Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Lecture 0.5: Review
Winter 2019

1 Things to Remember

Since CISC 102 is a prerequisite for this course, we will assume that you already have knowledge of each of the topics covered in that course. However, since some of you might not have taken CISC 102 recently, we will review some of the "big ideas" from that course before we begin.

1.1 Set Theory

A **set** is a collection of items that are related in some way by a common property or rule. Each item in the set is called an **element**.

Two of the most common sets we will see in this course are the set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ and the set of integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. Computer scientists are also particularly interested in the set of binary digits $\mathbb{B} = \{\texttt{0}, \texttt{1}\}$.

1.1.1 Definitions

A variety of notations exist for illustrating connections between elements and sets, or between sets and other sets. The **inclusion** of an element in a set is denoted by $\in$, and the exclusion of an element from a set is denoted by $\notin$.

For two sets A and B, if all elements of A are also elements of B, then A is a **subset** of B and we write $A \subseteq B$. Similarly, if all elements of A are also elements of B and B contains at least one element that A does not contain, then A is a **proper subset** of B and we write $A \subset B$.

We say that two sets A and B are **disjoint** if no element of A is an element of B and vice versa.

If we reflect the subset symbols in the vertical axis (to get the symbols $\supseteq$ and $\supset$), then we get the **superset** and **proper superset** notations, respectively. The definitions of these notations should be clear.

We can define **equality** of sets by using the subset and superset notations. For two sets A and B, if $A \subseteq B$ and $A \supseteq B$, then $A = B$.

There are two special sets. The **empty set**, denoted by $\emptyset$, contains no elements. The **universal set**, denoted by $\mathcal{U}$, contains all elements (specifically, all elements satisfying the property or rule under consideration). For all sets A, we have $\emptyset \subseteq A \subseteq \mathcal{U}$.

The **cardinality** (or **size**) of a set A, denoted by $|A|$, is the number of elements in A. If $|A| = m$ where $m \in \mathbb{N}$, then we say that A is a **finite** set. Otherwise, we say that A is an **infinite** set.

The **power set** of a set A, denoted by $\mathcal{P}(A)$, is the set consisting of all subsets of A. If A is a finite set, then $|\mathcal{P}(A)| = 2^{|A|}$.

1.1.2 Operations

We can take a number of sets and apply operations to each of those sets to get new sets as a result. Assume that our sets are called A and B.

The only unary set operation we have in our toolbox is the **complement** operation, denoted A^{C}. The complement of a set contains all elements that are in our universal set $\mathcal{U}$, but that are not also in A.

We have many binary set operations, and the most common are as follows. The **union** of two sets, denoted $A \cup B$, consists of all elements that are contained in A or in B (or in both). Similarly, the **intersection** of two sets, denoted $A \cap B$, consists of all elements that are contained in A and in B. Finally, the **difference** of two sets, denoted $A \setminus B$, consists of all elements that are in A, but that are not also in B.

Clearly, we can define our complement operation in terms of our difference operation by taking $A^{\mathsf{C}} = \mathcal{U} \setminus A$. From this, we also see that $\mathcal{U}^{\mathsf{C}} = \emptyset$ and $\emptyset^{\mathsf{C}} = \mathcal{U}$.

1.1.3 Algebra of Sets

The algebra of sets, also called the laws of set theory, defines the fundamental properties of sets and set operations that allow us to do interesting (and mathematically correct) things with sets. The word "algebra" in this context is a term of art, similar to how we use the word when we discuss numbers and equations.

The results here will be presented without justification. You will not be expected to memorize these results, but they may come in handy as we discuss future topics.

Proposition 1. *Let A, B, and C be sets. Then each of the following statements are true:*

1. *Idempotent laws: $A \cup A = A$ and $A \cap A = A$.*
2. *Identity laws: $A \cup \emptyset = \emptyset \cup A = A$ and $A \cap \mathcal{U} = \mathcal{U} \cap A = A$.*
3. *Null laws: $A \cup \mathcal{U} = \mathcal{U} \cup A = \mathcal{U}$ and $A \cap \emptyset = \emptyset \cap A = \emptyset$.*
4. *Complement laws: $A \cup A^{\mathsf{C}} = \mathcal{U}$ and $A \cap A^{\mathsf{C}} = \emptyset$.*
5. *Involution law: $(A^{\mathsf{C}})^{\mathsf{C}} = A$.*
6. *Commutative laws: $A \cup B = B \cup A$ and $A \cap B = B \cap A$.*
7. *Associative laws: $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$.*
8. *Distributive laws: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*
9. *Absorption laws: $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$.*
10. *De Morgan's laws: $(A \cup B)^{\mathsf{C}} = A^{\mathsf{C}} \cap B^{\mathsf{C}}$ and $(A \cap B)^{\mathsf{C}} = A^{\mathsf{C}} \cup B^{\mathsf{C}}$*

1.2 Relations and Functions

Relations and functions are mappings from one set to another. The set being mapped from is called the **domain**, and the set being mapped to is called the **range** (or **codomain**). All functions are relations, but not all relations are functions.

To discuss the notions of relations and functions, we first require the notion of an **ordered pair**. An ordered pair (a, b) of elements a and b is similar to the set $\{a, b\}$, but with the added condition that the order of the elements matters. That is, $\{a, b\} = \{b, a\}$, but $(a, b) \neq (b, a)$ when $a \neq b$.

1.2.1 Relations

A (binary) **relation** between sets A and B is a subset of the set $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$, where $\times$ denotes the **cross product** of A and B. In other words, a relation is just a set of ordered pairs where each element in the pair is related in some way.

Given the set $A \times A$, we can save space by writing A^2. We can also write $A^2 \times A$ as A^3, and so on.

We can define a number of properties of a relation R on a set A depending on which ordered pairs belong to the relation. Let a_1, a_2, and a_3 be elements of A.

- R is **reflexive** if, for all $a \in A$, $(a, a) \in R$.
- R is **symmetric** if, whenever $(a_1, a_2) \in R$, $(a_2, a_1) \in R$.
- R is **antisymmetric** if, whenever $(a_1, a_2) \in R$ and $(a_2, a_1) \in R$, $a_1 = a_2$.
- R is **transitive** if, whenever $(a_1, a_2) \in R$ and $(a_2, a_3) \in R$, $(a_1, a_3) \in R$.

Note that, despite their names, the properties of symmetry and antisymmetry are not mutually exclusive. A relation may be both symmetric and antisymmetric.

1.2.2 Functions

A **function** from a set A to a set B is a special kind of relation where every element of A is mapped to exactly one element of B. If a function f maps an element $a \in A$ to another element $b \in B$, we often write $f(a) = b$ as a shorthand.

Similar to relations, we can define a number of properties of a function f from a set A to a set B.

- f is **injective** (or **one-to-one**) if, for all $a_1, a_2 \in A$ where $a_1 \neq a_2$, $f(a_1) \neq f(a_2)$.
- f is **surjective** (or **onto**) if, for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.
- f is **bijective** if it is both injective and surjective.

1.2.3 Equivalence Relations

An **equivalence relation** is a relation that is reflexive, symmetric, and transitive. The term "equivalence relation" comes from the fact that, if R is an equivalence relation, then two elements a and b are equivalent with respect to that relation if $(a, b) \in R$.

Equivalence relations partition sets into **equivalence classes**, or subsets where all elements in the subset are equivalent with respect to the given relation.

1.2.4 Orderings

An **ordering** is a relation with certain properties. There are two kinds of orderings.

A **partial order** on a set A, denoted by the generic symbol $\sqsubseteq$, is a relation that is reflexive, antisymmetric, and transitive. The tuple $(A, \sqsubseteq)$ is called a partially-ordered set (or **poset**).

A **total order** on a set A, similarly denoted by the generic symbol $\sqsubset$, has all the properties of a partial order plus the "comparability" property: for any elements a and b in A, either $a \sqsubset b$ or $b \sqsubset a$. This additional property distinguishes total orders from partial orders, since a partially-ordered set may contain incomparable elements. The tuple $(A, \sqsubset)$ is called a totally-ordered set (but, confusingly, we don't call it a "toset"). A total order is alternatively called a **linear order**.

Remark. Take care not to confuse the symbols $\sqsubseteq$ and $\sqsubset$ with the more-common symbols $\leq$ and $<$. The latter pair of symbols denote the specific relations of "less than or equal to" and "less than", respectively.

1.3 Principle of Mathematical Induction

Although we will discuss the principle of mathematical induction in greater depth during our lectures on proof techniques, we state it here as a refresher.

To begin, a **statement** is a sentence that is either true or false. For instance, both "$1 < 2$" and "$1 > 2$" are statements, where the first is true and the second is false. On the other hand, "*Portrait of a Man with Arms Akimbo* is a beautiful painting" is a subjective sentence and, therefore, it has no inherent truth value.

The principle of mathematical induction allows us to use two hypotheses about a statement to show that the truth of the statement holds for all natural numbers.

Proposition 2 (Principle of mathematical induction)**.** *Let P be a statement over the set of natural numbers $\mathbb{N}$. If*

1. *$P(1)$ is true; and*
2. *$P(n)$ being true for any $n = k$ implies that $P(n)$ is true for $n = k + 1$,*

then P is true for all $n \in \mathbb{N}$.

The related strong principle of mathematical induction uses a stronger hypothesis in the place of "step 2", but we will leave this discussion for later.

1.4 The Integers

Although we will mostly use natural numbers in this course, we will occasionally need to branch out and introduce negative numbers. Hence, it is handy to know a few basic properties of the set of integers $\mathbb{Z}$.

1.4.1 Properties

Integers can be positive, negative, or zero. If an integer x is negative, we can get its unsigned value by applying the **absolute value** operation, denoted $|x|$. We define the absolute value of an integer x as

$$|x| = \begin{cases} x & \text{if } x \geq 0; \\ -x & \text{if } x < 0. \end{cases}$$

If we add or multiply two natural numbers, then we get a natural number in return. However, if we subtract or divide two natural numbers, we are not always guaranteed to get a natural number in return. The following proposition outlines the state of affairs for integers.

Proposition 3. *Let $a, b \in \mathbb{Z}$. Then*

1. *if $c = a + b$, then $c \in \mathbb{Z}$;*
2. *if $c = a - b$, then $c \in \mathbb{Z}$;*
3. *if $c = ab$, then $c \in \mathbb{Z}$; and*
4. *if $c = a/b$ and $b \neq 0$, then $c \in \mathbb{Q}$, where $\mathbb{Q}$ is the set of rational numbers.*

1.4.2 Divisibility

In Proposition 3, we saw that dividing two integers produced a rational number, like $1/2$. But what if this rational number is itself an integer, like $4/2$?

Let $a, b \in \mathbb{Z}$ as before, with $b \neq 0$. If $c = a/b$ and $c \in \mathbb{Z}$, then we say that b **divides** a (or, equivalently, a is divisible by b). We denote divisibility by writing $b \mid a$.

We can represent the division operation formally via the following theorem:

Theorem 4 (Division theorem)**.** *For all $a, b \in \mathbb{Z}$ where $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.*

Finally, we review a few general properties of division (without proof).

Proposition 5. *Let $a, b, c \in \mathbb{Z}$.*

1. *If $a \mid 1$, then $|a| = 1$.*
2. *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*
3. *If $a \mid b$ and $b \mid a$, then $|a| = |b|$.*
4. *If $a \mid b$, then $a \mid bc$.*
5. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.*
6. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*