9/10/14

HW 1 due NOW
HW 2 will be due Mon Sept 22
Exam 1 will be Wed Sept 24 IN CLASS.

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 hardware</u>.

This is the science of <u>binary 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 Algebra</u>.

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

We begin with set theory.

Definition: A <u>set</u> 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

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

The set of integers

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

The set of rational numbers

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

The set of real numbers

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

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

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

"<u>if</u> $x \in A$ <u>then</u> $x \in B$".

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

$$\{1,2,3\}, \quad \{1,2\}, \quad \{1\}, \quad \emptyset.$$
$$\{1,3\}, \quad \{2\},$$
$$\{2,3\}, \quad \{3\},$$

<u>Remark</u>: For <u>any</u> 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

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

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

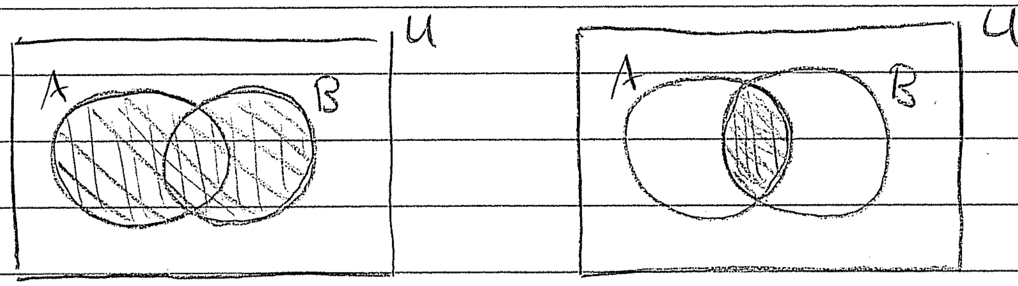
We define the union

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

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":

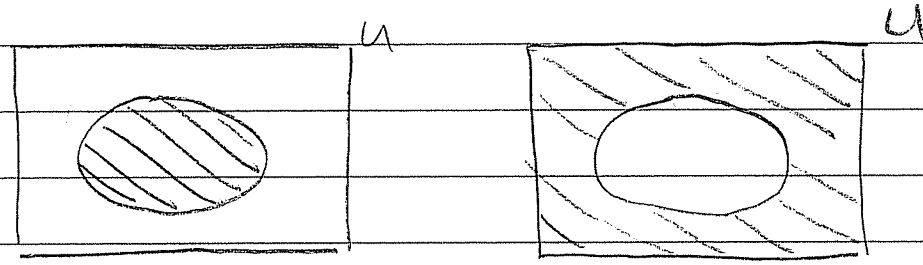


$A \cup B$ $\quad\quad$ $A \cap B$

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

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

Picture



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

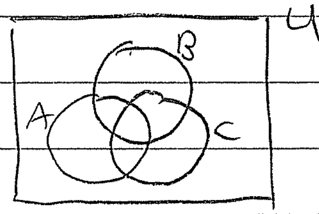
(2) $A \cap B = B \cap A$
$A \cup B = B \cup A$

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

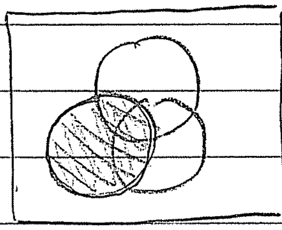
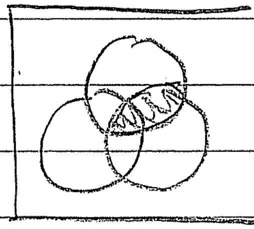
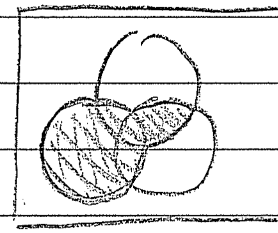
(4) $A \cup A^c = \mathcal{U}$
$A \cap A^c = \emptyset$

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

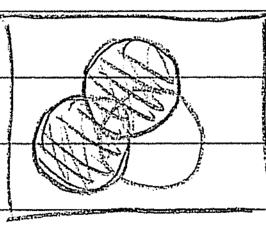
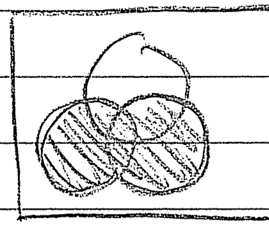
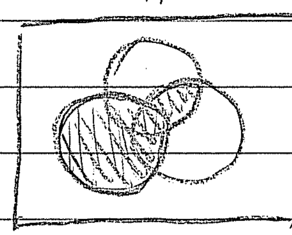
Those are <u>mostly</u> obvious, but we should probably check property (5).

Consider 

A $\quad$ $B \cap C$ $\quad$ $A \cup (B \cap C)$

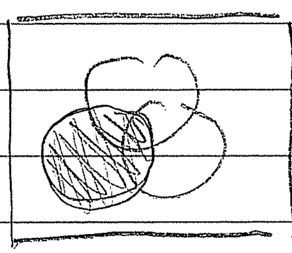
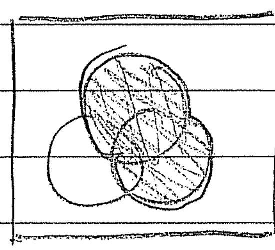
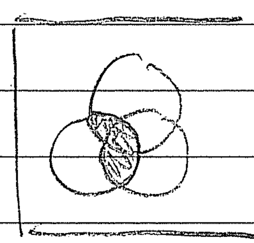
 $\cup$  $=$  ✓

$\|$

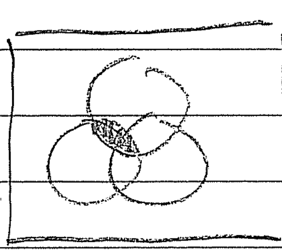
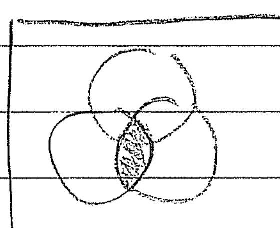
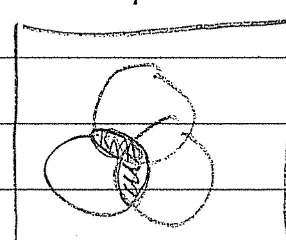
 $\cap$  $=$ 

$A \cup B$ $\quad$ $A \cup C$ $\quad$ $(A \cup B) \cap (A \cup C)$

A $\quad$ $B \cup C$ $\quad$ $A \cap (B \cup C)$

 $\cap$  $=$  ✓

$\|$

 $\cup$  $=$ 

$A \cap B$ $\quad$ $A \cap C$ $\quad$ $(A \cap B) \cup (A \cap C)$

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 "$A \nsubseteq B$" ?

9/15/14

HW 2 due next Mon Sept 22
Exam 1 next Wed Sept 24

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

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

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

$\forall$ universal quantifier

$\exists$ 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

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

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

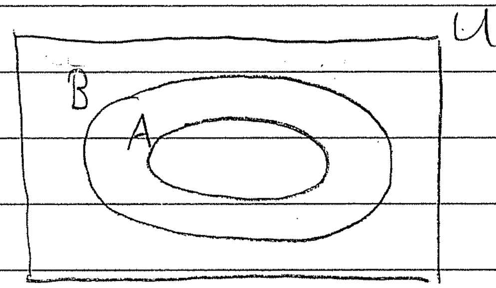
///

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:

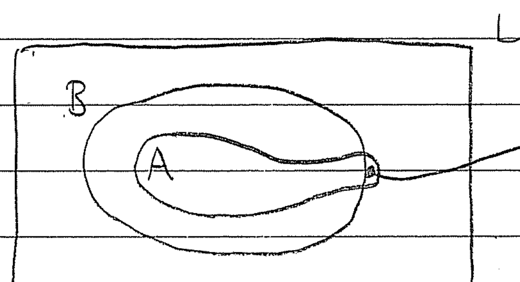


For convenience we can define

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

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

$$\text{"}A \not\subseteq B\text{"} = \neg \text{"}\forall x \in A,\ x \in B\text{"}$$
$$= \text{"}\exists x \in A,\ \neg\, x \in B\text{"}$$
$$= \text{"}\exists x \in A,\ x \notin B\text{"}.$$

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 U.

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

"A <u>union</u> B"

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

"A <u>intersect</u> B"

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

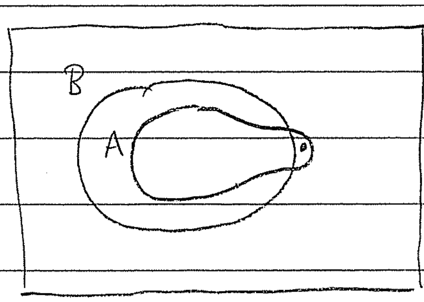
"A <u>complement</u>"

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

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:

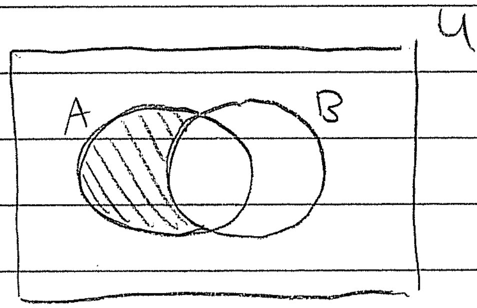
$$\boxed{\text{“}A \subseteq B\text{”} = \text{“}A \cap B^c = \emptyset\text{”}}$$

That might be useful later.

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

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

<u>Picture:</u>



$A - B$

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

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

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

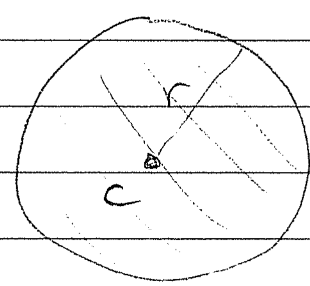
Epilogue

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:

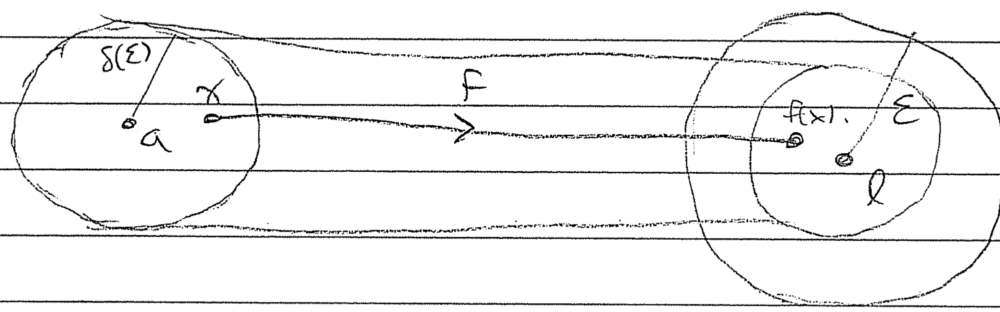


Let f be a function between spaces then we say "the limit of $f(x)$ as x approaches a equals l"

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

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

$\Big\downarrow$

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 <u>not</u> need to know about ε, δ for MTH 306.]

9/17/14

HW 2 due Monday beginning of class.
Review Session Monday
Exam 1 Wednesday in class

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

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

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 $A, B \subseteq \mathcal{U}$ we showed that

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

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. $$\begin{aligned} \text{“} A \subseteq B \text{''} &= \text{“} A \cap B = A \text{''} \\ &= \text{“} A \cup B = B \text{''} \\ &\ \vdots \end{aligned}$$

etc.

Q: In the definition of set intersection

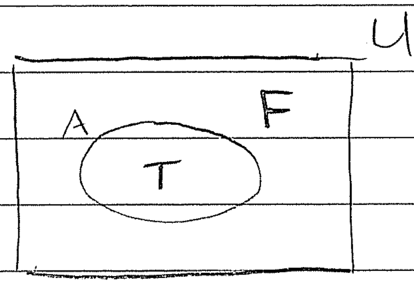
$$A \cap B := \{ x \in U : x \in A \text{ AND } x \in B \},$$

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?

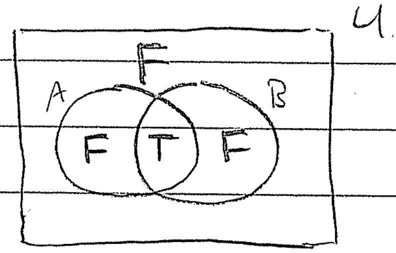
$$\left.\begin{array}{l} T \text{ AND } T = ? \\ T \text{ AND } F = ? \\ F \text{ AND } T = ? \\ F \text{ AND } F = ? \end{array}\right\} \text{ we need to define these.}$$

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

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

to emphasize the connection with set intersection. This is called <u>logical conjunction</u>.

Similarly, we will define OR.

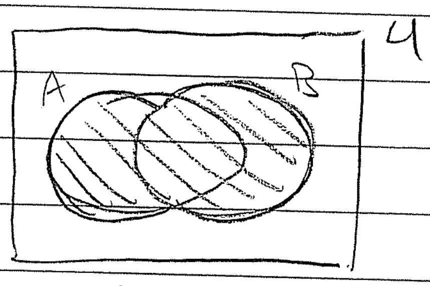
Recall the definition

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

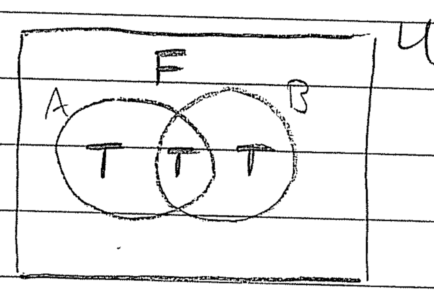
In other words, for all $x \in U$ we have

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

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 <u>inclusive</u> or. When we mean ex<u>clu</u>sive 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.

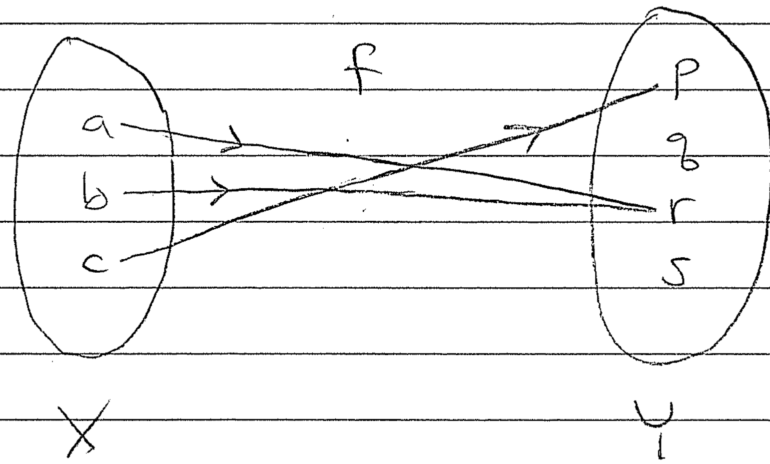
Definition: Let X and Y be sets. A function $f: X \to Y$ is a set of arrows $x \to y$ where $x \in X$ and $y \in Y$, satisfying two rules.

(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 $x \to y$.

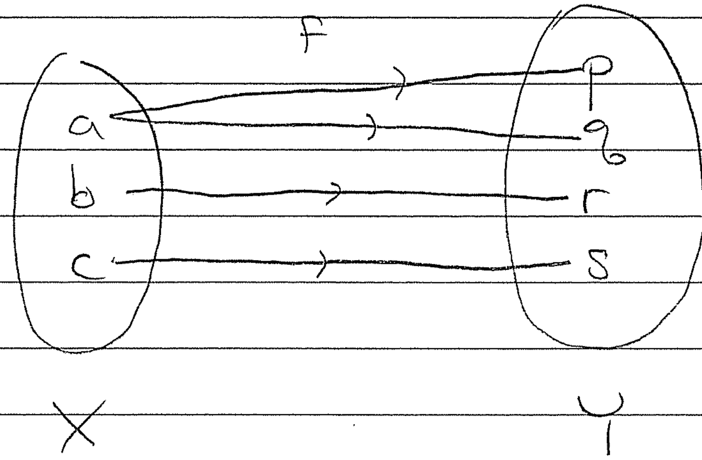
[To paraphrase we say: For all $x \in X$ there is exactly one $y \in Y$ such that $x \to y$. Since this y is unique we can give it a name. We will call it $f(x)$.]

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 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 $x \to y$.

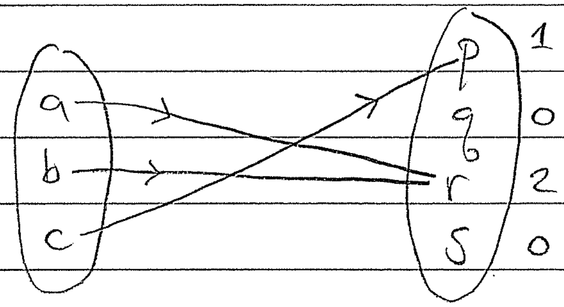
If (F3) holds we say f is injective (or "one-to-one"), if (F4) holds we say f is surjective (or "onto"), if (F3) & (F4) both hold we say f is bijective (or a "one-to-one" correspondence).

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

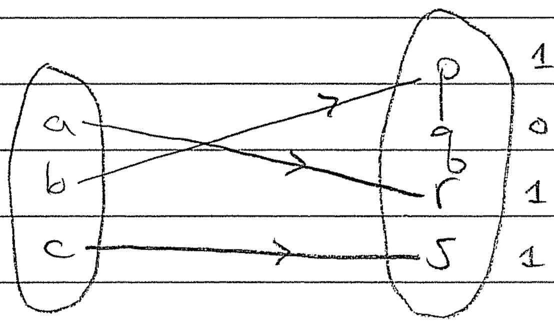
$$f^{-1} : Y \to X$$

the inverse of f.

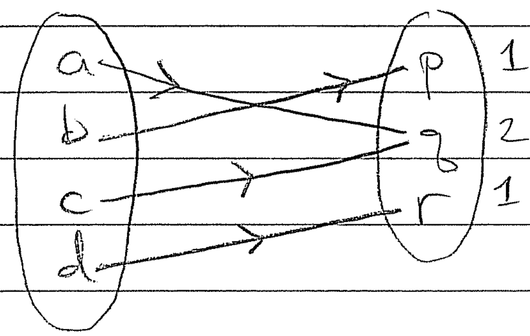
Examples: These are all functions.



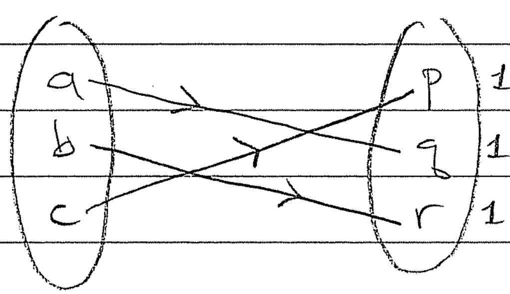
injective ✗
surjective ✓



injective ✓
surjective ✗



injective ✗
surjective ✓



injective ✓
surjective ✓
hence <u>bijective</u>.

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 previous examples. This is very relevant to HW 2.)

9/22/14

HW 2 due now.

Exam 1 on Wednesday

Today: Review for Exam 1

Topics for Exam 1:

- Solving simple recurrence equations
- Sums of p^{th} powers
- Proving formulas by induction
- Basic properties of
  - sets
  - logical statements
  - functions
- Set operators $\cap$, $\cup$, ^{c}
- Logical operators $\vee$, $\wedge$, $\neg$
- Venn diagrams and truth tables

Review: Recall that we define

$$S_p(n) := 1^p + 2^p + 3^p + \cdots + n^p = \sum_{k=1}^{n} k^p$$

We know some "closed formulas" for these:

$\downarrow$

- $S_0(n) = n$
- $S_1(n) = \dfrac{n(n+1)}{2}$
- $S_2(n) = \dfrac{n(n+1)(2n+1)}{6}$
- $S_3(n) = \dfrac{n^2(n+1)^2}{4}$

These formulas might not be easy to guess, but once we have the formula it is easy to prove by induction.

__Example__: Prove by induction that

$$S_2(n) = \frac{n(n+1)(2n+1)}{6} \quad \text{for } n \geq 1.$$

__Proof__: First we check the base case. The formula is correct when $n=1$ because $S_2(1) = 1^2 = 1$ and

$$\frac{1(1+1)(2\cdot 1+1)}{6} = \frac{1\cdot 2\cdot 3}{6} = 1 \quad \checkmark$$

Now we fix an arbitrary $n \geq 1$ and <u>assume</u> that

$$S_2(n) = \frac{n(n+1)(2n+1)}{6}.$$

In this hypothetical case we want to show that we must also have

$$S_n(n+1) = \frac{(n+1)\left((n+1)+1\right)\left(2(n+1)+1\right)}{6}$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}.$$

To show this we note that

$$S_n(n+1) = \left(1^2 + \cdots + n^2\right) + (n+1)^2$$

$$= S_2(n) + (n+1)^2$$

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

$$= (n+1)\left[\frac{n(2n+1)}{6} + (n+1)\right]$$

$$= \frac{(n+1)}{6}\left[n(2n+1) + 6(n+1)\right]$$

$$= \frac{(n+1)}{6}\left[2n^2 + n + 6n + 6\right]$$

$$= \frac{(n+1)}{6}\left[2n^2 + 7n + 6\right]$$

$$= \frac{(n+1)(n+2)(2n+3)}{6} \quad \checkmark$$

We are done by induction.

[(1) The formula starts out true.
(2) <u>If</u> the formula is true at some point, <u>then</u> it remains true after that.]

Problem: Solve the recurrence

$$\boxed{\begin{array}{l} \bullet\ f_0 = 1 \\ \bullet\ f_n = f_{n-1} + n^2 + n \quad \text{for } n \geq 1 \end{array}}$$

Solution: We have.

$$f_0 = 1$$
$$f_1 = 1 + 1^2 + 1$$
$$f_2 = 1 + 1^2 + 1 + 2^2 + 2$$

$f_3 = 1 + 1^2 + 1 + 2^2 + 2 + 3^2 + 3$

$\vdots$

$f_n = 1 + 1^2 + 1 + 2^2 + 2 + 3^2 + 3 + \cdots + n^2 + n$

$= 1 + (1 + 2 + 3 + \cdots + n) + (1^2 + 2^2 + 3^2 + \cdots + n^2)$

$= 1 + \frac{n(n+1)}{2} + \frac{n(n+1)(2n+1)}{6}$

$= 1 + \frac{1}{2}n^2 + \frac{1}{2}n + \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$

$= \frac{1}{3}n^3 + n^2 + \frac{2}{3}n + 1$

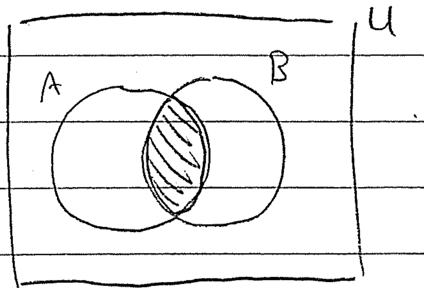
Given sets $A, B \subseteq U$ recall the Boolean set operations

$A \cap B := \{ x \in U : x \in A \overset{\text{"AND"}}{\wedge} x \in B \}$

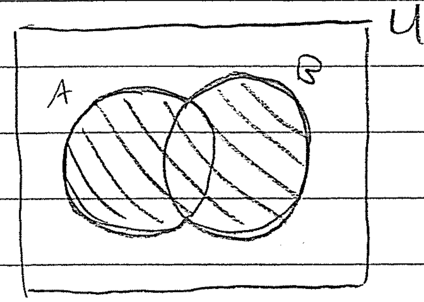
$A \cup B := \{ x \in U : x \in A \overset{\text{"OR"}}{\vee} x \in B \}$

$A^c := \{ x \in U : \overset{\text{"NOT"}}{\neg} x \in A \}$

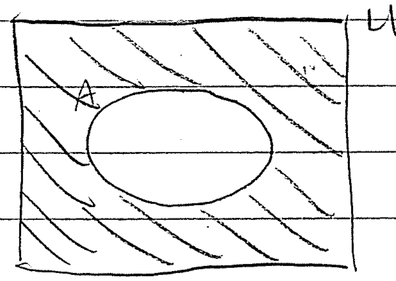
We can draw these sets with Venn diagrams



$A \cap B$



$A \cup B$



A^c

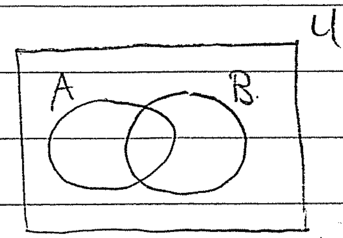
We can use Venn diagrams to prove basic properties of $\cap$, $\cup$, ^{c}.

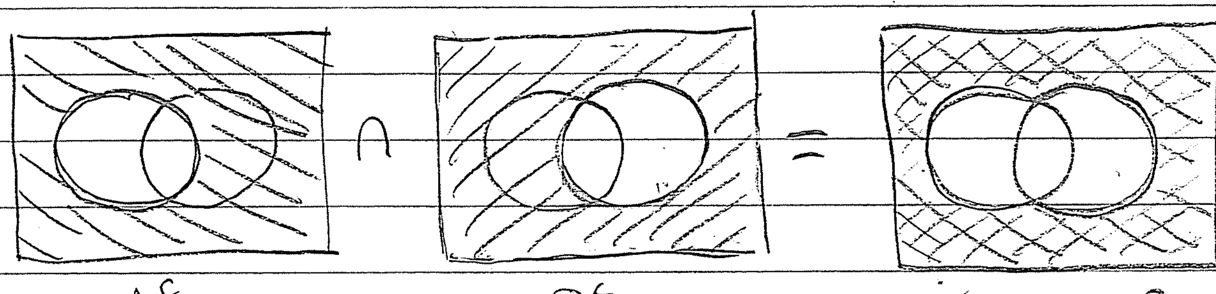
<u>Example</u>: Use Venn diagrams to show that for all sets $A, B \subseteq U$ we have

$$(A \cup B)^c = A^c \cap B^c.$$

[Remark: This is called

"de Morgan's identity"]

Proof: consider 



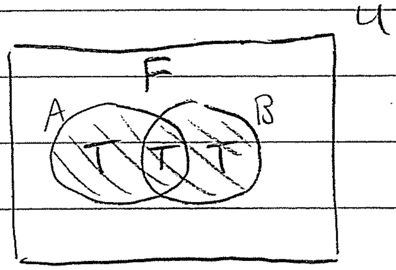
A^c $\qquad$ B^c $\qquad$ $(A \cup B)^c$

We can also think about Venn diagrams as truth tables.

Let P = "$x \in A$" and Q = "$x \in B$", so that

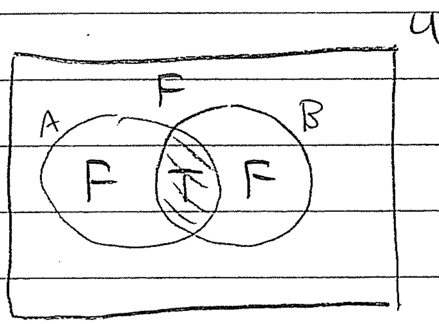
$P \wedge Q$ = "$x \in A$ AND $x \in B$" = "$x \in A \cap B$"
$P \vee Q$ = "$x \in A$ OR $x \in B$" = "$x \in A \cup B$"
$\neg P \wedge Q$ = "$x \notin A$ AND $x \in B$" = "$x \in A^c \cap B$"
$P \wedge \neg Q$ = "$x \in A$ AND $x \notin B$" = "$x \in A \cap B^c$"
$\vdots$
etc.

Examples :



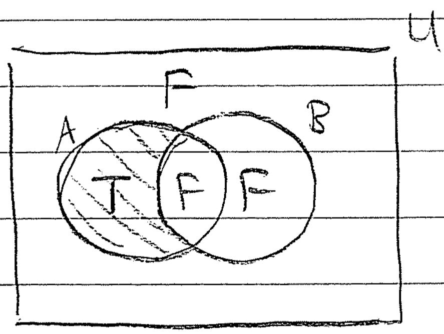
$A \cup B$

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F



$A \cap B$

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



$A \cap B^c$

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

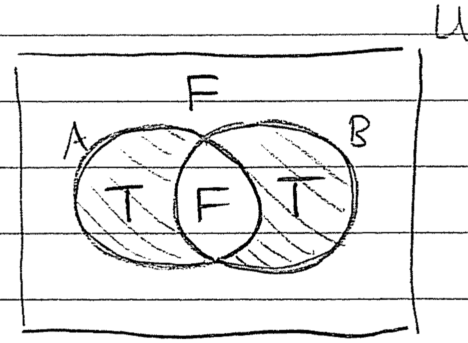
Problem: Let P, Q be logical statements and let $\varphi(P,Q)$ be the logical statement defined by the following truth table

P	Q	$\varphi(P,Q)$
T	T	F
T	F	T
F	T	T
F	F	F

Find a formula for $\varphi(P,Q)$ in terms of the Boolean operations $\wedge, \vee, \neg$.

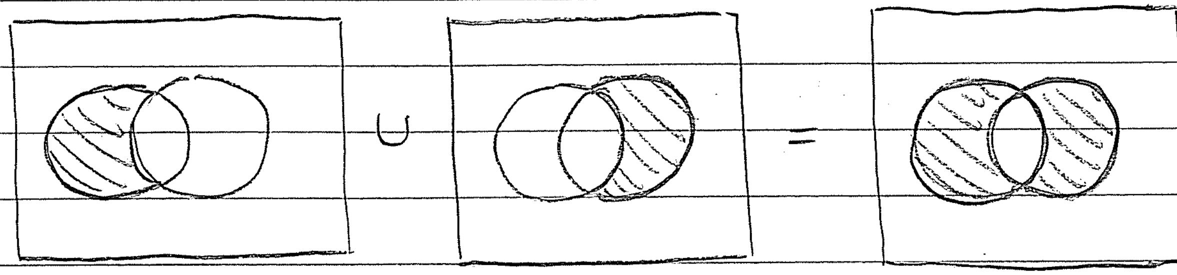
Solutions: It helps to consider the associated Venn diagram.

If $P =$ "$x \in A$" and $Q =$ "$x \in B$" then we have



$\varphi(P,Q)$

What set does this correspond to?



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

We conclude that

$$\begin{aligned} \varphi(P,Q) &= \text{“} x \in (A \cap B^c) \cup (A^c \cap B) \text{”} \\ &= \text{“} x \in A \cap B^c \vee x \in A^c \cap B \text{”} \\ &= \text{“} (x \in A \wedge \neg x \in B) \vee (\neg x \in A \wedge x \in B) \text{”} \\ &= (P \wedge \neg Q) \vee (\neg P \wedge Q) \end{aligned}$$

“(P AND NOT Q) OR (NOT P AND Q)”

Let's check that the formula works by building it up piece by piece.

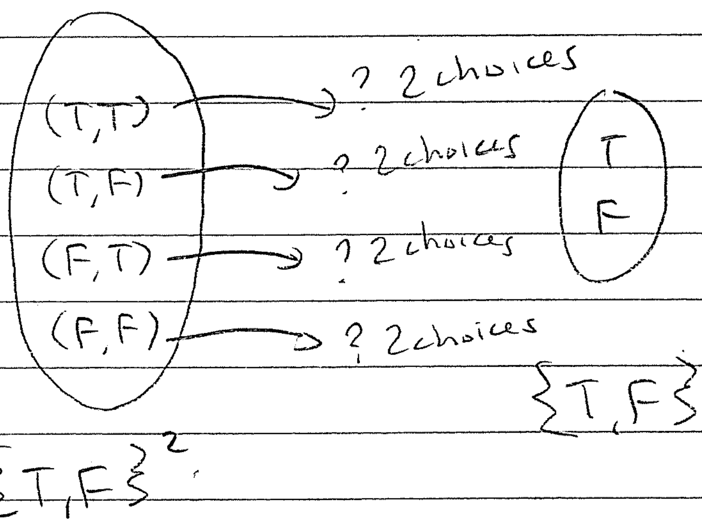
P	Q	$\neg P$	$\neg Q$	$P \wedge \neg Q$	$\neg P \wedge Q$	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$
T	T	F	F	F	F	F
T	F	F	T	T	F	T
F	T	T	F	F	T	T
F	F	T	T	F	F	F

$\checkmark$

Let $P, Q \in \{T, F\}$ be logical statements.
We can think of a statement $\varphi(P, Q) \in \{T, F\}$
as a <u>function</u> from the set

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

to the set $\{T, F\}$:

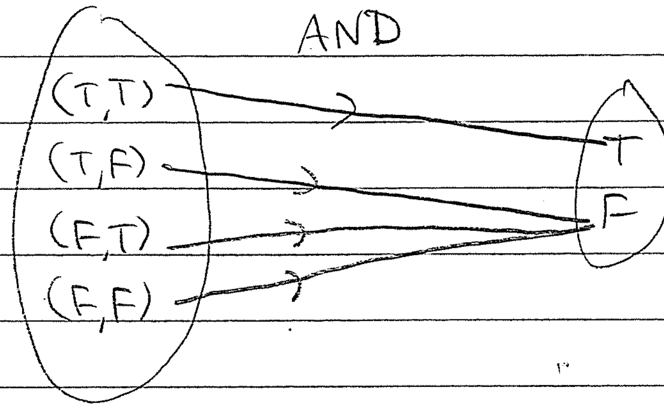


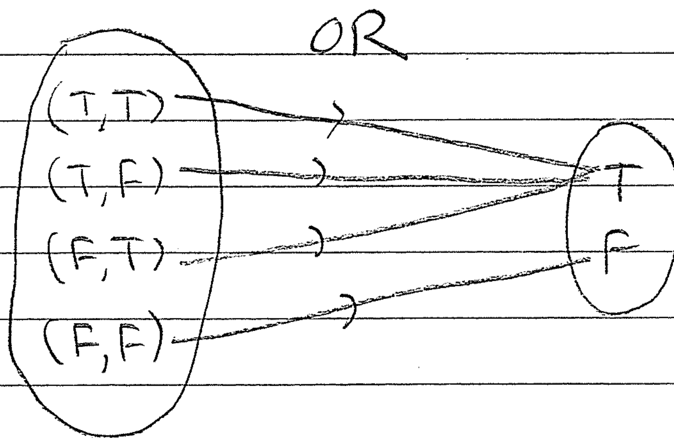
How many such functions are there?

Each arrow has 2 choices for its target
so the total number of choices is

$$2 \times 2 \times 2 \times 2 = 2^4 = 16.$$

We have named two of these functions:





Most of the other 14 also have names. We'll see them later.

You should also remember the definitions of injective/surjective/bijective functions.