# Introduction to Discrete Mathematics

Eric Pacuit
Department of Philosophy
University of Maryland, College Park
ai.stanford.edu/~epacuit
epacuit@umd.edu

September 14, 2012

These notes provide a very brief background in discrete mathematics.

## 1 Basic Set Theory

We often groups things together. Everyone in this class, your group of friends, your family. These are all collections of people. Set theory is an mathematical language to talk about collections. In this section, we define a number of operations on sets.

The easiest way to visualize a set is to use a *Venn diagram*. A Venn Diagram is a geometrical interpretation of a set. Intuitively, a set is just a collection of objects that have something in common. We will represent sets by capital letters, and elements of sets will be represented by lower case letters. We have two ways to write down the contents of a set:

1. List all the elements of the set. Each element should be separated by a comma and contained between curly brackets ({}). For example suppose $A$ is the set of the first 5 letters of the alphabet. Then $A = \{a, b, c, d, e\}$.

2. Write down a property that **all** elements of the set have in common. For example if $A$ is the set of all positive integers, then we can describe $A$ as follows $A = \{x \mid x \geq 0 \text{ and } x \text{ is an integer}\}$. This is read "$A$ is the set of all $x$ such that $x$ is an integer that is greater than or equal to zero".

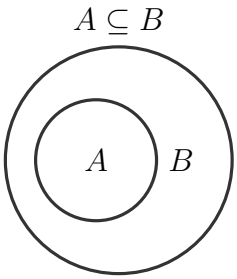
**Definition 1.1 (Set)** Any collection of objects (formally, a set is a collection of elements of a *universal set*[1]). ◁

**Definition 1.2 (Element)** A member of a set. ◁

We write $x \in A$ to mean "$x$ is an element of the set $A$".

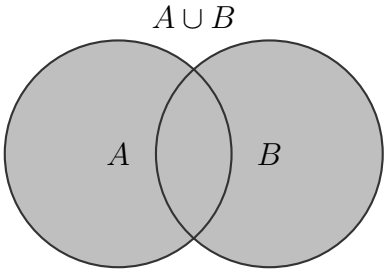
**Definition 1.3 (Subset)** A **subset** is a sub collection of a set. We write $A \subseteq B$ if $A$ is a **subset** of $B$, formally, $A \subseteq B$ when every element of $A$ is also an element of $B$. ◁

Notice that every set is a subset of the universal set. The notion of subset can be pictured as follows:




**Definition 1.4 (Union)** The **union** of two (or more) sets is a set that contains all the elements of each set. For two sets $A$ and $B$, the union of $A$ and $B$ is the set $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$. ◁

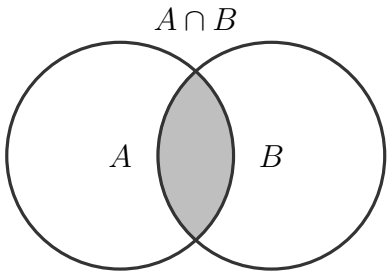
The union of two sets can be pictured as follows:




**Definition 1.5 (Intersection)** The **intersection** of two (or more) sets is the set of all items in common to each set. If $A$ and $B$ are two sets, then the intersection of $A$ and $B$ is the set $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$. ◁

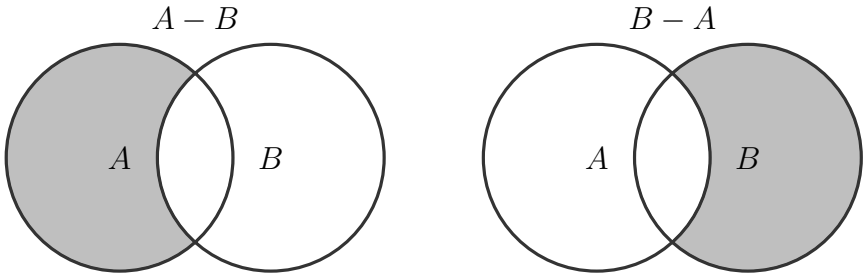
[1]Typically, we start by fixing a universal set that defines the "domain of discourse".

The intersection can be pictured as follows:




**Definition 1.6 (Set Difference)** The difference between two sets $A$ and $B$ ($A$ minus $B$) is all elements in $A$ but not in $B$. The difference between $A$ and $B$ is the set $A - B = \{x \mid x \in A \text{ and } x \notin B\}$. ◁

The differences between $A$ and $B$ can be pictured as follows:

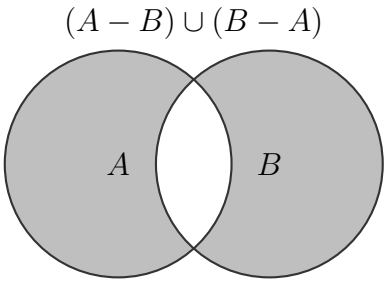



**Definition 1.7 (Complement)** The **Complement** of a set is the set of all elements not contained in that set. Formally, the complement of the set $A$ is $A^C = \{x \mid x \text{ is in the universal set and } x \notin A\}$ ◁

Why is the notion of a universal set necessary for this definition?

**Definition 1.8 (Symmetric Difference)** The symmetric difference of two sets is all the elements in either set *but not in both*. The symmetric difference is the set $(A - B) \cup (B - A)$. ◁

The symmetric difference can be pictured as follows:




**Definition 1.9 (Product)** The **Cartesian product** of two or more sets is all possible pairings of each elements of the sets. If $A$ and $B$ are two sets, then the cartesian product of $A$ and $B$ is the set $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$ ◁

**Definition 1.10 (Null Set)** The null or empty set is a set that contains no elements. We write $\emptyset$ to denote the set containing no elements. ◁

**Definition 1.11 (Power Set)** The **power set** is the set of all subsets. If $A$ is a set, the power set of $A$ is the set $\mathcal{P}(A) = \{B \mid B \subseteq A\}$. ◁

Notice that the empty set is a subset of every set.

**Definition 1.12 (Cardinality of a Set)** The cardinality of a finite set $A$ is the total number of elements in $A$, and is denoted $|A|$. ◁

**Definition 1.13 (Partition)** A **partition** of a set $S$ is a collection of sets $\mathcal{S} = \{S_1, S_2, \ldots\}$ (possibly infinite) such that

- the sets are **pairwise disjoint**: if $S_i, S_j \in \mathcal{S}$ with $i \neq j$, then $S_i \cap S_j = \emptyset$
- their union is $S$, that is, $S = \cup_{S_i \in \mathcal{S}} S_i$. ◁

# 2 Relations

**Definition 2.1 (Binary Relation)** A binary relation $R$ on two sets $A$ and $B$ is a subset of the cross product of $A$ and $B$, i.e., $R \subseteq A \times B$ ◁

You should be familiar with many binary relations: $=, \leq, \geq, <, >$ are relations on numbers (eg., the natural numbers $\mathbb{N}$, real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$, etc.) and $\subseteq$ is a relation on the power set of a given set $S$. For example the binary relation $\leq \subseteq \mathbb{N} \times \mathbb{N}$ is the set

$$\{(a, b) \mid a, b \in \mathbb{N} \text{ and } a \text{ is less than or equal to } b\}$$

Suppose that $R$ is a relation. We often write $aRb$ to mean $(a, b) \in R$. The following are properties of relations that may be of interest:

**Reflexivity** for all $a \in A$, $aRa$

**Transitivity** for all $a, b, c \in A$, if $aRb$ and $bRc$ then $aRc$

**Completeness** for all $a, b \in A$, either $aRb$ or $bRa$ (or $a = b$)

**Symmetry** for all $a, b \in A$, if $aRb$ then $bRa$

**Antisymmetric** for all $a, b \in A$, if $aRb$ and $bRa$ then $a = b$

**Definition 2.2 (Equivalence Relation)** A relation $R$ that is reflexive, symmetric and transitive is said to be an **equivalence relation** $\triangleleft$

**Definition 2.3 (Equivalence Class)** If $R$ is an equivalence relation on $A$, then for each $a \in A$, the equivalence class of $a$, denoted by $[a]$, is the following set $[a] = \{b \mid aRb\}$. $\triangleleft$

**Definition 2.4 (Partial Order)** A relation that is reflexive, antisymmetric and transitive is said to be a **partial order**. $\triangleleft$

The standard example of a partial order is the relation $\subseteq$.

The following is our first theorem. It is somewhat technical, but illustrates a fundamental idea about equivalence classes and partitions. Namely, that every partition has an equivalence relation associated with it, and every equivalence class has a partition associated with it.

**Theorem 2.5** *The equivalence classes of any equivalence relation $R$ on a set $A$ forms a partition of $A$, and any partition of $A$ determines an equivalence relation on $A$ for which the sets in the partition are the equivalence classes.*

**Proof.** Suppose $R$ is an equivalence relation on $A$. We must show that the equivalence classes of $R$ forms a partition of $A$.

1. Each equivalence class is non-empty, since $aRa$ for all $a \in A$.

2. Clearly $A$ is the union of all the equivalence classes (since each element of $A$ belongs to at least one equivalence class)

3. We must show any two equivalence classes are disjoint. Let $[a], [b]$ be two distinct equivalence classes. Suppose $c \in [a] \cap [b]$. Then $aRc$ and $bRc$. Hence by symmetry, $cRb$. And so by transitivity, $aRb$.

   Let $x \in [a]$, then $xRc$ and by the above argument $xRb$ (Why?), and so $x \in [b]$. Thus $[a] \subseteq [b]$. Using a similar argument, we can show $[b] \subseteq [a]$. Therefore $[a] = [b]$, which contradicts the fact that $[a]$ and $[b]$ are *distinct* equivalence classes.

For the second part of the theorem, suppose $\mathcal{A} = \{A_1, \ldots, A_n\}$ is any partition of $A$. Define $R = \{(a, b) \mid a \in A_i \text{ and } b \in A_i\}$. We must show that $R$ is reflexive. Let $a \in A$ be any element. Then $a \in A_i$ for some $i$, and hence by definition of $R$, $aRa$. Next we will show that $R$ is symmetric. Suppose $aRb$. Then $a \in A_i$ and $b \in A_i$ for some $i$. Then clearly, $b \in A_i$ and $a \in A_i$ and hence $bRa$. We must show $R$ is transitive. Suppose, $aRb$ and $bRc$. Then $a \in A_i$ and $b \in A_i$, and $b \in A_j$ and $c \in A_j$ for some $i, j$. Since $b \in A_i \cap A_j$, $A_i = A_j$ (since the elements of $\mathcal{A}$ are pairwise disjoint). Therefore, $a \in A_i$ and $c \in A_i$ and hence $aRc$. QED

We will think of a function as a special type of relation:

**Definition 2.6 (Function)** A function $f$ is a binary relation on $A$ and $B$ such that for all $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$. We will often write $f : A \to B$ and if $(a, b) \in f$, we will write $f(a) = b$. ◁

Suppose $f : A \to B$ is a function. $A$ is said to be the **domain** and $B$ the **codomain**.

**Definition 2.7 (Image)** The image of a set $A' \subseteq A$ is the set:

$$f(A') = \{b \mid b = f(a) \text{ for some } a \in A'\}$$

◁

**Definition 2.8 (Range)** The range of a function is the image of its domain. ◁

Suppose $f : A \to B$ is a function.

**Definition 2.9 (Surjection)** $f$ is a surjection (or onto) if its range is equal to its codomain. I.e., $f$ is surjective iff for each $b \in B$, there exists an $a \in A$ such that $f(a) = b$ ◁

**Definition 2.10 (Injection)** $f$ is an injection (or 1-1) if distinct elements of the domain produce distinct elements of the codomain. I.e., $f$ is 1-1 iff $a \neq a'$ implies $f(a) \neq f(a')$, or equivalently $f(a) = f(a')$ implies $a = a'$. $\triangleleft$

**Definition 2.11 (Bijection)** $f$ is a bijection if it is injective and surjective. In this case, $f$ is often called a one-to-one correspondence. $\triangleleft$

**Definition 2.12 (Inverse Image)** Suppose that $f : A \to B$ and that $Y \subseteq B$. The inverse image of $Y$ is the set $f^{-1}(Y) = \{x \mid x \in A \text{ and } f(x) \in Y\}$ $\triangleleft$

# 3 Proofs

## 3.1 Introduction

Learning how to write mathematical proofs takes time and hard work. One thing that must be stressed is knowing the formal definitions. A formal proof of a mathematical statement is simply an explanation of that statement *written in the language of mathematics*. If you don't know and understand the formal definitions, then you will not be able to write down your explanations. It would be like trying to explain something to someone in Italian without actually knowing the Italian language.

## 3.2 Proving Equality and Subset

How do you prove that two sets are equal? The answer to this question depends on who you are trying to convince. In this class, we will always error on the side of caution and given fairly detailed formal proofs. In turns out that proving two sets are equal reduces to proving the sets are subsets of each other.

**Fact 3.1** *$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$*

Why is this true? Well, if $A$ and $B$ are equal, then they both name the same collection of objects. I.e., $B$ is another name for the collection of objects that $A$ names and vice versa. So, if $A$ and $B$ are equal then of course $A \subseteq B$ since $A$ is always a subset of itself and $B$ is simply another name for $A$. Similarly, we can show $B \subseteq A$. Conversely, suppose $A \subseteq B$ and $B \subseteq A$. We want to know that $A$ and $B$ name the same collection of objects. Suppose they didn't, then there should be some object $x \in A$ that is not in $B$ **OR** some object $y \in B$ that is not in $A$. Well, we know the object $x$ cannot exist since $A \subseteq B$ and so every element of $A$ is an element of $B$. Similarly, the element $y$ cannot exist. Hence, $A$ and $B$

must name the same collection of objects.

What about trying to prove that two sets are *not* equal? This turns out to be easier. In order to show that $A$ does not equal $B$, you need only find an element in $A$ that is not in $B$ **OR** and element of $B$ that is not in $A$. It will turn out that in general it is always easier to show a negative fact than a positive fact.

Showing two sets are equal reduces to proving that the sets are subsets of each other. But, how to show that a set is a subset of another set? The general procedure to show $A \subseteq B$ is to show that each element of $A$ is also and element of $B$. This is straightforward if $A$ and $B$ are both finite sets. For example, suppose $A = \{2, 3, 4\}$ and $B = \{1, 2, 3, 4, 5, 6\}$. How do we show that $A \subseteq B$. Since $A$ is finite, we simply notice that $2 \in B$, $3 \in B$ and $4 \in B$.

What if $A$ is the set of even numbers and $B$ is the set of all integers? We would get awfully tired (and bored) if we waited around to show that each and every element of $A$ is also an element of $B$. Imagine $A$ and $B$ are two boxes, and you would like to know whether all the elements in $A$'s box are also in $B$'s box. Suppose you reach in box $A$ and select an element say 10. After inspecting 10, you notice that 10 is in fact an integer and so must also be an element of box $B$. But you are not satisfied, since you cannot be sure that the next element you choose from $A$ will also be an element of $B$. In fact, even if you have shown that the first million even integers are all members of box $B$, you cannot be sure that the next element you select from box $A$ will in fact be an integer. Instead you should consider the *property* that $x$ satisfies when it is a member of $A$, and show that it must be the case that $x$ is an element of $B$. What property does $x$ satisfy if it is contained in $A$'s box? The answer is $x = 2 \cdot n$, where $n$ is some integer. Then you simply notice that if $n$ is an integer, then $2 \cdot n$ is also an integer; and hence, $x$ is an element of $B$.

## 3.3 Examples

**Theorem 3.2** $\overline{A} \cup \overline{B} = \overline{A \cap B}$

**Proof.** We must show $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ and $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

We will show $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. Suppose $x \in \overline{A} \cup \overline{B}$. Then $x \in \overline{A}$ **OR** $x \in \overline{B}$. Suppose $x \in \overline{A}$ then $x \notin A$. Then $x \notin A \cap B$ (if $x$ is not in $A$ then $x$ is certainly not in both $A$ and $B$). Hence $x \in \overline{A \cap B}$. Suppose $x \in \overline{B}$. For similar reason,

$x \in \overline{A \cap B}$. Hence in either case, $x \in \overline{A \cap B}$. Therefore, $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

We must show $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. Suppose $x \in \overline{A \cap B}$. Then $x \notin A \cap B$, and so $x \notin A$ **OR**[2] $x \notin B$. Hence either $x \in \overline{A}$ or $x \in \overline{B}$. In either case, $x \in \overline{A} \cup \overline{B}$. QED

**Theorem 3.3** *$A \subseteq B$ iff $A \cap B = A$.*

**Proof.** We must show $A \subseteq B$ implies $A \cap B = A$ **AND** $A \cap B = A$ implies $A \subseteq B$.

Assume that $A \subseteq B$. We must show $A \cap B = A$. I.e. we must show (1) $A \cap B \subseteq A$ and (2) $A \subseteq A \cap B$. The first statement is trivial, it is always the case that $A \cap B \subseteq A$. For the second statement, assume $x \in A$. We must show $x \in A \cap B$. Since $A \subseteq B$, $x \in B$. Hence $x \in A \cap B$.

Assume $A \cap B = A$. We must show $A \subseteq B$. Let $x \in A$. Then $x \in A \cap B$ since $A = A \cap B$. Hence $x \in B$. QED

Suppose that $f : A \to B$. Then, we have the following

1. If $X \subseteq A$ and $Y \subseteq A$, then $f(X \cap Y) \neq f(X) \cap f(Y)$.

   **Proof.** Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. And $f : A \to B$ be defined as follows: $f(1) = c$, $f(2) = b$ and $f(3) = c$. Let $X = \{1, 2\}$ and $Y = \{2, 3\}$. Then $X \cap Y = \{2\}$ and $f(X \cap Y) = f(\{2\}) = \{f(2)\} = \{b\}$. But, $f(X) \cap f(Y) = \{f(1), f(2)\} \cap \{f(2), f(3)\} = \{c, b\} \cap \{b, c\} = \{b, c\}$. Hence, $f(X \cap Y) \neq f(X) \cap f(Y)$. QED

   It is true that for any function $f : A \to B$ and all subsets $X, Y \subseteq A$, $f(X \cap Y) \subseteq f(X) \cap f(Y)$ (for a proof see below).

2. If $X \subseteq A$, $Y \subseteq A$ and $f$ is 1-1,then $f(X \cap Y) = f(X) \cap f(Y)$.

   **Proof.** Suppose that $f : A \to B$ is a 1-1 function. Let $X \subseteq A$ and $Y \subseteq A$. We must show (1) $f(X \cap Y) \subseteq f(X) \cap f(Y)$ and (2) $f(X) \cap f(Y) \subseteq f(X \cap Y)$.

   Notice that (1) is true even if $f$ is not 1-1. Let $y \in f(X \cap Y)$. Then there is an element $x \in X \cap Y$ such that $f(x) = y$. Since $x \in X \cap Y$, $x \in X$

[2]NOTICE that $x \notin A \cap B$ **DOES NOT IMPLY** $x \notin A$ *and* $x \notin B$. The "and" in italics is shold be an "or". Make sure you clearly understand the logic here, since this is often misunderstood by students.

and $x \in Y$. Therefore, $y = f(x) \in f(X)$ and $y = f(x) \in f(Y)$. Hence, $y \in f(X) \cap f(Y)$.

We now prove (2). Let $y \in f(X) \cap f(Y)$. Then $y \in f(X)$ and $y \in f(Y)$. Since $y \in f(X)$ there is $x_1 \in X$ such that $f(x_1) = y$. Since $y \in f(y)$, there is $x_2 \in Y$ such that $f(x_2) = y$. Since $f$ is 1-1, $x_1 = x_2$. Therefore $x_1 = x_2 \in X \cap Y$; and so, $y = f(x_1) = f(x_2) \in f(X \cap Y)$. QED

3. If $X \subseteq B$ and $Y \subseteq B$, then $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.

**Proof.** Let $f : A \to B$ be any function and suppose $X \subseteq B$ and $Y \subseteq B$. We must show $f^{-1}(X \cap Y) \subseteq f^{-1}(X) \cap f^{-1}(Y)$ and $f^{-1}(X) \cap f^{-1}(Y) \subseteq f^{-1}(X \cap Y)$.

Suppose $x \in f^{-1}(X \cap Y)$. Then $f(x) \in X \cap Y$. Hence $f(x) \in X$ and $f(x) \in Y$. Since $f(x) \in X$, $x \in f^{-1}(X)$. Since $f(x) \in Y$, $x \in f^{-1}(Y)$. Therefore $x \in f^{-1}(X) \cap f^{-1}(Y)$.

Suppose $x \in f^{-1}(X) \cap f^{-1}(Y)$. Then $x \in f^{-1}(X)$ and $x \in f^{-1}(Y)$. Therefore, $f(x) \in X$ and $f(x) \in Y$. Hence, $f(x) \in X \cap Y$; and so, $x \in f^{-1}(X \cap Y)$. QED