Set Theory

We are done discussing Steiner's Problem and sums of p^{th} powers. This was intended as a set-piece and an introduction to the subject at a human level.

Now we'll switch gears to discuss the mathematics behind <u>computer</u> <u>hardware</u>.

This is the science of <u>binary</u> <u>arithmetic</u> (0s & 1s). It was initiated by Gottfried Leibniz in 1679, inspired by the ancient "I-Ching". It reached a modern form with George Boole's

"Investigation of the Laws of Thought" (1854).

The modern form of the subject is called <u>Boolean</u> <u>Algebra</u>.

The two main examples of Boolean Algebra are ① Set Theory
② Boolean Logic.

We begin with set theory.

Definition: A set is a "collection of things". It has just one attribute, called "membership". We use the notation

$$\boxed{x \in S}$$

to say that "thing x is a member of set S".

For finite sets we use a notation like this

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

Note that $1 \in S$

$3 \notin S$

orange $\notin S$

↓

The members of a set are not ordered:

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

Sets do not see repetition:

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

[Reason: Because we either have $3 \in S$ or $3 \notin S$. There are no other options.]

Sets can have other sets as members:

$$S = \{2, \{1\}, \{1, \{3,4\}\}\}$$

Q: $1 \in S$? NO.
$2 \in S$? Yes.
$\{1\} \in S$? Yes.
$\{2\} \in S$? NO.

There exists a unique set with no members. It is called the "empty set". We write it like this

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

Often we consider sets of numbers. Here are some favorites.

The set of natural numbers

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

The set of integers

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

The set of rational numbers

$$\mathbb{Q} = \{0, \tfrac{1}{2}, -\tfrac{3}{8}, \tfrac{57}{3}, \dots\}.$$

The set of real numbers

$$\mathbb{R} = \{0, 5, \sqrt{2}, \pi, e, \dots\}$$

[We probably need better definitions of these sets. Stay tuned.]

Given two sets A and B, we say that A is a subset of B if for all things x the following statement is true:

"**if** $x \in A$ **then** $x \in B$".

We use the notation

"$A \subseteq B$" = "A is a subset of B"

For example, the set $\{1, 2, 3\}$ has 8 different subsets. Can you find them?

Answer: They are

$$\begin{array}{llll} \{1,2,3\}, & \{1,2\}, & \{1\}, & \emptyset . \\ & \{1,3\}, & \{2\}, & \\ & \{2,3\}, & \{3\}, & \end{array}$$

Remark: For **any** set S, we have

$$\emptyset \subseteq S .$$

Sometimes we define a subset by requiring that its members have a certain property.

For example we can define the set of "even" integers

$$\{ n \in \mathbb{Z} : n \text{ is a multiple of } 2 \}.$$

"The set of integers n such that n is a multiple of 2".

In general, let S be a set and, for all members $x \in S$, let $P(x)$ be a logical statement about x. Then we define the set

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

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

This is called <u>set-builder</u> <u>notation</u>.

↓

For example, let

$S :=$ The set of people in this room.

Then

$\{x \in S : x \text{ is from Canada}\} = \{\text{me}\}$

$\{x \in S : x \text{ is 35 years old}\} = \{\text{me}\}$.

Another example from Bertrand Russell: Let

$S :=$ The set of all sets

and consider the subset

$R := \{A \in S : A \notin A\}$

Q: Is the set R a member of itself?

A: If $R \in R$ then by definition $R \notin R$.
But if $R \notin R$ then by definition $R \in R$.

Wait. Can the statement "$R \in R$" be both true and false at the same time?

This is called "Russell's Paradox".

Moral of the story: You are *not allowed* to discuss "the set of all sets".

In practice, we will always fix a "universal set" U, and then we will only allow ourselves to discuss *subsets* of U.

Given two sets $A, B \subseteq U$, there are two important ways to combine them into a *new* subset of U.

We define the *union*

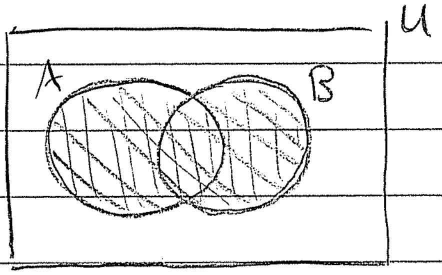
$$A \cup B := \{ x \in U : x \in A \text{ or } x \in B \}$$

and the *intersection*

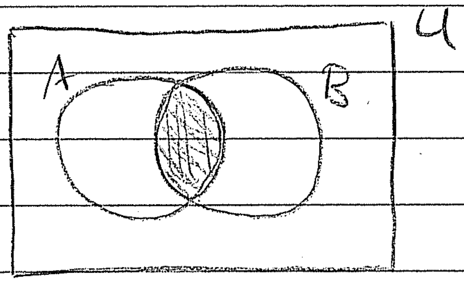
$$A \cap B := \{ x \in U : x \in A \text{ and } x \in B \}.$$

↓

Here are some helpful pictures, called "Venn diagrams":



$A \cup B$

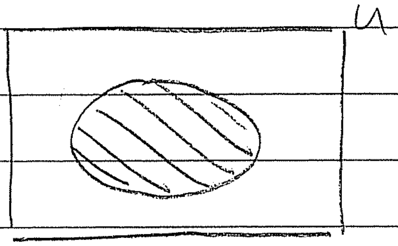


$A \cap B$

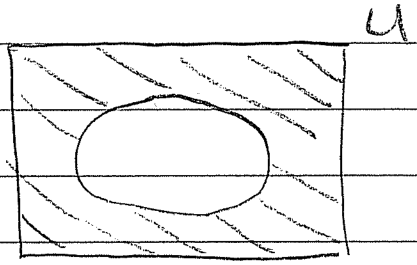
Given any subset $A \subseteq U$, we also define its complement:

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

Picture



A



A^c

[Remark: The notation A^c makes no sense unless we have a specific universal set U in mind.]

Some "algebraic" properties of sets.

Let $\mathcal{U}$ be the universal set. Then for all subsets $A, B, C \subseteq \mathcal{U}$ we have

① $A \cap (B \cap C) = (A \cap B) \cap C$
$A \cup (B \cup C) = (A \cup B) \cup C$

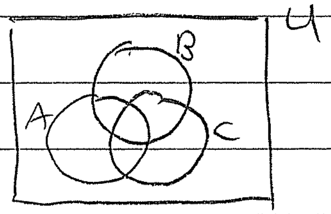
② $A \cap B = B \cap A$
$A \cup B = B \cup A$

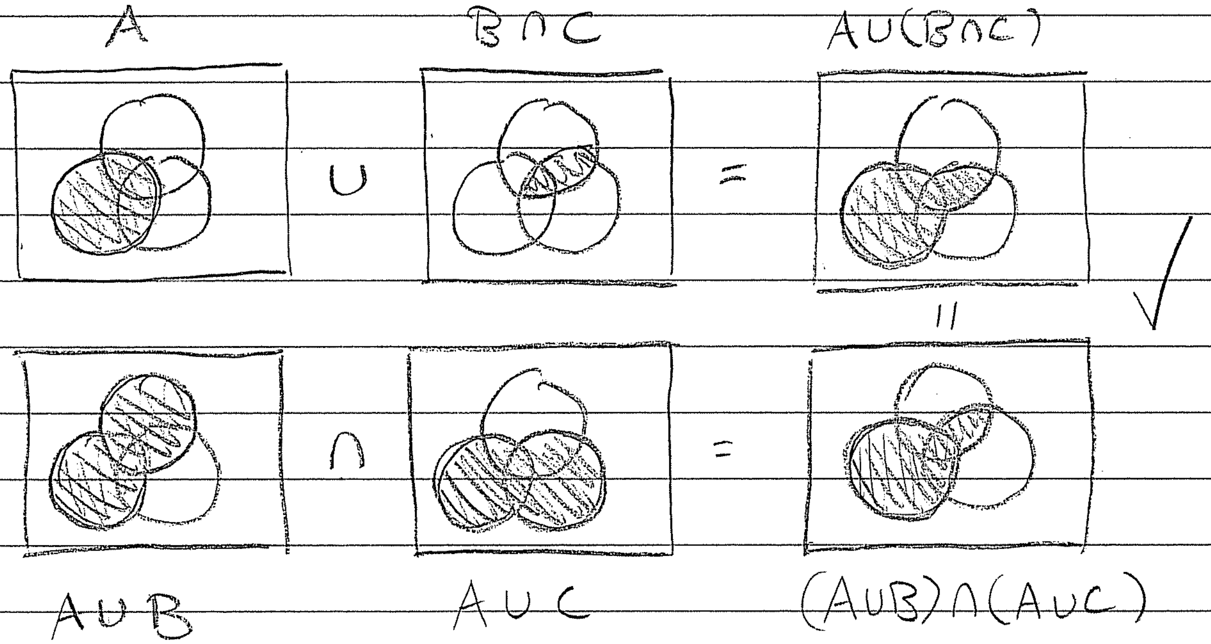
③ $A \cup \emptyset = A$
$A \cap \mathcal{U} = A$

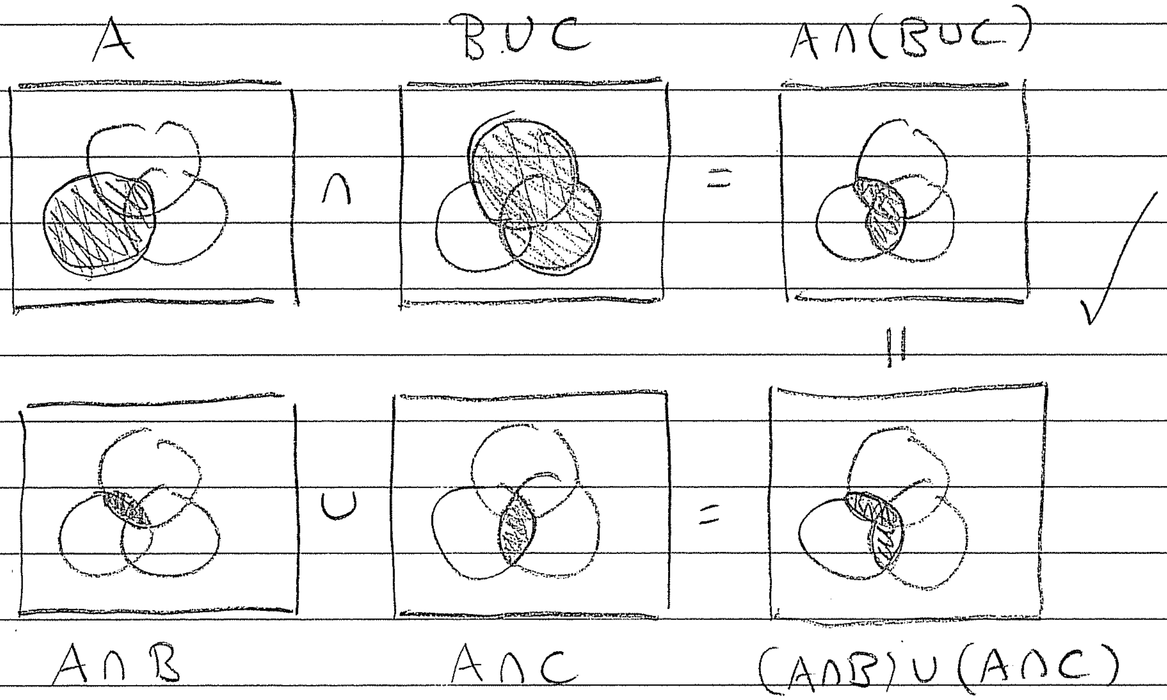
④ $A \cup A^c = \mathcal{U}$
$A \cap A^c = \emptyset$

⑤ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Those are <u>mostly</u> obvious, but we should probably check property ⑤.

Consider 





These are called "distributive laws"

I remember them by thinking about addition and multiplication of numbers

$$a \times (b+c) = (a \times b) + (a \times b).$$

Warning! This analogy is limited because

$$a + (b \times c) \neq (a+b) \times (a+c).$$

Thinking Problems:

- Consider $A, B \subseteq \mathcal{U}$. Can you express the statement "$A \subseteq B$" using only the symbols $A, B, \cup, \cap, {}^c, =$?

- How about the statement "$A \not\subseteq B$"?

Logic

Current Topic : Boolean Algebra.

The two main examples of Boolean algebra are ① Set Theory, and ② Logic. These provide the foundation for both math and computer science.

Last time we discussed sets.
Today we begin with logic.

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

Remark : This necessarily restricts the domain of logic because most (all ?) English sentences are *not* logical statements

↓

Examples:

- Let $n \in \mathbb{Z}$. The sentence

  "n is even"

  is a statement. I don't know if it's T or F, but it definitely is one (and only one) of them.

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

- "$1+2=3$" 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."

  We'll try to avoid sentences like this.

We already saw some statements last time when discussing sets. Consider

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

For all $x \in S$ we define the statement

$$P(x) := \text{" } x \text{ is on even integer "}$$

So $P(1) = F$
$P(2) = T$
$P(4) = T$
$P(\text{apple}) = F$.

and $\{x \in S : P(x)\} = \{2, 4\}$

Definition: Given a statement $P \in \{T, F\}$ we define its *negation* $\neg P$ as follows:

P	$\neg P$
T	F
F	T .

We say $\neg P =$ "not P". ///

Then we have

$$\{x \in S : \neg P(x)\} = \{1, \text{apple}\}.$$

Very often we want to discuss <u>all</u> the elements of a set at the same time. To do this we use the symbols

$$\forall \qquad\qquad\qquad \exists$$

universal quantifier   existential quantifier.

We read them as follows:

"$\forall x \in S, \ldots$" = "For all $x \in S, \ldots$"

"$\exists x \in S, \ldots$" = "There exists $x \in S$ such that $\ldots$"

For example, when $S = \{1, 2, 4, \text{apple}\}$ and $P(x) =$ "x is an even integer" we have

"$\forall x \in S, P(x)$" $= F$

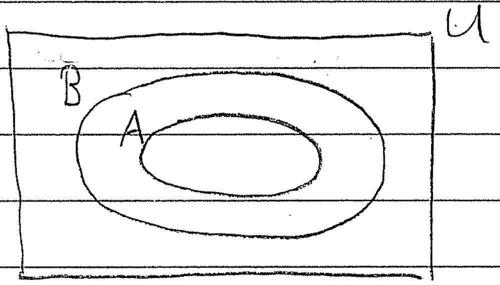
"$\exists x \in S, P(x)$" $= T$.

Recall that for sets A and B we say "A is a subset of B" (and write "$A \subseteq B$") if for all $x \in A$ we also have $x \in B$.

In symbols, we can write

$$\text{"}A \subseteq B\text{"} = \text{"}\forall x \in A,\ x \in B\text{"}$$

Picture:

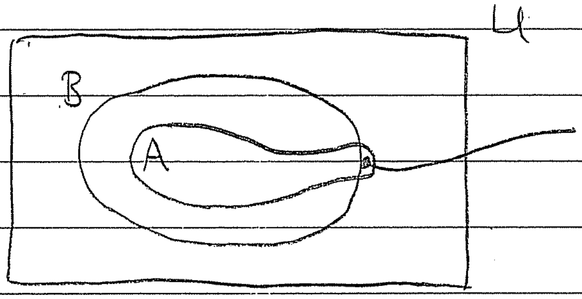


For convenience we can define

$$\text{"}A \nsubseteq B\text{"} := \neg \text{"}A \subseteq B\text{"}$$

Q: How can we say "$A \nsubseteq B$" more directly?

A: Think about a picture.



There exists $x \in A$ such that $x \notin B$.

So we have

$$\begin{aligned} \text{“}A \not\subseteq B\text{”} &= \neg \text{“}\forall x \in A,\ x \in B\text{”} \\ &= \text{“}\exists x \in A,\ \neg\, x \in B\text{”} \\ &= \text{“}\exists x \in A,\ x \notin B\text{”}. \end{aligned}$$

This illustrates a general principle. Let S be a set and for all $x \in S$ let $P(x)$ be a statement. Then we have

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

In this sense, the quantifiers

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

are something like "opposites".

Recall from last time that there is an "algebra" of sets. For this we <u>must</u> fix a universal set $\mathcal{U}$.

↓

Then for all $A, B \subseteq U$ we define

"A union B"

$$A \cup B := \{ x \in U : x \in A \text{ OR } x \in B \}$$

"A intersect B"

$$A \cap B := \{ x \in U ; x \in A \text{ AND } x \in B \}$$

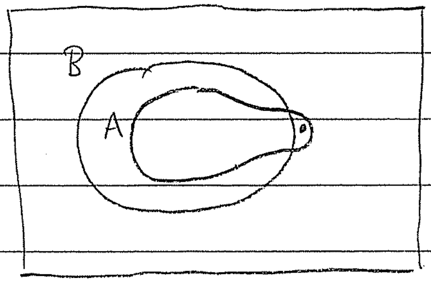
"A complement"

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

Recall the Thinking Problem:

How can we express "$A \subseteq B$" and "$A \nsubseteq B$" in terms of the operators $\cup, \cap, {}^c$?

The key is the picture of "$A \nsubseteq B$"



"$A \nsubseteq B$" = "$\exists x \in A, x \notin B$"

We could also say

$$\text{“}A \not\subseteq B\text{”} = \text{“}\exists x \in U,\ x \in A \text{ AND } x \notin B\text{”}$$
$$= \text{“}\exists x \in U,\ x \in A \text{ AND } x \in B^c\text{”}$$
$$= \text{“}\exists x \in U,\ x \in A \cap B^c\text{”}$$

and this is just saying that

$$\text{“}A \not\subseteq B\text{”} = \text{“}A \cap B^c \neq \emptyset\text{”}$$

Q: Does this help us express “$A \subseteq B$” ?

A: Yes. We have

$$\text{“}A \subseteq B\text{”} = \neg\text{“}A \not\subseteq B\text{”}$$
$$= \neg\text{“}A \cap B^c \neq \emptyset\text{”}$$
$$= \text{“}A \cap B^c = \emptyset\text{”}.$$

Summary:

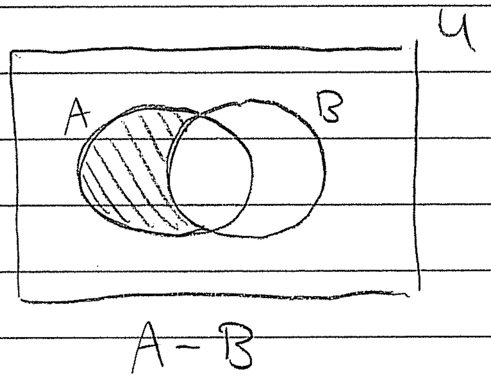
$$\boxed{\text{“}A \subseteq B\text{”} = \text{“}A \cap B^c = \emptyset\text{”}}$$

That might be useful later.

While we're here, let's define a notation:

$$\text{“}A - B\text{''} := \{x \in \mathcal{U} : x \in A \text{ AND } x \notin B\}$$
$$= A \cap B^c .$$

Picture:



//

The benefit of developing an "algebra" of sets (which was Boole's original goal) is that we can use it mindlessly.

Example: Show that "$A \subseteq B$" = "$B^c \subseteq A^c$".

Proof: "$A \subseteq B$" = "$A \cap B^c = \emptyset$"
= "$B^c \cap A = \emptyset$"
= "$(B^c) \cap (A^c)^c = \emptyset$"
= "$B^c \subseteq A^c$".

//

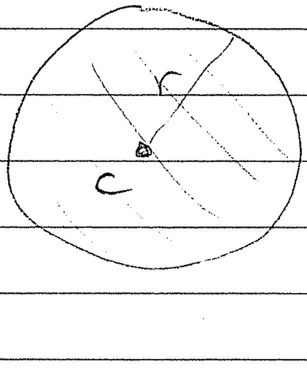
Epilogue

Here's an example from Calculus showing why "Booleon algebra" is useful.

Intuitively we know what $\lim_{x \to a} f(x) = l$ means.

But, if we ever want to prove something about Calculus then we need a more "formal" definition. The following (frightening!) definition was given by Bernard Bolzano in 1817.

Given a point c and a real number $r > 0$, we let $B_r(c)$ be the ball centered at c with radius r:

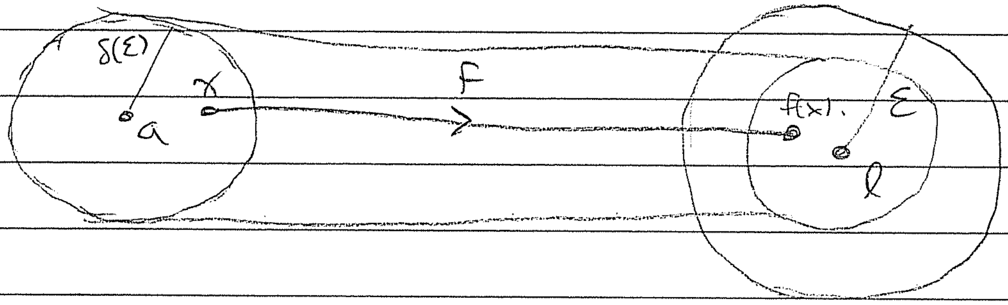


Let f be a function between spaces then we say "the limit of f(x) as x approaches a equals l"

and we write "$\lim_{x \to a} f(x) = \ell$" to mean that

$$\forall \varepsilon > 0,\ \exists \delta(\varepsilon) > 0,\ \forall x \in B_{\delta(\varepsilon)}(a),\ f(x) \in B_{\varepsilon}(\ell).$$

Maybe a picture will help.



"Given any $\varepsilon > 0$, I can find a number $\delta > 0$ (depending on ε) such that whenever x is in the δ-ball around a, $f(x)$ is in the ε-ball around ℓ."

So far, so good. But when I was an undergrad, I was once asked to prove that

$$\neg \text{"} \lim_{x \to a} f(x) = \ell \text{"}.$$

↓

This gave me trouble because I couldn't even parse it. I wish I had known the rules

$$\neg(\forall x \in S, P(x)) = \exists x \in S, \neg P(x)$$
$$\neg(\exists x \in S, P(x)) = \forall x \in S, \neg P(x).$$

Then I would have known that

$$\neg \text{“}\lim_{x \to a} f(x) = l\text{''}$$

$$= \neg(\forall \varepsilon > 0, \exists \delta > 0, \forall x \in B_\delta(a), f(x) \in B_\varepsilon(l))$$

$$= \exists \varepsilon > 0, \neg(\exists \delta > 0, \forall x \in B_\delta(a), f(x) \in B_\varepsilon(l))$$

$$= \exists \varepsilon > 0, \forall \delta > 0, \neg(\forall x \in B_\delta(a), f(x) \in B_\varepsilon(l))$$

$$= \exists \varepsilon > 0, \forall \delta > 0, \exists x \in B_\delta(a), f(x) \notin B_\varepsilon(l).$$

Maybe then I could have proved it.

[This epilogue was just culture. You do not need to know about ε, δ for MTH 306.]

Functions

Last time we discussed (logical) statements. Recall that a statement is any sentence that has a definite truth value (T or F)

Remark (Use-Mention Distinction): When I want to refer to a statement I will put quotes around it. If I don't put quotes I am asserting that the statement is true.

E.g. I am just referring to these

$$\text{“}1+2=5\text{”} \underset{\uparrow}{=} \text{“}1+7=3\text{”} \quad (=F)$$

I am asserting that this is true

We won't be too fussy about this. For example, I won't bother to write this:

$$\text{“ “}1+2=5\text{”} = \text{“}1+7=3\text{” ”} = T$$

(because where would this madness stop?)

Remark: Formal logic is a dangerous black hole. I will try to step lightly around it.

Recall that we applied logic to set theory.

Given sets $A, B \subseteq U$ we showed that

$$\begin{aligned} \text{“}A \not\subseteq B\text{”} &= \text{“}\exists x \in U,\ x \in A \text{ and } x \notin B\text{”} \\ &= \text{“}\exists x \in U,\ x \in A \cap B^c\text{”} \\ &= \text{“}A \cap B^c \neq \emptyset\text{”} \end{aligned}$$

and hence

$$\begin{aligned} \text{“}A \subseteq B\text{”} &= \neg\,\text{“}A \not\subseteq B\text{”} \\ &= \neg\,\text{“}A \cap B^c \neq \emptyset\text{”} \quad \text{(from above)} \\ &= \text{“}A \cap B^c = \emptyset\text{”} \end{aligned}$$

We will see later that there are other equivalent ways to say this.

e.g.
$$\begin{aligned} \text{“}A \subseteq B\text{”} &= \text{“}A \cap B = A\text{”} \\ &= \text{“}A \cup B = B\text{”} \\ &\ \ \vdots \\ &\ \ \text{etc.} \end{aligned}$$

Q: In the definition of set intersection

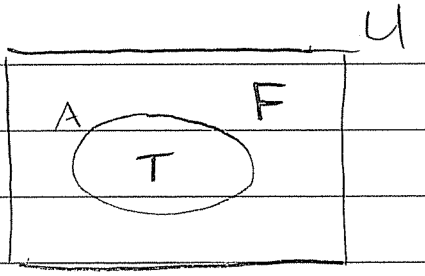
$$A \cap B := \{ x \in U : x \in A \text{ AND } x \in B \},$$

what does "AND" mean?

Note that "$x \in A$", "$x \in B$", and "$x \in A$ AND $x \in B$" are all either T or F. How are the three truth values related?

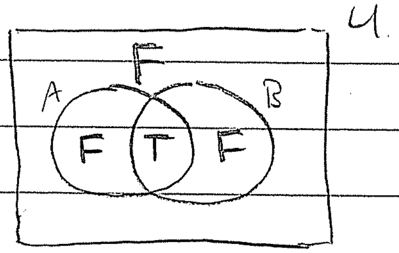
$$\left.\begin{array}{l} T \text{ AND } T = ? \\ T \text{ AND } F = ? \\ F \text{ AND } T = ? \\ F \text{ AND } F = ? \end{array}\right\} \text{we need to define these.}$$

We can look at Venn diagrams to see the answer. Given $A \subseteq U$ we can visualize the statement "$x \in A$" as



"$x \in A$"

So given two sets $A, B \subseteq U$ we can visualize the statement "$x \in A \cap B$"



"$x \in A \cap B$"

Since "$x \in A \cap B$" := "$x \in A$ AND $x \in B$" suggests how to define AND.

Definition: Given statements $P, Q \in \{T, F\}$ we define P AND Q as follows

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

Think : P = "$x \in A$"
Q = "$x \in B$"
P AND Q = "$x \in A$ AND $x \in B$".

Notation: Sometimes we will write

$$\text{"P AND Q"} = \text{"} P \wedge Q \text{"}$$

to emphasize the connection with set intersection. This is called logical conjunction.

//

Similarly, we will define OR.

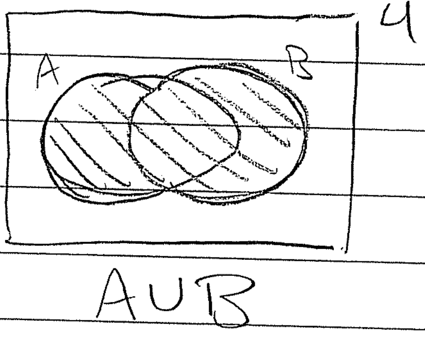
Recall the definition

$$A \cup B := \{ x \in U : x \in A \text{ OR } x \in B \}$$

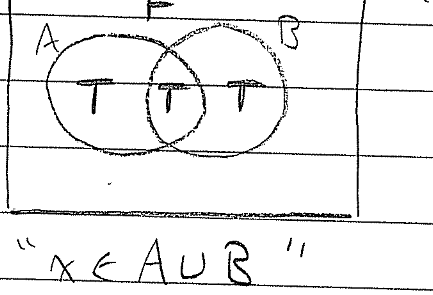
In other words, for all $x \in U$ we have

$$\text{"} x \in A \cup B \text{"} = \text{"} x \in A \text{ OR } x \in B \text{"}.$$

Look at the Venn diagram



$A \cup B$



"$x \in A \cup B$"

This suggests the following definition:
Given $P, Q \in \{T, F\}$ we define P OR Q as follows.

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

Think: $P = $ "$x \in A$"
$Q = $ "$x \in B$"
P OR Q = "$x \in A \cup B$"

Note that this is the inclusive or. When we mean exclusive or we will write XOR.

P	Q	P XOR Q
T	T	F
T	F	T
F	T	T
F	F	F

"P XOR Q" means "P or Q but not both."

Notation: We write "P OR Q" = "$P \vee Q$" and call this logical disjunction.

The set operations $\cap, \cup, {}^c$ are completely analogous to the logical operations $\wedge, \vee, \neg$. But what are they really? To explain this we need one final abstract concept: the concept of a function.

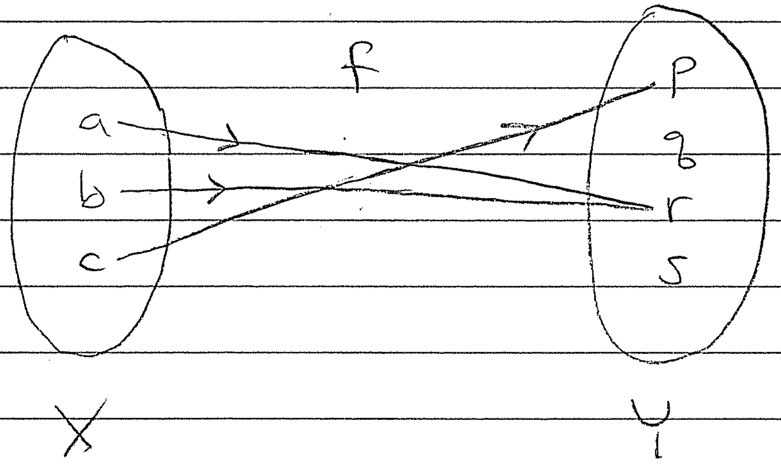
Definition: Let X and Y be sets. A function $f : X \to Y$ is a set of arrows $x \to y$ where $x \in X$ and $y \in Y$, satisfying two rules.

F1 For all $x \in X$, there is at most one $y \in Y$ such that $x \to y$.

F2 For all $x \in X$, there is at least one $y \in Y$ such that $x \to y$.

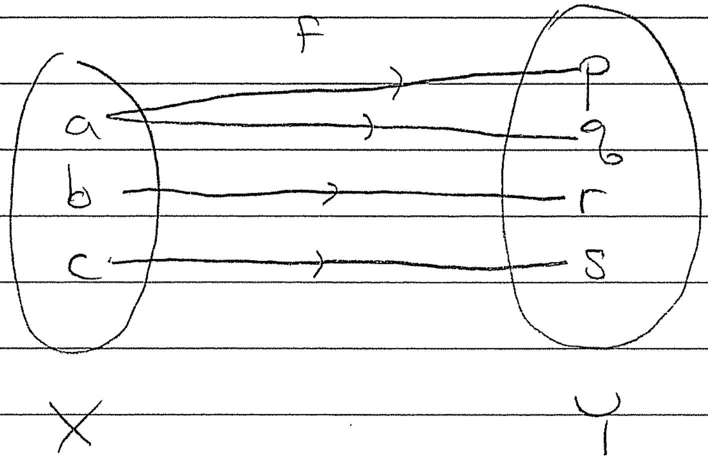
[To paraphrase we say: For all $x \in X$ there is exactly one $y \in Y$ such that $x \to y$. Since this y is unique we can give it a name. We will call it $f(x)$.]

Example: This is a function $f: X \to Y$.



We have $f(a) = r$, $f(b) = r$, $f(c) = p$.

Non-Example: This is not a function



because it violates rule $\boxed{F1}$

Problem: $f(a) = p$ or $f(a) = q$?

It can't be both!

On HW 2 you will investigate two *optional* properties of functions $f: X \to Y$.

F3 For all $y \in Y$ there is at *most* one $x \in X$ such that $x \to y$.

F4 For all $y \in Y$ there is at *least* one $x \in X$ such that $x \to y$.

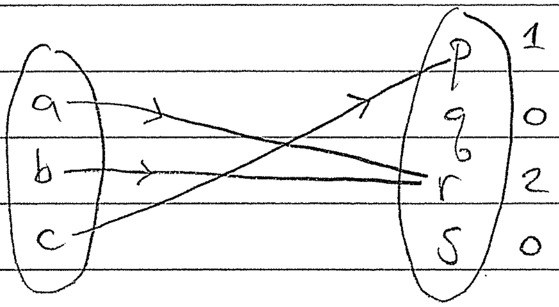
If F3 holds we say f is *injective* (or "one-to-one"), if F4 holds we say f is *surjective* (or "onto"), if F3 & F4 both hold we say f is *bijective* (or a "one-to-one" correspondence).

If f is *bijective*, note that the set of *reversed* arrows satisfies the rules F1 & F2 so it defines a function from Y to X. We call this function

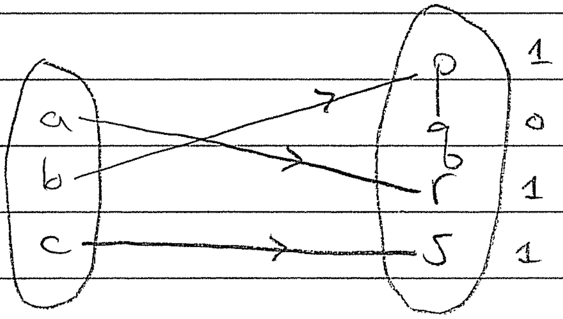
$$f^{-1} : Y \to X$$

the *inverse* of f.

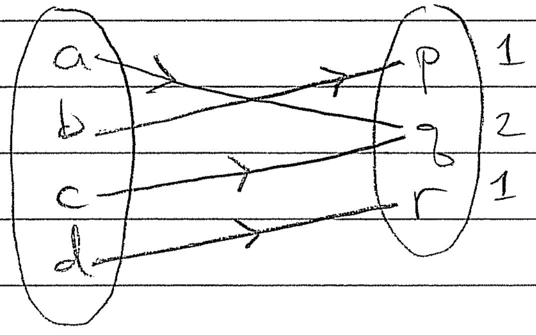
Examples: These are all functions.



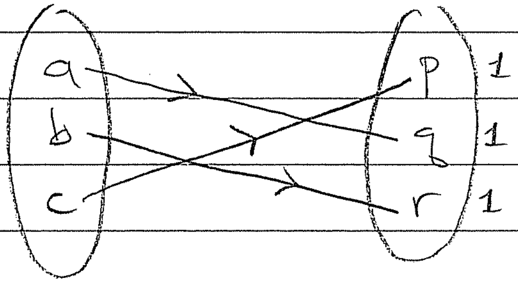
injective ✗
surjective X



injective ✓
surjective ✗



injective ✗
surjective ✓



injective ✓
surjective ✓
hence bijective.

The last function is invertible. The others are not.

Thinking Problem :

Let $f: X \to Y$ be a function and for each $y \in Y$ consider the number

$$d(y) := \# \{ x \in X : f(x) = y \}.$$

What do you get if you add up these numbers?

$$\sum_{y \in Y} d(y) = ?$$

(Try it on the previons examples.
This is very relevant to HW 2.)

Boolean Functions

We defined abstract functions $f: X \to Y$ but how does this agree with your previous experience?

Example: If X and Y are sets of numbers then we can define functions using "algebraic formulas".

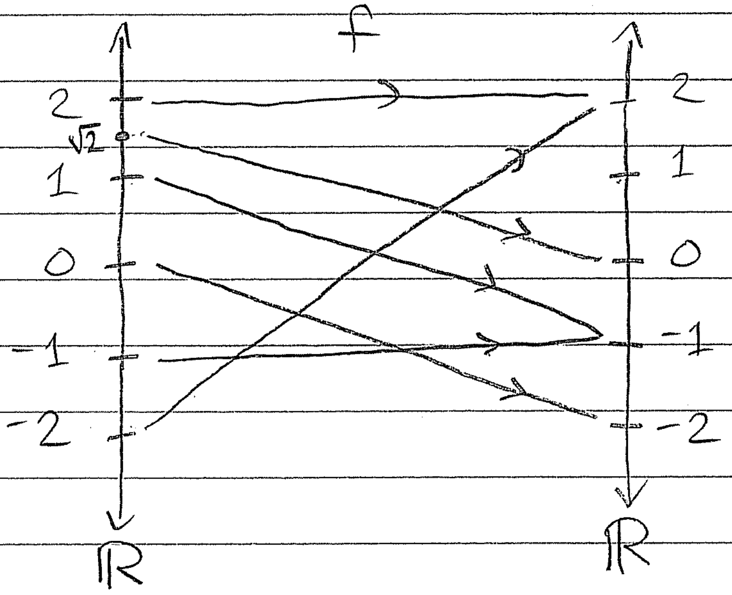
Recall the set of real numbers:

$\mathbb{R}$ = The set of numbers that have decimal expansions.

[Remark: It's difficult to define $\mathbb{R}$ formally, so we won't. See math 433 or 533 for this.]

The formula $f(x) = x^2 - 2$ defines a function $f : \mathbb{R} \to \mathbb{R}$.

How might we draw this function?



injective?
surjective?

There are too many arrows! I can't draw them all. Maybe there is a better way to represent this function?

We need another concept.

Definition: An ordered pair is a "set" with two elements in which order does matter. We will write it like this

$$\big(\underset{\substack{\nearrow \\ \text{1st element}}}{x}\ ,\ \underset{\substack{\nwarrow \\ \text{2nd element}}}{y}\big)$$

[Remark: If you really want to express (x,y) using set language you can say something like

$$(x,y) := \{x, \{y\}\}.$$

But we won't bother with this extreme level of formality.]

Then given two sets A and B we define their Cartesian product

$$A \times B := \{(x,y) : x \in A \text{ and } y \in B\}.$$

Example: Let $A = \{a, b\}$ and $B = \{p, q, r\}$. Then the Cartesian product is

$$A \times B = \{ (a,p), (a,q), (a,r), (b,p), (b,q), (b,r) \}$$

See the rectangle?

	p	q	r
a	(a,p)	(a,q)	(a,r)
b	(b,p)	(b,q)	(b,r)

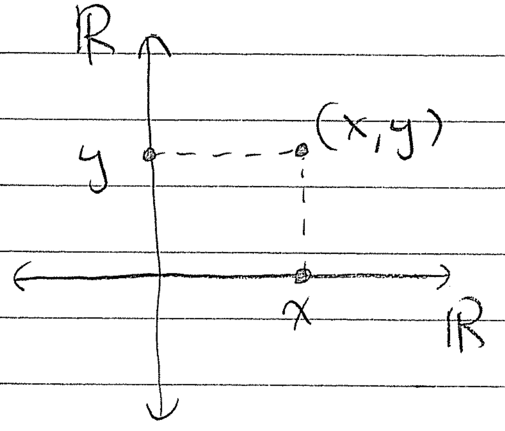
If A and B are finite sets then we have

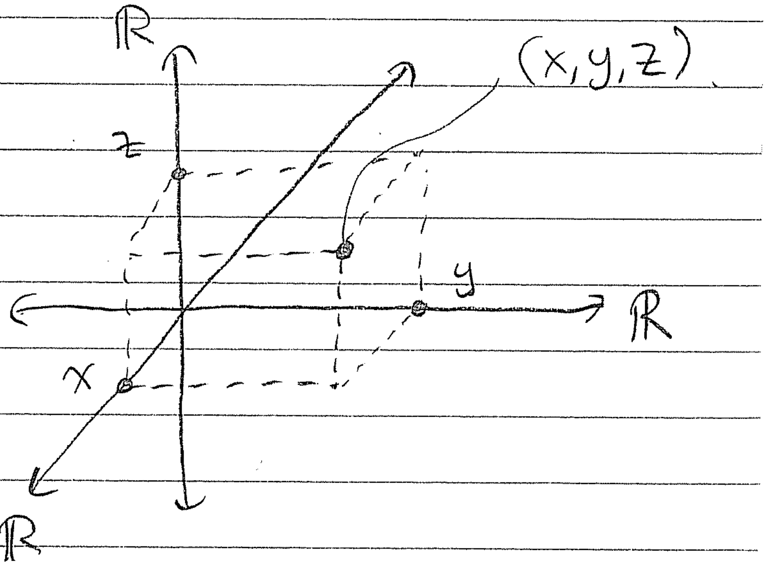
$$\#(A \times B) = \#A \times \#B.$$

(This explains the notation.) ///

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

A: In 1637 René Descartes had the revolutionary idea that the sets $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ and $\mathbb{R}^3 := \mathbb{R}^2 \times \mathbb{R} = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ could be used to represent 2D and 3D space.





[Wait! Did we define "ordered triples"? You can just say

$$(x,y,z) := ((x,y),z) \text{ or } (x,(y,z)).$$

It doesn't matter which. We say that the Cartesian product is "associative":

not really the same, but there is a natural bijection between them.

$$(A \times B) \times C = A \times (B \times C)$$

We'll just call this set $A \times B \times C$.]

Now we can define the "graph" of a function $f : A \to B$. To each arrow $x \longrightarrow f(x)$ we associate the ordered pair $(x, f(x)) \in A \times B$.

Definition: Let $f : A \to B$ be a function. Its graph is the following subset of $A \times B$

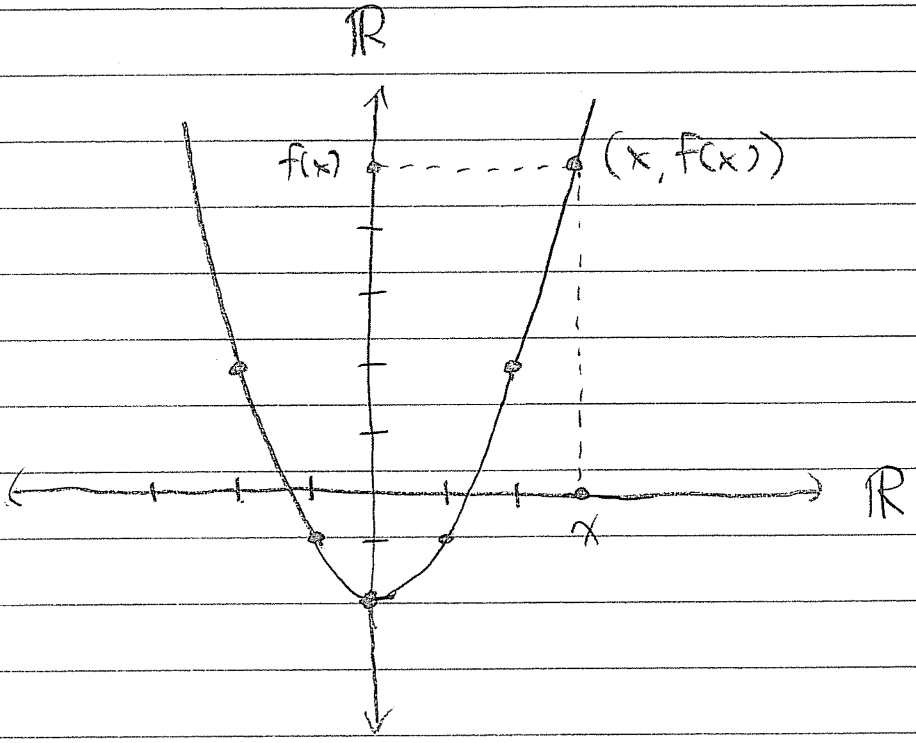
$$\{(x, f(x)) : x \in A\} \subseteq A \times B.$$

If the set $A \times B$ can be visualized, then this allows us to visualize functions $f: A \to B$ as certain subsets of $A \times B$.

Example: Recall the function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 2$. 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 $\mathbb{R}^2$.



This also allows us to rephrase the defining properties of a function.

Consider any subset $X \subseteq \mathbb{R}^2$. We say that X is a function if it satisfies two properties

F1 Every vertical line intersects X at most once

F2 Every vertical line intersects X at least once.

Additionally, we say X is injective if

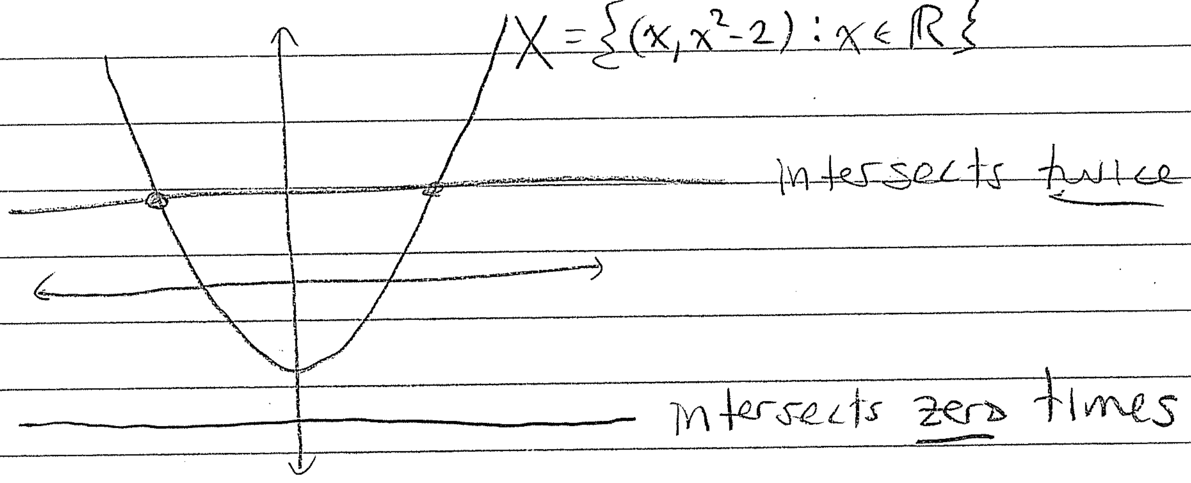
F3 Every horizontal line intersects X at most once.

We say X is surjective if

F4 Every horizontal line intersects X at least once.

Example: $f(x) = x^2 - 2$ is NOT injective and NOT surjective.

↓



We say X is bijective/invertible if it intersects each horizontal line exactly once, in which case the inverse function is obtained by reflecting across the line $y = x$.

Functions in Logic :

We also use the language of functions in the study of logic.

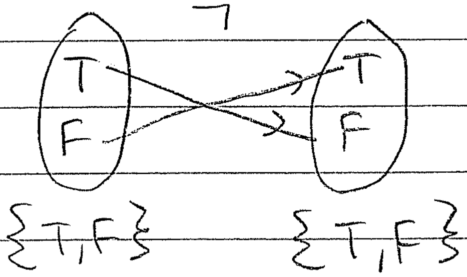
Definition: A Boolean function is any function of the form

$$f : \{T, F\}^n \to \{T, F\},$$

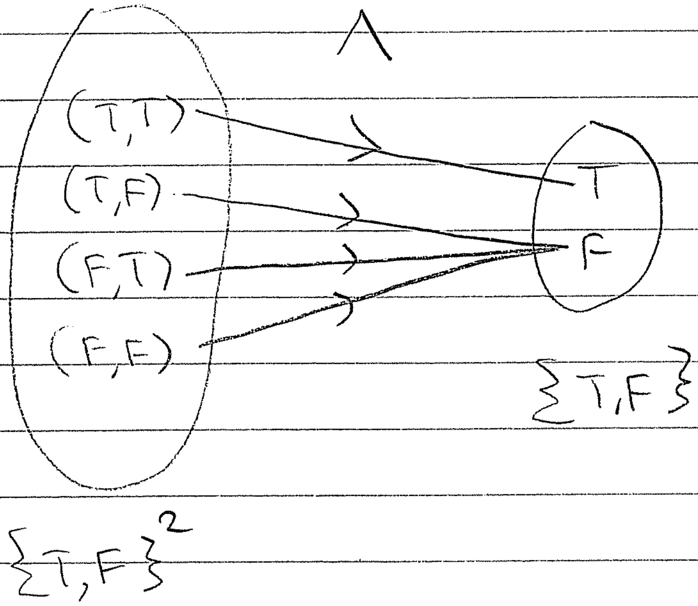
where $\{T,F\}^n$ is the set of "ordered n-tuples" of T's and F's.

We know three important examples:

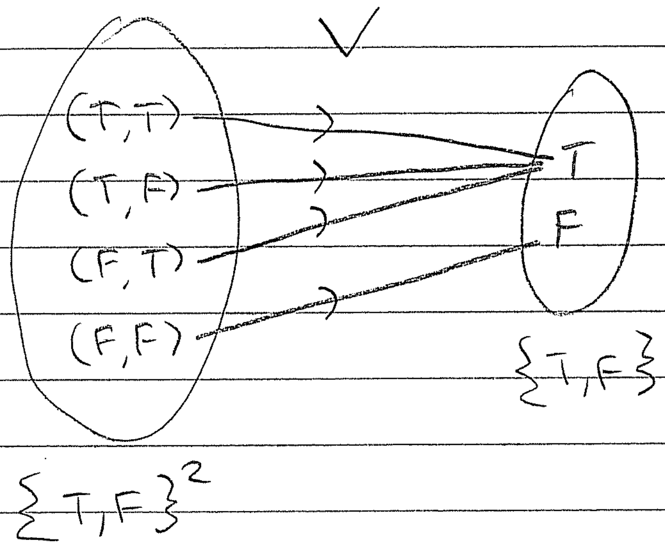
- $\neg : \{T,F\} \rightarrow \{T,F\}$



- $\wedge : \{T,F\}^2 \rightarrow \{T,F\}$



- $\vee : \{T,F\}^2 \to \{T,F\}$



What do the _graphs_ of these functions look like?

The graph of $\wedge : \{T,F\}^2 \to \{T,F\}$ is the _set_

$$\{((P,Q), P \wedge Q) : (P,Q) \in \{T,F\}^2\}$$

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

which is a subset of

$$\{T,F\}^2 \times \{T,F\} \quad \left(= \{T,F\}^3\right)$$

we might as well just write it like this

Since the graph is just a finite set we will prefer to write it as a table:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

A truth table is just the graph of a Boolean function

Thinking Problem:

How many different Boolean functions are there in n variables?

$$f : \{T,F\}^n \longrightarrow \{T,F\}$$

Abstract "Boolean Algebra"

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

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

disjunction $\vee : B \times B \to B$
conjunction $\wedge : B \times B \to B$
negation $\neg : B \to B$

and two special elements

$0 \in B$, $1 \in B$ 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 : $\forall\, a, b, c \in B$,

$$\boxed{\begin{aligned} a \wedge b &= b \wedge a \\ a \vee b &= b \vee a \end{aligned}}$$

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

$$\boxed{\begin{aligned} a \vee 0 &= a \\ a \wedge 1 &= a \end{aligned}}$$

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

$$\boxed{\begin{aligned} a \vee \neg a &= 1 \\ a \wedge \neg a &= 0 \end{aligned}}$$

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

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

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)

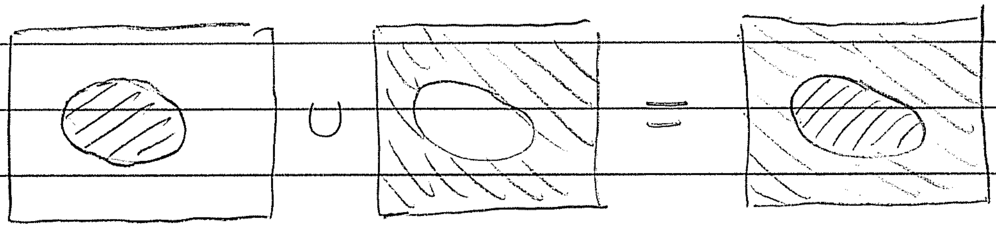
and special elements

$0 = \emptyset$ (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.

↓

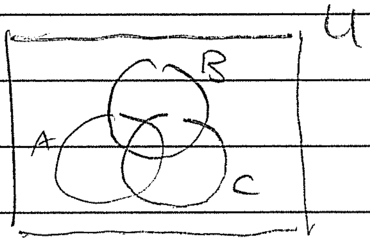
For all $S \in \wp(U)$ (i.e. $S \subseteq U$) do we have $S \cup S^c = U$?

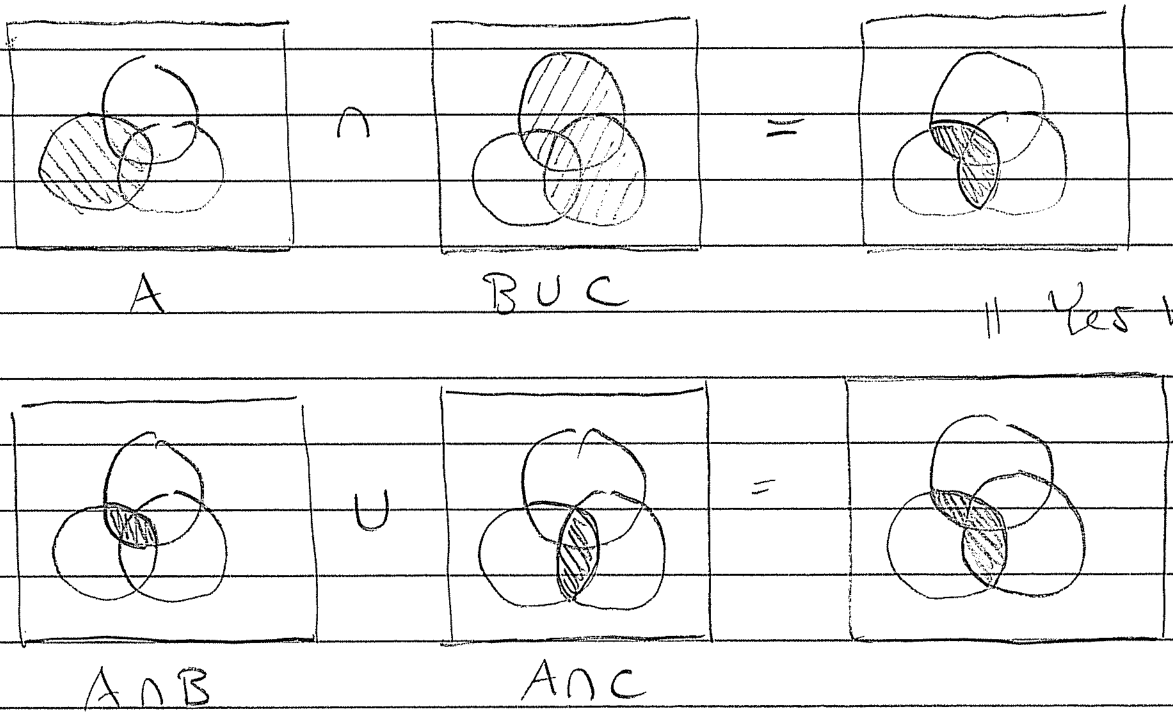


Yes ✓

For all $A, B, C \in \wp(U)$ do we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$?

Consider





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

$$\begin{aligned} \vee &= \text{OR} \\ \wedge &= \text{AND} \\ \neg &= \text{NOT} \end{aligned}$$

and special elements

$$\begin{aligned} 0 &= F \\ 1 &= T \end{aligned}$$

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	$\boxed{F}$
F	T	$\boxed{F}$

✓

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 ✓

3 Examples of Boolean Algebra:
Set Theory
Logic
Binary Arithmetic

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?

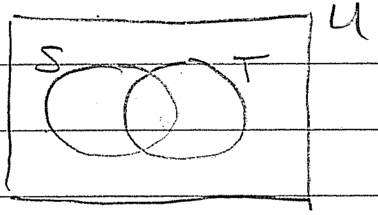
Example 1: The Boolean algebra of sets.

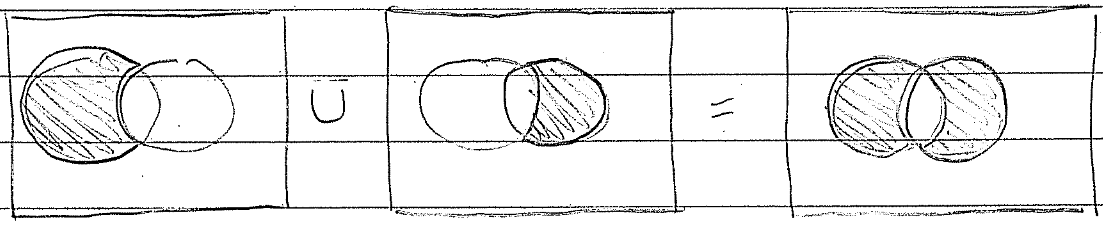
$$(\mathcal{P}(\mathcal{U}), \cup, \cap, {}^c, \emptyset, \mathcal{U})$$

In this language we have

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

Picture: Consider





$S \cap T^c$ $\qquad$ $S^c \cap T$ $\qquad$ $S \oplus T$

The set $S \oplus T$ is sometimes called the <u>sym</u>metric <u>dif</u>ference 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

$$\begin{aligned} P \oplus Q &= P \not\equiv Q \\ &= \neg(P \equiv Q) \end{aligned}$$

(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 operatos 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.

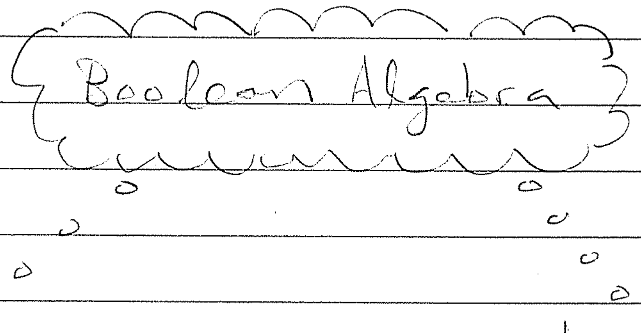
Disjunctive Normal Form

We <u>defined</u> 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 <u>two</u> main interpre<u>ta</u>tions in mind:



Set Theory | Logic

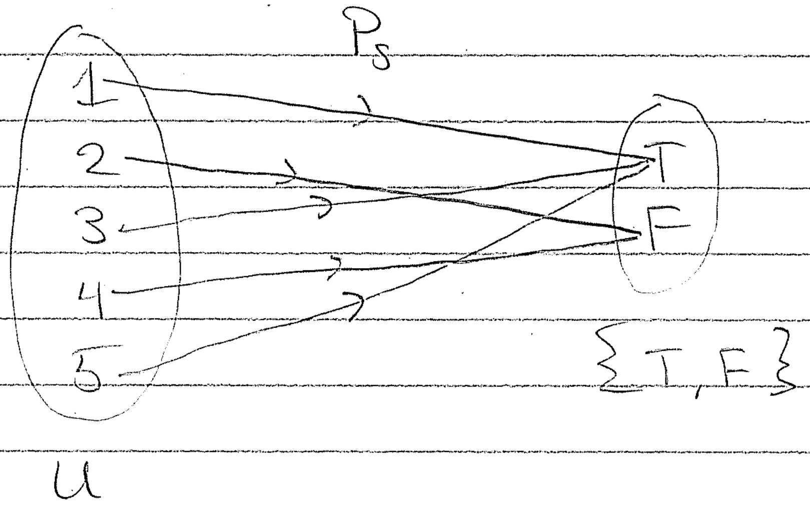
$(\mathcal{P}(U), \cup, \cap, {}^c, \emptyset, U)$ $\quad$ $(\{T,F\}, \text{OR}, \text{AND}, \text{NOT}, F, T)$

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 $P : \mathcal{U} \to \{T, F\}$ can we define a subset of $\mathcal{U}$?

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

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

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

$$\begin{array}{ccc} \text{subsets of } \mathcal{U} & \longleftrightarrow & \text{functions } \mathcal{U} \to \{T, F\} \\ S & \longmapsto & P_S \\ \mathcal{U}_P & \longleftarrow\!\shortmid & P \end{array}$$

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

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

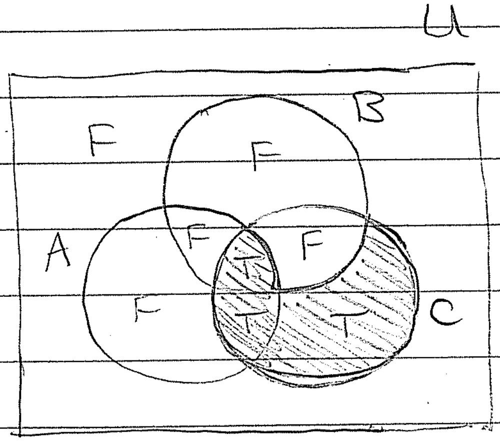
$$S \cup T := \{ x \in \mathcal{U} : x \in S \text{ OR } x \in T \}$$

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

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

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

Example: Let $A, B, C \subseteq U$ with corresponding statements $P, P, P : U \to \{T, F\}$. 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 any Boolean function

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

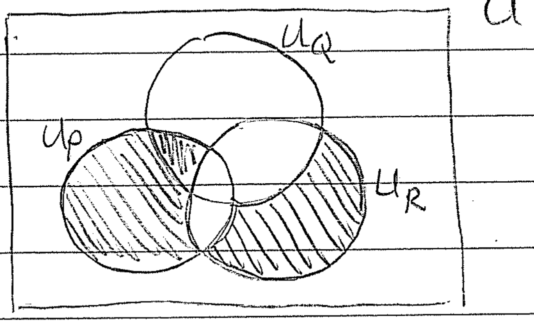
"a Boolean function of 3 variables."

in terms of the basic functions $\vee, \wedge, \neg$.

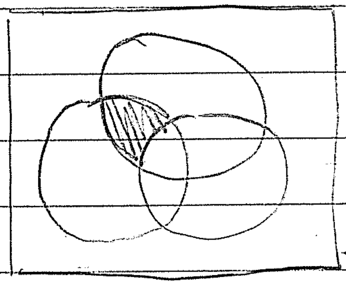
Example Problem: Express the following function $\varphi(P, Q, R)$ in terms of $\vee, \wedge, \neg$.

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

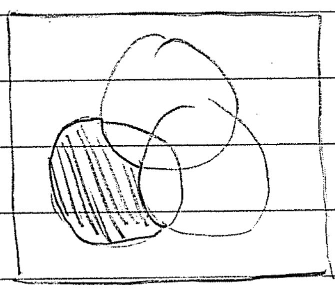
Solution: Think of it as a set.



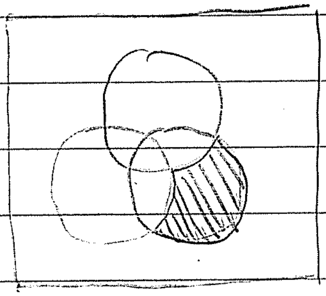
Break the set into a union of small pieces.



$\cup$



$\cup$



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

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 φ.

///

Two Remarks:

1. We showed that every 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 <u>only</u> 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.

$\circledast$ $\quad P \uparrow P = \neg (P \wedge P)$ $\qquad$ definition

$\qquad\qquad = \neg P$ $\qquad$ $\textcircled{6}$

$(P \uparrow P) \uparrow (Q \uparrow Q) = \neg P \uparrow \neg Q$ $\qquad$ $\circledast$

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

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

$\qquad = P \vee Q.$

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

$$\begin{aligned} &= \neg (P \uparrow Q) && \circledast \\ &= \neg\neg (P \wedge Q) && \text{definition} \\ &= P \wedge Q \, . \end{aligned}$$

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 ↑. It is called NAND flash memory. There is also NOR flash memory, based on "Peirce's arrow"

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