CS/Math 240: Introduction to Discrete Mathematics

Reading 3 : Sets

Author: Dieter van Melkebeek (updates by Beck Hasti and Gautam Prakriya)

In this reading we discuss sets which will serve as the building block for other concepts such as relations, functions, and graphs.

3.1 Sets

We start by defining what a set is.

Definition 3.1. *A* set *is a collection of elements from some domain. A set must be* well-defined*, which means that for every element of the domain, we can tell whether it belongs to the set or not.*

Let A be a set. We use the notation $x \in A$ to mean that x is an element of A. When x is not an element of the set A, we write $x \notin A$.

The next definition captures the notion of containment.

Definition 3.2. *If all elements of some set A also belong to another set B, we say that A is a* subset *of B. Furthermore, if B contains some element that is not in A, we say that A is a* strict subset *of B.*

We write $A \subseteq B$ to mean that A is a subset of B, and use $A \subset B$ to say that the containment is strict. Notice that the set containment symbols $\subseteq$ and $\subset$ resemble the inequality symbols $\leq$ and $<$. This is not a coincidence. Both of these symbols express that one object is, in some sense, "smaller" than some other object. Saying $A \subset B$ means that A is "less than" B in terms of containment.

When we list elements of a set, the order in which we list them does not matter. Thus, the set $B = \{\text{true}, \text{false}\}$ is the same as the set $\{\text{false}, \text{true}\}$. The elements of a set are listed between curly braces and separated by commas.

Sometimes the set has too many elements for us to list them all. In most cases, the set has some defining property. For example, to describe the set A of all natural numbers between 100 and 1000 inclusive, we could write $A = \{x \in \mathbb{N} \mid 100 \leq x \leq 1000\}$ or $A = \{x \mid x \in \mathbb{N} \wedge 100 \leq x \leq 1000\}$. The part of such definition before the $\mid$ symbol tells us what an element is called, and the part after the $\mid$ symbol tells us what properties this element must have in order to be in the set. Some ways to read the $\mid$ symbol is "such that" or "having the property that". For example, we could read our description of A as "the set of integers x such that $100 \leq x \leq 1000$."

The sets A and B we just defined are examples of a *finite sets*. A finite set contains a finite number of elements, which means that we can write them all down, given enough time.

Let's now write the set B, which is sometimes called the *Boolean domain*, in two different ways. This may sound redundant, but it is often convenient to represent the elements in different ways. One instance where multiple representations of sets are helpful is when we want to express operations on their elements in a different way. For example, suppose we represent the Boolean domain using the set $B' = \{0, 1\}$ where 0 means false and 1 means true. The conjunction operator $\wedge$ on elements of B corresponds to multiplication of elements of B'. Yet another way to represent B is as $B'' = \{-1, 1\}$ where -1 represents true and 1 represents false. Multiplication of elements of $B'\prime$ now corresponds to *exclusive or*, which captures the notion that exactly one of two values is true. Thus, an exclusive or is different from the or we used earlier because an or of two values is true even if they are both true.

3.1.1 Cardinality

The cardinality of a set is a measure of its size.

Definition 3.3. *The* cardinality *of a finite set S is the number of distinct elements in S.*

We use the notation $|S|$ to denote the cardinality of a set S.

For example, the cardinality of the Boolean domain B defined earlier is 2 because B has two distinct elements, true and false. Similarly, we have $|B'| = |B''| = 2$.

It may also happen that a set has no elements. If this is the case, we call it an *empty set*, and use the symbol $\emptyset$ to denote it. Note that $|\emptyset| = 0$.

3.1.1.1 Countable Sets

In reading 1 we said that discrete structures were the opposite of continuous. We also mentioned that we could somehow say that something is the first element, something is the second element, and so on. We now make this notion more precise.

Definition 3.4. *A set is* countable *iff*

- *it is finite, or*
- *it is infinite and there is an enumeration consisting exactly of all elements of A. Every position in the enumeration should correspond to a different element of A , and every element of A should appear in it.*

Think of an enumeration as an infinite list of elements of A. This is probably best explained with examples.

Example 3.1: The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ are countable. One enumeration of the natural numbers is 0, 1, 2, 3, ... Notice that number i appears in the $(i+1)$-th position in the enumeration, and, conversely, the i-th position in the enumeration is $i - 1$ which is a natural number. Thus, every position in the enumeration corresponds to a different natural number and all natural numbers appear in the enumeration. It follows that the natural numbers are a countable set. ⊠

Here we should warn the reader that one should be careful when using ellipsis (. . .) as part of a description of a list. It is important that the use of ellipsis is unambiguous and allows for only one logical way of continuing the sequence. Another problem with ellipsis is if we use them at the beginning of a list, as is illustrated in the next example.

Example 3.2: The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ are countable. A first attempt at an enumeration would be to start by listing the smallest elements first and then keep adding one like we did with the natural numbers. Unfortunately, the integers have no smallest element, so we would not know where to start such an enumeration. Instead, we use the enumeration 0, 1, -1, 2, -2, ...

- If i is odd , then the integer that appears at the i-th position is $-(i - 1)/2$. If i is even, then the integer that appears at i-th position is $i/2$. Thus, every position in the enumeration corresponds to a different integer.
- If x is a positive integer $(x > 0)$ then integer x appears at position $2x$ in the enumeration. If x is not a positive integer $(x \leq 0)$ then integer x appears at position $-2x + 1$ (note that this is positive when $x \leq 0$). Thus, every integer appears in the enumeration.

⊠

Even in the example above, we used some kind of a "natural ordering" in the sense that we first listed zero, then one and its additive inverse, then two and its additive inverse, and so on. We may be tempted to try an ordering like that for rational numbers, i.e., the set $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z} \land b \in \mathbb{N} \land b \neq 0\}$. Unfortunately, this is not going to work because for any rational numbers x and y, there is a rational number between them. When this is true for some set, we say that the set is *dense*. For example, $(x+y)/2$ is a rational number, and $x < (x+y)/2 < y$, so the rational numbers are dense. Thus, we cannot hope to enumerate all rational numbers in any sort of "natural ordering". This may lead us to believe that rational numbers are not countable. However, the next proposition tells us otherwise.

Proposition 3.5. *The set of rational numbers is countable.*

Proof. We write the rational numbers in a table. Some table entries may represent the same number, but that is not a problem. Recall that a rational number has the form a/b where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, and $b \neq 0$. Our table has one row for each possible value of a, and one column for each possible value of b. We use the enumeration of integers to decide which order the rows of our table come in because we need to be able to argue that every integer gets a row in our table. The entry corresponding to a's row and b's column is a/b. We show part of the table as Table 3.1a.

$a \setminus b$	1	2	3	4	$\cdots$
0	0	0	0	0	$\cdots$
1	1	1/2	1/3	1/4	$\cdots$
−1	−1	−1/2	−1/3	−1/4	$\cdots$
2	2	1	2/3	1/2	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(a) Part of the table we use for enumerating all rational numbers. The rows correspond to integers, and the columns correspond to positive integers.

$a \setminus b$	1	2	3	4	$\cdots$
0	1	2	4	7	$\cdots$
1	3	5	8	12	$\cdots$
−1	6	9	13		$\cdots$
2	10	14			$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(b) The order in which we traverse Table 3.1a in an attempt to enumerate all rational numbers.

Table 3.1: Enumerating all rational numbers

Observe that every entry in the table is a rational number because only integers are present as row labels, and only positive integers are present as column labels. Now consider any $a/b \in \mathbb{Q}$. Since we have used our earlier enumerations of integers and of positive integers, there is a row of the table labeled with a and a column labeled with b. The corresponding table entry is a/b. Since a/b was an arbitrary rational number, it follows that every rational number is present somewhere in our table.

If we argue that we can traverse our table in a way that eventually visits every table entry, we will have demonstrated an enumeration of the enumeration . The i-th entry in this enumeration will be the i-th *distinct* rational number we visit during our traversal of the table. We cannot traverse our table row by row or column by column because both rows and columns have infinite length. Instead, we choose to traverse the table diagonal by diagonal, where our diagonals go in the "southwest" direction. We show the first few steps of our traversal in Table 3.1b.

Traversing Table 3.1a as shown in Table 3.1b gives us the following list of rationals:

$$0, 0, 1, 0, \frac{1}{2}, -1, 0, \frac{1}{3}, -\frac{1}{2}, 2, \ldots,$$

and we drop all duplicates to get

$$0, 1, \frac{1}{2}, -1, \frac{1}{3}, -\frac{1}{2}, \ldots$$

as our enumeration of the rational numbers. □

Proposition 3.5 may give us hope that we could somehow enumerate the real numbers as well. Unfortunately, this is not possible. We do not give a proof of this. At the end of this reading, a more general argument is presented. This argument when modified appropriately, proves that the real numbers are not countable.

3.1.2 A Remark about Being Well-defined

We conclude the section on sets about with a remark about self-referential statements along the line of the sentence "This sentence is not true," which we introduced in lecture 2. Consider the collection $S = \{A \mid A \notin A\}$, that is, the collection of sets that do not contain themselves. Is $S \in S$? The truth of this statement is actually not defined, which means that we cannot tell whether $S \in S$, so S is not well-defined. This is known as *Russel's paradox*.

3.2 Operations on Sets

We would like to take old sets and make new sets out of them. For example, suppose you have three sets of students stored somewhere in a database.

- U: The set of all students at UW-Madison
- E_1: The set of all students enrolled in CS/Math 240
- E_2: The set of all students enrolled in CS 367

Now you would like to find all members of other sets, an operation that is commonly done in databases.

- S_1: Students who are taking at least one of CS/Math 240 and CS 367
- S_2: Students who are taking both CS/Math 240 and CS 367
- S_3: Students who are not taking CS 367
- S_4: Students who are taking CS/Math 240 but not CS 367

In the language of mathematics, we construct these new sets using Boolean operators similar to the ones we used to make new propositions from old. To get this information out of a database, we would use a query language such as SQL, and construct database queries from our mathematical descriptions of the sets we are interested in.

3.2.1 Boolean Operations on Sets

First let's describe the set S_1 of students who are taking at least one of CS/Math 240 and CS 367. This set contains all elements of E_1 and all elements of E_2. We say that S_1 is the *union* of the sets E_1 and E_2, and write $S_1 = E_1 \cup E_2$. Using set notation developed earlier, we define $E_1 \cup E_2 = \{x \mid x \in E_1 \vee x \in E_2\}$. Note the similarity between the union operator $\cup$ and the disjunction operator $\vee$. In fact, we are using $\vee$ in the definition of the union $E_1 \cup E_2$.

Now let's describe the set S_2 of students who are taking both CS/Math 240 and CS 367. This set contains only those elements of E_1 that are also in E_2. We say that S_2 is the *intersection* of the sets E_1 and E_2, and write $S_2 = E_1 \cap E_2$. We define the intersection of the two sets by $E_1 \cap E_2 = \{x \mid x \in E_1 \land x \in E_2\}$. Again, note the similarity between the intersection operator $\cap$ and the conjunction operator $\land$.

We can use *Venn diagrams* as a convenient way to describe various new sets made out of old sets. We can view these diagrams as the set analog of truth tables for propositions. A Venn diagram consists of multiple closed curves whose insides overlap. We label each closed curve with the name of some set. The inside of the closed curve represents all the elements of the corresponding set, and the outside represents elements that are not members of the set. In Figure 3.1, the set S_1 is represented by the combination of regions (1), (2) and (3), and the set S_2 is represented by region (2). Elements in region (4) don't belong to either E_1 or E_2.

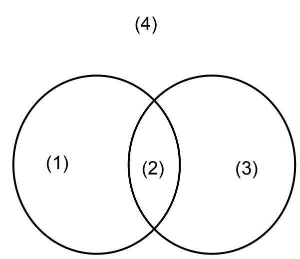


Figure 3.1: Venn diagrams

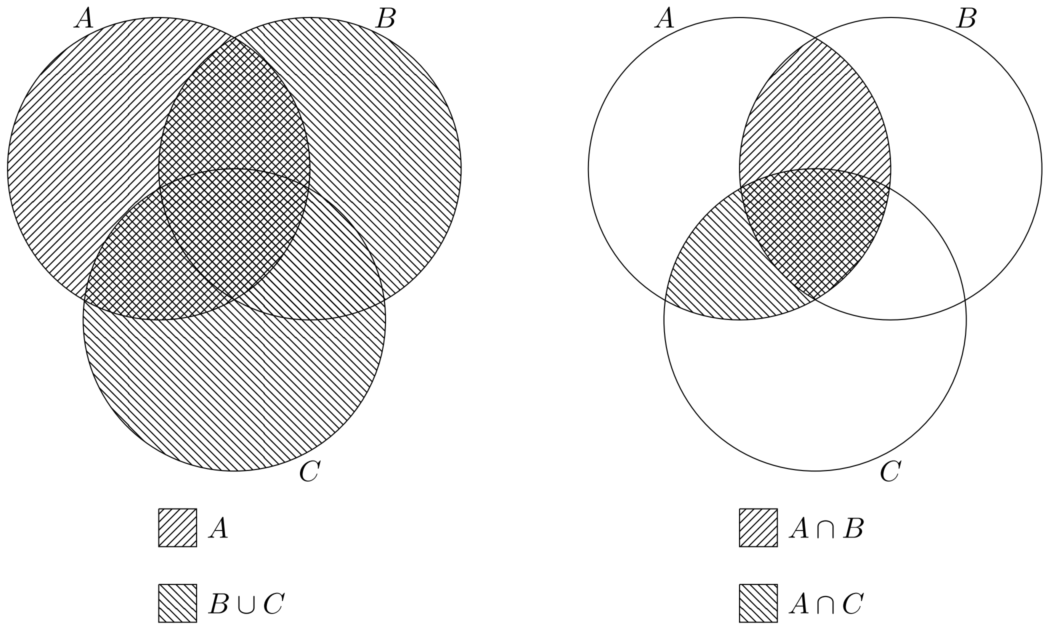
Venn diagrams are convenient, but become way too messy when more than three sets are involved. However, they are useful when fewer sets are involved. For example, we could use Venn diagrams to prove the distributive law for the union and intersection operators.

Proposition 3.6. *Let A, B, and C be sets. Then*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{3.1}$$

Proof. We draw a Venn diagram for both the left-hand side and the right-hand side of (3.1) and see that both sides define the same part of the diagram. The Venn diagrams are in Figure 3.2.

In Figure 3.2a, the area shaded with both kinds of shading is $A \cap (B \cup C)$. In Figure 3.2b, the area with any shading is $(A \cap B) \cup (A \cap C)$. We see that the area shaded with both kinds of shading in Figure 3.2a is the same as the area shaded with some kind of shading in Figure 3.2b, which means that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. □



(a) The region shaded with both kinds of shading is $A \cap (B \cup C)$

(b) The region shaded with at least one kind of shading is $(A \cap B) \cup (A \cap C)$.

Figure 3.2: Diagram for the proof of the distributive law for union and intersection.

Another way to prove Proposition 3.6 is to show that the statements $x \in A \land (x \in B \lor x \in C)$ and $(x \in A \land x \in B) \lor (x \in A \lor x \in C)$ are logically equivalent. In fact, even more is true. For any propositions P, Q and R, the statements $P \land (Q \lor R)$ and $(P \land Q) \lor (P \land R)$ are logically equivalent. This is known as the distributive law for the $\land$ and $\lor$ operators. Viewed differently, our proof of Proposition 3.6 actually proves that distributive law as well.

Let's return to the four sets from the last section. We are now interested in the set of students who are not taking CS 367. This set contains all elements of U that are not in E_2. We say that the set S_3 is the *complement* of E_2 in U, and write $S_3 = \overline{E_2}$. Using set notation, we would write $\overline{E_2} = \{x \mid x \notin E_2\}$.

When we talk about complements, we usually have a particular domain in mind. In our case, the domain is the set of all students at UW-Madison, i.e., the set U. Thus, to be more precise, we should define the complement of E_2 as $\overline{E_2} = \{x \mid x \notin E_2 \land x \in U\}$. This means that if Bob studies at UW-Whitewater, he is not in S_3 even though he is not enrolled in CS 367. It is common to omit the domain when it is understood from context. For example, one could just say that S_3 is the complement of E_2.

Finally, let's describe the set of students who are taking CS/Math 240 but not CS 367. Such students belong to E_1 but not to E_2. We call the set of such students the *set difference* of E_1 and E_2, and write $S_4 = E_1 - E_2$. Using our set notation, we have $E_1 - E_2 = \{x \mid x \in E_1 \land x \notin E_2\}$.

Note that we can describe the complement of a set using set difference. For example, $S_3 = U - E_2$.

3.2.2 Power Sets

Another way to create more sets is to take a set and look at its subsets. The set of all subsets of a set A is called the *power set* of A, and we denote it $\mathcal{P}(A)$. This is a set containing every single subset of A, so $\mathcal{P}(A)$ is a set of sets. Formally, we define $\mathcal{P}(A) = \{S \mid S \subseteq A\}$. This may be confusing at first, but we can list subsets just like we can list elements, so there is nothing new here. Let's see an example.

Example 3.3: Consider the set $B' = \{0, 1\}$ from earlier. Its subsets are the empty set $\emptyset$, the singleton sets $\{0\}$ and $\{1\}$, and the set $\{0, 1\}$. Thus, $\mathcal{P}(B') = \big\{\emptyset, \{0\}, \{1\}, \{0, 1\}\big\}$. ⊠

As we mentioned earlier, we often want to count how many elements a particular set has. Let's do this for the power set. The set $\mathcal{P}(\{0, 1, 2\})$ has cardinality $2^3 = 8$. To see this, note that $\{0, 1, 2\}$ has three elements. For each element, we can choose independently whether to place it in a subset or not, and each set of choices gives us a different subset of $\{0, 1, 2\}$. Thus, we get a total of $2 \cdot 2 \cdot 2 = 2^3 = 8$ different subsets of $\{0, 1, 2\}$, so $|\mathcal{P}(\{0, 1, 2\})| = 8$. In fact, a more general fact is true.

Proposition 3.7. *Let A be a finite set with $|A| = k$. Then $|\mathcal{P}(A)| = 2^k$.*

We do not prove Proposition 3.7 formally right now. It can be proved using induction which we'll talk about next week.

Proposition 3.7 also explains why we sometimes use the notation 2^A instead of $\mathcal{P}(A)$ for the power set of A.

3.2.3 Uncountable Sets

Earlier in this lecture, we stated that the real numbers were not countable. We use power sets to illustrate the technique for proving this. In particular, we show as Theorem 3.8 that the power set of the natural numbers is not countable. The proof we present is our first example of a *proof by contradiction.* In a proof by contradiction, we assume the negation of what we want to prove, and show that this assumption leads to a false statement.

Theorem 3.8. *The power set of the natural numbers, $\mathcal{P}(\mathbb{N})$, is not countable.*

Proof. Assume that $\mathcal{P}(\mathbb{N})$ is countable. This means that there exists some enumeration A_1, A_2, A_3, ... of all subsets of $\mathbb{N}$. We construct a subset $A \subseteq \mathbb{N}$ that is not present in this enumeration.

Consider a table whose rows correspond to subsets in our enumeration, and whose columns correspond to the natural numbers. The table entry in row corresponding to A_i and column j tells us whether $j - 1$ is a member of A_i.

Now let's construct our set A. We put j into A if $j \notin A_{j+1}$, and say that $j \notin A$ if $j \in A_{j+1}$. Hence, we have $A = \{x \mid (x - 1) \notin A_x\}$. This makes A well-defined because membership of j in A is determined only by membership of j in A_{j+1}.

Remember that our enumeration contains all subsets of the natural numbers. This means that $A = A_k$ for some k. But by the way we defined A, $k - 1 \in A$ if and only if $k - 1 \notin A_k$. This means that exactly one of A and A_k contains the element $k - 1$. Therefore, A is actually not A_k. Since k was arbitrary, this means that A is not part of our enumeration. This contradicts the assumption that we had an enumeration of all subsets of the natural numbers, so the assumption must be false. Furthermore, since we chose an arbitrary enumeration, this means that no enumeration of subsets of integers enumerates them all. It follows that $\mathcal{P}(\mathbb{N})$ is not a countable set. □

In the proof above, we showed that for every enumeration of subsets of natural numbers, there is a subset of the natural numbers that is not listed in that enumeration. Note that we are not allowed to make any assumptions about the enumeration besides the fact that it lists all subsets of the natural numbers. Making any additional assumption would result in a proof of the fact that no enumeration satisfying our assumption is an enumeration of all subsets of natural numbers, and that is not good enough.

To give you a better understanding of why our argument works, let's illustrate how it constructs A for one particular enumeration of subsets $\mathbb{N}$. Suppose $A_1 = \emptyset$, $A_2 = \{0\}$, $A_3 = \{1\}$, and $A_4 = \{1, 2, 3\}$ are the first four sets in some enumeration of the subsets of $\mathbb{N}$. Then since $0 \notin A_1$, we put 0 in A, which ensures that $A \neq A_1$. Next, since $1 \notin A_2$, we put 1 in A, and ensure that $A \neq A_2$. This process continues on, preventing all sets in the enumeration from being A. We show part of this process in Table 3.2. We see from Table 3.2 that in order to construct A, we just "flip" the diagonal entries of that table. For this reason, the technique we used in our proof by contradiction is called *diagonalization*.

$a \setminus b$	0	1	2	3	$\cdots$
A_1	**N**	N	N	N	$\cdots$
A_2	Y	**N**	N	N	$\cdots$
A_3	N	Y	**N**	N	$\cdots$
A_4	N	Y	Y	**Y**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
A	Y	Y	Y	N	$\cdots$

Table 3.2: Example of a table used to prove that $\mathcal{P}(\mathbb{N})$ is uncountable. A Y in row corresponding to A_i and column corresponding to j indicates that $j \in A_i$. An N indicates that $j \notin A_i$.

Now we have covered all the necessary tools for the proof that the real numbers are not countable. We leave the actual proof as an exercise for the reader, and only give you a hint: Write the numbers in binary and use diagonalization.