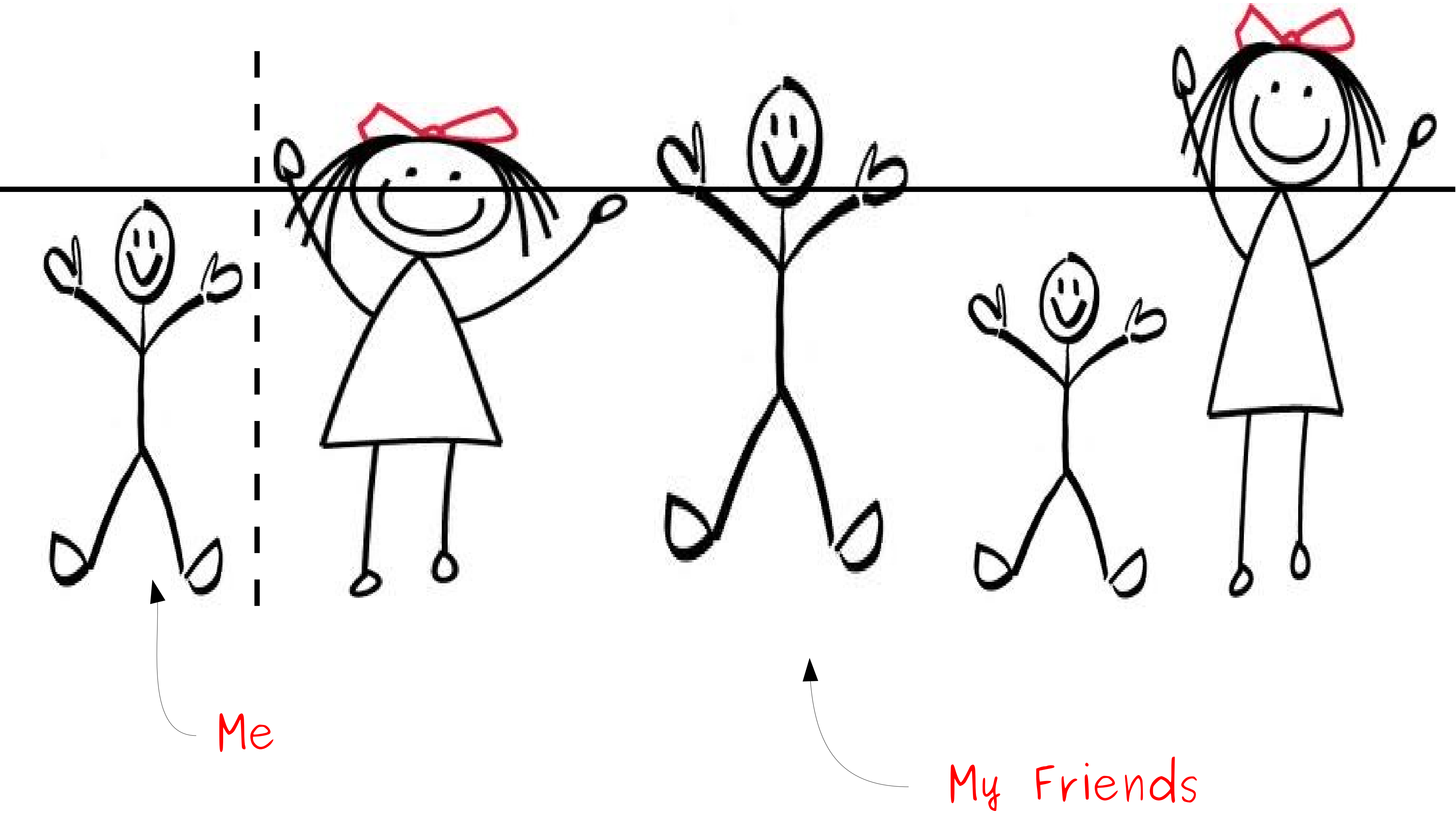
"All My Friends Are Taller Than Me"



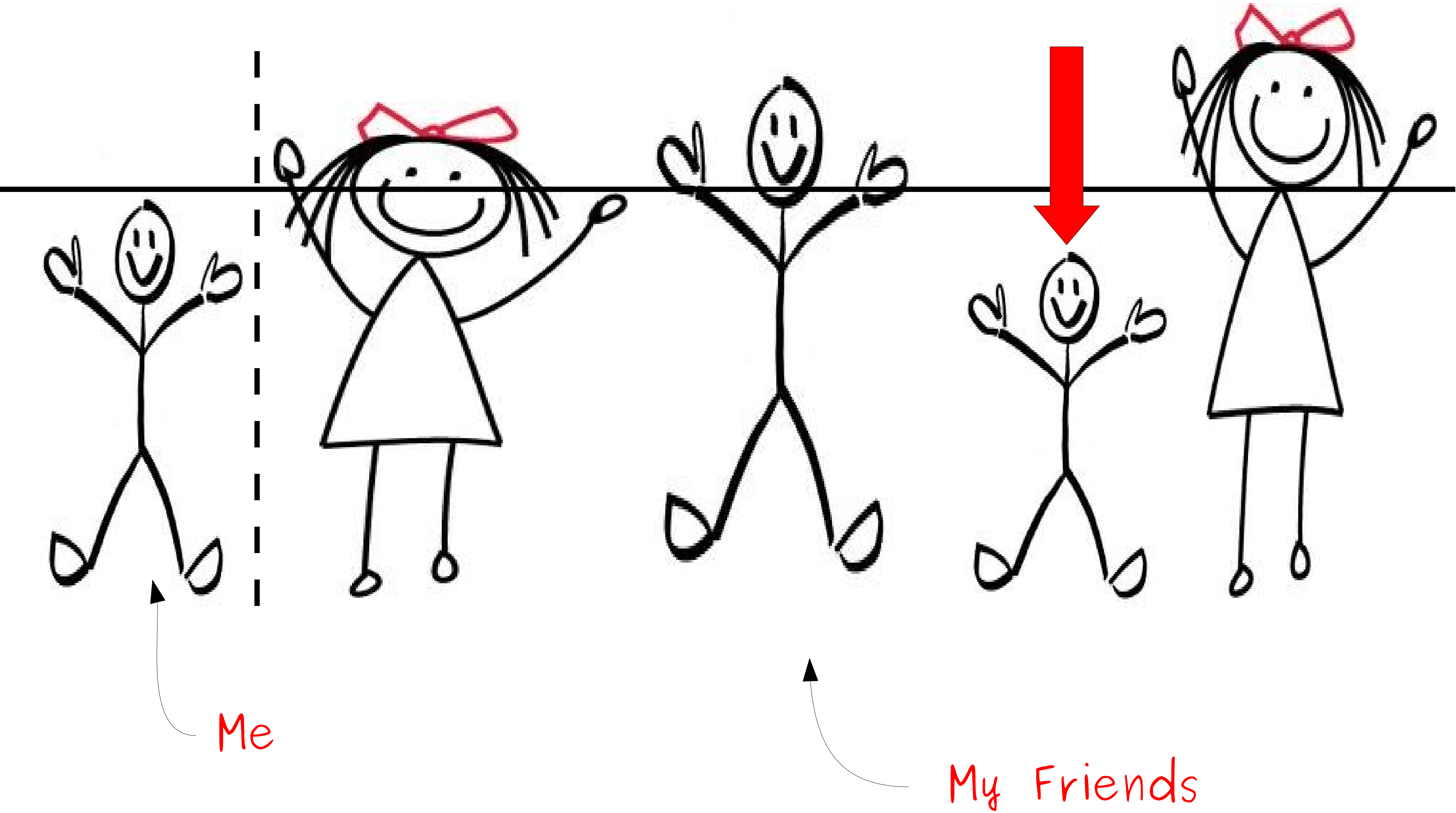
"All My Friends Are Taller Than Me"



“All My Friends Are Taller Than Me”



"All My Friends Are Taller Than Me"



The negation of the universal statement

For all *x*, P(*x*) is true.

is the existential statement

There exists an *x* such that P(*x*) is false.

The negation of the universal statement

For all *x*, P(*x*) is true.

is the existential statement

There exists an *x* such that P(*x*) is false.

For all natural numbers n,
the sum of all natural numbers
smaller than n is not equal to n.

For all natural numbers n,
the sum of all natural numbers
smaller than n is not equal to n.

For all natural numbers n,
the sum of all natural numbers
smaller than n is not equal to n.

becomes

For all natural numbers *n*,
the sum of all natural numbers
smaller than *n* is not equal to *n*.

becomes

There exists a natural number *n* such that
“the sum of all natural numbers
smaller than *n* ***is not*** equal to *n*”
is false.

For all natural numbers *n*,
the sum of all natural numbers
smaller than *n* is not equal to *n*.

becomes

There exists a natural number *n* such that
the sum of all natural numbers
smaller than *n* ***is*** equal to *n*

An Incorrect Proof

Theorem: For any natural number n, the sum of all natural numbers less than n is not equal to n.

Proof: By contradiction; assume that for any natural number n, the sum of all smaller natural numbers is equal to n. But this is clearly false, because $5 \neq 1 + 2 + 3 + 4 = 10$. We have reached a contradiction, so our assumption was false and the theorem must be true. ■

An Incorrect Proof

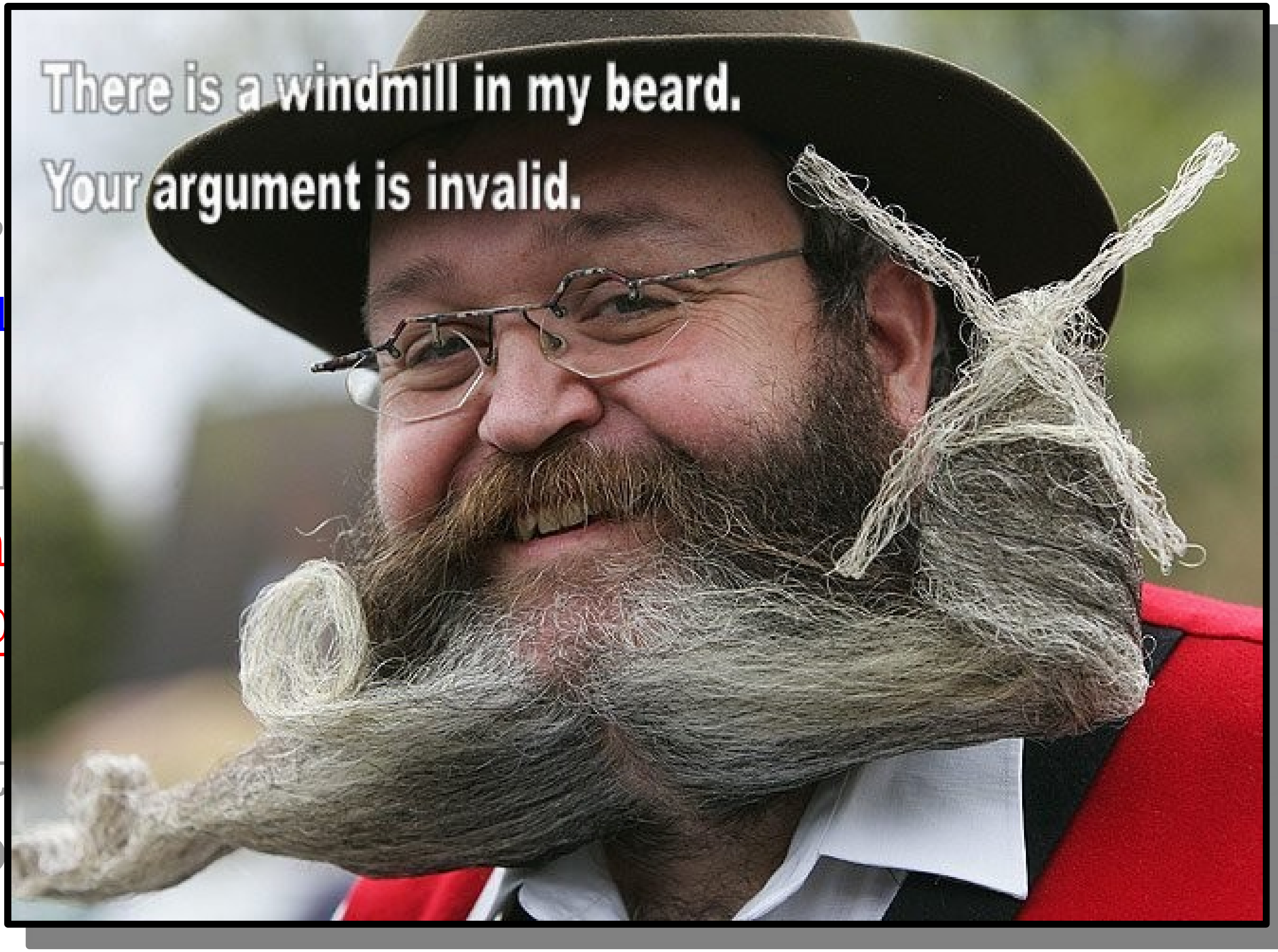
Theorem: For any natural number n, the sum of all natural numbers less than n is not equal to n.

Proof: By contradiction; assume that for any natural number n, the sum of all smaller natural numbers is equal to n. But this is clearly false, because $5 \neq 1 + 2 + 3 + 4 = 10$. We have reached a contradiction, so our assumption was false and the theorem must be true. ■

An Incorrect Proof

Theore of all
natu n.

Proof: natural
num umbers
is eq use
$5 \neq$ a
cont and the
theo



The negation of the existential statement

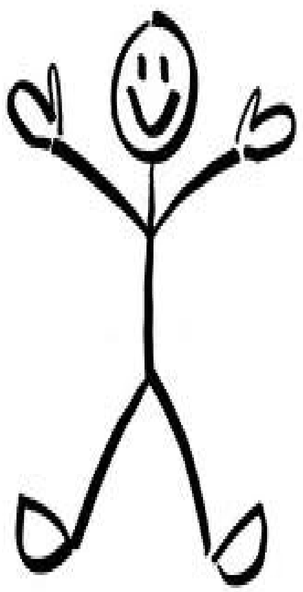
There exists an *x* such that P(*x*) is true.

is **not**

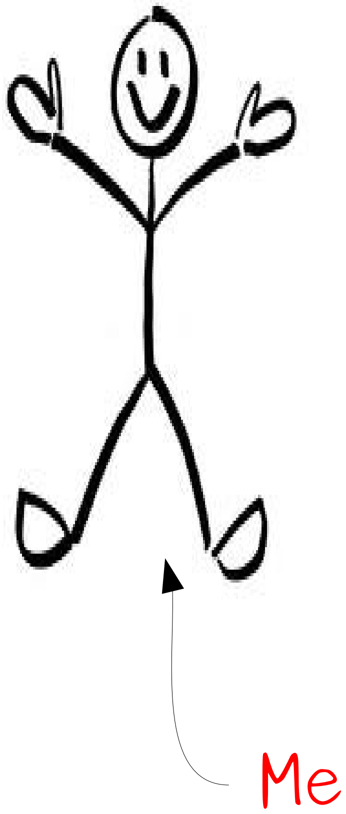
There exists an *x* such that P(*x*) is false.

“Some Friend Is Shorter Than Me”

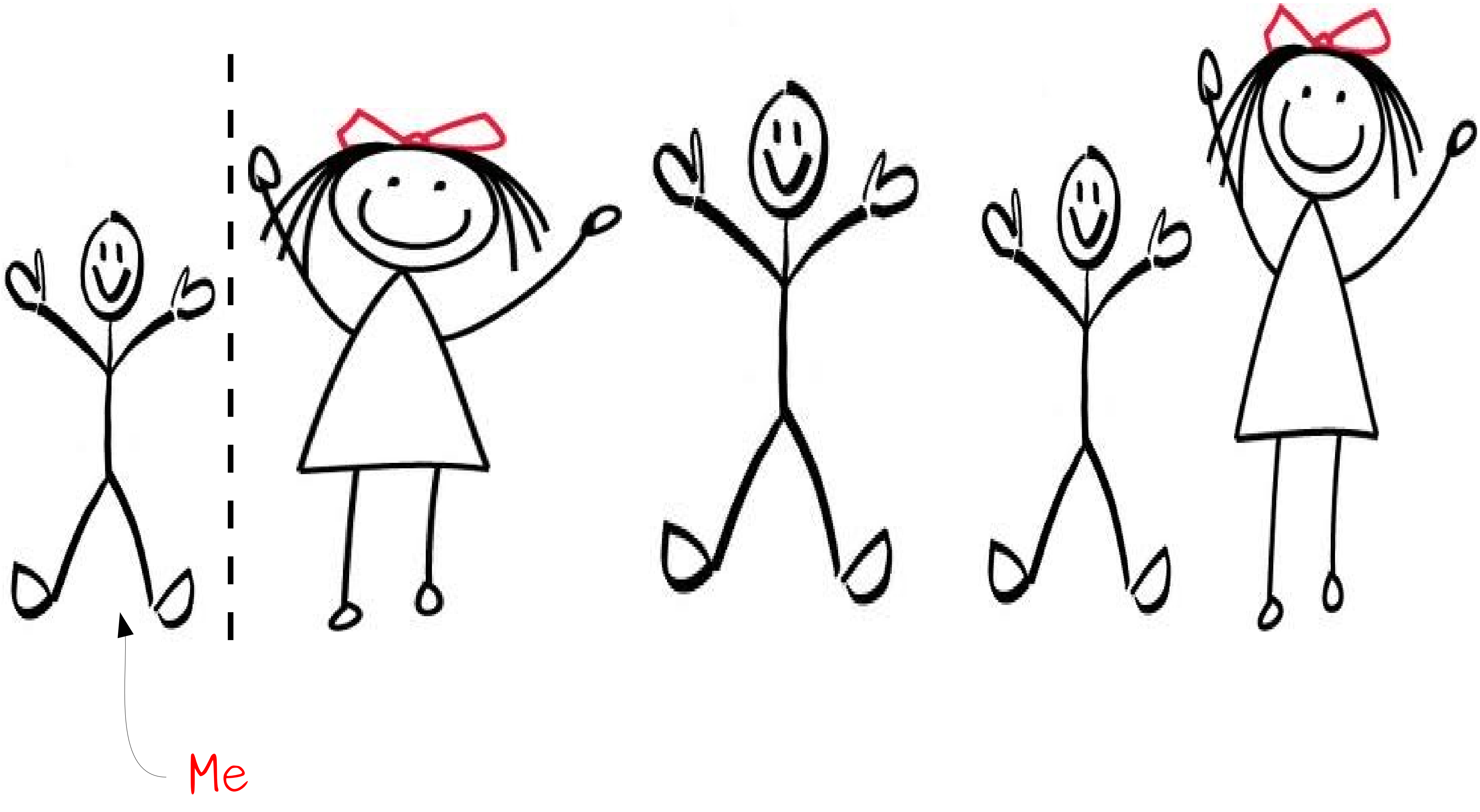
“Some Friend Is Shorter Than Me”



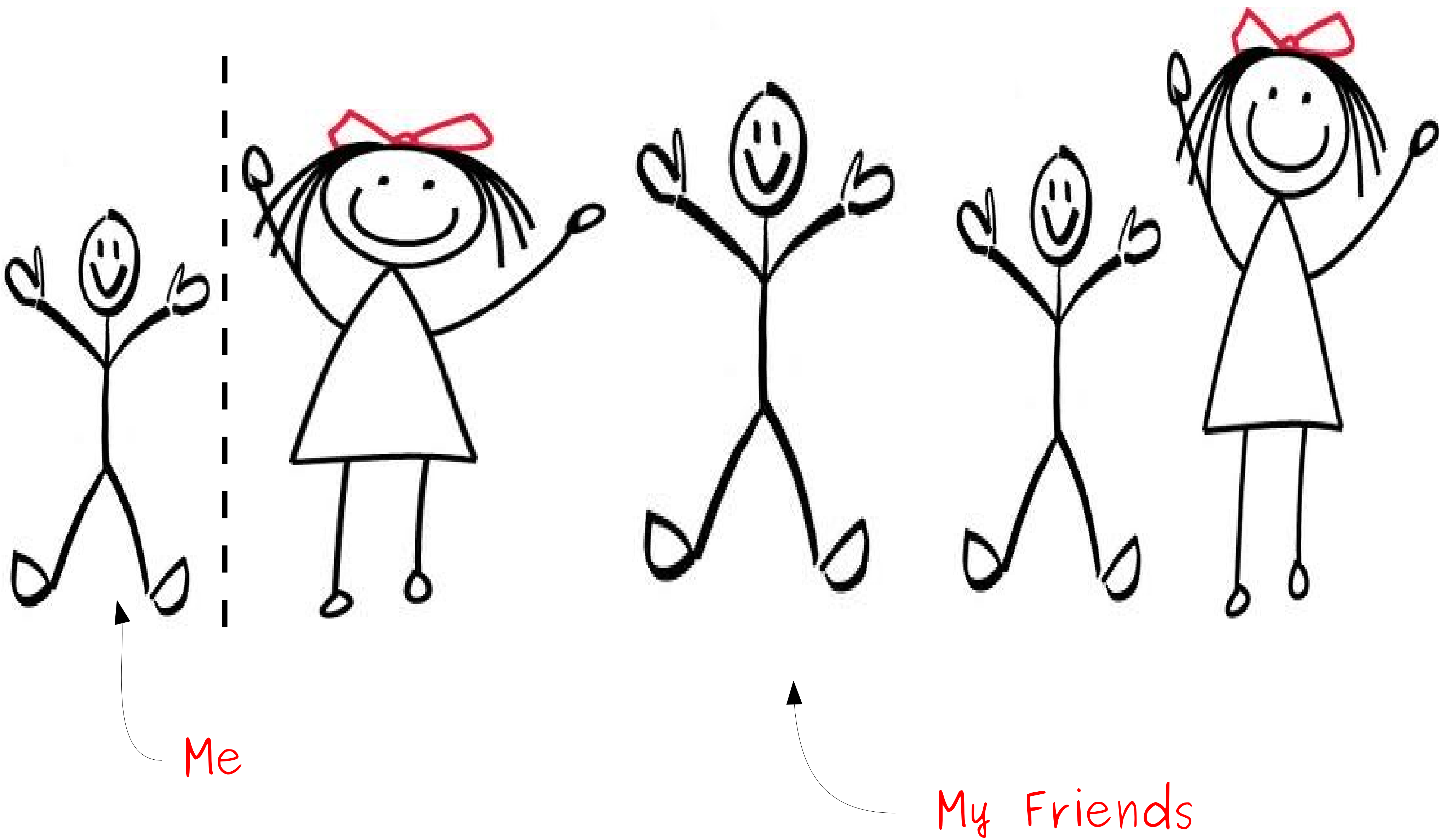
“Some Friend Is Shorter Than Me”



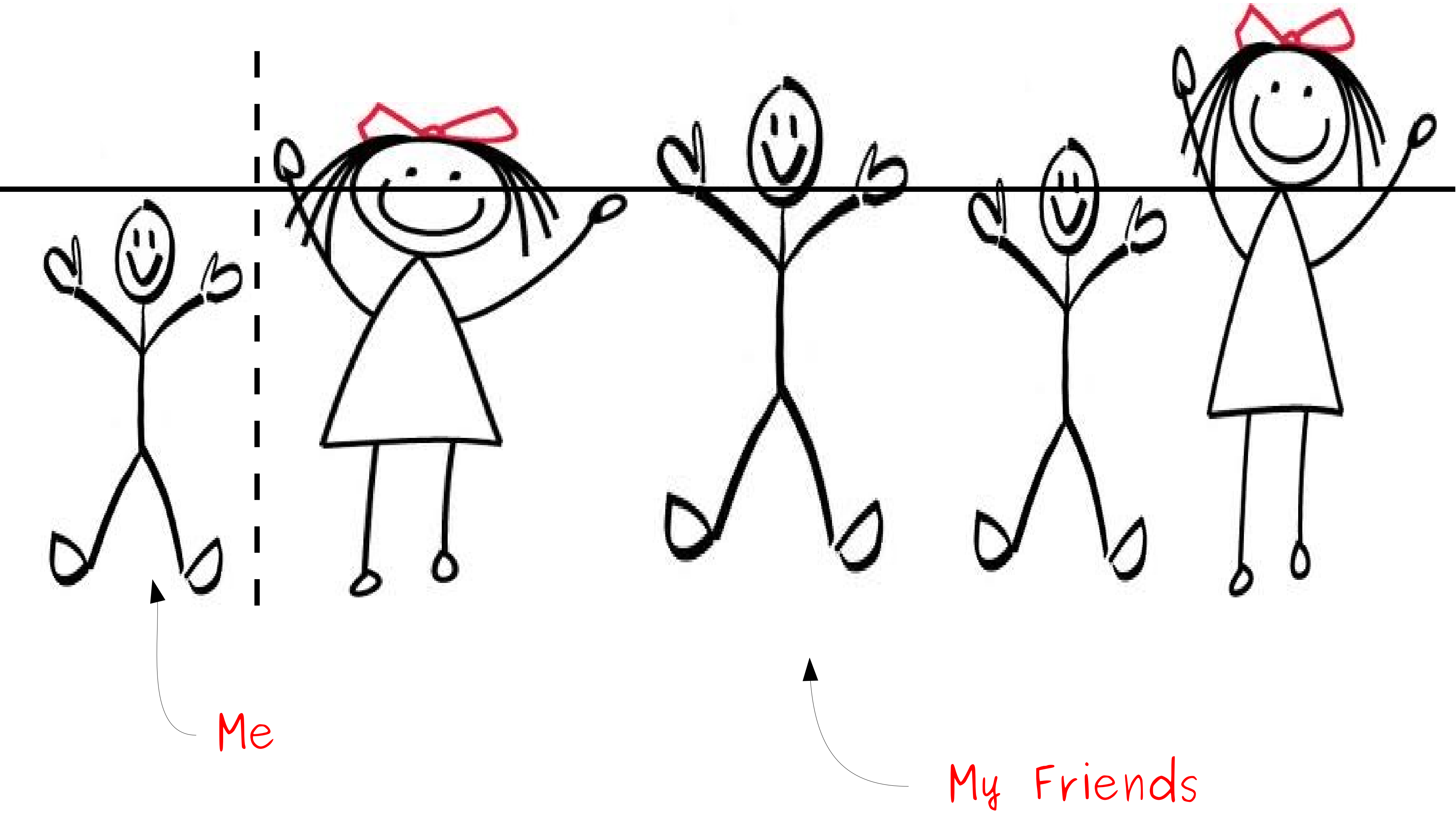
“Some Friend Is Shorter Than Me”



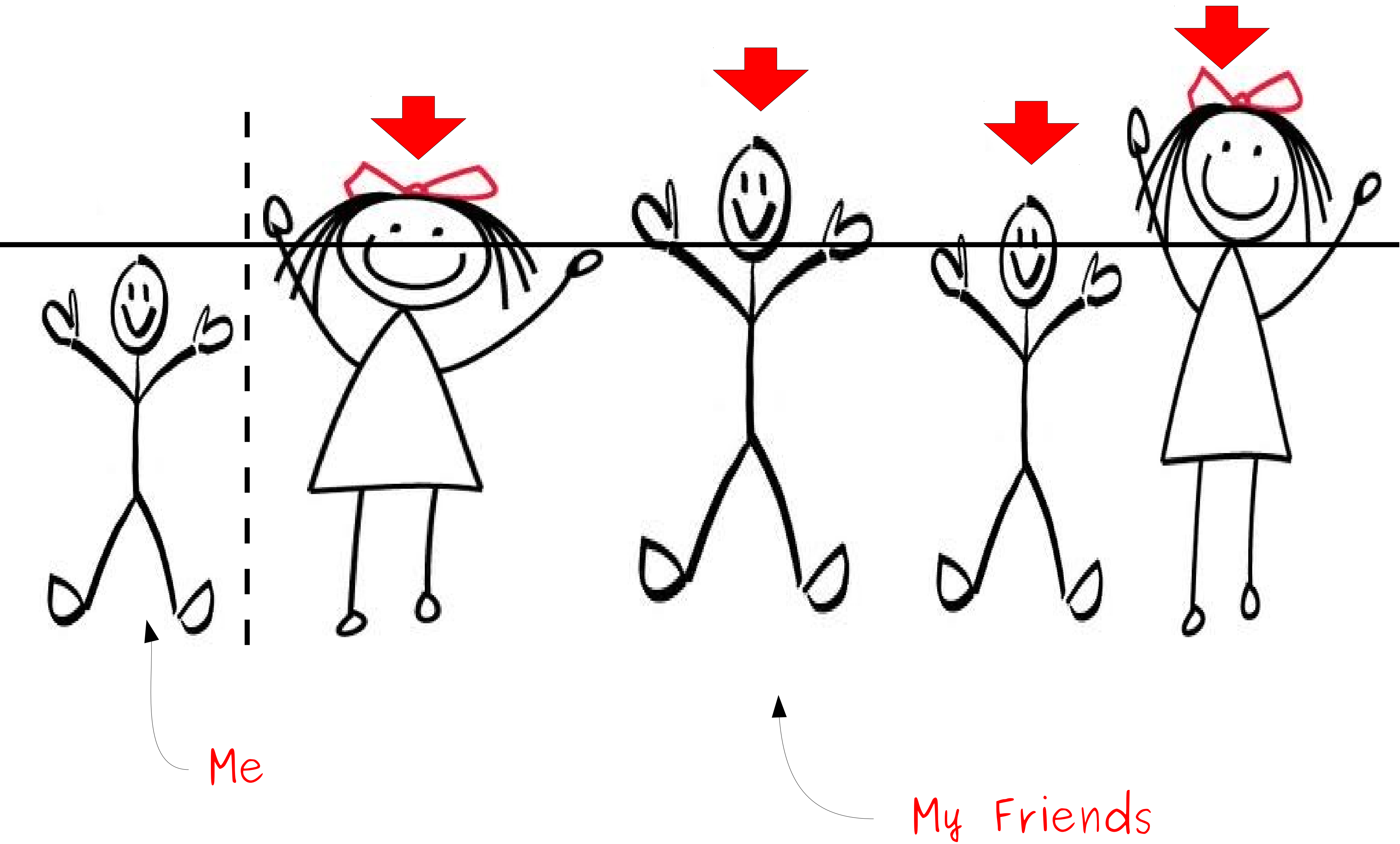
“Some Friend Is Shorter Than Me”



“Some Friend Is Shorter Than Me”



“Some Friend Is Shorter Than Me”



The negation of the existential statement

There exists an *x* such that P(*x*) is true.

is the universal statement

For all *x*, P(*x*) is false.

The negation of the existential statement

There exists an *x* such that P(*x*) is true.

is the universal statement

For all *x*, P(*x*) is false.

Negating Implications

"If *P*, then *Q*"

becomes

"*P* but not *Q*"

Negating Universal Statements

"For all *x*, P(*x*) is true"

becomes

"There is an *x* where P(*x*) is false."

Negating Existential Statements

"There exists an *x* where P(*x*) is true"

becomes

"For all *x*, P(*x*) is false."

Next Time

- **Proof by Induction**
  - Proofs on sums, programs, algorithms, etc.