CSE 150 Lectures

Jeffrey Jiang

Fall Semester 2023

Contents

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 $0 \leq r < b$. □

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 mod 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 mod 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, $\emptyset \subseteq S$. □

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 $A = B$. □

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 $\mid$ for "such that."

Definition. The *set-difference* of two sets, denoted $A - B$ or $A\setminus$ 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:

- $|\{1, 2, 3\}| = 3$
- $|\{\{1, 2, 3\}\}| = 1$
- $|\emptyset| = 0$
- $|\mathbb{Z}| = \infty$
- $|\text{Sym}_n| = n!$. 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]

□

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 $|\mathcal{P}^1(S)| = |\mathcal{P}(S)| = 2^{|S|}$. □

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. $|A - B| = |A| - |A \cap B| = |A \cup B| - |B|$

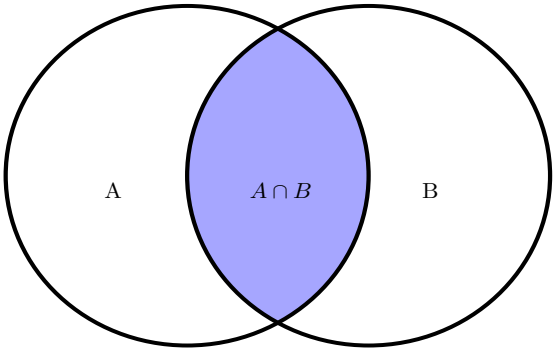
[2] The essential idea of the proof is that adding an element to a set will double the size of the power set since there are two possible subsets created for each of the subsets. There is a lot of mathematical variables which can be confusing. I used these variables to be as general as possible for the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

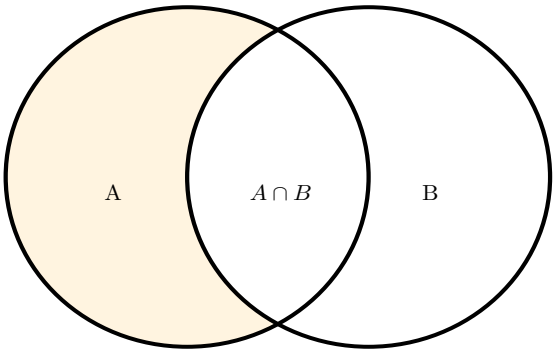
Graph of A, B, $A \cap B$



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 $|A - B| = |A \cup B| - |B|$

□

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. $R \subseteq S_1 \times S_2 \times \cdots \times S_k$.

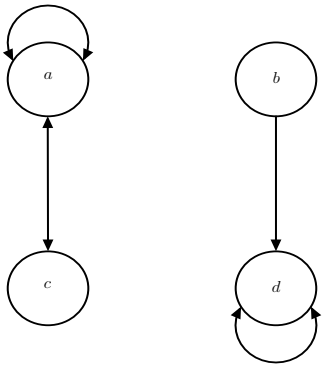
In other words, the k-ary relation is a set of k-tuples from the cross product of sets $S_1, S_2, \ldots, S_k$.

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 $(b, a) \in R$.

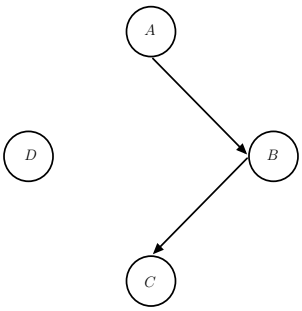
Definition. A binary relation $R \in S \times S$ is *transitive* if for all $a, b, c \in S$, $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

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

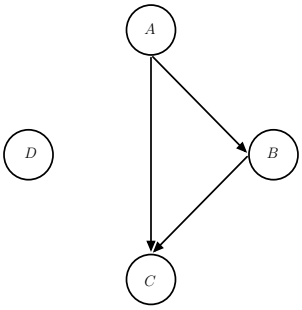
4.1.4 Examples of Properties of Relations

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

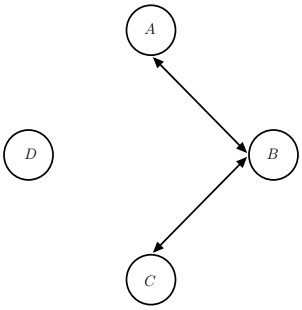
Example of non-reflexive, non-symmetric, non-transitive relation



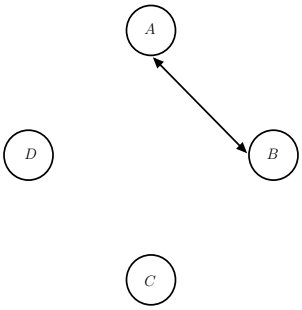
Example of non-reflexive, non-symmetric, transitive relation



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

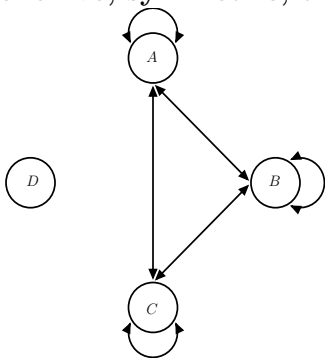


Example of non-reflexive, symmetric, non-transitive relation



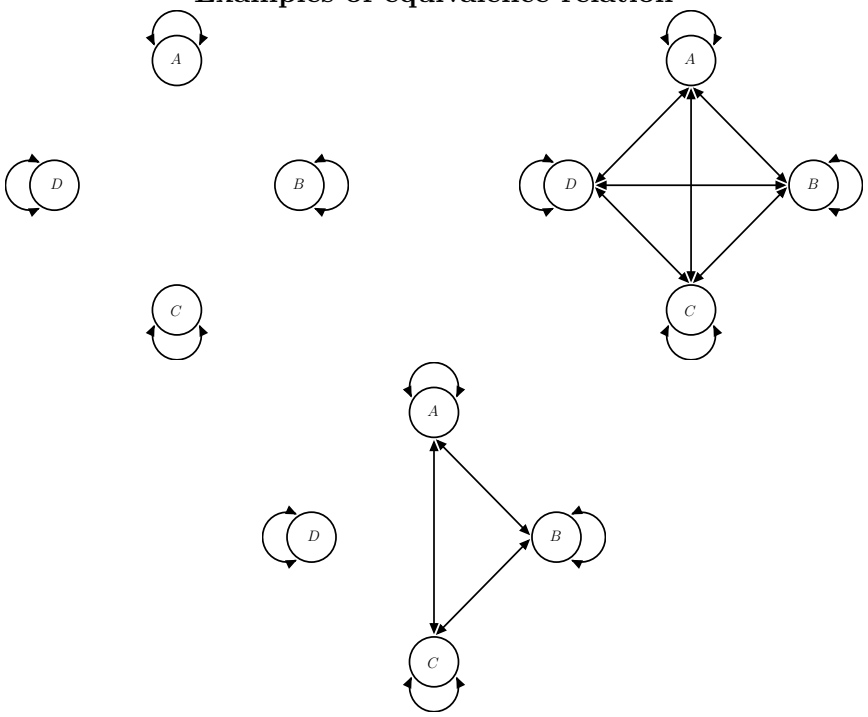
The graph above is not transitive because $(A, B) \in R$, $(R, A) \in R$ yet $(A, A) \notin R$.
Likewise for $(B, B) \notin R$.

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*.

Lecture 5

Written by Jeffrey J.

5.1 Introduction to Boolean Algebra, Continued.

5.1.1 Basic Definitions and Examples

Definition. A *proposition* is a statement that is either *true* or *false*.

Examples:

- "All humans are mortal." Proposition that is true[1]
- "$a^2 + b^2 + c^2 = d^2$ has no solutions where $a, b, c, d \in \mathbb{Z}$." Proposition that is true
- "The moon is purple." Proposition that is false
- Goldbach's Conjecture: "Every even number greater than 2 can be written as the sum of two primes." Proposition that has not been proven[2]
- "Did you do the dishes?" Not a proposition. It is a question.
- "Play Mario with me." Not a proposition. It is a command.

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 $\neg, \bar{x}, !x$ where x is a proposition.

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

[1] Does Henrietta Lacks count as immortal? Does her cancerous cells even count as being her?

[2] Fun fact. In 1937, Ivan Vinogradov proved that every large enough odd number can be written as the sum of three odd primes. In 2013, Harald Helfgott proved that every odd number greater than 5 can be written as the sum of three primes. This is called Goldbach's Weak Conjecture.

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

These fundamental operators give rise to more complex operations:

Definition. *Material conditional*, or *implication*, represents the idea of "implies." Given two propositions a, b, then $a \to b$ means that a implies b or "if a, then b." The statement is true unless a is true and b is false since a being true implies that b is also true. a is called the *antecedent* and b is called the *consequent*.

True Table for Material Conditional

a	b	$a \to b$
T	T	T
T	F	F
F	T	T
F	F	T

A note: It may seem paradoxical how $a \to b$ is true when a is false, but the true value is stating that the statement "a implies b" is true, not that the operands are true. The statement states that b is true when a is true. It does not state anything about what b is when a is false. Therefore, the whole statement is true.

Definition. The *converse* of conditional $a \to b$ is $b \to a$ given propositions a, b.

Proposition 5.1. *$a \to b$ is not equivalent to $b \to a$, i.e. they do not always evaluate to the same truth value.*

Proof. The truth table of the two reveals how the converse of a implication is not equivalent to the implication:

a	b	$a \to b$	$b \to a$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

□

Example:

- "If it is my birthday, then I am eating cake," is a conditional which is true. However, the converse is "If I am eating cake, it is my birthday." The converse is not necessarily true. For example, what if it is someone else's birthday, and I am eating their birthday cake. Eating the cake does not imply that it is my birthday.

Definition. A *vacuous conditional* is a statement that is true because the antecedent is false.

Example:

- "If the moon is purple, then the moon is made of cheese." This is a vacuous conditional because the "the moon is purple" is false. The conditional is true, however.

Definition. The *contrapositive* of a material conditional $a \to b$ is $\neg b \to \neg a$.

Proposition 5.2. *A material conditional $a \to b$ is equivalent to its contrapositive $\neg b \to \neg a$.*

Proof. The truth table of the two reveals how the contrapositive of a implication is equivalent to the implication:

a	b	$a \to b$	$\neg b \to \neg a$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

□

Definition. *Material biconditional* or *equivalence* represents the idea of "if and only if." Given two propositions a, b, then, $a \leftrightarrow b$ means that a implies b and b implies a. The statement is true if a and b are both true or both false.

True Table for Material Biconditional

a	b	$a \leftrightarrow b$
T	T	T
T	F	F
F	T	F
F	F	T

Material biconditional is also called equivalence, denoted $\equiv$, because it requires both the operands to be the same truth value. Additionally, if an implication and its converse is true, then it is a biconditional.

Perhaps the most important application of biconditionals is that all definitions are biconditionals. This is what makes a definition a definition. For example, consider the definition of a square, i.e. a square is a rectangle with four equal sides. If a rectangle has four equal sides, then it is a square. Likewise, if a shape is a square, then it is a rectangle with four equal sides. If a definition is presented as a conditional, its converse is also true. All definitions are biconditionals.

Definition. The *exclusive or*, or *XOR*, is true when its operands have different truth values. The symbol of XOR is typically $\oplus$.

True Table for Exclusive Or

a	b	$a \oplus b$
T	T	F
T	F	T
F	T	T
F	F	F

Definition. A proposition is *satisfiable* if some setting of truth values makes the proposition true.[3]

Definition. A proposition is a *tautology* if under all settings of truth values, the proposition is true.

Likewise, if all possible settings of truth values makes a proposition false, then it is called a *contradiction*.

Definition. A *predicate* is a proposition whose truth value depends on one or more variables. In this sense, it is a function that outputs a truth value.

Examples:

- $P(n) =$ "n is even". Then, $P(2) =$ true, $P(1) =$ false.
- $P(n) =$ "n is food". Then, $P(\text{Apple}) =$ true, $P(\text{Table}) =$ false

5.1.2 Properties in Boolean Algebra

All of the following may be proven using truth tables or with previous conclusions. The proofs are not shown, however. We will also denote true as 1 and false as 0 as is convention.[4]

[3] Satisfiability is a NP-complete problem

[4] I'm just too lazy to type true and false every time.

Proposition 5.3. ***Basic Properties of Disjunction***

- *Disjunction is associative, i.e.* $(A \vee B) \vee B \equiv A \vee (B \vee C)$ *for all propositions* A, B, C.
- *Disjunction is commutative, i.e.* $A \vee B \equiv B \vee A$ *for all propositions* A, B.
- *The identity of disjunction is* 0*, i.e.* $A \vee 0 \equiv 0 \vee A \equiv A$ *for all proposition* A.
- *The annihilator of disjunction is* 1*, i.e.* $A \vee 1 \equiv 1 \vee A \equiv 1$ *for all proposition* A.

Proposition 5.4. ***Basic Properties of Conjunction***

- *Conjunction is associative, i.e.* $(A \wedge B) \wedge B \equiv A \wedge (B \wedge C)$ *for all propositions* A, B, C.
- *Conjunction is commutative, i.e.* $A \wedge B \equiv B \wedge A$ *for all propositions* A, B.
- *The identity of conjunction is* 1*, i.e.* $A \wedge 1 \equiv 1 \wedge A \equiv A$ *for all proposition* A.
- *The annihilator of conjunction is* 0*, i.e.* $A \wedge 0 \equiv 0 \wedge A \equiv 0$ *for all proposition* A.

Proposition 5.5. ***Distributivity of Disjunction and Conjunction.***
For all propositions A, B, C*:*

- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

Proposition 5.6. ***Complementation of Disjunction and Conjunction***
For all propositions A*:*

- $A \vee \neg A \equiv 1$
- $A \wedge \neg A \equiv 0$

Proposition 5.7. *Double negation states that for all proposition* A *that* $\neg\neg A \equiv A$.

Proposition 5.8. ***De Morgan's Law***
For all propositions A, B*:*

- $\neg(A \vee B) \equiv \neg A \wedge \neg B$
- $\neg(A \wedge B) \equiv \neg A \vee \neg B$

Proposition 5.9. *For all propositions* A, B*:*

- $A \wedge (A \vee B) \equiv A$
- $A \vee (A \wedge B) \equiv A$

Proposition 5.10. *For all propositions A, B:*

- $(\neg(A \equiv B)) \equiv (A \oplus B)$
- $(\neg(A \oplus B)) \equiv (A \equiv B)$

An application of the above properties:

- Given `if (x >= 0 && (x < 0 || y))`. Let $A =$ (`x>=0`) and $B =$ `y`. Note that `x<0` is equivalent to $\neg A$. Therefore, the code can be rewritten as $A \wedge (\neg A \vee B)$ in boolean algebra. Apply the distributive property for conjunction, $(A \wedge \neg A) \vee (A \wedge B)$. Note the annihilator property for conjunction, $0 \vee (A \wedge B)$. Now apply the identity for disjunction, $A \wedge B$. In conclusion, the expression above simplifies to $A \wedge B$ or `x >= 0 && y`.[5]

[5] In class, we proved a similar example using a truth table. However, knowing these properties allows you to simplify the statements without using a truth table

Lecture 6

Written by Jeffrey J.

6.1 Introduction to Boolean Algebra, Continued.

6.1.1 Summary and Further Explanations

Truth Table of basic binary logical operators

P	Q	$P \wedge Q$	$P \vee Q$	$P \to Q$	$P \leftrightarrow Q$	$P \oplus Q$
T	T	T	T	T	T	F
T	F	F	T	F	F	T
F	T	F	T	T	F	T
F	F	F	F	T	T	F

Truth Table of Negation

P	$\neg P$
T	F
F	T

Note: For material conditional, or implication, it can be viewed analogously to a promise. Given $A \to B$, then someone can promise that if A occurs, then they will do B. If A occurs and B does not result, then the promise is broken and is a lie (i.e. is false). If A does not happen, then B may or may not happen. Still the promise is kept (i.e. is true) since A never occurs.

Implication plays a role in theorems. Theorems are implications where if an initial condition P is satisfied, then the result that the theorem describes Q is also true. In symbolic logic, it is $P \to Q$.

Definition. The inverse of conditional $A \to B$ is $\neg A \to \neg B$.

Note that the converse and the inverse are contrapositives.

Proposition 6.1. $(P \to Q) \equiv (\neg P \vee Q)$

Proof. I will provide two proofs, one using properties of the logical operators and another using a truth table:

- Consider when $P \to Q$ is false. It is false when P is true and Q is false. Therefore, $P \wedge \neg Q$ is when $P \to Q$ is false. Therefore, $P \to Q$ is true when $\neg(P \wedge \neg Q)$. Applying De Morgan's law reveals $(\neg P \vee Q) \equiv (P \to Q)$.
- Clearly, $(P \to Q) \equiv (\neg P \vee Q)$.

P	Q	$P \to Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

□

Corollary 1. $(\neg(P \to Q)) \equiv (P \wedge \neg Q)$

Proof. Apply De Morgan's Law. □

One examples of tautologies include the annihilator of disjunction $A \vee \neg A$ or simply $A \to A$. One example of a contradiction includes the annihilator of conjunction $A \wedge \neg A$ or simply $\neg(A \to A)$.

6.1.2 Quantifiers

There are two main logical quantifiers:

- "For all" represented by $\forall$
- "There exists" represented by $\exists$

Examples:

- Let $P(x) \equiv x^2 \geq 0$. Then, $\forall\, x$, $P(x)$ is true. Additionally, $\exists\, x$ where $P(x)$ is true.
  - The set which x belongs to is implicit in this case. Typically, the set which x belongs to is explicitly stated.
- Let $P(x) \equiv x^2 \geq 0$. Then $\forall\, x \in \mathbb{C}$, $P(x)$ is false. However, $\exists\, x \in \mathbb{C}$ where $P(x)$ is true.
- Let $P(x) \equiv x^2 > 0$. Then $\forall\, x \in \mathbb{Z}$, $P(x)$ is false. However, $\exists\, x \in \mathbb{Z}$ where $P(x)$ is true.

There is a less common quantifier called the uniqueness quantification which means "there exists an unique." It is denoted by $\exists!$. For example, Euclidean division states that given $a, b \in \mathbb{Z}\ \exists!\, q, r \in \mathbb{Z}$ such that $(a = bq + r) \wedge (r \in [0, b))$.

6.1.3 Ambiguity in Converting English to Logic

English can be ambiguous when converting English to logic. For example, take "You may either eat cake or eat ice cream." There is two possible meanings. Let C represent eating cake and I represent eating ice cream. The statement can be interpreted two ways:

- You may eat cake but not ice cream, or you may eat ice cream but not cake. This is represented by $C \oplus I$ since you are not allowed to eat both. Therefore, it is exclusive.
- You may either eat cake, ice cream, or both. This is represented by $C \vee I$.

Thus, in English, the word *or* can either mean "logical or" or "exclusive or."

Another example: "Every American has a dream." Let A be the set of Americans and D be the set of dreams. Additionally, let $H(a, d)$ represent "a has dream b." Then, there is two meaning:

- $\exists\, d \in D \forall\, a \in A, H(a, d)$. This means: there exists a dream such that all americans has this dream.
- $\forall\, a \in A\, \exists\, d \in D, H(a, d)$. This means: for each americans, there exists a dream which they have.

A final example: "If you can solve any problem, then you get an A." Let P be the set of problems and predicate $G(p)$ mean "you can solve problem p." Let A be the proposition of getting an A. Then, there is two potential meanings:

- $(G(p)\, \forall\, p \in P) \to A$. This means: if you can solve every problem, then you get an A.
- $(\exists\, p \in P, G(p)) \to A$. This means: if there exists a problem you can solve, then you can get an A.

Here "any" can mean existence or for all.

Lecture 7

Written by Jeffrey J.

7.1 Introduction to Boolean Algebra, Continued.

7.1.1 More Notes on Quantifiers

The order of quantifiers matter! For example, take Goldbach's Conjecture.

Proposition 7.1. *Every even integer greater than* 2 *is the sum of two prime numbers.*[1]

This can be written in propositional logic as follows: Let $\mathbb{E}$ be the set of even numbers greater than 2. Let P be the set of prime numbers. Goldbach's conjecture states $\forall\, x \in \mathbb{E}\, \exists\, a, b \in P\ a + b = x$. However, switching the quantifiers would make the statement $\exists\, a, b \in P\, \forall\, x \in \mathbb{E}\ a + b = x$. This means that there exists two primes a, b where their sum is equal to all the even integers greater than 2. This is clearly incorrect and has a different meaning from Goldbach's conjecture.

More specifically, the order of quantifiers matter between different quantifiers. If two quantifiers next to each other are the same, then they can be readily switched. For example, consider $\forall\, a, b$ which is the same as $\forall\, a\, \forall\, b$. This is equivalent to $\forall\, b\, \forall\, a$.

This is how negation affects existential quantifiers:

- $\neg(\forall\, x\, P(x)) \Rightarrow\ \exists\, x\, \neg P(x)$
- $\neg(\exists\, x\, P(x)) \Rightarrow\ \forall\, x\, \neg P(x)$

An example of simplifying a proposition containing quantifiers is shown below:

$$\begin{aligned}\neg(\forall\, x\, \exists\, y\, \forall\, z\, P(x, y, z)) &= \exists\, x\, \neg(\exists\, y\, \forall\, z\, P(x, y, z)) \\ &= \exists\, x\, \forall\, y\, \neg(\forall\, z\, P(x, y, z)) \\ &= \exists\, x\, \forall\, y\, \exists\, z\, \neg P(x, y, z)\end{aligned}$$

A note: The $\forall$ can be thought as a sequence of $\wedge$ which require that all x to satisfy the predicate. In notation,

$$(\forall\, x \in S\, P(x)) \equiv (\bigwedge_{x \in S} P(x))$$

[1] Here prime numbers are defined to be the positive prime elements in the integers. Colloquially, prime numbers are positive, but the mathematical definition of prime includes the negatives, i.e. p is prime if and only if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Similarly, the $\exists$ can be thought as a sequence or $\vee$ which require that at least a single x to satisfy the predicate. In notation,

$$(\exists\, x \in S\, P(x)) \equiv (\bigvee_{x \in S} P(x))$$

Here the large conjunction and disjunction represents performing conjunction and disjunction in a sequence. This is akin to how $\sum$ is used for summation and $\prod$ is used for multiplying in a sequence.

Another note: Given $\forall\, x \in S\, P(x)$, it means $\forall\, x\, (x \in S) \rightarrow P(x)$. However, given $\exists\, x \in S\, P(x)$, it means $\exists\, x\, (x \in S) \wedge P(x)$.

7.1.2 Limits on Symbolic Logic

There are sometimes limits on symbolic logic. This usually occurs when the it is self-referential. Take the following example:

Let proposition P be "This sentence contains a double negative." This is a false statement. However, consider $\neg\neg P$ to be "It is not the case that the sentence does not contains a double negative." This is a true statement. However, $\neg\neg P \equiv P$ which is false since one is true and the other is false.

Lecture 8

Written by Jeffrey J.

8.1 Set Theory: Relations

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

8.1.1 Basic Properties of Relations

Definition. A relation R on set S is *reflexive* if $\forall\, a \in S\ (a, a) \in R$.

Definition. A relation R on set S is *symmetric* if $\forall\, a, b \in S\ (a, b) \in R \Rightarrow (b, a) \in R$.

Definition. A relation R on set S is *transitive* if $\forall\, a, b, c \in S\ (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.

Written Examples

Let S = the set of people. Let relation R = "is brother of." This relation is neither reflexive, symmetric, nor transitive:

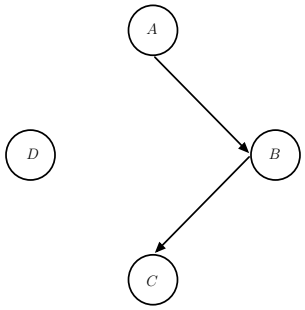
- R is not reflexive because it is not possible for one to be their own brother.
- R is not symmetric because if $a \in S$ is female and $b \in S$ is male, then $(a, b) \in R$ but $(b, a) \notin R$ because a is b's sister.
- R is not transitive because if $a, b \in S$ are brothers, then $(a, b) \in R$ and $(b, a) \in R$. This implies according to transitivity that $(a, a) \in R$, but this is false because you cannot be your own brother. Therefore, R is not transitive.

Let S = the set of people. Let R = "is sibling of." This relation is not reflexive or transitive, but it is symmetric:

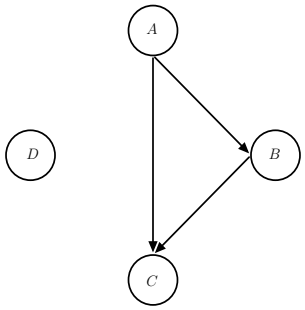
- R is not reflexive because it is impossible for one to be their own sibling.
- R is symmetric because if $a, b \in S$ are siblings, then $(a, b) \in R$ and $(b, a) \in R$.
- R is not transitive because if $a, b \in S$, then $(a, b) \in R$ and $(b, a) \in R$. Transitivity would imply $(a, a) \in R$, but again a cannot be their own sibling. Therefore, R is not transitive.

Graphical Examples

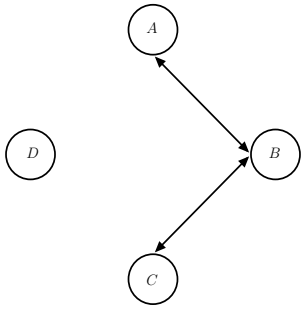
Example of non-reflexive, non-symmetric, non-transitive relation



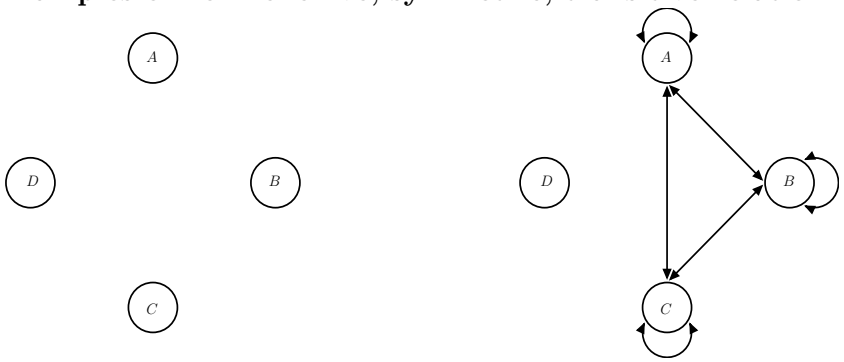
Example of non-reflexive, non-symmetric, transitive relation



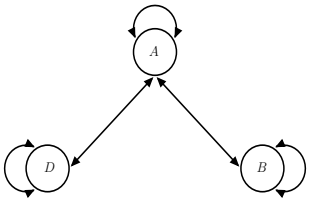
Example of non-reflexive, symmetric, non-transitive relation



Examples of non-reflexive, symmetric, transitive relation



Example of reflexive, symmetric, non-transitive relation



Back to Definitions

Definition. A relation R on set S is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Definition. Given equivalence relation $R \subseteq S \times S$ of set S, the *equivalence class* of $a \in A$ is $\{x \in A \mid (x, a) \in R\}$. The elements of this set is said to be *equivalent* to a.[1]

Definition. A *partition* of A is any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A (I is some indexing set) such that $A = \bigcup_{i \in I} A_i$ and $A_i \cap A_j = \emptyset \, \forall \, i, j \in I \; i \neq j$. In other words, A is the disjoint union of all the sets in the partition. [2]

Proposition 8.1. *Given equivalence relation R, then the set of equivalence classes of R forms a partition of A.*

Proof. Let $K = \{A_i \mid i \in I\}$ be the set of equivalence classes of equivalence relation R where A_i is an equivalence class. Therefore, it needs to be proven that $A = \bigcup_{i \in I} A_i$ and $A_i \cap A_j = \emptyset \, \forall \, i, j \in I \; i \neq j$.

Assume $A \neq \bigcup_{i \in I} A_i$. Therefore, there exists $n \in A$ such that $\forall i \in I \, n \notin A_i$. However, R is an equivalence relation, meaning it is reflexive which implies $(n, n) \in R$. Therefore, n

[1] This definition comes from David S. Dummit's & Richard M. Foote's *Abstract Algebra*
[2] ditto.

belongs to the equivalence class $\{x \in A \mid (x, n) \in R\}$. However, K is defined to contain all equivalence classes, meaning $\exists\, i \in I\ n \in A_i$. This contradicts that n is not in any equivalence class. Therefore, by contradiction, $A = \bigcup_{i \in I} A_i$.

Assume for some $i, j \in I\ i \neq j$, $A_i \cap A_j = P$ where P is a nonempty set. Therefore, $\exists\, p \in P$ such that $p \in A_i$ and $p \in A_j$. By definition of the equivalence classes, $(p, y) \in R$ for any $y \in A_i$ and $(p, z) \in R$ for any $z \in A_j$. Applying the symmetric property, $(y, p) \in R$ as well. Now applying the transitive property yields $(y, z) \in R$. This means that y, z are in the same equivalence class. Therefore, $A_i = A_j$ since all elements since all elements between the two are equivalent to each other. However, this contradicts how $A_i \neq A_j$ since $i \neq j$. Thus, $A_i \cap A_j = \emptyset$.

In conclusion, K is a partition of A, and it is said that the equivalence relation on A partitions the set A. □

Proposition 8.2. *If $\{A_i \mid i \in I\}$ is a partition of set A. Then, there exists an equivalence relation R on set S whose equivalence classes are $A_i\ \forall\, i \in I$.* [3]

Examples

Proposition 8.2 states that if there exists a partition on a set, then there must exist an equivalence relation. Therefore, equivalence relations are common:

- Let $S =$ set of species and binary relation $R =$"is the same species as." This is an equivalence relation.
- Let $S = \mathbb{Z}$ and the equivalence relation $R =$"has the same remainder modulo m." [4]
- Let $S = \mathbb{Z}$ and the equivalence relation $R =$"equals."
- Let $S =$ set of all people and equivalence relation $R =$"same age as."

Equivalence relationship formed by remainder when dividing by m is crucial in many mathematical studies such as number theory. Modular arithmetic is primarily focused on the binary equivalence relation called modular congruences.

Definition. Given $a, b \in \mathbb{Z}$, a is congruent to b modulo m, i.e. $a \equiv b \pmod{m}$, if $m \mid a - b$.

The $\mid$ symbol means "divides." Therefore, $a \equiv b \pmod{m}$ if m divides the difference between a and b.

Proposition 8.3. *$m \mid a - b$ is an equivalence relation on $\mathbb{Z}$.*

Proof. To prove that $m \mid a - b$ is an equivalence relation R, all the properties need to be proven:

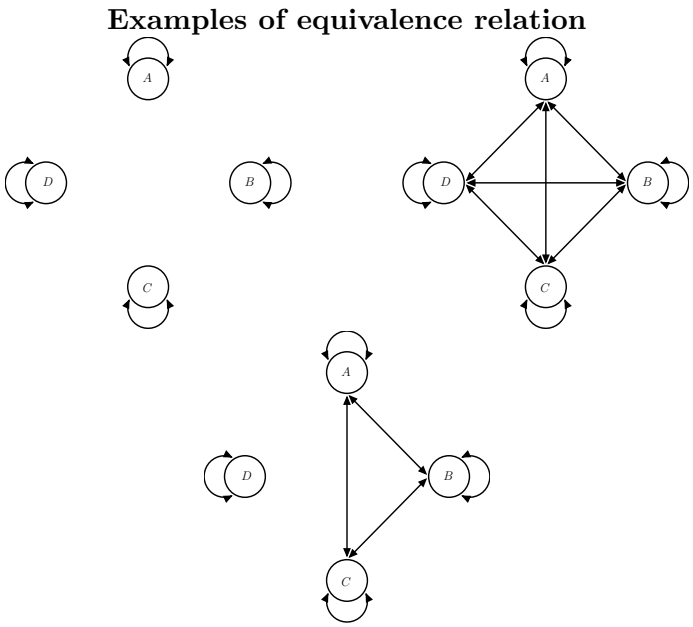
[3] I am not doing this proof.
[4] This is an ubiquitous example of equivalence relation. More on this later.

- $\forall\, a \in \mathbb{Z}\; m \mid a - a$ which is logically equivalent to $m \mid 0$ which is always true. Therefore, $\forall\, a \in \mathbb{Z}\; (a, a) \in R$. This proves reflexive property.
- Given $(a, b) \in R$, then $m \mid a - b$. Multiplying $a - b$ by -1 yields $b - a$. Therefore, $m \mid b - a$ and $(b, a) \in R \,\forall\, a, b \in \mathbb{Z}$. This proves the symmetric property.
- Given $(a, b) \in R$ and $(b, c) \in R$. By definition, $m \mid a - b$ and $m \mid b - c$. Therefore, $m \mid (a - b) + (b - c)$ which yields $m \mid a - c$ meaning $(a, c) \in R \,\forall\, a, b, c \in \mathbb{Z}$. This proves the transitive property.

Therefore, $m \mid a - b$ is an equivalence relation. □

Note: The definition of the relation as $m \mid a - b$ is different from the above definition as having the same remainder. Thinking more about it, it should be clear that if two numbers a, b have the same remainder, then $m \mid a - b$ and it satisfies the relation. However, this definition is more mathematical and allows us to perform operations like the ones shown above to prove properties. Additionally, the idea of modular congruence extends beyond the integers (like into integer polynomials and Gaussian integers). In some cases, like the Gaussian integers, there are some ambiguity over the definition of remainder, i.e. there may be more than one valid quotient and remainder. This definition avoids this issue.[5]

Graphical Examples



[5] Number theory is very interesting.

8.1.2 More Properties of Relations

Definition. A relation $R \subseteq S \times S$ on set S is *asymmetric* if $\forall\, x, y \in S\ (x, y) \in R \Rightarrow (y, x) \notin R$.

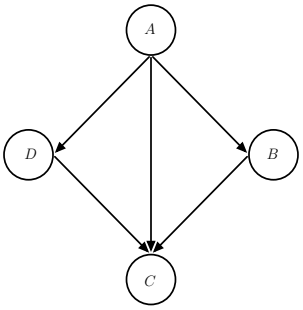
Intuitively, the relation is one-directional. Additionally, a relation that is asymmetric cannot be reflexive (having self-loops) as asymmetry implies if $(a, a) \in S$ then $(a, a) \notin S$.

Definition. A relation $R \subseteq S \times S$ on set S is *antisymmetric* if $\forall x, y \in S (x \neq y) \wedge (x, y) \in R \Rightarrow (y, x) \notin R$.

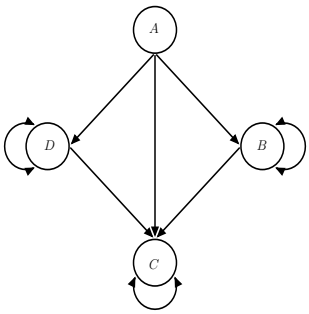
Intuitively, the relation is one-directional, but also allows for self-loops. An antisymmetric relation can be reflexive since if $(a, b) \in R$ and $(b, a) \in R$, antisymmetry would imply that $a = b$. Additionally, asymmetry implies antisymmetry.

Graphical Examples

Example of Transitive and Asymmetric Relation



Example of Transitive and Antisymmetric Relation



8.1.3 Partial and Total Order

Definition. A *partial order* is a relation R on set S that is transitive, reflexive, and antisymmetric.

Partial orders may also called *weak partial order*, *reflexive partial order*, or *non-strict partial order*. A simple example of partial order is the relation $R =$"greater than or equal to" on set $S = \mathbb{Z}$. Reflexivity is satisfied because $\forall\, x \in \mathbb{Z}\, x \geq x$. Antisymmetry is satisfied as $\forall\, x, y \in \mathbb{Z}\, x \neq y \wedge (x \geq y) \Rightarrow \neg(y \geq x)$. Additionally, transitivity is satisfied as $\forall\, x, y, z \in \mathbb{Z}\, (x \geq y) \wedge (y \geq z) \Rightarrow (x \geq z)$. This concludes that relation R is partially ordered.

Definition. A *strict partial order* is a relation R on set S that is transitive and asymmetric.

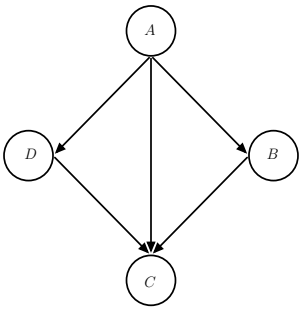
A simple example of strict partial order is with relation $R =$"less than" on set $S = \mathbb{Z}$. The proof is similar to the above, but modified to fit the properties of transitivity and asymmetry.

Definition. A *strict total order* $\prec$ is a strict partial order where $\forall\, x, y \in S\, (x \neq y) \Rightarrow (x \prec y) \vee (y \prec x)$.

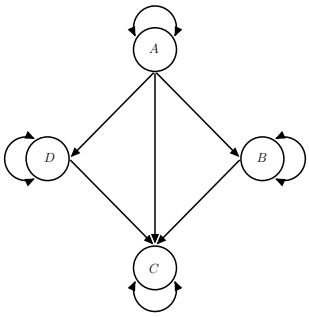
Intuitively, in the graph diagram, all nodes must be connected to the other nodes in either direction. Additionally, the nodes can be rearranged into a line where the order is defined as the position of a node relative to another.

Graphical Examples

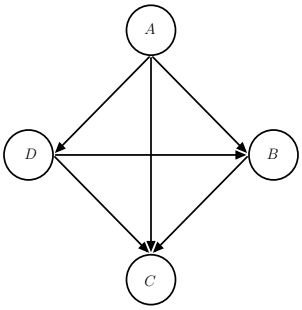
Example of Strict Partial Order



Example of Weak Partial Order



Example of Strict Total Order



In this example, the order of the nodes on a line from left to right would be $A \prec D \prec B \prec C$.

Index