CIS 23
Mathematical Background *

Eric Pacuit

March 20, 2005

Introduction

- What is an algorithm?
- Thinking about algorithms
- What is the complexity of an algorithm?
- Comparing algorithms
- Proving facts about algorithms
- Recursive algorithms

What is an algorithm?

- Finite set of actions to achieve a certain outcome, i.e. to solve a problem

- Leave out implementation details, I.e hardward/software independant: The choice of language or machine should not change the outcome of the algorithm

- How should we write down an algorithm? What language should we use?

Psuedo-code conventions

- Often to explain or describe an algorithm informally, we use the language of (non-formal) set theory.

Basic Set Theory

There are two basic ways to define a set:

1. List all the elements of the set. Each element should be separated by a comma and contained between curly brackets ({}). For example suppose A is the set of the first 5 letters of the alphabet. Then $A = \{a, b, c, d, e\}$.

2. Write down a property that **all** elements of the set have in common. For example if A is the set of all positive integers, then $A = \{x \mid x \geq 0 \text{ and } x \text{ is an integer}\}$. This is read "$x$ such that x is greater than or equal to zero and x is an integer".

Basic Definitions

Suppose A and B are two sets.

Definition 1 (Universal Set) *The* **Universal Set** *will be represented by the letter* U.

Definition 2 (Element) *If we want to say* x *is an element of* A, *then we write* $x \in A$

Definition 3 (Subset) $A \subseteq B$ *if and only if every element of* A *is also an element of* B

Definition 4 (Union) $A \cup B = \{x | x \in A \textit{ or } x \in B\}$

Definition 5 (Intersection) $A \cap B = \{x \mid x \in A \textit{ and } x \in B\}$

Definition 6 (Complement) $A^{\mathsf{C}} = \{x \mid x \notin A\}$

Definition 7 (Set Difference) $A \backslash B = \{x \mid x \in A \textit{ and } x \notin B\}$

Definition 8 (Cross Product) $A \times B = \{(a, b) \mid a \in A \textit{ and } b \in B\}$

Definition 9 (Empty Set) *The set with no elements is denoted by* $\varnothing$

Definition 10 (Power Set) *The poser set of a set* S *is the set of all subsets of* S, including S and $\varnothing$, *and is denoted* 2^S *or* $\mathcal{P}(S)$

Definition 11 (Cardinality of a Set) *The cardinality of a finite set* S *is the total number of elements in* S*, and is denoted* $|S|$.

Definition 12 (Partition) *A* **partition** *of a set* S *is a collection of sets* $\mathcal{S} = \{S_1, S_2, \ldots\}$ *(possibly infinite) such that*

- *the sets are* **pairwise disjoint**, *that is* $S_i, S_j \in \mathcal{S}$ *and* $i \neq j$ *imply* $S_i \cap S_j = \varnothing$

- *their union is* S, *that is,*

$$S = \cup_{S_i \in \mathcal{S}} S_i$$

Some Useful Properties

- (Distributive Law) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- (Distributive Law) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (DeMorgan's Law) $(A \cup B)^C = A^C \cap B^C$
- (DeMorgan's Law) $(A \cap B)^C = A^C \cup B^C$
- $(A^C)^C = A$
- $|A \times B| = |A| \cdot |B|$
- $|A \cup B| = |A| + |B| - |A \cap B|$

- $|2^A| = 2^{|A|}$

- $A = B$ iff $A \subseteq B$ *and* $B \subseteq A$

You should be able to prove each of these properties

Relations

Definition 13 (Binary Relation) *A binary relation R on two sets A and B is a subset of the Cross Product $R \subseteq A \times B$*

You should be familiar with many binary relations: $=, \leq, \geq, <, >$. For example the binary relation $\leq \subseteq \mathbb{N} \times \mathbb{N}$ is the set

$\{(a,b) \mid a, b \in \mathbb{N}$ and a is less than or equal to $b\}$

Suppose R is a relation. We often write aRb to mean $(a,b) \in R$.

Some Important Properties of Relations

Suppose R is any relation on A and, that is $R \subseteq A \times A$. Suppose $a, b, c \in A$.

Reflexivity aRa for all $a \in A$ (*in this case* $A = B$)

Symmetry if aRb then bRa

Antisymmetric if aRb and bRa then $a = b$

Transitive if aRb and bRc then aRc

Definition 14 (Equivalence Relation) *A relation R that is reflexive, symmetric and transitive is said to be an* **equivalence relation**

Definition 15 (Equivalence Class) *If R is an equivalence relation on A and B, then for each $a \in A$, the equivalence class of a, denoted by $[a]$ is the following set*

$$[a] = \{b \in B \mid aRb\}$$

Definition 16 (Partial Order) *A relation that is reflexive, antisymmetric and transitive is said to be a* **partial order***.*

Theorem 17 *The equivalence classes of any equivalence relation R on a set A forms a partition of A, and any partition of A determines an equivalence relation on A for which the sets in the partition are the equivalence classes.*

Proof Suppose R is an equivalence relation on A. We must show that the equivalence classes of R forms a partition of A.

1. Each equivalence class is non-empty, since aRa for all $a \in A$.

2. Clearly A is union of all the equivalence classes (since each element of A belongs to at least one equivalence class)

3. We must show any two equivalence classes are disjoint. Let $[a], [b]$ be two distinct equivalence classes. Suppose $c \in [a] \cap [b]$. Then aRc and bRc. Hence by symmetry, cRb. And so by transitivity, aRb.

   Let $x \in [a]$, then xRc and by the above argument xRb (Why?), and so $x \in [b]$. Thus $[a] \subseteq [b]$. Using a similar argument, we can show $[b] \subseteq [a]$. Therefore $[a] = [b]$, which contradicts the fact that $[a]$ and $[b]$ are *distinct* equivalence classes.

For the second part of the theorem, suppose $\mathcal{A} = \{A_1, \ldots, A_n\}$ is any partition of A. Define $R = \{(a, b) \mid a \in A_i \text{ and } b \in A_i\}$. It will be left up to you to show R is reflexive, symmetric and transitive.
$\blacksquare$

Graph Theory

We have seen that you can use Venn Diagrams to visualize sets, but what about relations? Can we visualize a relation?

Perhaps, not so surprising, but the answer is yes. We can use a graph to visualize a relation:

Suppose $A = \{a, b, c\}$ and $R = \{(a, a), (a, b), (c, b), (c, c)\}$. Then the following is a "picture" of this relation:

Actually, the field of Graph Theory is used for much more than just visualizing relations. We will talk a lot more about Graph Theory later in the semester.

Definition 18 *A* **Graph** *is a pair* (V, E)*, where* V *is a set of nodes (usually finite) and* $E \subseteq V \times V$ *is called the set of edges.*

Graph's can be directed or undirected. A graph is undirected if for each there are no arrows. This can be stated by saying that E is assumed to be symmetric. It should be clear from the context if we mean a directed graph or an undirected graph.

Functions

We will think of a function as a special type of relation:

Definition 19 (Function) *a function f is a binary relation on A and B such that for all $a \in A$, there exists a $b \in B$ such that $(a, b) \in f$. We will often write $f : A \to B$ and if $(a, b) \in f$, we will write $f(a) = b$.*

Suppose $f : A \to B$ is a function. A is said to be the **domain** and B the **codomain**.

Definition 20 (Image) *The image of a set $A' \subseteq A$ is the set:*

$$f(A') = \{b \mid b = f(a) \text{ for some } a \in A'\}$$

Definition 21 (Range) *The range of a function is the image of its domain.*

Suppose $f : A \to B$ is a function.

Definition 22 (Surjection) *f is a surjection (or onto) if its range is equal to its codomain. I.e., f is surjective iff for each $b \in B$, there exists an $a \in A$ such that $f(a) = b$*

Definition 23 (Injection) *f is an injection (or 1-1) if distinct elements of the domain produce distinct elements of the codomain. I.e., f is 1-1 iff $a \neq a'$ implies $f(a) \neq f(a')$, or equivalently $f(a) = f(a')$ implies $a = a'$.*

Definition 24 (Bijection) *f is a bijection if it is injective and surjective. In this case, f is often called a one-to-one correspondence.*

Properties of Exponentials

For all real $a \neq 0$, m, and n, we have the following identities:

$$
\begin{aligned}
a^0 &= 1 \\
a^1 &= a \\
a^{-1} &= 1/a \\
(a^m)^n &= a^{mn} \\
(a^m)^n &= (a^n)^m \\
a^m a^n &= a^{m+n}
\end{aligned}
$$

Properties of Logarithms

Definition 25 (Logarithm) $\log_b a = n$ *if and only if* $b^n = a$

For all real $a > 0$, $b > 0$, $c > 0$ and n,

$$\begin{aligned}
a &= b^{\log_b a} \\
\log_c(ab) &= \log_c a + \log_c b \\
\log_b(a^n) &= n \log_b a \\
\log_b a &= \frac{\log_c a}{\log_c b} \\
\log_b(1/a) &= -\log_b a \\
\log_b a &= \frac{1}{\log_a b} \\
a^{\log_b n} &= n^{\log_b a}
\end{aligned}$$

For this course we will assume $\log n = \log_2 n$ **and** $\ln n = \log_\mathrm{e} n$

Summations

Given a sequence $a_1, a_2, \ldots$ of numbers, the finite sum $a_1 + a_2 + \cdots + a_n$ can be written as

$$\sum_{i=1}^{n} a_i$$

The infinite sum $a_1 + a_2 + \cdots$ can be written as

$$\sum_{i=1}^{\infty} a_i$$

and is interpreted to mean

$$\lim_{n \to \infty} \sum_{k=1}^{n} a_k$$

If the limit does not exist, then the sum is said to **diverge**; otherwise it **converges**.

Arithmetic Series $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$

Linearity $\sum_{k=1}^{n}(ca_k+db_k) = c\sum_{k=1}^{n} a_k+d\sum_{k=1}^{n} b_k$

Geometric Series For real $x \neq 1$, $\sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}$; and when $|x| < 1$, $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$

Harmonic Series $\sum_{k=1}^{n} \frac{1}{k} = \ln n + C$, for some constant C.