Handout # 4
A Few Facts about Sets, Functions and Induction

COMP 321
Wesleyan University

February 24, 1998

1 What is a set?

This is a difficult question to answer in a non-circular way. To say:

A set is a collection of objects

doesn't really tell us very much. After all...what's a collection?...What's an object?

Before proceeding, a word of warning. In our definitions we are going to be a little cautious in a way that reflects a pragmatic prejudice of modern mathematics not shared by the ancient Greeks. Euclid wrote *a point is that which has no breadth.* While this gives the reader some intuitions about what Euclid had in mind, it is not the kind of definition that can be applied mathematically. What seems to matter in proofs is how points are *used*: how they *interact* with lines or the other objects forming part of the mathematical universe being discussed. You will never find a proof in Euclid which appeals to the fact that a point has no breadth. Only axioms and theorems stating facts about points, lines and angles are used.

Concepts like "point" and "line", which are never explicated in terms of more basic ones, are called primitive notions.

So back to sets: Rather than say what they are, I'll just say how we will *build* them and *use* them, via some axioms. In these axioms we will make use if the membership relation $\in$, a primitive notion. We will write

$$x \in S$$

to mean *x is a member of the set S.*

1. There is a set $\varnothing$, called the empty set, which has no members. A restatement of this axiom as a formal proposition is: $x \in \varnothing \to \perp$.

2. The collection of natural numbers $\mathbb{N} = \{0, 1, 2 \ldots\}$ is a set. Some more sets of numbers we will use are listed after definition (2.1).

3. Two sets are equal if they have precisely the same members. This means that to show two sets A and B equal, we have to show *both* of the following facts:

Whenever $x \in A$ then $x \in B$.
Whenever $x \in B$ then $x \in A$.

4. We say one set A is *contained* in another set B (or is a *subset* of B) if any member of A is also a member of B. We can write this as:

$$A \subseteq B$$

5. Any finite collection $S = \{a_1, a_2, \ldots, a_n\}$ of members of some set is a set. We say the members of the set S are being explicitly displayed in $\{a_1, a_2, \ldots, a_n\}$. Thus $a_1 \in S$, $a_2 \in S$, ..., $a_n \in S$, and nothing else is in S.

   In particular, if a and b are numbers (or sets) then so is $\{a\}$ (the set whose sole member is a) and so is $\{a, b\}$. There is also a special set $\langle a, b\rangle$ called the *ordered pair* of a and b. It is defined thus:

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}.$$

   a and b are called the first and second *components* of $\langle a, b\rangle$. Do not confuse $\langle a, b\rangle$ with $\{a, b\}$. There is no difference between the sets $\{a, b\}$ and $\{b, a\}$ since they both have the same members, but, if a, b are distinct, $\langle a, b\rangle \neq \langle b, a\rangle$ since they do *not* have the same members.

   In fact two ordered pairs $\langle a, b\rangle$ and $\langle a', b'\rangle$ are equal if and only if each of the two components are equal: $a = a'$ and $b = b'$.

6. If A and B are sets then so is $A \cup B$ the *union* of A and B, which is the set of those x which are either members of A or members of B. We write this:

$$A \cup B \stackrel{\text{def}}{\equiv} \{x : x \in A \text{ or } x \in B\}$$

7. If A and B are sets then so is $A \cap B$, the *intersection* of A and B, which is the set of those x which are members of *both* A and B, i.e., $A \cap B \stackrel{\text{def}}{\equiv} \{x : x \in A \text{ and } x \in B\}$.

8. If A and B are sets then so is $A - B$ the *difference* of A and B, which is the set of those X which are in A but not in B.

9. If A is a set so is the *power* set of A, $\wp(A)$, the collection of *all subsets of* A.

10. If A and B are sets, so is the set $A \times B$ (called the Cartesian product of A and B) consisting of all *ordered pairs* $\langle a, b\rangle$ of members of A and of B, i.e.,

$$A \times B \stackrel{\text{def}}{\equiv} \{\langle a, b\rangle : a \in A \text{ and } b \in B\}$$

    Thus, for example $\{1, 2, 3\} \times \{u, v\} = \{\langle 1, u\rangle, \langle 2, u\rangle, \langle 3, u\rangle, \langle 1, v\rangle, \langle 2, v\rangle, \langle 3, v\rangle\}$

Notice that if you lay out the members of $\{1, 2, 3\} \times \{u, v\}$ in a more suggestive manner

$$\begin{array}{ccc} \langle 1, u\rangle & \langle 2, u\rangle & \langle 3, u\rangle \\ \langle 1, v\rangle & \langle 2, v\rangle & \langle 3, v\rangle \end{array}$$

it will be clearer why this set is called a product of $\{1, 2, 3\}$ and $\{u, v\}$. If you think of how we usually visualize $\mathbb{R} \times \mathbb{R}$, where $\mathbb{R}$ is the set of real numbers, namely as the set of points in the plane labelled with x and y co-ordinates, you will see why it is called "Cartesian".

2 What is a function?

Functions are probably the most important objects in mathematics. Functions can be thought of as operations taking inputs and producing outputs. How do we make precise what we mean by function? Here are two stabs at a definition:

Functions are "rules" (new objects in our universe): A function is a rule f associating with every member (input) a of some set A a *unique* member (output) $f(a)$ of another set B. For example, the rule

$$f(x) = \frac{x-1}{x}$$

associates a unique *rational* , output 6/7 to the *natural number* input 7. It associates a unique output to every member of the set of real numbers $\mathbb{R}$except 0. Notice that the rule $f(x) = x^2$ associates a unique output to every input, but *not the other way around.* Both inputs 3 and -3 are sent to the same output 9. We will write $f : A \to B$ to indicate that f is a function from A to B.

Functions are special kinds of sets: A function f from a set A to a set B is often defined as a *set of ordered pairs* $\langle a, b\rangle$ where $a \in A$ and $b \in B$, satisfying the following *requirements* :

Every member a of A shows up as the first coordinate of some pair $\langle a, b\rangle$ *exactly once.*

This rather abstract-looking definition says that a function is really just a table of $x - y$ values. In other words, for example, the squaring function $f : \mathbb{N} \to \mathbb{N}$ given by the rule $f(x) = x^2$ is just a set of input-output pairs $\{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 4\rangle, \langle 3, 9\rangle \ldots\}$. This is just a way of formalizing in set theory the familiar description of a function as a *table*:

$$\begin{array}{ccc} x & & f(x) \\ \hline 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 9 \\ & \vdots & \end{array}$$

and so on...

A question to think about: are both definitions of function equivalent? What does each approach suggest about how we might define two functions to be equal?

And now, some more facts about functions.

Definition 2.1 *If f is a function from the set A to the set B, we call A the* **domain** *of F and B the* **range** *or* **codomain** *of F. A function $f : A \to B$ is* **one-to-one** *if every member of the domain is sent to a different member of the range, i.e.,* if

$$x \neq y \Rightarrow f(x) \neq f(y)$$

A function is **onto** *its range (or just "onto") if every member y of the range is the image $f(x)$ of some member X of the domain.*

Officially, the domain and range of a function are considered part of its definition[1].

Some examples. We will make use of the following sets of numbers that you may recall from high-school algebra:

1. $\mathbb{N}$= the set of *natural numbers* $\{0, 1, 2, 3, \ldots\}$
2. $\mathbb{Z}$ =the *integers* $\{\ldots, -2, -1, 0, 1, 2, 3, \cdots\}$
3. $\mathbb{Q}$= the *rational numbers* $\{\frac{p}{q} : p, q \in \mathbb{Z}\}$.
4. $\mathbb{R}$= the *real numbers*
5. $\mathbb{R}^+$ = the *non-negative real numbers*
6. $\mathbb{C}$= the *complex numbers* $a + bi : a, b \in \mathbb{R}$

Consider the squaring function $f(x) = x^2$ from the domain $\mathbb{Z}$ to the range $\mathbb{Z}$ (we write this $f : \mathbb{Z} \to \mathbb{Z}$). Is it *one-to-one?* No, since $f(-1) = f(1)$. Is it *onto?* No, since nothing is mapped to -1. (That is to say, -1 is the square of no integer).

Now consider the same rule f with a different domain and range.

- $f : \mathbb{N} \to \mathbb{Z}$ is certainly *one-to-one* but not onto.
- $f : \mathbb{N} \to \mathbb{N}$ is *one-to-one* but not onto.
- $f : \mathbb{R} \to \mathbb{R}$ is not one-to-one nor onto.

What about $f : \mathbb{R}^+ \to \mathbb{R}^+$ or $f : \mathbb{C} \to \mathbb{C}$?

3 Equivalence Relations

Let S be a set. A (binary) *relation R on S* is a set of ordered pairs $\langle a, b\rangle$ with $a \in S$ and $b \in S$. In other words, it is any subset of $S \times S$. This is a way of formalizing such relationships

[1] Thus, strictly speaking, the squaring operation from $\mathbb{N}$ to $\mathbb{N}$ is a different function from the squaring operation from $\mathbb{R}$ to $\mathbb{R}$.

between things, such as as "__ is greater than __" on the natural numbers $\mathbb{N}$. Formally, the "is greater than" relation on $\mathbb{N}$ can be treated as a the set

$$> \stackrel{\text{def}}{\equiv} \{\langle 1,0\rangle, \langle 2,0\rangle, \langle 3,0\rangle, \ldots, \langle 2,1\rangle, \langle 3,1\rangle, \ldots\}$$

i.e., it's the set of all ordered pairs of natural numbers $\langle n,m\rangle$ with $n > m$. The statement $\langle x,y\rangle \in R$ is often written xRy.

Definition 3.1 *A relation R on a set S is* **reflexive** *if for every $x \in S$, $\langle x,x\rangle \in R$, i.e., if every member of S is R-related to itself. (Example: the identity relation "=" is reflexive on on $\mathbb{N}$, since $x = x$ is always true.) A relation R is* **symmetric** *if whenever xRy we must also have yRx. (Examples: equality, "__ is a sibling of __"). A relation is* **transitive** *if whenever xRy and yRx then xRz.*

for example: if Joe is a sibling of Mary and Mary is a sibling of Fred then Joe is a sibling of Fred. [2]

Consider the relation "$\leq$" on $\mathbb{Z}$ for example. Is it reflexive? transitive? symmetric? Let n be any natural number. Let $\stackrel{n}{\sim}$ be the relation

$$x \stackrel{n}{\sim} y \stackrel{\text{def}}{\equiv} (x-y) \text{ is divisible by } n$$

So, for example $1 \stackrel{12}{\sim} 13$, but it is not the case that $3 \stackrel{12}{\sim} 10$ or that $1 \stackrel{5}{\sim} 13$.

Definition 3.2 *A relation R on a set S is an* **equivalence relation** *if it is reflexive, symmetric and transitive. If R is an equivalence relation on S, and $x \in S$, we define the* **equivalence class of** *x, written $[x]_R$, (or just $[x]$ when the context makes R clear), by:*

$$[x]_R \stackrel{\text{def}}{\equiv} \{y : y \in S \textit{ and } xRy\}.$$

Is $\stackrel{n}{\sim}$ an equivalence relation? If R is $\stackrel{4}{\sim}$, then what is $[1]_R$? (This equivalence class is usually written $[1]_4$).

Definition 3.3 *Two sets A and B are* **disjoint** *if $A \cap B = \varnothing$. If S is a set, we say that a collection of sets $\{S_1, S_2, \ldots, S_n, \ldots\}$ is a* **partition** *of S if $S_1 \cup S_2 \cup \ldots \cup S_n \cup \ldots = S$ but any two members S_i, S_j of the collection are disjoint.*

All this says is that a partition of a set is a breaking up of the set into distinct pieces. For example:

$$\begin{aligned} [0]_2 &= \{0, 2, 4, 6, \ldots, 2n, \ldots\} \\ [1]_2 &= \{1, 3, 5, 7, \ldots, 2n+1, \ldots\} \end{aligned}$$

is a partition of $\mathbb{N}$ into evens and odds. Can you think of other partitions?

[2] We have to allow people to be their own siblings, or transitivity will be violated.

Lemma 3.4 *If R is an equivalence relation, then xRy iff $[x] = [y]$.*

Lemma 3.5 *If R is an equivalence relation on S, it* **partitions** *S into the equivalence classes $\{[x] : x \in S\}$.*

A simple example of what's going on: consider the equivalence relation: "x can be reached on land from y" defined on the set S of all points on land on planet earth. Convince yourself that this is an equivalence relation. What are the equivalence classes? The continents!

The converse of the preceding lemma is also true: If P is a partition of S then P automatically induces an equivalence relation given by

$$x \simeq y \quad \text{if } x \text{ and } y \text{ are in the same component of } P.$$

A final fact before we go on to another topic. The equivalence relation $x \overset{n}{\sim} y$ defined above is officially written:

$$x \equiv y (mod n)$$

and is described by: "x is **congruent** to y mod n". Thus, the fact that "1300 hours" is really[3] one o'clock is just a restatement of: $13 \equiv 1(mod 12)$.

4 Cardinality

Cardinality is another name for the *size* or number of elements in a set. First we will discuss finite sets, and then we will try to extend the notion of cardinality to infinite ones, with surprising results. In what follows, we will be using the word **bijection** to refer to a function that is one-to-one and onto. These functions play a central role in talking about cardinality.

Definition 4.1 *Let n be a natural number. We will let I_n denote the set $\{1, 2, \cdots, n\}$. The sets I_n are called the* initial segments *of the natural numbers $\mathbb{N}$. We say that a set A* **has cardinality n** *and write*

$$|A| = n$$

if there is a bijection from I_n to A. We say that A **has at least n** *members if there is a one-to-one function $f : I_n \to A$ and that A has* **at most n** *members if there is a one-to-one function $g : A \to I_n$. Given any two sets A and B we say A and B* **have the same cardinality**, *and write*

$$A \equiv B$$

if there is a bijection from A to B. We say A is no greater than B and write

$$A \preceq B$$

if there is a one-to-one function $g : A \to B$.

[3] in military circles...

We now introduce several new operations on sets, called *exponentiation* and *sum* or disjoint union.

Definition 4.2 *Let A and B be sets. The we define B^A to be the set of functions from A to B:*

$$B^A = \{f \mid f : A \to B\}.$$

This set is sometimes also written $[A \Rightarrow B]$. We also define the **disjoint union** *of A and B, written $A \sqcup B$ or just $A + B$ to be the set*

$$\{\langle 0, a\rangle : a \in A\} \cup \{\langle 1, b\rangle : b \in B\}.$$

Notice that disjoint union, like union, brings together the members of two sets, but first *marks* them so that if an element x is in A and also in B it will show up in $A + B$ as two different elements $\langle 0, x\rangle$ and $\langle 1, x\rangle$.

Here are a few problems about some of the set-theoretic ideas we've been studying. Assume that some large set U has been defined at the outset, and that all sets mentioned below are subsets of U. Such a set is usually called the "universe of discourse". Given some universe of discourse U, it is customary to define $\bar{A}$, the *complement* of A, to mean $U \setminus A$.

Problem 1 *Prove the following:*

1. $A \subseteq A \cup B$.
2. $A \cap B \subseteq A$.
3. $A \cap \bar{A} = \varnothing$
4. $A \cup A = A$
5. $A = A \cup (A \cap B)$
6. $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Problem 2 *Show that $(A \times (B \times C))$ and $((A \times B) \times C)$ have the same cardinality. Show $A \times B \equiv B \times A$. Also show that $\equiv$ is a symmetric and transitive relation, i.e. that if $A \equiv B$ then $B \equiv A$, and if $A \equiv B$ and $B \equiv C$ then $A \equiv C$.*

Problem 3 *Show that $|A + B| = |A| + |B|$ and that $|A \times B| = |A| \times |B|$.*

Problem 4 *Prove that*

$$A \times (B + C) \equiv A \times B + A \times C.$$

5 The Least Number Principle and Induction

We close this handout on sets with a discussion of some principles that will play an important role in the material that lies ahead. We begin with the so-called *least number principle*, which we will take as an axiom.

Axiom **LNP***:* *Suppose* S *is a* **nonempty** *subset of* $\mathbb{N}$*. Then* S *has a least member* r_o*.*

This seems simple enough, but it will turn out to have surprisingly interesting consequences The first, and most famous one is the so-called *induction axiom.*

5.1 Inductive arguments

Imagine a ladder stretching up into the clouds, and going on forever. Suppose that its first rung is marked with a 1, its second rung marked with a 2 and so on: every rung has a natural number associated with it, in ascending order. Now suppose that I take a (large) bucket of red paint and a brush and carry out the following instructions.

1. I paint rung# 1.

2. Whenever I've finished painting rung # x, I paint rung # x+1.

It might take a while to carry out such instructions...but we are already being asked to accept infinite ladders...so why not imagine that I *do* finish my task. Will I have painted every rung in the ladder? Could I have missed some? If you believe I got them all then you believe the principle of *induction*, which says that the collection of numbers containing 0 and having the property that

$$\textit{if } x \textit{ is in the collection then so is } x+1$$

must in fact contain all the natural numbers. In symbols:

$$0 \in S \wedge \text{ for every } x \ \ (x \in S \rightarrow x+1 \in S) \rightarrow \text{ for every x } x \in S$$

Put another way...if you want to show all numbers have a certain property it suffices to show that 0 has the property and that whenever x has the property so does $x+1$. We'll illustrate with an example: here's a nice fact about numbers and its proof by induction:

The sum of the first n *odd numbers is equal to* n^2*.*

proof: We will show that *every natural number* n *has the property*

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

by showing that 0 has the property, i.e. that $P(0)$ holds (called the *base case* of the induction) and by showing that

$$\textit{If } \ P(x) \qquad \textit{then } P(x+1)$$

called the *inductive step or case*.

Base case: $P(0)$ is the statement: the sum of the first 0 odd numbers is 0^2. So it is true.

inductive step: Suppose

$$P(n) : 1 + 3 + \cdots (2n - 3) + (2n - 1) = n^2 \tag{1}$$

is true. Then

$$1 + 3 + \cdots + (2n - 3) + (2n - 1) + \mathbf{(2n + 1)} = n^2 + (2n + 1).$$

But the right-hand side is equal to $(n + 1)^2$, so the claim $P(n + 1)$ is also true. *By induction*, the property $P(n)$ holds for every n. ▮

It's time to define a bit more precisely the principle we've been using.

Definition 5.1 (The Principle of Mathematical Induction) *Let $P(x)$ be a property of natural numbers x. If $P(0)$ is true and for every natural number x,*

$$P(x) \to P(x + 1)$$

then every natural number has property P.

And now for the first interesting consequence of the least number principle.

Theorem 5.2 *Induction follows from axiom* **LNP**.

proof: Suppose $P(0)$ is true and that for every natural number x,

$$P(x) \to P(x + 1). \tag{2}$$

We want to show $P(x)$ holds for every x. Suppose not. Then B, the set of "bad" numbers: $\{x \in \mathbb{N} : \neg P(x)\}$ is nonempty. By the least number principle, B has a least element b_o. But b_o can't be 0, since $P(0)$ holds. So then b_o must be $x + 1$ for some $x \in \mathbb{N}$. x cannot be in B since it is smaller than b_o, so $P(x)$ must hold. By (2) $P(x) \to P(x + 1)$, so $P(b_o)$ holds, a contradiction. So our supposition, that $P(x)$ fails to hold for some x, was false. ▮

Problem 5 *Analyze the preceding proof, and show what natural deduction rules were used.*