CSE 311: Foundations of Computing I

Set Theory

What is a Set?

Set Theory introduces us to a new type of definition. For any unary predicate $P(x)$, we can define the *set* of elements that satisfy P, which we can write in "set builder" notation as:

$$S ::= \{x : P(x)\}$$

Conversely, each set defines an "element of" predicate, written $x \in S$. This predicate is true iff x is in the set, which occurs exactly when $P(x)$ holds.

Putting these together, we get inference rules that allow us to translate between the conditions of being in the set and of satisfying the underlying predicate:

Def of S
$\dfrac{x \in S}{\therefore \quad P(x)}$

Undef S
$\dfrac{P(x)}{\therefore \quad x \in S}$

We can see that sets and predicates are closely related: we can turn a predicate into a set using "set builder" notation and a set into a predicate using "element of". In some sense, sets are just another way of thinking about predicates, but like any new perspective, they lead to some new ideas.

Set Operations

If A and B are two sets, then we can form new sets from them using set operations:

$A \cap B$	$::= \{x : (x \in A) \wedge (x \in B)\}$	Intersection
$A \cup B$	$::= \{x : (x \in A) \vee (x \in B)\}$	Union
$A \setminus B$	$::= \{x : (x \in A) \wedge \neg(x \in B)\}$	Difference
$A \oplus B$	$::= \{x : (x \in A) \oplus (x \in B)\}$	Symmetric Difference

We can also define a new set from just one set A, namely, the set of elements not in A:

$$\overline{A} ::= \{x : \neg(x \in A)\} \qquad \text{Complement}$$

This is sometimes instead written as A^C.

By default, $\overline{A}$ contains all elements of the *domain of discourse* that are not in the set A. However, we often want to be more restrictive about what elements we put in the new set. If we restrict $\overline{A}$ to just elements of some set $\mathcal{U}$ that are not in A, then we call this the "complement of A relative to the universe $\mathcal{U}$". If a universe is not specified or is not clear from context, then it is taken to be all objects in the domain of discourse.

Since each of these defines a new set, we can use inference rules to reason about their elements. For example, if we are given that $x \in A \cup B$, then we know that $(x \in A) \vee (x \in B)$ by "Def of $A \cup B$": since $A \cup B$ has a definition (in set builder notation), being an element means satisfying the predicate from its definition. In the case of $A \cup B$, the predicate is $(x \in A) \vee (x \in B)$, so x must satisfy that to be an element of $A \cup B$.

Set Comparison

Whenever we introduce a new type of mathematical object, one of the first questions to ask is what does it mean for two described objects to be the same. For sets, we define the equality predicate as follows:

$$A = B \ ::= \ \forall x\,((x \in A) \leftrightarrow (x \in B))$$

This sets that $A = B$ holds when the two sets contain the same elements, i.e., when their "element of" predicates are equivalent.

Equality requires an "iff" relationship to hold. If we only ask for an implication to hold between the "element of" predicates, then this becomes the "subset" relationship between the sets:

$$A \subseteq B \ ::= \ \forall x\,((x \in A) \rightarrow (x \in B))$$

This says that A is a subset of B exactly when every element of A is also an element of B. A subset relationship allows B to contain elements that are not in A, but all the element of A must be elements of B.

By the biconditional equivalence, $A = B$ is equivalent to the two conditions $A \subseteq B$ and $B \subseteq A$.

As a simple example, we can prove that $A \setminus B$ is a subset of $A \cap \overline{B}$ as follows:

1.1.	Let x be arbitrary	
1.2.1	$x \in A \setminus B$	Assumption
1.2.2	$(x \in A) \land \neg(x \in B)$	Def of Difference: 1.2.1
1.2.3	$(x \in A) \land (x \in \overline{B})$	Undef Complement: 1.2.2
1.2.4	$x \in A \cap \overline{B}$	Undef Intersection: 1.2.3
1.2.	$(x \in A \setminus B) \rightarrow (x \in A \cap \overline{B})$	Direct Proof
1.	$\forall x\,((x \in A \setminus B) \rightarrow (x \in A \cap \overline{B}))$	Intro $\forall$
2.	$A \setminus B \subseteq A \cap \overline{B}$	Def of Subset

In fact, $A \setminus B$ is actually equal to $A \cap \overline{B}$. We could prove that by adding a proof of the converse of the implication above inside the formal proof. However, there is a simpler approach in this case (and in general). Proving that an "$\leftrightarrow$" always holds is proving an equivalence, and we can prove equivalences, for example, using a chain of equivalence steps. Each definition is an equivalence, so we can establish the biconditional as follows:

$$\begin{aligned} x \in A \setminus B &\equiv (x \in A) \land \neg(x \in B) && \text{Def of Difference} \\ &\equiv (x \in A) \land (x \in \overline{B}) && \text{Def of Complement} \\ &\equiv x \in A \cap \overline{B} && \text{Def of Intersection} \end{aligned}$$

We can use this to shorten the proof that the sets are equal like this:

1.1.	Let x be arbitrary	
1.2.	$(x \in A \setminus B) \leftrightarrow (x \in A \cap \overline{B})$	Tautology (see above)
1.	$\forall x\,((x \in A \setminus B) \leftrightarrow (x \in A \cap \overline{B}))$	Intro $\forall$
2.	$A \setminus B = A \cap \overline{B}$	Def of Equal Sets

More Set Operations

We are familiar with putting numbers into pairs to form Cartesian coordinates, e.g., $(2,3)$. We can use this operation to define a new way of combining sets:

$$A \times B \ ::= \ \{x : \exists a \in A, \exists b \in B\,(x = (a,b))\} \qquad \text{Cartesian Product}$$

This says that the Cartesian Product of A and B, written $A \times B$, is the set of all pairs (a,b), where the first part of each pair is from A and the second part is from B.

One final way of building new sets from an existing one constructs a set whose elements are not elements of A but rather *sets* of elements from A:

$$\mathcal{P}(A) \ ::= \ \{B : B \subseteq A\} \qquad \text{Power Set}$$

The Power Set of A, denoted $\mathcal{P}(A)$, is a set that contains all the subsets of A as elements.

Both of the above are definitions, so we can use them in equivalence chains or apply them in a formal proof using "Def of" and "Undef".

Sets and Quantifiers

Our second to last example included the proposition $\forall x\,((x \in A \setminus B) \to (x \in A \cap \overline{B}))$. When we recognize this as a *domain restriction*, we see that it says that every element of $A \setminus B$ is an element of $A \cap \overline{B}$.

This special case of a domain restriction to elements of a specific set occurs so often that we introduce special notation for it:

$$\forall x \in S\,(P(x)) \quad \text{is shorthand for} \quad \forall x\,((x \in S) \to P(x))$$

In other words, we put the restriction "$\in S$" as part of the declaration of x occurring at "$\forall x$".

Adding a set restriction to a quantified variable should be natural for us as it is essentially declaring a data type for the variable. Doing so has important benefits. First, it makes the statement more readable since the reader no longer needs know the (often unspecified) domain of discourse. Instead of assuming that all readers will know the domain from which the variables are drawn, we list a domain explicitly next to each variable. Second, it makes the truth of our statements independent of the domain of discourse we choose.[1] In many cases, it can be difficult to explain what that domain is: to use these last set operations we may need to include not only numbers but also pairs and then sets of numbers and pairs and so on. Since the truth value of the statement is the same for any reasonable domain of discourse once we include set restrictions on all quantified variables, we no longer need to be distracted by the details of how the actual domain is constructed.

For those reasons, we will adopt the practice of including set restrictions on all quantified variables whenever it is practical to do so.

Well-Known Sets

Some commonly used sets are the following:

- $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of *Natural Numbers*.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of *Integers*.
- $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \wedge q \neq 0\}$ is the set of *Rational Numbers*.
- $\mathbb{R}$ is the set of *Real Numbers*.

[1] We require only that all the sets we use to constrain quantifiers are included in that domain.