CSE 150 Lectures

Jeffrey Jiang

Fall Semester 2023

Contents

Lecture 1 **3**
1.1 Introduction to Modular Arithmetic 3

Lecture 2 **5**
2.1 Introduction to Set Theory 5
2.1.1 Basic Definitions and Examples 5
2.1.2 Set Operations 6

Lecture 3 **8**
3.1 Introduction to Boolean Algebra 8
3.2 Introduction to Set Theory, Continued. 9
3.2.1 Set-Builder Notation 9
3.2.2 More Set Operations 9

Lecture 4 **12**
4.1 Set Theory, Continued. 12
4.1.1 Cardinality of Sets 12
4.1.2 Pairs, Triplets, k-tuple 15
4.1.3 Relations 15
4.1.4 Examples of Properties of Relations 16

Lecture 1

Based on work by Eduardo L., edited by Jeffrey J.

1.1 Introduction to Modular Arithmetic

Theorem 1.1. ***Quotient-Remainder Theorem*** *states that given integers $a, b \in \mathbb{Z}$ that there exists integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof. [1] Consider the set of integers in the form $a - xb \in \mathbb{Z}$. Since this is the set of integers, it contains the positive integers. Therefore, there exists a minimal positive number denoted by $a - qb$. Define $r = a - qb$. This is equivalent to $a = qb + r$ meaning such q, r exists. Now to prove that $0 \leq r < b$. Assume that $r = a - qb \geq b$. Thus, an additional b can be subtracted from both sides, $r - b = a - qb - b = a - (q+1)b \geq 0$. However, $r - b < r$ and it is positive. This contradicts the claim that $r = a - qb$ is the smallest possible positive integer in the set (minimality of r is contradicted). In conclusion, $q, r \in \mathbb{Z}$ exists and $0 \leq r < b$. $\square$

q is often called the quotient, and r is called the remainder. The process of finding such q, r is called *Euclidean division*.

Definition. *Modulo* is a binary operation accepting a pair of integers $\mathbb{Z} \times \mathbb{Z}$ and outputs one integer $\mathbb{Z}$. It is denoted typically with the operator by "mod." The output of $a \bmod b$ is the remainder when performing Euclidean division with a and b.[2] Here, b is often called the *modulus*.

In class, we described a process of calculating the result of a modulo operation. Given $a \bmod b$, consecutively add or subtract b from a until $0 \leq a < b$. This is the same process described in the proof the quotient-remainder theorem to prove that such r exists in that range.

[1] This is not my proof. This proof comes from Ireland, K., Rosen, M. (1982). *A Classical Introduction to Modern Number Theory*, Bogden and Quigley, Inc. Publishers. All credit goes to them.

[2] Typically in modular arithmetic, mathematicians do not define a modulo operator. They instead define modular congruences.

Examples:

- $42 \bmod 8 = 2$
- $(3 + 5) \bmod 4 = 8 \bmod 4 = 0$
- $-3 \bmod 7 = 4$

As an aside, this definition of modulo is not universal. For example, different programming languages can output different results from modulo. Some preserve the sign of the modulus while others require the result to be nonnegative. These cases can arise when either operand is negative.

With these definitions, it can be useful to define some operations:

$$
\begin{aligned}
+_n : \quad & \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \\
& (a, b) \longrightarrow (a + b) \bmod n
\end{aligned}
$$

Similar operations can be defined for $-_n$, and $\times_n$. It is not defined for division since integers are not closed under division. When there is no ambiguity surrounding the modulus, it may not be stated.

Examples:

- $5 +_7 5 = 3$
- $-3 -_8 16 = 5$
- $7 \times_5 4 = 3$

Lecture 2

Written by Jeffrey J.

2.1 Introduction to Set Theory

2.1.1 Basic Definitions and Examples

Definition. A *set* is a grouping of mathematical objects.

A set is an unordered collection where the multiplicity,i.e. number of times the element occurs, of elements does not matter.

Some important common sets:

- The set of natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$[1]
- The set of integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
  - Sometimes, positive and negative integers are denoted as $\mathbb{Z}^+$ and $\mathbb{Z}^-$ respectively.
  - Nonnegative integers can be denoted as $\mathbb{Z}_{\geq 0}$.
- The set of rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
- The set of irrational numbers, $\mathbb{R} - \mathbb{Q}$
- The set of complex numbers, $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$

Some more uncommon sets:

- The set of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$
- Complete set of residue classes modulo n, $\mathbb{Z}/n\mathbb{Z}$.
  - The element of $\mathbb{Z}/n\mathbb{Z}$ is the set of integers $\mathbb{Z}$ whose remainders are the same when divided by n.
  - e.g. $\mathbb{Z}/2\mathbb{Z}$ is the set containing the set of even numbers and the set of odd numbers.
  - This is an example of a set containing sets.

[1] Some include 0 as part of the natural numbers.

- The set of integer polynomials, i.e. polynomials with integer coefficients and variable x, $\mathbb{Z}[x]$
  - Likewise, the set of real and complex polynomials are $\mathbb{R}[x]$ and $\mathbb{C}[x]$ respectively.
  - These are examples of sets containing polynomials.
- The set of invertible $n \times n$ matrices with real entries, $\mathrm{GL}_n(\mathbb{R})$
  - This is an example of a set containing matrices.
- The set of permutations on set S, Sym_S
  - A permutation is a function that "rearranges" the order of the set.
  - This is an example of a set containing functions.

Sets are flexible, and they can contain many more mathematical constructs than listed above.

Definition. The *empty set* $\emptyset$ is the set without any elements.

2.1.2 Set Operations

Definition. Two sets are *equal* if they contain the same elements. Likewise, two sets are *not equal* if they do not contain the same elements. Set equality and inequality is denoted by $=$ and $\neq$ respectively.

Definition. If set S *contains* element x, then $x \in S$.

Definition. Set A is a *subset* of set B if set B contains all elements of A, i.e. $a \in B \, \forall \, a \in A$. This is denoted as $A \subseteq B$.

Examples:

- $\{1, 2\} \subseteq \{1, 2, 3\}$
- $\{2, 4\} \not\subseteq \{1, 2, 3\}$
- $2 \not\subseteq \{1, 2, 3\}$ but $2 \in \{1, 2, 3\}$
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\mathbb{R} - \mathbb{Q} \subseteq \mathbb{R}$
- $\mathbb{Z}[i] \subseteq \mathbb{C}$
- $\emptyset \subseteq \{-2, 4, 7, 0\}$

Proposition 2.1. *The empty set $\emptyset$ is a subset of any set S.*

Proof. Since the empty set does not contain any elements, by definition, S contains all of its elements. Therefore, $\emptyset \subseteq S$. $\square$

Proposition 2.2. *Given sets A, B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Proof. Given $A = B$. Then, by definition, all elements in A is contained in element B. Therefore, $A \subseteq B$. Additionally, all elements of B are contained in A. So, $B \subseteq A$.

Now to prove the converse. Given $A \subseteq B$ and $B \subseteq A$, assume that $A \neq B$. This means that there exists an element in A or B which is not contained in the other set. Consider the case where this element x is in A but not B, i.e. $x \in A$, $x \notin B$. By definition, the statement $A \subseteq B$ implies that all elements of A are contained in B. This is a contradiction. The same contradiction is reached if $x \in B$ and $x \notin A$. Therefore, if $A \subseteq B$ and $B \subseteq A$, then $A = B$. $\square$

Definition. Set A is a *proper subset* of set B if A is a subset of B and A is not equal to B. This is denoted as $A \subset B$.

A corollary of proposition 2.1 is the empty set $\emptyset$ is a proper subset of any set S as long as $S \neq \emptyset$.

The symbol $\subseteq$ can be interpreted as "proper subset or equal." This train of thought is analogous to how $\leq$ is equivalent to "less than or equal" (Note the bottom of the equals sign below both). Similarly how $x < y$ implies $x \leq y$, $A \subset B$ implies $A \subseteq B$. By this token, it is clear that for all set S that $S \subseteq S$ as S $S = S$

Tricky Problems

- $2 \in \{1, 2, 3\}$, $\{2\} \notin \{1, 2, 3\}$, $\{2\} \subset \{1, 2, 3\}$
- $\emptyset \in \{\emptyset\}$, $\emptyset \subseteq \{\emptyset\}$, $\emptyset \subseteq \emptyset$, $\emptyset = \emptyset$, $\emptyset \notin \emptyset$

Lecture 3

Written by Jeffrey J.

3.1 Introduction to Boolean Algebra

Boolean algebra is a branch of algebra that deals with true and false values. It is used to mathematically represent logic. True is represented by T, and false is represented by F.

There are three fundamental operations in boolean algebra:

- *Conjunction.* This is "logical and" and it is denoted with $\wedge$.
- *Disjunction.* This is "logical or" and it is denoted with $\vee$.
- *Negation.* This is "logical not" and it is denoted with $\neg$.

The truth tables of these basic operation are shown below:

Truth Table for Conjunction

x	y	$x \wedge y$
T	T	T
T	F	F
F	T	F
F	F	F

Truth Table for Disjunction

x	y	$x \vee y$
T	T	T
T	F	T
F	T	T
F	F	F

Truth Table for Negation

x	$\neg x$
T	F
F	T

3.2 Introduction to Set Theory, Continued.

3.2.1 Set-Builder Notation

Set-Builder Notation is a notation used to describe the elements of a set. In its most abstract form, it can be represented as $\{x \mid \lambda(x)\}$. x is the element that would make up the set. The $\mid$ symbol represents "such that" and $\lambda(x)$ is a *predicate* (a function that returns true or false). λ defines the properties that x needs to be included in the set. Additionally, you may specify the domain of the elements of the set. For example, $\{x \in \mathbb{Z} \mid \lambda(x)\}$ meaning the set contains all elements of the set of integers that satisfy λ.[1]

Examples:

- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$.
  - The complex numbers are the set whose elements are in the form $a + bi$ such that a, b are real numbers and i is the square root of -1.
- $K = \{x \mid \sqrt{x} \in \mathbb{Z}\}$.
  - This is the set of integer squares. This reads K is the set that has elements x such that the square root of x is an integer.
- $\mathbb{E} = \{x \in \mathbb{Z} : 2 \mid x\}$. Here I use : for "such that" to differentiate from the "divides" operator.
  - This is the set of evens. This reads that $\mathbb{E}$ is the set of integers where 2 evenly divides the integer.
- $\mathcal{P}(S) = \{X \mid X \subseteq S\}$.
  - The power set of S is all the sets X such that X is a subset of S.
- $S \times R = \{(s, r) \mid s \in S, r \in R\}$. This set is called the cartesian product of set S and R. For example, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is set of pairs of real numbers.

More complex sets can be constructed in set builder notation in conjunction with the logical operators. For example, $\{x \in \mathbb{Z} \mid 0 < x < 12 \wedge x \bmod 2 = 1\}$ is the set of odd integers between 0 and 12.

3.2.2 More Set Operations

Definition. The *union* of two sets is the set containing all the elements of both sets. It is denoted with $\cup$, and it is represented as $A \cup B = \{x \mid x \in A \vee x \in B\}$.

Definition. The *intersection* of two sets is the set whose elements are in both sets. It is denoted with $\cap$, and it is represented as $A \cap B = \{a \in A \mid a \in B\}$ or $\{x \mid x \in A \wedge x \in B\}$.

[1] Some set-builder notation uses : instead of | for "such that."

Definition. The *set-difference* of two sets, denoted $A - B$ or $A\backslash$ with sets A, B, is all the elements of A that are not in B. In set-builder notation, $A - B = \{a \in A \mid a \notin B\}$ or $A - B = \{x \mid x \in A \wedge x \notin B\}$.

There was two different representation of intersection and set difference in set-builder notation provided. Although they both describe the same action, they have different semantic meaning. Take intersection, $A \cap B = \{a \in A \mid b \in B\}$ means is the set of elements of A such that they are also in B. However, $\{x \mid x \in A \wedge x \in B\}$ means the set of values such that the value are both contained in A and B. What the "values" are is unstated. Typically, these values are assumed, or the domain was previously established. The "values" are implied.

Examples:

- $\{a, b\} \cup \{b, c\} = \{a, b, c\}$
- $\{a, b\} \cap \{b, c\} = \{b\}$
- $\{a, b\} - \{b, c\} = \{a\}$
- $S \cup \emptyset = S$
- $S \cap \emptyset = \emptyset$
- $S - \emptyset = S$
- $\emptyset - S = \emptyset$
- $\mathbb{R} - \mathbb{Q}$ is the set of irrational numbers.

Definition. The *complement* of a set S is the set of values which are not in S. The domain of set of "values" is implied or was previously established. It is typically denoted by $\overline{S}$.

The complement of a set is a specific case of set difference. Namely, if $\overline{S}$ is the complement to set R, then $\overline{S} = R - S$. Importantly, $S \subseteq R$. This last requirement for complement is not required for regular set difference (e.g. $\{a, b\} - \{b, c\} = \{a\}$ and $\{b, c\} \not\subseteq \{a, b\}$).

Examples:

- The complement of $\{2, 3, 4\}$ to $\{1, 2, 3, 4, 5\}$ is $\overline{\{2, 3, 4\}} = \{1, 5\}$.
- Given that $\mathbb{E}$ is the set of even integers, $\overline{\mathbb{E}} = \mathbb{O}$ where $\mathbb{O}$ is the set of odd integers. This assumes that it is the complement to the set of integers $\mathbb{Z}$.

Definition. Two sets are *disjoint* if they do not share any elements, i.e. the intersection of the sets is the empty set.

A simple example is that $\mathbb{E}$ is disjoint to $\mathbb{O}$ where they denote even and odd integers respectively.

Definition. The *cardinality* or *order* of a set is the number of unique elements in the set.

Examples:

- $|\{1, 2, 3\}| = 3$
- $|\{\{1, 2, 3\}\}| = 1$
- $|\emptyset| = 0$
- $|\mathbb{Z}| = \infty$
- $|\mathrm{Sym}_n| = n!$. Sym_n is the set of permutations on set $\{x \in \mathbb{Z} \mid 0 < x \leq n\} = \{1, 2, \ldots, n\}$, i.e. the different ways which the set can be rearranged.
- The order of the set of symmetries on a regular n-sided polygon is $2n$, denoted as $|D_{2n}| = 2n$.

Definition. The *power set* of set S denoted with $\mathcal{P}(S)$ is the set of all subsets of S. In set builder notation, it is $\mathcal{P}(S) = \{X \mid X \subseteq S\}$.

Examples:

- $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$

Lecture 4

Written by Jeffrey J.

4.1 Set Theory, Continued.

4.1.1 Cardinality of Sets

Proposition 4.1. *The cardinality of the power set on set S, $\mathcal{P}(S)$, is $|\mathcal{P}(S)| = 2^{|S|}$.*

Proof. I will supply three proofs:

- Associate an unique $|S|$-bit string to each subset K of S, $K \subseteq S$. For each bit in the subset, if it is 1, the corresponding element in S is contained in K. If the bit is 0, then the corresponding element is not contained in S. For example, given set $S = \{a, b, c, d\}$, bit-string 1101 corresponds to subset $\{a, b, d\} \subseteq S$, 1000 to $\{a\} \subseteq S$, 1111 to $\{a, b, c, d\} \subseteq S$, and 0000 to $\emptyset \subseteq S$. Therefore, the number of possible bit-strings with length $|S|$ is the number of subsets of S, i.e. $|\mathcal{P}(S)|$. The number of bit-strings is $2^{|S|}$. In conclusion, $|\mathcal{P}(S)| = 2^{|S|}$.[1]
- Logically, the subset $X \subseteq S$ has the order $0 \leq |X| \leq |S|$. It is possible to count the number of subsets of length n for all $n \in [0, |S|]$. The number of ways for selecting the elements from S to be in subset S where the order of the selection does not matter (since sets are naturally unordered) can be represented through *combination* or the binomial coefficient $\binom{|S|}{k}$ for subset of size K. Therefore, $\mathcal{P}(S) = \sum_{k=0}^{|S|} \binom{|S|}{k}$. It is known that this sum equals $2^{|S|}$. Therefore, $\mathcal{P}(S) = 2^{|S|}$.
- Proof by induction: Define S_i to be the set such that $|S_i| = i$ for all $i \in \mathbb{Z}_{\geq 0}$ and $S_i \subset S_j$ when $i < j$. Thus, $S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_n$. Note that any set S_n can be constructed this way, i.e. adding (through union) an unique single value, starting from the empty set. For example, $\{1, 2, 3\}$ can be stated as $\emptyset \subset \{1\} \subset \{1, 2\} \subset \{1, 2, 3\}$. By definition, $S_0 = \emptyset$. Define the elements of generic set S to be a_i where i represents the S_i in which the element is union. Thus, $S_{i+1} = S_i \cup \{a_{i+1}\}$. Consider $\mathcal{P}(S_0) = \{\emptyset\}$. Thus, $|\mathcal{P}(S_0)| = 1 = 2^0$. Now consider $S_1 = S_0 \cup \{a_1\}$ and $\mathcal{P}(S_1) = \mathcal{P}(S_0 \cup \{a_1\})$. $\mathcal{P}(S_1) = \{\emptyset, \{a_1\}\}$. This process can be thought of in terms of $S_0 \cup \{a_1\}$: for all sets K in $\mathcal{P}(S_0)$, two new subsets of $S_0 \cup \{a_1\}$ can be generated, one is K itself and the other is $K \cup \{a_1\}$. Therefore, $|\mathcal{P}(S_1)| = 2|\mathcal{P}(S_0)| = 2(2^0) = 2^1$. Now consider $S_2 = S_1 \cup \{a_2\}$. $\mathcal{P}(S_2) = \mathcal{P}(S_1 \cup \{a_2\}) = \{\emptyset, \{a_2\}, \{a_1\}, \{a_1, a_2\}\}$. Again, each set in $\mathcal{P}(S_1)$ can

[1] This is Professor Bender's proof. All credit goes to him.

be used to generate two sets each: the set itself or the set with element a_2 added. Thus, $|\mathcal{P}(S_2)| = 2|\mathcal{P}(S_1)| = 2(2^1) = 2^2$. Thus, for $i \in [0, 2]$, $|\mathcal{P}(S_i)| = 2^i$. Now assume that this statement is true for $i \in [0, k]$. Thus, $|\mathcal{P}(S_k)| = 2^k$. Consider $S_{k+1} = S_k \cup \{a_k\}$, again $\mathcal{P}(S_{k+1})$ can be generated from $\mathcal{P}(S_k)$ and a_{k+1}. In the same way, all the sets in $\mathcal{P}(S_k)$ can each be used to generated two more sets, the set as is or the set with a_{k+1} added. Therefore, $|\mathcal{P}(S_{k+1})| = 2|\mathcal{P}(S_k)| = 2(2^k) = 2^{k+1}$. This proves the induction assumption and for all $i \in \mathbb{Z}_{\geq 0}$ that $|\mathcal{P}(S_i)| = 2^i$. Also recall from the definition of S_i that $|S_i| = i$ and so $|\mathcal{P}(S_i)| = 2^{|S_i|}$. Since any set S can be broken down in the way described above, $|\mathcal{P}(S)| = 2^{|S|}$. [2]

$\square$

Examples:

- $|\mathcal{P}(\emptyset)| = 1$ as $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $|\mathcal{P}(\mathcal{P}(\emptyset))| = 2$ as $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
- $|\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))| = 4$ as $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

Define set $\mathcal{P}^n$ as operation of nesting $\mathcal{P}$ n times on a set S.[3]

Proposition 4.2. *Given set S, for $\mathcal{P}^n(S)$ with $n \in \mathbb{Z}^+$, $|\mathcal{P}^n(S)| = 2^{|\mathcal{P}^{n-1}(S)|}$ when $n > 1$ and $|\mathcal{P}^n(S)| = |\mathcal{P}(S)| = 2^{|S|}$ when $n = 1$.*

Proof. Corollary of proposition 4.1. The S in $\mathcal{P}(S)$ is a nested power set with one less $\mathcal{P}$ when $n > 1$ and $|\mathcal{P}^1(S)| = |\mathcal{P}(S)| = 2^{|S|}$. $\square$

Proposition 4.3. *Given sets A and B:*

1. $|A \cup B| + |A \cap B| = |A| + |B|$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $|A \cap B| = |A| + |B| - |A \cup B|$
4. $|A - B| = |A| - |A \cap B| = |A \cup B| - |B|$

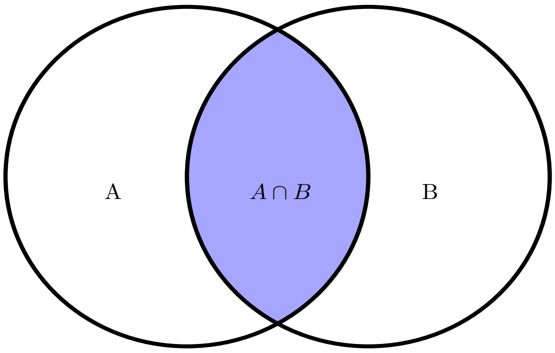
[2] The essential idea of the proof is that adding an element to a set will double the size of the power set since there are two possible subsets created for each of the subsets. There is a lot of mathematical variables which can be confusing. I used these variables to be as general as possible for the proof.

[3] This is my own notation to represent this idea. I am not sure if there is more formal mathematical notation to represent this idea.

Proof. Consider the venn diagram representing set A and set B and their intersection representing $|A \cap B|$. The whole venn diagram represents $|A \cup B|$.

1. See the following diagram:

   Graph of A, B, $A \cap B$

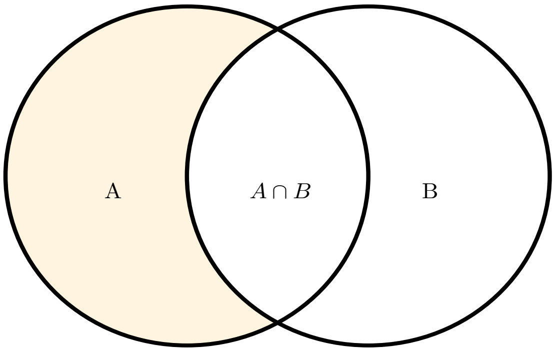
   Note that $A \cup B$ is the whole venn diagram, and $A \cap B$ is the blue-shaded region in the center. See that $|A| + |B|$ would encompass the whole diagram meaning $|A \cup B| < |A| + |B|$. However, adding the order of the two sets means that $A \cup B$ is double-counted. Therefore, $|A| + |B| = |A \cup B| + |A \cap B|$.

2. Algebraic manipulation on (1)

3. Algebraic manipulation on (1)

4. See the following diagram:

   Graph of A, B, $A - B$

   The area shaded in the light orange color is $A-B$. Thus, it is clear that $|A|-|A \cap B|$. Then substitute (3) into 4 to get that $|A - B| = |A \cup B| - |B|$

$\square$

4.1.2 Pairs, Triplets, k-tuple

Definition. The *cartesian product*, or *cross product*, of sets S and R is $S \times R = \{(s, r) \mid s \in S, r \in R\}$.

Examples:

- $\{a, b\} \times \{x, y\} = \{\{a, x\}, \{a, y\}, \{b, x\}, \{b, y\}\}$
- $\{a, b\} \times \emptyset = \emptyset$
- $\emptyset \times \{a, b\} = \emptyset$
- $\emptyset \times \emptyset = \emptyset$
- $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the set of 2-dimensional real vectors, called the vector space, represented by pairs (a, b) where $a, b \in \mathbb{R}$.

Proposition 4.4. *Given sets A, B, then $|A \times B| = |A||B|$.*

Proof. By definition, $A \times B$ is the set of all possible pairs (a, b) where $a \in A$ and $b \in B$. There is thus $|A|$ possible values for a, and there is $|B|$ possible values for B. Since these are independent events, the total possible values for $|A \times B|$ is $|A||B|$. Therefore, $|A \times B| = |A||B|$. □

Definition. The *cartesian product* is defined to satisfy the following property $A \times B \times C = (A \times B) \times C = A \times (B \times C)$. Therefore, the cross product is associative.

This allows the definition of *triplets* and *k-tuple*. Triplets are the cross product of three sets. A k-tuple is cross product of k sets. Although cartesian products are associative, it does not mean they are commutative since order of the pairs, triplets, and k-tuples matter.

4.1.3 Relations

Definition. A k-ary relation R on sets $S_1, S_2, \ldots, S_k$ is a subset of $S_1 \times S_2 \times \cdots \times S_k$, i.e. $R \subseteq S_1 \times S_2 \times \cdots \times S_k$.

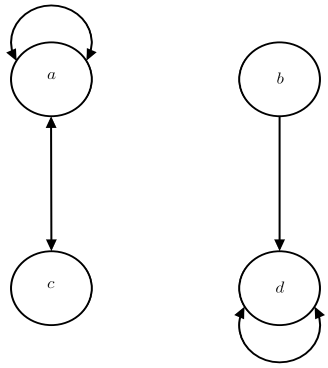
In other words, the k-ary relation is a set of k-tuples from the cross product of sets $S_1, S_2, \ldots, S_k$.

Definition. A binary relation R on set S is a subset of $S \times S = S^2$, i.e. $R \subseteq S^2$.

A binary relation can also be on two sets. However, when only one set S is provided in a k-ary relation, it is assumed that relation R is a subset of S^k.

Additionally, a binary relation on a set can be represented pictorially. For example, given $S = \{a, b, c, d\}$ and relation R on S where $R = \{\{a, c\}, \{b, d\}, \{d, d\}, \{a, a\}, \{c, a\}\}$, the following graph can be drawn:

Graph of Relation R



The arrows in the relation are formed from the first element to the second element of the ordered pair in the relation. If (a, b) and (b, a) are in R, then its represented by the double arrow.

Definition. A binary relation $R \in S \times S$ is *reflexive* if for all $a \in S$ $(a, a) \in R$.

Definition. A binary relation $R \in S \times S$ is *symmetric* if for all $(a, b) \in R$ implies that $(b, a) \in R$.

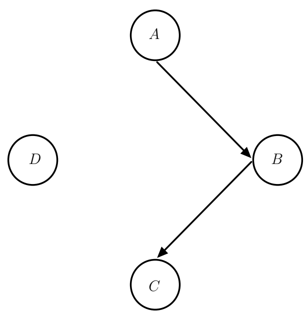
Definition. A binary relation $R \in S \times S$ is *transitive* if for all $a, b, c \in S$, $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

Definition. If a relation is reflexive, symmetric, and transitive, it is an *equivalence* relation.

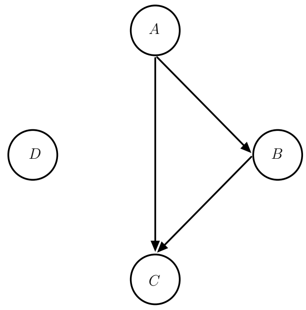
4.1.4 Examples of Properties of Relations

The following uses relation $R \subseteq S \times S$ where set $S = \{a, b, c, d\}$.

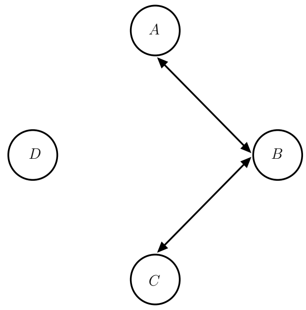
Example of non-reflexive, non-symmetric, non-transitive relation



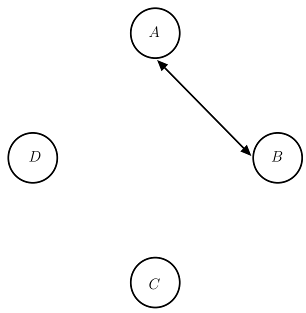
Example of non-reflexive, non-symmetric, transitive relation



Example of non-reflexive, symmetric, non-transitive relation

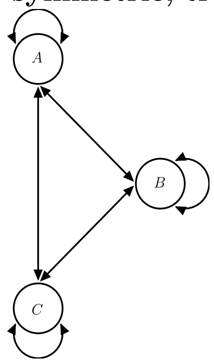


Example of non-reflexive, symmetric, non-transitive relation



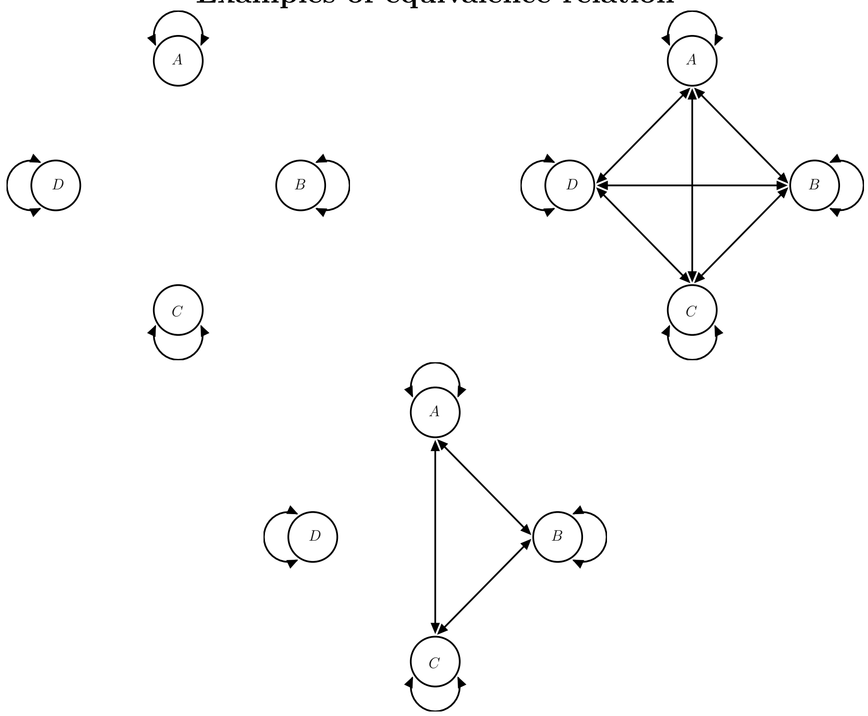
The graph above is not transitive because $(A, B) \in R$, $(R, A) \in R$ yet $(A, A) \notin R$. Likewise for $(B, B) \notin R$.

Example of non-reflexive, symmetric, transitive relation



The graph above is not reflexive because $(d, d) \notin R$ and reflexivity requires all elements of S to do so.

Examples of equivalence relation



These examples shows an important property of equivalence relations: equivalence relations *partitions* the set S with each connected sections forming an *equivalence class*.

Index

Boolean Algebra, 8

Modular Arithmetic, 3
    Modulo, 3

Quotient-Remainder Theorem, 3
    Euclidean Division, 3

Set Theory, 5, 9, 12
    Common Sets, 5
    Empty Set, 6
    Equivalence Relation, 16
    Relations, 15
    Set, 5
    Set Operations, 6, 9, 15
    Set-Builder Notation, 9
    Tuple, 15