7/2/14

Course webpage is up!
www.miami.edu/~armstrong/309sum14.html

HW 1 due Monday
Quiz 1 on Monday.
NO CLASS FRIDAY.

---

We ran out of time discussing a "proof" that

$$L_n = L_{n-1} + n.$$

We'll discuss it now. (I won't write it again 'cause it's already in the notes twice.)

Discussion:

1. I just wanted to show you what a modern mathematical proof looks like. I don't expect you to fully appreciate it today. (Hopefully when you look back in August it will make more sense.)

2. • There is something difficult about this. The proof does not manipulate numbers or symbols, but ideas.

• Most of the proof is not on the page, but in our heads

• The proof asks us to imagine (or assume, or grant the existence of) a fixed but indeterminate situation:

The $n$ fixed, but indeterminate lines $l_1, l_2, l_3, \ldots, l_n$ form exactly $L_n$ regions in the plane. Can you see them? There they are!

Mathematicians get so used to imagining fixed but indeterminate situations that we forget it's a learned skill.

3. Is it possible to put every detail of the proof on the page, leaving nothing to the imagination?

In theory, yes, but it will take a long time and it will become unreadle to human beings.

4. Okay, fine. Suppose you <u>still</u> want to formalize the proof. Then we need to discuss the language of

LOGIC.

---

<u>Warning</u>: The technical term "logic" does not mean the same as the English word "logic". Formal logic may or may not have any relationship to the way we think. In this class we will discuss only the particular flavor of logic used by modern computers.

Boolean Algebra (George Boole, 1854):

A set is a "collection of things". It has just one property, called "membership":

$$\boxed{\begin{array}{c} x \in S \\ \text{"thing } x \text{ is a member of the set } S\text{"} \end{array}}$$

For finite sets we use a notation like this

$$S = \{1, 2, 4, \text{apple}\}$$

Note $1 \in S$

$3 \notin S$

$\text{orange} \notin S$

The elements of a set are not ordered:

$$\{1, 3, 2\} = \{1, 2, 3\}$$

Sets do not see repetition:

$$\{1, 2, 3, 1\} = \{1, 2, 3\}$$

Sets can have other sets as elements:

$$S = \{\{1\}, \{\{2, 3\}, 1\}, 3\}$$

Q: $2 \in S$ ? NO!

$1 \in S$ ? NO!

$3 \in S$ ? YES!

$\{1\} \in S$ ? YES!

There is a unique set with no elements

$$\emptyset := \{\}$$

This is called the <u>empty set</u>.

The most famous set is the set of <u>natural numbers</u>

$$\mathbb{N} := \{0, 1, 2, 3, 4, \ldots\}$$

There are two useful <u>quantifiers</u> for discussing elements of sets

| $\forall$ | $\exists$ |
|---|---|
| universal quantifier | existential quantifier |

We translate them as follows:

"$\forall x \in S$" = "For all $x \in S$ ..."

"$\exists x \in S$" = "there exists $x \in S$ such that ..."

We can use these to define inclusion of sets. Given sets $S, T$ we define

$$\text{“}S \subseteq T\text{''} := \text{“}\forall x \in S,\ x \in T\text{''}$$
$$= \text{“for all } x \in S \text{ we have } x \in T\text{''}$$
$$= \text{“every member of } S \text{ is a member of } T\text{''}$$

If $S \subseteq T$, we say that $S$ is a subset of $T$, or $S$ is included in $T$.

Q: How can we say $S \not\subseteq T$ using quantifiers?

Q: What does the equals sign mean when I say something like

"statement 1" = "statement 2" ?

Q: What is a "statement" anyway?

7/3/14

HW 1 due Monday
Quiz 1 on Monday
No Class Tomorrow

We are discussing Boolean Algebra/Logic

A set $S$ is a "collection of things".
The notation

$$x \in S$$

means "thing $x$ is a member of set $S$".

Today we will also discuss "statements".

Definition: A statement is a sentence that has a definite truth value. That is, a statement is either T or F. Not both. Not neither.

This restricts the domain of logic because most English sentences are not statements.

Examples:

- Let $n \in \mathbb{N}$. Then the sentence

"$n$ is even"

is a statement. I don't know if it's T OR F, but it <u>is</u> one of them.

- The sentence "democracy is a good form of government" is <u>not</u> a stament.

- "$1+2=3$" and "$1+2=4$" are both statements because

$$\text{“}1+2=3\text{”} = T$$
$$\text{“}1+2=4\text{”} = F.$$

- What about this one?

"This sentence is not a statement."

Things can be tricky...

Statements allow us to define sets.
Let $S$ be a set and for all $x \in S$ ($\forall x \in S$) let $P(x)$ be a statement (P is for Proposition). Then we can define the set

$$\{ x \in S : P(x) \}$$

"The set of $x$ in $S$ such that property $P(x)$ is true."

Every statement $P$ has an opposite statement $\neg P$ which is defined as follows:

| $P$ | $\neg P$ |
|---|---|
| T | F |
| F | T |

We say $\neg P =$ "not $P$". Note that "$x \in S$" is a statement. For convenience we define the notation

$$x \notin S := \neg \text{"} x \in S \text{"}$$
$$= \text{"thing } x \text{ is } \underline{\text{not}} \text{ a member of set } S\text{"}$$

Recall the Thinking Problem from last time:

Let $S$ be a set and for all $x \in S$, let $P(x)$ be a statement (depending on $x$). Then we define two new statements

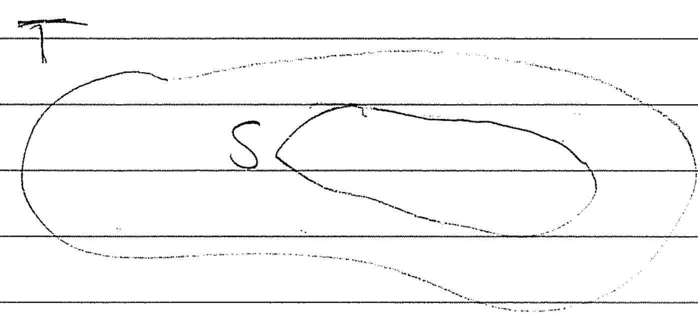
$$\text{"}\forall x \in S, P(x)\text{"} := \text{"}P(x) \text{ is true for all } x \in S\text{"}.$$

$$\text{"}\exists x \in S, P(x)\text{"} := \text{"There exists some } x \in S \text{ such that } P(x) \text{ is true"}$$

Using this we define the <u>subset</u> relation. Given two sets $S, T$ we say

$$\text{"}S \subseteq T\text{"} := \text{"}\forall x \in S, x \in T\text{"}$$
$$= \text{"Every element of } S \text{ is an element of } T\text{"}.$$

Picture:




Thinking Problem: How would you define

$$\text{"}S = T\text{"}\ ??$$

For convenience we define

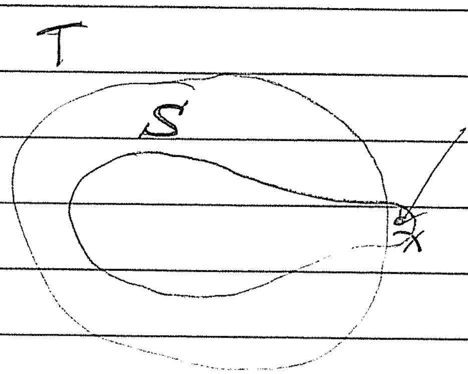
$$\text{"}S \not\subseteq T\text{"} := \neg \text{"}S \subseteq T\text{"}$$

How can this be expressed using the quantifiers $\forall$ and $\exists$ ?

Answer :

$$\begin{aligned} \text{"}S \not\subseteq T\text{"} &= \neg \text{"}S \subseteq T\text{"} \\ &= \neg \text{"}\forall x \in S, \ x \in T\text{"} \\ &= \text{"}\exists x \in S, \ x \notin T\text{"} \end{aligned}$$

Picture :




There exists $x \in S$ such that $x \notin T$.

This is an example of a general principle. Let $S$ be a set and for all $x \in S$ let $P(x)$ be a statement then we have

$$\boxed{\neg(\forall x \in S, P(x)) = \exists x \in S, \neg P(x)}$$

The opposite of "Every $x \in S$ satisfies property $P$" is "There exists some $x \in S$ that does not satisfy property $P$.

Substituting $Q(x) = \neg P(x)$ we also get

$$
\begin{aligned}
\neg(\exists x \in S, Q(x)) &= \neg(\exists x \in S, \neg P(x)) \\
&= \neg\neg(\forall x \in S, P(x)) \\
&= \forall x \in S, P(x) \\
&= \forall x \in S, \neg Q(x).
\end{aligned}
$$

Conclusion:

$$\boxed{\neg(\exists x \in S, Q(x)) = \forall x \in S, \neg Q(x).}$$

In this sense the quantifiers

$$\forall \text{ and } \exists$$

are something like "opposites".

We would also like to define the "opposite" of a set $S$, as follows

$$S^c := \{ \overset{?}{x} : x \notin S \}$$

= "The set of things $x$ such that $x$ is not a member of $S$"

But this makes no sense! <u>Where</u> are all these "things"....?
(<u>This leads to logical paradoxes.</u>)

<u>Remember</u>: Our definition must have the form

$$\{ x \boxed{\in T} : P(x) \}.$$

this part is necessary.

For this reason we introduce the idea of a <u>universal set</u> $U$.

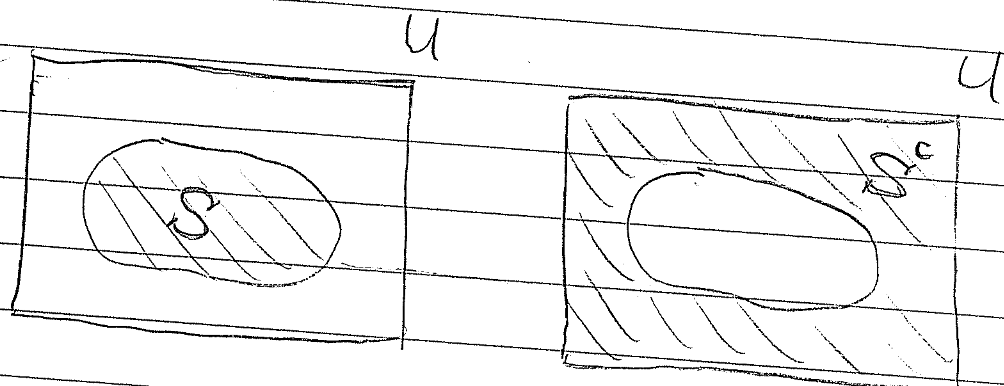
Let $U$ = The set of all things <u>relevant</u> to our current discussion.

This means we will only discuss subsets of $\mathcal{U}$. Now we can define the complement.

Given $S \subseteq \mathcal{U}$ we define

$$S^c := \{ x \in \mathcal{U} : x \notin S \}.$$

Picture:




We know what it means for two statements to be equal: They have the same truth value.

Formally, given statements $P, Q$ we define the statement "$P = Q$" by

| $P$ | $Q$ | $P = Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

But what does it mean to say two <u>sets</u> are <u>equal</u>?

Here is the formal definition:
Given sets $S, T$ we define

$$\text{“}S = T\text{”} := \text{“}S \subseteq T\text{”} \text{ AND } \text{“}T \subseteq S\text{”}$$

What is this!? We didn't define it yet.

Tease: AND is an example of a "function"

7/7/14.

HW 1 due NOW

Quiz 1 NOW. (20 Minutes)

We are discussing Boolean Algebra, which is the basic language of

**sets** and **logical statements**.

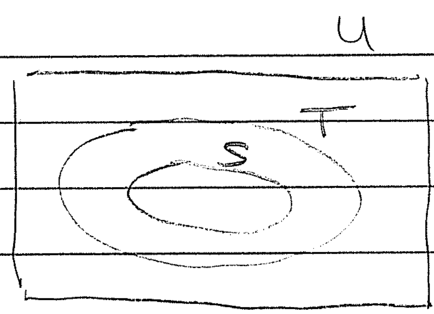
Recall the definition of **subset**. Given two sets $S, T$ we say

$$\text{"} S \subseteq T \text{"} := \text{"} \forall x \in S,\ x \in T \text{"}$$

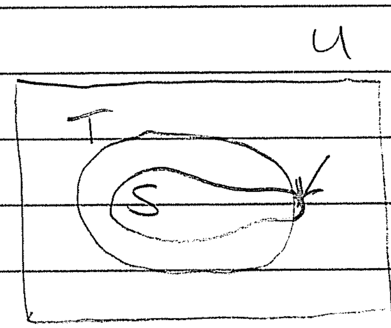
We also have

$$\begin{aligned} \text{"} S \not\subseteq T \text{"} &:= \neg \text{"} S \subseteq T \text{"} \\ &= \neg \text{"} \forall x \in S,\ x \in T \text{"} \\ &= \text{"} \exists x \in S,\ \neg x \in T \text{"} \\ &= \text{"} \exists x \in S,\ x \notin T \text{"} \end{aligned}$$

Pictures:




$S \subseteq T$




$S \not\subseteq T$

Q: How do we formally say that two sets are <u>equal</u>?

A:

"$S = T$" $\equiv$ "$S \subseteq T$" AND "$T \subseteq S$"

[Remark: Maybe I'll start using the symbol "$\equiv$" for equivalence of statements. Hopefully this avoids some confusion...]

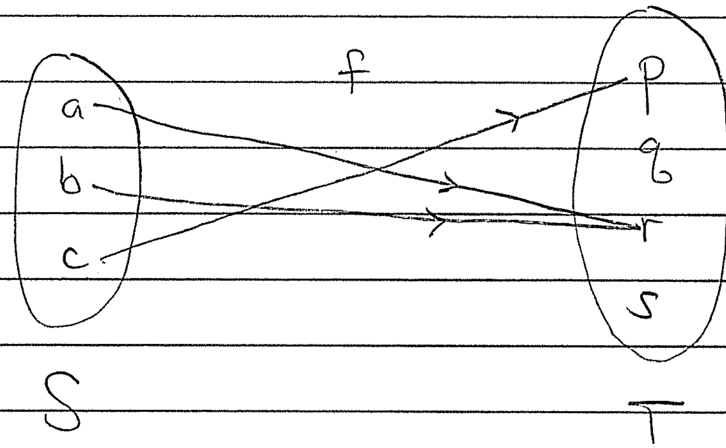
But what is "AND"? We didn't define it yet. To define it we must discuss the concept of a "function".

---

Definition: Let $S$ and $T$ be sets. A <u>function</u> $f: S \to T$ is a set of arrows satisfying two rules:

- Every arrow points from an element of $S$ to an element of $T$.
- Every element of $S$ has <u>exactly one</u> arrow pointing from it.

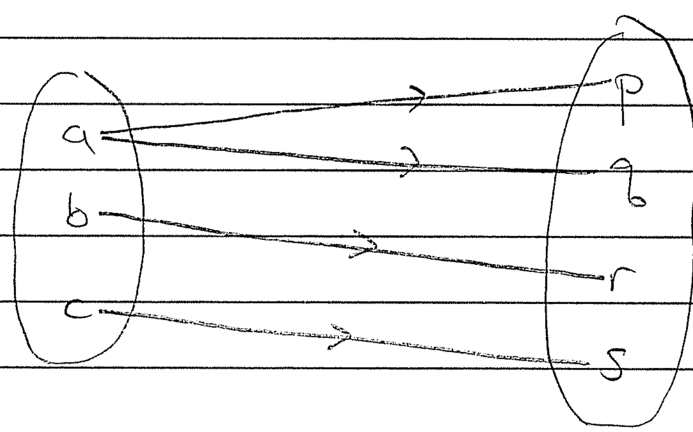
Example: This is a function $f: S \to T$.




For convenience we use the notation

$$f(a) = r, \quad f(b) = r, \quad f(c) = p.$$

Non-Example: This is NOT a function.



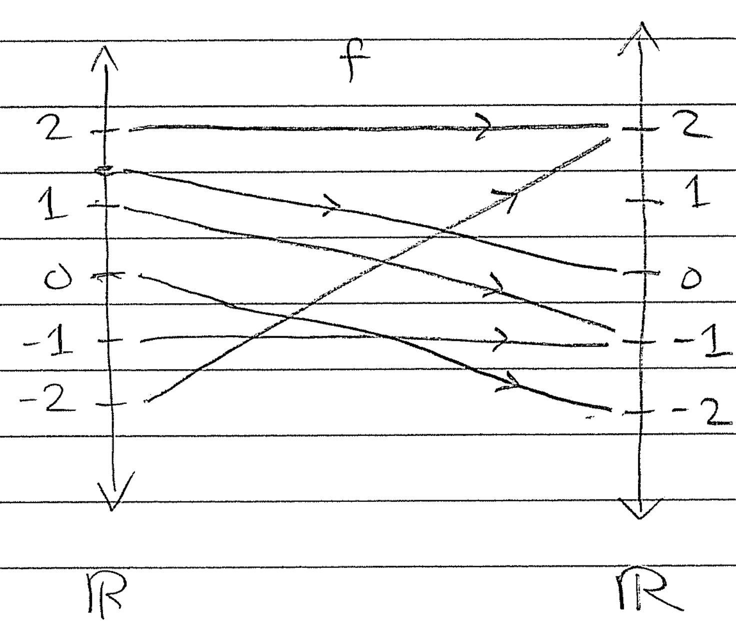

It violates the second rule.

$$a \to p, \quad a \to q \qquad f(a) = ?$$

Example: If $S, T$ are sets of numbers, then we can define functions using algebraic formulas.

The formula $f(x) = x^2 - 2$ defines a function $f : \mathbb{R} \to \mathbb{R}$, where $\mathbb{R}$ is the set of real numbers.

How might we draw this function?




There are too many arrows!
I can't draw them all.
Maybe there's a different / better way to draw this function ...

We need another concept.

Definition: An *ordered pair* is a set with two elements in which order does matter. We use the notation

$$(x, y)$$

1st element $\qquad$ 2nd element.

Then given two sets $S$, $T$ we define their *Cartesian product*

$$S \times T := \{ (s,t) : s \in S, \ t \in T \}$$

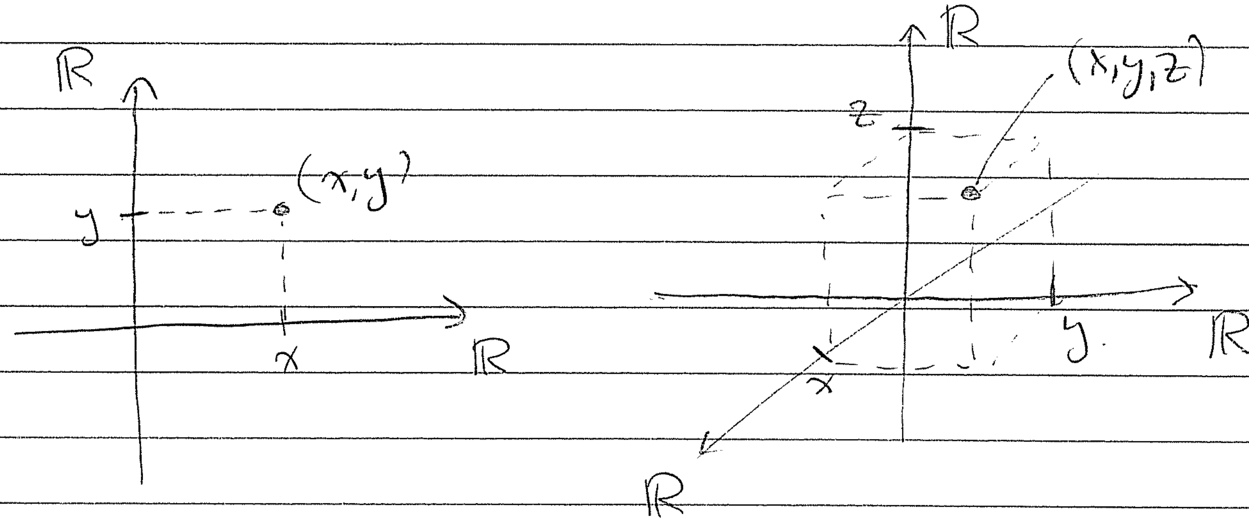
Example: Let $S = \{a, b\}$, $T = \{x, y, z\}$. Then the Cartesian product is

$$S \times T = \{ (a,x), (a,y), (a,z), (b,x), (b,y), (b,z) \}$$

Q: Why is this called the "Cartesian" product?

A : In 1637, Renée Des**cartes** had the revolutionary idea that the sets $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ and $\mathbb{R}^3 := \mathbb{R}^2 \times \mathbb{R}$ can be use to represent 2D and 3D space.

"cartesion coordinates"




This lets us define the "graph" of a function $f : S \to T$. To each arrow $x \longrightarrow f(x)$ we associate the ordered pair $(x, f(x)) \in S \times T$.

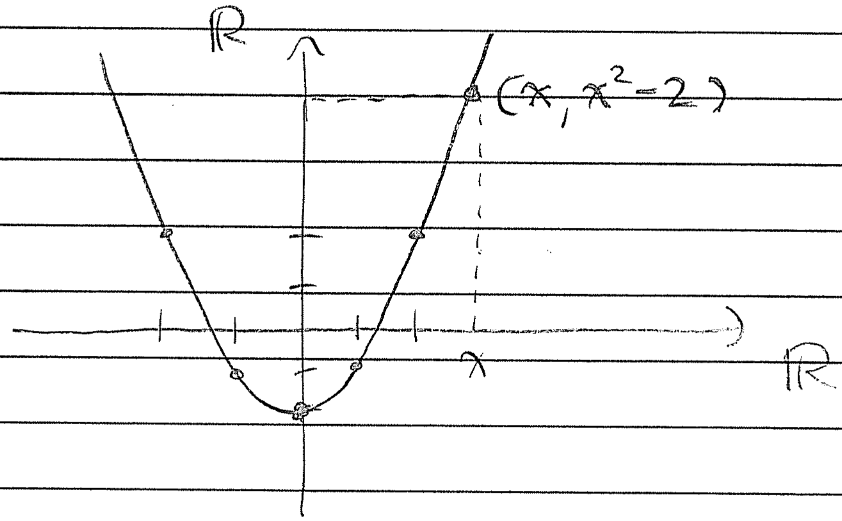
Definition : The **graph** of $f : S \to T$ is the set

$$\{ (x, f(x)) : x \in S \} \subseteq S \times T ,$$

Example: Consider the function $f: \mathbb{R} \to \mathbb{R}$ defined by the formula $f(x) := x^2 - 2$. Its graph is the set

$$\{(x, x^2-2) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$$

which we can visualize as a "curve" in the Cartesian plane $\mathbb{R}^2$.



7/8/14

HW 2 due FRIDAY
Quiz 2 MONDAY.

We are ready to define the fundamental operations of Boolean Algebra.

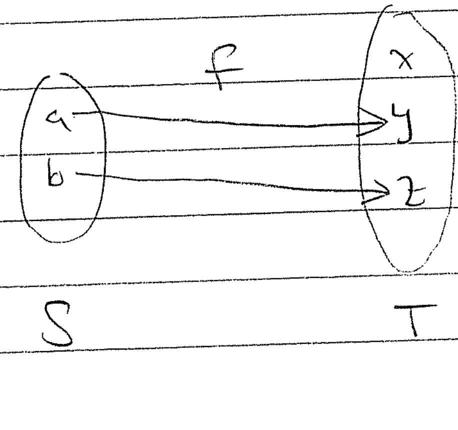
Recall that a function $f: S \to T$ between sets $S$ & $T$ is a set of "arrows" satisfying two rules.

1. Every arrow points from an element of $S$ to an element of $T$.

2. Every element of $S$ has exactly one arrow pointing from it.

Formally, we could think of an "arrow" $s \longrightarrow t$ as an ordered pair $(s,t) \in S \times T$. So a function is a certain special kind of subset of $S \times T$.

Example:



We could think of this function as the set

$$\{(a,y),(b,z)\} \subseteq S \times T.$$

[Recall:

$$S \times T = \{ (a,x), (a,y), (a,z), (b,x), (b,y), (b,z) \}.]$$

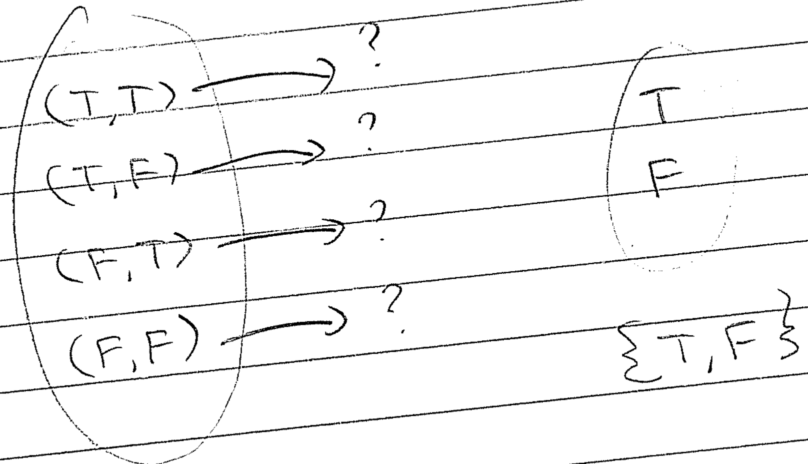
Today we will consider functions

$$f : \{T,F\}^2 \to \{T,F\}.$$

Note that

$$\{T,F\}^2 := \{T,F\} \times \{T,F\}$$
$$= \{ (T,T), (T,F), (F,T), (F,F) \}.$$

So a function $\{T,F\}^2 \to \{T,F\}$ is a set of <u>four arrows</u>:



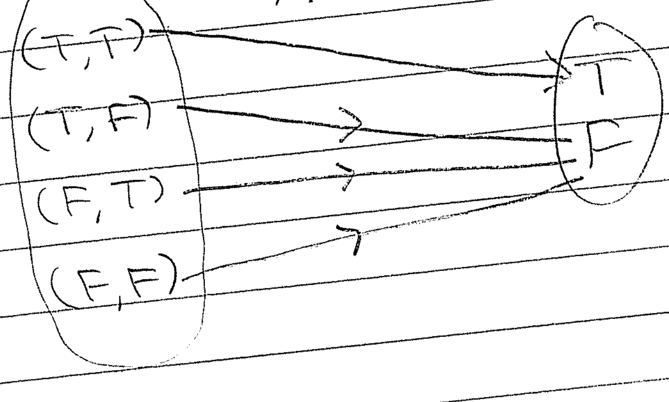

$\{T,F\}^2$

Q: How many choices do we have?

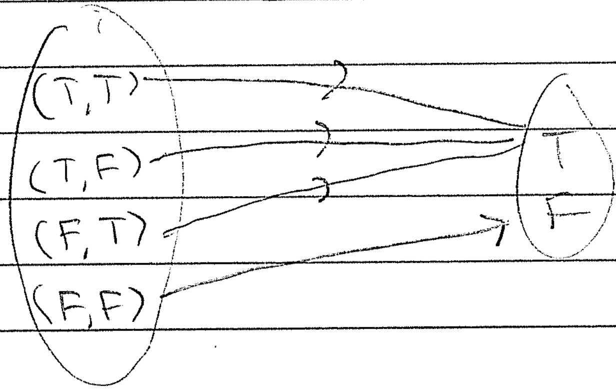
A: There are exactly 16 possibilities. (See HW 2).

I am interested in two special functions called AND and OR.

AND.



OR




We will use the notation of binary operations, similar to "+" and "×"

So:

| | |
|---|---|
| T AND T = T | T OR T = T |
| T AND F = F | T OR F = T |
| F AND T = F | F OR T = T |
| F AND F = F | F OR F = F |

What do the "graphs" of these functions look like? Recall that the <u>graph</u> of a function $f : S \to T$ is the set

$$\{ (x, f(x)) : x \in S \} \subseteq S \times T$$

So the graph of AND : $\{T,F\}^2 \to \{T,F\}$ is the set

$$\{((T,T),T), ((T,F),F), ((F,T),F), ((F,F),F)\}.$$

We prefer to write this information in a table, called a <u>truth table</u>:

| $P$ | $Q$ | $P$ AND $Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

| $P$ | $Q$ | $P$ OR $Q$ |
|---|---|---|
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

---

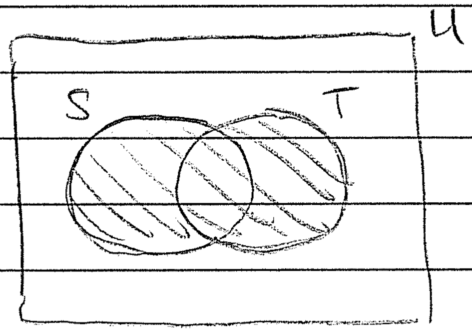
There are two corresponding binary operations on sets.

Let $\mathcal{U}$ be the "universal set". Then for all subsets $S, T \subseteq \mathcal{U}$ we define the <u>union</u> $S \cup T \subseteq \mathcal{U}$ and the <u>intersection</u> $S \cap T \subseteq \mathcal{U}$ as follows:

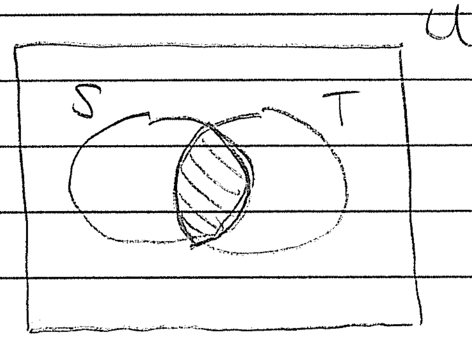
$$S \cup T := \{ x \in U : x \in S \text{ OR } x \in T \}$$

$$S \cap T := \{ x \in U : x \in S \text{ AND } x \in T \}.$$

Here are some helpful pictures:




$S \cup T$

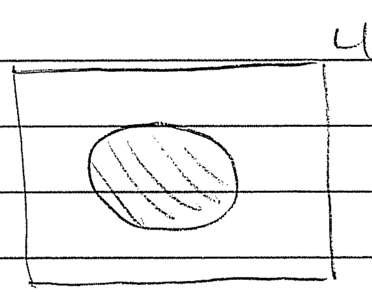



$S \cap T$

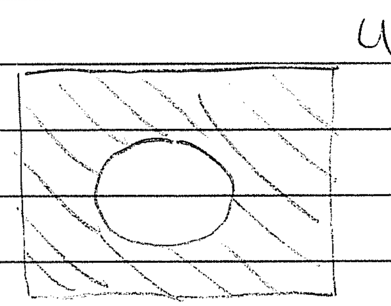
Recall that logical negation corresponds to the <u>complement</u> of a set

$$S^c := \{ x \in U : \text{NOT } x \in S \}.$$

Picture:




$S$




$S^c$

Now we have all the ingredients necessary to define "Boolean Algebra".

Definition: A Boolean algebra is a set $B$ together with three functions called

$$\begin{aligned}&\text{disjunction} \quad \vee : B \times B \to B\\ &\text{conjunction} \quad \wedge : B \times B \to B\\ &\text{negation} \quad \neg : B \to B\end{aligned}$$

and two special elements

$$0 \in B, \quad 1 \in B \quad \text{with } 0 \neq 1$$

satisfying the following five rules/axioms:

(1) Associative Property. $\forall\, a, b, c \in B$,

$$\boxed{\begin{aligned} a \wedge (b \wedge c) &= (a \wedge b) \wedge c.\\ a \vee (b \vee c) &= (a \vee b) \vee c \end{aligned}}$$

(2) Commutative Property : $\forall a, b, c \in B$,

$$\boxed{\begin{array}{l} a \wedge b = b \wedge a \\ a \vee b = b \vee a \end{array}}$$

(3) Property of 0 & 1 : $\forall a \in B$,

$$\boxed{\begin{array}{l} a \vee 0 = a \\ a \wedge 1 = a \end{array}}$$

(4) Property of Negation : $\forall a \in B$,

$$\boxed{\begin{array}{l} a \vee \neg a = 1 \\ a \wedge \neg a = 0 \end{array}}$$

(5) Distributive Property : $\forall a, b, c \in B$,

$$\boxed{\begin{array}{l} a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \end{array}}$$

We have already met two examples of a Boolean algebra.

Example 1: Let $U$ be a set (the "universal set") and let

$$\mathcal{P}(U) := \text{The set of all subsets of } U.$$

Then the set $B = \mathcal{P}(U)$ with operations

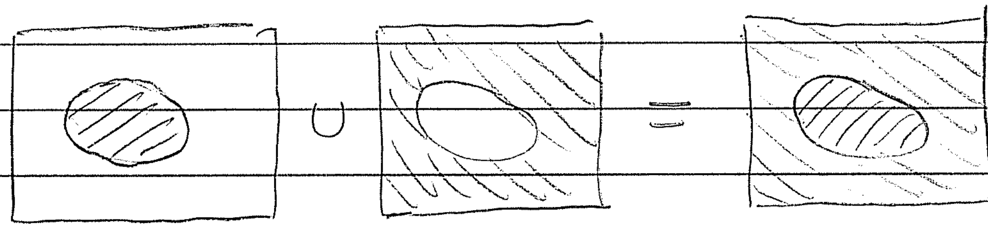
$\vee = \cup$ (union)
$\wedge = \cap$ (intersection)
$\neg = {}^c$ (complement)

and special elements

$0 = \emptyset$ (empty set)
$1 = U$ (universal set)

is a Boolean algebra. It would be tedious to verify all the axioms so we'll just check a couple.

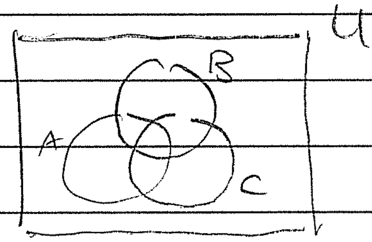
For all $S \in \mathcal{P}(U)$ (i.e. $S \subseteq U$) do we have $S \cup S^c = U$?

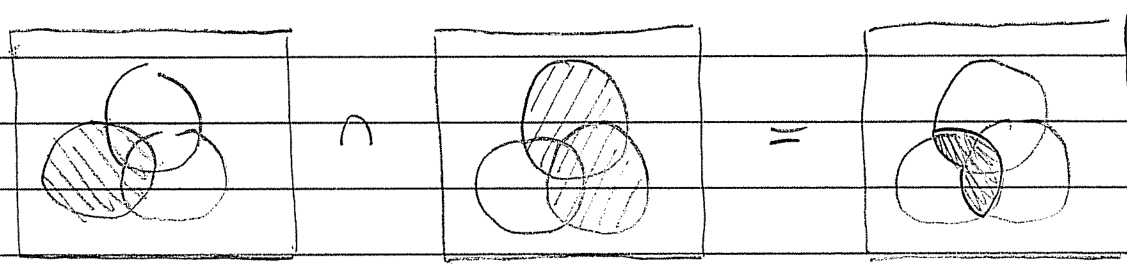


Yes ✓

For all $A, B, C \in \mathcal{P}(U)$ do we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$?

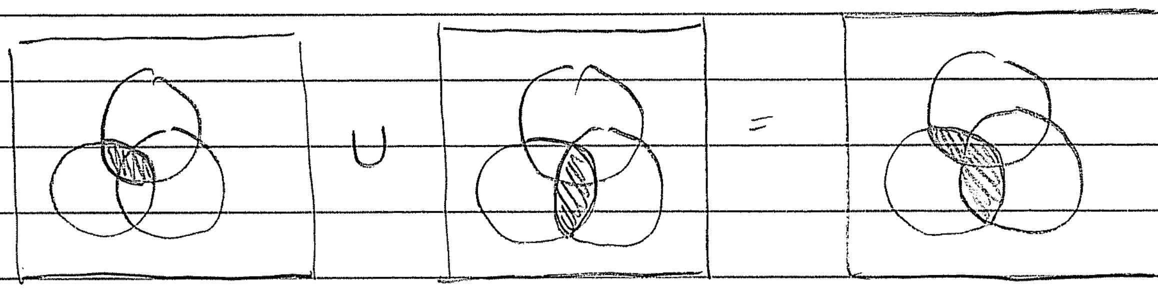
Consider



A $\qquad$ $B \cup C$

‖ Yes ✓



$A \cap B$ $\qquad$ $A \cap C$

Example 2: The set $B = \{T, F\}$ together with operations

$\vee$ = OR
$\wedge$ = AND
$\neg$ = NOT

and special elements

$0 = F$
$1 = T$

is a Boolean algebra. In this case we would use truth tables to verify all the axioms. Here are a couple of example calculations.

Show that $\forall P \in B$, P AND (NOT P) = F.

| P | NOT P | P AND (NOT P) |
|---|---|---|
| T | F | F |
| F | T | F |

✓

Show that $\forall P, Q, R \in B$ we have

$$P \text{ AND } (Q \text{ OR } R) = (P \text{ AND } Q) \text{ OR } (P \text{ AND } R).$$

| P | Q | R | Q OR R | P AND (Q OR R) |
|---|---|---|---|---|
| T | T | T | T | T |
| T | T | F | T | T |
| T | F | T | T | T |
| T | F | F | F | F |
| F | T | T | T | F |
| F | T | F | T | F |
| F | F | T | T | F |
| F | F | F | F | F |

| P | Q | R | P AND Q | P AND R | (P AND Q) OR (P AND R) |
|---|---|---|---|---|---|
| T | T | T | T | T | T |
| T | T | F | T | F | T |
| T | F | T | F | T | T |
| T | F | F | F | F | F |
| F | T | T | F | F | F |
| F | T | F | F | F | F |
| F | F | T | F | F | F |
| F | F | F | F | F | F |

They are the same ✓

7/9/14

HW 2 due Friday
Quiz 2 Monday

Today we will think like computers.

(See the handout on Boolean Algebras)

I don't know how long it will take.
If there's time, we will discuss
"Boolean addition".

Boolean Addition:

There is an alternative way to encode
Boolean algebras, using the following
operation. For all $a, b \in B$ we define

$$a \oplus b := (a \wedge \neg b) \vee (\neg a \wedge b)$$

What interpretation does this have
in the two cases we know?

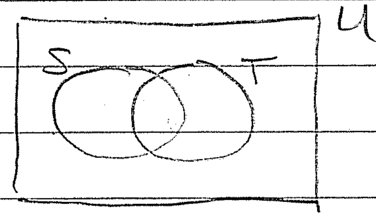
Example 1: The Boolean algebra of sets.

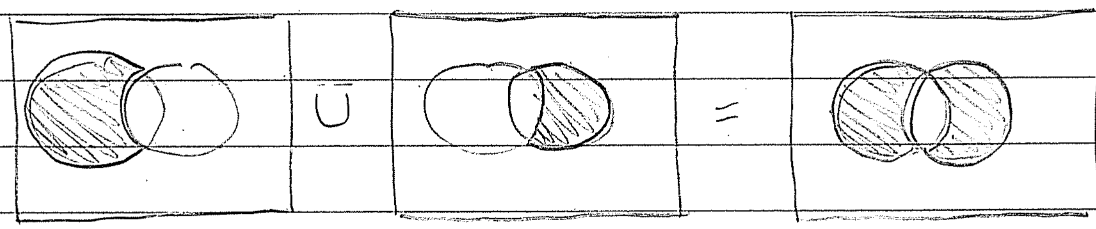
$$(\mathcal{P}(U), \cup, \cap, {}^c, \emptyset, U)$$

In this language we have

$$S \oplus T := (S \cap T^c) \cup (S^c \cap T)$$

Picture: Consider



$S \cap T^c$ $\cup$ $S^c \cap T$ $=$ $S \oplus T$

The set $S \oplus T$ is sometimes called the <u>symmetric</u> <u>difference</u> of $S$ and $T$.

Example 2: The Boolean algebra

$$(\{T, F\}, \text{OR}, \text{AND}, \text{NOT}, T, F).$$

Given $P, Q \in \{T, F\}$ we define

$$P \oplus Q := (P \text{ AND NOT } Q) \text{ OR } (\text{NOT } P \text{ AND } Q)$$

Truth Table:

| P | Q | NOT P | NOT Q | P AND NOT Q | NOT P AND Q | $P \oplus Q$ |
|---|---|---|---|---|---|---|
| T | T | F | F | F | F | F |
| T | F | F | T | T | F | T |
| F | T | T | F | F | T | T |
| F | F | T | T | F | F | F |

So maybe a better symbol would be

$$P \oplus Q = P \not\equiv Q$$
$$= \neg(P \equiv Q)$$

(also called XOR)

Example 3: The set $\{0, 1\}$ is itself a Boolean algebra in the obvious way in this case we can interpret

$$a \oplus b = a + b \pmod 2$$

"addition mod 2"

$$a \wedge b = ab \pmod 2$$

"multiplication mod 2"

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

So, in general, $\oplus$ and $\wedge$ act like $+$ and $\times$.

Q: Why do we then prefer $\vee$ and $\wedge$ as the basic operations of Boolean algebra?

Three Answers:

A1. Because of the Duality Principle

$$\vee \leftrightarrow \wedge, \quad 0 \leftrightarrow 1$$

A2. Because the operators AND, OR and $\cap$, $\cup$ seem natural to us humans.

A3. No good reason; it was a random historical choice. Apparently, computer engineers prefer

$$P \text{ NAND } Q := \text{NOT } (P \text{ AND } Q)$$
$$P \text{ NOR } Q := \text{NOT } (P \text{ OR } Q)$$

because they're more efficient.

7/10/14

HW 2 due tomorrow

Quiz 2 on Monday.

We defined a Boolean algebra as an abstract structure

$$(B, \vee, \wedge, \neg, 0, 1)$$

satisfying five axioms. There are many other equivalent definitions but we chose this one.

We have two main interpretations in mind:

Boolean Algebra

Set Theory

$(\mathcal{P}(U), \cup, \cap, ^c, \emptyset, U)$

Logic

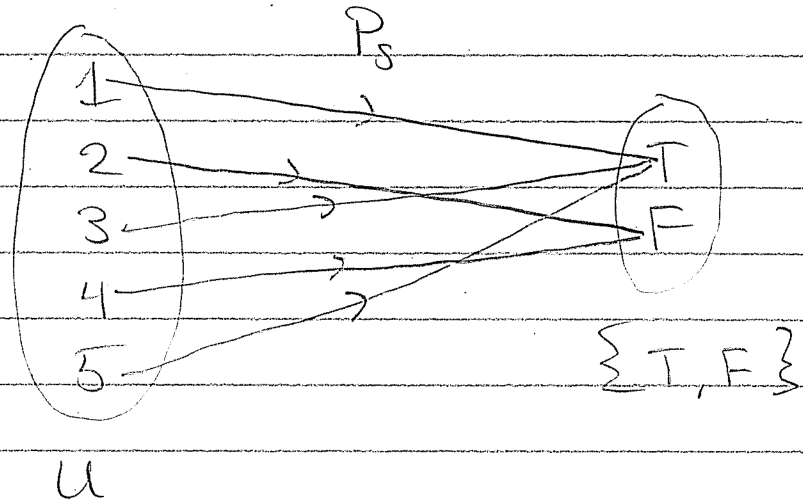
$(\{T, F\}, \text{OR}, \text{AND}, \text{NOT}, F, T)$

In fact, there is a neat dictionary between these two interpretations.

To each set $S \subseteq \mathcal{U}$ we associate the function $P_S : \mathcal{U} \longrightarrow \{T, F\}$ defined by

$$P_S(x) := \text{“} x \in S \text{”}$$

Example: Let $\mathcal{U} = \{1, 2, 3, 4, 5\}$. Then the subset $S := \{1, 3, 5\} \subseteq \mathcal{U}$ is represented by the function




We could call this function

“is a member of $S$”.

Can we go backwards?

That is, given a function $P: U \to \{T,F\}$ can we define a subset of $U$?

Yes. I already told you how to do this. We can define the subset

$$U_P := \{ x \in U : P(x) (= T) \}$$

This gives us a "1-to-1 correspondence"

$$\begin{array}{ccc} \text{subsets of } U & \longleftrightarrow & \text{functions } U \to \{T,F\} \\ S & \longmapsto & P_S \\ U_P & \longmapsfrom & P \end{array}$$

[<u>You</u> will explore the example $U = \{1,2,3\}$ on HW 2.]

This correspondence gives us a "dictionary": Given $S, T \subseteq U$ we have

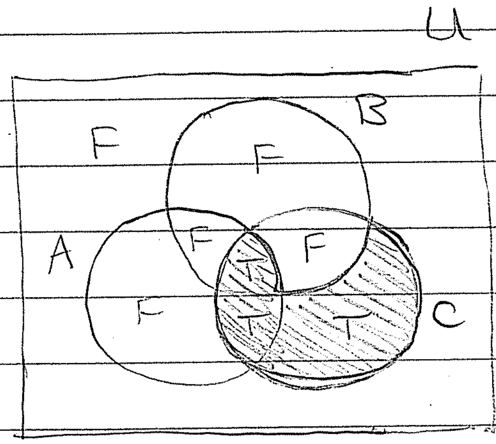
$$S \cup T := \{ x \in U : x \in S \text{ OR } x \in T \}$$

$$S \cap T := \{ x \in U : x \in S \text{ AND } x \in T \}$$

$$S^c := \{ x \in U : \text{NOT } x \in S \}$$

We also have a correspondence between Venn diagrams and truth tables.

Example: Let $A, B, C \subseteq \mathcal{U}$ with corresponding statements $P, P, P : \mathcal{U} \to \{T, F\}$. Then the set $(A \cup B^c) \cap C$ and corresponding statement $(P_A \text{ OR NOT } P_B) \text{ AND } P_C$ are represented by




$(A \cup B^c) \cap C$

| $P_A$ | $P_B$ | $P_C$ | $(P_A \vee \neg P_B) \wedge P_C$ |
|---|---|---|---|
| T | T | T | T |
| T | T | F | F |
| T | F | T | T |
| T | F | F | F |
| F | T | T | F |
| F | T | F | F |
| F | F | T | T |
| F | F | F | F |

There are 8 regions of the Venn diagram and 8 rows of the truth table. The correspondence is

shaded = T

unshaded = F

///

Incidentally, this gives us an easy way to express <u>any</u> Boolean function

$$\varphi : \{T, F\}^3 \longrightarrow \{T, F\}$$
$$(P, Q, R) \longmapsto \varphi(P, Q, R).$$

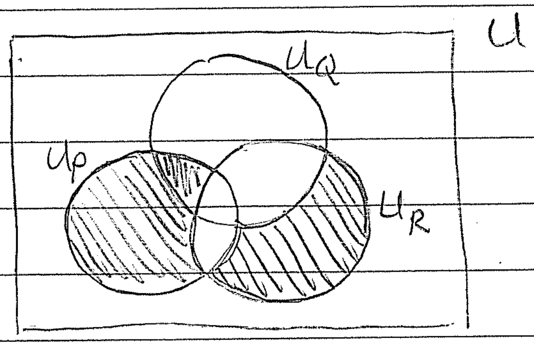
"a Boolean function of 3 variables."

in terms of the <u>basic</u> functions $\vee, \wedge, \neg$.

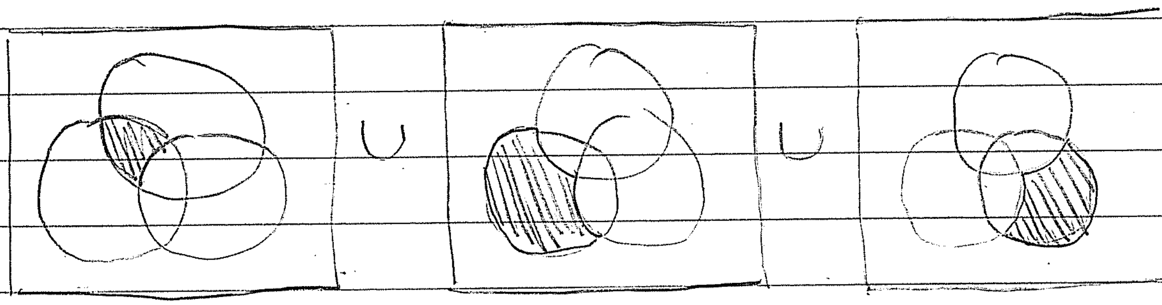
Example Problem: Express the following function $\varphi(P, Q, R)$ in terms of $\vee, \wedge, \neg$.

| P | Q | R | $\varphi(P,Q,R)$ |
|---|---|---|---|
| T | T | T | F |
| T | T | F | T |
| T | F | T | F |
| T | F | F | T |
| F | T | T | F |
| F | T | F | F |
| F | F | T | T |
| F | F | F | F |

Solution: Think of it as a set.




Break the set into a union of small pieces.




$(U_P \cap U_Q \cap U_R^c)$ $(U_P \cap U_Q^c \cap U_R^c)$ $(U_P^c \cap U_Q^c \cap U_R)$

The small pieces have easy formulas in terms of $\cap$ and $^c$.

Translate this expression back into logic.

$$\varphi(P,Q,R) = (P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)$$

This expression is called the "disjunctive normal form" of $\varphi$.

Two Remarks:

1. We showed that <u>every</u> Boolean function $\{T,F\}^3 \to \{T,F\}$ can be expressed in terms of $\vee, \wedge, \neg$. More generally, the "same" method works to express any function $\{T,F\}^n \to \{T,F\}$ in terms of $\vee, \wedge, \neg$.

2. We now have an algorithm to determine whether two Boolean functions are equal: Put them both in disjunctive normal form and compare.

Thinking Problem:

3. Define the "Sheffer stroke" (or NAND function) by

$$P \uparrow Q = P \text{ NAND } Q := \text{NOT}(P \text{ AND } Q).$$

| $P$ | $Q$ | $P \uparrow Q$ |
|---|---|---|
| T | T | F |
| T | F | T |
| F | T | T |
| F | F | T |

Show that every Boolean function $\{T, F\}^n \to \{T, F\}$ can be expressed using only the Sheffer stroke.

[Hint: Express $\vee, \wedge, \neg$ in terms of $\uparrow$ ]

[Bigger Hint: Show that

$$\neg P = P \uparrow P$$

$$P \vee Q = (P \uparrow P) \uparrow (Q \uparrow Q)$$

$$P \wedge Q = (P \uparrow Q) \uparrow (P \uparrow Q).$$ ]

OK, let's do it together.

(*) $P \uparrow P = \neg(P \wedge P)$ definition

$= \neg P$ (6)

$(P \uparrow P) \uparrow (Q \uparrow Q) = \neg P \uparrow \neg Q$ (*)

$= \neg(\neg P \wedge \neg Q)$ definition

$= \cancel{\neg}\cancel{\neg}(P \vee Q)$ de Morgan

$= P \vee Q.$

$(P \uparrow Q) \uparrow (P \uparrow Q)$

$$= \neg (P \uparrow Q) \qquad (*)$$
$$= \cancel{\neg}\cancel{\neg} (P \wedge Q) \qquad \text{definition}$$
$$= P \wedge Q .$$

Bonus Remarks:

4. This illustrates the utility of abstract Boolean algebra (particularly De Morgan's identities). These calculations would have been much longer using truth tables.

5. Apparently, one type of flash memory (invented 1984 by Toshiba) is based on the Sheffer stroke $\uparrow$. It is called NAND flash memory. There is also NOR flash memory, based on "Peirce's arrow"

$$P \downarrow Q = P \text{ NOR } Q := \text{NOT}(P \text{ OR } Q).$$