

Mathematical Foundations

Definitions and (Some) Proof Techniques (Part 1)

Wednesday, September 5, 2007

Reading: Stoughton 1.1

CS235 Languages and Automata

Department of Computer Science
Wellesley College

Goals for today and tomorrow

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

- Sets
- Tuples
- Relations
- Functions
- Graphs

See a few examples of some proof techniques (more in Lec # 3)

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

You can find most of this in Section 1.1 of Stoughton, though some of my definitions and notations differ slightly (e.g., proper subset notation, the definition of a function).

Basic Logic

- reasoning about boolean values T (true) and F (false)
- negation (not): $\neg T = F$; $\neg F = T$; $\neg(\neg p) = p$
- 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.
- 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 $(\neg p) \vee q$. It's also written:
"p implies q", "if p then q", "q if p", "p only if q"
- 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 also written "p if and only if q" or "p iff q".

Definitions & proofs 2-3

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 \emptyset .
- $x \in A$ 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 $A \neq B$. (Stoughton uses a different notation.)

Definitions & proofs 2-4

Some Common Sets

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

Note that $\text{Nat} \subset \text{Int} \subset \text{Rat} \subset \text{Real}$.

Definitions & proofs 2-5

Set Builder Notation

The notation $\{\text{expression} \mid \text{conditions for expression}\}$ is commonly used to describe sets. The vertical bar \mid is pronounced “such that”, which is also abbreviated “s.t.”

For example:

- Alternative definition of $\text{Nat} = \{i \mid i \in \text{Int} \text{ and } i \geq 0\}$
- Evens = $\{n \mid n \in \text{Int} \text{ and } (n \bmod 2) = 0\}$
- Squares = $\{x^2 \mid x \in \text{Nat}\}$
- Ramanujan = $\{x^3 + y^3 \mid x, y \in \text{Nat} \text{ and there exist } a, b \in \text{Nat} \text{ s.t. } \{a, b\} \neq \{x, y\} \text{ and } x^3 + y^3 = a^3 + b^3\}$.

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

Definitions & proofs 2-6

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): $P(A) = \{X \mid X \subseteq A\}$

E.g.

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

Definitions & proofs 2-7

Generalized Unions

- If S is a set of sets, then $\bigcup S = \{x \mid x \in A \text{ and } A \in S\}$
E.g. $\bigcup \{ \{2, 5\}, \{1\}, \{2, 3, 6\} \} = \{1, 2, 3, 5, 6\}$
- If S is a set of sets indexed by a set B and $C \subseteq B$,
then $\bigcup_{(y \text{ in } C)} S_y = \{x \mid y \in C \text{ and } x \in S_y\}$
E.g., suppose $S_i = \{n \mid n \in \text{Nat} \text{ and } n \text{ is a multiple of } i\}$
Then $\bigcup_{k \text{ in } \{2,3,5\}} S_k = \{n \mid n \text{ is a multiple of } 2, 3, \text{ or } 5\}$ (Hamming numbers)
- We can generalize intersections similarly.

Definitions & proofs 2-8

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): $A \cup \emptyset = A = \emptyset \cup A$
- Zero (intersection only): $A \cap \emptyset = \emptyset = \emptyset \cap A$
- Distributivity:
 - (1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
 - (2) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
 - (3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 - (4) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
- De Morgan's Laws:
 - (1) $\overline{A \cup B} = \overline{A} \cap \overline{B}$
 - (2) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Definitions & proofs 2-9

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.



Definitions & proofs 2-10

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 $B \subseteq A$.

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

Definitions & proofs 2-11

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:

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

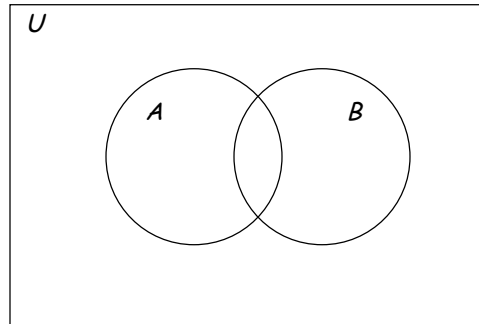
$$2) \overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$$

(See Stoughton for a proof of Distributivity Law (1).)

Definitions & proofs 2-12

Alternative Approach: Proof by Picture

DeMorgan's Law. For any two sets A and B ,
 $\overline{A \cup B} = \overline{A} \cap \overline{B}$.



Definitions & proofs 2-13

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:

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

Definitions & proofs 2-14

Proof by Contradiction: Why is $\sqrt{2}$ Irrational?

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

1. *Assume the opposite of what is to be proven:*
In this case, assume $\sqrt{2}$ 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 the prime factorization of a^2 has an even number of elements and the prime factorization of $2b^2$ has an odd number of elements! This cannot be! **X**