

# CSCE 355, Homework 1

The point of this homework is to make sure you understand basic concepts about sets, relations, functions, and strings, and that you can prove some facts about these things.

**Instructions:** Submit your homework as a pdf through Blackboard. The deadline is always 11:30pm on the due date found on the course homepage. If for some reason you cannot submit to Blackboard by the deadline, send your submission as an email attachment directly to the TA (Nicholas Miklaucic, [nmiklaucic@sc.edu](mailto:nmiklaucic@sc.edu)) and cc me ([fenner@cse.sc.edu](mailto:fenner@cse.sc.edu)) *before* the deadline. *No homework will be accepted (through either channel) after the deadline.* These instructions apply to all future homeworks as well.

## 1 Definitions

These concepts can mostly be found in the typeset Course Notes (<https://cse.sc.edu/~fenner/csce355/coursenotes/course-notes.pdf>), Sections 1–6.1. I will only lecture on the material in Section 6.1 (Strings), however, so you will not be tested directly on the material before that. It is good to go through it and familiarize yourself with all the concepts below, and at least attempt the non-string exercises. I use the symbol “ $:=$ ” throughout to mean “equals by definition.” I invite you to refer back to these definitions throughout the course as a kind of crib sheet. I may add more to this section as time goes on.

### 1.1 Sets

Below are standard definitions of set relations and operations. Union, intersection, difference, and symmetric difference are called *Boolean* operations because they are defined by using just the Boolean connectives inside the set formers. For any sets  $A$  and  $B$ ,

**Membership:**  $a \in A$  means  $a$  is a member (or element) of the set  $A$ . ( $a$  could be any object.)

**Subset:**  $A \subseteq B$  means that for all  $a \in A$  we have  $a \in B$ . ( $A \subseteq B$  and  $B \subseteq A$  implies  $A = B$ .)

**Union:**  $A \cup B := \{x : x \in A \text{ or } x \in B\}$ . ( $\cup$  is commutative and associative.)

**Intersection:**  $A \cap B := \{x : x \in A \text{ and } x \in B\}$ . ( $\cap$  is commutative and associative.)

**Difference (Relative Complement):**  $A - B := \{x : x \in A \text{ and } x \notin B\}$ . (also written  $A \setminus B$ .)

**Symmetric Difference:**  $A \triangle B := (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$ .

**The Empty Set:**  $\emptyset$  or  $\{\}$ . ( $\emptyset$  has no members;  $\emptyset \subseteq A$  for all sets  $A$ .)

**Ordered Pairs:**  $(a, b) := \{\{a\}, \{a, b\}\}$  for any  $a$  and  $b$ . ( $(a, b) = (c, d)$  implies  $a = c$  and  $b = d$ .)

**Cartesian Product:**  $A \times B := \{(a, b) : a \in A \text{ and } b \in B\}$ .

**Powerset:**  $2^A := \{S : S \subseteq A\}$ .

**Cardinality:** The *cardinality* of  $A$  (denoted  $|A|$ ) is the number of elements of  $A$ .

We have two distributive laws:  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  and  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$  for all sets  $A, B, C$ .

## 1.2 Numbers

We let  $\mathbb{N} := \{0, 1, 2, \dots\}$ , and the elements of  $\mathbb{N}$  are the *natural numbers*. We include 0 as a natural number even though some books don't.

We let  $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ , and the elements of  $\mathbb{Z}$  are the *integers*.

We let  $\mathbb{Q} := \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$ , and the elements of  $\mathbb{Q}$  are the *rational numbers*.

We let  $\mathbb{R}$  denote the set of real numbers. Real numbers that are not rational are called *irrational*, e.g.,  $\pi$ ,  $e$ ,  $\sqrt{2}$ , etc.

## 1.3 Relations

If  $A$  and  $B$  are sets, a *relation on  $A, B$*  is any subset  $R \subseteq A \times B$ . For  $a \in A$  and  $b \in B$ , we typically write  $aRb$  to mean  $(a, b) \in R$ . If  $A = B$ , we say that  $R$  is a relation *on  $A$* .

Let  $R$  be a relation on a set  $A$ .

- $R$  is *reflexive* (on  $A$ ) if  $aRa$  for all  $a \in A$ .
- $R$  is *symmetric* if  $aRb$  implies  $bRa$  for all  $a, b \in A$ .
- $R$  is *transitive* if  $aRb$  and  $bRc$  imply  $aRc$  for all  $a, b, c \in A$ .
- $R$  is *antisymmetric* if  $aRb$  and  $bRa$  imply  $a = b$  for all  $a, b \in A$ .
- $R$  is a *quasiorder* (or *preorder*) if  $R$  is reflexive and transitive.
- $R$  is a *partial order* if  $R$  is a quasiorder and antisymmetric.
- $R$  is a *total order* (or *linear order*) if  $R$  is a partial order and either  $aRb$  or  $bRa$  for all  $a, b \in A$ .
- $R$  is an *equivalence relation* if  $R$  is reflexive, symmetric, and transitive.

We often use  $\leq$  to denote an order of some kind. We often use  $\equiv$  or  $\cong$  to indicate an equivalence relation. The equality relation  $=$  is an equivalence relation on any set.

**Partitions and equivalence relations.** For any set  $A$ , a *partition* of  $A$  is a collection  $\mathcal{P}$  of subsets of  $A$  such that every element of  $A$  is in exactly one set in the partition  $\mathcal{P}$ . Equivalently, the sets in  $\mathcal{P}$  are pairwise disjoint and their union is  $A$ .

Every equivalence relation  $\equiv$  on  $A$  induces a unique partition of  $A$  into nonempty sets called *equivalence classes*. This partition, denoted  $A/\equiv$ , has the property that for all  $a, b \in A$ ,  $a \equiv b$  if and only if  $a$  and  $b$  belong to the same equivalence class.

## 1.4 Functions

For sets  $A$  and  $B$ , a relation  $f$  on  $A, B$  is a *function from  $A$  to  $B$*  (denoted  $f : A \rightarrow B$ ) if, for every  $a \in A$  there is a unique  $b \in B$  such that  $(a, b) \in f$ . For any  $a \in A$ , we let  $f(a)$  denote the unique  $b \in B$  such that  $(a, b) \in f$ . Alternatively, we say that  $f$  *maps* (or *takes*)  $a$  to  $f(a)$ . If  $b = f(a)$ , we say that  $b$  is the *image of  $a$  under  $f$*  and that  $a$  is a *pre-image of  $b$  under  $f$* .

Functions are sometimes called *mappings* or *maps*.

**Domain, codomain, range.** If  $f : A \rightarrow B$ , then we say that  $A$  is the *domain* of  $f$  and that  $B$  is a *codomain* of  $f$ . The *range* of  $f$  is

$$\text{rng}(f) := \{f(a) \mid a \in A\} = \{b \in B \mid (\exists a \in A)[b = f(a)]\},$$

that is, the set of all images of elements of  $A$  under  $f$ . We have  $\text{rng}(f) \subseteq B$ .

**One-to-one, onto, and bijective functions.** A function  $f : A \rightarrow B$  is *one-to-one* (or *injective*) if  $a \neq b$  implies  $f(a) \neq f(b)$  for all  $a, b \in A$ . A pair  $a, b$  such that  $a \neq b$  and  $f(a) = f(b)$  is called a *collision*. Thus  $f$  is one-to-one iff it has no collisions. A function  $f : A \rightarrow B$  is *onto* (or *surjective*) if  $\text{rng}(f) = B$ , that is, if every element of  $b$  has a pre-image under  $f$ . In this case, we may also say that  $f$  *maps  $A$  onto  $B$* .

Two basic facts: if  $f : A \rightarrow B$  is one-to-one, then  $|A| \leq |B|$ ; if  $f : A \rightarrow B$  is onto, then  $|A| \geq |B|$ .

A function  $f : A \rightarrow B$  is *bijective* (or a *bijection*, *one-to-one correspondence*, or a *perfect matching*) if it is both one-to-one and onto. In this case, we have  $|A| = |B|$ .

**Finiteness of sets.** A set  $A$  is *finite* if there exists a bijection  $c : A \rightarrow \{1, 2, \dots, n\}$  for some natural number  $n$ . If this is the case, then  $n = |A|$ ; otherwise,  $A$  is infinite. The union of any finite collection of finite sets is a finite set.

## 1.5 The pigeonhole principle

There are at least two equivalent formulations of the pigeonhole principle, one using partitions and the other using functions.

**Theorem 1** (Pigeonhole Principle (Partition Form)). *Let  $A$  be any finite set of  $n$  elements, for some  $n \in \mathbb{N}$ , and let  $\mathcal{P}$  be any partition of  $A$  into  $m > 0$  sets. Then there exists a set in the partition  $\mathcal{P}$  with at least  $n/m$  elements. In particular, if  $n > m$ , then some set in the partition contains at least two elements.*

**Theorem 2** (Pigeonhole Principle (Functional Form)). *Let  $A$  be any finite set of  $n$  elements, for some  $n \in \mathbb{N}$ , and let  $f : A \rightarrow B$  be any function from  $A$  to some finite set  $B$  with  $m > 0$  elements. Then there exists an element of  $B$  with at least  $n/m$  many pre-images under  $f$ . In particular, if  $n > m$ , then  $f$  is not one-to-one.*

Informally, if you divide  $n$  things into  $m$  groups, then some group has at least  $n/m$  things in it.

## 1.6 Strings

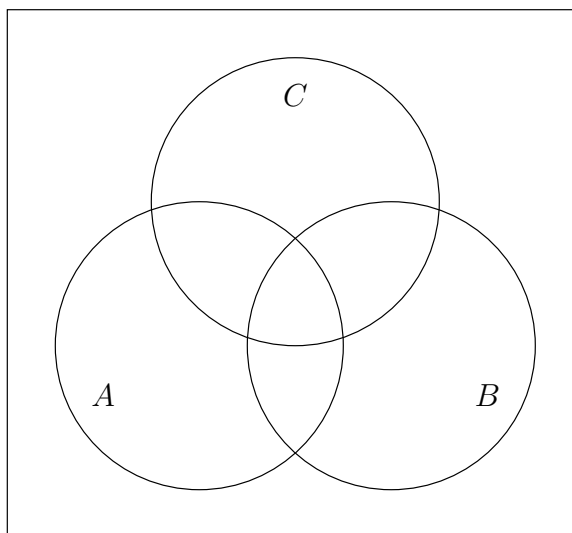
Read Section 6.1 of the typeset Course Notes (<https://cse.sc.edu/~fenner/csce355/coursenotes/course-notes.pdf>).

## 2 Problems

The problems below under the headings Sets, Relations, and Functions will not be tested on exams. Only the last section, on Strings will be tested.

### 2.1 Sets

1. Let  $A := \{1, 2, 3, 4\}$  and  $B := \{2, 5\}$ . What are (a)  $A \cup B$ , (b)  $A \cap B$ , (c)  $A - B$ , and (d)  $A \triangle B$ ? What are (e)  $A \times B$  and (f)  $2^B$ ? In each case, also give the cardinality of the set.
2. True or false:  $2^\emptyset = \emptyset$ . Explain.
3. Using just braces and commas, write the set  $2^{2^{\{\emptyset\}}}$  in “long hand.”
4. Using the figure shown below as a template, draw and fill in a Venn diagram to illustrate each of the expressions below involving sets  $A$ ,  $B$ ,  $C$ . That is, shade the regions that are part of the expression (one Venn diagram per expression):



- (a)  $A \cap B \cap C$
- (b)  $A \cup B \cup C$
- (c)  $A \cap (B \cup C)$
- (d)  $A - (B \cap C)$
- (e)  $(A \cup B) - C$
- (f)  $A - (B - C)$
- (g)  $(A \triangle B) \triangle C$
- (h)  $(A \cap B) \cup (A \cap C)$
- (i)  $A \triangle (B \triangle C)$
- (j)  $A \triangle (B \cap C)$

5. What set theoretic identities holding for all  $A, B, C$  are shown by your Venn diagrams in the last problem?
6. Show that the symmetric difference operation  $\triangle$  on sets is commutative and associative, and that  $A \triangle A = \emptyset$  for all sets  $A$ .

## 2.2 Relations

Let  $A := \{1, 2, 3, 4\}$  as in the first problem, above.

7. Let  $R := \{(1, 2), (2, 3), (3, 4)\}$ . ( $R$  is a relation on  $A$ .)
  - (a) Add the fewest possible ordered pairs to  $R$  to make a reflexive relation (on  $A$ ).
  - (b) Add the fewest possible ordered pairs to  $R$  to make a symmetric relation.
  - (c) Add the fewest possible ordered pairs to  $R$  to make a transitive relation.
  - (d) Add the fewest possible ordered pairs to  $R$  to make an equivalence relation on  $A$ . How many equivalence classes are there?
8. Same as the last problem, but now let  $R := \{(1, 2), (2, 3), (3, 1), (4, 4)\}$ .
9. Give an example of a nonempty binary relation on  $A$  that is symmetric and transitive but not reflexive.
10. Suppose  $\leq$  is a quasiorder on some set  $A$ . For every  $a, b \in A$ , define

$$a \equiv b \iff (a \leq b \text{ and } b \leq a).$$

Show that  $\equiv$  is an equivalence relation on  $A$ .

## 2.3 Functions

Let  $A$  and  $B$  be as in the first problem, above.

11. Give an example of a one-to-one function  $f : B \rightarrow A$ . How many such functions are there?
12. Give an example of an onto function  $g : A \rightarrow B$ . How many such functions are there?

## 2.4 Strings

Reproduced below are Exercises 6.1.6 and 6.1.7 of the Course Notes (<https://cse.sc.edu/~fenner/csce355/coursenotes/course-notes.pdf>). Unlike the problems in previous sections above, I *will* test you directly on the techniques used to do these two exercises. You will be graded on the clarity, logical organization, and precision of your proofs.

13. Give inductive proofs of the following for all strings  $x$ ,  $y$ , and  $z$ . You may assume without proof standard facts about natural numbers.
  - (a)  $|x| \geq 0$ .

- (b)  $|xy| = |x| + |y|$ .
  - (c) (Right Cancellation.) If  $xz = yz$ , then  $x = y$ .
  - (d) (Left Cancellation.) If  $xy = xz$ , then  $y = z$ .
14. The *reversal* of a string  $x$  (denoted  $x^R$ ) is the string formed by putting the symbols of  $x$  in reverse order. (For example,  $(abcb)^R = bcba$ .)
- (a) Give a precise, inductive definition of the reversal  $x^R$  of a string  $x$ .
  - (b) Using your definition, give proofs by induction that  $|x^R| = |x|$  and that  $(x^R)^R = x$  for any string  $x$ .