Adam Blank | Spring 2016

CSE 311

Foundations of Computing I

Some Reminders/Hints for HW3

Style matters in proofs!

Do NOT manipulate large statements by equivalences! This is horrible style and will lose points if there is a significantly cleaner proof.

Our inference rules can only prove things true. Do not "prove the negation false"! It doesn't make sense.

After you're done writing your proof, you should proof-read (heh) it.

Set Operations

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

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

$A \setminus B = \{ x : (x \in A) \wedge (x \notin B) \}$ Set Difference

A = {1, 2, 3}
B = {4, 5, 6}
C = {3, 4}

QUESTIONS
Using A, B, C and set operations, make…
[6] = A ∪ B = A ∪ B ∪ C
{3} = C ∖ B = A ∖ B = A ∩ B
{1,2} = A ∖ C = (A ∪ B) ∖ C

More Set Operations

$A \oplus B = \{ x : (x \in A) \oplus (x \in B) \}$ Symmetric Difference

$\bar{A} = \{ x : x \notin A \}$ (with respect to universe U) Complement

A = {1, 2, 3}
B = {1, 4, 2, 6}
C = {1, 2, 3, 4}

QUESTIONS
Let S = {1, 2}.
If the universe is A, then $\bar{S}$ is… **A ∖ S =** {3}
If the universe is B, then $\bar{S}$ is… **B ∖ S =** {4, 6}
If the universe is C, then $\bar{S}$ is… **C ∖ S =** {3, 4}

Power Set

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

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

- Let Days = {M, W, F}. Suppose we wanted to know the possible ways that we could allocate class days to be cancelled. Let's call this set $\mathcal{P}(\text{Days})$.

e.g. $\mathcal{P}(\text{Days}) = \{$
$\varnothing,$
$\{M\}, \{W\}, \{F\},$
$\{M, W\}, \{W, F\}, \{M, F\},$
$\{M, W, F\}$
$\}$

e.g. $\mathcal{P}(\varnothing) = \{\emptyset\}$

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 × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

$A \times \emptyset = \{(a, b) : a \in A \wedge b \in \emptyset\} = \{(a, b) : a \in A \wedge F\} = \emptyset$

Russell's Paradox

$$S = \{ x : x \notin x \}$$

Suppose for contradiction that S ∈ S. Then, by definition of S, S ∉ S, but that's a contradiction.

Suppose for contradiction that S ∉ S. Then, by definition of the set comprehension, S ∈ S, but that's a contradiction.

This is reminiscent of the truth value of the statement "This statement is false."

It's Boolean algebra again

- Definition for ∪ based on ∨

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

- Definition for ∩ based on ∧

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

- Complement works like ¬

$$\overline{A} = \{ x : x \notin A \}$$

(with respect to universe U)

De Morgan's Laws

Prove $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Let U be the universe.

$$\begin{aligned}
\overline{A \cup B} &= \{x : x \notin A \cup B\} \\
&= \{x : \neg(x \in A \cup B)\} \\
&= \{x : \neg((x \in A) \vee (x \in B))\} \\
&= \{x : (x \notin A) \wedge (x \notin B)\} \\
&= \{x : (x \in \overline{A}) \wedge (x \in \overline{B})\} \\
&= \{x : (x \in \overline{A})\} \cap \{x : (x \in \overline{B})\} \\
&= \overline{A} \cap \overline{B}
\end{aligned}$$

Prove $\overline{A \cap B} = \overline{A} \cup \overline{B}$

De Morgan's Laws

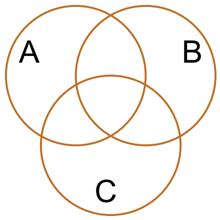
Prove $\overline{A \cap B} = \overline{A} \cup \overline{B}$

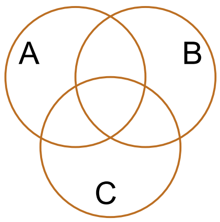
Let U be the universe.

$$\begin{aligned}
\overline{A \cap B} &= \{x : x \notin A \cap B\} \\
&= \{x : \neg(x \in A \cap B)\} \\
&= \{x : \neg((x \in A) \wedge (x \in B))\} \\
&= \{x : (x \notin A) \vee (x \notin B)\} \\
&= \{x : (x \in \overline{A}) \vee (x \in \overline{B})\} \\
&= \{x : (x \in \overline{A})\} \cup \{x : (x \in \overline{B})\} \\
&= \overline{A} \cup \overline{B}
\end{aligned}$$

Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$





One More

Prove $(A \cap B) \subseteq A$

Remember the definition of subset?

$$X \subseteq Y \leftrightarrow \forall x\, (x \in X \rightarrow x \in Y)$$

Let x be an arbitrary element of $A \cap B$. Then, by definition of $A \cap B$, $x \in A$ and $x \in B$. It follows that $x \in A$, as required.

Representing Sets Using Bits

- Suppose universe U is $\{1,2,\ldots,n\}$
- Can represent set $B \subseteq U$ as a vector of bits:

  $b_1 b_2 \ldots b_n$ where $b_i = 1$ when $i \in B$

  $b_i = 0$ when $i \notin B$

  – Called the *characteristic vector* of set B

- Given characteristic vectors for A and B
  – What is characteristic vector for $A \cup B$? $A \cap B$?

UNIX/Linux File Permissions

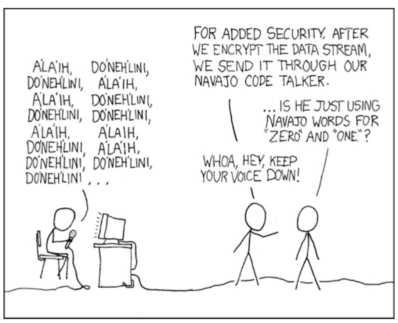
- **ls -l**

```
drwxr-xr-x ... Documents/
-rw-r--r-- ... file1
```

- Permissions maintained as bit vectors
  – Letter means bit is 1
  – "–" means bit is 0.

CSE 311: Foundations of Computing

Lecture 10: Modular Arithmetic



Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing
- Many significant applications
  – Cryptography
  – Hashing
  – Security
- Important tool set

Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

I'm ALIVE!

```
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: "a divides b"
For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:
$$a \mid b \leftrightarrow \exists(k \in \mathbb{Z})\ b = ka$$

Check Your Understanding. Which of the following are true?

5 | 1	**25 | 5**	**5 | 5**	**3 |2**
5 | 1 iff 1 = 5k	25 | 1 iff 1 = 25k	5 | 5 iff 5 = 5k	3 | 2 iff 2 = 3k
1 | 5	**5 | 25**	**0 | 1**	**2 | 3**
1 | 5 iff 5 = 1k	1 | 25 iff 25 = 1k	0 | 1 iff 1 = 0k	2 | 3 iff 3 = 2k

Division Theorem

Division Theorem
For $a \in \mathbb{Z}, d \in \mathbb{Z}^+$:
Then, there exists *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$.

To put it another way, if we take a/d, we get a dividend and a remainder: $q = a$ **div** d $\quad r = a$ **mod** d

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

```
----jGRASP exec: java Test2
-1

----jGRASP: operation complete.
```

Note: r ≥ 0 even if a < 0.
Not quite the same as `a % d`.

Arithmetic, mod 7

$a +_7 b = (a + b) \bmod 7$

$a \times_7 b = (a \times b) \bmod 7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Definition: "a is congruent to b modulo m"
For $a \in \mathbb{Z}, b \in \mathbb{Z}, m \in \mathbb{Z}$:
$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

A ≡ 0 (mod 2)
This statement is the same as saying "A is even"; so, any A that is even (including negative even numbers) will work.

1 ≡ 0 (mod 4)
This statement is false. If we take it mod 1 instead, then the statement is true.

A ≡ -1 (mod 17)
If A = 17x – 1 = 17x + 16, then it works.
Note that (m – 1) mod m = ((m mod m) + (-1 mod m)) mod m
= (0 + -1) mod m = -1 mod m

Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer. Then, a ≡ b (mod m) if and only if a mod m = b mod m.

Suppose that a ≡ b (mod m).
Then, m | (a – b) by definition of congruence.
So, a – b = km for some integer k by definition of divides.
Therefore, a = b+km.
Taking both sides modulo m we get:
a mod m=(b+km) mod m = b mod m.

Suppose that a mod m = b mod m.
By the division theorem, a = mq + (a mod m) and
b = ms + (b mod m) for some integers q,s.
Then, a – b = (mq + (a mod m)) – (mr + (b mod m))
= m(q – r) + (a mod m – b mod m)
= m(q – r) since a mod m = b mod m
Therefore, m | (a-b) and so *a* ≡ *b* (mod *m*).