CSCB36

Summary Of Vassos Hadzilacos'

Course notes for CSC B36/236/240

INTRODUCTION TO THE THEORY OF COMPUTATION

Computer & Mathematical Sciences
UNIVERSITY OF TORONTO
SCARBOROUGH

Instructor:	**Dr.Nick Cheng**
Email:	nick@utsc.utoronto.ca
Office:	IC348
Office Hours:	TBA

1 PRELIMINARIES

Sets: A collection of objects **(Elements)**.
If an object a is an element of set A, we say that a is a **member of** A; denoted $a \in A$
The collection that contains no elements is called the **empty** or **null** set' denoted $\varnothing$
Cardinality/Size: Number of elements in a set. The **cardinality** of set A is denoted $|A|$, and is a non-negative integer. If A has a infinite number of elements, $|A| = \infty$, and if $A = \varnothing$, then $|A| = 0$.

Extensional Description: Describing a set by listing its elements explicitly, e.g. $A = \{1, 4, 5, 6\}$
Intentional Description: Describing a set by stating a property that characterizes its elements, e.g. $A = \{x|\text{x is a positive integer less than } 5\}$

Let A and B be sets.
If every element of A is also an element of B,
then A is a **subset** of B ($A \subseteq B$), and B is a **superset** of A ($B \supseteq A$).

If $A \subseteq B$ and $B \subseteq A$, then A is **equal** to B ($A = B$).
If $A \subseteq B$ and $A \neq B$, then A is a **proper subset** of B; ($A \subset B$ and B) is a **proper superset** of A ($B \supset A$).
Note the empty set is a subset of every set, and a proper subset of every set other than itself.

The **union** of A and B ($A \cup B$), is the set of elements that belong to A or B (or both).
The **intersection** of A and B ($A \cap B$), is the set of elements that belong to both A and B.
If no elements belongs to both A and B, their intersection is empty, and they are **disjoint** sets.
The **difference** of A and B, ($A - B$), is the set of elements that belong to A but do not belong to B.
Note that: $A - B = \varnothing \iff A \subseteq B$
The **union** and **intersection** can also be defined for an arbitrary (even infinite) number of sets.
let I be a set of indices, such that for each $i \in I$ there is a set A_i

$$\cup_{i \in I} A_i = \{x : \text{for some } i \in I, x \in A_i\}$$
$$\cap_{i \in I} A_i = \{x : \text{for each } i \in I, x \in A_i\}$$

The **powerset** is the set of subsets, e.g. $A = \{a, b, c\}, \mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
Partition of a set A, is pairwise disjoint subsets of A whose union is A. A partition of set A is a set $\mathcal{X} \subseteq \mathcal{P}(A)$, such that:

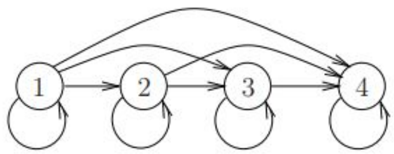
(i) for each $X \in \mathcal{X}, X \neq \varnothing$
(ii) for each $X, Y \in \mathcal{X}, X \neq Y$
(iii) $\cup_{X \in \mathcal{X}} X = A$

Ordered Pair: A mathematical construction that bundles two objects a, b together, in a particular order, denoted (a, b). By this definition, $(a, b) = (c, d) \iff a = c \wedge b = d$ and $(a, b) \neq (b, a)$ unless $a = b$.
We define an ordered pair (a, b) as the set $\{\{a\}, \{a, b\}\}$. We can also define ordered triples as ordered pairs, (a, b, c) can be defined as $(a, (b, c))$. This definition holds for ordered quadruples, quintuples, and ordered n-tuples for any integer $n > 1$.

Cartesian Product of A and B is denoted $A \times B$ and is the set of ordered pairs (a, b) where $a \in A, b \in B$.
$|A \times B| = |A| \cdot |B|$, note that if A, B are distinct nonempty sets, $A \times B \neq B \times A$
The Cartesian product of $n > 1$ sets $A_1, A_2, \ldots, A_n$ denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in A_i, i \in [1, n]$

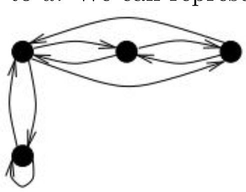
Relation R between sets A and B is a subset of the Cartesian product $A \times B$ ($R \subseteq A \times B$).
Arity: number of sets involved in the relation.
Two relations are **equal** if they contain exactly the same sets of ordered pairs. The two relations must refer to the exact same set of ordered pairs.

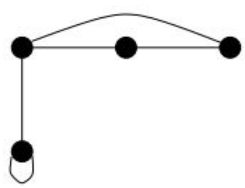
A binary relation (**arity** 2) between elements of the **same** set, can be represented graphically as a **directed graph**.
E.g. $R = \{(a, b)|a, b \in \{1, 2, 3, 4\}$ and $a \leq b\}$



R is a **reflexive** relation, if for each $a \in A, (a, a) \in R$, e.g. the relation $a \leq b$ between integers is reflexive, while $a < b$ is not.

R is a **symmetric** relation if for each $a, b \in R, (b, a) \in R$,
E.g. $R_1 = \{(a, b)|a$ and b are persons with atleast one parent in common$\}$ is symmetric. In the directed graph that represents a symmetric relation, whenever there is an arrow from a to b, there is an arrow from b to a. We can represent this with an **undirected graph**.





directed graph on the left, undirected graph on the right

R is a **transitive** relation if for each $a, b, c \in A, (a, b) \in R \wedge (b, c) \in R \longrightarrow (a, c) \in R$,
E.g. $R = \{(a, b)|a$ and b are persons and a is an ancestor of b$\}$
We see that if a is an ancestor of b, and b is an ancestor of c, then a is an ancestor of c.

R is an **equivalence relation** if it is reflexive, symmetric and transitive,
E.g. $R = \{(a, b)|a$ and b are persons with the same parents$\}$
a and a are the same person, thus have the same parents ($(a, a) \in R$), R is **reflexive**.
a and b share the same parents, b and a share the same parents ($(a, b) \in R, (b, a) \in R$), R is **symmetric**.
a and b share the same parents, b and c share the same parents, a and c must share the same parents. R is **transitive**.
thus we say R is an **equivalence relation**.

Let R be an equivalence relation and $a \in A$. The **equivalence class** of a under R is defined as the set $R_a = \{b|(a, b) \in R\}$, i.e., the set of all elements that are related to a by R.
If R is reflexive, then we know $\forall a \in A, R_a \neq \varnothing$
If R is transitive, then we know $\forall a, b \in R, R_a \neq R_b \longrightarrow R_a \cap R_b = \varnothing$

R is **partial order** if it is anti-symmetric and transitive.
R is **total order** if it is partial order and satisfies for each $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$.

Let A and B be sets. A **function** f from A to B is a special kind of relation where each element $a \in A$ is associated with one element in B.
The relation $f \subseteq A \times B$ is a **function** if for each $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in f$.

We write $f : A \to B$ to denote that f is a function from A to B, where A is the **domain** of the function, and B is the **range**.

The function $f : A \to B$ is:
onto/surjective if for every $b \in B$ there is at least one $a \in A$ such that $f(a) = b$
one-to-one/injective if for every element $b \in B$, there is at most one element $a \in A$ such that $f(a) = b$
bijective if it is **one-to-one** and **onto**, if $f : A \to B$ is a bijection, then $|A| = |B|$.
The **restriction** of a function $f : A \to B$ is to a subset A' of its domain, denoted $f|A'$, is a function $f' : A' \to B$ such that for every $a \in A, f'(a) = f(a)$.
An **initial segment** I of $\mathbb{N}$ is a subset of $\mathbb{N}$ with the following property: for any element $k \in I$, if $k > 0$ then $k - 1 \in I$. Thus, an initial segment of $\mathbb{N}$ is either the empty set, or the set $\{0, 1, 2, \ldots, k\}$ for some nonnegative integer k, or the entire set $\mathbb{N}$

let A be a set. A **sequence over** A is a function $\sigma : I \to A$, where I is an initial segment of $\mathbb{N}$.

Intuitively $\sigma(0)$ is the first element in the sequence, $\sigma(1)$ is the second and so on. if $I = \varnothing$, then σ is the **empty** or **null** sequence, denoted ϵ. if $I = \mathbb{N}$ then σ is an infinite sequence; otherwise it is a finite sequence. The **length** of σ is $|I|$ -i.e., the cardinality of I.

let $\sigma : I \to A$ and $\sigma' : I' \to A$ be sequences over the same set A, and suppose that σ is finite.
Informally, the **concatenation** of σ and σ', denoted $\sigma \circ \sigma'$ and sometimes as $(\sigma\sigma')$, is the sequence over A that is obtained by juxtaposing the elements of σ' after the elements of σ.
More precisely, if $I' = \mathbb{N}$ (i.e., σ is infinite), then if we let $j = \mathbb{N}$; otherwise let J be the initial segment $\{0, 1, \ldots, |I| + |I'| - 1\}$. Then $\sigma \circ \sigma'; J \to A$, where for any $i \in I, \sigma \circ \sigma'(i) = \sigma(i)$, and for any $i \in I, \sigma \circ \sigma(|I| + i) = \sigma'(i)$.
Informally, the **reversal** of σ, denoted σ^R, is the sequence of the elements of σ in revresed order, more precisely, $\sigma^R : I \to A$ is the sequence so that, for each $i \in I, \sigma^R(i) = \sigma(|I| - 1 - i)$.

Since, strictly speaking, a sequence is a function of a special kind, sequences $\sigma : I \to A$ and $\sigma' : I \to A$ is equal if and only if, for every $k \in I, \sigma(k) = \sigma'(k)$.

From the definitions of concatenation and equality of sequences, it is easy to verify the following facts:

1. For any sequences $\sigma, \epsilon \circ \sigma = \sigma$; if σ is finite, $\sigma \circ \epsilon = \sigma$.
2. For any sequences σ, τ over the same set, if is finite and $\circ\sigma = \sigma$, then $= \epsilon$; if σ is finite and $\sigma\circ = \sigma$, then $= \epsilon$.

A sequence σ is a **subsequence** of sequence if the elements of σ appear in and do so in the same order. for example $\langle b, c, f\rangle$ is a subsequence of $\langle a, b, c, d, e, f, g\rangle$. Note that we do not require elements of σ to be consecutive elements of , we only require that hey appear in the same order as they do in .

If, in fact, the elements of σ are consecutive elements of , we say that σ is a **contiguous subsequence** of τ.
Formally the definition of the subsequence relationship between sequences is as follows. let A be a set, I and J be initial segments of $\mathbb{N}$ such that $|I| \leq |J|$, and $\sigma : I \to A, J \to A$ be sequences over A. The sequence σ is a subsequence of if there is an increasing function $f : I \to J$ so that, for all $i \in I, \sigma(i) = (f(i))$. If σ is a subsequence of and is not equal to , we say that σ is a **proper subsequence** of .

An **alphabet** is a nonempty set Σ; the elements of an alphabet are called its **symbols**. A **string** (over alphabet Σ) is simply a finite sequence over Σ.
The empty sequence is a string and is denoted, as usual, ϵ. The set of all strings over alphabet Σ is denoted $\Sigma*$. Note that $\epsilon \in \Sigma*$, for any alphabet Σ.

Since strings are simply (finite) sequences over a specified set, various notions defined for sequences apply to string as well. In particular, this is the case for the notion of length which must now be a natural number, and cannot be inf. We use the term **substring** as synonymous to contiguous subsequence.

Let A be a finite set, A **permutation** of A is a sequence in which every element of A appears once and only once. For example if $A = \{a, b, c, d\}$ then $\langle b, a, c, d\rangle, \langle a, c, d, b\rangle \ldots$
Sometimes we speak of permutations of a sequence rather than a set. In this case, the definition is as follows: Let $\alpha : I \to A$ and $: I \to A$ be finite sequences over A. The sequence is a permutaiton of α is there is a bijective function $f : I \to I$ so that for every $i \in I, (i) = \alpha(f(i))$

2 INDUCTION

Fundamental properties of the natural numbers
The natural numbers are nonnegative integers $0, 1, \ldots$ denoted $\mathbb{N}$;
Principle of well-ordering: Any nonempty subset A of $\mathbb{N}$ contains a minimum element; i.e., $\forall A \subseteq N, \ni$: $A \neq \varnothing, \exists a \in A, \ni: \forall a' \in A, a \leq a'$
This applies to all nonempty subsets of $\mathbb{N}$ and to infinite subsets of $\mathbb{N}$. This principle does not apply to other sets.

Simple induction
Let A be any set that satisfies the following properties:
$0 \in A$
$\forall i \in \mathbb{N}, i \in A \Rightarrow i + 1 \in A$
Then A is a superset of $\mathbb{N}$.

Complete induction
Let A be any set that satisfies the following property:
$\forall i \in \mathbb{N}$, if evrey natural number less than $i \in A$ then $i \in A$.
Then A is a supserset of $\mathbb{N}$.
This principle is similar to the principle of simple induction, although there are some differences.
The requirement that $0 \in A$ is implicit as for any $i \in \mathbb{N}, 0 \leq \mathbb{N} \Rightarrow 0 \in A$. The second difference is we require i to be an element of A if all elements preceding i are in A. In contrast, we require $i \in A$ if $i - 1 \in A$.

Equivalence of the three principles
Theorem 1.1 The principle of well-ordering, induction, and complete induction are equivalent.
Proof. We prove this by establishing a "cycle" of implications. Specifically, we prove that (a) well-ordering implies induction, (b) induction implies complete induction, and (c) complete induction implies well ordering.
(a) well-ordering implies induction: Assume that the principle of well-ordering holds. We will prove that principle of induction is also true.
let A be a set that satisfies the following:
$0 \in A$
$\forall i \in \mathbb{N}, i \in A \Rightarrow i + 1 \in A$