Lecture 6

Recall that a binary operation $*$ on a set X takes ordered pairs $(x,y) \in X^2$ to single elements $x*y \in X$. Below, we use the notation $\forall$ to mean 'for all'.

Common notation for binary operations: $x+y$, xxy, $x \cdot y$, xy etc

Commutative $(\forall x, y \in X)(x*y = y*x)$.

associative $(\forall x, y, z \in X)((x*y)*z = x*(y*z))$.

idempotent $(\forall x \in X)(x*x = x)$.

e is an identity $(\forall x \in X)(e*x = x = x*e)$.

z is a zero $(\forall x \in X)(z*x = z = x*z)$.

If $\bullet$ is another binary operation on X, we say that $*$ distributes over $\bullet$ if

$$(\forall x,y,z \in X)\Big(\quad x*(y\bullet z) \quad = (x*y)\bullet(x*z)\Big).$$

[This is left distributivity. There is also right distributivity]

Example There are two important binary operations on $\mathbb{R}$: $+$ (addition), $\cdot$ (multiplication).

[We usually write simply xy instead of $x\cdot y$]

- $x+(y+z) = (x+y)+z$. Addition is associative.
- $x+y = y+x$. Addition is Commutative
- $x+0 = x = 0+x$. 0 is the additive identity

- $x(yz) = (xy)z$. Multiplication is associative.
- $xy = yx$. Multiplication is Commutative.
- $x1 = x = 1x$. 1 is the multiplicative identity
- $x0 = 0 = 0x$. 0 is the multiplicative zero.

- $x(y+z) = xy + xz$

Thus Multiplication distributes over addition.

We now list the properties of the Boolean operations

Let A, B, C be any sets.

$A \cap (B \cap C) = (A \cap B) \cap C$ Associativity	$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap B = B \cap A$ Commutativity	$A \cup B = B \cup A$
$A \cap A = A$ Idempotence	$A \cup A = A$
$A \cap \emptyset = \emptyset = \emptyset \cap A$ $\emptyset$ is the zero for $\cap$	$A \cup \emptyset = A = \emptyset \cup A$ $\emptyset$ is the identity for $\cup$

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

Intersection distributes over union

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

Union distributes over intersection.

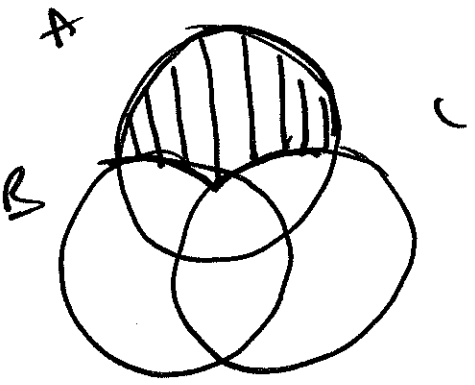
The following are unique to Boolean operations and are called <u>De Morgan's laws</u>

- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

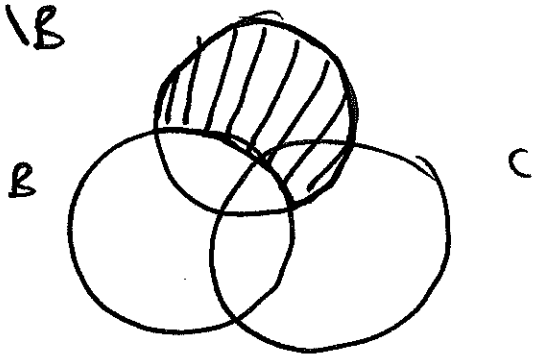
We can illustrate many of these properties using Venn diagrams.

Example Illustrate $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ using Venn diagrams.

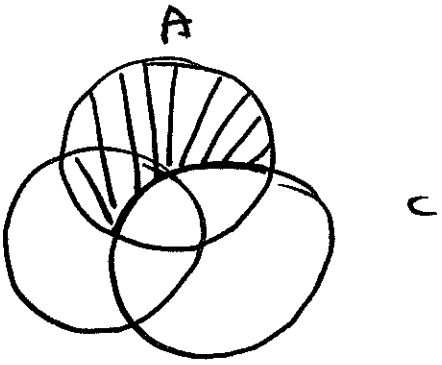
$A \setminus (B \cup C)$



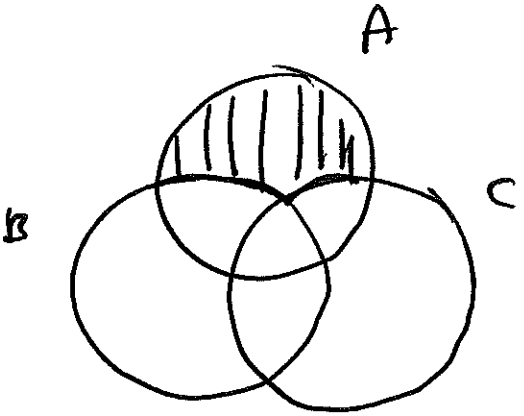
$A \setminus B$



$A \setminus C$



$(A \setminus B) \cap (A \setminus C)$



These Venn diagrams illustrate the result, though they do not prove it

Prop that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

We show that

(1) $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$.

(2) $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$.

---

(1) Let $x \in A \setminus (B \cup C)$.

Then $x \in A$ and $x \notin B \cup C$.

Since $x \notin B \cup C$ it follows that

$x \notin B$ and $x \notin C$.

We have that $x \in A$ and $x \notin B$ $\Rightarrow$ $x \in A \setminus B$

We have that $x \in A$ and $x \notin C$ $\Rightarrow$ $x \in A \setminus C$.

We have therefore proved that $x \in (A \setminus B) \cap (A \setminus C)$

We have proved that $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ ▨□

---

(2) Let $x \in (A \setminus B) \cap (A \setminus C)$

Then $x \in A \setminus B$ and $x \in A \setminus C$. So,

$(x \in A)$ and $(x \notin B)$ and $(x \in A)$ and $(x \notin C)$.

Since $(x \notin B)$ and $(x \notin C)$ then $x \notin (B \cup C)$

But $x \in A$ so $x \in A \setminus (B \cup C)$ ■

An important consequence of associativity is that when a binary operation is associative, we do not need brackets.

Thus $\left.\begin{array}{l} A_1 \cup \dots \cup A_n \\ A_1 \cap \dots \cap A_n \end{array}\right\}$ both unambiguous

We would usually write these as

$$\bigcup_{i=1}^{n} A_i$$

$$\bigcap_{i=1}^{n} A_i$$

This material was not discussed in the lectures. It is for background at this stage. I hope to return to it at the end of the course.

Proofs

We need to prove our unproved theorems. To do this, we shall use some counting principles.

We need the notion of a bijective function. Let $f : A \to B$ be a function. It is called injective if $f(a) = f(a') \Rightarrow a = a'$. It is called surjective if for each $b \in B$ there exists $a \in A$ such that $f(a) = b$. A bijective function is one that is both injective and surjective.

Counting principles

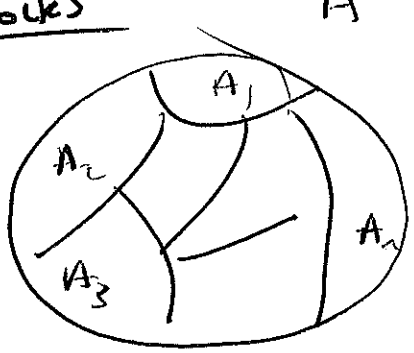
(I) Sets X and Y have the same cardinality when there is a bijection from X to Y.

(II) Let A be a non-empty set. A partition of A is a set $P = \{A_1, \dots, A_n\}$ where $A_1, \dots, A_n$ are called blocks

(1) $A_i \neq \emptyset$ for all $1 \leq i \leq n$.

(2) $A_i \cap A_j = \emptyset$ if $i \neq j$.

(3) $A = A_1 \cup \dots \cup A_n$.



Then $|A| = |A_1| + \dots + |A_n|$

We use these two principles to determine $|A \times B|$.

Let $a \in A$. Then there is a bijection between

$$\{a\} \times B \text{ and } B.$$

So, $|\{a\} \times B| = |B|$.

Then the set $\{\{a\} \times B : a \in A\}$ is a partition of $A \times B$. Thus

$$|A \times B| = |A|\,|B|.$$

By induction (see later)

$$|A_1 \times \dots \times A_n| = |A_1| \dots |A_n|.$$

We shall call this Counting principle (II).

Theorem 1 $|P(X)| = 2^{|X|}$

Proof Let X be the set $\{0,1\}^{|X|}$ This has $2^{\wedge}$ elements by (III). We define a bijection between $P(X)$ and $\{0,1\}^{|X|}$ which establishes the result by (I).

Order the elements of X: $x_1, \ldots, x_n$. Let $A \subseteq X$ then define $f(A)$ to be $(a_1, \ldots, a_{|X|})$ where

$a_i = 0$ if $x_i \notin A$ and $a_i = 1$ if $x_i \in A$. ∎

Theorem 5 Let $|X| = n$ and $0 \leq k \leq n$.

Then the number of k-permutations is $\frac{n!}{(n-k)!}$

Proof Partition the set of all k-permutations so that all elements of the same block begin with the same letter.

By (II), we have that $nP_k = n^{n-1}P_{k-1}$.

Now repeat. ∎

Theorem 2. Let $|X| = n$. Let $0 \leq k \leq n$.

The number of k-subsets is $\dfrac{n!}{k!\,(n-k)!}$

Proof Partition the set of all k-permutations so that two k-perms are in the same block if they permute the same elements. Then

$$ {}_nP_k = k! \; {}_nC_k$$

Thus $${}_nC_k = \frac{1}{k!} \, {}_nP_k$$ ∎