LECTURE #3

Methods of Proof (1.6 in text)
Starting on p.37 of John's notes.

Theorem: a statement that can be shown to be true. (result)

Proof: a demonstration of the correctnest of a theorem.

Lemma: a less important, but helpful result, typically used to construct a proof

Corollary: a result / fact that can be established directly from an existing proof

Conjecture: a statement proposed as true, but for which we have no proof.

What is a Proof?

Direct Proof: To prove the implication $p \to q$ start by assuming p is true. Now prove that q is true under this assumption.

Ex: Prove "If n is an odd integer, then n^2 is an odd integer"

Assume "n is an odd integer"

Then $n = 2k + 1$ for some k

so $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2\underbrace{(2k^2 + 2k)}_{t} + 1$

$= 2t + 1$ (which is odd).

$\therefore n^2$ is odd.

It is the implication we are trying to prove, not p or q.

Indirect Proof (Proof by Contraposition)

Recall that $p \to q \equiv \neg q \to \neg p$. So to prove $p \to q$ we could prove $\neg q \to \neg p$ using a direct proof, so assume $\neg q$ and show $\neg p$.

Ex: If $3n+2$ is odd, then n is odd.

p: $3n+2$ is odd

q: n is odd.

Assume n is not odd, or $\neg q$, prove $\neg q \to \neg p$.

$\neg q$, so $n = 2k$ for some k.

then
$$
\begin{aligned}
3n+2 &= 3(2k)+2 \\
&= 6k+2 \\
&= 2(3k+1) \\
&= 2t
\end{aligned}
$$
- so has form $2k$, so $3n+2$ is even!

Vacuous / Trivial Proofs

When proving $p \to q$, if p is false then the statement follows automatically.

Ex: Let $P(n)$ = "if $n > 1$, then $n^2 > n$". Prove $P(0)$.

The statement reads "if $0 > 1$ then $0^2 > 0$", but "$0 > 1$" is false, so the hypothesis is false and the claim follows trivially."

More Examples

Ex: Prove that the sum of two rational numbers is rational.

Suppose r, s. are rational numbers.

Then $r = \frac{a}{b}$, $s = \frac{c}{d}$ 　 Assume $\{a,b,c,d\} \in \mathbb{Z}^+$, $b, d \neq 0$

$$
\begin{aligned}
rs &= \frac{a}{b} + \frac{c}{d} \\
&= \frac{ad+cb}{bd} \leftarrow \text{all integers}
\end{aligned}
$$

$\therefore$ $r+s$ is rational (A direct proof).

Ex: If n is an integer and n^2 is odd, then n is odd. $p \rightarrow q$

Direct? Assume $O(n) \rightarrow O(n^2)$.

$$n^2 = 2k+1$$
$$n = \sqrt{2k+1}$$

This isn't helpful as we don't know k.

Indirect

Assume n is even $(\neg q)$ and prove $\neg q \rightarrow \neg p$.

$$n = 2k$$
$$n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2t$$

So n^2 is even if n is even.

Proof By Contradiction

Suppose we want to prove p. If we can show $\neg p \rightarrow F$ (i.e. $\neg p$ leads to a contradiction) is true, then $\neg p$ must be false $\therefore$ p is T.

Ex: $\sqrt{2}$ is irrational. — i.e. we cannot express $\sqrt{2}$ as $\frac{a}{b}$ where $\{a,b\} \in \mathbb{Z}^+$

Suppose $\sqrt{2}$ is rational.

Thus $\sqrt{2} = \frac{a}{b}$ for $\{a,b\} \in \mathbb{Z}^+$ and $b \neq 0$.

Also, assume a, b have no common factors (i.e. they cannot be reduced.)

Square both sides $2 = \frac{a^2}{b^2}$

Then $a^2 = 2b^2$, so a^2 is an even number, and thus a is even and we can state $a = 2c$

Thus $2b^2 = (2c)^2 = 4c^2$ so $b^2 = 2c^2$, thus b is also an even number.

So both a, b are even, thus they share a common factor '2'.

This is a contradiction, so our assumption $\neg p$ is false, so $\sqrt{2}$ is irrational.

Proof by Cases (Time permitting prove if $m+n$ and $m+p$ are even then $m+p$ is even.)

If we wish to prove $p \to q$ and we can break p down into n cases such that

$$(p_1 \vee p_2 \vee p_3 \cdots \vee p_m) \to q$$

then we can prove the (logically equivalent) statement:

$$[(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_m \to q)]$$

Ex: $x, y \in \mathbb{R}$ then prove that $|xy| = |x||y|$

There are four possible combinations of sign values for x and y.

Case 1: $x \geq 0,\ y \geq 0$ then $xy \geq 0$

Then $|xy| = xy = |x||y|$

Case 2: $x \geq 0,\ y < 0$ [$xy < 0$ and $y < 0$ implies $|y| = -y$]

Then $|xy| = -xy = x(-y) = |x||y|$

Case 3: $x < 0,\ y \geq 0$ [we use same arg on x].

Then $|xy| = -xy = (-x)y = |x||y|$

Case 4: $x < 0,\ y < 0$ [$xy > 0$].

Then $|-x \cdot -y| > 0$

Hence $|xy| = xy = (-x)(-y) = |x||y|$

Equivalence Proofs

To prove $p \leftrightarrow q$ prove $(p \to q) \wedge (q \to p)$

Ex: n is odd, iff n^2 is odd.

Step ① Assume n is odd, then $n = 2k+1$ and $n^2 = 4k^2 + 4k + 1$

$= 2(k^2 + 2k) + 1$

$= 2t + 1$ (odd)

Step ② Assume n^2 is odd, show that n is odd through the indirect proof on previous page.

Existence Proofs.

To prove $\exists x\, P(x)$.

Constructive : Find example of a s.t. $P(a)$ is true.

Non-constructive : prove it some other way, (i.e. don't need to find 'a', just show that an a must exist.

Ex: (Constructive)

Show that there is a positive integer that can be written as the sum of cubes in two different ways.

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Ex: (Non-constructive)

Show that there exist irrational numbers x, y s.t x^y is rational.

How?

Start : we know $\sqrt{2}$ is irrational number.

What about $\sqrt{2}^{\sqrt{2}}$ $(x = \sqrt{2}, y = \sqrt{2})$, if it is rational we are done, otherwise we are not done.

So let $z = \sqrt{2}^{\sqrt{2}}$ (which would be irrational). and $y = \sqrt{2}$

$$z^x = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \text{ (which is rational)}.$$

Key – we don't know if z^x or x^y is irrational, but one of them must be.

Uniqueness Proofs.

First show that $P(x)$ is true for some x, and then show that if $P(y), y \neq x$ $y \neq x$ then $P(y)$ is False. (or that if $P(y)$ is true, $y = x$).

Ex: If p is an integer, then there exists a unique q. s.t. $p + q = 0$.

Existence: Let $q = -p$ then $p + q = p - p = 0$

Uniqueness : Suppose $p + r = 0$ and $p + q = 0$ with $q \neq r$.

Then $\cancel{p} + r = \cancel{p} + q$, so $r = q$ – a conradiction.

Counter Examples

For a statement of the form $\forall x P(x)$, we can prove $\forall x P(x) = F$ if we can find a single a s.t. $P(a) = F$.

Ex: Show that "If a and b are irrational numbers, then $a \cdot b$ is irrational".

Counter - example
$a = \sqrt{5}$ $b = \sqrt{5}$ then $\sqrt{5} \cdot \sqrt{5} = 5 = \frac{5}{1} = a \cdot b$.

So our conjecture is not true.

SETS - Chapter 2

Section 2.1 (Sets)

A set is a collection of unordered objects. (this is vague?).

The objects in a set are called elements (members) of the set.

The set contains its elements.

> Say we have an object x and a set Z (typically use u.c. for sets an l.c for elements).

$x \in Z$ if object x is an element of Z.

$x \notin Z$ if " " " not an element of Z.

> Describing sets, list elements

$\{a, b, c\}$ set containing first 3 letters of the alphabet.

> The type of object for each element need not be the same

$\{\text{dog}, \sqrt{2}, \pi, m\}$

Ellipses can be used (in the brackets) if a pattern is clear..

$\{1,2,3,4,\ldots,50\}$ all integers from 1 to 50.

> Some sets, which we commonly refer to have commonly agreed upon notations:

$\mathbb{R}$: real numbers. $\mathbb{Z}$: integers. ($\mathbb{Z}^+$ - +ve integers).

$\mathbb{N}$: natural numbers $\mathbb{Q}$: rational numbers.

> The elements of a set may be other sets:

$A = \{1,2,3\}$ $B = \{a,b,c\}$ $C = \{A,B\}$

> It is possible to have an empty set $\{\}$ which we write $\emptyset$. It is not the same as $\{\emptyset\}$, which is a set containing one set (which happens to be empty). [Folders example].

> One common way to define sets is to use set builder notation:

$\mathbb{R} = \{r \mid r \text{ is a real number}\}$

$A = \{x \mid x \in \mathbb{Z}^+ \text{ and } x < 7\} = \{1,2,3,4,5,6\}$.

> <u>Cardinality</u>: the number of distinct elements in a set, we denote it $|A|$, if $|A|$ is ∞ (eg $|\mathbb{R}|$) then we say the set is infinite

> Order & duplicate elements <u>do not</u> matter

eg.

$\{2,4,6,8\} = \{8,6,4,2\}$

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

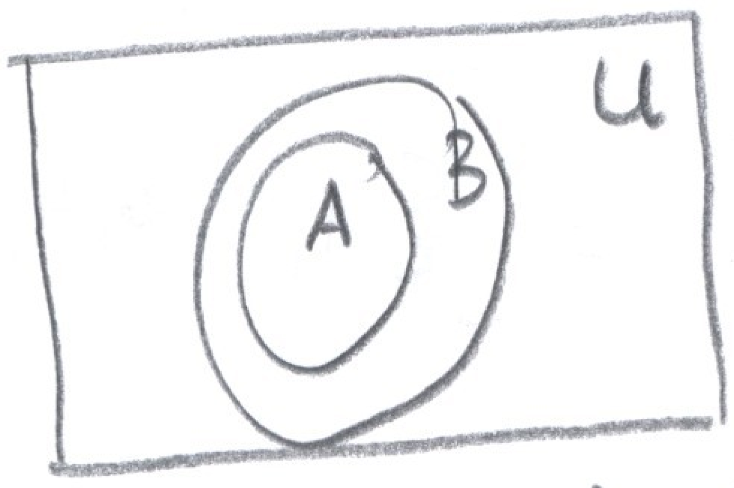
Venn Diagrams

A graphical representation for sets. We begin with a rectangle representing the universal set U (domain).

Inside a circle (or other shape) represents the set(s). If desired points can be drawn to indicate particular elements of the set.

Subsets: A is a subset of B iff every element of A is also an element of B

Denoted $A \subseteq B$ – A is subset of B.



Note that $A \subseteq A$ by this defn.

Examples:

$\{1, 2, 3\} \subseteq \mathbb{Z}^+$

$\{x, y, z\} \subseteq A$ – where A is letters of the alphabet.

people in this class $\subseteq$ carleton university students.

all Canadians $\subseteq$ all Canadians

Proper Subset

$A \subseteq B$ and $A \neq B$ then we say A is a proper subset of B and write:

$$A \subset B$$

$\boxed{\text{Break Time (10min)}}$

Subsets (con't)

Note that $A \subseteq B \longleftrightarrow \forall x\,(x \in A \rightarrow x \in B)$

For any set S:

1. $\emptyset \subseteq S$

Proof: $\forall x\,(x \in \emptyset \longrightarrow x \in S)$

Since $|\emptyset| = 0$, $x \in \emptyset = F$ for all x.

$F \rightarrow q \equiv T$, so this is true for any x.

Equality

Two sets are equal if they are subsets of each other

$A \subseteq B$ and $B \subseteq A$.

$$(A \subseteq B) \wedge (B \subseteq A) \Longleftrightarrow \forall x\,((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A))$$

$$\Longleftrightarrow \forall x\,(x \in A \leftrightarrow x \in B)$$

$$\rightarrow A = B.$$

Power Set

The power set of set A is the set of all subsets of S, denoted $P(A)$.

Ex: What is the power set of $\{a, b, c\}$

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a, b, c\}\}$$

Cartension Product

If A and B are sets, then the cartesian product of A and B, $A \times B$, is the set of ordered pairs where the first element is drawn from A and the second from B

Ex: $A \times B = \{(a,b) \mid (a \in A) \wedge (b \in B)\}$

$A = \{1,2\}$ $\quad \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$

$B = \{a, b, c\}$

If we have sets $A_1, A_2, A_3 \ldots A_n$ the cartesian product is $A_1 \times A_2 \times \ldots \times A_n$ - and is a set of n-tuples $(a_1, a_2 \ldots a_n)$ where $a_i \in A_i$

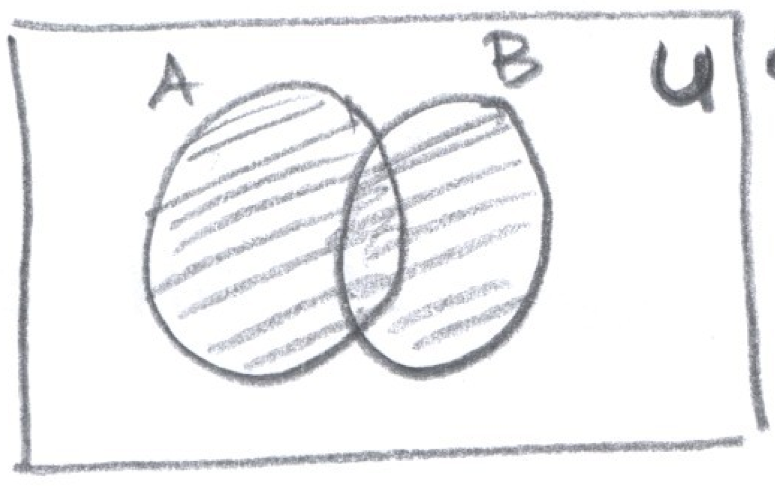
Ex: $A = \{a\}$
$B = \{b, c\}$
$C = \{d, e, f\}$
$A \times B \times C = \{ (a,b,d), (a,b,e), (a,b,f), (a,c,d), (a,c,e), (a,c,f) \}$

Set Operations

How can we combine two sets? (or more).

Union

Let A and B be sets. The union of sets A and B, denoted $A \cup B$, is the set containing the elements in A, B, and both.



← shaded area is $A \cup B$.

Ex: $A = \{a, b, c, d\}$, $B = \{a, f, g\}$ ⟩ $A \cup B = \{a, b, c, d, f, g\}$

$A \cup B = \{x \mid x \in A \vee x \in B\}$

$\forall x \{ [(x \in A) \vee (x \in B)] \rightarrow x \in [A \cup B] \}$.

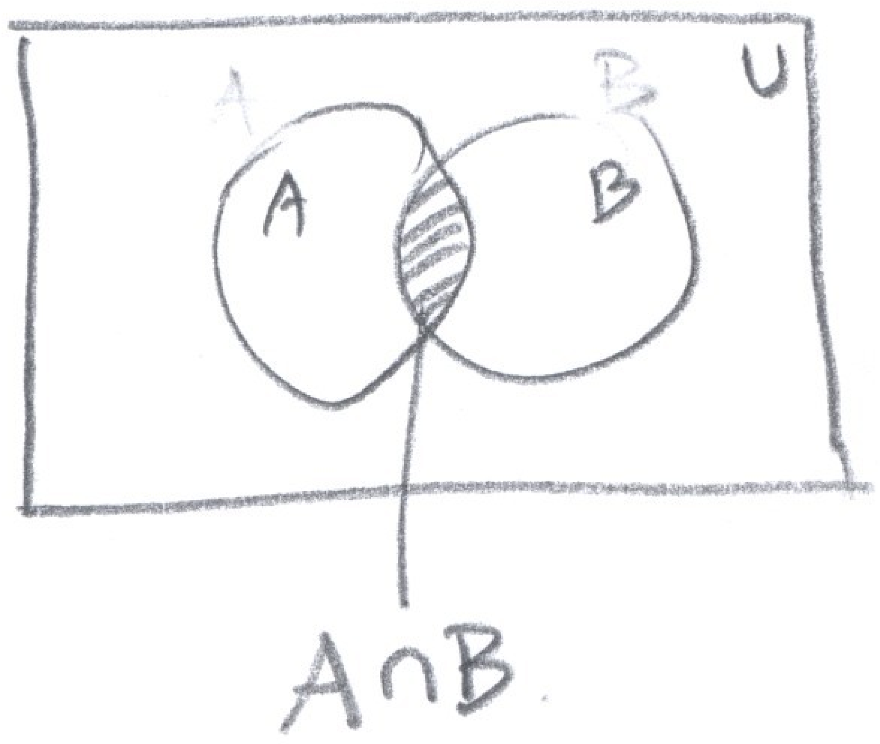
We can have the union of many sets.

$A \cup B \cup C \cup D$

Intersection

Let A and B be sets. The intersection of A and B, denote $A \cap B$ is the set containing elements in both A and B.

Venn



$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

$$\boxed{\forall x\left(\left[(x \in A) \wedge (x \in B)\right] \rightarrow (x \in (A \cap B))\right)}$$

$A = \{2, 4, 6, 8\}$ $\qquad$ $A \cap B = \{4, 6\}$

$B = \{4, 5, 6, 7\}$

We say that A and B are disjoint if $A \cap B = \emptyset$.

Difference

A, B sets. The difference, denoted $A - B$, is the set containing those elements in A that are not in B.

Often denoted $A \setminus B$

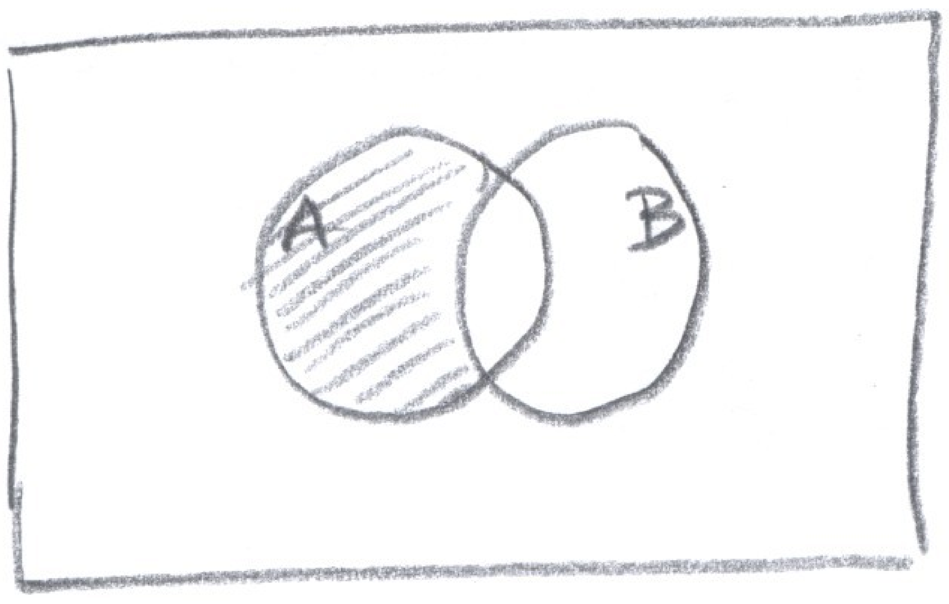
Ex

$A = \{a, b, c, d\}$

$B = \{b, d\}$

$$A \setminus B = \{a, c\}$$

Note: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

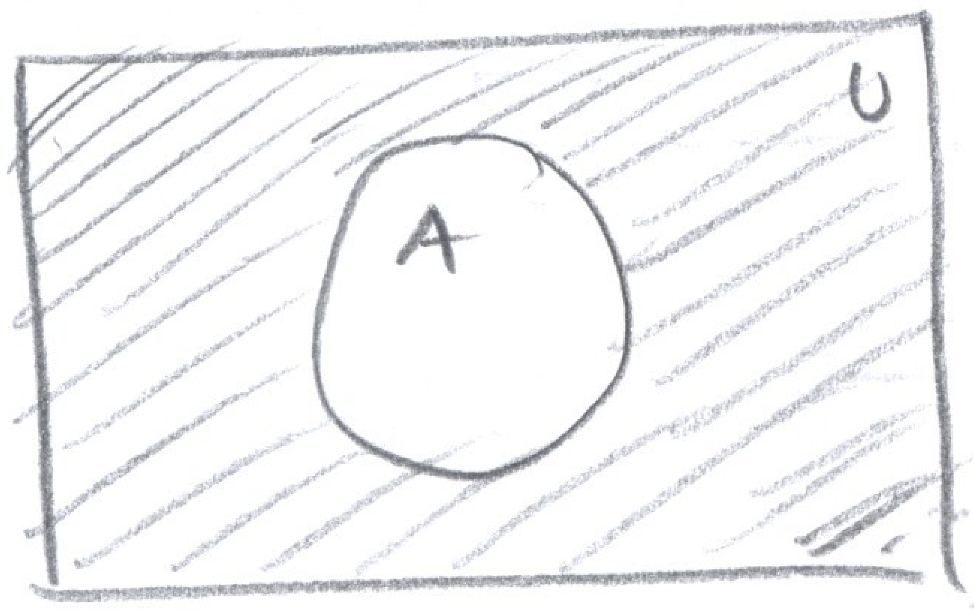


Complement

Let U be the universal set. Then the complement of set A, denoted $\bar{A}$, is the set of elements not in A.

$$\bar{A} = U \setminus A$$

$$\bar{A} = \{x \mid x \notin A\}$$



Ex: Let A be set of positive integers > 5.

$$\bar{A} = \{0, 1, 2, 3, 4, 5\}$$

Ex: Domain $\mathbb{Z}^+$

$$A = \{x \mid x \text{ is an even } \#\}$$
$$\bar{A} = \{x \mid x \text{ is an odd } \#\}$$

Membership Tables

In general, we can combine sets in much the same way as we combine propositions.
Asking if element x is in the resulting set is like asking if a proposition is true.

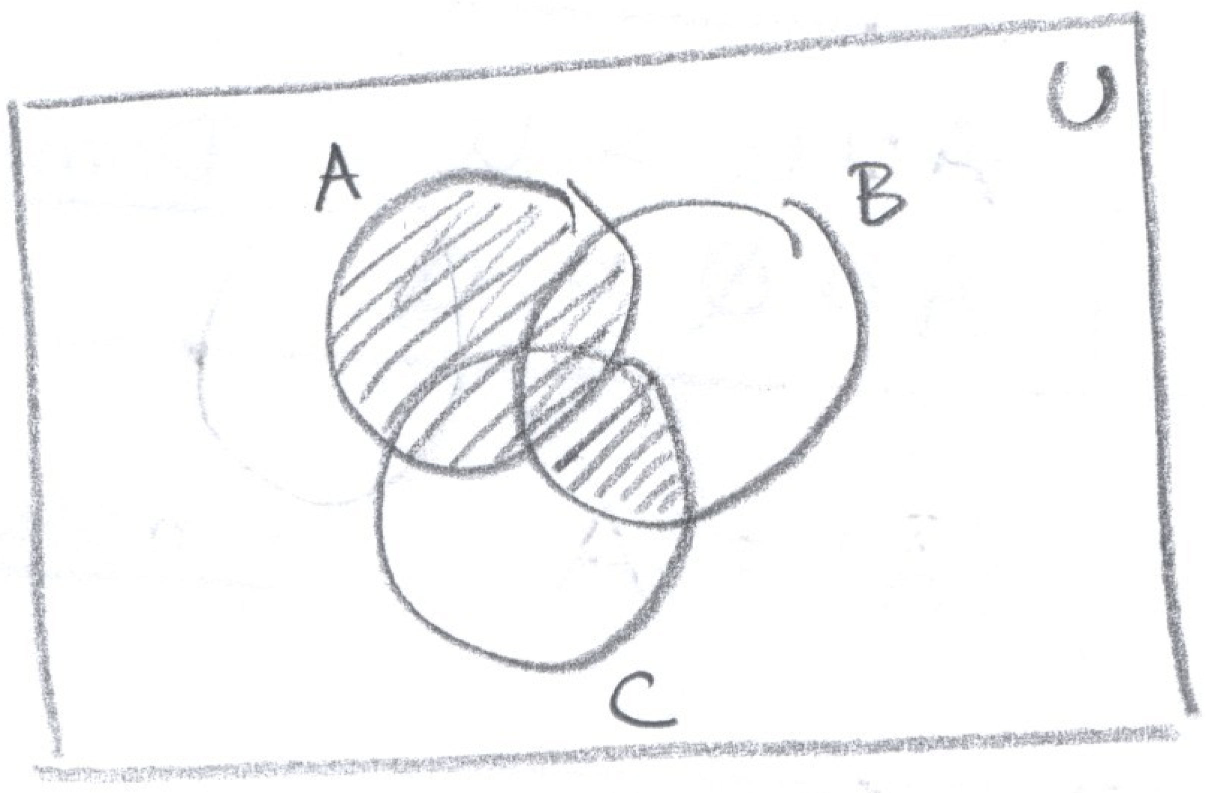
'x' could be in any of the original sets.

Let '1' denote $x \in S$
0 denote $x \notin S$

What does $A \cup (B \cap C)$ look like.

A	B	C	$(B \cap C)$	$A \cup (B \cap C)$
1	1	1	1	1
1	1	0	0	1
1	0	1	0	1
1	0	0	0	1
0	1	1	1	0
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

Venn



How do we show that sets are equal. (show they are subsets of each other)

Ex: Show $\overline{A \cap B}$ and $\bar{A} \cup \bar{B}$ are equal.

$x \in \overline{A \cap B} \rightarrow x \notin (A \cap B)$
$\rightarrow \neg(x \in (A \cap B))$
$\rightarrow \neg((x \in A) \wedge (x \in B))$
$\rightarrow \neg(x \in A) \vee \neg(x \in B)$ DeMorgan
$\rightarrow x \notin A \vee x \notin B$
$\rightarrow x \in \bar{A} \vee x \in \bar{B}$
$\rightarrow \bar{A} \cup \bar{B}$

$x \in (\bar{A} \cup \bar{B}) \rightarrow x \in \bar{A} \vee x \in \bar{B}$
$\rightarrow x \notin A \vee x \notin B$
$\rightarrow \neg(x \in A) \vee \neg(x \in B)$
$\rightarrow \neg((x \in A) \wedge (x \in B))$
$\rightarrow \neg(x \in (A \cap B))$
$\rightarrow x \notin (A \cap B))$
$\rightarrow x \in (\overline{A \cap B})$

$\therefore$ if $x \in (\overline{A \cap B})$ then $x \in (\bar{A} \cup \bar{B})$ and vice-versa.

Or, using a membership table

A	B	$A\cap B$	$\overline{A\cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A}\cup\overline{B}$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

these are same so the sets are equal.

Finally, we can use SET IDENTITIES (see Logical Equivalences) or Laws

$A\cup\emptyset = A$ $A\cap U = A$ Identity	$A\cup U = U$ $A\cap\emptyset = \emptyset$ Domination
$A\cup A = A$ $A\cap A = A$ Idempotent	$\overline{(\overline{A})} = A$ Complementation
$A\cup B = B\cup A$ $A\cap B = B\cap A$ Commutative	$A\cup(B\cup C) = (A\cup B)\cup C$ $A\cap(B\cap C) = (A\cap B)\cap C$ Associative
$A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$ $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$ Distributive	$\overline{A\cup B} = \overline{A}\cap\overline{B}$ $\overline{A\cap B} = \overline{A}\cup\overline{B}$ De Morgans
$A\cup(A\cap B) = A$ $A\cap(A\cup B) = A$ Absorption	$A\cup\overline{A} = U$ $A\cap\overline{A} = \emptyset$ Complement

What about set differences.

We use $A \setminus B = A \cap \overline{B}$ "Difference Equivalence"

Ex: Is $(A \setminus C) \cap (B \setminus C) = (A \cap B) \cap \overline{C}$?

① Membership Table

A	B	C	$A \setminus C$	$B \setminus C$	$(A \setminus C) \cap (B \setminus C)$	$A \cap B$	$\overline{C}$	$(A \cap B) \cap \overline{C}$
1	1	1	0	0	0	1	0	0
1	1	0	1	1	1	1	1	1
1	0	1	0	0	0	0	0	0
1	0	0	1	0	0	0	1	0
0	1	1	0	0	0	0	0	0
0	1	0	0	1	0	0	1	0
0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0

same

So they are equivalent.

② Using <u>SET IDENTITIES</u>

$$(A \setminus C) \cap (B \setminus C) = (A \cap \overline{C}) \cap (B \cap \overline{C}) \quad \text{"Diff Equiv."}$$

$$= (A \cap B) \cap (\overline{C} \cap \overline{C}) \quad \text{"Associative, Commutative"}$$

$$= (A \cap B) \cap \overline{C} \quad \text{"Idempotent"}$$