Indirect Proofs

Announcements

- Review session tonight in **370-370** from 7–8PM
  - **Note the room change!**
- Problem Set 1 out, due Friday, October 7 at 2:15PM (right before class).
  - **Start early!**
  - Later problems are harder than earlier ones; don't extrapolate from the first few problems.
  - Email us at **cs103@cs.stanford.edu** or stop by OH with questions.

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.”
- Equivalent formulations:
  - “If P, then Q.”
  - “P only if Q.”
  - “Q whenever P.”
  - “P implies Q”
- **Notation**: We write “If P, then Q” as **P** → **Q**.
  - Read: “P implies Q.”

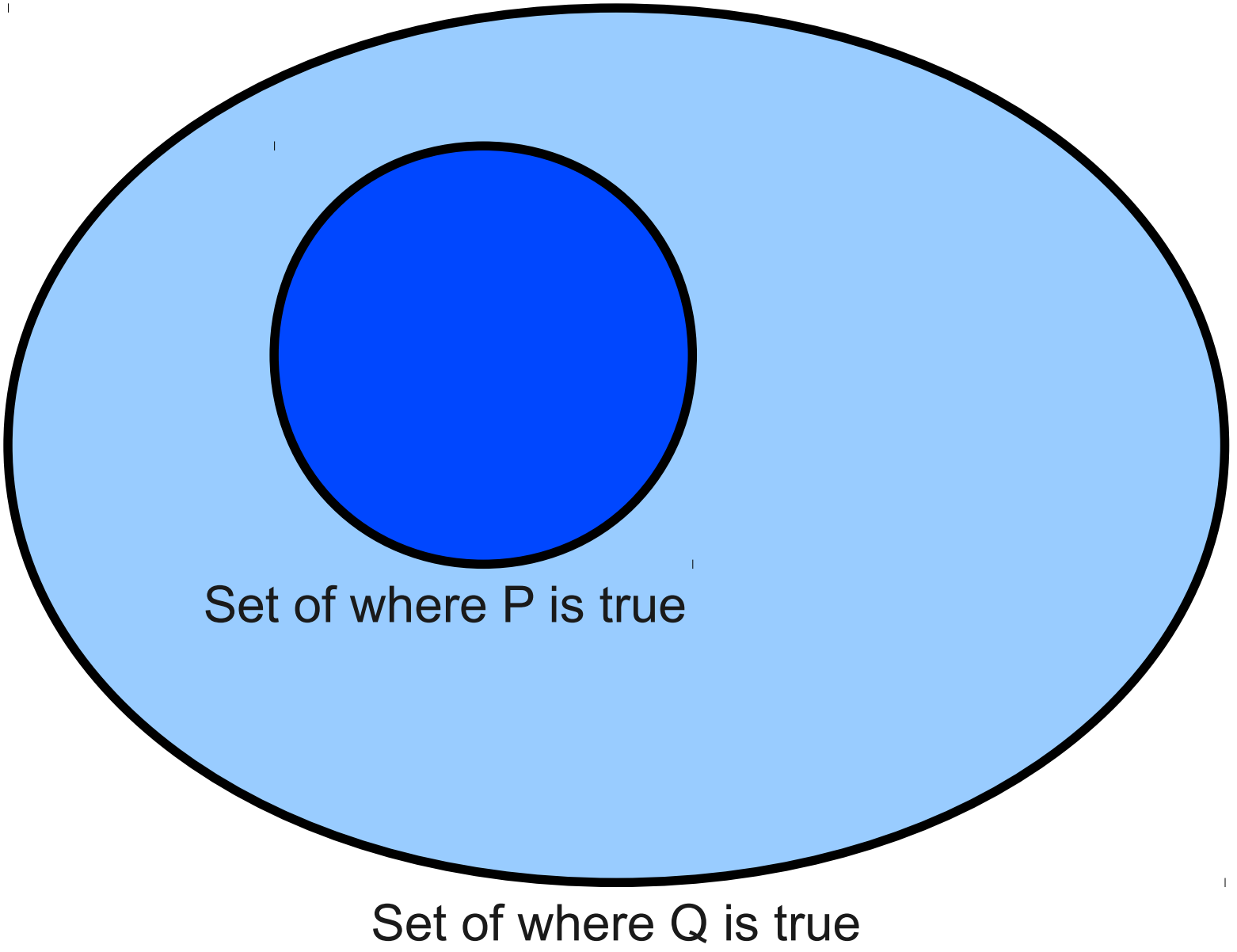
What does Implication Mean?

- What does it mean for the statement $P \to Q$ to be true?
- In any case where P is true, Q must be true as well.
- For example:
  - n is even $\to$ n^2 is even.
  - $x \in S \to x \in T$.
  - $xRy \to yRx$.
- If $P \to Q$, we call P the **antecedent** and Q the **consequent**.

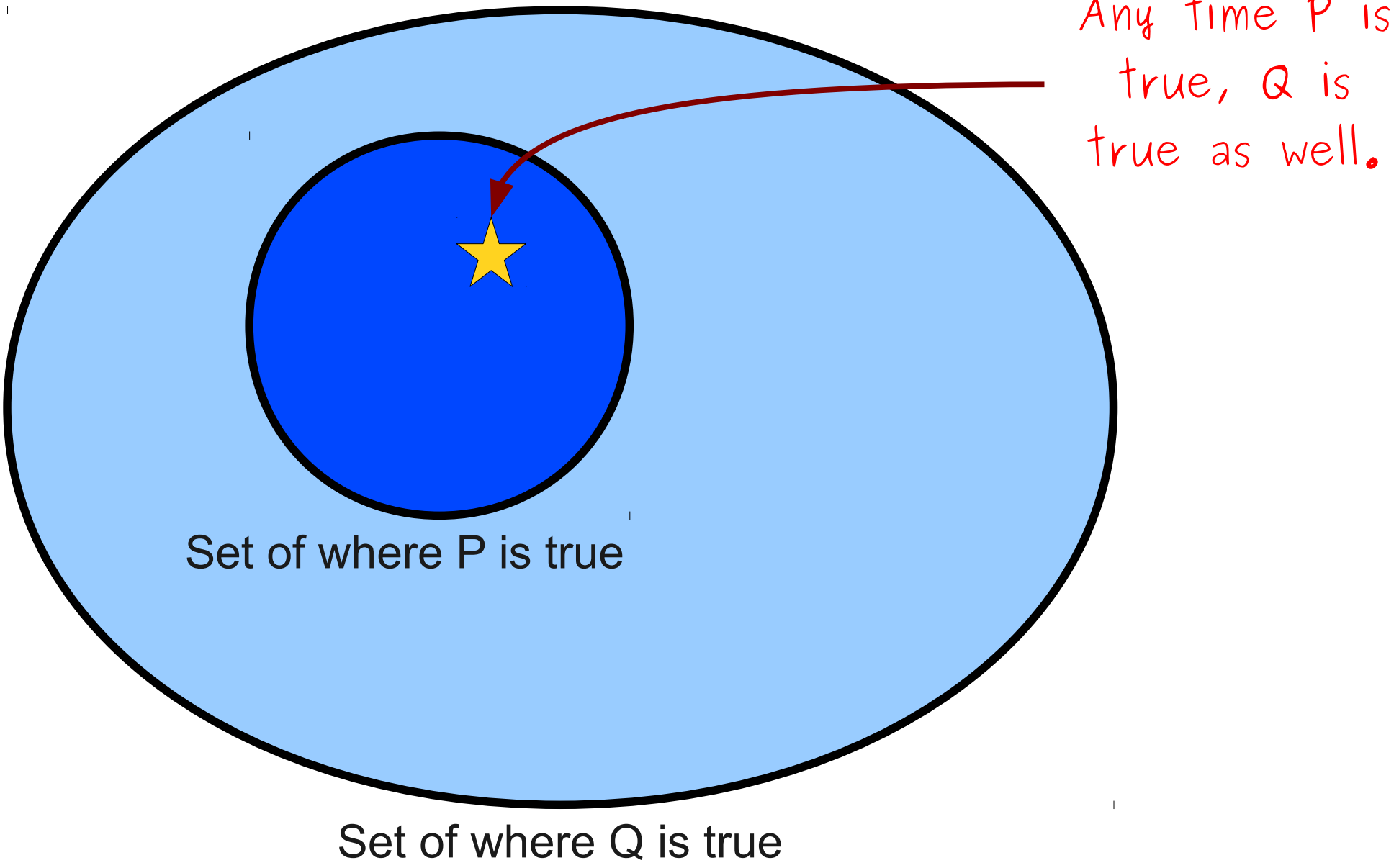
What does Implication **Not** Mean?

- P → 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.
  - (That would overcrowd the dorms)
- P → Q does **not** say anything about what happens if P is false.
  - “If you are a wide receiver, you catch the football” does not mean that if you're not a wide receiver, you don't catch the football.
  - (You might be Andrew Luck)
  - **Vacuous truth:** If P is never true, then P → Q is automatically true.
- P → Q does **not** say anything about causality.
  - “If I will it to be true, 2 + 2 = 4” is true because any time that I want it to be true, 2 + 2 = 4 already was true.
  - “If I will it to be false, 2 + 2 = 4” is also (vacuously) true.

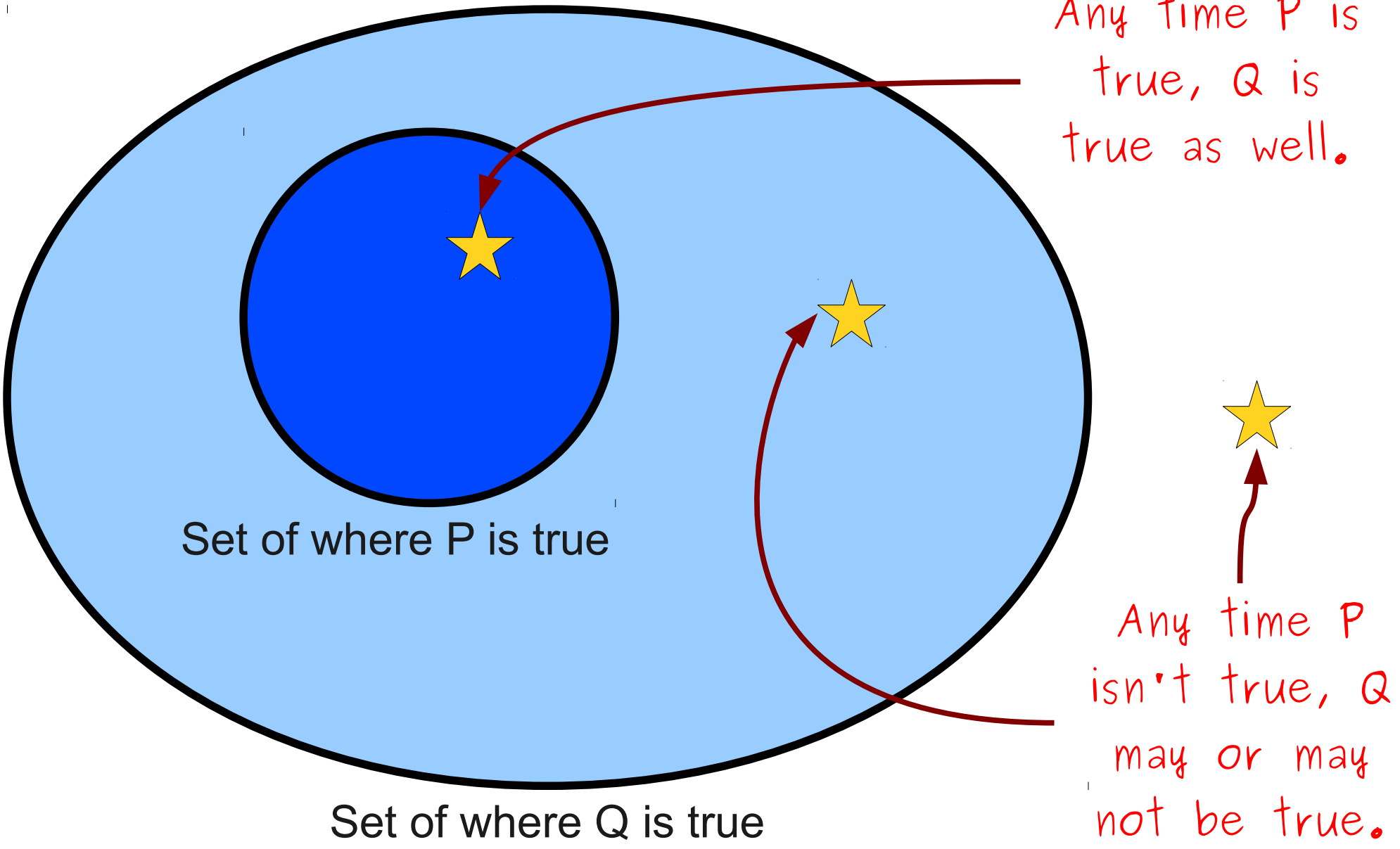
Implication, Diagrammatically



Implication, Diagrammatically



Implication, Diagrammatically



When P does not imply Q

- What would it mean for P → Q to be false?

When P does not imply Q

- What would it mean for P → Q to be false?
- **Answer**: There must be some way for P to be true and Q to be false.

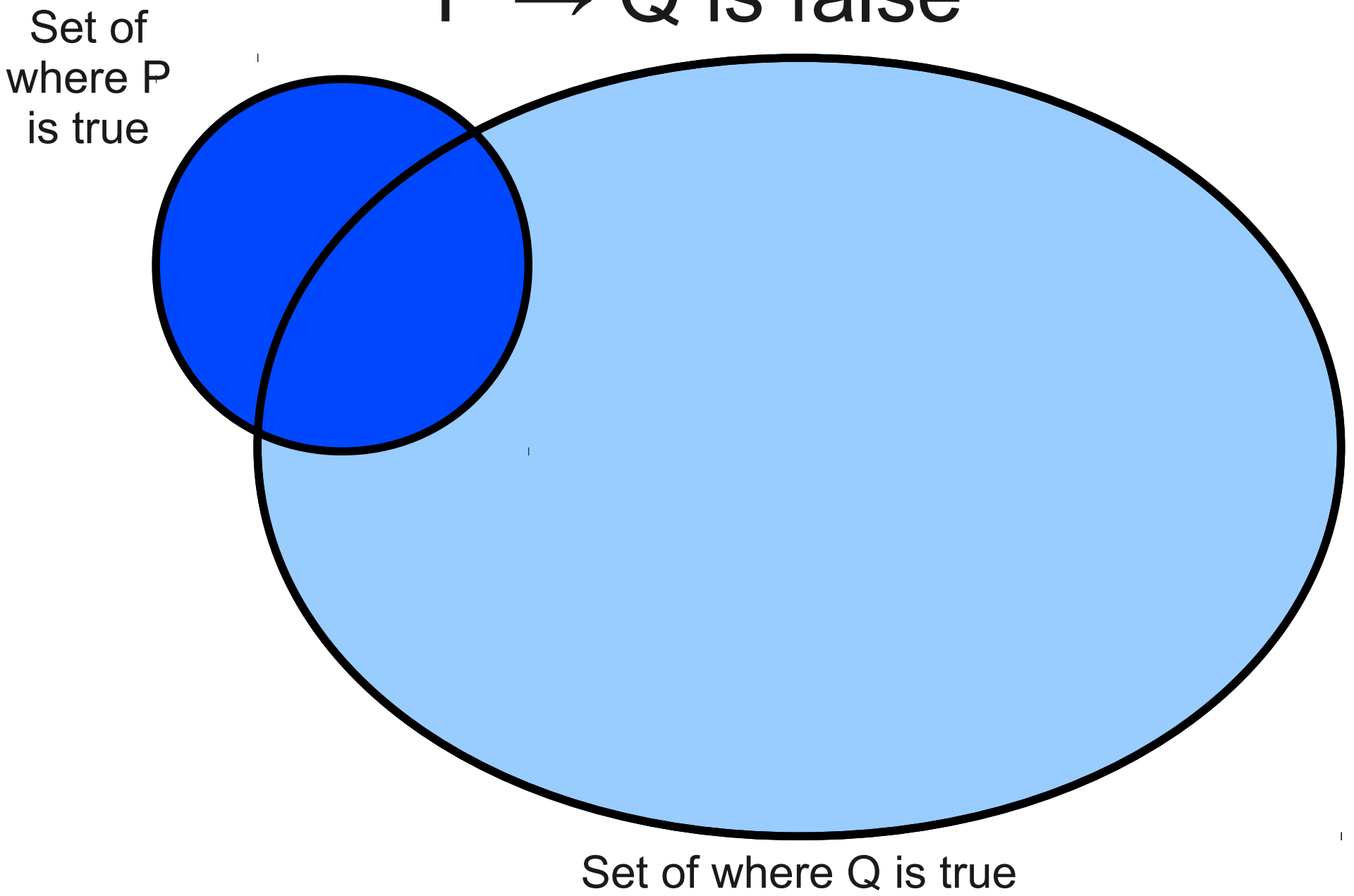
When P does not imply Q

- What would it mean for P → Q to be false?
- **Answer**: There must be some way for P to be true and Q to be false.
- Why?

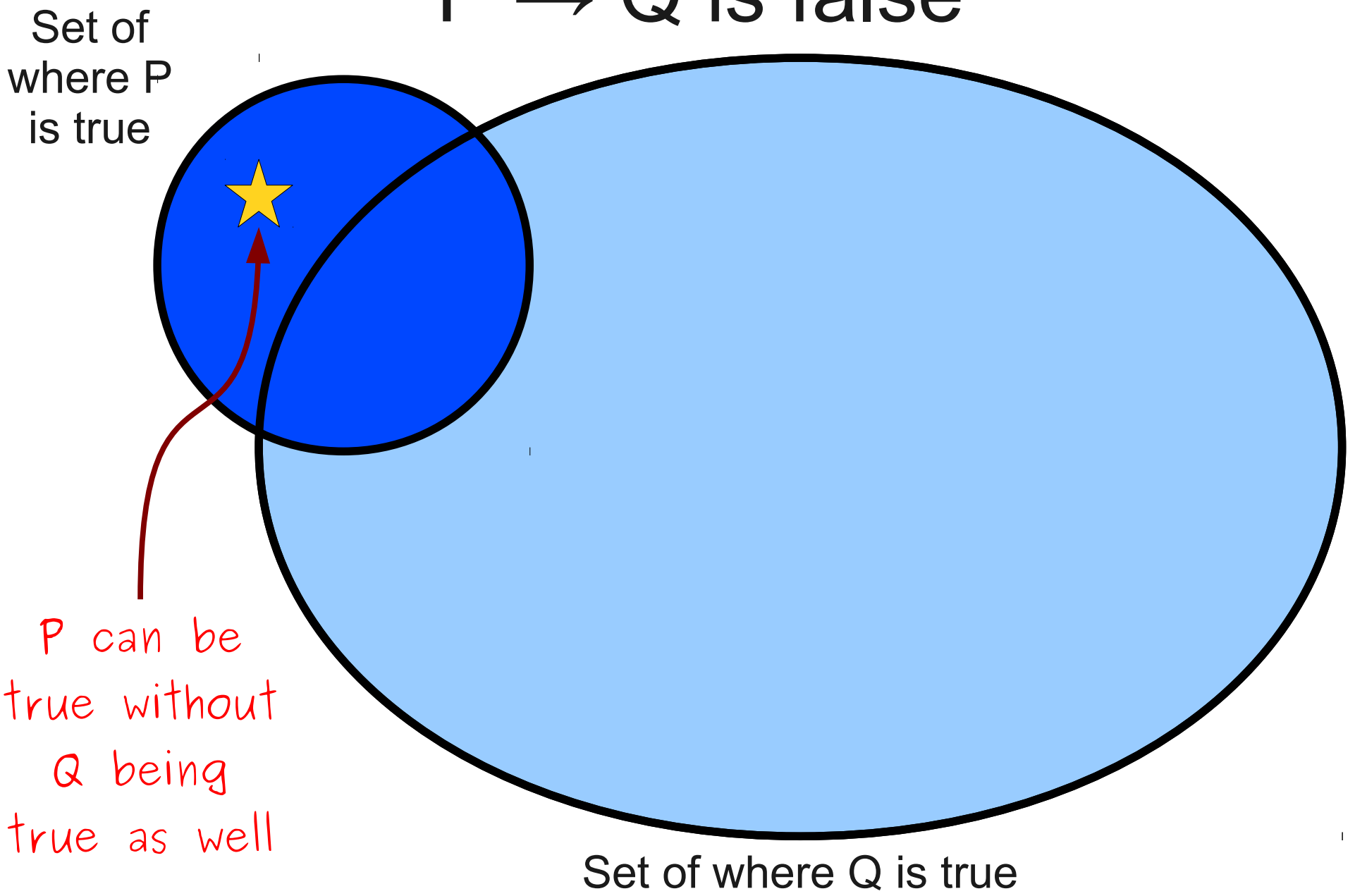
When P does not imply Q

- What would it mean for P → Q to be false?
- **Answer**: There must be some way for P to be true and Q to be false.
- Why?
  - P → Q means “any time P is true, Q is true.”
  - 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 → Q is false, find an example of where P is true and Q is false.

$P \rightarrow Q$ is false



$P \rightarrow Q$ is false

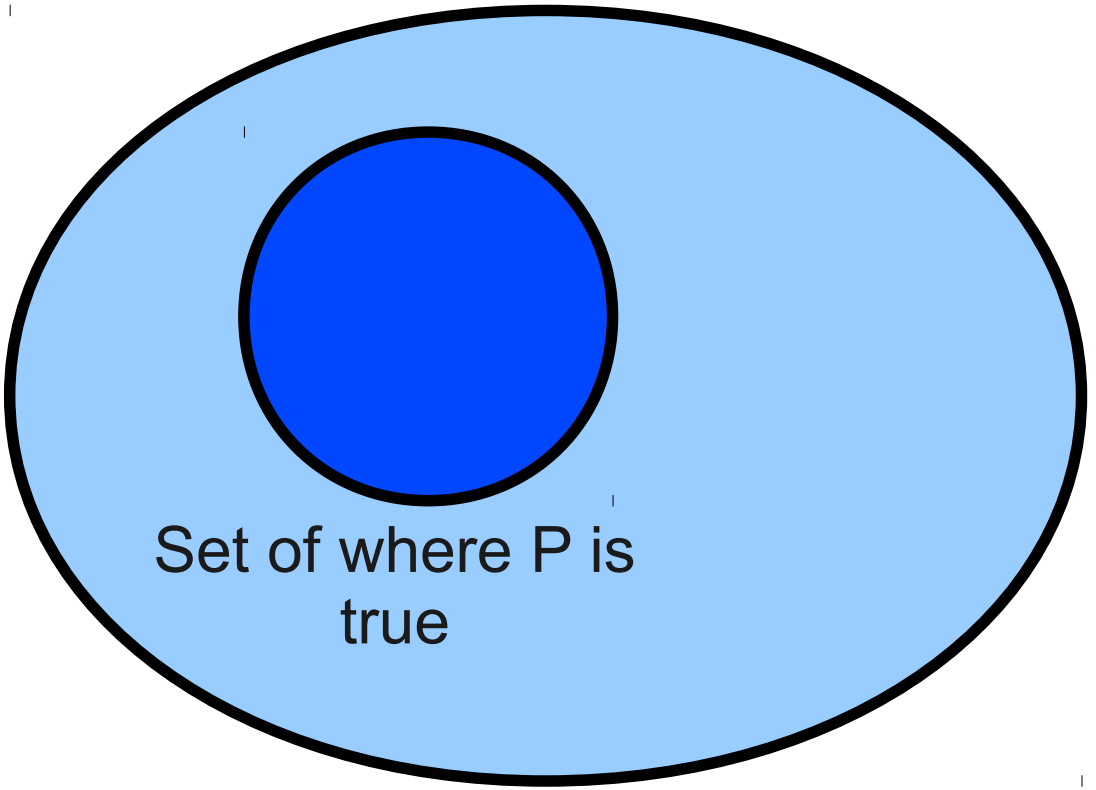


A Common Mistake

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

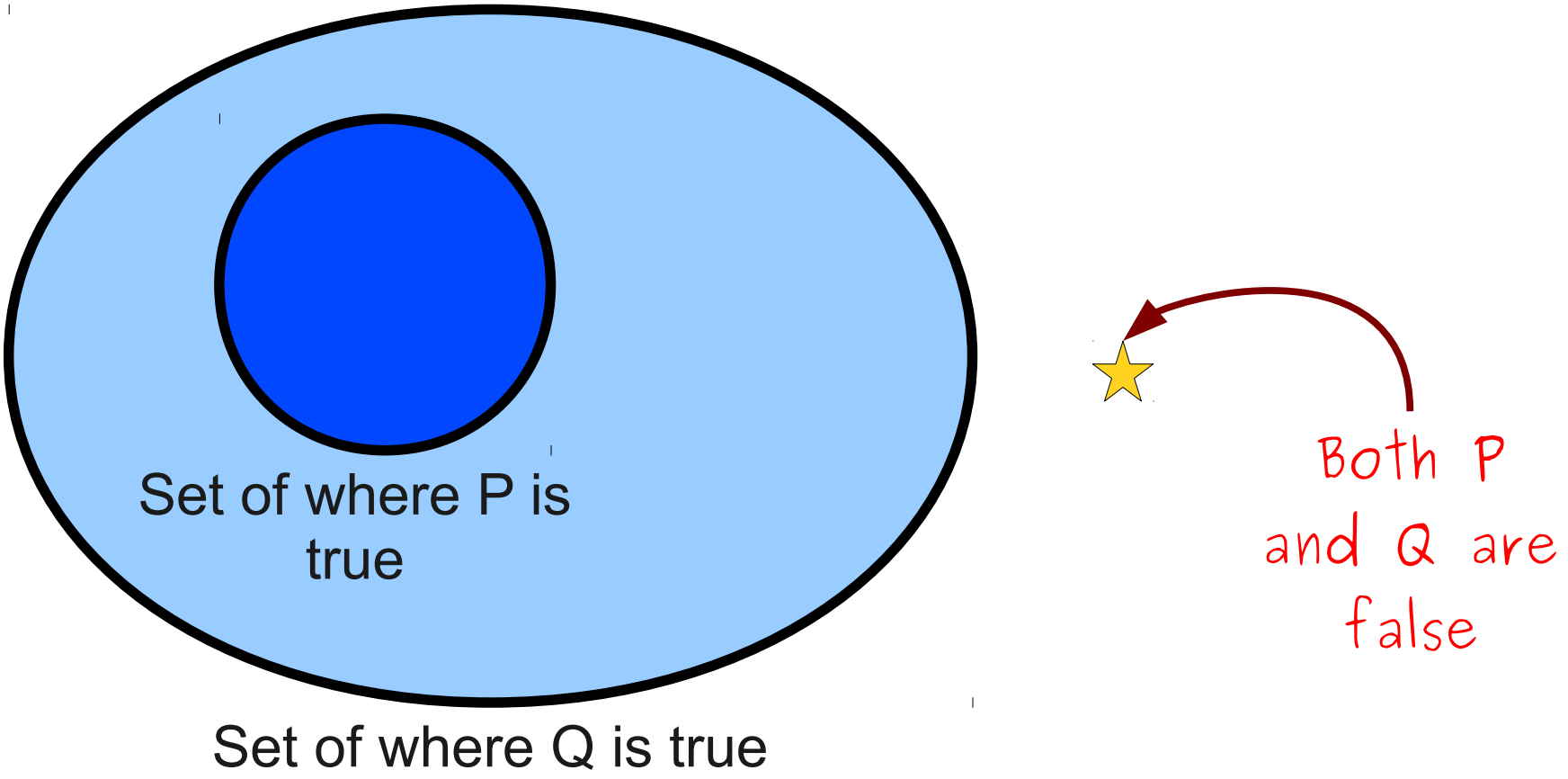
A Common Mistake

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



A Common Mistake

- To show that P → 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

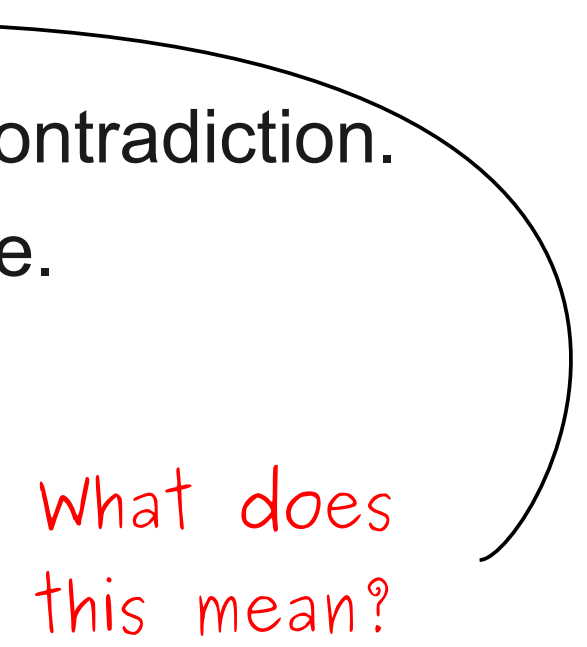
- A **proof by contradiction** is a proof that works as follows:
  - To prove that P is true, assume that P is not true.
  - Based on the assumption that P is not true, conclude something impossible.
  - Assuming the logic is sound, the only option is that the assumption that P is not true is incorrect.
  - 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 $P \to Q$ 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^2 is even, then n is even.

A Simple Proof by Contradiction

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

A Simple Proof by Contradiction

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

A Simple Proof by Contradiction

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

A Simple Proof by Contradiction

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

A Simple Proof by Contradiction

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

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

A Simple Proof by Contradiction

Theorem: If n^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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 clearly impossible, since n^2 is even.

A Simple Proof by Contradiction

Theorem: If n^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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 clearly impossible, since n^2 is even.

Last time, I accidentally wrote "n^2 is even." That's incorrect; n^2 really is odd here.

A Simple Proof by Contradiction

Theorem: If n^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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 clearly impossible, since n^2 is even.

A Simple Proof by Contradiction

Theorem: If n^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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 clearly impossible, since n^2 is even.

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

A Simple Proof by Contradiction

Theorem: If n^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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 clearly impossible, since n^2 is even.

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

A Simple Proof by Contradiction

Theorem: If n^2 is even, then n is even.
Proof: By contradiction; assume n^2 is even but 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 clearly impossible, since n^2 is even.

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

Biconditionals

- Combined with what we saw on Friday, we have proven
  - If n is even, n^2 is even.
  - If n^2 is even, n is even.
- We sometimes write this as

  n is even **if and only if** n^2 is even.
- This is often abbreviated

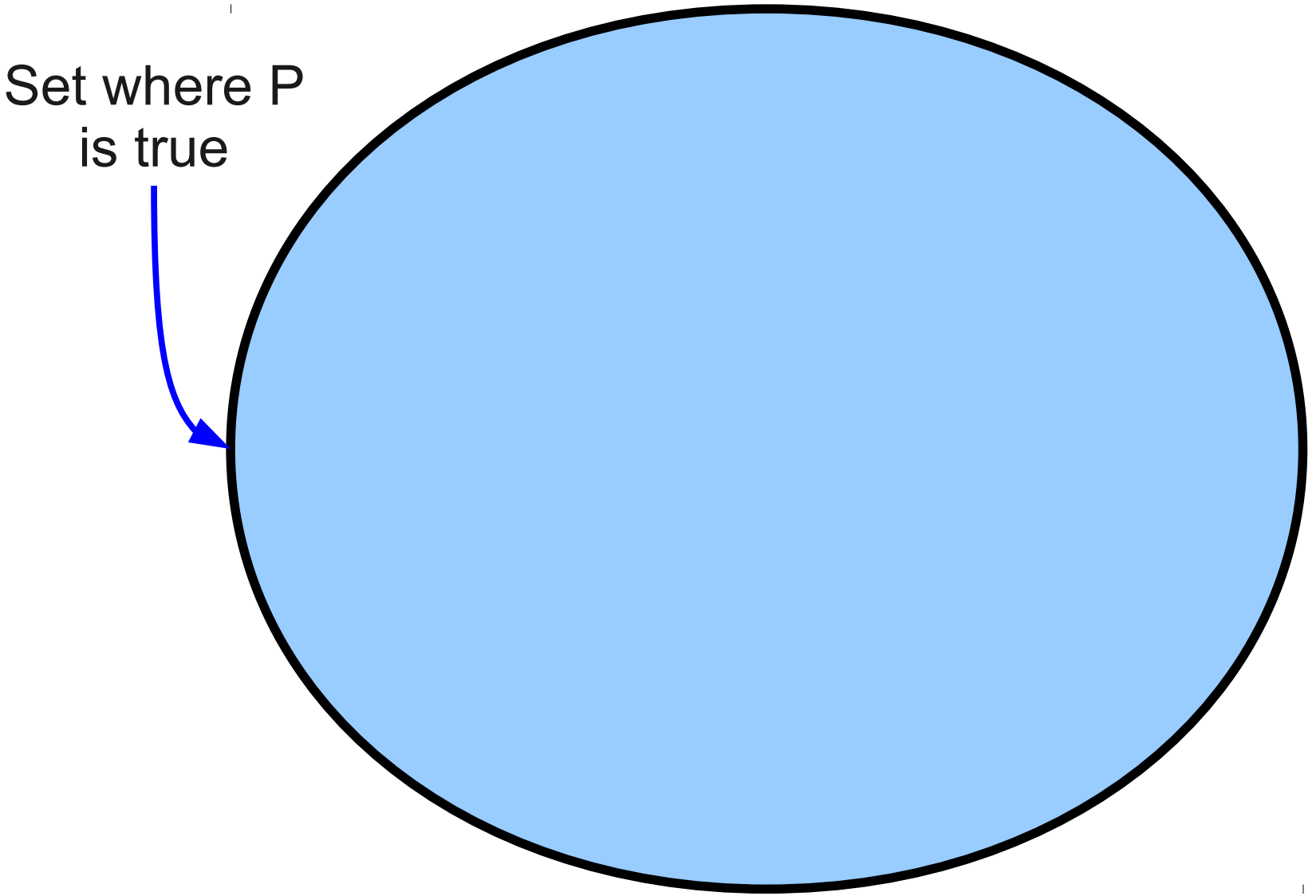
  n is even **iff** n^2 is even.

  or as

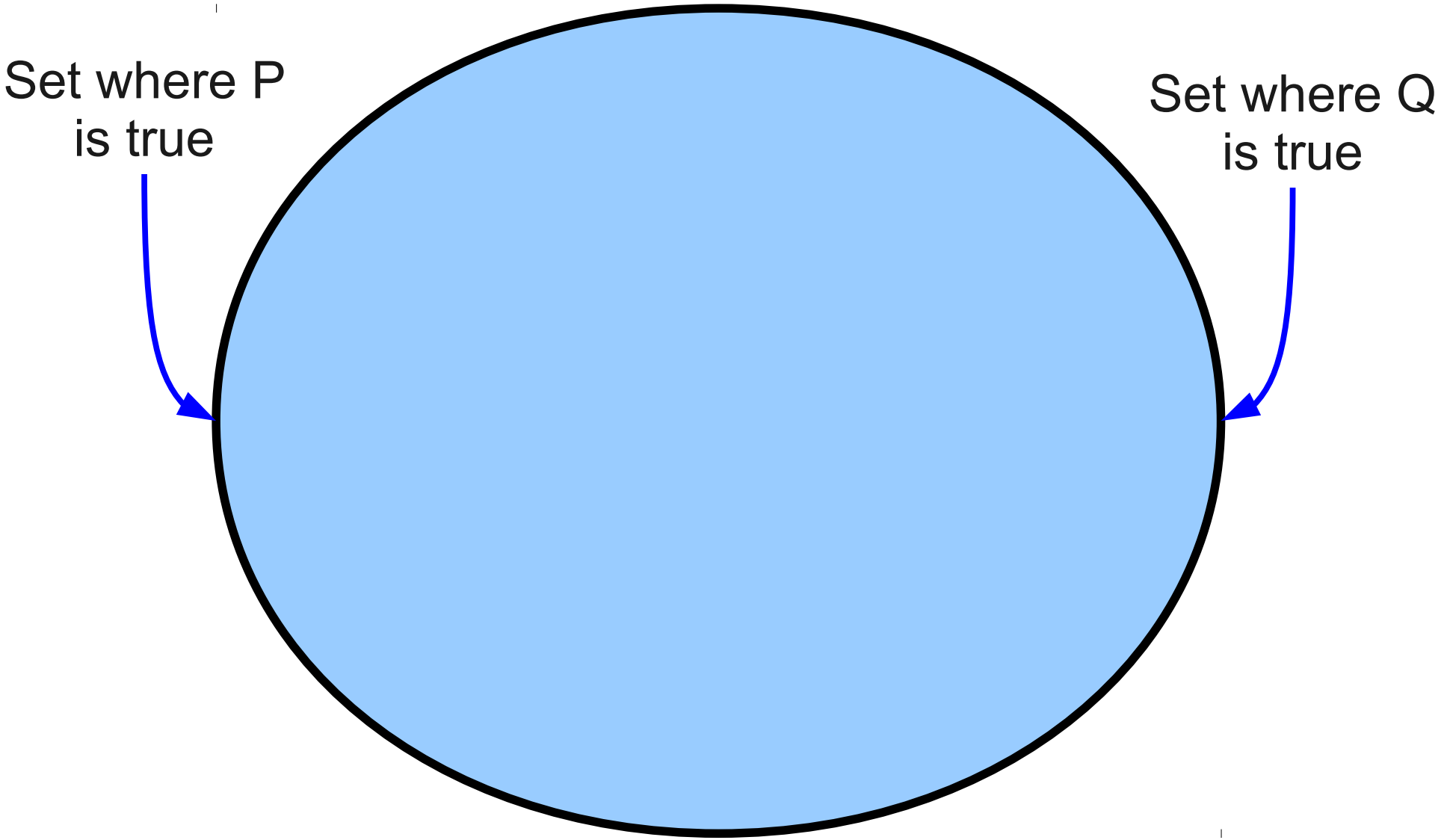
  n is even $\leftrightarrow$ n^2 is even
- This is called a **biconditional**.

$$P \leftrightarrow Q$$

$$P \leftrightarrow Q$$



$P \leftrightarrow Q$



Proving Biconditionals

- To prove P iff Q, you need to prove that
  - **P** → **Q**, and
  - **Q** → **P**.
- You may use any proof techniques you'd like when doing so.
  - In our case, we used a direct proof and a proof by contradiction.
- **Make sure to prove both directions of implication**.

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 positive integer n, the sum of all smaller positive integers is not equal to n.

An Incorrect Proof

Theorem: For any positive integer n, the sum of all smaller positive integers is not equal to n.

Proof: By contradiction; assume that for any positive integer n, the sum of all smaller positive integers *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

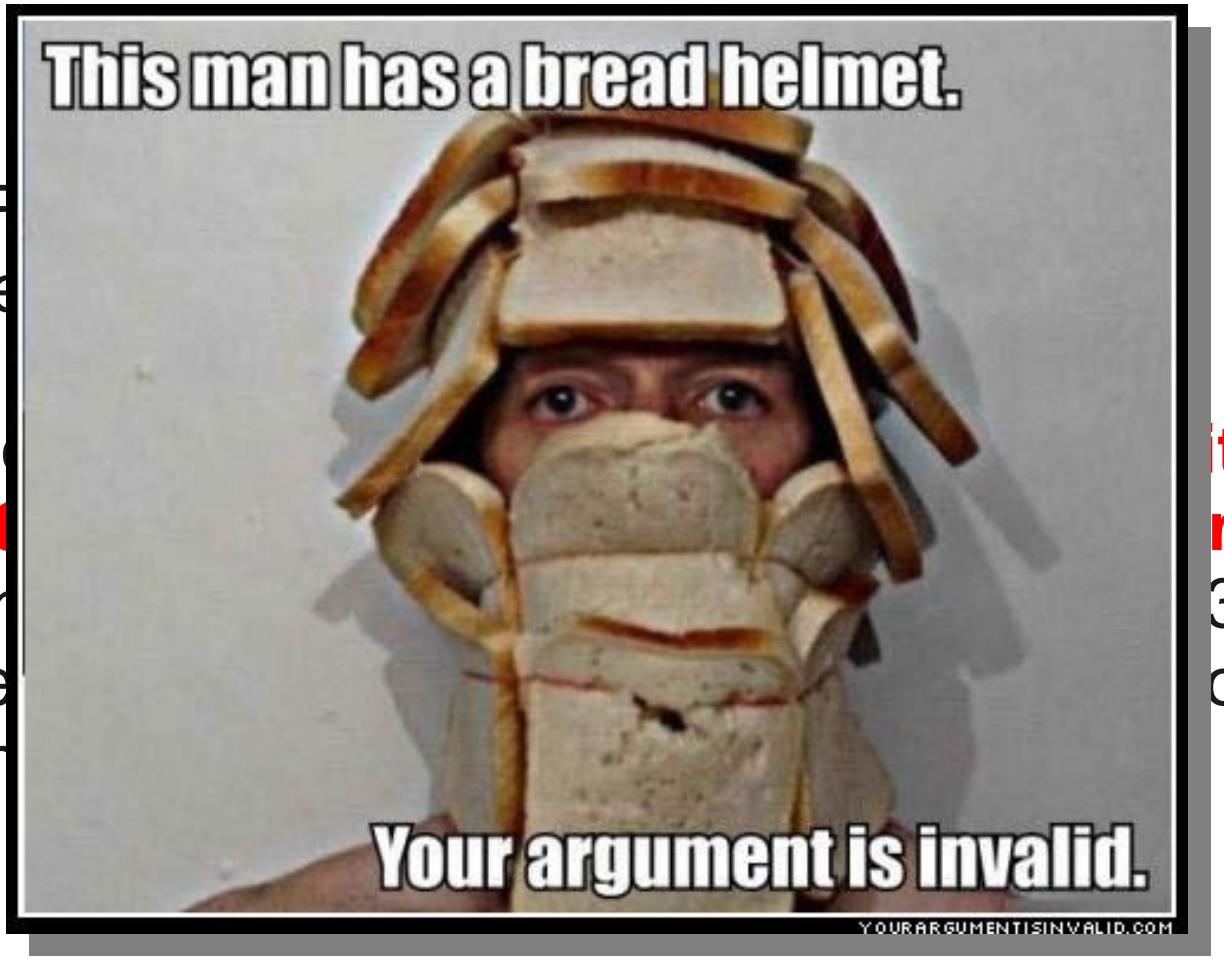
Theorem: For any positive integer n, the sum of all smaller positive integers is not equal to n.

Proof: By contradiction; **assume that for any positive integer n, the sum of all smaller positive integers *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: F smaller positive inte

Proof: By c itive **integer n, t rs *is* equal to n**. But th 3 + 4 = 10. We have re on was false and th



The contradiction of

“for all x, P(x) is true”

is **not**

“for all x, P(x) is false.”

The contradiction of

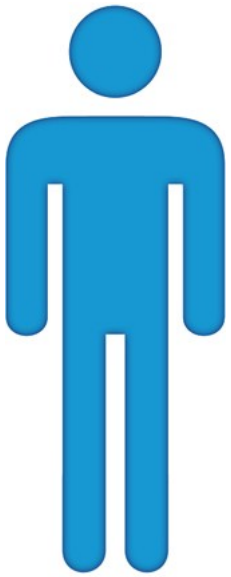
"for all x, P(x) is true"

is

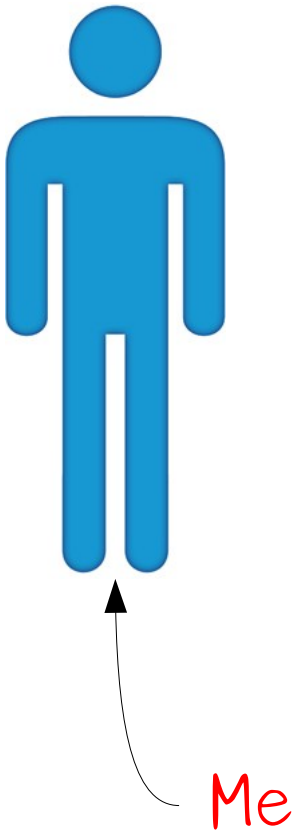
"for **some choice of x**, P(x) is false."

“All My Friends Are Taller Than Me”

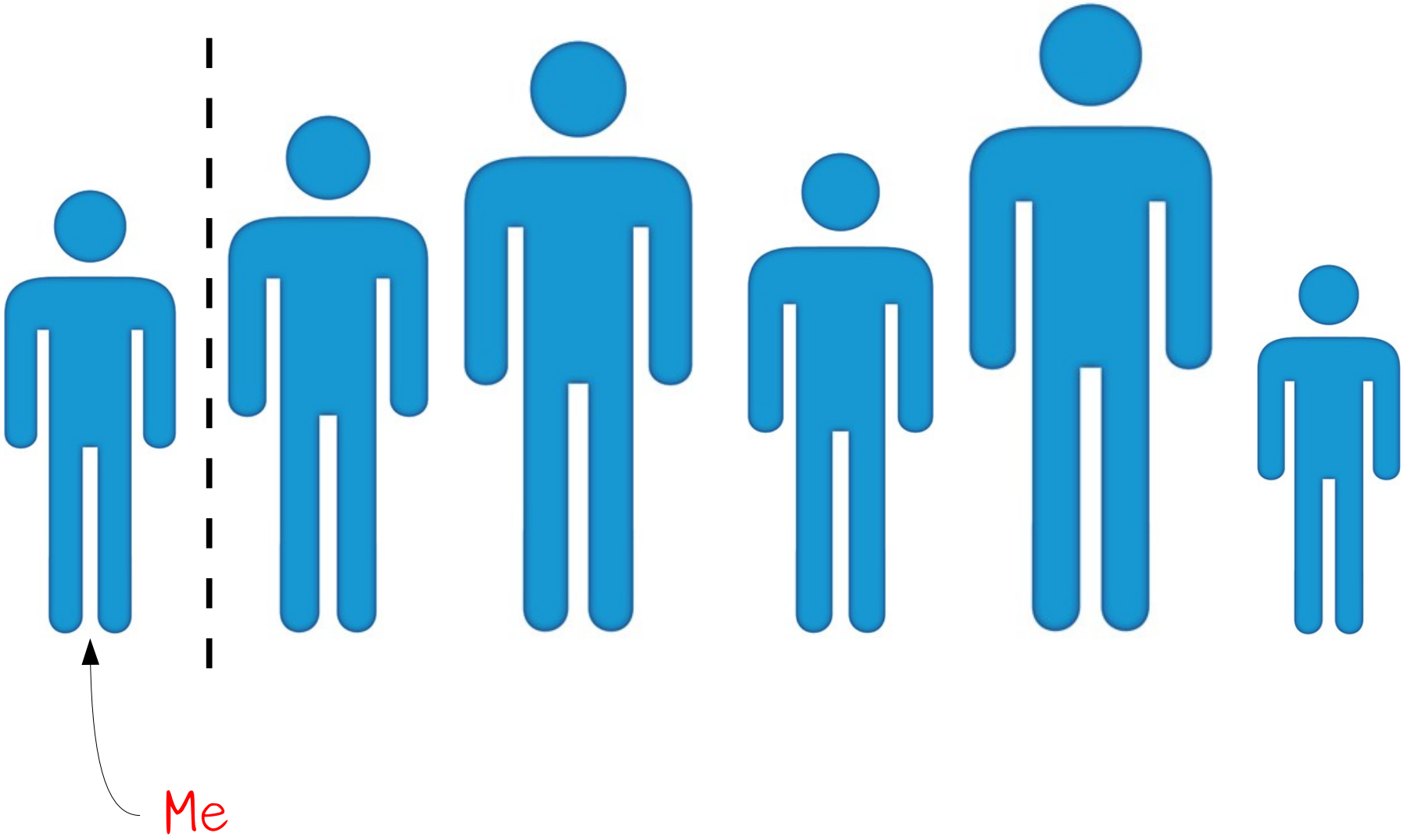
“All My Friends Are Taller Than Me”



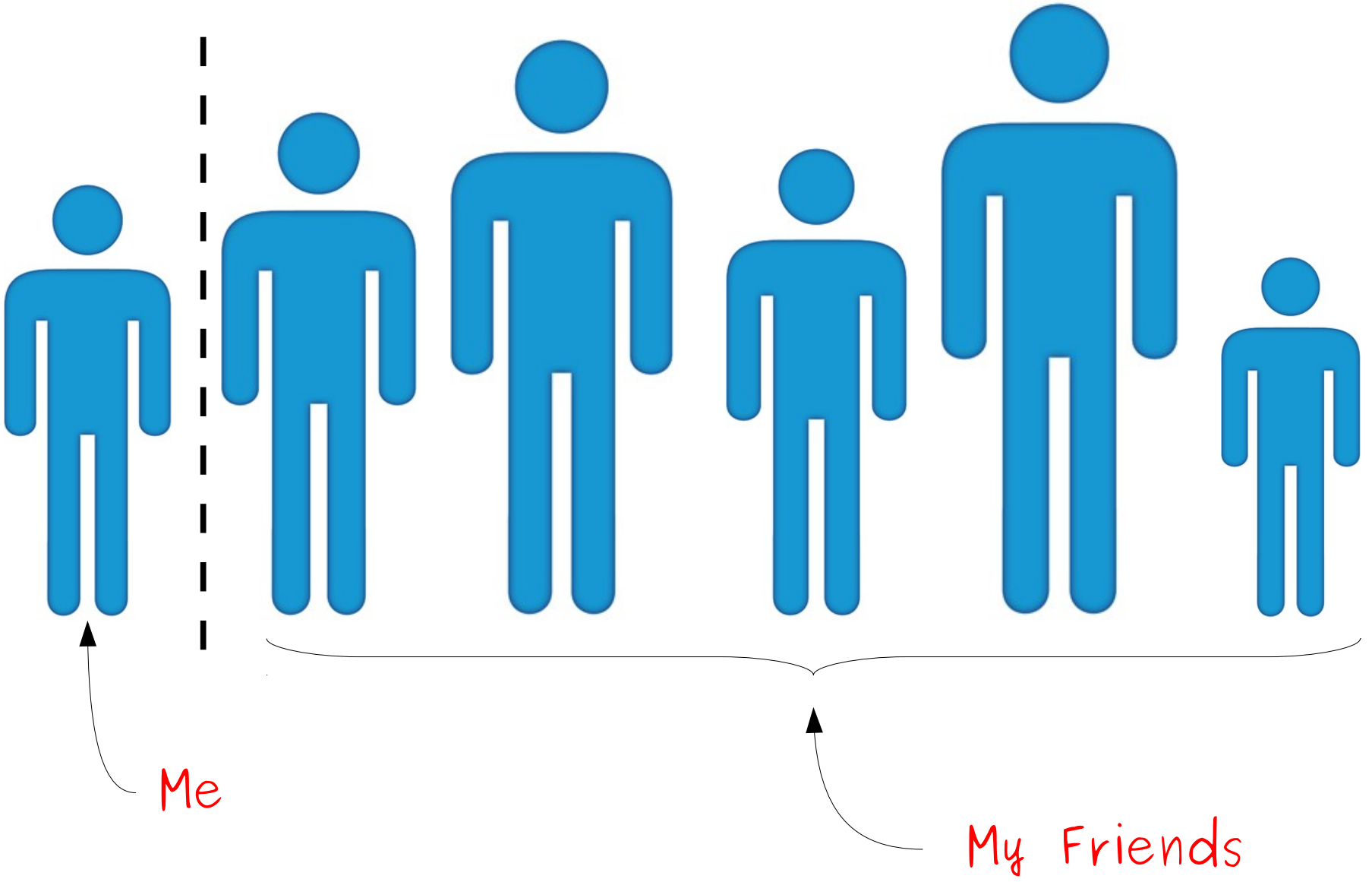
“All My Friends Are Taller Than Me”



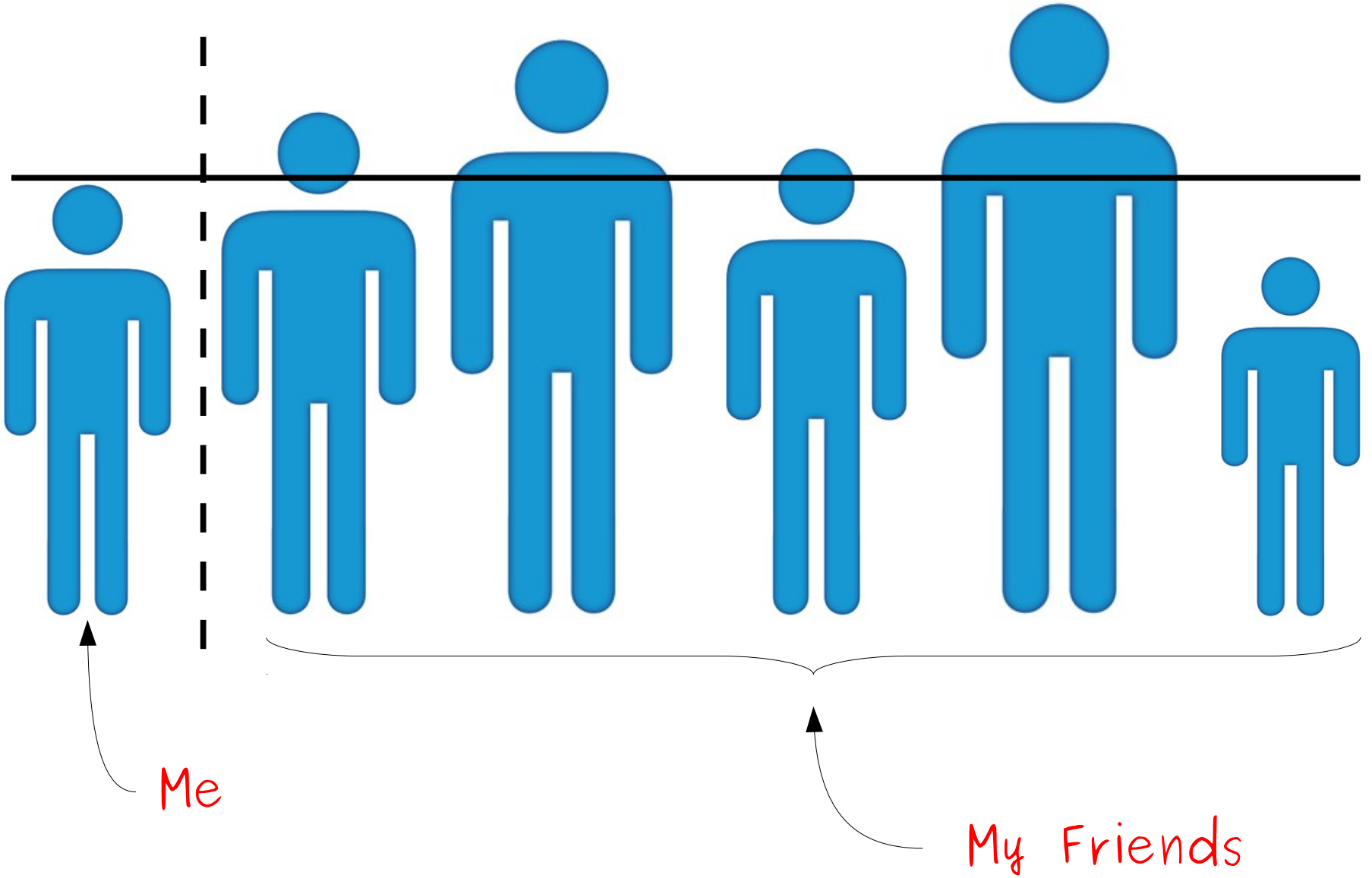
“All My Friends Are Taller Than Me”



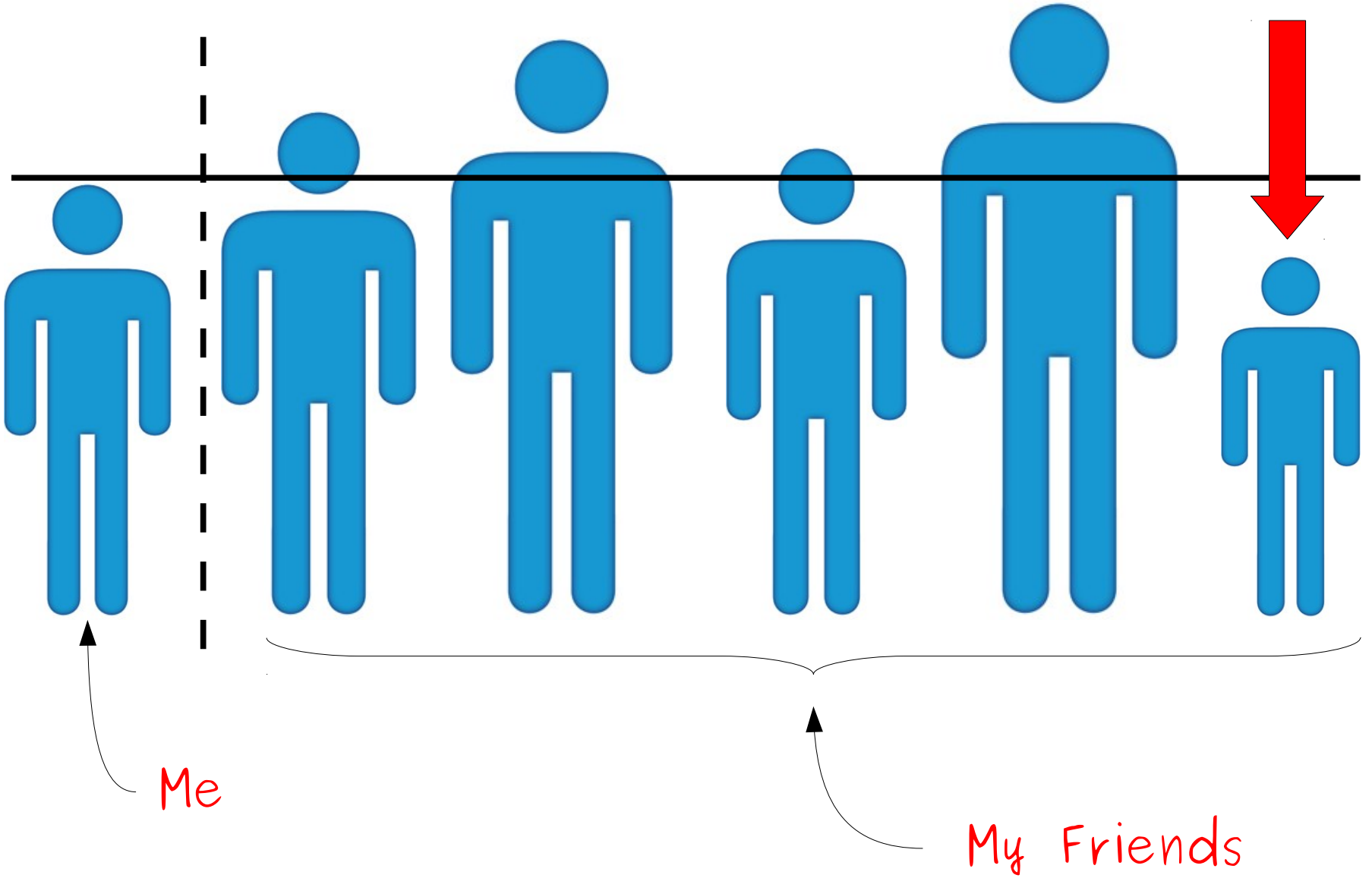
“All My Friends Are Taller Than Me”



“All My Friends Are Taller Than Me”



“All My Friends Are Taller Than Me”



What is the contradiction of the following statement?

"For any positive integer n, the sum of all smaller positive integers is not equal to n."

What is the contradiction of the following statement?

"For any positive integer n, the sum of all smaller positive integers is not equal to n."

Answer:

"For **some** positive integer n, the sum of all smaller positive integers **is** equal to n."

Another Incorrect Proof

Theorem: There is an integer that is smaller than all other integers.

Proof: By contradiction; assume that there is an integer that is *larger* than all other integers (call this integer n). Then n + 1 is an integer, and n < n + 1. But this contradicts the fact that n is larger than all other integers. We have reached a contradiction, so our assumption was false and the theorem is true. ■

Another Incorrect Proof

Theorem: There is an integer that is smaller than all other integers.

Proof: By contradiction; **assume that there is an integer that is *larger* than all other integers** (call this integer n). Then n + 1 is an integer, and n < n + 1. But this contradicts the fact that n is larger than all other integers. We have reached a contradiction, so our assumption was false and the theorem is true. ■

Another Incorrect Proof

Theorem: There i than all other integers.

Proof: By contrad **s an integer that is *larger* tha** his integer n). Then n + 1 is an i this contradicts the fact that n is l . We have reached a contra was false and the theorem is true. ■

The contradiction of

"for some x, P(x) is true"

is **not**

"for some x, P(x) is false."

The contradiction of

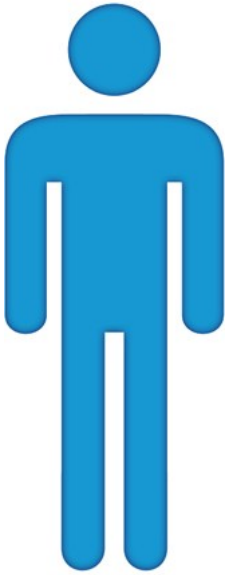
"for some x, P(x) is true"

is

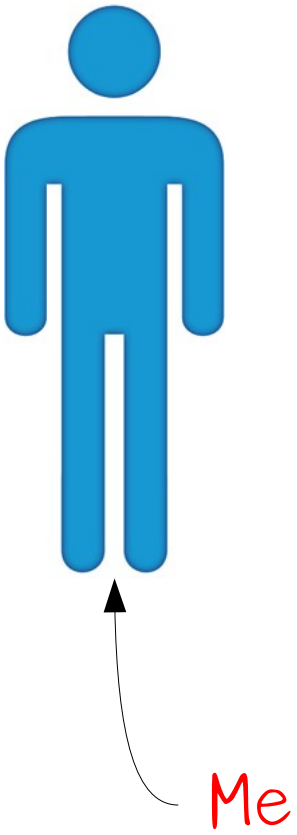
"for **all x**, P(x) is false."

“Some Friend is Shorter than Me”

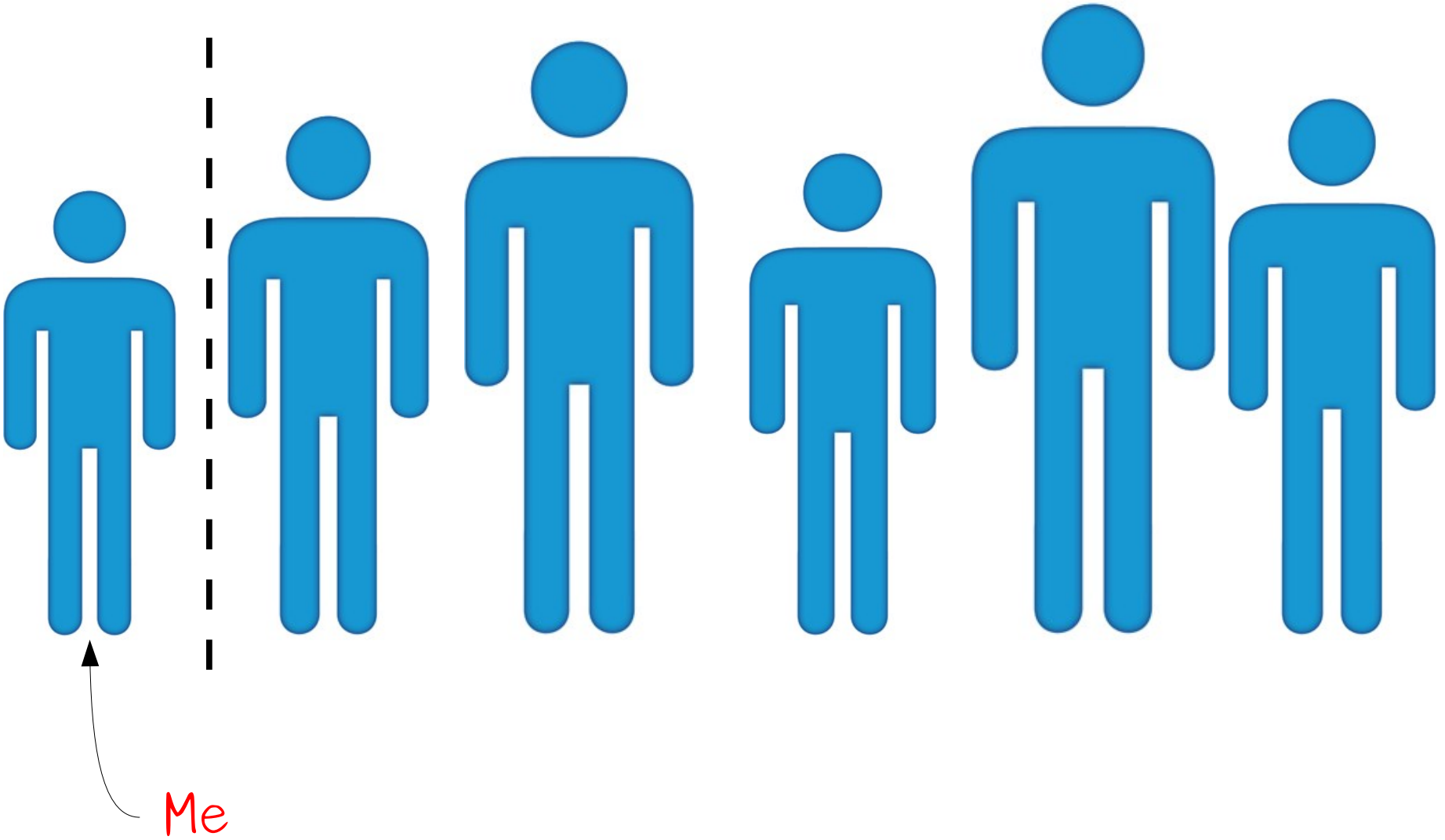
“Some Friend is Shorter than Me”



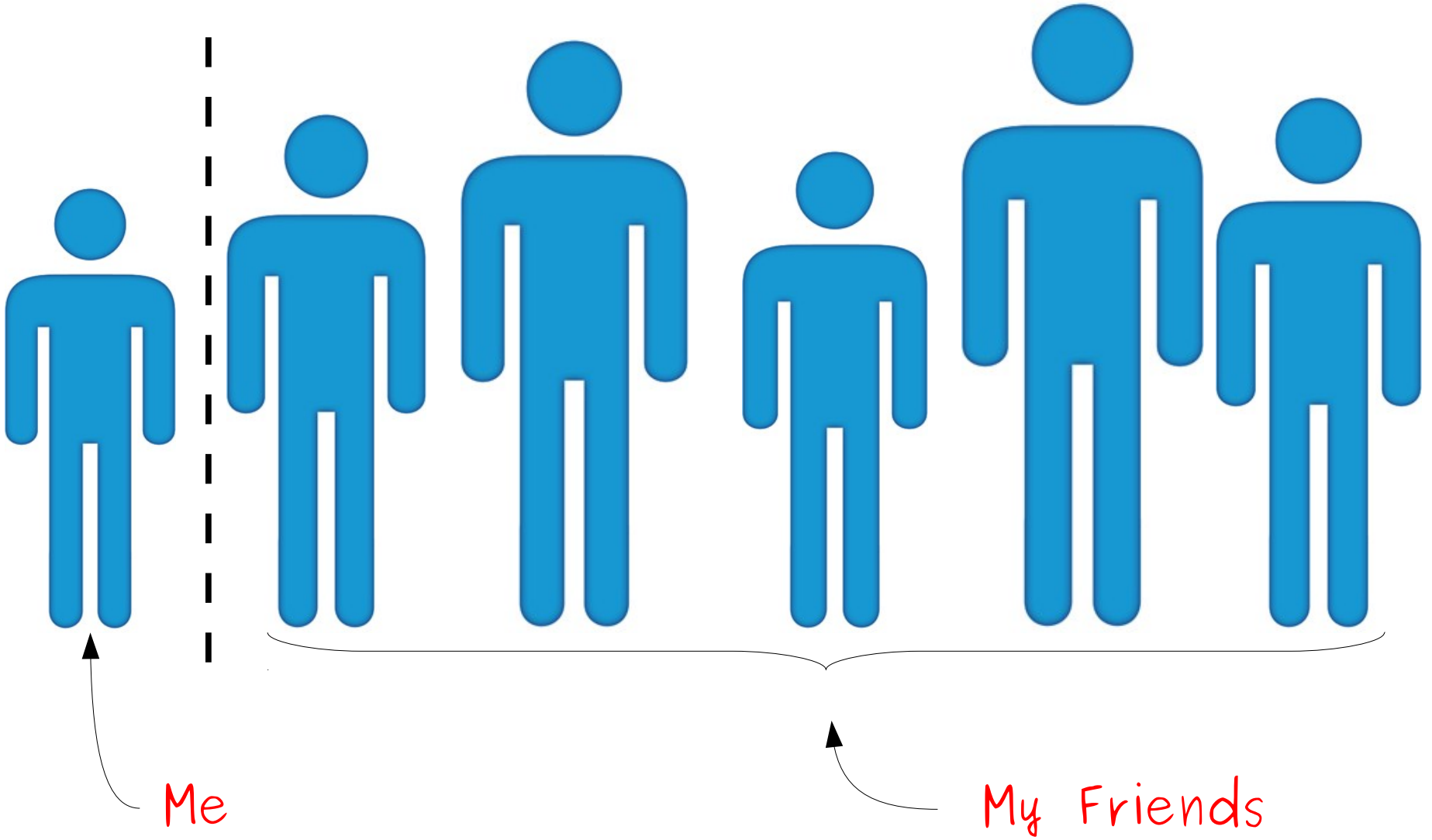
“Some Friend is Shorter than Me”



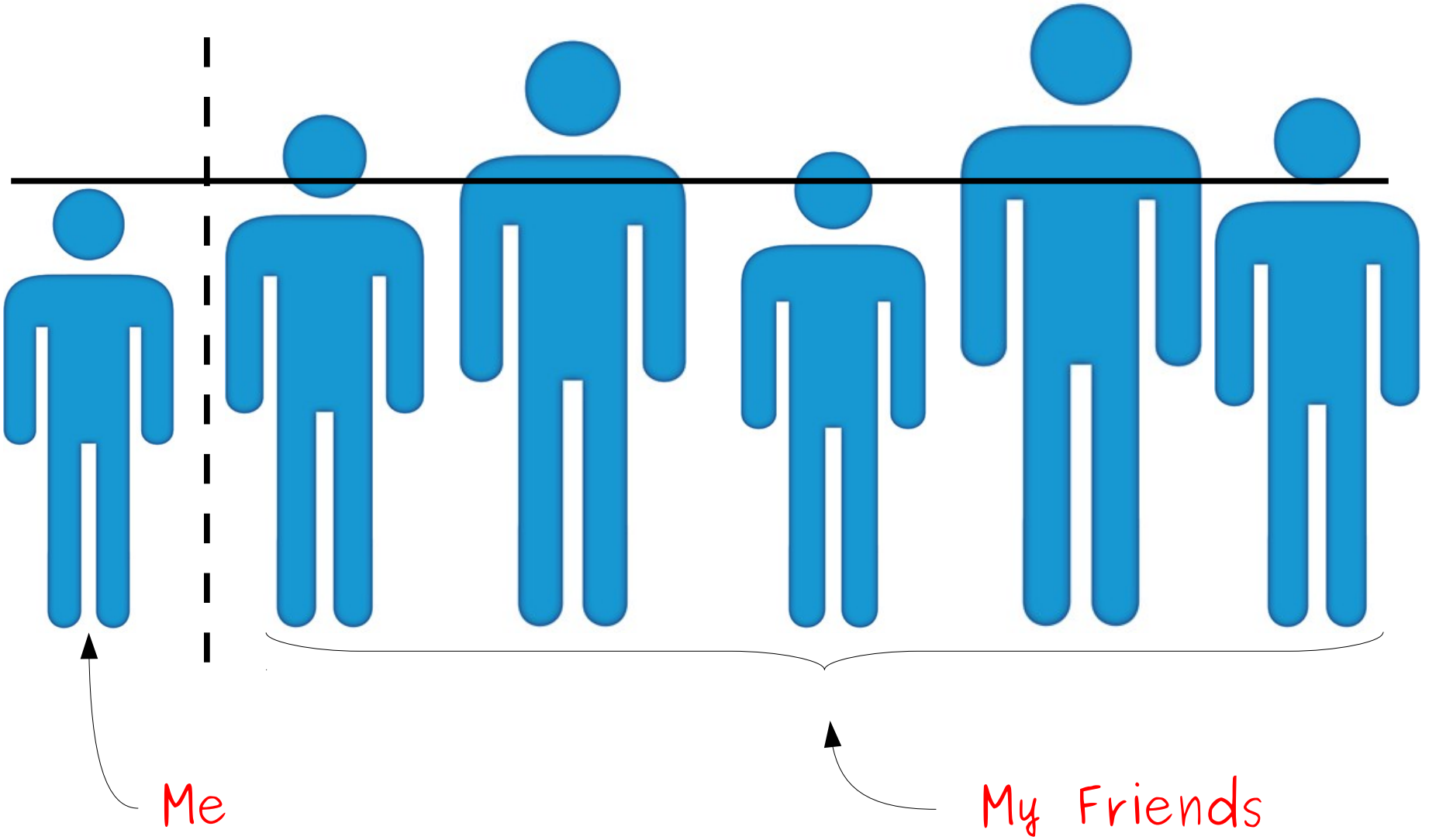
“Some Friend is Shorter than Me”



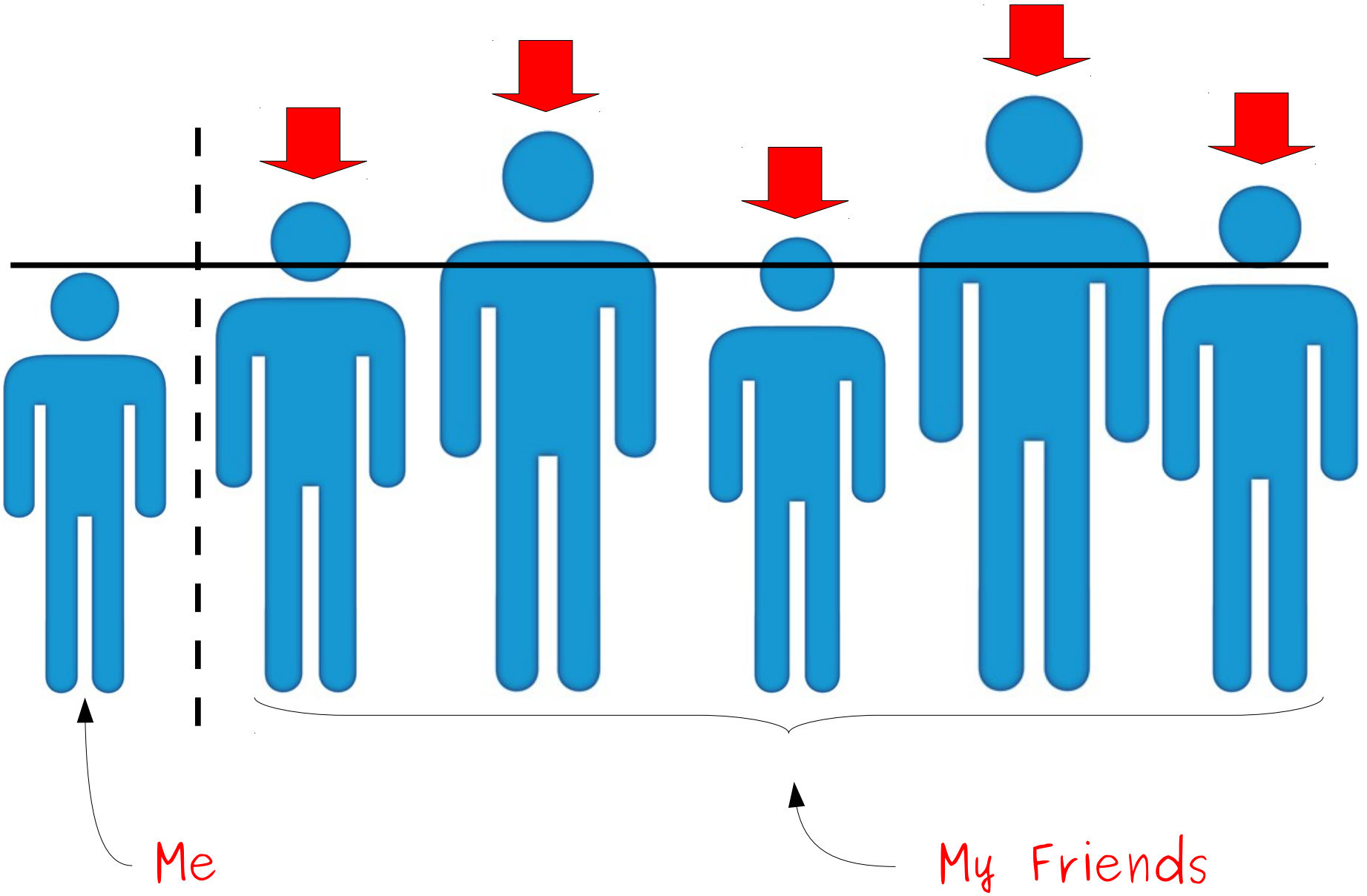
“Some Friend is Shorter than Me”



“Some Friend is Shorter than Me”



“Some Friend is Shorter than Me”



What is the contradiction of the following statement?

“There is an integer that is smaller than all other integers.”

What is the contradiction of the following statement?

“There is an integer that is smaller than all other integers.”

Answer:

“**Every integer** is **not** smaller than all other integers”

What is the contradiction of the following statement?

“There is an integer that is smaller than all other integers.”

Answer:

“**Every integer** is **not** smaller than all other integers”

What is the contradiction of the following statement?

"There is an integer that is smaller than all other integers."

Answer:

"**Every integer** is at least as large as some other integer."

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**.

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.

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 $q \neq 0$, $p = \sqrt{2}q$, 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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, 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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, 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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, p is even. Thus there is an integer k such that $p = 2k$.

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

By our earlier result, q must be even, so $q = 2m$ for some integer m.

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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, p is even. Thus there is an integer k such that $p = 2k$.

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

By our earlier result, q must be even, so $q = 2m$ for some integer m.

But this means that both p and q have 2 as a common divisor, contradicting 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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, p is even. Thus there is an integer k such that $p = 2k$.

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

By our earlier result, q must be even, so $q = 2m$ for some integer m.

But this means that both p and q have 2 as a common divisor, contradicting our earlier assertion that their only common divisors are 1 and -1.

We have reached a contradiction, so our assumption was wrong and $\sqrt{2}$ 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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, p is even. Thus there is an integer k such that $p = 2k$.

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

By our earlier result, q must be even, so $q = 2m$ for some integer m.

But this means that both p and q have 2 as a common divisor, contradicting our earlier assertion that their only common divisors are 1 and -1.

We have reached a contradiction, so our assumption was wrong and $\sqrt{2}$ 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 $q \neq 0$, $p = \sqrt{2}q$, so $p^2 = 2q^2$.

This means that p^2 is even, so by our earlier result, p is even. Thus there is an integer k such that $p = 2k$.

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

By our earlier result, q must be even, so $q = 2m$ for some integer m.

But this means that both p and q have 2 as a common divisor, contradicting our earlier assertion that their only common divisors are 1 and -1.

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

Proof by Contrapositive

The Contrapositive

- The contrapositive of “If P, then Q” is “If **not** Q, then **not** P.”
- Example:
  - “If I'd raptor-proofed my house, then I would have survived the dinosaur attack.”
  - Contrapositive: “If I didn't survive the dinosaur attack, then I didn't raptor-proof my house.”
- 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.”

Notation

- Recall that we can write “If P, then Q” as $P \rightarrow Q$.
- Notation: We write “not P” as **¬P**.
- Examples:
  - “If P is false, then Q is true:” $\neg P \rightarrow Q$
  - “Q is false whenever P is false:” $\neg P \rightarrow \neg Q$
- The contrapositive of $P \rightarrow Q$ is **$\neg Q \rightarrow \neg P$**.

Theorem: If $\neg Q \to \neg P$, then $P \to Q$.

Theorem: If $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.
Proof: By contradiction. Assume that $\neg Q \rightarrow \neg P$, but that $P \rightarrow Q$ is false.

Theorem: If $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.
Proof: By contradiction. Assume that $\neg Q \rightarrow \neg P$, but that $P \rightarrow Q$ is false. Since $P \rightarrow Q$ is false, it must be true that P is true and Q is false.

Theorem: If ¬Q → ¬P, then P → Q.
Proof: By contradiction. Assume that ¬Q → ¬P, but that P → Q is false. Since P → Q is false, it must be true that P is true and **Q is false**.

Theorem: If ¬Q → ¬P, then P → Q.
Proof: By contradiction. Assume that ¬Q → ¬P, but that P → Q is false. Since P → Q is false, it must be true that P is true and **¬Q is true**.

Theorem: If $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.
Proof: By contradiction. Assume that $\neg Q \rightarrow \neg P$, but that $P \rightarrow Q$ is false. Since $P \rightarrow Q$ is false, it must be true that P is true and $\neg Q$ is true.

Theorem: If $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.
Proof: By contradiction. Assume that $\neg Q \rightarrow \neg P$, but that $P \rightarrow Q$ is false. Since $P \rightarrow Q$ is false, it must be true that P is true and $\neg Q$ is true. Since $\neg Q$ is true and $\neg Q \rightarrow \neg P$, $\neg P$ is true.

Theorem: If $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.
Proof: By contradiction. Assume that $\neg Q \rightarrow \neg P$, but that $P \rightarrow Q$ is false. Since $P \rightarrow Q$ is false, it must be true that P is true and $\neg Q$ is true. Since $\neg Q$ is true and $\neg Q \rightarrow \neg P$, $\neg P$ is true. But this means that we have shown P and $\neg P$, which is impossible. We have reached a contradiction, so if $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.

Theorem: If $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$.
Proof: By contradiction. Assume that $\neg Q \rightarrow \neg P$, but that $P \rightarrow Q$ is false. Since $P \rightarrow Q$ is false, it must be true that P is true and $\neg Q$ is true. Since $\neg Q$ is true and $\neg Q \rightarrow \neg P$, $\neg P$ is true. But this means that we have shown P and $\neg P$, which is impossible. We have reached a contradiction, so if $\neg Q \rightarrow \neg P$, then $P \rightarrow Q$. ■

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: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Theorem: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Proof: By contrapositive. **????**

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

both $x < 8$ and $y < 8$

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

both $x < 8$ and $y < 8$

Pro tip: The opposite of "either A or B" is "not A and not B"

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

both $x < 8$ and $y < 8$

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

both $x < 8$ and $y < 8$

then

If

$x + y = 16$

then

either $x \geq 8$ or $y \geq 8$

If

both $x < 8$ and $y < 8$

then

$x + y \neq 16$

Theorem: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Proof: By contrapositive. **????**

Theorem: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Proof: By contrapositive. We prove that if both $x < 8$ and $y < 8$, then $x + y \neq 16$.

Theorem: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Proof: By contrapositive. We prove that if both $x < 8$ and $y < 8$, then $x + y \neq 16$. Since both $x < 8$ and $y < 8$, then $x + y < 16$, so $x + y \neq 16$.

Theorem: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Proof: By contrapositive. We prove that if both $x < 8$ and $y < 8$, then $x + y \neq 16$. Since both $x < 8$ and $y < 8$, then $x + y < 16$, so $x + y \neq 16$. ■

Theorem: If $x + y = 16$, then either $x \geq 8$ or $y \geq 8$.

Proof: By contrapositive. We prove that if both $x < 8$ and $y < 8$, then $x + y \neq 16$. Since both $x < 8$ and $y < 8$, then $x + y < 16$, so $x + y \neq 16$. ■

If

n^2 is even

then

n is even

If

n^2 is even

then

n is even

If

If

n^2 is even

then

n is even

If

n is odd

If

n^2 is even

then

n is even

If

n is odd

then

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, n^2 is odd. Since n is odd, $n = 2k + 1$ for some integer k. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so n^2 is odd. ■

An Incorrect Proof

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

An Incorrect Proof

Theorem: For any sets A and B, if $x \in A$, then $x \in A \cap B$.
Proof: By contrapositive, we show that if $x \notin A$, then $x \notin A \cap B$. This is true by definition: $x \in A \cap B$ iff $x \in A$ and $x \in B$. Since $x \notin A$, $x \notin A \cap B$ either. ■

An Incorrect Proof

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

Proof: By contrapositive, we show that **if $x \notin A$, then $x \notin A \cap B$**. This is true by definition: $x \in A \cap B$ iff $x \in A$ and $x \in B$. Since $x \notin A$, $x \notin A \cap B$ either. ■

An Incorrect Proof

Theorem: For …hen $x \in A \cap B$.

Proof: By cont… **$\notin A$, then**

$x \notin A \cap$ …: $x \in A \cap B$ iff

$x \in A$ a… $A \cap B$ either. ■

Common Pitfalls

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

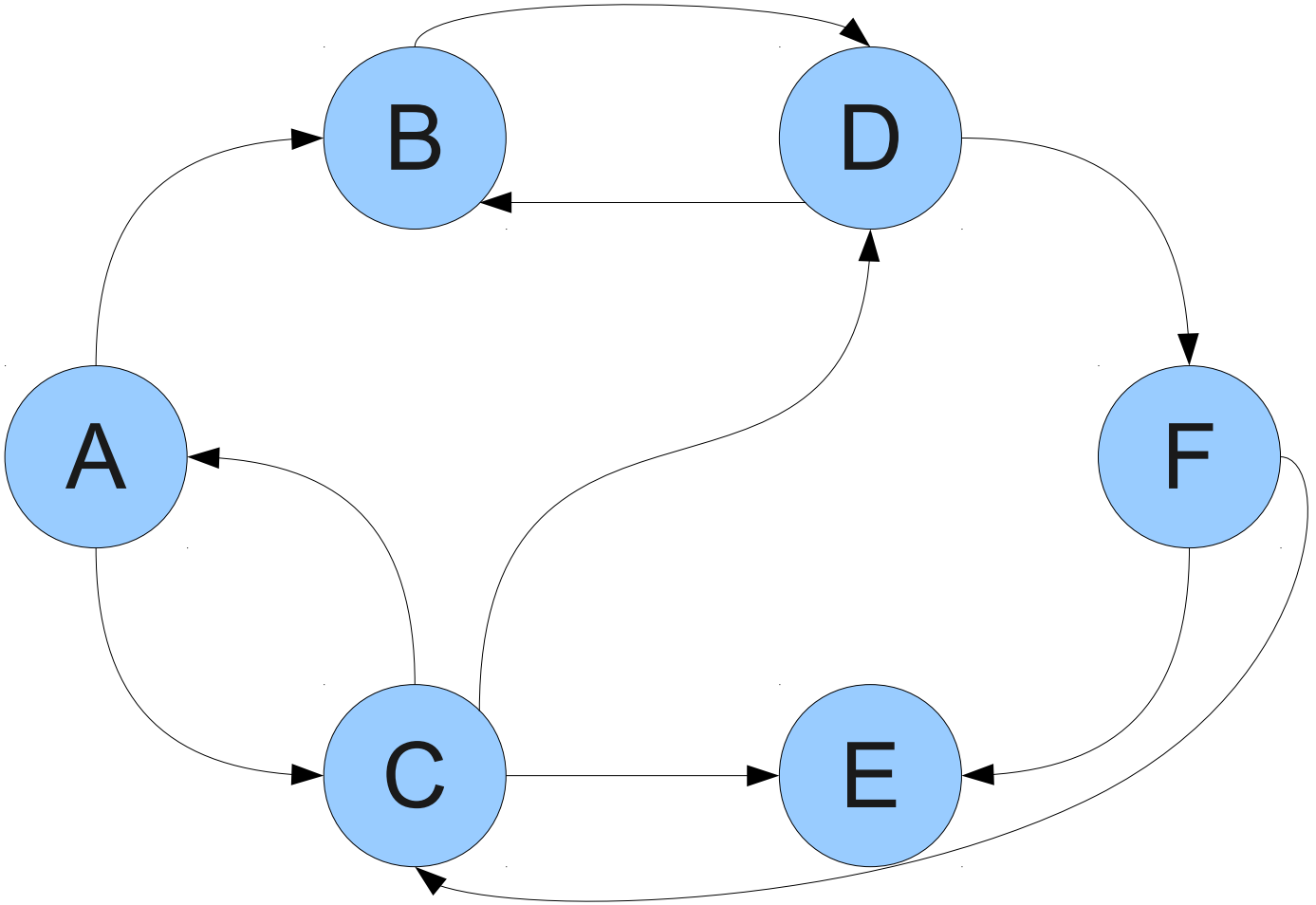
$$\neg Q \rightarrow \neg P$$

Do not show that

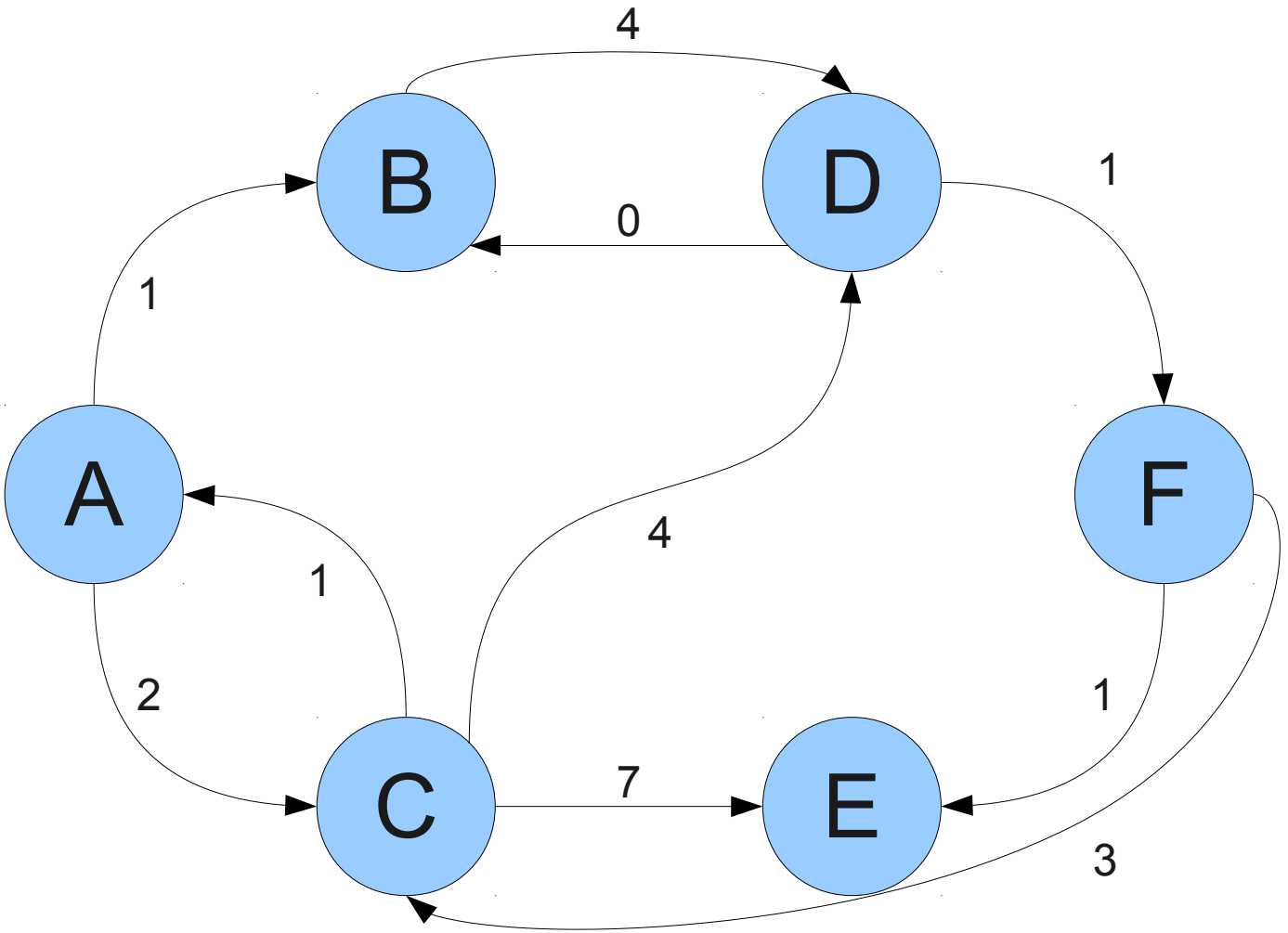
$$\neg P \rightarrow \neg Q$$

(This is equivalent to showing that $Q \rightarrow P$!)

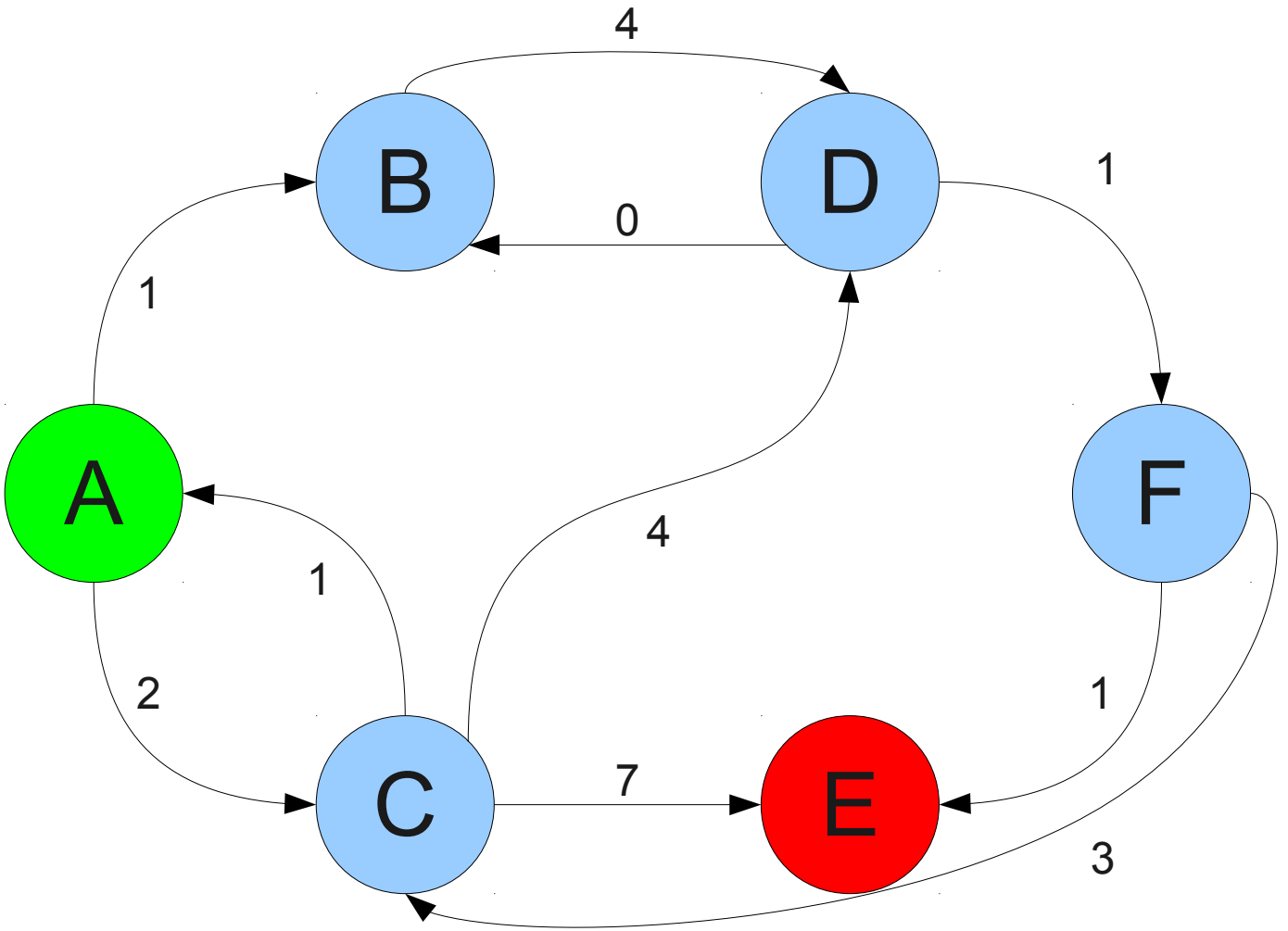
Shortest Paths in a Graph



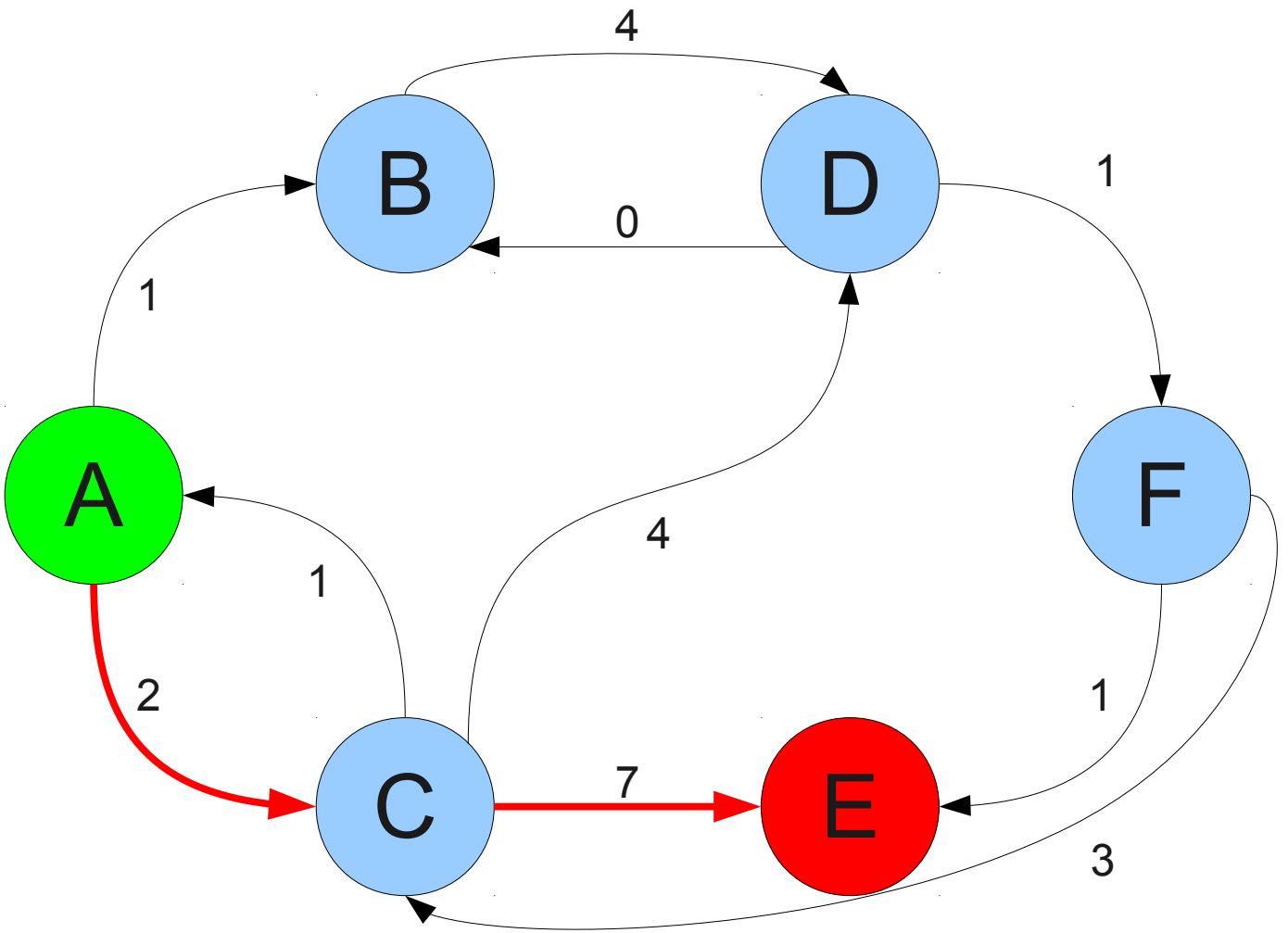
Shortest Paths in a Graph



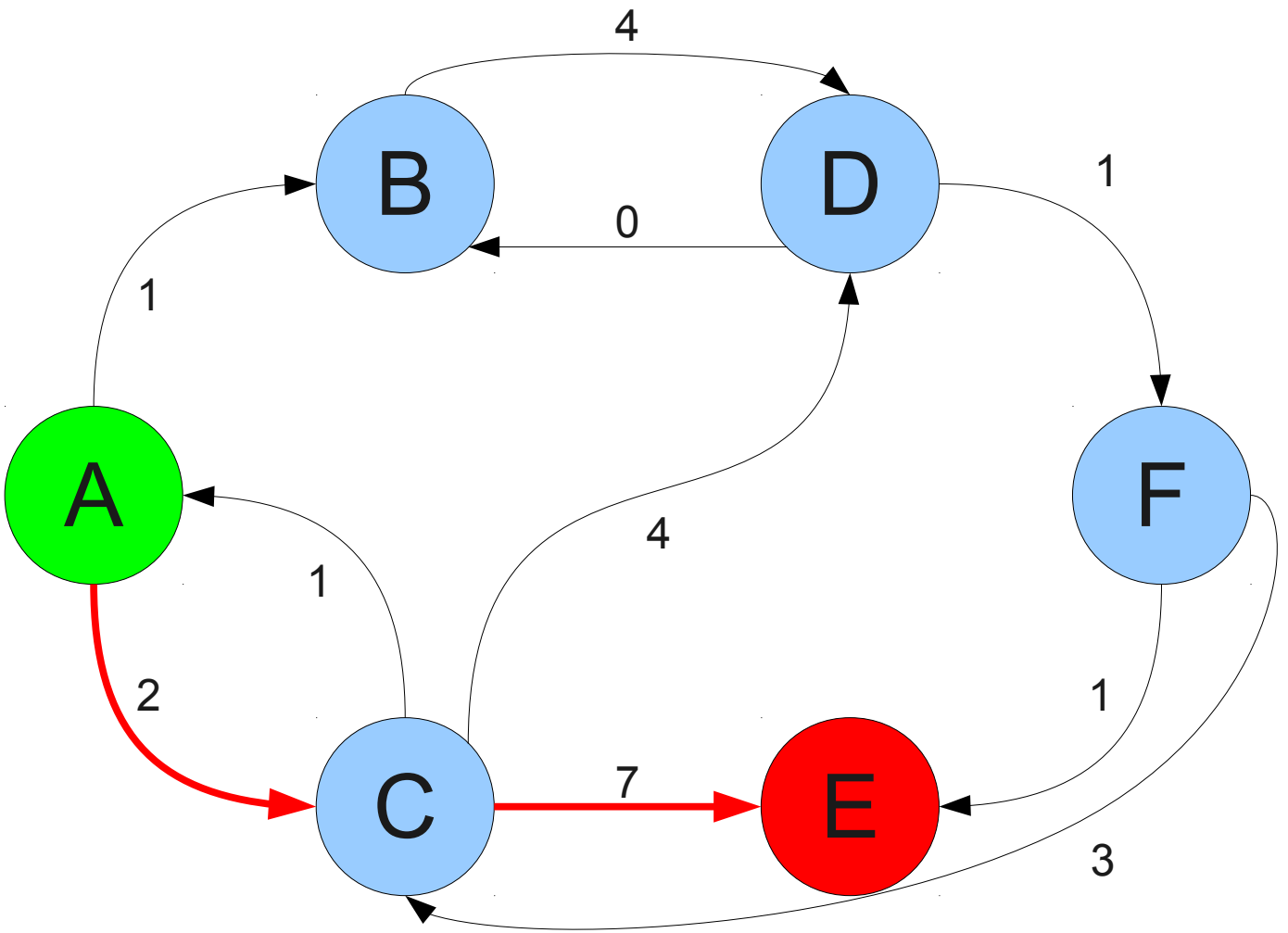
Shortest Paths in a Graph



Shortest Paths in a Graph

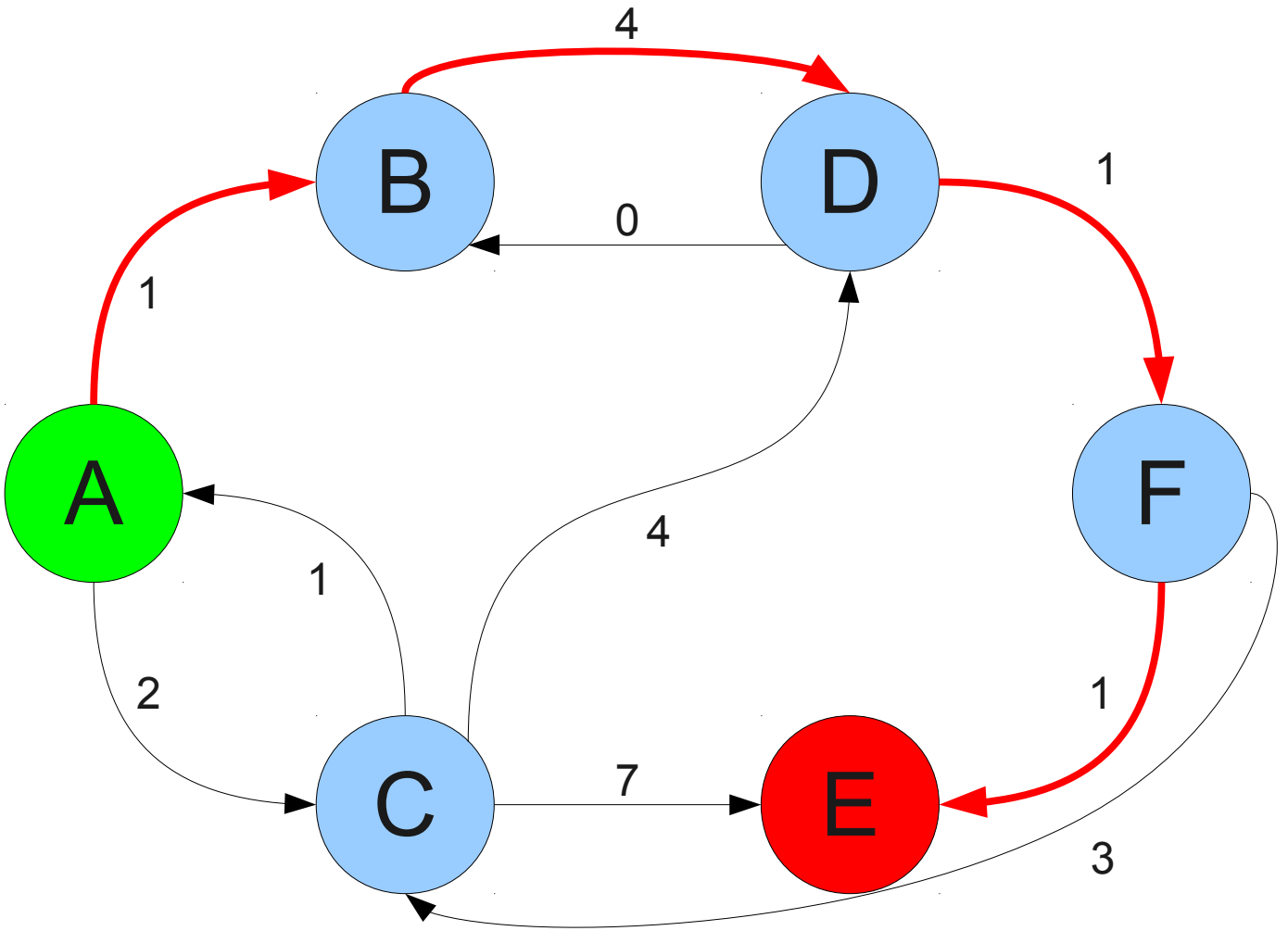


Shortest Paths in a Graph

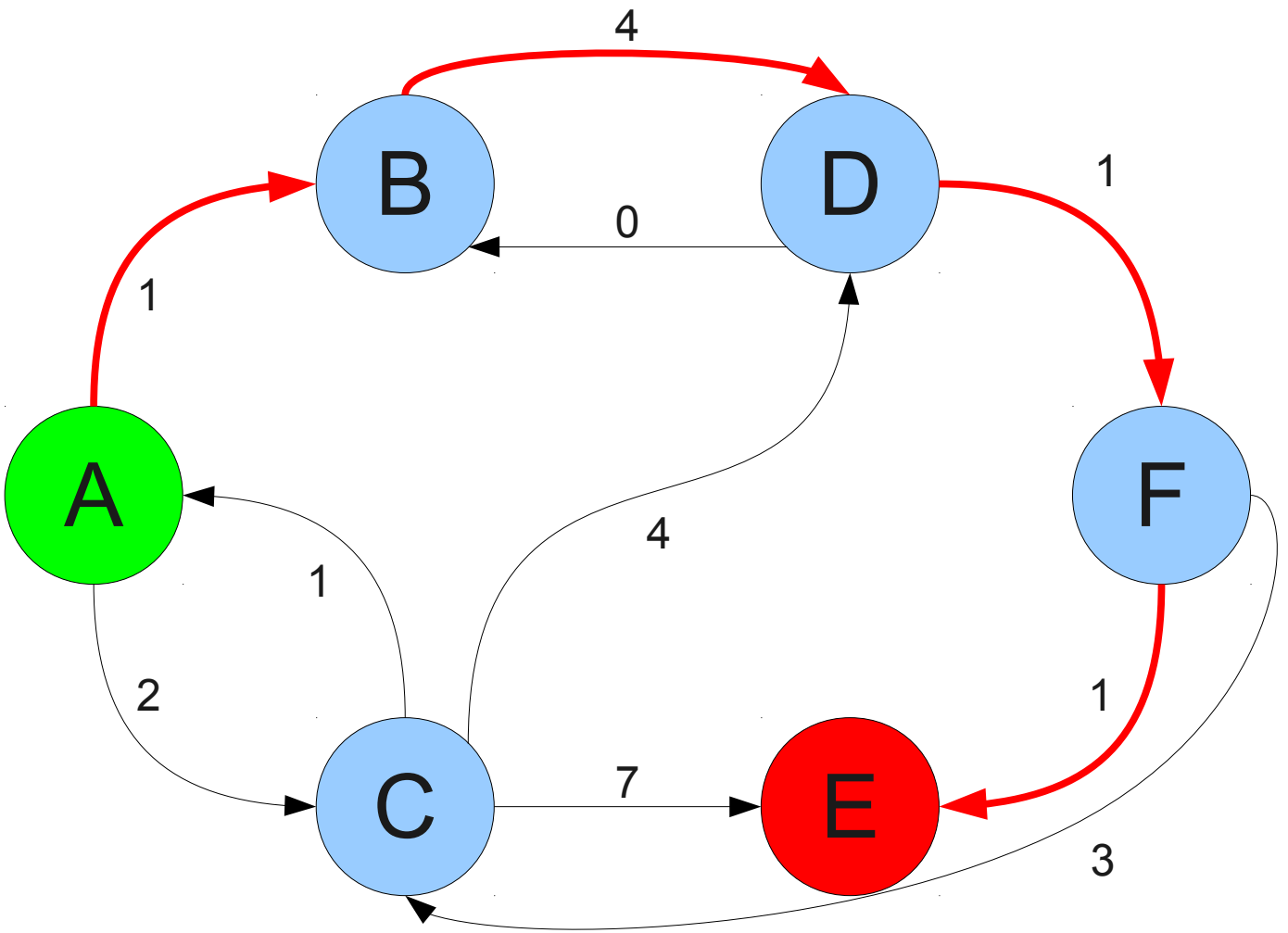


Cost: **9**

Shortest Paths in a Graph

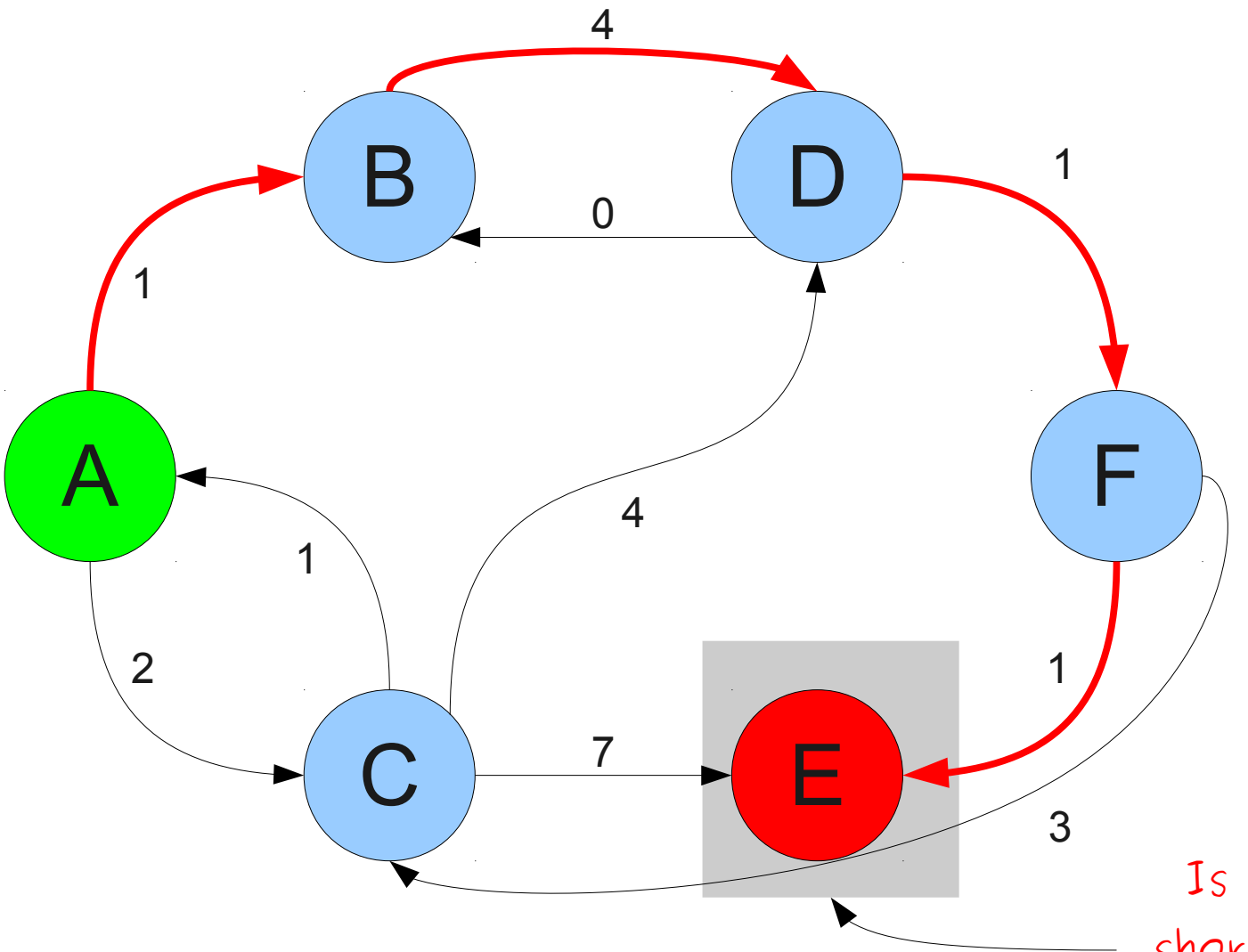


Shortest Paths in a Graph



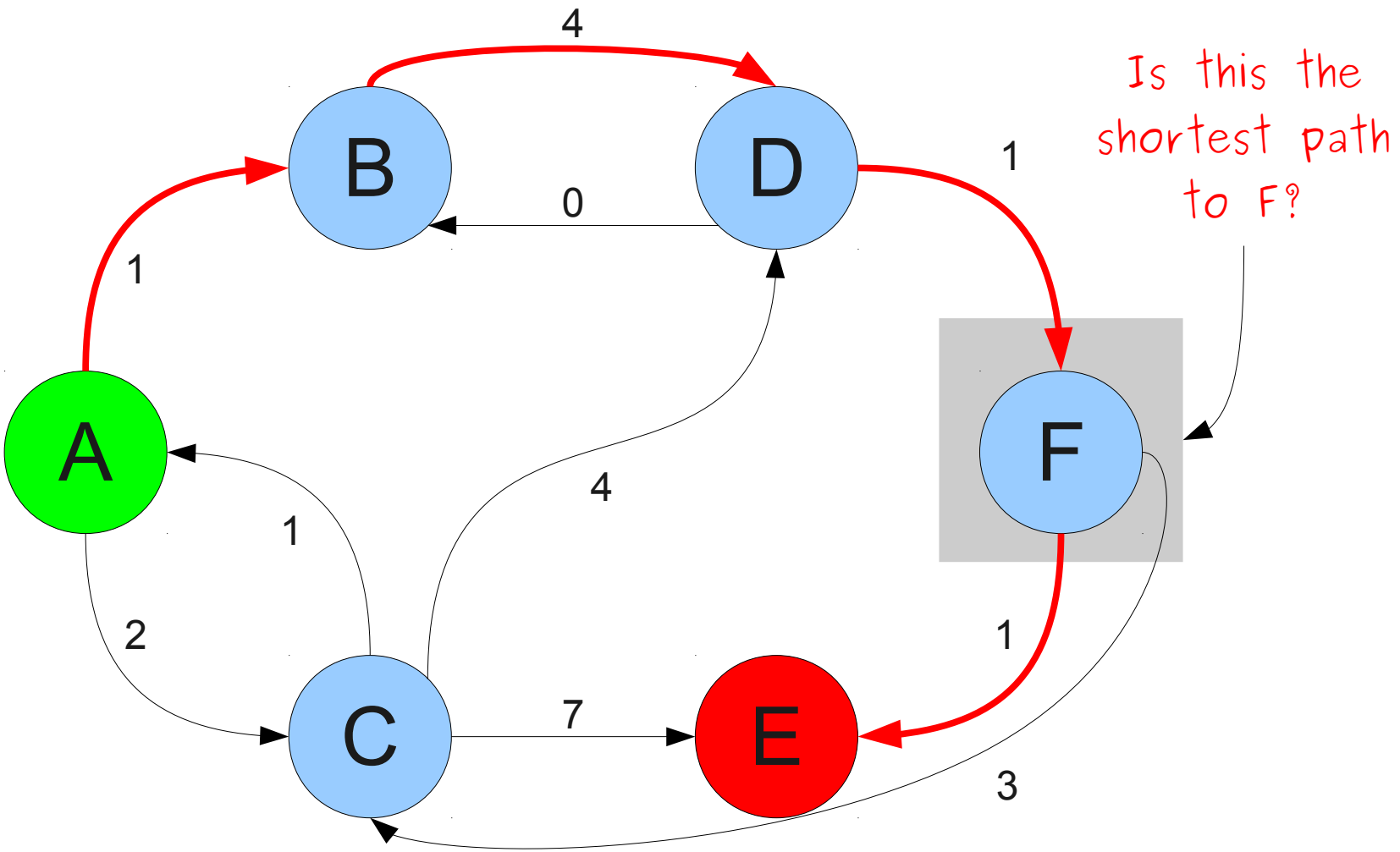
Cost: **7**

Shortest Paths in a Graph



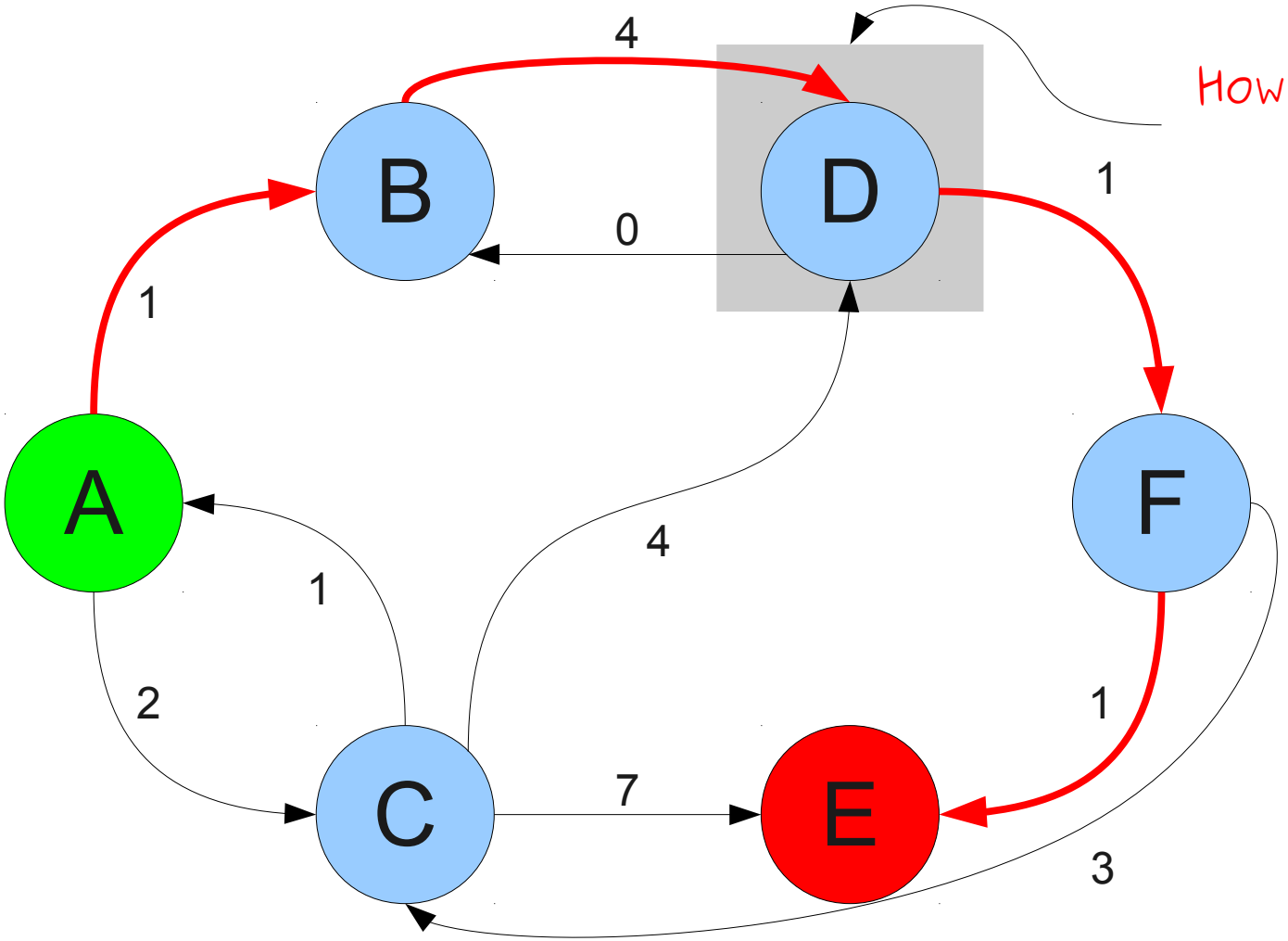
Cost: **7**

Shortest Paths in a Graph



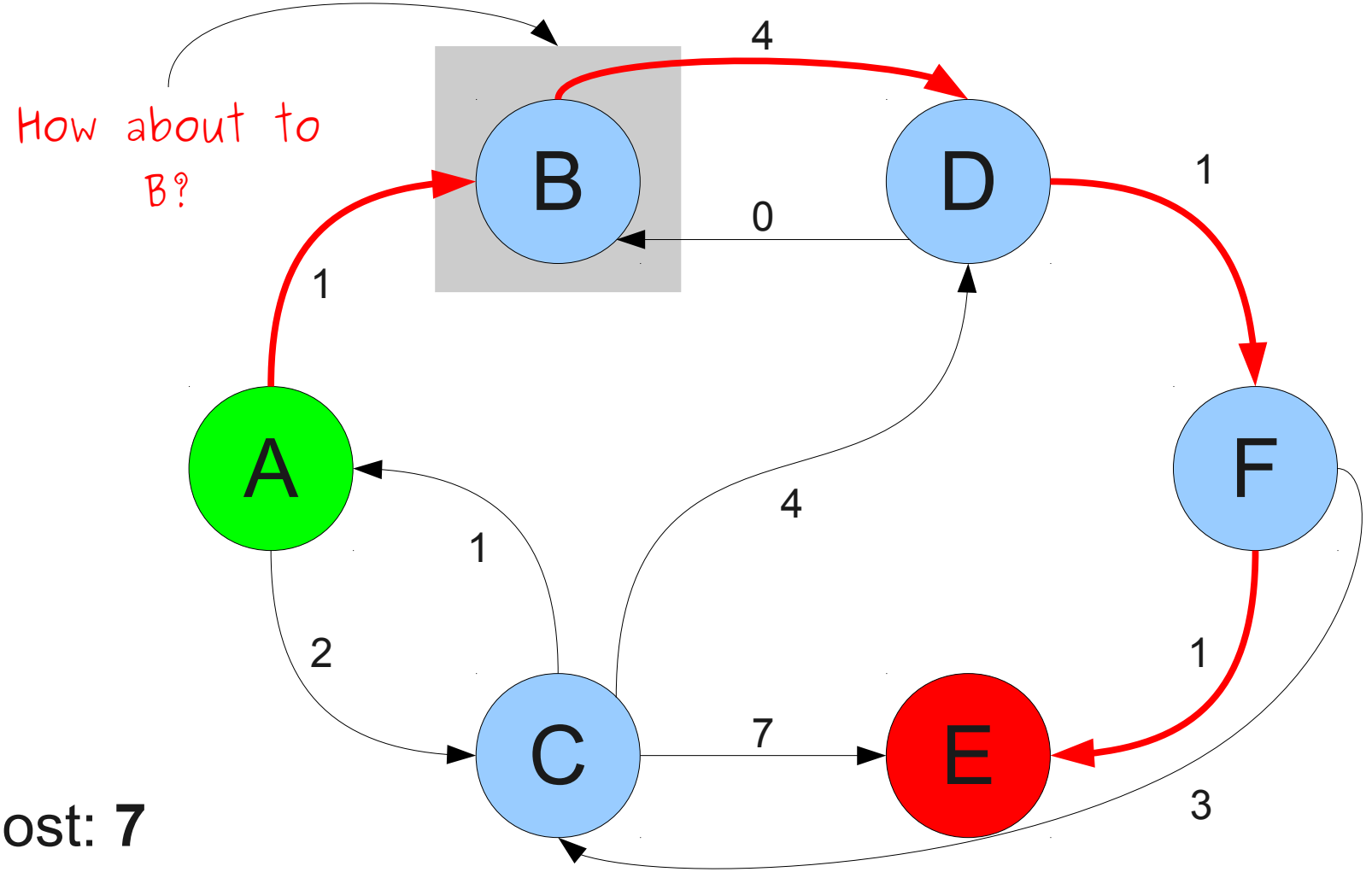
Cost: **7**

Shortest Paths in a Graph



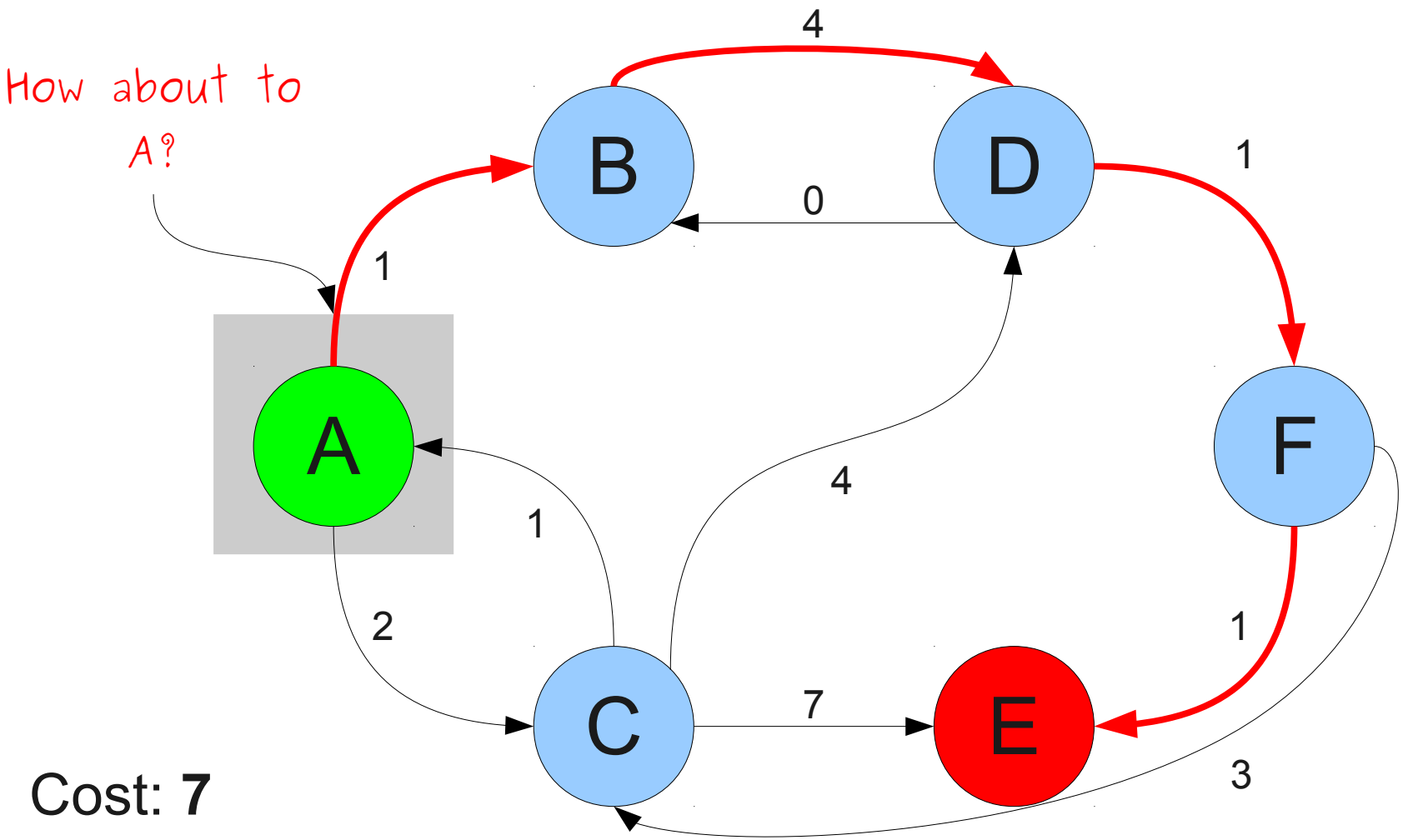
Cost: **7**

Shortest Paths in a Graph



Cost: **7**

Shortest Paths in a Graph



Question

Suppose we have a shortest path from u to v.

Is that path also the shortest path to each other node in the path?

Question

Suppose **we have a shortest path from u to v**.

Is that path also the shortest path to each other node in the path?

Question

Suppose **$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.**

Is that path also the shortest path to each other node in the path?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

Is that path also the shortest path to each other node in the path?

Question

Pro tip: Assign numbers to elements of a sequence.

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

Is that path also the shortest path to each other node in the path?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

Is that path also the shortest path to each other node in the path?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

Is that path also the shortest path to **each other node** in the path?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

For any $k \leq n$, is the path a shortest path from v_0 to v_k?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

For any $k \leq n$, is the path a shortest path from v_0 to v_k?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

For any $k \leq n$, is **the path** a shortest path from v_0 to v_k?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

For any $k \leq n$, is **$((v_0, v_1), \ldots, (v_{k-1}, v_k))$** a shortest path from v_0 to v_k?

Question

Suppose $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n.

For any $k \leq n$, is $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ a shortest path from v_0 to v_k?

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

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

If

$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n,

then

for any $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

If

$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n,

then

for any $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

If

If

$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n,

then

for any $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

If

for **some** $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is **not** a shortest path from v_0 to v_k.

If

$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n,

then

for any $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

If

for **some** $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is **not** a shortest path from v_0 to v_k.

then

If

$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n,

then

for any $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

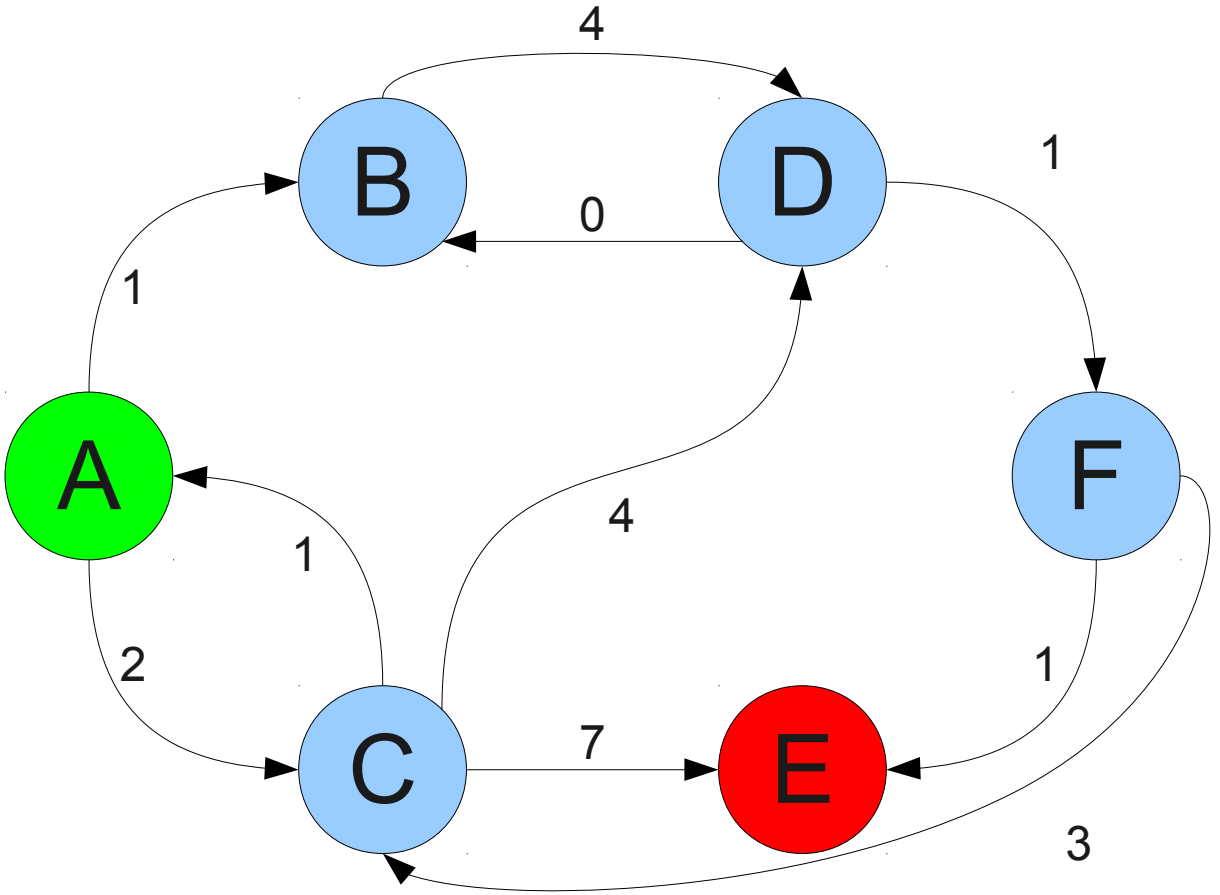
If

for **some** $k \leq n$, $((v_0, v_1), \ldots, (v_{k-1}, v_k))$ is **not** a shortest path from v_0 to v_k.

then

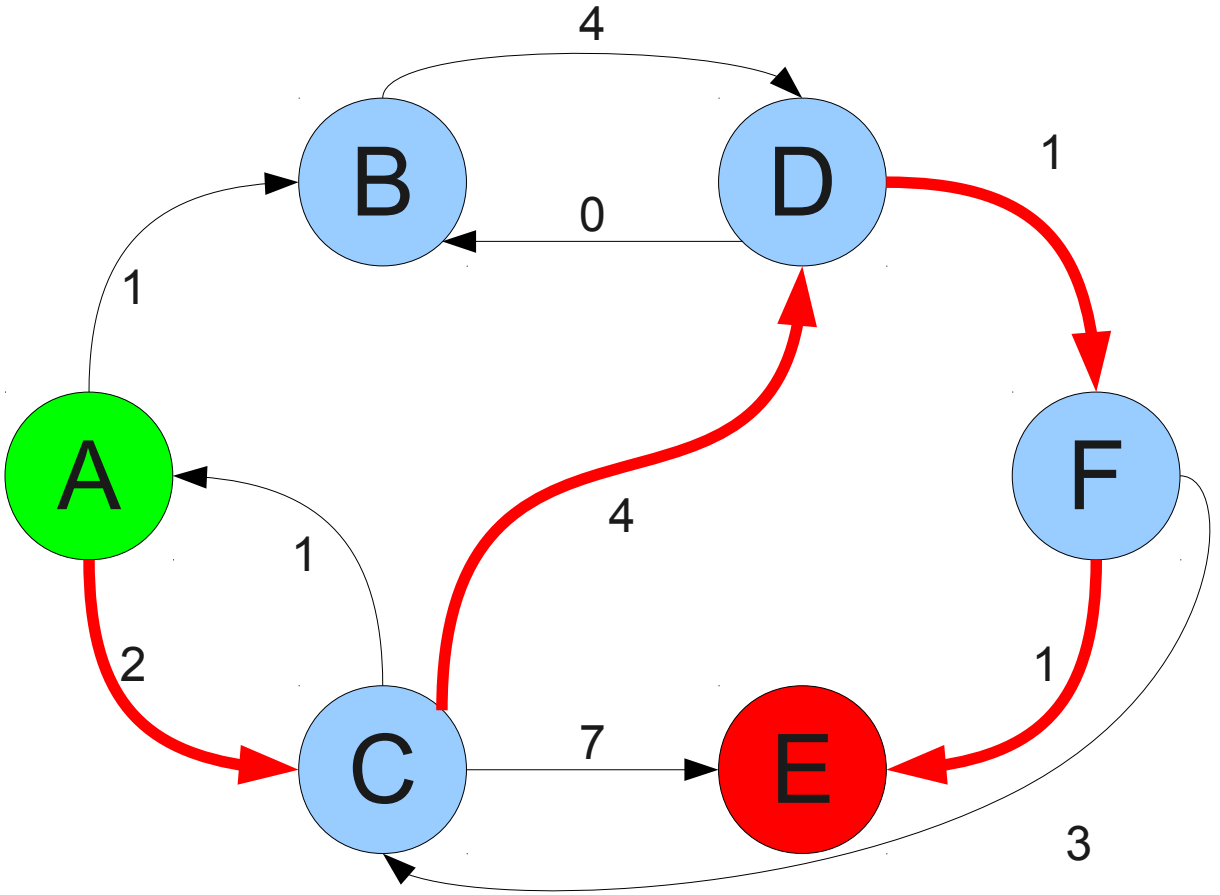
$((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is **not** a shortest path from v_0 to v_n,

An Intuition



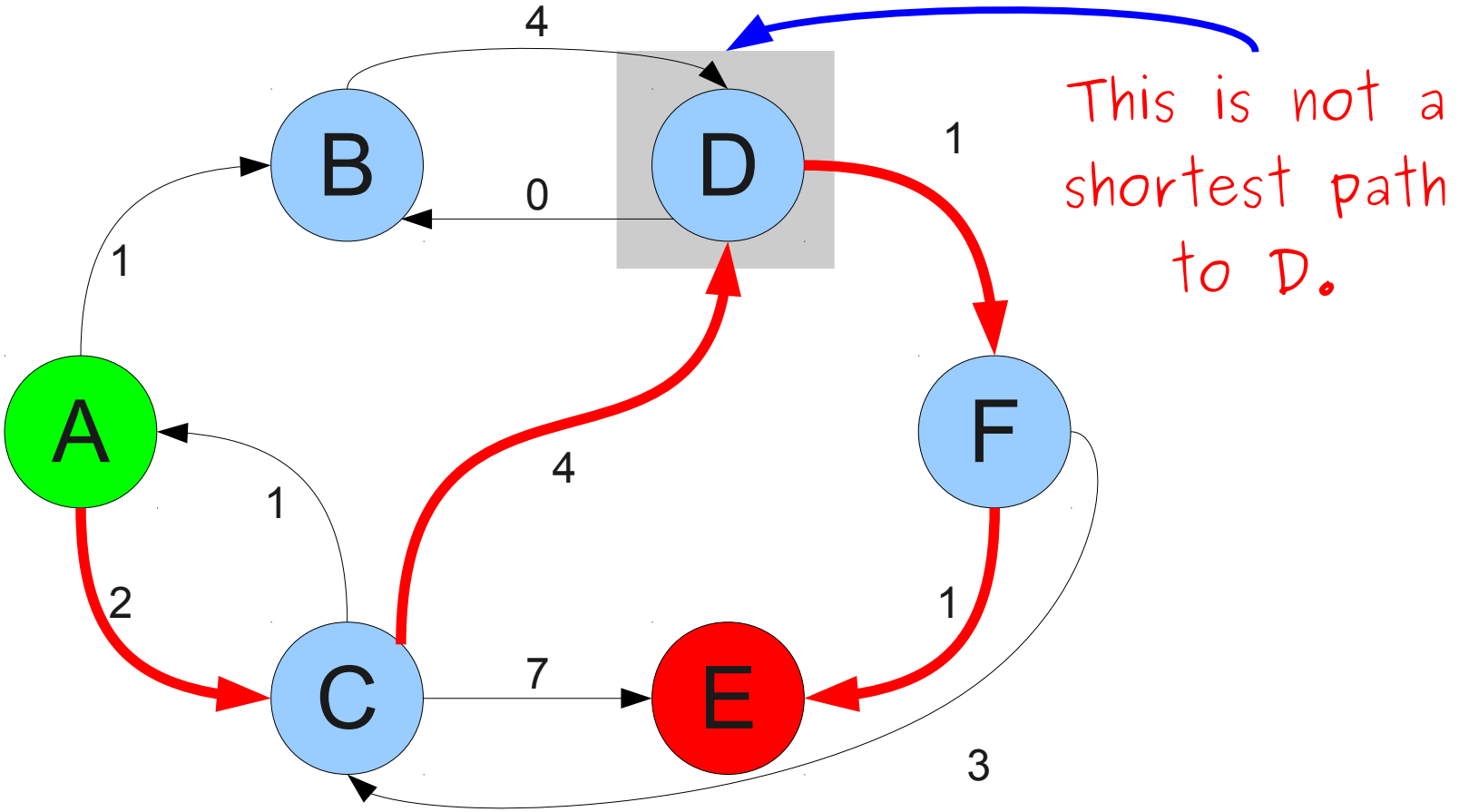
If for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

An Intuition



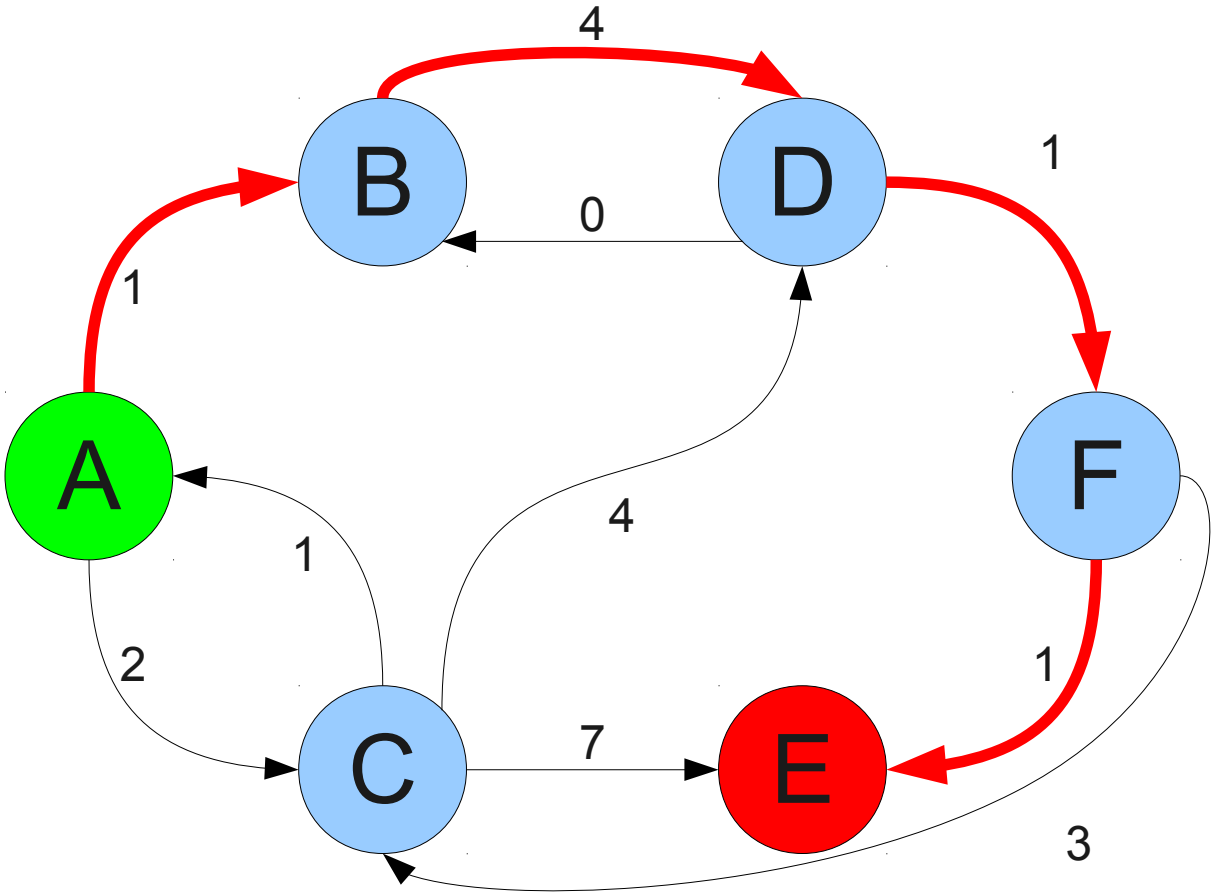
If for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

An Intuition



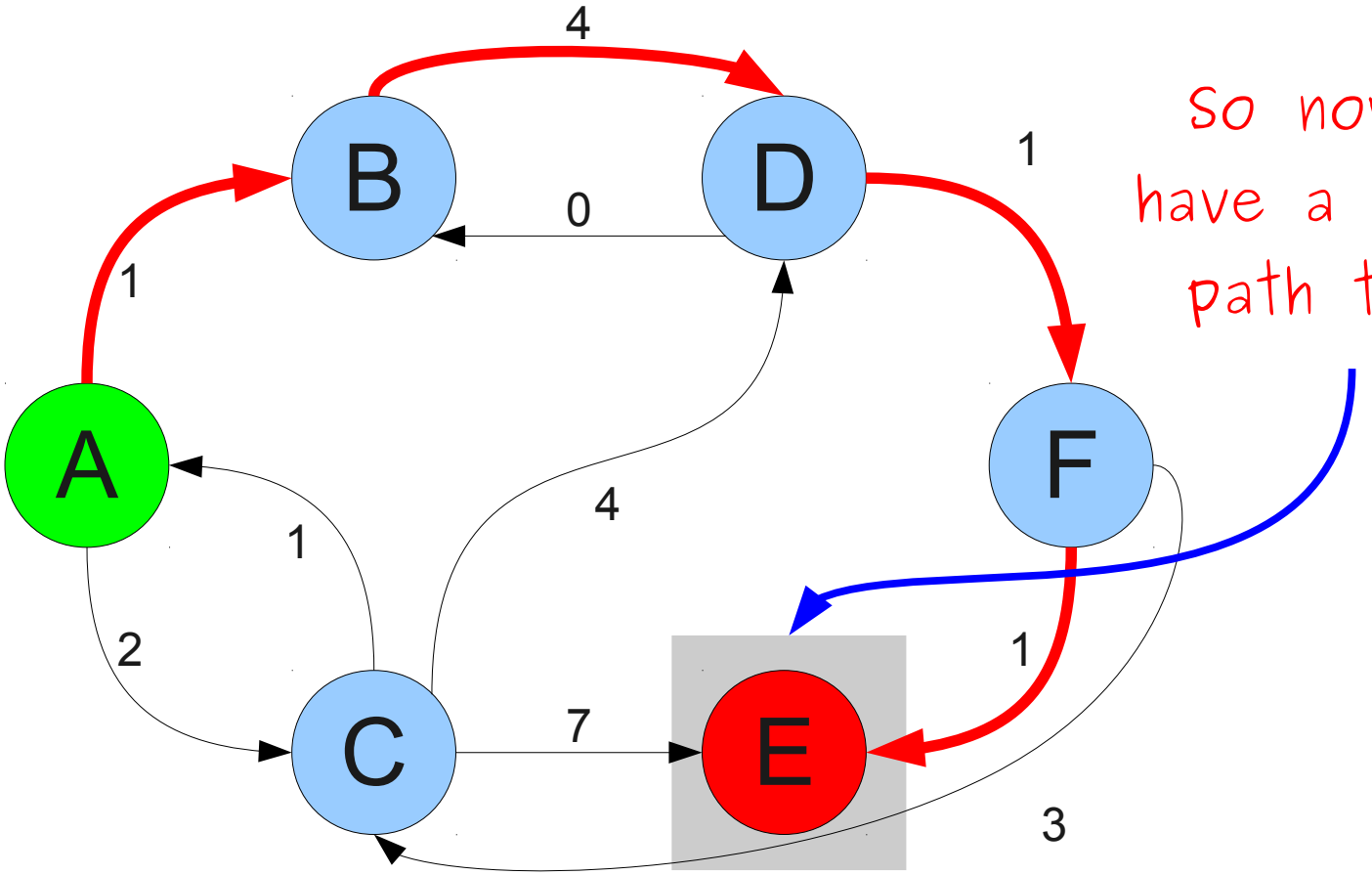
If for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

An Intuition



If for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

An Intuition



If for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

Proof: By contrapositive; we show that if for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

Proof: By contrapositive; we show that if for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

Since $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, there must be some path $((v_0, u_1), (u_1, u_2), \ldots, (u_m, v_k))$ that is a shorter path.

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

Proof: By contrapositive; we show that if for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

Since $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, there must be some path $((v_0, u_1), (u_1, u_2), \ldots, (u_m, v_k))$ that is a shorter path.

Then the path $((v_0, u_1), (u_1, u_2), \ldots, (u_m, v_k), (v_k, v_{k+1}), \ldots, (v_{n-1}, v_n))$ is a shorter path from v_0 to v_n than our original path, so our original path is not a shortest path.

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

Proof: By contrapositive; we show that if for some $k \leq n$, if $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, then $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is not a shortest path from v_0 to v_n.

Since $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is not a shortest path from v_0 to v_k, there must be some path $((v_0, u_1), (u_1, u_2), \ldots, (u_m, v_k))$ that is a shorter path.

Then the path $((v_0, u_1), (u_1, u_2), \ldots, (u_m, v_k), (v_k, v_{k+1}), \ldots, (v_{n-1}, v_n))$ is a shorter path from v_0 to v_n than our original path, so our original path is not a shortest path. ■

Theorem: If $((v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n))$ is a shortest path from v_0 to v_n, then for any $k \leq n$, $((v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k))$ is a shortest path from v_0 to v_k.

Proof: By con…me k ≤ n, if $((v_0, v_1), (v_1, v$ …th from v_0 to v_k, then $((v_0, v$ …ortest path from v_0 to v_n.

Since $((v_0, v_1)$ …test path from v_0 to v_k, there … $_2), \ldots, (u_m, v_k))$ that is a short…

Then the path $((v_0, u_1), (u_1, u_2), \ldots, (u_m, v_k), (v_k, v_{k+1}), \ldots, (v_{n-1}, v_n))$ is a shorter path from v_0 to v_n than our original path, so our original path is not a shortest path. ■

Review

- A **proof** is a series of logically sound steps that proves a **conclusion** from a set of **hypotheses**.
- A **direct proof** works by showing the conclusion directly follows from the hypotheses.
  - To prove “if A, then B,” assume A and use it to show B.
  - To prove “for any x, P is true,” prove that for any choice of x, P is true.
  - To prove “there is some x for which P is true”, choose a specific x that demonstrates it.
- A **proof by contradiction** works by assuming the conclusion is false and arriving at an impossibility.
  - The contradiction of “if A, then B” is “A and not B.”
  - The contradiction of “for all x, P is true” is “for some x, P is false.”
  - The contradiction of “for some x, P is true” is “for all x, P is false.”
- A **proof by contrapositive** proves that A implies B by proving that not B implies not A.

Next Time

Proof by Induction