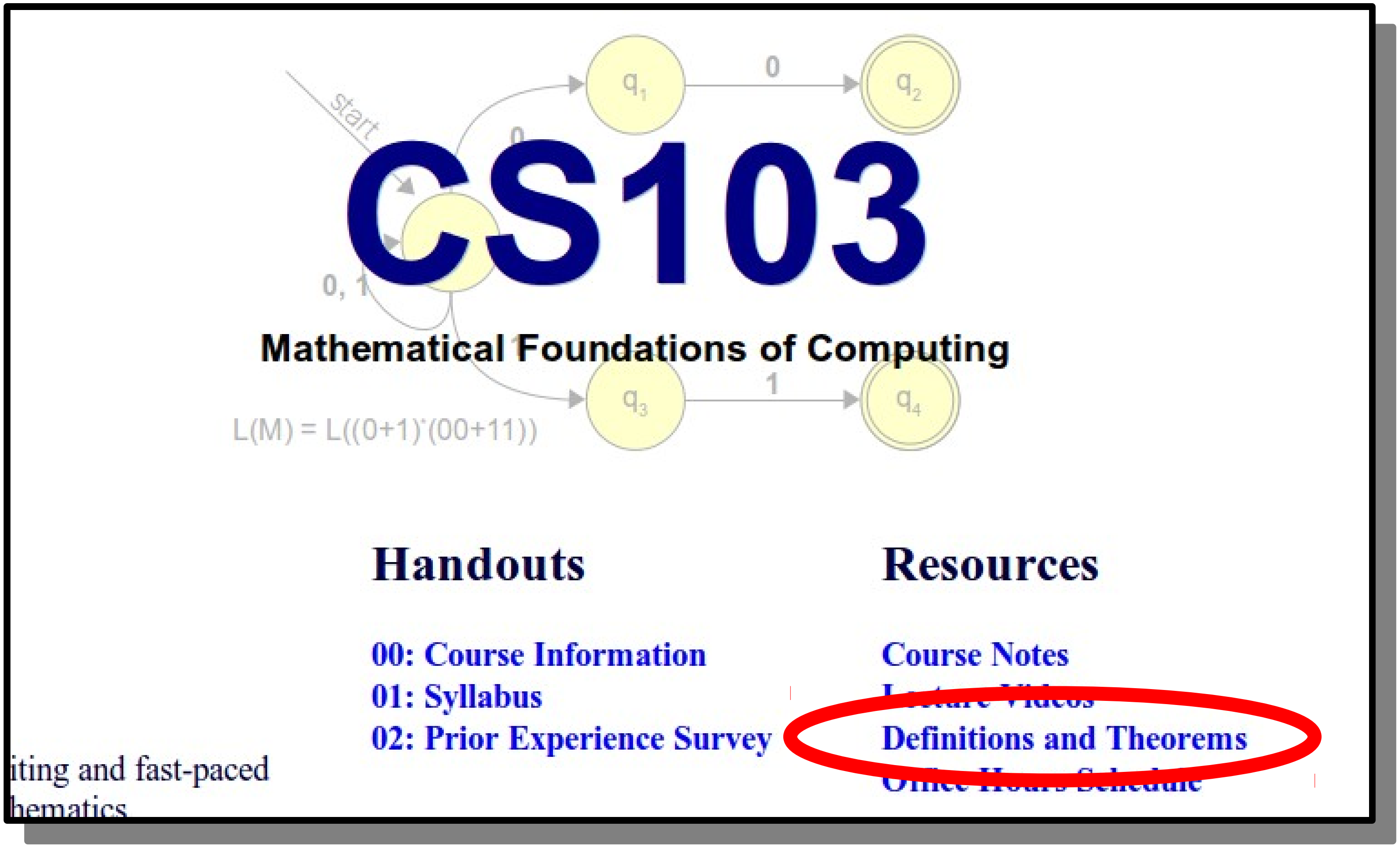
Indirect Proofs

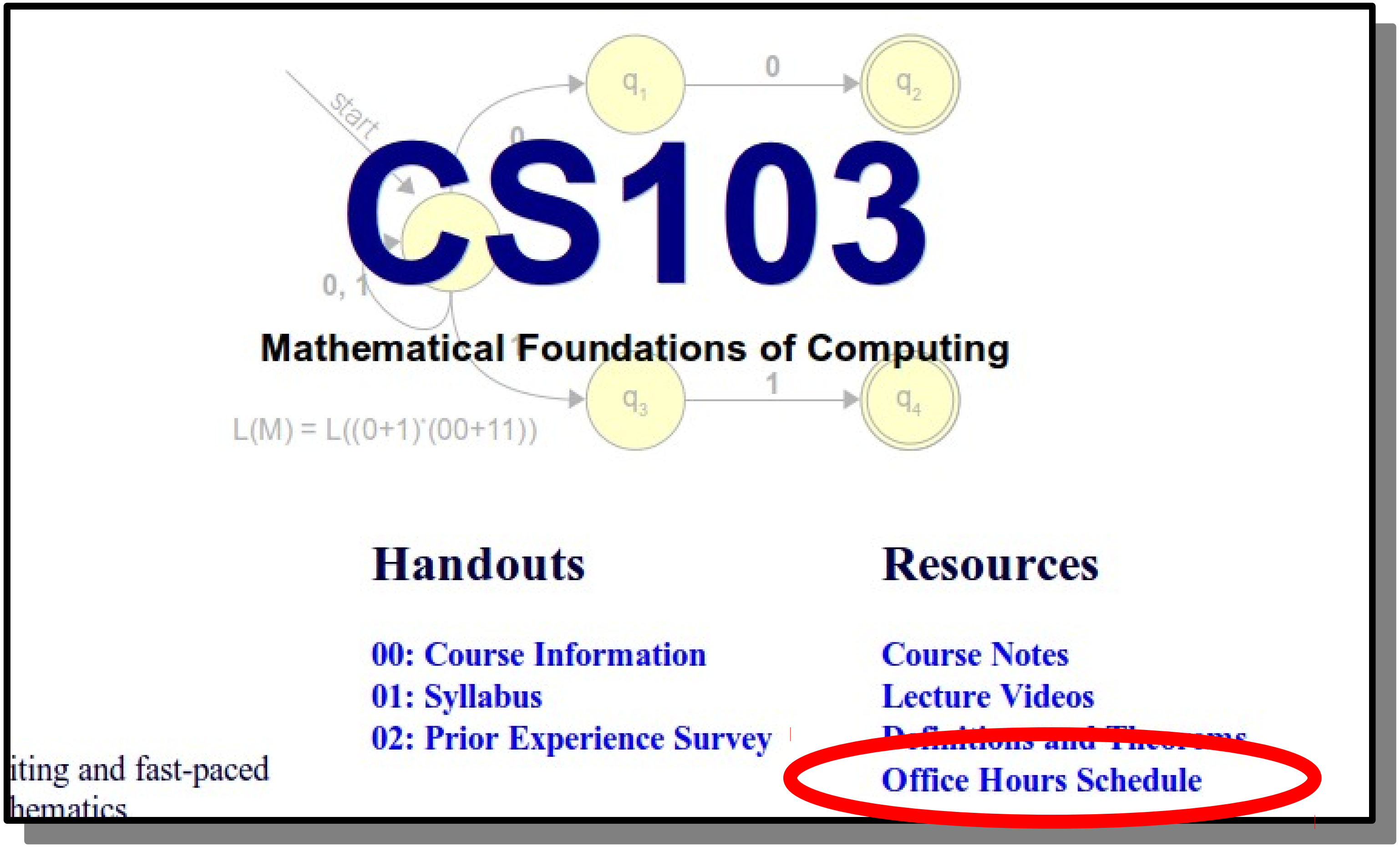
Announcements

- Problem Set 1 out.
- **Checkpoint** due Monday, January 14.
  - Graded on a "did you turn it in?" basis.
  - 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, January 18.
  - 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-win1213-submissions@lists.stanford.edu and attaching your solution as a PDF. (Please don't email the staff list directly with submissions).
- Late policy:
  - Three 72-hour “late days.”
  - Can use at most one per assignment.
  - No work accepted more than 72 hours after due date.


CS103
Mathematical Foundations of Computing
L(M) = L((0+1)*(00+11))
Handouts
00: Course Information
01: Syllabus
02: Prior Experience Survey
Resources
Course Notes
Definitions and Theorems
iting and fast-paced
hematics


start
0
0
0, 1
1
1
L(M) = L((0+1)*(00+11))
CS103
Mathematical Foundations of Computing
Handouts
00: Course Information
01: Syllabus
02: Prior Experience Survey
Resources
Course Notes
Lecture Videos
Office Hours Schedule
iting and fast-paced
hematics

Office hours start Monday.

Schedule available on the course website.

Recitation Sections

- Some office hours times are marked as recitation sections.
- Discussion problems distributed each week.
- Stop by recitation sections to work through them and learn how to attack different types of problems.

Friday Four Square

Don't be this guy!

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

Prior Experience Survey

- We have a prior experience survey to get a better sense of everyone's background.
- Optional, but would be really useful for tailoring the course.

Outline for Today

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

Logical Implication

Implications

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

  If P, then Q.

- We write "If P, then Q" as $P \to Q$.
  - Read: "P implies Q."
- When $P \to Q$, we call P the **antecedent** and Q the **consequent**.

What does Implication Mean?

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

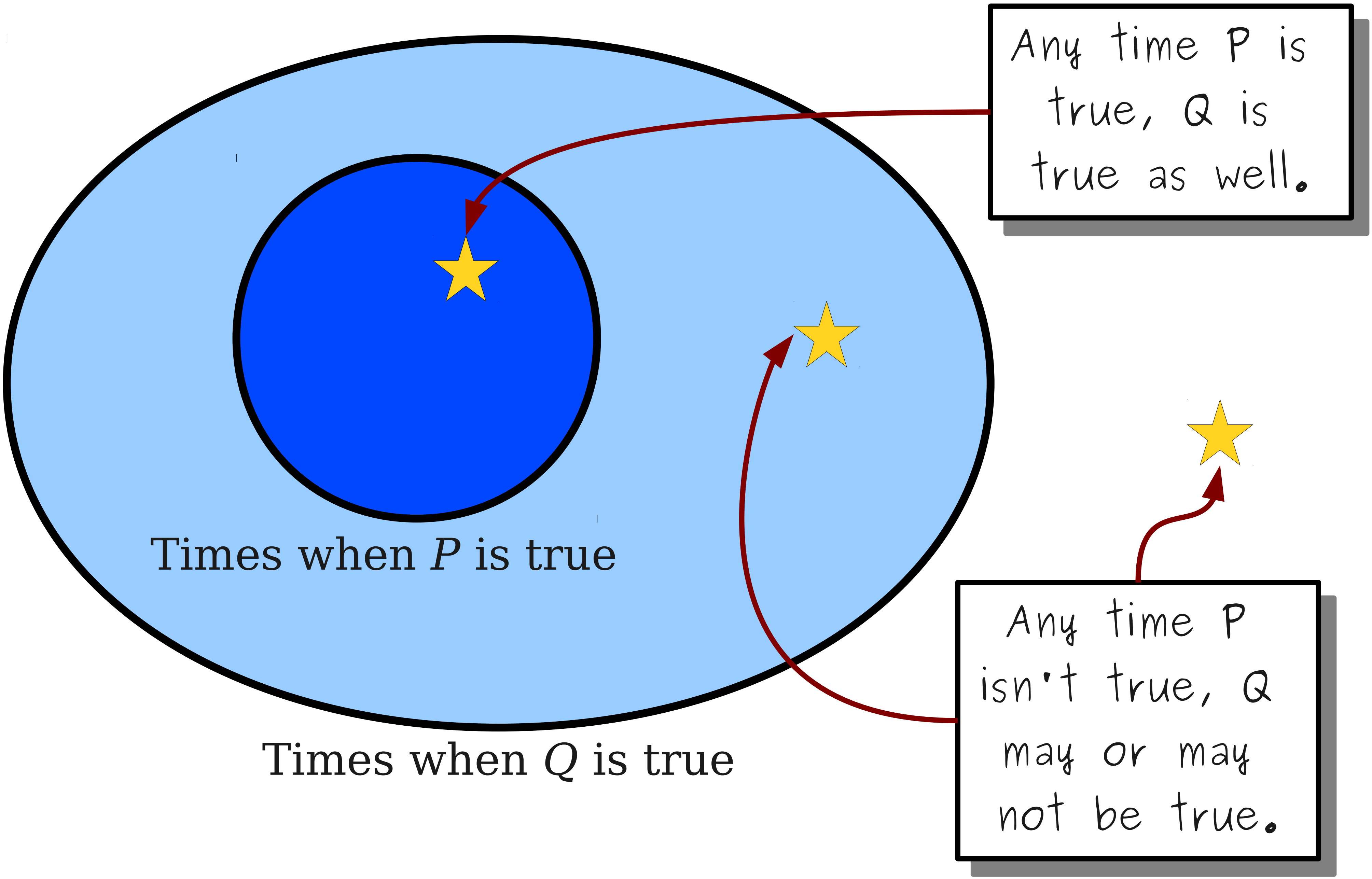
If *P* is true, then
***Q* must be true as well.**

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

What does Implication **Not** Mean?

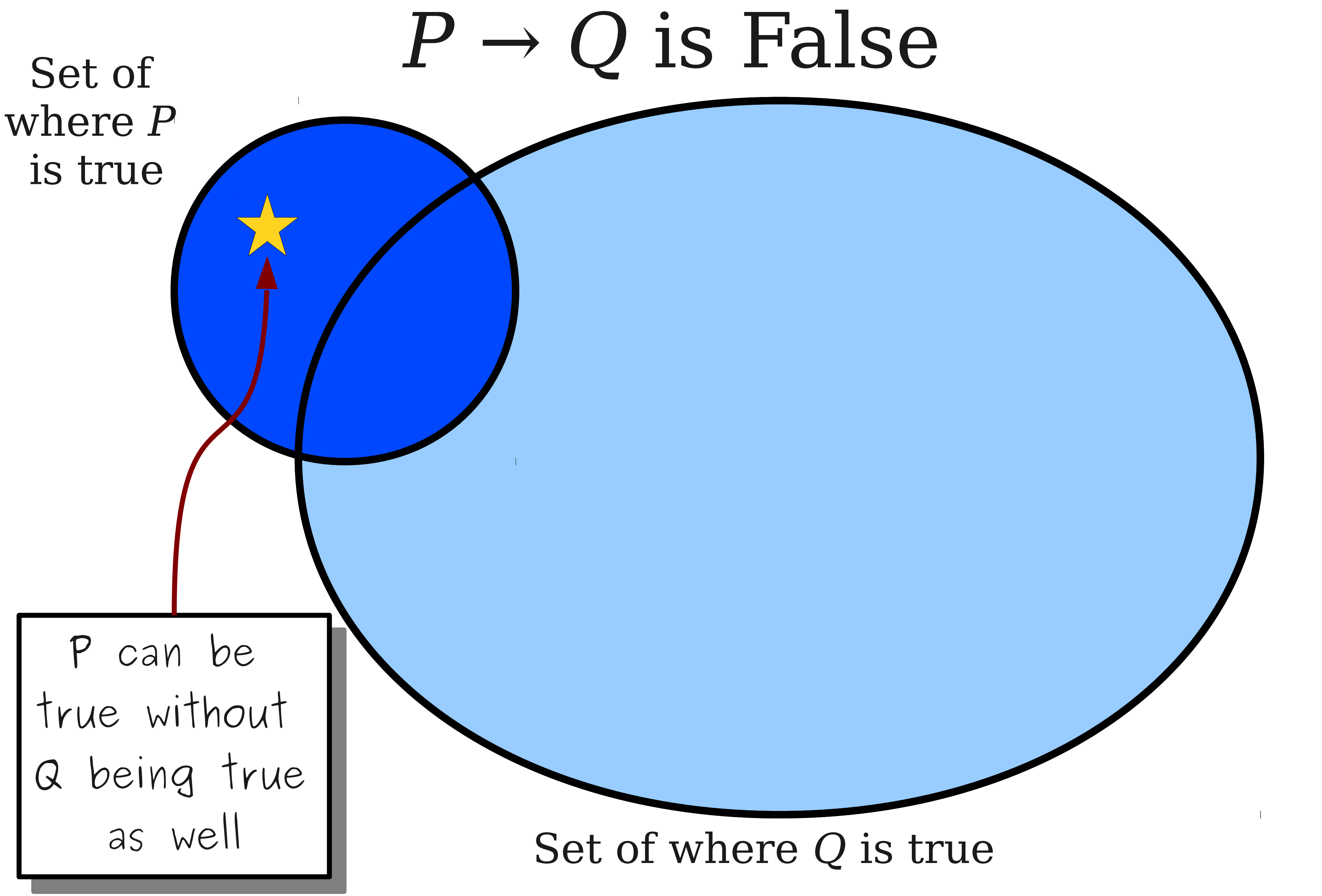
- $P \to Q$ does **not** mean that whenever Q is true, P is true.
  - “If you are a Stanford student, you wear cardinal” does **not** mean that if you wear cardinal, you are a Stanford student.
- $P \to Q$ does **not** say anything about what happens if P is false.
  - “If you hit another skier, you're gonna have a bad time” doesn't mean that if you don't hit other skiers, you're gonna to have a good time.
  - **Vacuous truth:** If P is never true, then $P \to Q$ is always true.
- $P \to Q$ does **not** say anything about causality.
  - “If I want math to work, then $2 + 2 = 4$” is true because any time that I want math to work, $2 + 2 = 4$ already was true.
  - “If I don't want math to work, then $2 + 2 = 4$” is also true, since whenever I don't want math to work, $2 + 2 = 4$ is true.

Implication, Diagrammatically



When P Does Not Imply Q

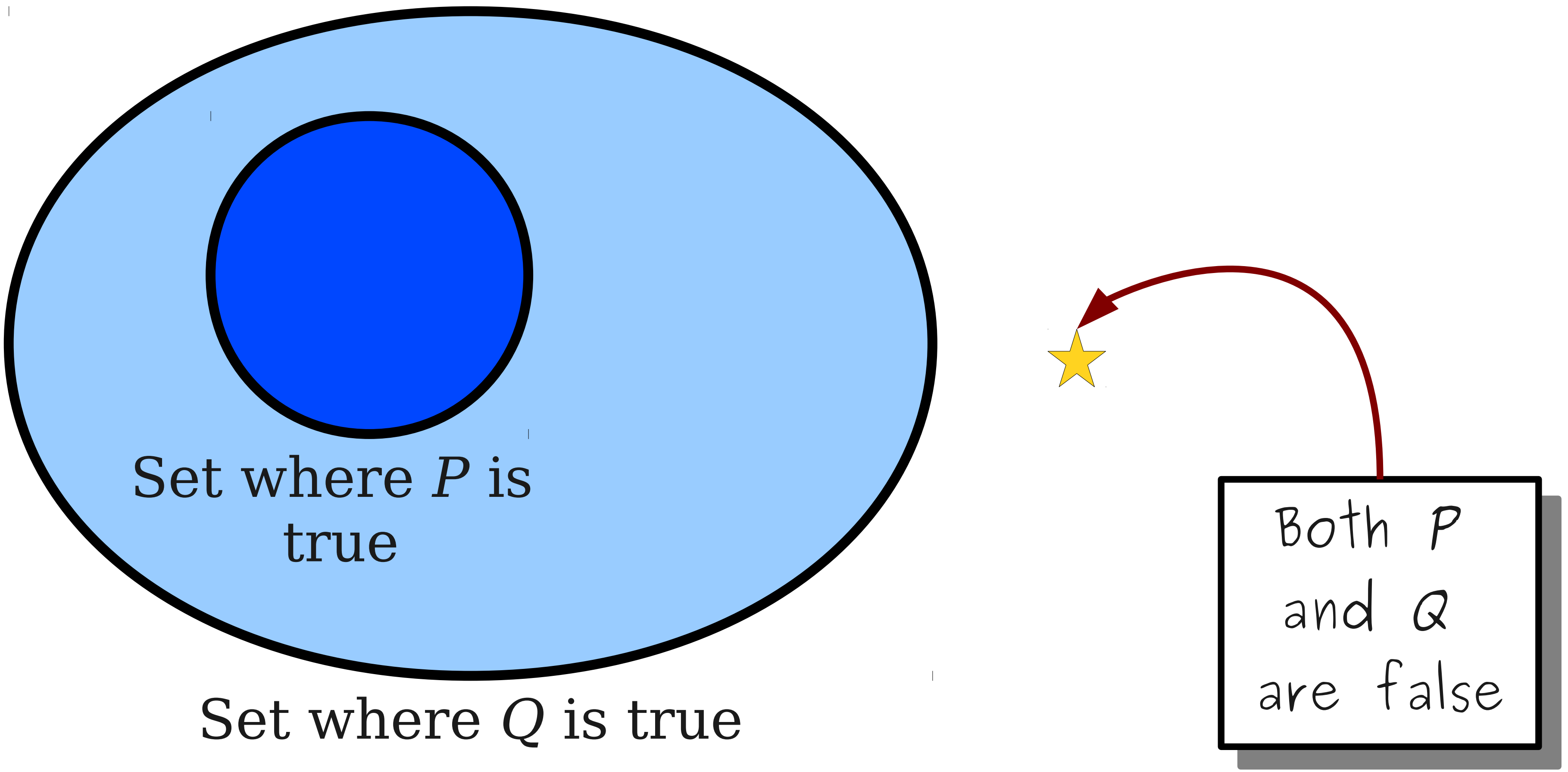
- What would it mean for $P \to Q$ to be false?
- **Answer**: There must be some way for P to be true and Q to be false.
- $P \to Q$ means "If P is true, Q is true as well."
  - The only way to disprove this is to show that there is some way for P to be true and Q to be false.
- To prove that $P \to Q$ is false, find an example of where P is true and Q is false.



$P \to Q$ is False
Set of where P is true
P can be true without Q being true as well
Set of where Q is true

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.



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 option is that the assumption that P is not true is incorrect.
  - Conclude, therefore, that P is 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.

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.

You must include all three of these steps in your proofs!

1.

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. ■

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.

- We sometimes write this as

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

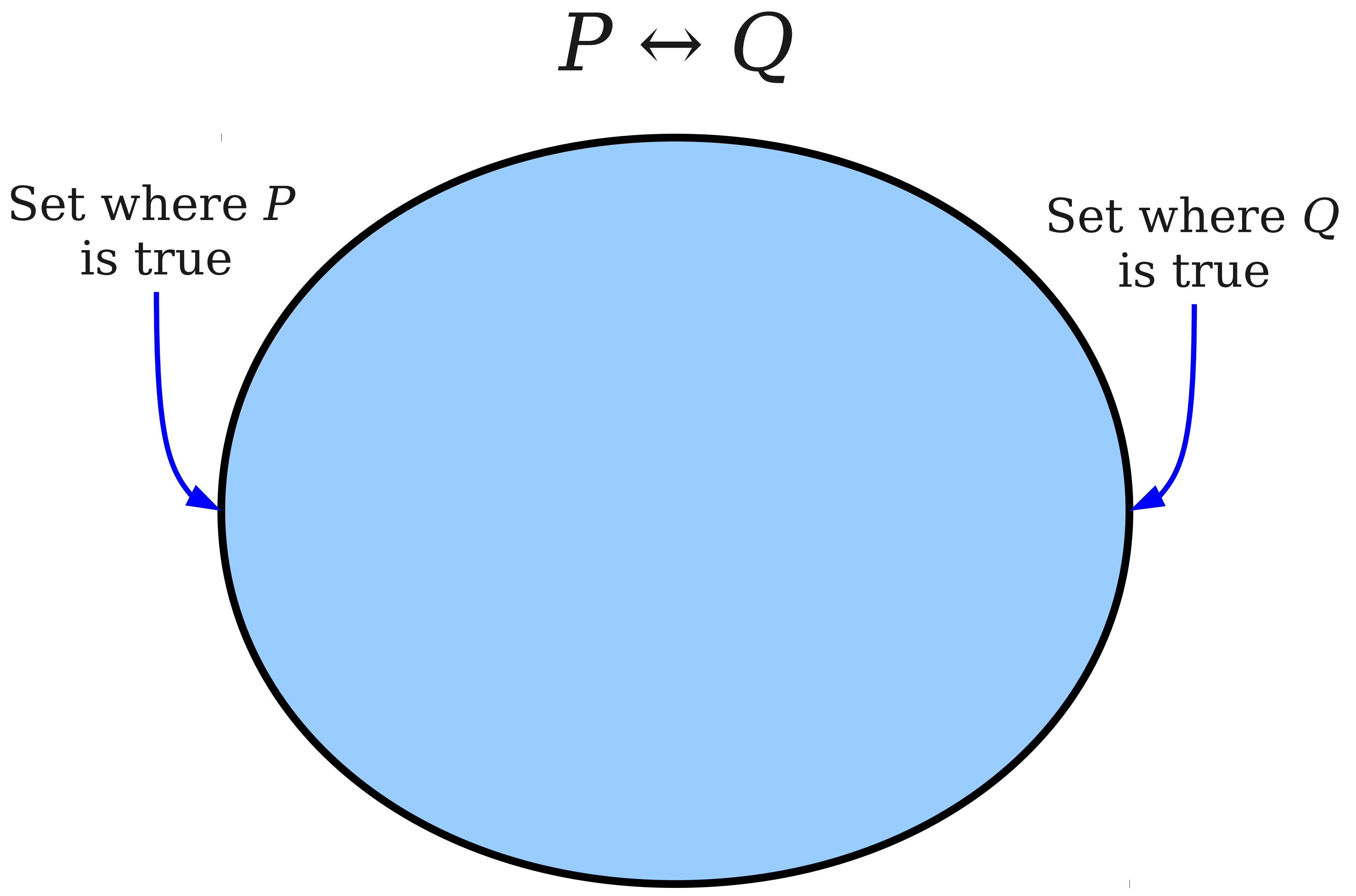
- This is often abbreviated

n is even **iff** n^2 is even.

or as

n is even $\leftrightarrow$ n^2 is even

- This is called a **biconditional**.


$P \leftrightarrow Q$
Set where P is true
Set where Q is true

Proving Biconditionals

- To prove ***P* iff *Q***, you need to prove that

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

- and

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

- Similar to proving $A \subseteq B$ and $B \subseteq A$ to prove $A = B$.
- Use any proof techniques you'd like in each part.
  - In our case, we used a direct proof and a proof by contradiction.
- ***Just make sure to prove both directions of implication!***

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,
  - $q \neq 0$, and
  - p and q have no common divisors other than ±1.
- A number that is not rational is called **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.

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.

You must include all three of these steps in your proofs!

. By

s

our

This

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, your **entire proof is invalid**.

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 $5 \neq 1 + 2 + 3 + 4$ … eached a contradiction, so o… as false and the theorem must be t…

Is this really the opposite of the original statement?

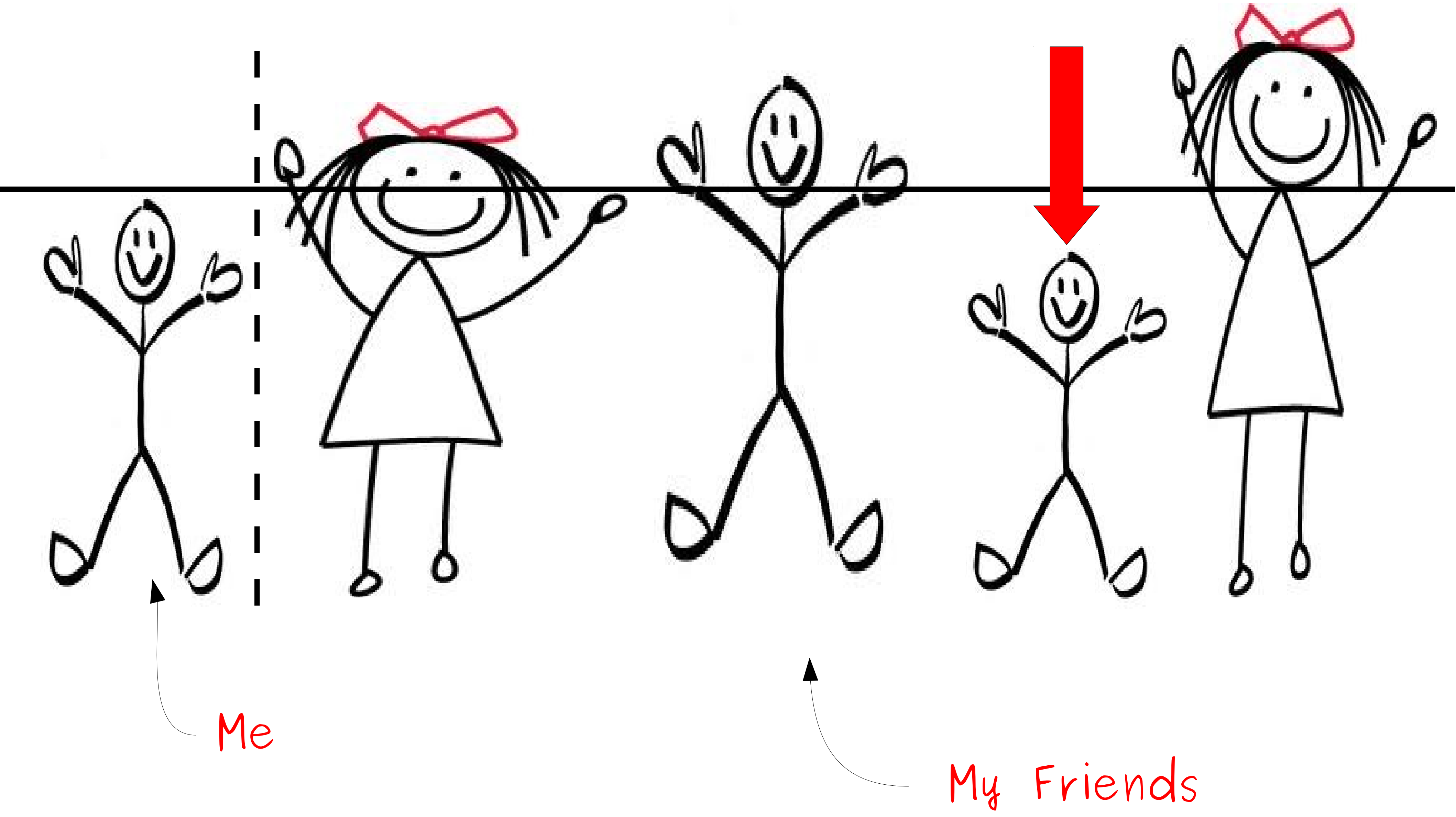
The contradiction of the universal statement

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

is **not**

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

“All My Friends Are Taller Than Me”



The contradiction 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*.

becomes

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

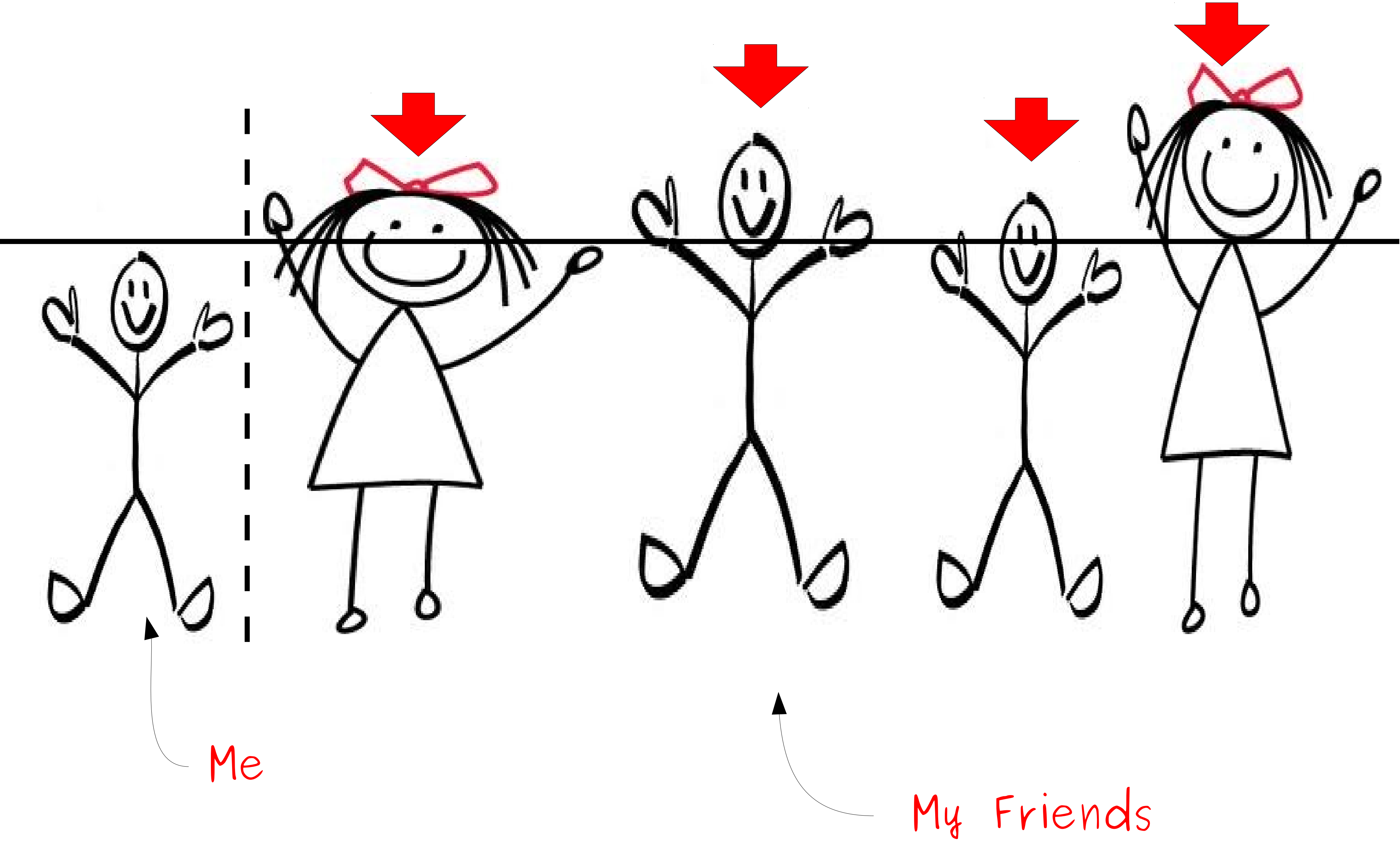
The contradiction of the existential statement

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

is **<u>not</u>**

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

“Some Friend Is Shorter Than Me”



The contradiction 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.

A Terribly Flawed Proof

Theorem: There exists an integer n such that for every integer m, we have $m \leq n$.

Proof: By contradiction; assume that there exists an integer n such that for every integer m, we have $m > n$.

Since for any m, we have that $m > n$ is true, it should be true when $m = n - 1$. Thus $n - 1 > n$. But this is impossible, since $n - 1 < n$.

We have reached a contradiction, so our assumption was incorrect. Thus there exists an integer n such that for every integer m, we have $m \leq n$. ■

A Terribly Flawed Proof

Theorem: There exists an integer n such that for every integer m, we have $m \leq n$.

Proof: By contradiction; assume that there exists an integer n such that for every integer m, we have $m > n$.

Since for any m, we have that $m > n$ is true, it should be true when $m = n - 1$. Thus $n - 1 > n$. But this is impossible, since $n - 1 < n$.

We have reached a contradiction, so our assumption was incorrect. Thus there exists an integer n such that for every integer m, we have $m \leq n$. ■

There exists an integer n such that
for every integer m, $m \leq n$.

becomes

For every integer n,
There exists an integer m such that
m > n

For every integer m,
$m \leq n$

becomes

There exists an integer m such that
$m > n$

A Terribly Flawed Proof

Theorem: There exists an integer n such that for every integer m, we have $m \leq n$.

Proof: By contradiction; assume that there exists an integer n such that for every integer m, we have $m > n$.

Since f … e, it
should … $> n$.
But th …

We ha …
assum … sts
an integer n such that for every integer m, we have $m \leq n$. ■

For every integer *n*,
There exists an integer *m* such that
m > n

The Story So Far

Proof by Contrapositive

Honk **if** You Love Formal Logic

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 I had been a good test subject, then I would have received cake."
  - Contrapositive: "If I didn't receive cake, then I wasn't a good test subject."

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**.

If

n^2 is even

then

n is even

If

n is odd

then

n^2 is odd

Theorem: 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

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

Since $(2k^2 + 2k)$ is an integer, n^2 is odd. ■

Theorem: 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 integ

$n^2 =$
$n^2 =$
$n^2 =$

Since odd. ■

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.

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. ■

Common Pitfalls

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

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

<u>Do not</u> show that

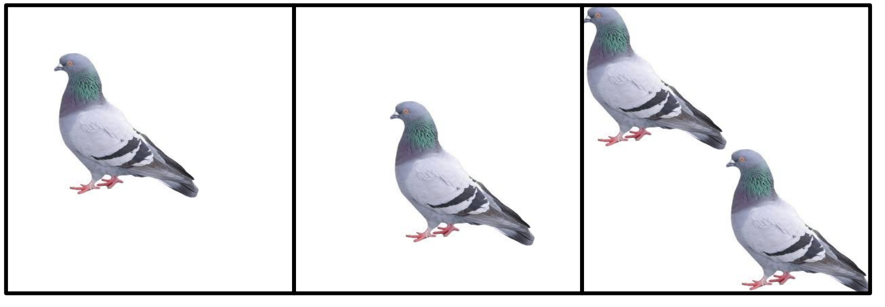
$$\neg P \to \neg Q$$

(Showing $\neg P \to \neg Q$ proves that $Q \to P$, not the other way around!)

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.



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

$$m = \sum_{i=1}^{n} x_i$$

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

$$m = \sum_{i=1}^{n} x_i \leq \sum_{i=1}^{n} 1 = n$$

So $m \leq n$, as required. ■

Using the Pigeonhole Principle

- The pigeonhole principle is an enormously useful lemma in many proofs.
  - If we have time, 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.

Next Time

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