CSE 311: Foundations of Computing

Lecture 10: Sets & Number Theory
Sets are collections of objects called elements.

Write $a \in B$ to say that $a$ is an element of set $B$, and $a \notin B$ to say that it is not.

Some simple examples:
- $A = \{1\}$
- $B = \{1, 3, 2\}$
- $C = \{\Box, 1\}$
- $D = \{{17}, 17\}$
- $E = \{1, 2, 7, \text{cat, dog, } \emptyset, \alpha\}$
Last Time: Operations on Sets

• Definition for $\cup$ based on $\lor$

$$A \cup B = \{ x : (x \in A) \lor (x \in B) \}$$

• Definition for $\cap$ based on $\land$

$$A \cap B = \{ x : (x \in A) \land (x \in B) \}$$

• Complement based on $\neg$

$$\overline{A} = \{ x : \neg(x \in A) \}$$
De Morgan’s Laws

\[ A \cup B = \bar{A} \cap \bar{B} \]

\[ A \cap B = \bar{A} \cup \bar{B} \]
De Morgan’s Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x \ (x \in (A \cup B)^C \iff x \in A^C \cap B^C)$

Proof: Let $x$ be an arbitrary object.

Since $x$ was arbitrary, we have shown, by definition, that $(A \cup B)^C = A^C \cap B^C$.  

Proof technique:
To show $C = D$ show $x \in C \rightarrow x \in D$ and $x \in D \rightarrow x \in C$
De Morgan’s Laws

Formally, prove $\forall x \ (x \in (A \cup B)^c \leftrightarrow x \in A^c \cap B^c)$

1. Let $x$ be arbitrary
   2.1. $x \in (A \cup B)^c$ Assumption
       ...
       2.3. $x \in A^c \cap B^c$
2. $x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c$ Direct Proof
   3.1. $x \in A^c \cap B^c$ Assumption
       ...
       3.3. $x \in (A \cup B)^c$
3. $x \in A^c \cap B^c \rightarrow x \in (A \cup B)^c$ Direct Proof
   4. $(x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c) \land (x \in A^c \cap B^c \rightarrow x \in (A \cup B)^c)$ Intro $\land$: 2, 3
5. $x \in (A \cup B)^c \leftrightarrow x \in A^c \cap B^c$ Biconditional: 4
6. $\forall x \ (x \in (A \cup B)^c \leftrightarrow x \in A^c \cap B^c)$ Intro $\forall$: 1-5
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

Proof: Let \(x\) be an arbitrary object.
Suppose \(x \in (A \cup B)^C\).

... 

Thus, we have \(x \in A^C \cap B^C\).
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

Proof: Let \(x\) be an arbitrary object.
Suppose \(x \in (A \cup B)^C\). Then, by the definition of complement, we have \(\neg(x \in A \cup B)\).

... 

Thus, we have \(x \in A^C \cap B^C\).
De Morgan’s Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x \ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

**Proof:** Let $x$ be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by definition, that $\neg(x \in A \lor x \in B)$.

... 

Thus, we have $x \in A^C \cap B^C$. 

De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)\)

**Proof:** Let \(x\) be an arbitrary object.

Suppose \(x \in (A \cup B)^C\). Then, by the definition of complement, we have \(\neg(x \in A \cup B)\). The latter says, by definition, that \(\neg(x \in A \lor x \in B)\).

...

Thus, \(x \in A^C\) and \(x \in B^C\), so we we have \(x \in A^C \cap B^C\) by the definition of intersection.
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x \ (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

**Proof:** Let \(x\) be an arbitrary object.

Suppose \(x \in (A \cup B)^C\). Then, by the definition of complement, we have \(\neg (x \in A \cup B)\). The latter says, by definition, that \(\neg (x \in A \lor x \in B)\).

... 

Thus, \(\neg (x \in A)\) and \(\neg (x \in B)\), so \(x \in A^C\) and \(x \in B^C\) by the definition of compliment, and we can see that \(x \in A^C \cap B^C\) by the definition of intersection.
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)
Formally, prove \(\forall x (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

**Proof:** Let \(x\) be an arbitrary object.

Suppose \(x \in (A \cup B)^C\). Then, by definition of complement, we have \(\neg(x \in A \cup B)\). The latter says, by definition, that \(\neg(x \in A \lor x \in B)\), or equivalently \(\neg(x \in A) \land \neg(x \in B)\) by De Morgan’s law. Thus, we have \(x \in A^C\) and \(x \in B^C\) by the definition of complement, and we can see that \(x \in A^C \cap B^C\) by the definition of intersection.

Proof technique:
To show \(C = D\) show
\(x \in C \rightarrow x \in D\) and
\(x \in D \rightarrow x \in C\)
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x \ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)\)

Proof: Let \(x\) be an arbitrary object.

Suppose \(x \in (A \cup B)^C\). Then, \(x \in A^C \cap B^C\).

Suppose \(x \in A^C \cap B^C\). Then, by the definition of intersection, we have \(x \in A^C\) and \(x \in B^C\). That is, we have \(\neg (x \in A) \land \neg (x \in B)\), which is equivalent to \(\neg (x \in A \lor x \in B)\) by De Morgan’s law. The last is equivalent to \(\neg (x \in A \cup B)\), by the definition of union, so we have shown \(x \in (A \cup B)^C\), by the definition of complement.
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x \ (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

Proof: Let \(x\) be an arbitrary object.

The stated biconditional holds since:

\[
x \in (A \cup B)^C \equiv \neg(x \in A \cup B)
\equiv \neg(x \in A \lor x \in B)
\equiv \neg(x \in A) \land \neg(x \in B)
\equiv x \in A^C \land x \in B^C
\equiv x \in A^C \cap B^C
\]

Def of \(-^C\)
Def of \(\lor\)
Def of \(-^C\)
Def of \(\land\)
Def of \(-^C\)
Def of \(\land\)

Since \(x\) was arbitrary, we have shown the sets are equal. \(\blacksquare\)
Distributive Laws

\[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \]
\[ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \]
It’s Propositional Logic Again!

Meta-Theorem: Translate any Propositional Logic equivalence into “=” relationship between sets by replacing $\cup$ with $\lor$, $\cap$ with $\land$, and $\cdot^C$ with $\neg$.

“Proof”: Let $x$ be an arbitrary object.
The stated bi-condition holds since:

$x \in \text{left side} \equiv \text{replace set ops with propositional logic}$

$\equiv \text{apply Propositional Logic equivalence}$

$\equiv \text{replace propositional logic with set ops}$

$\equiv x \in \text{right side}$

Since $x$ was arbitrary, we have shown the sets are equal. ■
Power Set

• Power Set of a set $A = \text{set of all subsets of } A$

$$\mathcal{P}(A) = \{ B : B \subseteq A \}$$

• e.g., let $\text{Days} = \{M,W,F\}$ and consider all the possible sets of days in a week you could ask a question in class

$$\mathcal{P}(\text{Days})=?$$

$$\mathcal{P}(\emptyset)=?$$
Power Set

- Power Set of a set $A = \text{set of all subsets of } A$

\[ \mathcal{P}(A) = \{ B : B \subseteq A \} \]

- e.g., let $\text{Days} = \{M, W, F\}$ and consider all the possible sets of days in a week you could ask a question in class

\[ \mathcal{P}(\text{Days}) = \{\{M, W, F\}, \{M, W\}, \{M, F\}, \{W, F\}, \{M\}, \{W\}, \{F\}, \emptyset\} \]

\[ \mathcal{P}(\emptyset) = ? \]
Power Set

- Power Set of a set $A$ = set of all subsets of $A$

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

- e.g., let $\text{Days} = \{M, W, F\}$ and consider all the possible sets of days in a week you could ask a question in class

$$\mathcal{P}(\text{Days}) = \{\{M, W, F\}, \{M, W\}, \{M, F\}, \{W, F\}, \{M\}, \{W\}, \{F\}, \emptyset\}$$

$$\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$$
Cartesian Product

\[ A \times B = \{ (a, b): a \in A, b \in B \} \]

\( \mathbb{R} \times \mathbb{R} \) is the real plane. You’ve seen ordered pairs before.

These are just for arbitrary sets.

\( \mathbb{Z} \times \mathbb{Z} \) is “the set of all pairs of integers”

If \( A = \{1, 2\}, B = \{a, b, c\} \), then \( A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\} \).
Cartesian Product

\[ A \times B = \{ (a, b) : a \in A, b \in B \} \]

\( \mathbb{R} \times \mathbb{R} \) is the real plane. You’ve seen ordered pairs before.

These are just for arbitrary sets.

\( \mathbb{Z} \times \mathbb{Z} \) is “the set of all pairs of integers”

If \( A = \{1, 2\}, B = \{a, b, c\} \), then \( A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\} \).

What is \( A \times \emptyset \)?
Cartesian Product

\[ A \times B = \{ (a, b) : a \in A, b \in B \} \]

\( \mathbb{R} \times \mathbb{R} \) is the real plane. You’ve seen ordered pairs before.

These are just for arbitrary sets.

\( \mathbb{Z} \times \mathbb{Z} \) is “the set of all pairs of integers”

If \( A = \{1, 2\}, B = \{a, b, c\} \), then \( A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\} \).

\[ A \times \emptyset = \{ (a, b) : a \in A \land b \in \emptyset \} = \{ (a, b) : a \in A \land F \} = \emptyset \]
Russell’s Paradox

\[ S = \{ x : x \notin x \} \]

Suppose that \( S \in S \)...
Russell’s Paradox

\[ S = \{ x : x \notin x \} \]

Suppose that \( S \in S \). Then, by the definition of \( S \), \( S \notin S \), but that’s a contradiction.

Suppose that \( S \notin S \). Then, by the definition of \( S \), \( S \in S \), but that’s a contradiction too.

This is reminiscent of the truth value of the statement “This statement is false.”
Number Theory
Number Theory (and applications to computing)

• Branch of Mathematics with direct relevance to computing

• Many significant applications
  – Cryptography
  – Hashing
  – Security

• Important toolkit
Modular Arithmetic

- Arithmetic over a finite domain
- Almost all computation is over a finite domain
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println("I will be alive for at least " +
                        SEC_IN_YEAR * 101 + " seconds." );
    }
}
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println("I will be alive for at least "+
                        SEC_IN_YEAR * 101 + " seconds."
                        );
    }
}

---jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

---jGRASP: operation complete.
Divisibility

Definition: “b divides a”

For $a, b \in \mathbb{Z}$ with $b \neq 0$:

$$b \mid a \iff \exists q \in \mathbb{Z} \ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1  25 | 5  5 | 0  3 | 2

1 | 5  5 | 25  0 | 5  2 | 3
Check Your Understanding. Which of the following are true?

- $5 \mid 1$ (5 divides 1) if $1 = 5k$
- $25 \mid 5$ (25 divides 5) if $5 = 25k$
- $5 \mid 0$ (5 divides 0) if $0 = 5k$
- $3 \mid 2$ (3 divides 2) if $2 = 3k$
- $1 \mid 5$ (1 divides 5) if $5 = 1k$
- $5 \mid 25$ (5 divides 25) if $25 = 5k$
- $0 \mid 5$ (0 divides 5) if $5 = 0k$
- $2 \mid 3$ (2 divides 3) if $3 = 2k$

**Definition: “b divides a”**

For $a, b \in \mathbb{Z}$ with $b \neq 0$: $b \mid a \iff \exists q \in \mathbb{Z} (a = qb)$
Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide $b$ into $a$.

If $b \mid a$, then, by definition, we have $a = qb$ for some $q \in \mathbb{Z}$. The number $q$ is called the quotient.

Dividing both sides by $a$, we can write this as

$$\frac{a}{b} = d$$

(We want to stick to integers, though, so we’ll write $a = qb$.)
For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide $b$ into $a$.

If $b \nmid a$, then we end up with a remainder $r \in \mathbb{Z}$ with $0 < r < b$. Now,

\[
\frac{a}{b} = q + \frac{r}{b}
\]

instead of $\frac{a}{b} = q$ we have

Multiplying both sides by $a$ gives us

\[
a = qb + r
\]

(A bit nicer since it has no fractions.)
For \(a, b \in \mathbb{Z}\) with \(b > 0\), we can divide \(b\) into \(a\).

If \(b \mid a\), then we have \(a = qb\) for some \(q \in \mathbb{Z}\).

If \(b \nmid a\), then we have \(a = qb + r\) for some \(q, r \in \mathbb{Z}\) with \(0 < r < b\).

In general, we have \(a = qb + r\) for some \(q, r \in \mathbb{Z}\) with \(0 \leq r < b\),
where \(r = 0\) iff \(b \mid a\).
Division Theorem

For $a, b \in \mathbb{Z}$ with $b > 0$
there exist unique integers $q, r$ with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide $b$ into $a$, we get a unique quotient $q = a \; \text{div} \; b$
and non-negative remainder $r = a \; \text{mod} \; b$

Note: $r \geq 0$ even if $a < 0$.
Not quite the same as $a \% d$. 

To put it another way, if we divide \( b \) into \( a \), we get a unique quotient \( q = a \texttt{ div } b \) and non-negative remainder \( r = a \texttt{ mod } b \).

### Division Theorem

For \( a, b \in \mathbb{Z} \) with \( b > 0 \), there exist unique integers \( q, r \) with \( 0 \leq r < b \) such that \( a = qb + r \).

```java
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

Note: \( r \geq 0 \) even if \( a < 0 \). Not quite the same as \( a \% d \).