Notes 5

8 Sets

A *set* is a collection of objects. The order of elements is not important and including the same object more than once is redundant.

- $\{1, 2, 3\}$.
- ϕ the *empty set*.
- $\{\phi\}$.
- $\{1, \{1, 2\}\}$.
- $\{n \in \mathbb{N} \mid n \text{ is even }\}$.

We say that $a \in A$ ("a is in A" or "a is an element of A") if a is an object in the set A. The empty set satisfies the proposition $(\forall x)x \notin \emptyset$.

Set theory is perhaps the most fundamental part of mathematics: almost everything else (such as the Peano axioms) can be formulated as theorems within set theory. Set theory can be done in an *extremely* formal way, starting with a collection of axioms that seem ridiculously obvious (but aren't):

- The *axiom of extensionality* says that two sets are equal iff they have the same elements.
  - $\{n \in \mathbb{N} \mid 2 \text{ divides } n\} = \{2n \mid n \in \mathbb{N}\}$.
- The *axiom of comprehension* says that we can form a new set by including all objects of a given set that share a common property. For example,
  - $\{x \in \mathbb{R} \mid P(x)\}$ where $P(x) =$ "x is rational" denotes the set of all rational numbers.

  Set builder notation above may implicitly use a universe of discourse, like our predicate quantifiers.

We say that $A \subseteq B$ ("A is a subset of B") if every element of A is also an element of B (that is, $(\forall x)(x \in A \implies x \in B)$).

We say that A is a *proper* subset of B ($A \subset B$) if $A \subseteq B$ and $A \neq B$.

Note $(\forall X)\emptyset \subseteq X$

Can we have both $A \in B$ and $A \subseteq B$?

Theorem 8.1 *$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

This observation is very important as it provides a simple way to prove that 2 sets are equal.

The size of a set A (the number of elements it contains) is written $|A|$.

8.1 Set operations

There are several standard operations on sets. In axiomatic set theory, the claim that these operation yield new sets is an axiom.

1. $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$. *union*
2. $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$. *intersection*
3. $A - B = \{x \mid x \in A \text{ and } x \notin B\}$. *difference*. Also $A \setminus B$.
4. $A^c = \{x \mid x \notin A\}$. *complement*. Also $\bar{A}$.
5. $A \oplus B = A \cup B - A \cap B$. *symmetric difference*

Union and intersection can be applied to more than two sets. Given a collection of sets A_i, $i = 1, \ldots, n$,

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

is the set of elements in at least one of the A_i. Intersection for multiple sets is defined similarly. If $\mathcal{S}$ is a *set of sets*, then

$$\bigcap \mathcal{S}$$

denotes the intersection of all the sets in $\mathcal{S}$.

Complement is different from all the other operations, because it assumes some universe where we can find the things not in A. This universe is often implicit, like the universe of discourse for predicate logic. In this way, all sets in consideration are supposed to be subsets of Ω. For example, $A^c = \Omega - A$.

Correspondence between set operations and logical operations; sets and predicates.

8.1.1 Power Set

Another very important operation on sets is that of the *power set* of a given set A. It is denoted by $\mathcal{P}(A)$ and consists of the set of all subsets of A. In other words, $\mathcal{P}(A) = \{x \mid x \subseteq A\}$. In particular, for any set A, $\phi \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$.

If $A = \{1, 2\}$ then $\mathcal{P}(A) = \{\phi, \{1\}, \{2\}, \{1, 2\}\}$.

Theorem 8.2 *If A has n elements, then $P(A)$ has 2^n elements.*

Proof. Induction. ■

In fact, $\mathcal{P}(A)$ is sometimes denoted 2^A.

8.2 Proving Set Identities

Theorem 8.3 $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$

Proof. We show equality by proving each is contained in the other.

- $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Suppose $x \in A \cup (B \cap C)$. Then by definition, $x \in A$ or $x \in (B \cap C)$. We argue by cases. If $x \in A$, then by definition $x \in A \cup B$ and similarly $x \in A \cup C$. It follows by definition of intersection that x is in the intersection of these two sets.
- $A \cup (B \cap C) \supseteq (A \cap B) \cup (A \cap C)$. Suppose $x \in (A \cup B) \cap (A \cup C)$. It follows that $x \in A \cup B$ and $x \in A \cup C$. We argue by cases. If $x \in A$, then certainly $x \in A \cup (B \cap C)$. So suppose $x \notin A$. Then since $x \in A \cup B$, we know $x \in B$. Similarly, $x \in C$. Therefore, $x \in B \cap C$. It follows that $x \in A \cup (B \cap C)$.

■

Theorem 8.4 *De Morgan's rule:* $(A \cup B)^c = A^c \cap B^c$.

Proof. We have to show that $(A \cup B)^c \subseteq A^c \cap B^c$ and that $A^c \cap B^c \subseteq (A \cup B)^c$.

1. $(A \cup B)^c \subseteq A^c \cap B^c$: Let $x \in (A \cup B)^c$. Then by definition $x \notin A \cup B$. It follows (proof by contradiction) that $x \notin A$ and $x \notin B$. In other words, $x \in A^c$ and $x \in B^c$. Therefore, by definition, $x \in A^c \cap B^c$.

2. $A^c \cap B^c \subseteq (A \cup B)^c$: Let $x \in A^c \cap B^c$. Then x is in A^c and in B^c. Therefore, x is in neither A nor B and therefore not in $A \cup B$. We conclude that $x \in (A \cup B)^c$.

■

The above two theorems have *dual theorems* produced by swapping $\cap$ and $\cup$.

Theorem 8.5 $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$

Theorem 8.6 $(A \cap B)^c = A^c \cup B^c$.

8.3 Russell's paradox

We might think that set theory is obvious, but this is not the case. Consider the set $S = \{X \mid X \text{ is a set}\}$. This seems like a perfectly reasonable set (well, maybe a bit strange—note $S \in S$). If our set theory allows for such an entity, we get into trouble as follows.

Consider the set $Q = \{x \mid x \text{ is a set and } x \notin x\}$ (note $Q \subseteq S$). Clearly, the set $A = \{1, 2, 3\}$ is not an element of itself so that $A \in Q$. Also, the set $P = \{$ all infinite sets$\}$ is infinite and therefore $P \in P$ so that $P \notin Q$. The question is: is $Q \in Q$?

1. If $Q \in Q$ then $Q \notin Q$, a contradiction.
2. If $Q \notin Q$ then $Q \in Q$ also a contradiction.

This is clearly a paradox. In fact, this paradox was a blow to the then current attempts to formalize all of mathematics ($\sim$1900). Mathematicians had to work very hard to find a consistent set of axioms (note a consistent set of axioms does not allow this paradox to arise). The problem with naive set theory is that you can form a set by describing its members, as we did for Q above. Axiomatic set theory has a specific set of rules for how you can form sets—rules that don't allow the set Q above to specified, and therefore avoid the paradox.

8.4 Cartesian products

Another important set operation is the *Cartesian product*. For sets A and B define $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$. Here, (a, b) is considered an *ordered* pair so that $(a, b) \neq (b, a)$.

Example 1 If $A = \{0, 1\}$ and $B = \{a, b\}$ then $A \times B = \{(0, a), (0, b), (1, a), (1, b)\}$.

Order is important! In the above example, $(a,0) \notin A \times B$, though $(a,0) \in B \times A$. We can generalize Cartesian products to apply to more than 2 sets and define $A_1 \times \cdots \times A_k = \times_{i=1}^{k} A_i = \{(a_1, \cdots, a_k) \mid a_i \in A_i \text{ for } 1 \leq i \leq k\}$ (note Cartesian product is associate *up to isomorphism*). Also, we write A^k for $\times_{i=1}^{k} A$.

- $\{0,1\}^n$ is the set of all n-tuples of 0's and 1's.
- $\Re^2$ is the real plane.

9 Relations

A *binary relation* from a set A to a set B is a subset $R \subseteq A \times B$. A binary relation *on* a set A is a subset $R \subseteq A^2$. We can write $a \sim_R b$ or aRb if $(a,b) \in R$.

We can also define a *ternary* relations as a subset $R \subseteq A^3$ or, in general, a k-ary relation as a subset $R \subseteq A^k$.

1. flight schedules.
2. The relation "is taking class" as a subset of $\{$students at MIT$\} \times \{$classes at MIT$\}$. extra info?
3. The relation "is living in the same room as" is a subset of $\{$students at MIT$\} \times \{$students at MIT$\}$
4. The relation "can drive from first to second city"
5. Relation "are connected by a wire"
6. "meet one another on a given day"
7. "likes"
8. Let $A = \mathbb{N}$ and define $a \sim_R b$ iff $a \leq b$.
9. let $A = \mathcal{P}(\mathbb{N})$ and define $a \sim_R b$ iff $|a \cap b|$ is finite.
10. Let $A = \Re^2$ and define $a \sim_R b$ iff $d(a,b) = 1$.
11. Let $A = \mathcal{P}(\{1, \cdots, n\})$ and let $a \sim_R b$ if $a \subseteq b$.

9.1 Properties of Relations

A binary relation R on A is:

1. *reflexive* if for every $a \in A$, $a \sim_R a$.
2. *symmetric* if for every $a, b \in A$, $a \sim_R b$ implies $b \sim_R a$.
3. *antisymmetric* if for every $a, b \in A$, $a \sim_R b$ and $b \sim_R a$ implies $a = b$.
4. *transitive* if for every $a, b, c \in A$, $a \sim_R b$ and $b \sim_R c$ implies $a \sim_R c$.

Among out examples,

- Relation 5 is symmetric but not transitive. Whether it is reflexive is open to interpretation.
- Relation 3 above is reflexive, symmetric and transitive.
- Relation 10 is only symmetric.
- Relation 11 is reflexive, antisymmetric and transitive.

9.2 Representation

Lists, Matrices, Graphs.

Reflexivity, symmetry, transitivity in each representation.

Examples using divisibility relation.

9.3 Composition

A *composition* of relations $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$ is the relation $R_1 \circ R_2 = \{(a, c) \mid (\exists b)((a, b) \in R_1) \wedge ((b, c) \in R_2)\}$.

Composition of relations is equivalent to matrix multiplication, with $+$ replaced by $\vee$ (Boolean or) and $*$ replaced by $\wedge$.

Examples: composition of parent-of relation with itself gives grandparent-of. Composition of parent-of relation with child-of relation gives sibling-of relation.

The composition $A \circ A$ of A with itself is written A^2; similarly A^n denotes A composed with itself n times (recursive definition: $A^n = A \circ A^{n-1}$).

Lemma 9.1 $A \circ (B \circ C) = (A \circ B) \circ C$

Theorem 9.2 *For* $n > 1$, $R^n = R^{n-1} \circ R$

Proof. By induction on n. Base case $n = 2$ trivial. Suppose $(a, b) \in R^n$. Then $(\exists a')((a, a') \in R) \wedge (a', b) \in R^{n-1}$. By induction, $(\exists b')((a', b') \in R^{n-2}) \wedge ((b', b) \in R)$. It follows that $(a, b') \in R^{n-1}$. Therefore, $(a, b) \in R^{n-1} \circ R$. ■

Theorem 9.3 *R is transitive if and only if $R^n \subseteq R$ for all integers n.*

Proof. (If part) If $R^n \subseteq R$ for every n, then $R^2 \subseteq R$. Follows that R is transitive.

(Only if part) By induction. Base case easy. Suppose $R^n \subseteq R$. Show $R^{n+1} \subseteq R$. Say $(a, b) \in R^{n+1}$. Then $(a, c) \in R^n$ and $(c, b) \in R$ for some c. Then $(a, c) \in R$ by induction. This by transitivity $(a, b) \in R$. ■

10 Equivalence relations and partitions

An *equivalence* relation is a relation which is reflexive, symmetric and transitive. For example, the first relation above is an equivalence relation. A trivial example is the "=" relation. One interesting fact about equivalence relations is that they partition the universe in a very natural way. Given a set A, a *partition* is a collection of subsets $\{A_1, \cdots, A_k\}$ such that any two of them are disjoint (for any $i \neq j$, $A_i \cap A_j = \phi$) and such that their union is A. That is, every element of A is in exactly one subset.

Fix an equivalence relation R on A. For an element $a \in A$, let $[a]$ denote the set $\{b \in A \mid a \sim_R b\}$. We call this set the *equivalence class of a under R*. We claim that the sets $[a]$ for $a \in A$ constitute a partition of A.

Lemma 10.1 *For every $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \phi$.*

Proof. Fix $a, b \in A$. If $[a] = [b]$ then we are done. Otherwise, suppose that c is an element in only one set (suppose that $c \in [b] - [a]$). If $[a] \cap [b] = \phi$ then we are done. Otherwise, suppose that $d \in [a] \cap [b]$. We will get a contradiction by showing that $a \sim_R c$ and therefore that $c \in [a]$. First, $a \sim_R d$ because $d \in [a]$ (note that $d = a$ is a possibility but this is ok because R is reflexive). Second, $d \sim_R b$ and $b \sim_R c$ because both $c, d \in [b]$ and R is symmetric. This implies, by transitivity, that $d \sim_R c$. Finally, by transitivity, $a \sim_R c$ because $a \sim_R d$ and $d \sim_R c$. ■

Conversely, any partition $\{A_1, \cdots, A_k\}$ of A defines an equivalence relation by letting $a \sim_R b$ iff a and b are in the same A_i. Therefore, we can look at partitions and at equivalence relations as different versions of each other.

10.1 Integers modulo m

In the previous lecture, we considered the modulo operation as a function. A cleaner way to think of it is as a definition of equivalence classes of natural numbers. Consider the following definition.

Definition 10.2 *We say* $a = b \pmod{m}$ *if* $m \mid (a - b)$.

An equivalent formulation says that $a = b + km$ for some integer k.

Theorem 10.3 *Equality modulo m is an equivalence relation.*

Proof. We need to show the relation is reflexive, symmetric, and transitive.

reflexive Clearly $m \mid 0 = a - a$, so $a = a \pmod{m}$.

symmetric If $a = b + km$ then $b = a + (-k)m$.

transitive If $a = b \pmod{m}$ and $b = c \pmod{m}$, this means that $m \mid (a-b)$ and $m \mid (b-c)$. It follows from a theorem in the previous lecture that $m \mid (a - c) = (a - b) + (b - c)$.

■

The equivalence class of a is simply the set $[a] = \{km + a \mid k \in \mathbb{Z}$.

It turns out that we can perform a lot of standard arithmetic modulo m. That is, we can *extend* the standard notions of sum and product to the equivalence classes mod m. For example, we can define $[a] + [b]$, given two equivalence classes mod m, to be the equivalence class $[a + b]$. This is not as obvious as it seems: notice that the result is given in terms of a and b, two selected representative from the equivalence classes, but that it is supposed to apply to the equivalence classes themselves. To prove that this works, we have to show that it doesn't matter which representative of the equivalence class we choose.

Lemma 10.4 *If* $a = x \pmod{m}$ *and* $b = y \pmod{m}$ *then* $(a + b) = (x + y) \pmod{m}$.

Proof. $m \mid (a - x)$ and $m \mid (b - y)$ so $m \mid ((a - x) + (b - y)) = (a + b) - (x + y)$, ■

It follows that if we are interested only the result of the addition modulo m, which is the case, for example, in the RSA cryptosystem, that we can at any time replace a given number with a different number equivalent to it, without changing the value (equivalence class) of the final answer.

The same fact can be proven for multiplication. This is the basis of the fast exponentiation algorithm presented in section.

10.2 Fast Exponentiation

Let's say that we want to compute $a^n \pmod b$. Here's a crude way to do it:

1. Compute a^n.
2. Divide by b and take the remainder.

There are actually two big problems with this. First of all, a^n could be a gigantic number; and secondly, we're using n multiplications, which could take a long time if n is large.

Let's correct the first problem first.

1. Initialize $p = 1$.
2. Repeat n times:
   (i) Set $p \leftarrow ap$.
   (ii) Set $p \leftarrow p \pmod b$.
3. Return p.

To see why this works, we have to use the fact that $x \pmod b * y \pmod b = (x * y) \pmod b$. This can be shown by arguments as in the preceding section of the notes.

Now to reduce the number of multiplications, we try to use squaring whenever possible.

Algorithm `fast-exp(a,n,b)`

1. If $n = 1$ then return $a \pmod b$.
2. Else if n is odd return $a*$ `fast-exp(a,n-1,b)` $\pmod b$.
3. Else (n is even), set $p \leftarrow$ `fast-exp(a,n/2,b)` and return $p^2 \pmod b$.

In recitation, we'll prove a few things about this algorithm — first, that it terminates with the correct answer for $n \geq 1$; and second, that it uses at most $2 \log n$ multiplications (a huge savings over n multiplications even for moderate values of n).