# Mathematical Foundations

## Logic, Sets, and (Some) Proof Techniques

Wednesday, August 31

Reading: Sipser 0.2 – beginning of 0.4; Stoughton 1.1.1 – 1.1.4

**CS235 Languages and Automata**

Department of Computer Science
Wellesley College

## Goals for the next few lectures

Review/learn standard mathematical structures we'll use throughout the course:

- Sets
- Tuples
- Relations
- Functions
- Trees
- Graphs

See a few examples of some proof techniques

- Proof by picture
- Proof by algebra
- Proof by construction
- Proof by contradiction (including diagonalization)
- Proof by induction



## Basic Logic

- reasoning about boolean values T (true) and F (false)
- negation (not): $\neg$ T = F; $\neg$ F = T; $\neg$ ($\neg$ p)
- conjunction (and): p $\wedge$ q is T only if both p and q are T; otherwise it's F. It's associative and commutative.
- disjunction (or): p $\vee$ q is F only if both p and q are F; otherwise it's T. It's associative and commutative.
- exclusive or (xor): p $\oplus$ q is T only if exactly one of p and q is T; otherwise it's T. It's associative and commutative.



## Implication

- **implication**: p $\Rightarrow$ q is T only when p is F or q is T; it's F if p is T and q is F. It's equivalent to ($\neg$ p) $\vee$ q.

  Pronounced in *many* different ways:

  "p implies q", "if p then q", "q if p", "p only if q",

  "p is sufficient for q", "q is necessary of p", "q follows from p"

  Example: raining $\Rightarrow$ garden wet

  *Note:* Sipser uses $\rightarrow$ instead of $\Rightarrow$, but this will be confusing when we talk about functions.

- **contrapositive**: of p $\Rightarrow$ q is the equivalent $\neg$ q $\Rightarrow$ $\neg$ p.
- **two-way implication**: p $\Leftrightarrow$ q means (p $\Rightarrow$ q) $\wedge$ (q $\Rightarrow$ p). It's pronounced "p if and only if q" (abbreviated "p iff q") and "p is necessary and sufficient for q".

  Example: lightning $\Leftrightarrow$ thunder

  Proofs of $\Leftrightarrow$ are have two cases: $\Rightarrow$ (sufficiency) & $\Leftarrow$ (necessity)

## Sets

- Sets are collections of elements.
- Finite sets are usually written with elements in braces: e.g., {2, 3, 5, 7, 11}. The empty set {} is also written ∅.
- $x \in A$ indicates x is an element of the set A.
- $x \notin A$ indicates x is not an element of the set A.
- If A and B are sets, A = B means A and B have exactly the same elements
- $A \subseteq B$ indicates A is a **subset** of B: every element in A is also in B (or, equivalently, $x \in A$ implies $x \in B$.)
- $A \subset B$ indicates A is a **proper subset** of B: A is a subset of B but $A \neq B$.



## Some Common Sets

- The booleans: Bool = {T, F}
- The natural numbers: Nat (N)= {0, 1, 2, 3, …}. Note that Nat includes 0, essential for many proofs by induction.
- The integers: Int (Z) = {…, -2, -1, 0, 1, 2, …}
- The rationals = all ratios of two integers:
  Rat = {…, -1, -2/3, -1/2, -1/3, 0, 1/3, 1/2, 2/3, …}
- The reals: Real (R) = all points on the real number line; in addition to the rationals, includes irrationals (like π, *e*, √2). We'll soon prove that √2 is irrational.

Note that Nat ⊂ Int ⊂ Rat ⊂ Real.



## Set Builder Notation

The notation {*expression* | *conditions for expression*} is commonly used to describe sets. The vertical bar | is pronounced "such that", which is also abbreviated "s.t."

For example:

- Alternative definition of Nat = {i | i ∈ Int and i ≥ 0}
- Evens = {n | n ∈ Int and (n mod 2) = 0}
- Squares = {$x^2$ | x ∈ Nat}
- Ramanujan = {$x^3 + y^3$ | x,y ∈ Nat and there exist a,b ∈ Nat s.t. {a,b} ≠ {x,y} and $x^3 + y^3 = a^3 + b^3$ }.

I.e., Ramanujan numbers can be expressed as a sum of two cubes in at least two different ways. E.g., 1729 = $1^3 + 12^3 = 9^3 + 10^3$.



## Set Operations

- Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- Difference: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$ (sometimes written $A \setminus B$)
- Complement: $\overline{A} = U - A$, where U is some *universe* of elements understood from context.
- Powerset (set of all subsets): $\mathcal{P}(A) = \{ X \mid X \subseteq A\}$

E.g.

- PositiveEvens = Evens ∩ (Nat - {0})
- PositiveOdds = (Int - Evens) ∩ Nat
- $\mathcal{P}$(Bool) = { {}, {T}, {F}, {T,F} }

## Generalized Unions

- If S is a set of sets, then $\cup S = \{x \mid x \in A \text{ and } A \in S\}$

  E.g. $\cup\{\{2, 5\}, \{1\}, \{2, 3, 6\}\} = \{1, 2, 3, 5, 6\}$

- If S is a set of sets indexed by a set B and $C \subseteq B$, then $\cup_{(y \text{ in } C)} S_y = \{x \mid y \in C \text{ and } x \in S_y\}$

  E.g., suppose $i \in Nat$ and $S_i = \{n \cdot i \mid n \in Nat\}$

  Then $\cup_{(k \text{ in } \{2,3,5\})} S_k = \{m \mid m \text{ is a multiple of 2, 3, or 5}\}$

  (Hamming numbers)

- We can generalize intersections similarly.



## Properties of Set Operations

*Associativity*: $A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$

*Commutativity*: $A \cup B = B \cup A$; $A \cap B = B \cap A$

*Idempotence*: $A \cup A = A$; $A \cap A = A$

*Identity (union only)*: $A \cup \varnothing = A = \varnothing \cup A$

*Zero (intersection only)*: $A \cap \varnothing = \varnothing = \varnothing \cap A$

*Distributivity:*

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

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

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

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

*De Morgan's Laws:*

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

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



## Proofs = Mathematical Arguments

- How can we show that the claimed set properties are actually true?
- A **proof** is a convincing logical argument that a statement is true.
- A criminal trial demands proof beyond a reasonable doubt.
- A mathematician demands proof beyond all doubt.



## How to Prove Two Sets are Equal

To show A = B, we must show they contain the same elements. In other words:

(1) If $x \in A$ then $x \in B$ (i.e., $A \subseteq B$)

(2) If $x \in B$ then $x \in A$ (i.e., $B \subseteq A$)

So A = B if and only if $A \subseteq B$ and $B \subseteq A$.

(recall "if and only if" is also written "iff" and $\Leftrightarrow$)

## Batting practice

Prove DeMorgan's Law (1): For any two sets A and B,

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

*We need to show two subset inclusions:*

*1)* $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$

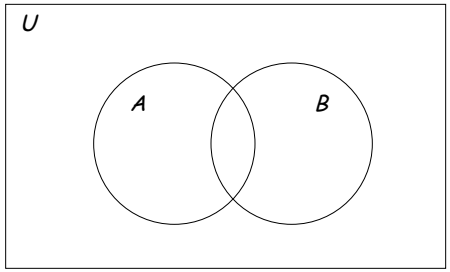
*2)* $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$



## Alternative Approach: Proof by Picture

DeMorgan's Law. For any two sets A and B,

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




* Such pictures are known as Venn diagrams



## Case Analysis in Proofs with Unions

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

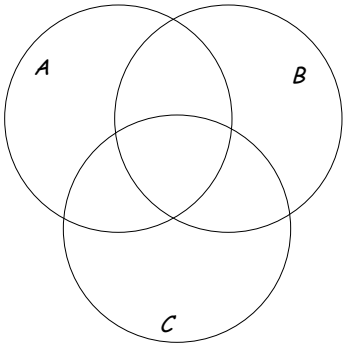
(1) Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

(2) Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$



## Another Proof by Picture

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



## Proof by Algebra

Sometimes we can construct a proof by algebraic properties.

For example, suppose we are given:

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

Use other set properties to prove:

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

*Note: renaming is important!*



## Proof by Contradiction: Why is √2 Irrational?

This is a classic example of a *proof by contradiction*:

1. *Assume the opposite of what is to be proven:*

   Here, assume √2 is a rational number a/b.

2. *Show that a contradiction results from this assumption:*

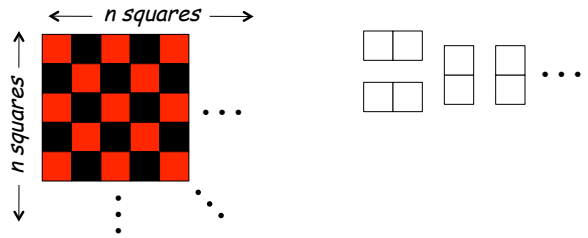
   In this case, $\sqrt{2} = a/b \Rightarrow 2b^2 = a^2$.
   But $a^2$ has an even number of prime factors and
   $2b^2$ has an odd number of prime factors.

   This cannot be! **X**



## Checkerboards and Dominoes

You have an n x n checkerboard and lots of dominoes






Can you cover the checkerboard with the dominoes if

- n is even? *(proof by construction)*
- n is odd? *(proof by contradiction)*
- n is even, but you cut out the red corners? *(contradiction)*