Lecture 5: Properties of Sets, Formal Methods, and Paradoxes

Theorem 5.2.1, Some Subset Relations

Inclusion of Intersection:
\[ A \cap B \subseteq A \text{ and } A \cap B \subseteq B \]

Inclusion in Union:
\[ A \subseteq A \cup B \text{ and } B \subseteq A \cup B \]

Transitivity of Subsets:
If \( A \subseteq B \) and \( B \subseteq C \), then \( A \subseteq C \)

To prove that a set \( X \) is a subset of another set \( Y \), prove that any element \( x \in X \) also belongs to \( Y \).

Theorem 5.2.2, Set Identities
The first 3 (Commutative, Associative, Distributive Laws) are familiar.

4. Intersection with \( U \)

5. Double Complement Law

6. Idempotent Laws \( A \cap A = A \cup A \)

7. De Morgan's Laws (involve complements)
\[ (A \cup B)^c = (A \cap B)^c \]

8. Union with \( U \)

9. Absorption Laws
\[ A \cup (A \cap B) = A \cap (A \cup B) = \]

10. Alternate Representation for Set Difference
\[ A - B = A \cap B^c \]
Proofs that 2 expressions involving sets are equal  Usually one of 2 types:

1. An element argument:

| To show that set X = set Y, show that any element $x \in X$ also belongs to Y AND any element $x \in Y$ also belongs to X. |

So show the left side is a subset of the right side:

   i) Let $x \in$ left side, show...
  then show that the right side is a subset of the left side:

   ii) Let $x \in$ right side, show...

2. An argument from known set properties and already proven theorems—two column proof

| ----------- | = | ----------- |
| reason     | = | reason     |
| reason     | = | reason     |

To disprove a set equality, it is enough to show a counterexample. A Venn diagram (showing sets of points in the plane) can provide the counterexample.

Is a set statement true? First use a Venn diagram to get a sense of whether the statement is true or not. If true, use an argument. If false, provide a counterexample.

ex. Show $(A - B) \cup (A \cap B) = A$
ex. Show \( A - ( B - C ) = ( A - B ) - C \)

ex. Show \( A - B \subseteq A \)

ex. Prove if \( A \subseteq B \) and \( B \subseteq C \), then \( A \subseteq C \).
**Proving Empty Sets**
To show that a set is empty, assume there is $x \in$ the set and reason to a contradiction.

ex. For all sets $A$ and $B$, prove $(A - B) \cap (A \cap B) = \varnothing$

Suppose $x$

ex. For all sets $A$, $B$, $C$ prove $(A - C) \cap (B - C) \cap (A - B) = \varnothing$
Most of what we have been doing for the last 4 weeks has involved **Boolean Algebras**.

A **Boolean algebra** is a set of objects for which **2 operations** are defined that obey the following:

<table>
<thead>
<tr>
<th>Boolean algebra (General)</th>
<th>Boolean Logic</th>
<th>Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>∨</td>
<td>∪</td>
</tr>
<tr>
<td>·</td>
<td>∧</td>
<td>∩</td>
</tr>
<tr>
<td>Commutativity of +</td>
<td>∨</td>
<td>∪</td>
</tr>
<tr>
<td>Comm. of ·</td>
<td>∧</td>
<td>∩</td>
</tr>
<tr>
<td>Associativity of +</td>
<td>∨ ∨</td>
<td>∪ ∪</td>
</tr>
<tr>
<td>Assoc. of ·</td>
<td>∧ ∧</td>
<td>∩ ∩</td>
</tr>
<tr>
<td>Distrib. of + over ·</td>
<td>∨ (∨ ∧)</td>
<td>∪ (∩)</td>
</tr>
<tr>
<td>Distrib. of · over +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity for +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity for ·</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existence of a Complement</td>
<td>p ∨ ~ p =</td>
<td>∪</td>
</tr>
<tr>
<td></td>
<td>p ∧ ~ p =</td>
<td>∩</td>
</tr>
</tbody>
</table>
Properties of a Boolean Algebra.

Theorem 5.3.2 Properties of a Boolean Algebra

Let $B$ be any Boolean Algebra.

1. **Uniqueness of the Complement Law:** For all $a$ and $x$ in $B$, if $a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$.

2. **Uniqueness of 0 and 1:** If there exists $x$ in $B$ such that $a + x = a$ for all $a$ in $B$, then $x = 0$, and if there exists $y$ in $B$ such that $a \cdot y = a$ for all $a$ in $B$, then $y = 1$.

3. **Double Complement Law:** For all $a \in B$, $\overline{\overline{a}} = a$.

4. **Idempotent Law:** For all $a \in B$,
   
   (a) $a + a = a$ \hspace{1cm} \text{and} \hspace{1cm} (b) $a \cdot a = a$.

5. **Universal Bound Law:** For all $a \in B$,
   
   (a) $a + 1 = 1$ \hspace{1cm} \text{and} \hspace{1cm} (b) $a \cdot 0 = 0$.

6. **De Morgan’s Laws:** For all $a$ and $b \in B$,
   
   (a) $\overline{a + b} = \overline{a} \cdot \overline{b}$ \hspace{1cm} \text{and} \hspace{1cm} (b) $\overline{a \cdot b} = \overline{a} + \overline{b}$.

7. **Absorption Laws:** For all $a$ and $b \in B$,
   
   (a) $(a + b) \cdot a = a$ \hspace{1cm} \text{and} \hspace{1cm} (b) $(a \cdot b) + a = a$.

8. **Complements of 0 and 1:**
   
   (a) $\overline{0} = 1$ \hspace{1cm} \text{and} \hspace{1cm} (b) $\overline{1} = 0$.

Proofs in Boolean Algebra

Prove Idempotent: For all $a \in B$, $a + a = a$. 

Lecture 5 p. 6
Using Boolean algebra definitions and Idempotent, prove
For all $a$ and $b$ in $B (a \cdot b) + a = a$.

**Russell’s Paradox:**

Form set $S$ as the set of all sets that do not contain themselves.

$$ S = \{ A \mid \} $$

Should $S$ contain itself?

If $S \in S$,

If $S \notin S$,  

Lecture 5 p. 7
The Barber Puzzle:
The male barber in Zooville shaves all the male inhabitants of Zooville who do not shave themselves. He shaves no one else. Who shaves the barber?

As a statement: "Given the scenario above, the barber shaves himself."

Is this statement true or false?

If the barber shaves himself,

If the barber does not shave himself,

Implication of the Paradox: $S \in S \rightarrow S \notin S$ and $S \notin S \rightarrow S \in S$

To Avoid the Paradox: $S = \{A \mid$

Prove $S \in S \rightarrow S \notin S$.
Suppose $S \in S$.

Prove $S \notin S \rightarrow S \in S$.
Suppose $S \notin S$.

Statement: A sentence which (in our universe) can be judged to be either true or false.

ex. If Loyola is in Buffalo, then cats fly.

ex. If Loyola is in Maryland, then all computers are powered by gerbils.

ex. The sentence in this box is a lie.
**Halting Problem**: Does a program loop forever?

Is it possible to write a program that could analyze any computer program with a certain set of input data for the program and determine whether the program halts (stops) or gets caught in an infinite loop when that data is used?

*Is this possible?*

---

**Example**: Suppose this is the program, P.

```java
x = myScan.nextInt();
while (x != 0)
    System.out.println(x);
    x = x - 2;
```

Let $(P, D)$ represent the program $P$ with input data $D$.

Does $(P, 12)$ halt?

Does $(P, 13)$ halt?

Could we have a program, CheckHalt, so that CheckHalt $(P, D)$ sends back “halts” or “loops”?

**Let’s assume that CheckHalt can be written**.

(i.e., we can build a program that given another program $P$ and a set of data $D$ will answer “halts” or “loops” to the question "Will $P$ halt with input $D$?")

Then let’s build another program, Test. Test will accept a program $P$ as its input and then do three things:

1. Make a copy of the input program $P$.
2. Call CheckHalt sending it $P$ as the program AND $P$ also as the data. In other words it calls CheckHalt $(P, P)$.
3. When it gets the results of CheckHalt, it acts as follows:
   - If CheckHalt $(P, P)$ answers “loops”, Test stops.
   - If CheckHalt $(P, P)$ answers “halts”, Test enters an infinite loop (doesn't halt).
Now, Test is itself a program, i.e., just a sequence of characters in a file. We could call Test and send it a *copy of itself*. In other words call Test (Test). Then CheckHalt (Test, Test) would be called.

![Diagram of Test and CheckHalt](image.png)

If CheckHalt (Test, Test) answers “loops”, Test stops. (But when CheckHalt answers "loops", it means…

If CheckHalt (Test, Test) answers “halts”, Test enters an infinite loop. (But when CheckHalt answers "halts"…

HUH?