Day 10

Tuesday June 5, 2012

1   Set Theory

1.1   Russell's Paradox

Thus far we have defined several ways to make new sets:

- Union: The union of two (or more) sets is the set of elements which are in at least one of the sets.

- Intersection: The intersection of two (or more) sets is the set of elements which are in all of the sets.

- Relative Complement: The relative compliment of two sets $A \setminus B$ is the set of things in A and not in B.

- Set Builder: The set $\{x \in A \mid P(x)\}$ is the set of elements in the set A that is not in the set B.

Notice that these all have the quality that they make a new set out of an existing set. The last way is actually quite powerful, and can capture the middle two:

$$A \cap B = \{\, x \in A \mid x \in B \,\}$$
$$A \setminus B = \{\, x \in A \mid x \notin B \,\}$$

A natural question to ask is what are the "atomic sets" that is the sets that we begin with, that we can do the above with to make new sets. We have thus far conjectured the existence of the following sets: $\emptyset$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Mathematics is sometimes very philosophical and, likewise, scientific. Those sets are not concrete objects, therefore we have no choice but to just claim that they exist.

So, can we just claim any set exists? Or are they some sets which cannot on principle exist if we expect to be able to perform the above operations to form new sets.

This natural question leads to one particular instance: Is there a set of all sets?

Theorem 1 (Bertrand Russell 1901). *If one is able to do comprehension (set builder notation) to form new sets, there cannot be a set of all sets.*

Proof. For sake of contradiction, let us suppose that this theorem is false. Then we know that there is a set of all sets, and we are able to do comprehension. Let Ω be the set of all set. Now, we want to get a contradiction, and we suspect (given the way the theorem was stated) it has something to do with comprehension. So define a set B as follows:

$$B = \{\, x \in \Omega \mid x \notin x \,\}$$

That is, B is the set of all sets which do not contain themselves as members. We don't know much about B; maybe it is empty, maybe it is very large. But as B is a set, we are allowed to ask questions to B about who are its members. B itself is either a member of B, or not.

> Case 1: $B \in B$.
> We defined B by comprehension, so something gets inside of B only when it satifies the above formula. Therefore, we know $B \notin B$, which is a contradiction.
> Case 2: $B \notin B$.
> Look at the definition of B. We put a set x in B exactly when $x \notin x$. As $B \notin B$ we know therefore that $B \in B$, which of course is a contradiction.

As B is a set, one of these two cases must hold, but they both lead to contradictions. Therefore, we can conclude that our initial assumption was incorrect: Ω is not a set. $\qquad\square$

Therefore, we can conclude that the set of all sets is not a set. Russell's result was important because it showed that the lax rules of set theory at the time (the turn of the 20th century) did not suffice for a formal system. It was riddled with paradoxes.

To solve the problem, during the early 20th century, a program was started to write down what people believed were the rules for set theory. These are rules that you can understand (for the most part): $\emptyset$ and $\mathbb{N}$ are sets, one can take unions and use comprehension. Over the decades, more had to be added to make the system more powerful, but the spirit was always the same.

The idea of Russell's Paradox is an important one. The underlying principle of **self-reference**; we define B, and then as whether B satisfies the very property that defines it. This idea will be re-explored next week when we talk about Cantor's Theorem. To see another interpretation of Russell's Paradox, we have the following story:

Example 1 (Barber's Paradox)**.** Consider a town in which every man is clean-shaven. There is one male barber, and the barber shaves every man who does not shave himself.

Who shaves the barber?

1.2 Powersets

We learn a new way to make a set out of another set. This is another way to form sets which is simply conjectured by the rules of set theory.

Definition 1. The **powerset** of a set A, denoted $\wp(A)$, is the set of all subsets of A.

Example 2. Let $A = \{1, 2, 3\}$. Then

$$\wp(A) = \{\, \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{1,2\}, \{1,2,3\} \,\}$$

Theorem 2. *For any set A, we have $\wp(A) \neq \emptyset$.*

Proof. To show $\wp(A) \neq \emptyset$, we need only show that $\wp(A)$ has a member. In other words, we need to show that A has a subset. Well, as stated, $\emptyset \subseteq X$ for any set X, therefore $\emptyset \subseteq A$. So $\emptyset \in \wp(A)$, so $\wp(A)$ is nonempty. $\qquad\square$

Theorem 3.
$$\wp(A \cap B) = \wp(A) \cap \wp(B)$$

Proof. ($\subseteq$) Take $X \in \wp(A \cap B)$. Then $X \subseteq A \cap B$. As $X \subseteq A \cap B$ we know ever member of X is in A, so $X \subseteq A$; similar ever member of X is in B so $X \subseteq B$. Therefore $X \in \wp(A)$ and $X \in \wp(B)$, so $X \in \wp(A) \cap \wp(B)$.

($\supseteq$) Take $X \in \wp(A) \cap \wp(B)$. Then $X \in \wp(A)$ and $X \in \wp(B)$. Thus $X \subseteq A$ and $X \subseteq B$. We want to show that $X \in \wp(A \cap B)$, ie. $X \subseteq A \cap B$. So, take $x \in X$ arbitrary. As $X \subseteq A$ we know $x \in A$, and similar as $X \subseteq B$ we know $x \in B$. Therefore, $x \in A \cap B$, which is what we wanted. $\qquad\square$

For the homework, you'll be asked the prove an analogous result for $\cup$.

Theorem 4. *For every $n \in \mathbb{N}$, we have $[n] \in \wp(\mathbb{N})$.*

Proof. Suffices to show that for every n, we have $[n] \subseteq \mathbb{N}$. But this is obvious, as if $x \in [n]$ then as $[n] = \{\, 1, 2, 3, \ldots, n \,\}$ we have $x = i$ for some $0 < i \leq n$ in the naturals. $\qquad\square$

Question 1. If a set A has n members, then how many members does $\wp(A)$ have?

Answer 1. 2^n; you can prove this with induction.

If A has 0 members, then $A = \emptyset$, and the only subset of A is $\emptyset$. Therefore $\wp(A)$ has 1 member.

Assume any set of size n has 2^n subsets. Look at an arbitrary set of size $n + 1$; call it A. Want to show that A as 2^{n+1} subsets. Well, take $x \in A$. And look at $A \setminus \{x\}$. This is a set with n members. Thus it has 2^n subsets. For each one of these subsets there is another subset in which x is added.

One must argue that every subset can be formed this way, but that is straightforward as every subset either has x or does not, and if it does have x in it, then it is still a subset when x is removed.

1.3   Cartesian Product

So far, we have looked at sets. Sets have absolutely no structure or order. Most of math, however, has structure. The natural numbers have lots of structure; there is an ordering, there is arithmetic, etc.

In order to solve this problem we introduce the Cartesian product (named after René Descartes). You have really already seen the concept before.

Remark 1. Recall the **Cartesian Plane** is the set of ordered pairs (x, y) where x and y are reals. These make a plane in geometry.

Definition 2. The **Cartesian Product** or sets A and B, denoted $A \times B$ (spoken as A cross B) is the set of ordered pairs, where the first coordinate comes from A and the second from B. That is, if $x \in A$ and $y \in B$ then
$$(x, y) \in A \times B$$

Example 3.
$$[3] \times [2] = \{ (1, 1), (2, 1), (3, 1), (1, 2), (2, 2), (3, 2) \}$$

Therefore the notation for the Cartesian Plane is $\mathbb{R} \times \mathbb{R}$.

This is the first bit of structure we have put on a set. If we have an ordered pair, we can "recover" which is the first element, and which is the second. This simple idea is very, very powerful and will be the backbone of defining all complicate structures on sets.

Remark 2. Ordered pairs can be compared; $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

2   Relations

With the Cartesian product allowing us to make structures, we talk about our first structure: Relations.

Example 4. We have many natural relations in our day to day life. "Sibling of" is one. A is a sibling of B if they have the same parents. This relation has a number of interesting properties:

- A is a sibling of B means that B is a sibling of A.

- A is a sibling of B and B is a sibling of C means that A is a sibling of C.

There is another relation "ancestor of". This relation fails on the first property above (if A is my ancestor, that does not make me the ancestor of A) but does pass on the second.

Definition 3. If A and B are sets then a **relation R relating** A **to** B is a subset of $A \times B$.

If $(a, b) \in R$ for $a \in A$ and $b \in B$ then we say a **is R-related to** b. We typically write R in either infix or prefix notation. Therefore the following are all equivalent (although context dependent)

- $(a, b) \in R$

- aRb

- Rab

Notice, they are all atomic statements which are either true or false and can be verified just by checking membership in R.

If $A = B$ (as is frequently the case) then we say R **is a relation on** A

Example 5. A natural example is $<$ on the natural numbers $\mathbb{N}$. Then we have $(a, b) \in <$ if and only if a is smaller than b with respect to the usual ordering on the natural numbers. We typically write this in infix notation: $a < b$ instead of $(a, b) \in <$.

We can certainly make our own relations too.

Example 6. Consider R relating $[5]$ to $[10]$ by
$$R = \{ (a, b) \in [5] \times [10] \mid 2a = b \}$$

Writing this out explicitly
$$R = \{ (1, 2), (2, 4), (3, 6), (4, 8), (5, 10) \}$$

Example 7. A natural relation to define on the integers is **divisibility**. We define R to be a relation on $\mathbb{Z}$ and say that a is R-related to b if and only if a divides b. Written formally:

$$R = \{\, (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid \exists c \in \mathbb{Z} \,\textbf{.}\, a \cdot c = b \,\}$$

For this relation this is a special symbol we have already seen: $\mid$ which we typically write in infix. So, we we write $a|b$ to mean $(a,b) \in R$ where R is defined above.

This relation we will use as a toy for the rest of the day to talk about properties a relation may have.

2.1 Reflexivity

The first relation property we will discuss is **reflexivity**.

Definition 4. A relation R on a set A is **reflexive** if for every $a \in A$ we have a is R-related to a.
    Similarly, a relation R on a set A is **irreflexive** if for every $a \in A$ we have that a is not R-related to a.

Question 2. Is irreflexive the negation of reflexive?

Answer 2. No; irreflexive says nothing is related to itself, where as not reflexive would mean there is a at least one thing that is not related to itself

Example 8. We have seen many reflexive relations. For example $\leq$ is a reflexive relation on $\mathbb{N}$. We certain have $n \leq n$ for every $n \in \mathbb{N}$.
    We have also seen irreflexive relations. For example $<$ is irreflexive as every $n \in \mathbb{N}$ has the property that $n \not< n$

Question 3. Is the divisibility relation on $\mathbb{Z}$ reflexive?

Answer 3. Yes! We just need to show that $\exists c \in \mathbb{Z} \,\textbf{.}\, a \cdot c = a$. Well, if $c = 1$ then $a \cdot 1 = a$.

Question 4. Can a relation R which is reflexive be empty?

Answer 4. Yes; namely if the set itself the relation is over is empty. If however, the set is nonempty then a reflexive relation is never empty. Can you prove this?