Propositional Logic

Question: How do we formalize the definitions and reasoning we use in our proofs?

Where We're Going

- ***Propositional Logic*** (Today)
  - Reasoning about Boolean values.
- ***First-Order Logic*** (Wednesday/Friday)
  - Reasoning about properties of multiple objects.

Propositional Logic

A ***proposition*** is a statement that is, by itself, either true or false.

Some Sample Propositions

- I am not throwing away my shot.
- I’m just like my country.
- I’m young, scrappy, and hungry.
- I’m not throwing away my shot.
- I’m ‘a get a scholarship to King’s College.
- I prob’ly shouldn’t brag, but dag, I amaze and astonish.
- The problem is I got a lot of brains but no polish.

Things That Aren't Propositions

Commands cannot be true or false.

Things That Aren't Propositions

Questions cannot be true or false.

Propositional Logic

- ***Propositional logic*** is a mathematical system for reasoning about propositions and how they relate to one another.
- Every statement in propositional logic consists of ***propositional variables*** combined via ***propositional connectives***.
  - Each variable represents some proposition, such as "You liked it" or "You should have put a ring on it."
  - Connectives encode how propositions are related, such as "If you liked it, then you should have put a ring on it."

Propositional Variables

- Each proposition will be represented by a ***propositional variable***.
- Propositional variables are usually represented as lower-case letters, such as *p, q, r, s,* etc.
- Each variable can take one one of two values: true or false.

Propositional Connectives

- There are seven propositional connectives, many of which will be familiar from programming.
- First, there's the logical "NOT" operation:

$$\neg p$$

- You'd read this out loud as "not *p*."
- The fancy name for this operation is ***logical negation***.

Propositional Connectives

- There are seven propositional connectives, many of which will be familiar from programming.
- Next, there's the logical "AND" operation:

$$p \land q$$

- You'd read this out loud as "*p* and *q*."
- The fancy name for this operation is ***logical conjunction***.

Propositional Connectives

- There are seven propositional connectives, many of which will be familiar from programming.
- Then, there's the logical "OR" operation:

$$\boldsymbol{p \lor q}$$

- You'd read this out loud as "*p* or *q*."
- The fancy name for this operation is ***logical disjunction***. This is an *inclusive* or.

Truth Tables

- A ***truth table*** is a table showing the truth value of a propositional logic formula as a function of its inputs.
- Let's go look at the truth tables for the three connectives we've seen so far:

$$\neg \qquad \land \qquad \lor$$

Summary of Important Points

- The ∨ connective is an *inclusive* "or." It's true if at least one of the operands is true.
  - Similar to the `||` operator in C, C++, Java, etc. and the `or` operator in Python.
- If we need an exclusive "or" operator, we can build it out of what we already have.

Try it yourself: Combine the ¬, ∧, and ∨ operators together to form an expression that represents the exclusive or of p and q (something that's true if and only if exactly one of p and q are true).

Respond at pollev.com/cs103

Mathematical Implication

Implication

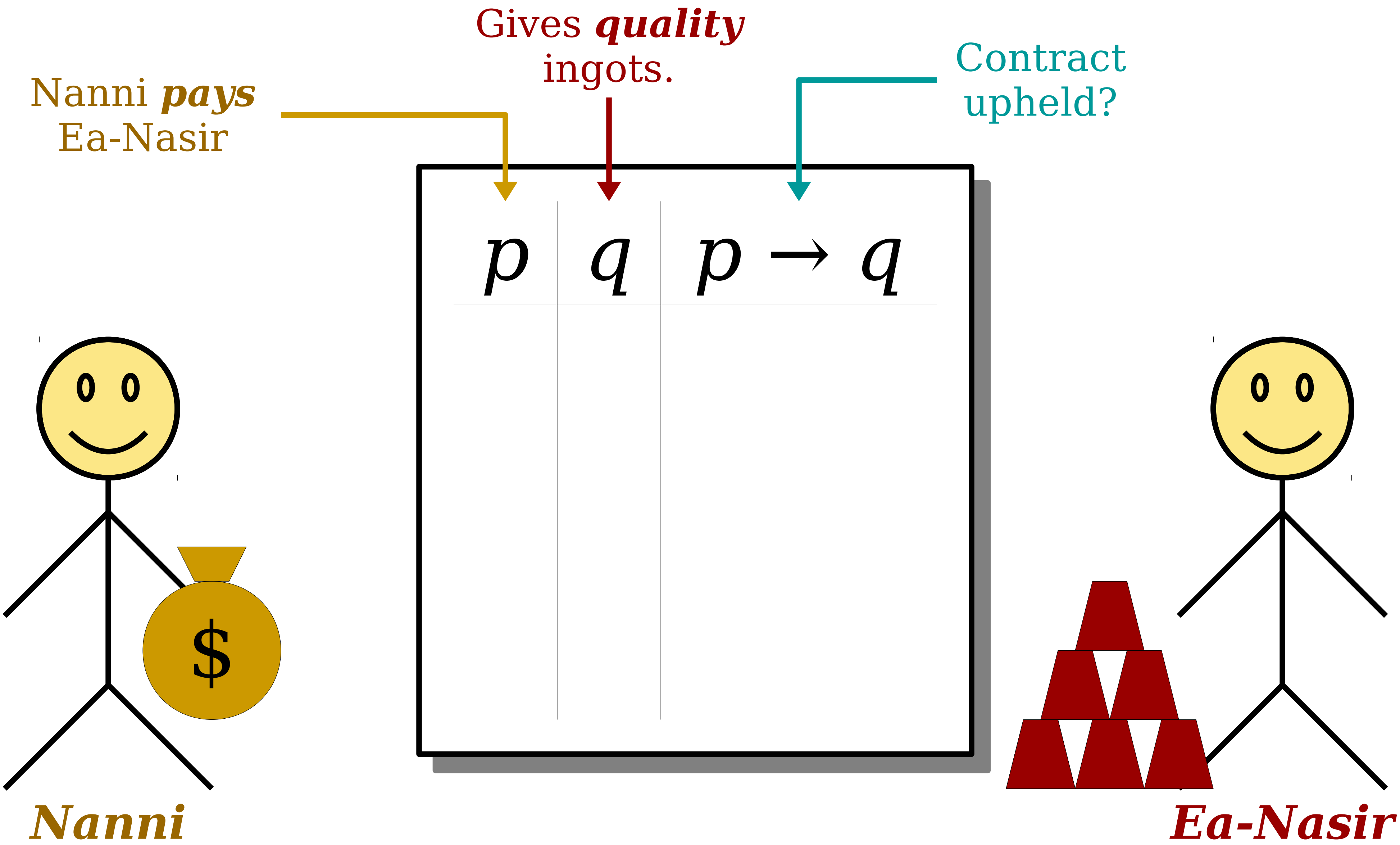
- We can represent implications using this connective:

$$p \to q$$

- You'd read this out loud as "p implies q."
  - The fancy name for this is the ***material conditional***.

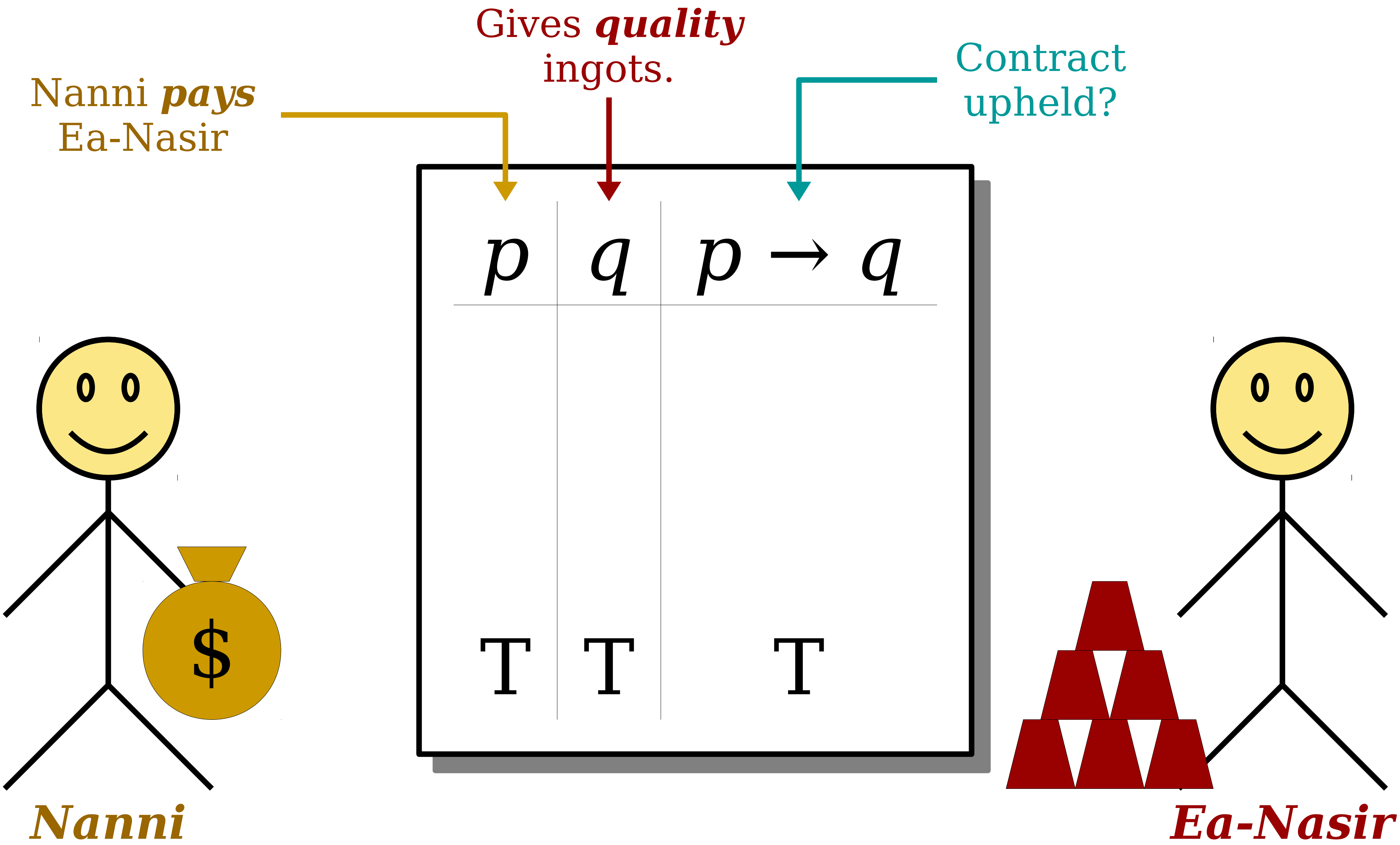
Question: What should the truth table for $p \to q$ look like? Enter your guess as a list of four values to fill in the rightmost column of the table.

Respond at pollev.com/cs103



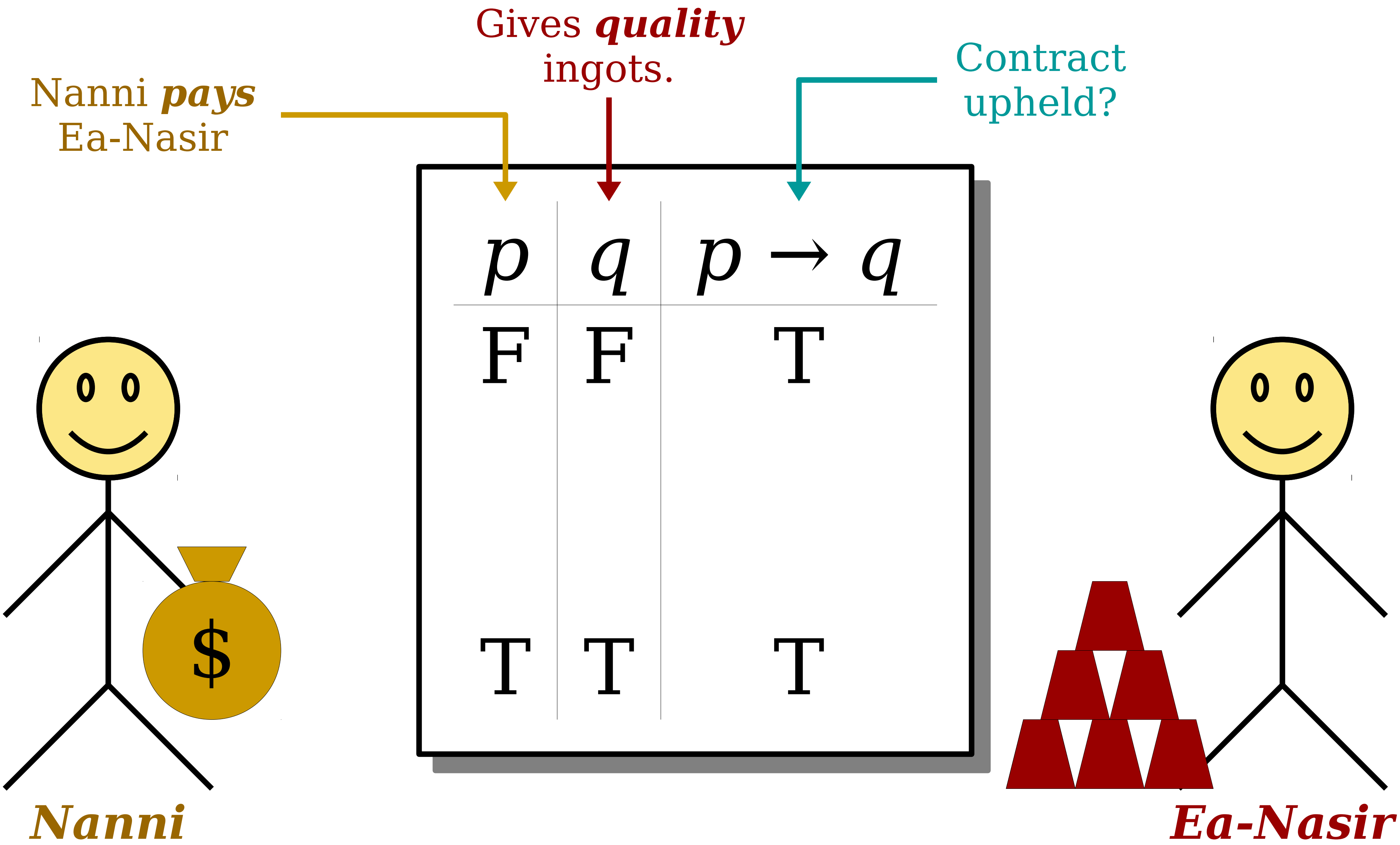
Ancient Contract:

If Nanni pays money to Ea-Nasir, then
Ea-Nasir will give Nanni quality copper ingots.



Ancient Contract:

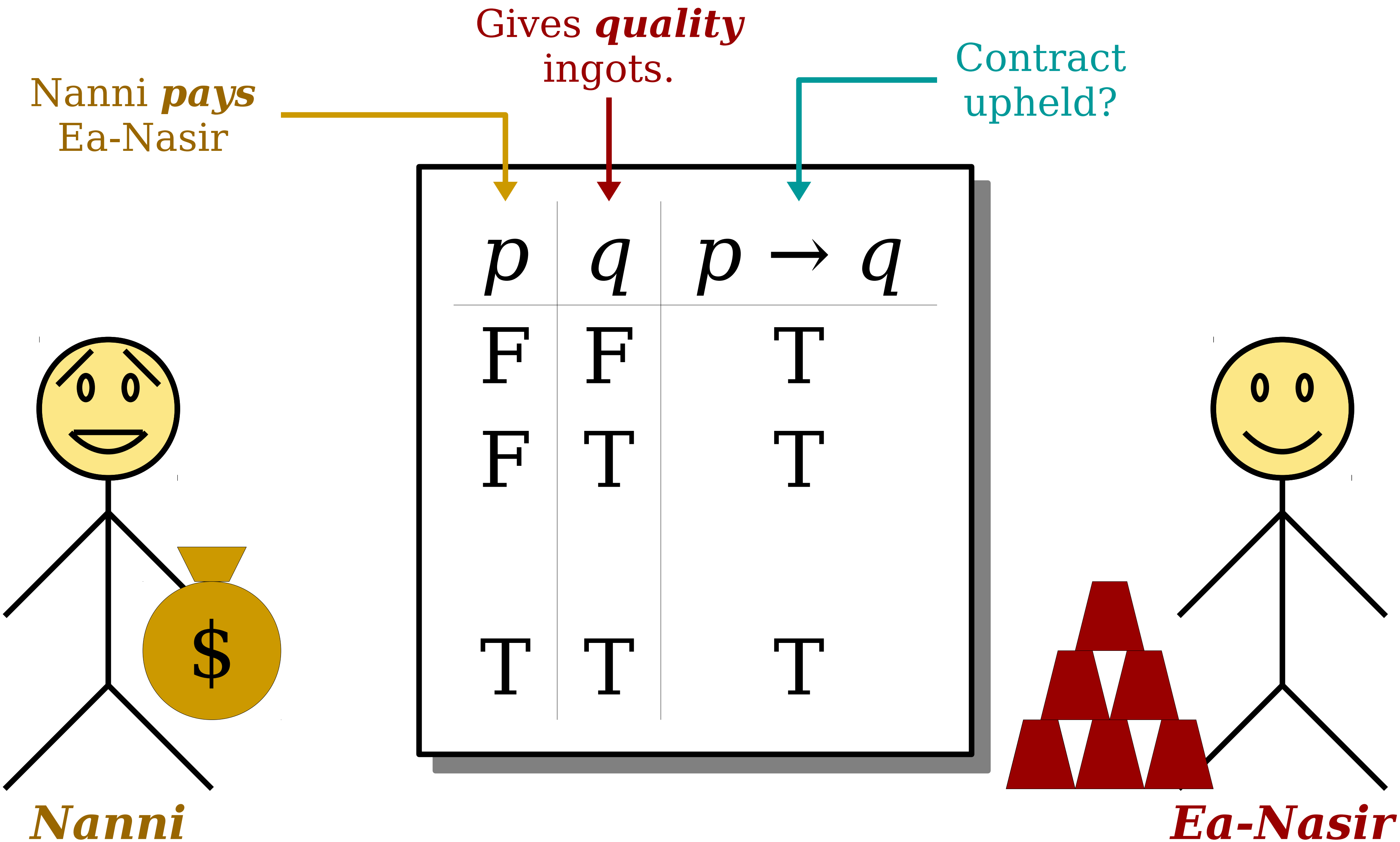
If Nanni pays money to Ea-Nasir, then
Ea-Nasir will give Nanni quality copper ingots.



p	q	$p \to q$
F	F	T
T	T	T

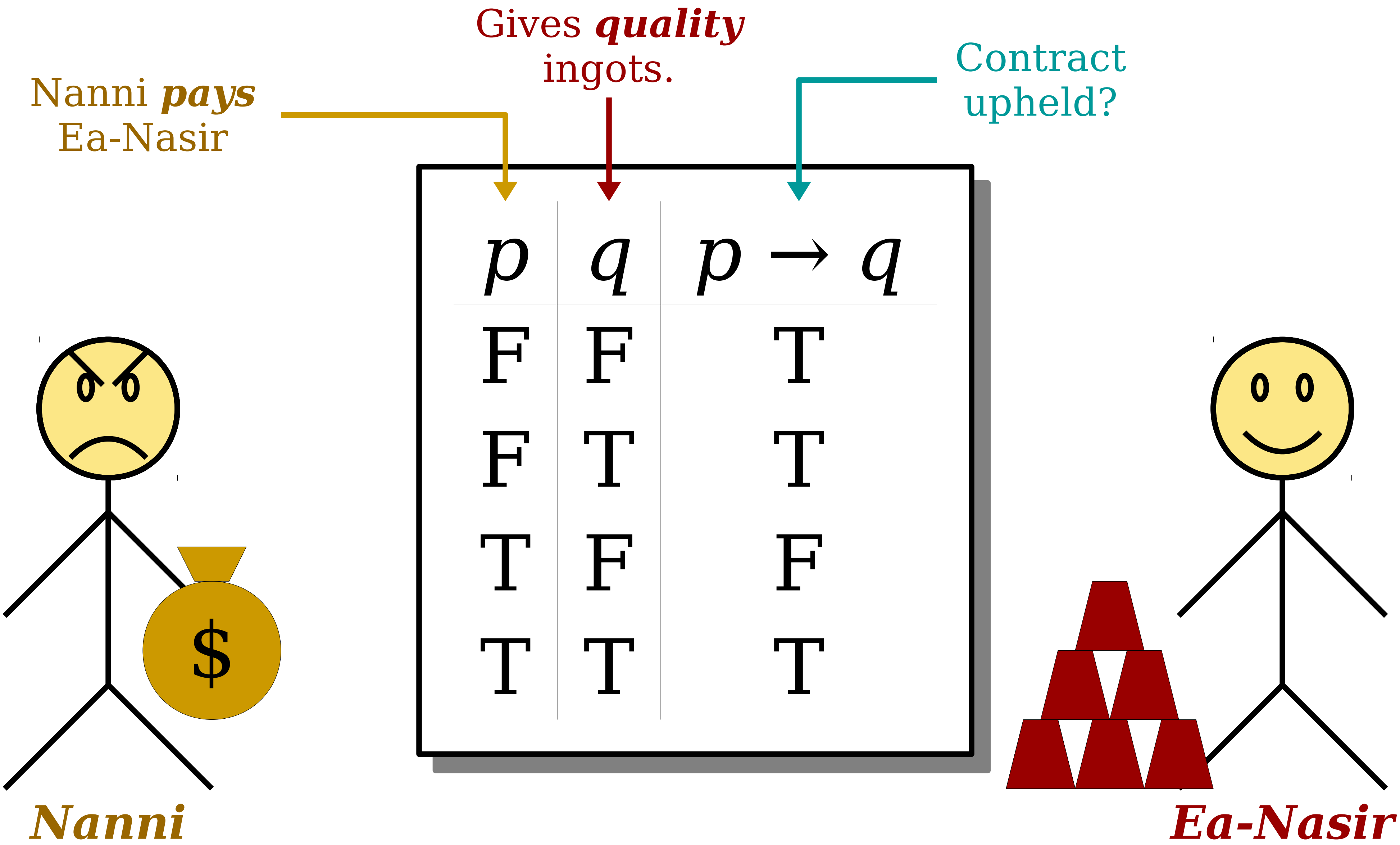
Ancient Contract:

If Nanni pays money to Ea-Nasir, then
Ea-Nasir will give Nanni quality copper ingots.



Ancient Contract:

If Nanni pays money to Ea-Nasir, then
Ea-Nasir will give Nanni quality copper ingots.

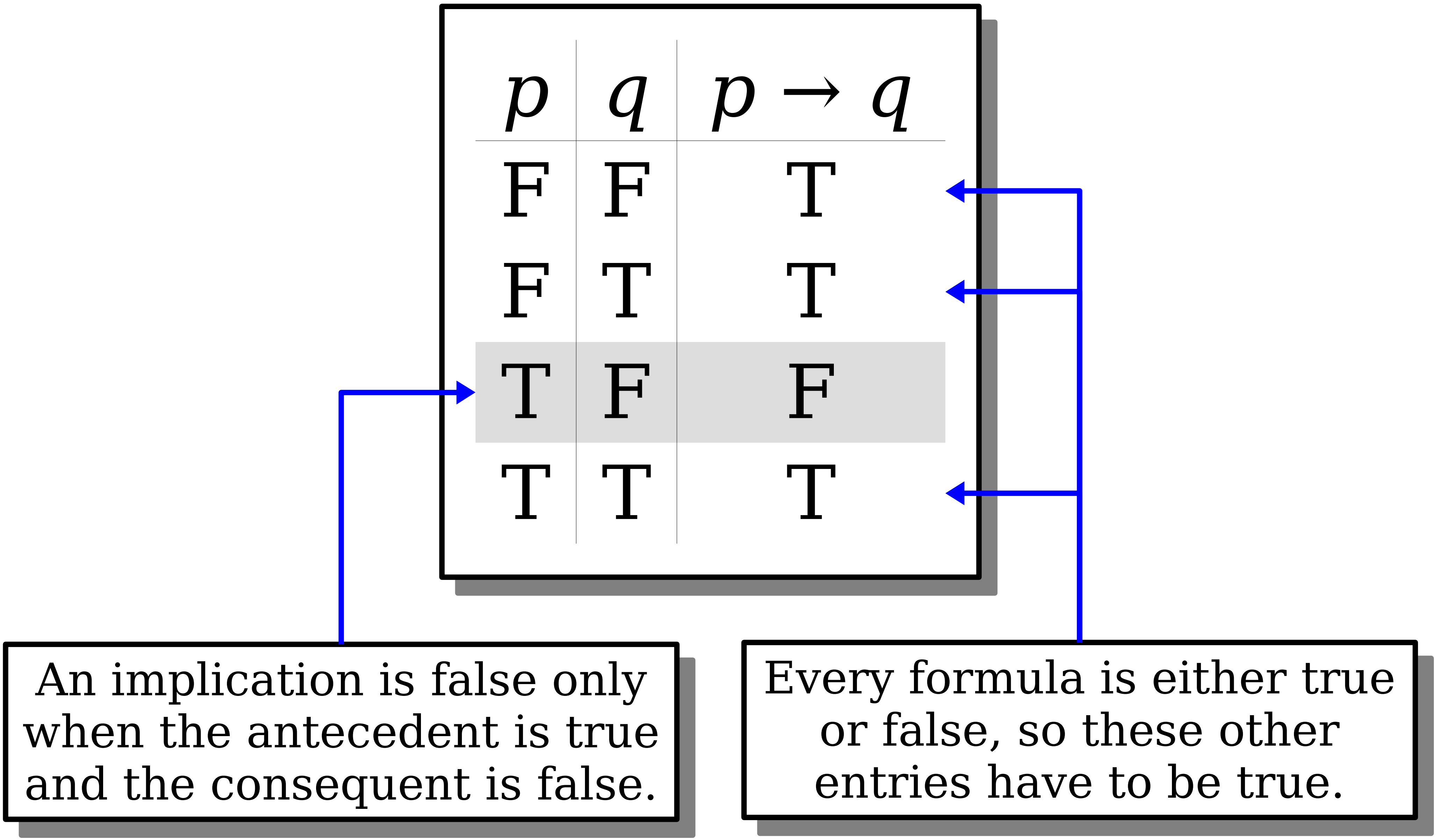


p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Ancient Contract:

If Nanni pays money to Ea-Nasir, then Ea-Nasir will give Nanni quality copper ingots.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T


p q p → q
F F T
F T T
T F F
T T T
An implication is false only when the antecedent is true and the consequent is false.
Every formula is either true or false, so these other entries have to be true.

p	q	$p \rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

Important observation:

The statement $p \rightarrow q$ is true whenever $p \wedge \neg q$ is false.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

An implication with a false antecedent is called ***vacuously true***.

An implication with a true consequent is called ***trivially true***.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Please commit this table to memory. We're going to need it, extensively, over the next couple of weeks.

Fun Fact: The Contrapositive Revisited

The Biconditional Connective

The Biconditional Connective

- On Friday, we saw that "p if and only if q" means both that $p \to q$ and $q \to p$.
- We can write this in propositional logic using the ***biconditional*** connective:

$$p \leftrightarrow q$$

- This connective's truth table has the same meaning as "p implies q and q implies p."

Question: What should the truth table for $p \leftrightarrow q$ look like? Enter your guess as a list of four values to fill in the rightmost column of the table.

Respond at pollev.com/cs103

Biconditionals

- The ***biconditional*** connective $p \leftrightarrow q$ is read "p if and only if q."
- Here's its truth table:

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

Biconditionals

- The ***biconditional*** connective $p \leftrightarrow q$ is read "p if and only if q."
- Here's its truth table:

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

One interpretation of $\leftrightarrow$ is to think of it as equality: the two propositions must have equal truth values.

True and False

- There are two more “connectives” to speak of: true and false.
  - The symbol ⊤ is a value that is always true.
  - The symbol ⊥ is value that is always false.
- These are often called connectives, though they don't connect anything.
  - (Or rather, they connect zero things.)

Proof by Contradiction

- Suppose you want to prove *p* is true using a proof by contradiction.
- The setup looks like this:
  - Assume *p* is false.
  - Derive something that we know is false.
  - Conclude that *p* is true.
- In propositional logic:

$$(\neg p \to \bot) \to p$$

Operator Precedence

- How do we parse this statement?

$$\neg x \to y \lor z \to x \lor y \land z$$

- Operator precedence for propositional logic:

$$\neg$$

$$\land$$

$$\lor$$

$$\to$$

$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$\neg x \rightarrow y \vee z \rightarrow x \vee y \wedge z$$

- Operator precedence for propositional logic:

$$\neg$$
$$\wedge$$
$$\vee$$
$$\rightarrow$$
$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \to y \lor z \to x \lor y \land z$$

- Operator precedence for propositional logic:

$$\neg$$

$$\land$$

$$\lor$$

$$\to$$

$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \to y \vee z \to x \vee y \wedge z$$

- Operator precedence for propositional logic:

$$\neg$$

$$\mathbf{\wedge}$$

$$\vee$$

$$\to$$

$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \to y \lor z \to x \lor (y \land z)$$

- Operator precedence for propositional logic:

$$\neg$$
$$\land$$
$$\lor$$
$$\to$$
$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \rightarrow y \vee z \rightarrow x \vee (y \wedge z)$$

- Operator precedence for propositional logic:

$$\neg$$
$$\wedge$$
$$\vee$$
$$\rightarrow$$
$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \rightarrow (y \vee z) \rightarrow (x \vee (y \wedge z))$$

- Operator precedence for propositional logic:

$$\neg$$

$$\wedge$$

$$\vee$$

$$\rightarrow$$

$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \to (y \lor z) \to (x \lor (y \land z))$$

- Operator precedence for propositional logic:

$$\neg$$
$$\land$$
$$\lor$$
$$\to$$
$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \to ((y \lor z) \to (x \lor (y \land z)))$$

- Operator precedence for propositional logic:

$$\neg$$
$$\land$$
$$\lor$$
$$\to$$
$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- How do we parse this statement?

$$(\neg x) \rightarrow ((y \vee z) \rightarrow (x \vee (y \wedge z)))$$

- Operator precedence for propositional logic:

$$\neg$$

$$\wedge$$

$$\vee$$

$$\rightarrow$$

$$\leftrightarrow$$

- All operators are right-associative.
- We can use parentheses to disambiguate.

Operator Precedence

- The main points to remember:
  - $\neg$ binds to whatever immediately follows it.
  - $\wedge$ and $\vee$ bind more tightly than $\rightarrow$.
- We will commonly write expressions like $p \wedge q \rightarrow r$ without adding parentheses.
- For more complex expressions, we'll try to add parentheses.
- Confused? ***Please ask!***

The Big Table

Connective	Read Aloud As	C++ Version	Fancy Name
$\neg$	"not"	`!`	Negation
$\wedge$	"and"	`&&`	Conjunction
$\vee$	"or"	`||`	Disjunction
$\to$	"implies"	*see PS2!*	Implication
$\leftrightarrow$	"if and only if"	*see PS2!*	Biconditional
$\top$	"true"	`true`	Truth
$\bot$	"false"	`false`	Falsity

Time-Out for Announcements!

Office Hours

- Office hours start today. Think of them as “drop-in help hours” where you can ask questions on problem sets, lecture topics, etc.
  - Check the Guide to Office Hours on the course website for the schedule.
- Most office hours are held in person in the Huang basement. A few are purely online.
- Once you arrive, sign up on QueueStatus so that we can help people in the order they arrived:

  https://queuestatus.com/queues/2367
- Office hours are much less crowded earlier in the week than later.

Back to CS103!

Recap So Far

- A ***propositional variable*** is a variable that is either true or false.
- The ***propositional connectives*** are
  - Negation: $\neg p$
  - Conjunction: $p \land q$
  - Disjunction: $p \lor q$
  - Implication: $p \to q$
  - Biconditional: $p \leftrightarrow q$
  - True: $\top$
  - False: $\bot$

Translating into Propositional Logic

Some Sample Propositions

a: I will be in the path of totality.

b: I will see a total solar eclipse.

Some Sample Propositions

a: I will be in the path of totality.

b: I will see a total solar eclipse.

"I won't see a total solar eclipse if I'm not in the path of totality."

Question: How would you express this statement in propositional logic?

Respond at pollev.com/cs103

“***p* if *q***”

translates to

$$q \rightarrow p$$

It does *not* translate to

⚠ $p \rightarrow q$ ⚠

Some Sample Propositions

a: I will be in the path of totality.

b: I will see a total solar eclipse.

c: There is a total solar eclipse today.

Some Sample Propositions

a: I will be in the path of totality.

b: I will see a total solar eclipse.

c: There is a total solar eclipse today.

"If I will be in the path of totality, but there's no solar eclipse today, I won't see a total solar eclipse."

Question: How would you express this statement in propositional logic?

Respond at pollev.com/cs103

“***p*, but *q***”

translates to

$\boldsymbol{p \wedge q}$

The Takeaway Point

- When translating into or out of propositional logic, be very careful not to get tripped up by nuances of the English language.
  - In fact, this is one of the reasons we have a symbolic notation in the first place!
- Many prepositional phrases lead to counterintuitive translations; make sure to double-check yourself!

Propositional Equivalences

Quick Question:

What would I have to show you to convince you that the statement $p \land q$ is false?

Quick Question:

What would I have to show you to convince you that the statement $p \lor q$ is false?

de Morgan's Laws

- Using truth tables, we concluded that

$$\neg(p \land q)$$

  is equivalent to

$$\neg p \lor \neg q$$

- We also saw that

$$\neg(p \lor q)$$

  is equivalent to

$$\neg p \land \neg q$$

- These two equivalences are called ***De Morgan's Laws***.

de Morgan's Laws in Code

- ***Pro tip:*** Don't write this:

```
if (!(p() && q())) {
    /* … */
}
```

- Write this instead:

```
if (!p() || !q()) {
    /* … */
}
```

- (This even short-circuits correctly!)

An Important Equivalence

- Earlier, we talked about the truth table for $p \to q$. We chose it so that

$$p \to q \quad \textit{is equivalent to} \quad \neg(p \land \neg q)$$

- Later on, this equivalence will be incredibly useful:

$$\neg(p \to q) \quad \textit{is equivalent to} \quad p \land \neg q$$

Another Important Equivalence

- Here's a useful equivalence. Start with

$$p \to q \quad \textit{is equivalent to} \quad \neg(p \land \neg q)$$

- By de Morgan's laws:

$$\begin{aligned} p \to q \quad & \textit{is equivalent to} \quad \neg(p \land \neg q) \\ & \textit{is equivalent to} \quad \neg p \lor \neg\neg q \\ & \textit{is equivalent to} \quad \neg p \lor q \end{aligned}$$

- Thus $p \to q$ is equivalent to $\neg p \lor q$

Another Important Equivalence

- Here's a useful equivalence. Start with

$$p \to q \quad \textit{is equivalent to} \quad \neg(p \land \neg q)$$

- By de Morgan's laws:

$p \to q$ *is equivalent*

is equivalent

is equivalent

If p is false, then $\neg p \lor q$ is true. If p is true, then q has to be true for the whole expression to be true.

- Thus $p \to q$ is equivalent to $\neg p \lor q$

Proofwriting Workshop

An Incorrect Set Theory Proof

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

⚠ ***Incorrect!*** ⚠ ***Proof:*** Consider arbitrary sets A, B, and C where $C \subseteq A \cup B$.

This means that every element of C is in either A or B. If all elements of C are in A, then $C \subseteq A$. Alternately, if everything in C is in B, then $C \subseteq B$. In either case, everything inside of C has to be contained in at least one of these sets, so the theorem is true. ■

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

⚠ ***Incorrect!*** ⚠ ***Proof:*** Consider arbitrary sets A, B, and C where $C \subseteq A \cup B$.

This means that every element of C is in either A or B. If all elements of C are in A, then $C \subseteq A$. Alternately, if everything in C is in B, then $C \subseteq B$. In either case, everything inside of C has to be contained in at least one of these sets, so the theorem is true. ■

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

⚠ ***Incorrect!*** ⚠ ***Proof:*** Consider arbitrary sets A, B, and C where $C \subseteq A \cup B$.

This means that every element of C is in either A or B. If all elements of C are in A, then $C \subseteq A$. Alternately, if everything in C is in B, then $C \subseteq B$. In either case, everything inside of C has to be contained in at least one of these sets, so the theorem is true. ■

This is just repeating definitions and not making specific claims about specific variables.

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

⚠ ***Incorrect!*** ⚠ ***Proof:*** Consider arbitrary sets A, B, and C where $C \subseteq A \cup B$.

This means that every element of C is in either A or B. If all elements of C are in A, then $C \subseteq A$. Alternately, if everything in C is in B, then $C \subseteq B$. In either case, everything inside of C has to be contained in at least one of these sets, so the theorem is true. ■

Why is this bad?

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

⚠ ***Incorrect!*** ⚠ ***Proof:*** Consider arbitrary sets A, B, and C where $C \subseteq A \cup B$.

This means that every element of C is in either A or B. If all elements of C are in A, then $C \subseteq A$. Alternately, if everything in C is in B, then $C \subseteq B$. In either case, everything inside of C has to be contained in at least one of these sets, so the theorem is true. ■

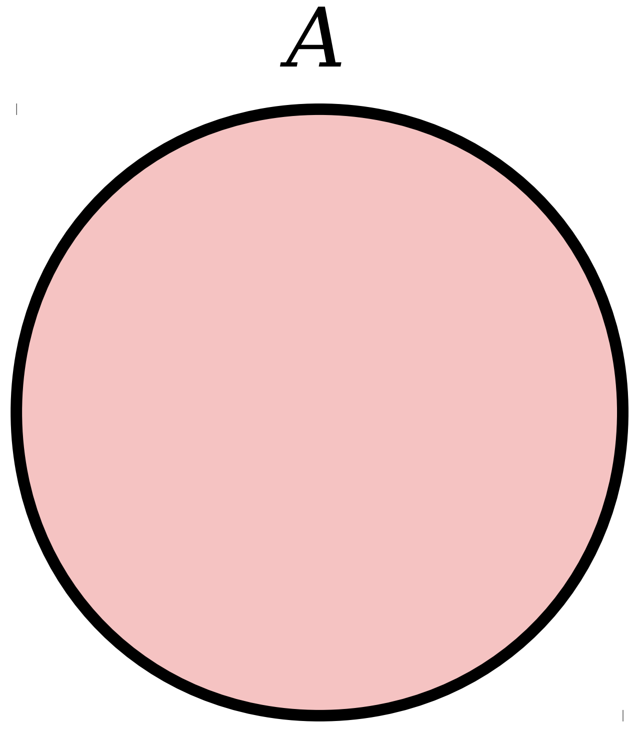
While this claim is true, it does not imply the theorem is true. In fact, this theorem is actually false.

Let’s Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

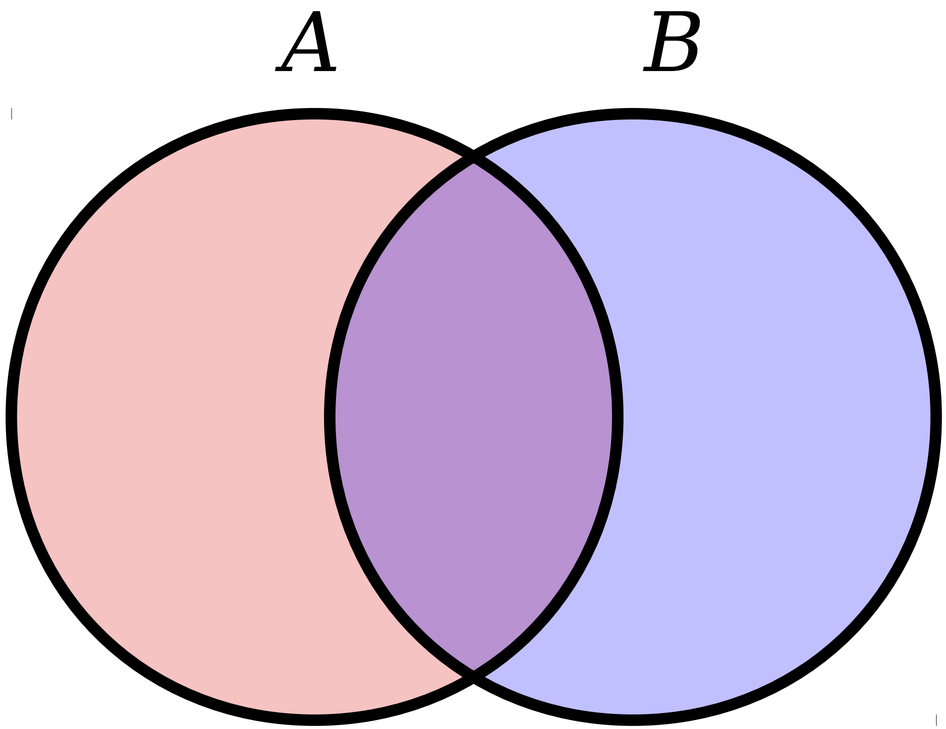
Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.



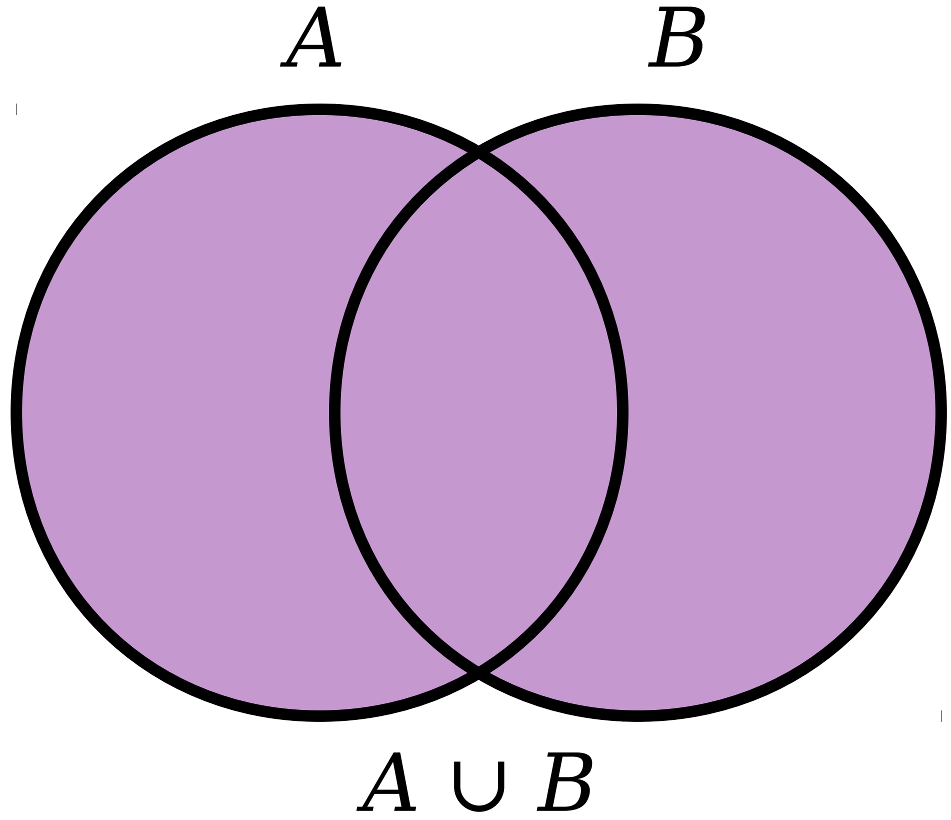
Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.



Let's Draw Some Pictures!

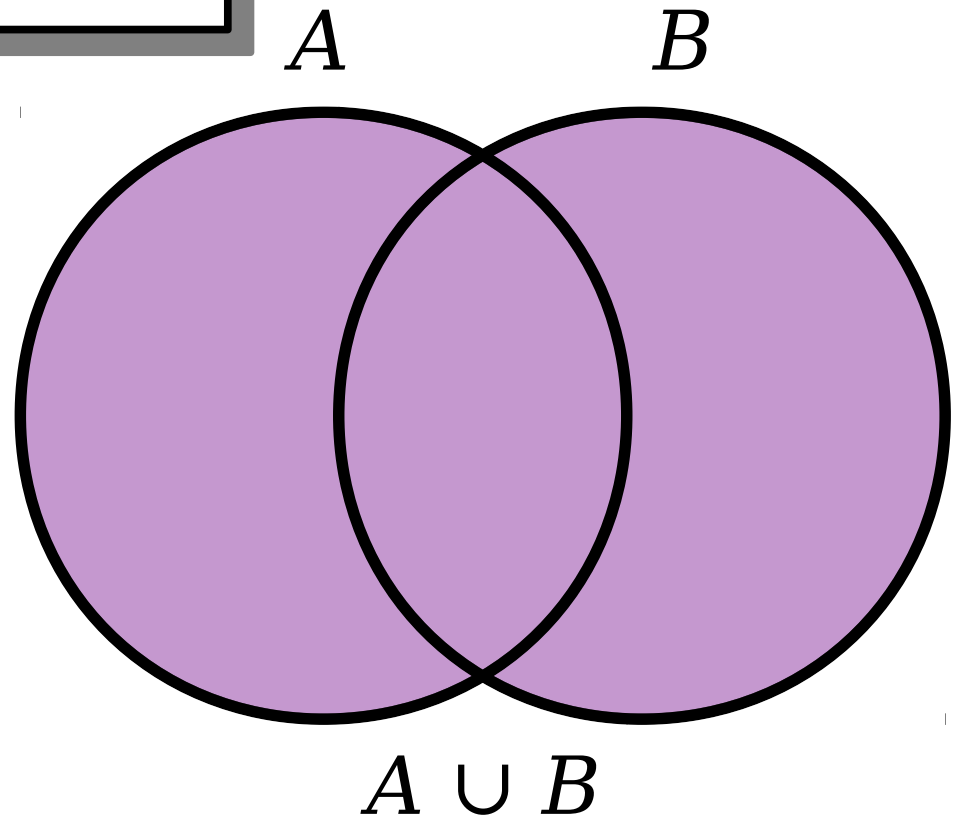
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.



Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Recall the intuition of a subset being "something I can circle"

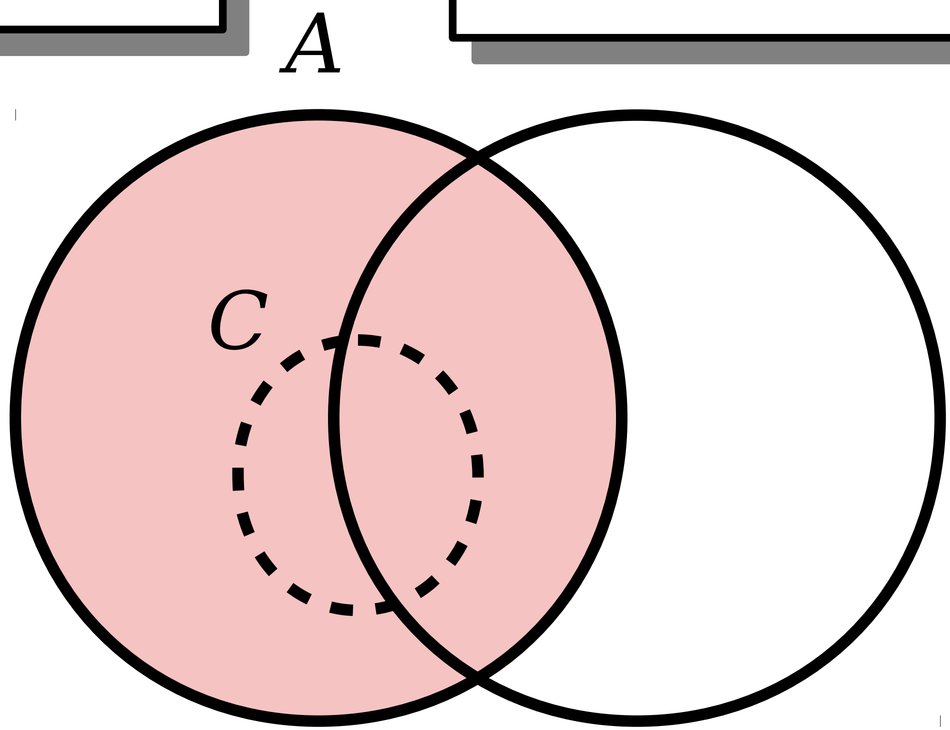


Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Recall the intuition of a subset being "something I can circle"

So $C \subseteq A$ would mean that C is something I can circle in this region.

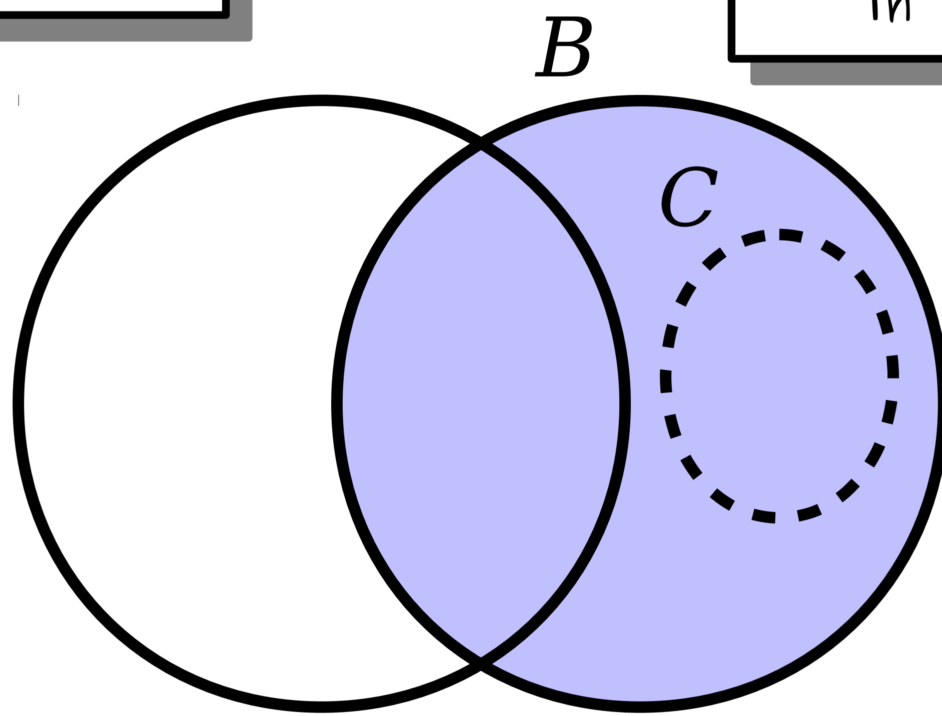


Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

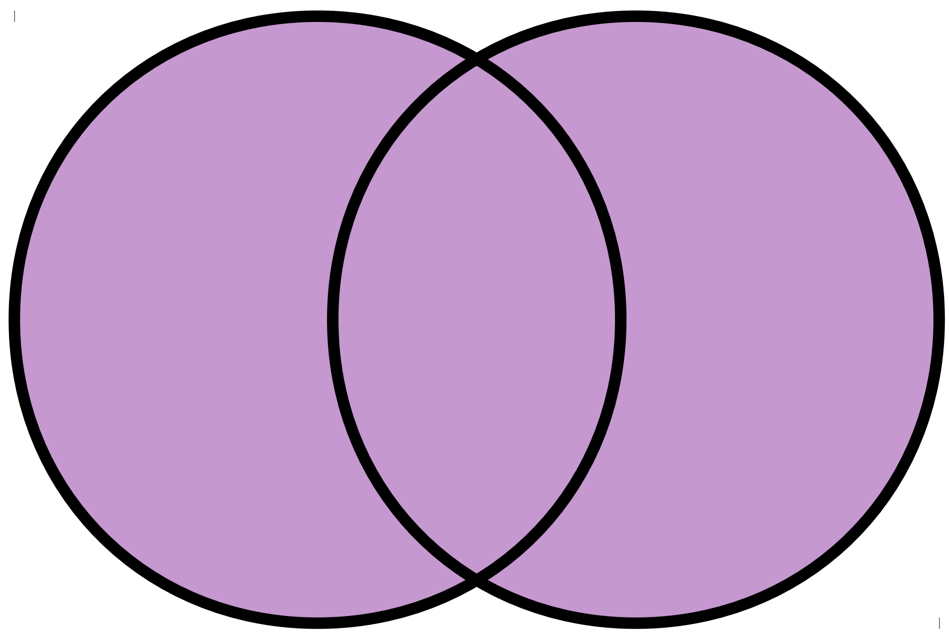
Recall the intuition of a subset being "something I can circle"

Likewise, $C \subseteq B$ would mean that C is something I can circle in this region.



Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

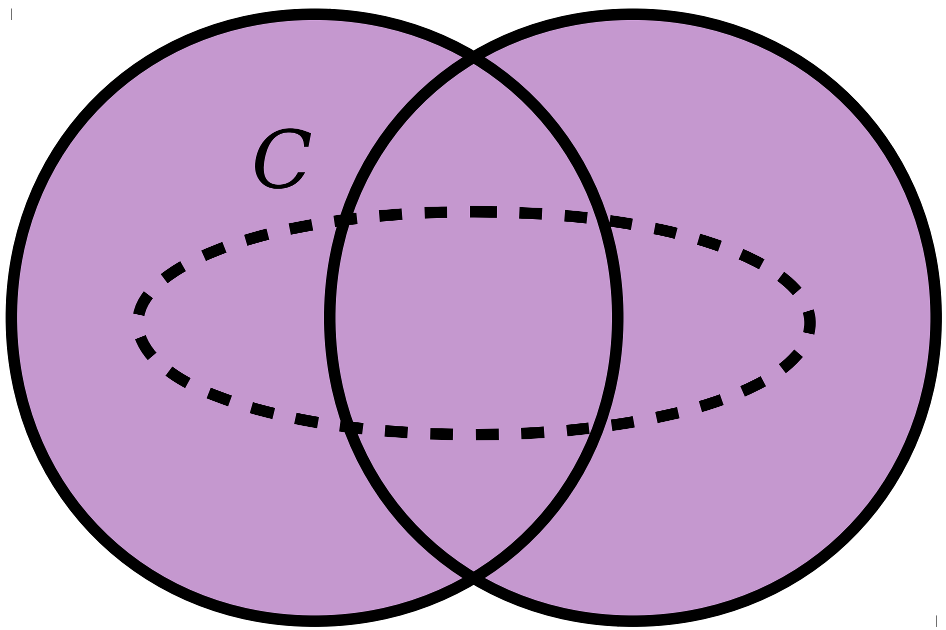


$A \cup B$

Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

But when I look at A∪B, I can draw C as a circle containing elements from both A and B!



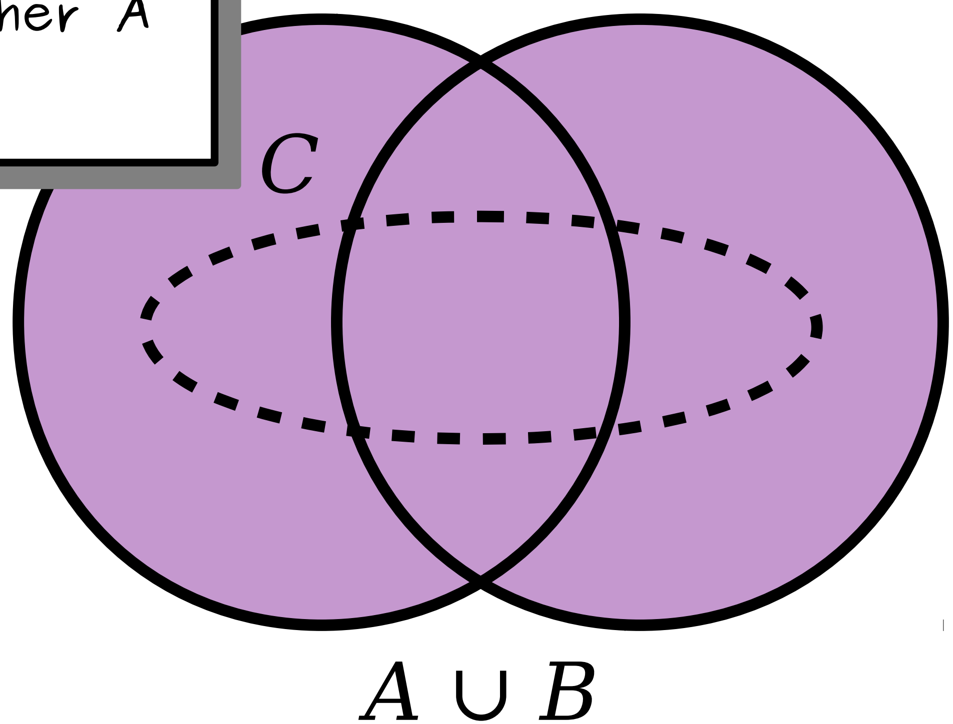
$A \cup B$

Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

But when I look at $A \cup B$, I can draw C as a circle containing elements from both A and B!

Do you see why this circle is in neither A nor B?

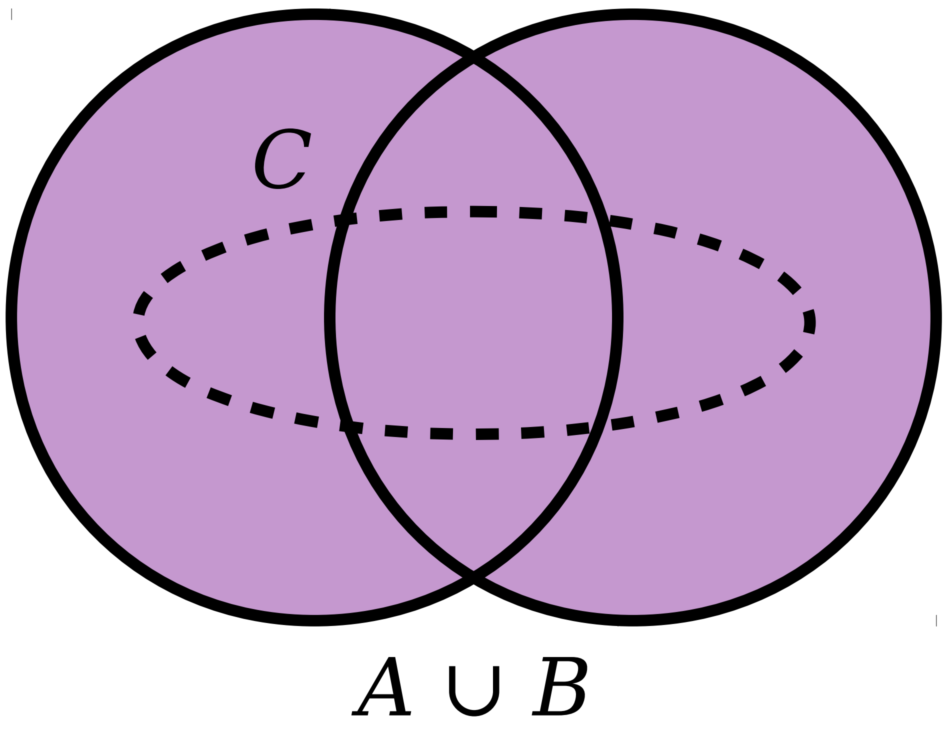


Let's Draw Some Pictures!

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Using this visual intuition, come up with a choice of sets A, B, and C that show this claim is false.

Respond at pollev.com/cs103



Proofs vs. Disproofs

- A ***proof*** is an argument that explains why some ***theorem*** is true.
- A ***disproof*** is an argument that explains why some ***claim*** is false.
- You've seen lots of examples of proofs. What does a disproof look like?

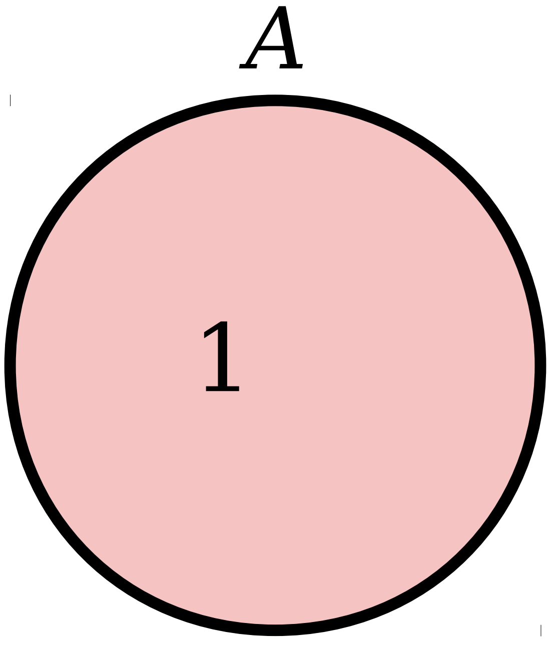
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \nsubseteq A$ and $C \nsubseteq B$.

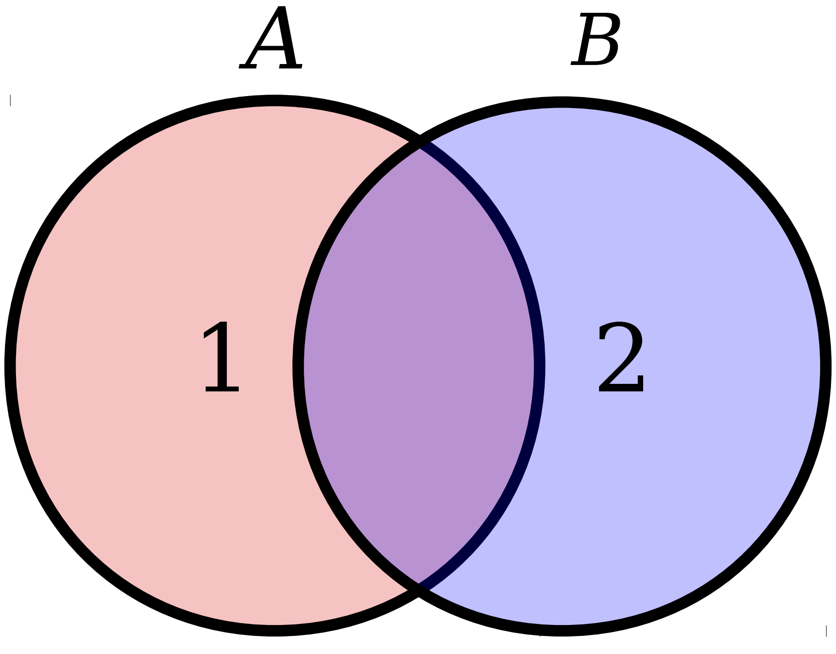
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \nsubseteq A$ and $C \nsubseteq B$. Consider the sets $A = \{1\}$



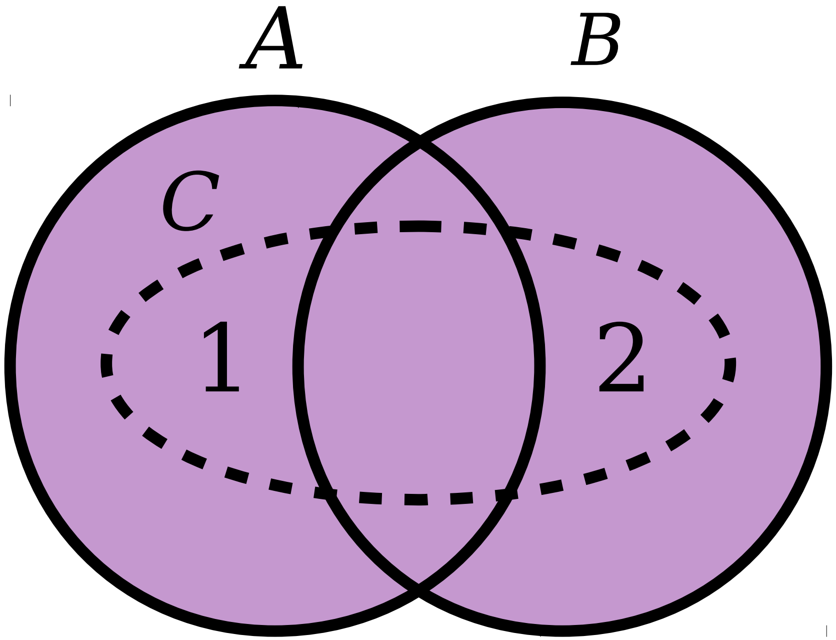
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \not\subseteq A$ and $C \not\subseteq B$. Consider the sets $A = \{1\}$, $B = \{2\}$



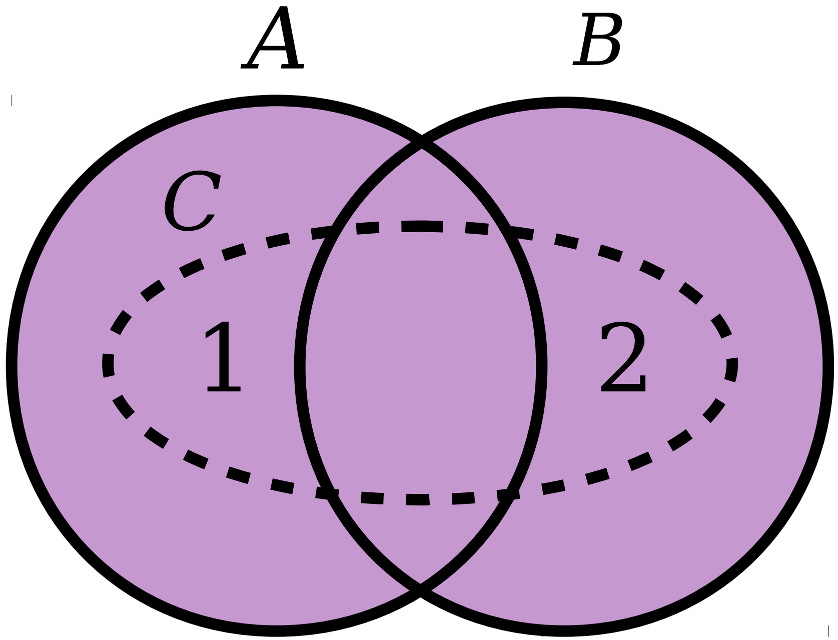
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \not\subseteq A$ and $C \not\subseteq B$. Consider the sets $A = \{1\}$, $B = \{2\}$, and $C = \{1, 2\}$.



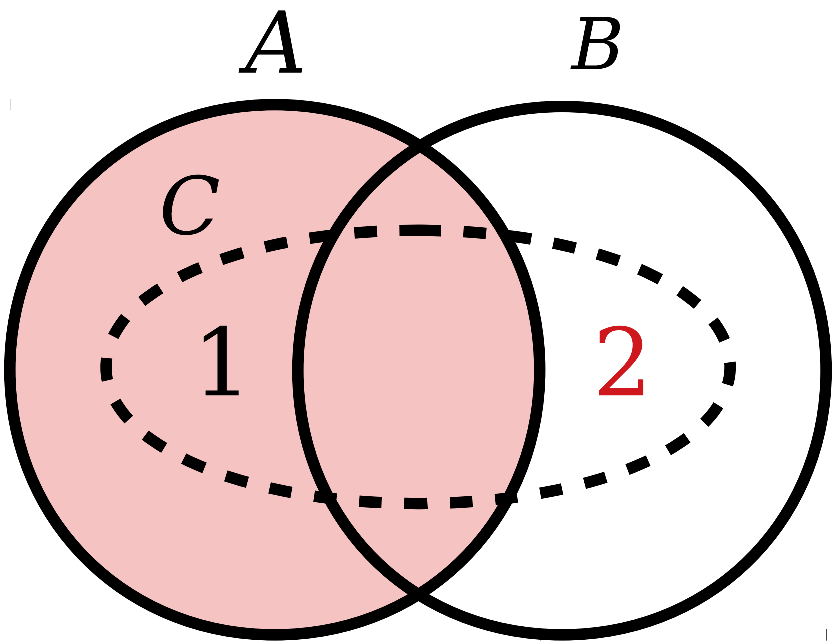
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \not\subseteq A$ and $C \not\subseteq B$. Consider the sets $A = \{1\}$, $B = \{2\}$, and $C = \{1, 2\}$. Now notice that $\{1, 2\} \subseteq A \cup B$ so $C \subseteq A \cup B$



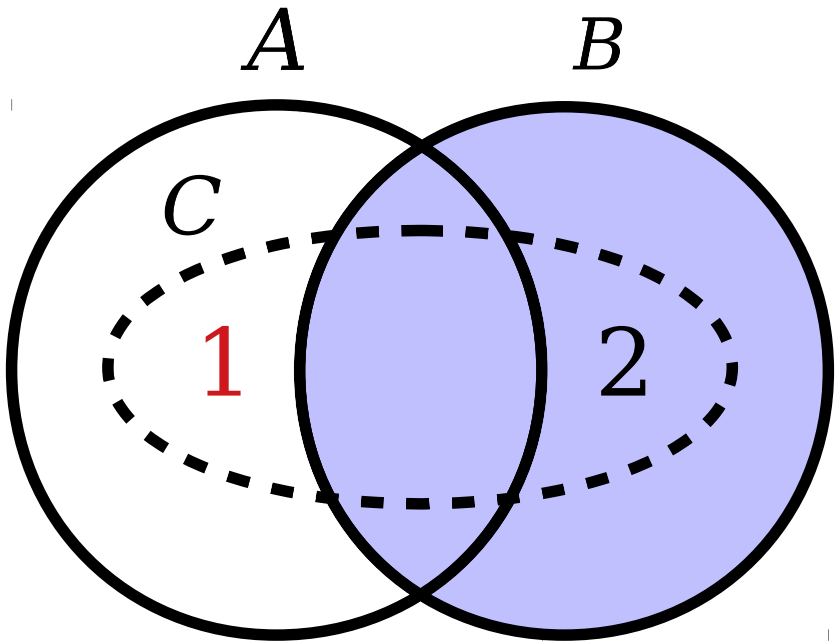
Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \not\subseteq A$ and $C \not\subseteq B$. Consider the sets $A = \{1\}$, $B = \{2\}$, and $C = \{1, 2\}$. Now notice that $\{1, 2\} \subseteq A \cup B$ so $C \subseteq A \cup B$, but $C \not\subseteq A$ because $2 \in C$ but $2 \notin A$



Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \not\subseteq A$ and $C \not\subseteq B$. Consider the sets $A = \{1\}$, $B = \{2\}$, and $C = \{1, 2\}$. Now notice that $\{1, 2\} \subseteq A \cup B$ so $C \subseteq A \cup B$, but $C \not\subseteq A$ because $2 \in C$ but $2 \notin A$, and $C \not\subseteq B$ because $1 \in C$ but $1 \notin B$.



Claim: If A, B, and C are sets and $C \subseteq A \cup B$, then $C \subseteq A$ or $C \subseteq B$.

Disproof: We will show that there are sets A, B, and C where $C \subseteq A \cup B$, but $C \nsubseteq A$ and $C \nsubseteq B$. Consider the sets $A = \{1\}$, $B = \{2\}$, and $C = \{1, 2\}$. Now notice that $\{1, 2\} \subseteq A \cup B$ so $C \subseteq A \cup B$, but $C \nsubseteq A$ because $2 \in C$ but $2 \notin A$, and $C \nsubseteq B$ because $1 \in C$ but $1 \notin B$.

Thus we've found a set C which is a subset of $A \cup B$ but is not a subset of either A or B, which is what we needed to show. ■

Proofwriting Advice

- Be ***very wary*** of proofs that speak generally about "all objects" of a particular type.
  - As you've just seen, it's easy to accidentally prove a false statement at this level of detail.
  - Making broad, high-level claims often indicates deeper logic errors or conceptual misunderstanding (like *code smell* but for proofs!)

Proofwriting Advice

A Very Good Idea: After you've written a draft of a proof, run through all of the points on the Proofwriting Checklist.

- This is a *great* exercise that you can do with a partner!

Proofs on Subsets

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Hold on, isn't this the claim we just disproved?

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

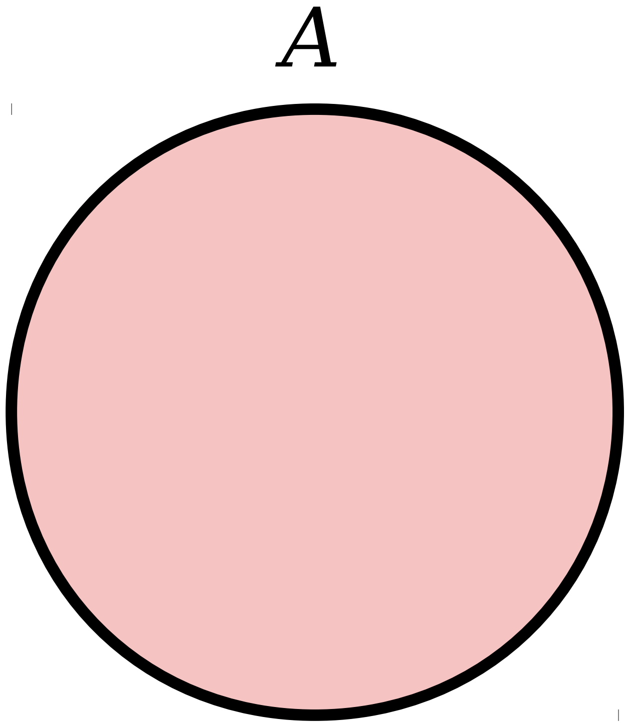
Notice that that's an intersection, not a union! It turns out that this claim is actually true.

Let's Draw Some Pictures!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

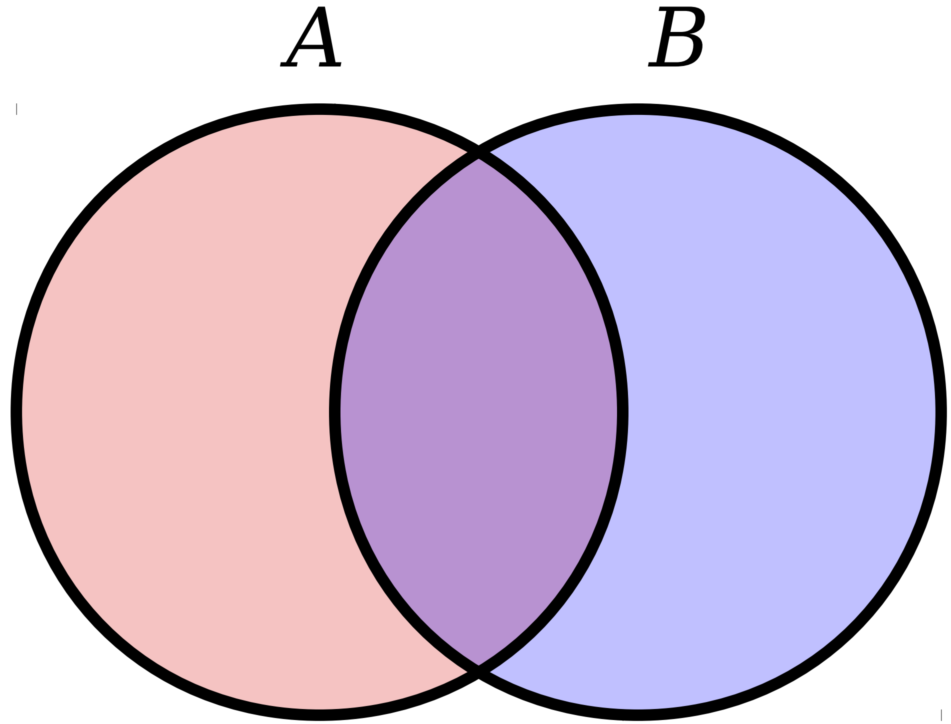
Let's Draw Some Pictures!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.



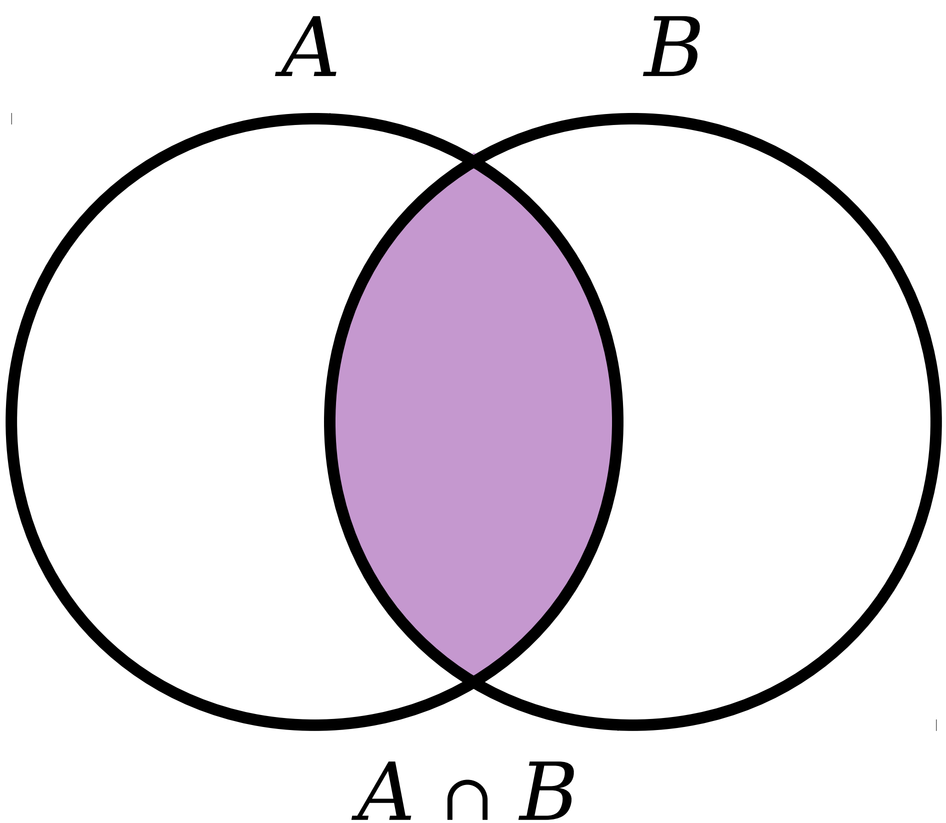
Let's Draw Some Pictures!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.



Let's Draw Some Pictures!

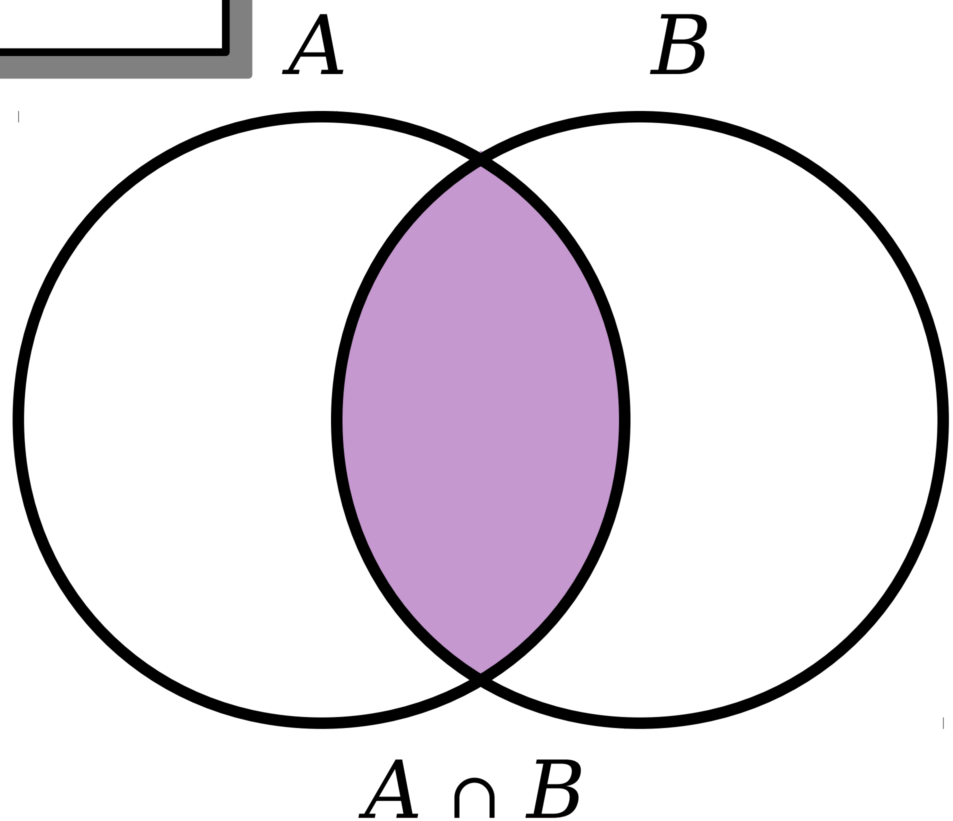
Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.



Let's Draw Some Pictures!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Recall the intuition of a subset being "something I can circle"

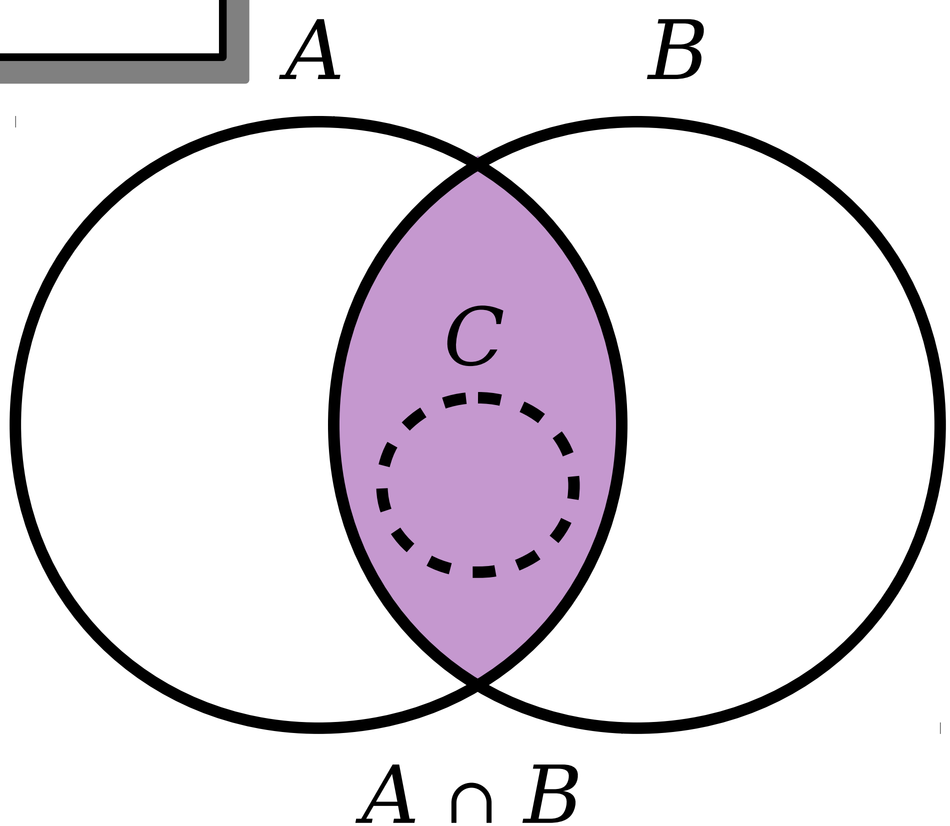


Let's Draw Some Pictures!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Recall the intuition of a subset being "something I can circle"

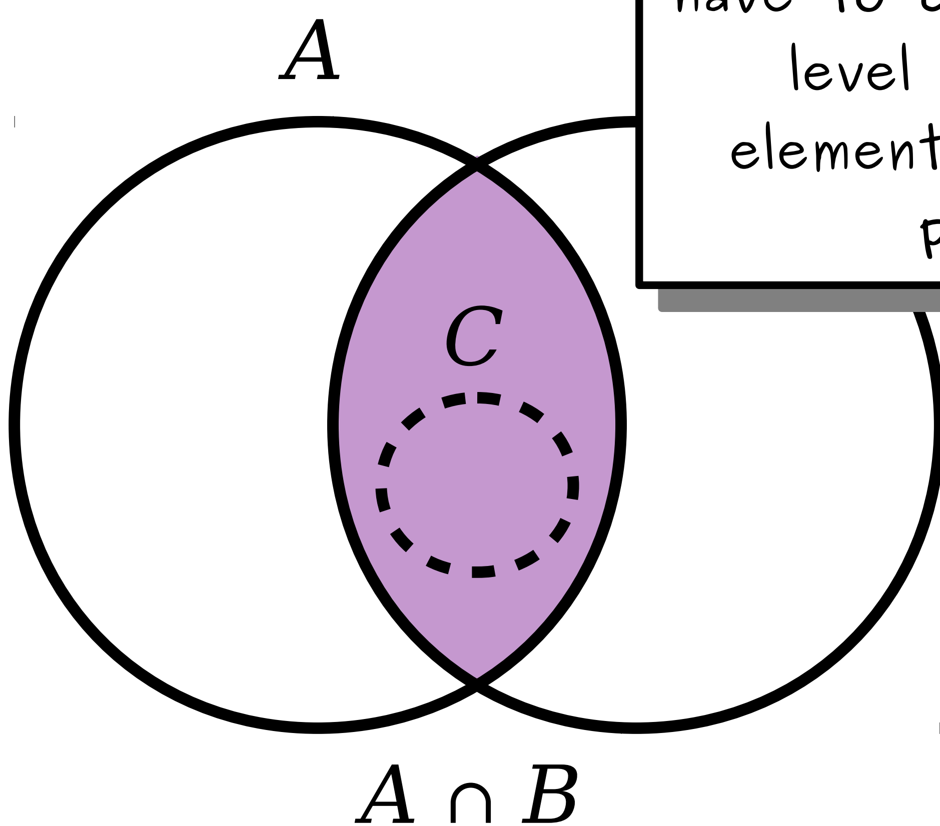
When I look at $A \cap B$, any circle I can draw in this region can be found in both A and B.



Let's Draw Some Pictures!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

This is a great visual intuition to see why the theorem is true. Now we have to drill down to the level of individual elements to write the proof.



Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming	*What We Need To Show*

When confronted with a theorem to prove, the first step is to make sure you understand where you're starting and where you're going.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming	*What We Need To Show*
• A, B, and C are sets • $C \subseteq A \cap B$	• $C \subseteq A$ and $C \subseteq B$

A great proofwriting strategy is to ***write down relevant definitions***. This gives you a better sense of what you need to prove and what tools you have at hand.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming	*What We Need To Show*
• A, B, and C are sets • $C \subseteq A \cap B$	• $C \subseteq A$ and $C \subseteq B$

Before we start:

- What is the definition of subset?
- How do you prove that one set is a subset of another?
- If you know that one set is a subset of another, what can you conclude?

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Definition: If S and T are sets, then $S \subseteq T$ when for every $x \in S$, we have $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Definition: If S and T are sets, then $S \subseteq T$ when for every $x \in S$, we have $x \in T$.

To prove that $S \subseteq T$:

Pick an arbitrary $x \in S$, then prove $x \in T$.

If you know that $S \subseteq T$:

If you have an $x \in S$, you can conclude $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Definition: If S and T are sets, then $S \subseteq T$ when for every $x \in S$, we have $x \in T$.

To prove that $S \subseteq T$:
Pick an arbitrary $x \in S$, then prove $x \in T$.

If you know that $S \subseteq T$:
If you have an $x \in S$, you can conclude $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

This reading of the definition is usually helpful for unpacking this column!

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Definition: If S and T are sets, then $S \subseteq T$ when for every $x \in S$, we have $x \in T$.

To prove that $S \subseteq T$:
Pick an arbitrary $x \in S$, then prove $x \in T$.

If you know that $S \subseteq T$:
If you have an $x \in S$, you can conclude $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$

How can we apply this general template to our specific problem?

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$
  - Pick an $x \in C$, show that $x \in A$
  - Pick an $x \in C$, show that $x \in B$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$
  - Pick an $x \in C$, show that $x \in A$
  - Pick an $x \in C$, show that $x \in B$

Now we know that ultimately, we're going to have to do these two things. Let's see what tools we have that can get us here!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$
  - Pick an $x \in C$, show that $x \in A$
  - Pick an $x \in C$, show that $x \in B$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

This reading of the definition is usually helpful for unpacking this column!

ow

that $x \in A$

how

Definition: If S and T are sets, then $S \subseteq T$ when for every $x \in S$, we have $x \in T$.

To prove that $S \subseteq T$:
Pick an arbitrary $x \in S$, then prove $x \in T$.

If you know that $S \subseteq T$:
If you have an $x \in S$, you can conclude $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$
  - Pick an $x \in C$, show that $x \in A$
  - Pick an $x \in C$, show that $x \in B$

Before we continue:

- What is the definition of set intersection?

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming	*What We Need To Show*
• A, B, and C are sets • $C \subseteq A \cap B$	• $C \subseteq A$ and $C \subseteq B$ • Pick an $x \in C$, show that $x \in A$

Definition: The set $S \cap T$ is the set where, for any x:

$$x \in S \cap T \quad \text{when} \quad x \in S \text{ and } x \in T$$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming	*What We Need To Show*
• A, B, and C are sets • $C \subseteq A \cap B$	• $C \subseteq A$ and $C \subseteq B$ • Pick an $x \in C$, show that $x \in A$

Definition: The set $S \cap T$ is the set where, for any x:

$$x \in S \cap T \quad \text{when} \quad x \in S \text{ and } x \in T$$

To prove that x ∈ S ∩ T:

Prove both that $x \in S$ and that $x \in T$.

If you know that x ∈ S ∩ T:

You can conclude both that $x \in S$ and that $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

This is the one we want!

- Pick an $x \in C$, show that $x \in A$

Definition: The set $S \cap T$ is the set where, for any x:

$$x \in S \cap T \quad \text{when} \quad x \in S \text{ and } x \in T$$

To prove that $x \in S \cap T$:

Prove both that $x \in S$ and that $x \in T$.

If you know that $x \in S \cap T$:

You can conclude both that $x \in S$ and that $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$.
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$
  - Pick an $x \in C$, show that $x \in A$
  - Pick an $x \in C$, show that $x \in B$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

What We're Assuming

- A, B, and C are sets
- $C \subseteq A \cap B$

Our Tools

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$.
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

What We Need To Show

- $C \subseteq A$ and $C \subseteq B$
  - Pick an $x \in C$, show that $x \in A$
  - Pick an $x \in C$, show that $x \in B$

Let's go and try and do the proof with what we've got here!

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - Conclude $x \in A$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$

  What goes here?

  - Conclude $x \in A$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - Conclude $x \in A$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - Conclude $x \in A$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - $x \in A$ and $x \in B$
  - Conclude $x \in A$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - $x \in A$ and $x \in B$
  - Conclude $x \in A$

Relevant Definitions

- In general to show that $S \subseteq T$, pick an arbitrary $x \in S$, show that $x \in T$
- If you know that $S \subseteq T$ and you have an $x \in S$, you can conclude $x \in T$.
- If you know that $x \in S \cap T$, we can conclude that $x \in S$ and $x \in \mathrm{T}$.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - $x \in A$ and $x \in B$
  - Conclude $x \in A$

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - $x \in A$ and $x \in B$
  - Conclude $x \in A$

We also need to prove that $C \subseteq B$.

Notice that if you take the outline here and literally swap the variable A for the variable B, you get a working proof.

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq B \cap A$
- Proving $C \subseteq B$
  - Pick an $x \in C$
  - $x \in B \cap A$
  - $x \in B$ and $x \in A$
  - Conclude $x \in B$

In a case like this where your proof would have two completely symmetric branches, it's fine to write up just one and say "***by symmetry***, [the other branch] is also true."

Theorem: If A, B, and C are sets and $C \subseteq A \cap B$, then $C \subseteq A$ and $C \subseteq B$.

Rough Outline

- Assume $C \subseteq A \cap B$
- Proving $C \subseteq A$
  - Pick an $x \in C$
  - $x \in A \cap B$
  - $x \in A$ and $x \in B$
  - Conclude $x \in A$

Try it yourself: Take a few minutes and write up a proof of the theorem using this outline.

Then share your proof with your neighbors and critique each other!

Respond at pollev.com/cs103

Next Time

- ***First-Order Logic***
  - Reasoning about groups of objects.
- ***First-Order Translations***
  - Expressing yourself in symbolic math!