Chapter 8 Discrete Mathematics Notes

Miagao

Contents

8 Properties of Relations

8.1 Relations on Sets

- This section will review relations from Chapter 1.
- Recall that an element of one set may be related to another by a relation R as long as they satisfy its definition.

Example: Less-than Relation

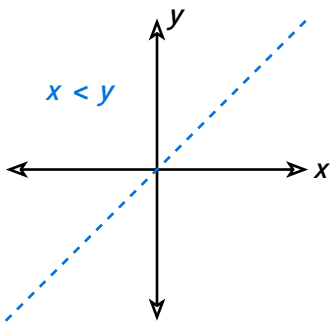
A relation L from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

For all real numbers x *and* y,

$$x \mathrel{L} y \Leftrightarrow x < y$$

- $53 \mathrel{L} 67$?
  - True, $53 < 67$.
- $141 \mathrel{L} 141$?
  - False, $141 = 141$.
- $12 \mathrel{L} -1$?
  - False, $12 > -1$.

Additionally, L may be graphed as a subset of $\mathbb{R} \times \mathbb{R}$, the Cartesian plane using its rule, $x < y$.



Graph 8.1.1: *Anything ordered pair above the dotted line satisify* L.

Example: Congruence Modulo 2 Relation

A relation E from $\mathbb{Z}$ to $\mathbb{Z}$ is defined as follows:

For every $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m \mathrel{E} n \Leftrightarrow m - n \text{ is even}$$

Prove that if n is any odd integer, then $n \mathrel{E} 1$.

Continued on next page

Example: *Congruence Modulo 2 Relation continued*

Proof:

- Suppose n is any odd integer.
- By definition of odd, $n = 2k + 1$ for some integer k.
- By definition of E, $n\,E\,1$ if, and only 1if, $n - 1$ is even.
- By substitution,

$$2k + 1\,E\,1 \Leftrightarrow 2k + 1 - 1 \text{ is even}$$

- As said earlier, k is an integer, so by extension, $2k$ is even by definition of even.
- Therefore, $n\,E\,1$.
- Notably, integers m and n are only related by E if, and only if,

$$m \bmod 2 = n \bmod 2$$

- This means that m and n are **congruent modulo 2**.

This may also apply to modulo relations other than 2. For example, if T is defined from $\mathbb{Z}$ to $\mathbb{Z}$ as follows:

For all integers m and n,

$$m\,T\,n \Leftrightarrow 3 \mid (m - n)$$

then m and n are **congruent modulo 3** by the relation T.

Inverse Relations

Definition:

Let R be relation from A to B. The inverse relation R^{-1} may be defined as follows:

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}$$

- Or, more formally,

$$\forall x \in A \text{ and } y \in B,$$
$$(y, x) \in B \times A \Leftrightarrow (x, y) \in R$$

- On finite sets, an easy way to determine the inverse relation is to reverse the direction of the arrows in the original relation's arrow diagram.

Example: Finite Relation Inverse

Given $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$, let R be the *divides* relation from A to B defined as follows:

For every ordered pair $(x, y) \in A \times B$,

$$x\,R\,y \Leftrightarrow x \mid y$$

What are the ordered pairs of R and R^{-1}?

Continued on next page

Example: *Finite Relation Inverse continued*

- By listing out each ordered pair of R, R^{-1} may be easily found by reversing the order of each tuple.

$$R = \{(2,2),(2,6),(2,8),(3,6),(4,8)\}$$
$$R^{-1} = \{(2,2),(6,2),(8,2),(6,3),(8,4)\}$$

- The same methodology applies to their arrow diagrams as well.

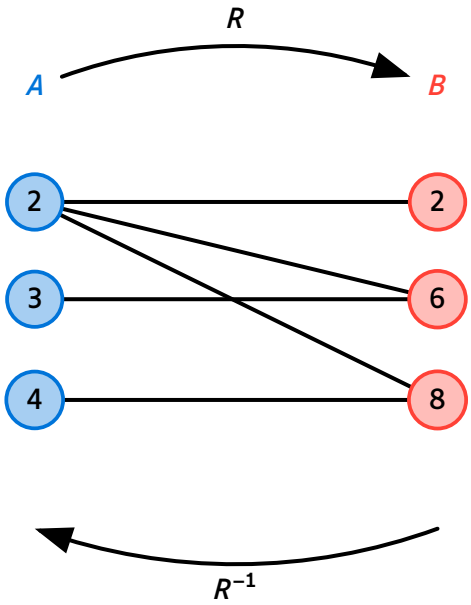


Diagram 8.1.4: *The arrow diagrams of R and R^{-1} are identical aside from the direction.*

- However, for relations on infinite sets, the inverse for the relation's rule must be found.

Example: Infinite Relation Inverse

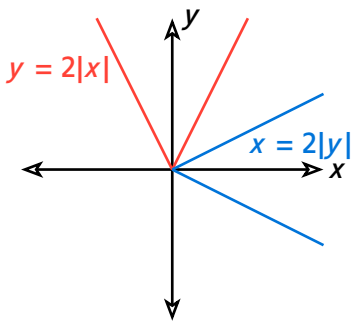
Let R be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined as follows:

$$\text{For every ordered pair } (x,y) \in \mathbb{R} \times \mathbb{R},$$
$$x\,R\,y \Leftrightarrow y = 2|x|$$

If the graph of R^{-1} are drawn on the Cartesian plane, will it be a function?

- Using R's definition, R^{-1} may be expressed as a function of y.

$$R^{-1} = \{(y,x) \in \mathbb{R} \mid x = 2|y|\}$$



Continued on next page

Example: *Infinite Relation Inverse continued*

- Given this, the following tables may be procured:

x	y
0	0
1	2
−1	2
2	4
−2	4

y	x
0	0
2	1
2	−1
4	2
4	−2

- From the table above, it can be seen that R^{-1} has two x-values for each $y > 0$. For instance, both $(2, 1)$ and $(2, -1)$ are in R^{-1}, so it is not a function.

- While arrow diagrams can be a useful tool for finding inverse relations, their layouts do not clearly show arrow diagram properties, especially on one set.
- However, they *are* similar to directed graphs, and applying graph properties from previous chapters will make them more useful in those cases.

Directed Graph of a Relation

Definition:
A **relation on a set** A is a relation from A to A.

- In this case, if a relation R is defined on set A, then the relation's arrow diagram may also be expressed as a **directed graph**.
- Elements related to themselves are expressed as a loop.

Example: Directed Graph of a Relation
Let set $A = \{3, 4, 5, 6, 7, 8\}$
Let a relation R be defined on set A as follows:

$$\text{For every } x, y \in A,$$

$$x \, R \, y \Leftrightarrow 2 \mid (x - y)$$

- A directed graph can be created as follows:

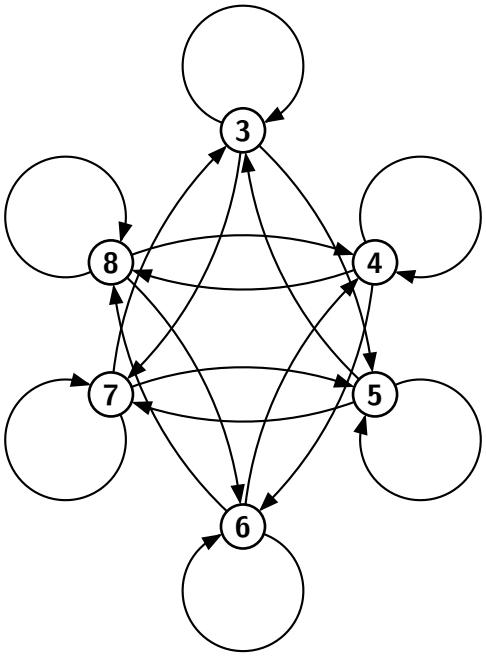


Diagram 8.1.7: The directed graph for R.

Notice how every vertex in the directed graph connects to itself. This means that every element in A is related to itself by R. By extension, all vertices are only connected to vertices with the same parity.

- Many previously learned graph properties are present in the previous example's diagram, including loops, parallel edges, and connectedness.
- As mentioned earlier, some of those properties imply properties of the relation.

N-ary Relations and Relational Databases

- Particular relations formed from Cartesian products of n sets, known as N-ary relations, are the mathematical basis for relational database theory.

Definition:
Given the sets $A_1, A_2, ..., A_n$, the n-**ary relation** on
$A_1 \times A_2 \times \cdots \times A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$. The following special cases are defined as the following:

- 2-ary is **binary**.
- 3-ary is **tertiary**.
- 4-ary is **quaternary**.

In a database, these n-ary relations can be thought of as tables with n columns with the headers $A_1, A_2, ..., A_n$.

8.2 Reflexivity, Symmetry, and Transitivity

Definition:
Let R be a relation on set A.

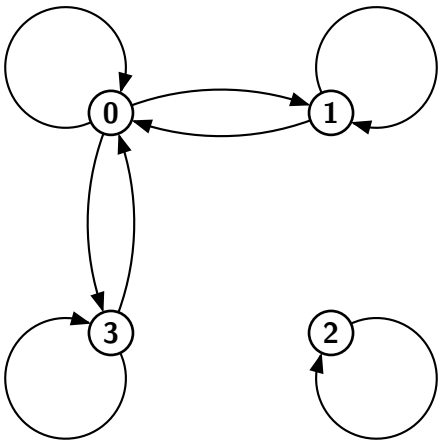
1. R is **reflexive** $\Leftrightarrow$ for all $x \in A$, $x\,R\,x$.
2. R is **symmetric** $\Leftrightarrow$ for every $x, y \in A$, if $x\,R\,y$, then $y\,R\,x$.
3. R is **transitive** $\Leftrightarrow$ for all $x, y, z \in A$, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$.

- Relating this back to directed graphs for relations, these properties may be identified graphically:
  1. The reflexive property may be shown by loops on every vertex.
  2. The symmetric property may be shown by connections between two vertices always being through opposite parallel edges.
  3. The transitive property may be shown by there being no *incomplete directed triangles*.
- Logically, the following negations may be used to disprove them:
  1. R is **not reflexive** $\Leftrightarrow \exists x \in A$ such that $(x, x) \notin R$.
  2. R is **not symmetric** $\Leftrightarrow \exists x, y \in A$ such that if $(x, y) \in R$, then $(y, x) \notin R$.
  3. R is **not transitive** $\Leftrightarrow \exists x, y, z \in A$ such that if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \notin R$.

Example: Properties of Relations on Finite Sets
Let $A = \{0, 1, 2, 3\}$ and R, S, and T be defined as follows:

$$R = \{(0,0), (0,1), (0,3), (1,0), (1,1), (2,2), (3,0), (3,3)\}$$
$$S = \{(0,0), (0,2), (0,3), (2,3)\}$$
$$T = \{(0,1), (2,3)\}$$

Is R reflexive, symmetric, and/or transitive?



Graph 8.2.8: *The directed graph for R.*

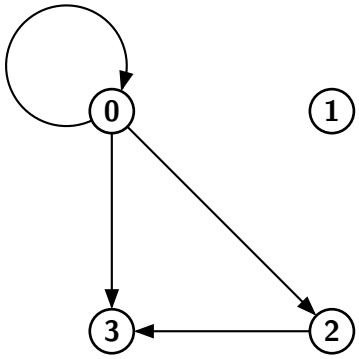
- R is reflexive because there is a loop an each vertex in the directed graph.
- R is also symmetric because for each connection from one vertex to another, there is a second connection from the second vertex to the first.
- However, R is not transitive because there is no complete directed triangle on the directed graph (no directed edge from 1 to 3)

Continued on next page

Example: *Properties of Relations on Finite Sets continued*

Is S reflexive, symmetric, and/or transitive?

- Similar to the first example, creating a directed graph makes this easier.

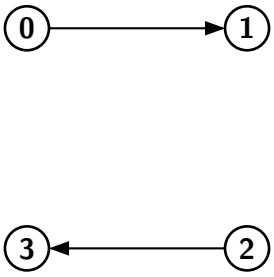


Graph 8.2.10: *The directed graph for S.*

- S is not reflexive because the only vertex with a loop is 0.
- S is not symmetric because when there are connections between vertices, it is only from one vertex to another.
- S is transitive because there is one case where a vertex is both directly and transitively connected to a vertex ($0 \to 2 \to 3$ and $0 \to 3$)

Is T reflexive, symmetric, and/or transitive?

- Again, we will create a directed graph to represent T.



Graph 8.2.11: *The directed graph for T.*

- T is not reflexive because no vertices are connected to themselves via a loop.
- T is not symmetric because when there are connections between vertices, it is only from one vertex to another.
- T is not transitive because there only exists two edges in the graph.

Properties of Relations on Infinite Sets

- For proving relation properties on infinite sets, we have to refer back to their definitions
  - Recall that to prove that a relation is symmetric, we must prove

$$\forall x, y \in A, x \, R \, y \Rightarrow y \, R \, x$$

- For instance, to prove an *equality* relation on the set of all real numbers, we have to prove

$$\forall x, y \in \mathbb{R}, x = y \Rightarrow y = x$$

- While these examples are intuitive, generalizing from the generic particular is often necessary to prove properties.

Example: Equality Relation

Let R be a relation defined on $\mathbb{R}$ as follows:

For all real numbers x and y,

$$x \, R \, y \Leftrightarrow x = y$$

Is R reflexive?

- Yes. x is equal to itself, meaning that $x \, R \, x$.

Is R symmetric?

- Yes. Equality is symmetric; $x = y \Rightarrow y = x$. Thus, $x \, R \, y \Rightarrow y \, R \, x$.

Is R transitive?

- Yes. Equality is transitive; $x = y$ and $y = z \Rightarrow x = z$. Thus, $x \, R \, y \wedge y \, R \, z \Rightarrow x \, R \, z$.

- Recall that two integers may be congruent modulo for integers other than 2 as long as that integer divides their difference.

Example: Properties of Congruence Modulo 2

Let a relation T be defined on $\mathbb{Z}$ as follows:

For all integers m and n,

$$m \, T \, n \Leftrightarrow 3 \mid (m - n)$$

Is T reflexive?

- **Proof:**
- Suppose m is a *particular but arbitrarily chosen* integer such that $m \, T \, m$.
- By definition of T,

$$3 \mid (m - m) = 3 \mid 0$$

- By definition of divisibility, 3 divides 0 because $0 = 0 \cdot 3$.
- Thus, T is reflexive.

Is T symmetric?

- **Proof:**
- Suppose m and n are *particular but arbitrarily chosen* integers such that $m \, T \, n$.
- By definition of T,

$$3 \mid (m - n)$$

- By definition of divisibility, $m - n = 3k$ for some integer k.

$$m - n = 3k \text{ for some integer } k$$
$$n - m = 3(-k) \text{ for some integer } k \text{ by algebra}$$

- $\mathbb{Z}$ is closed under multiplication, so $-k$ is an integer.
- Therefore, by definition of divisibility, $3 \mid (n - m)$.
- Thus, T is symmetric.

Continued on next page

Example: *Properties of Congruence Modulo 2 continued*

Is T transitive?

- **Proof:**
- Suppose m, n, and p are *particular but arbitrarily chosen* integers such that $m\,T\,n$ and $n\,T\,p$.
- By definition of T,

$$3 \mid (m-n) \text{ and } 3 \mid (n-p)$$

- By definition of divisibility, $m-n=3r$ and $n-p=3s$ for some integers r and s.

$$(m-n)+(n-p)=3r+3s \text{ by adding both together}$$
$$m-p=3(r+s) \text{ by algebra}$$

- $(r+s)$ is an integer because $\mathbb{Z}$ is closed under addition.
- Therefore, by definition of divisibility, $3 \mid (m-p)$.
- Thus, T is transitive.

The Transitive Closure of a Relation

Definition:

The **transitive closure** of R, denoted R', is a relation on set A that satisfies the following three properties:

1. R^t is **transitive**.
2. $R \subseteq R^t$.
3. Given S, another transitive relation containing R, $R^t \subseteq S$.

- Generally, relations are not transitive because the property requires a particular pair to exist in the relation given a transitive connection between two elements on the set.
- Thus, to find the next closest transitive relation, the transitive closure, tuples need to be added to ensure the transitivity of the relation.

Example: Transitive Closure of a Relation

Let $A=\{0,1,2,3\}$.

Let relation R be defined on A as follows:

$$R=\{(0,1),(1,2),(2,3)\}$$

What is the transitive closure of R?

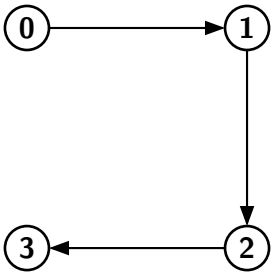
- Given the **second property** of transitive closures defined earlier:

$$\{(0,1),(1,2),(2,3)\} \subseteq R^t$$

Continued on next page

Example: *Transitive Closure of a Relation continued*

- First, a directed graph for R may be constructed.

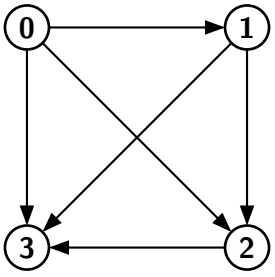


Graph 8.2.14: *The directed graph for R. From here, we can see transitive connections from vertices* **0** *and* **1**, *respectively, to other vertices in the graph.*

- Now we can look for potential edges that can be added to create R^t.
- From vertex **0**, we know that we can add edges to vertex **2** and **3** because vertex **0** has indirect connections to them.
- Additionally, we can add an edge from vertex **1** to **3** because it is transitively connected to it through vertex **2**.
- Thus, we can say that R^t equals

$$R^t = \{(0,1),(0,2),(0,3),(1,2),(1,3),(2,3)\}$$

- This works because we know that the previous ordered pairs are at least in R^t. However, this relation is transitive, thus it equals R^t.



Graph 8.2.15: *The directed graph for R^t.*

8.3 Equivalence Relations

The Relation Induced by a Partition

- Recall that a **partition** of a set is a collection of mutually disjoint sets whose union is the original set.

Definition:
Given a partition of set A, the **relation induced by the partition**, R, is defined on A as follows:

For every $x, y \in A$,

$x \, R \, y \Leftrightarrow$ There is a subset A_i of the partition such that both x and y are in A_i.

Example: Relation Induced by the Partition
Let $A = \{0, 1, 2, 3, 4\}$. A partition of A is as follows:

$$\{0, 3, 4\}, \{1\}, \{2\}$$

What is the relation R induced by this partition?

- *We can evaluate the ordered pairs in R by analyzing the contents of each set in the partition.*
- According to the contents of the first set:

$$0 \, R \, 0$$
$$0 \, R \, 3$$
$$0 \, R \, 4$$
$$3 \, R \, 0$$
$$3 \, R \, 3$$
$$3 \, R \, 4$$
$$4 \, R \, 0$$
$$4 \, R \, 3$$
$$4 \, R \, 4$$

- Additionally, according to the contents of the other sets:

$$1 \, R \, 1$$
$$2 \, R \, 2$$

- Therefore,

$$R = \{(0, 0), (0, 3), (0, 4), (3, 0), (3, 3), (3, 4), (4, 0), (4, 3), (4, 4), (1, 1), (1, 2)\}$$

Theorem 8.3.1:
Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.

Definition of an Equivalence Relation

Definition:
Let A be a set and R be a relation on A. R is an **equivalence relation**, if, and only if, R is reflexive, symmetric, and transitive.

Example: An Equivalence Relation on a Set of Subsets
Let X be the set of all nonempty subsets of $\{1, 2, 3\}$. Then,

$$X = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Define a relation R on X as follows:

For every A and B in X,

$$A\,R\,B \Leftrightarrow \text{The least element in } A \text{ equals the least element in } B.$$

Prove that R has all three properties. **Prove that R is reflexive:**
- Suppose that A is a nonempty subset of $\{1, 2, 3\}$.
- Logically, the least element of A should always equal the least element of A.
- Therefore, $A\,R\,A$.
- R is reflexive.

Prove that R is symmetric:
- Suppose that A and B are nonempty subsets of $\{1, 2, 3\}$ such that $A\,R\,B$.
- If $A\,R\,B$, then the least element of A equals the least element in B.
- This implies that the least element in B equals the last element of A.
- So, in this case, $B\,R\,A$.
- R is symmetric.

Prove that R is transitive:
- Suppose that A, B, and C are nonempty subsets of $\{1, 2, 3\}$ such that $A\,R\,B$ and $B\,R\,C$.
- By definition of R, the least element of A equals the least element in B, and the least element in B equals the least element in C.
- As a result, the least element of A must equal the least element in C.
- Hence, $A\,R\,C$.
- R is transitive.

Because R is reflexive, symmetric, and transitive, it is an equivalence relation.

Equivalence Classes of an Equivalence Relation

Definition:
Suppose that R is an equivalence relation on a set A. For each element a in A, the **equivalence class of a**, denoted $[a]$ and called the **class of a** for short, is the set of all elements $x \in A$ such that $x\,R\,a$.

$$[a] = \{x \in A \mid x\,R\,a\}$$

- Procedurally,

$$\text{for every } x \in A, x \in [a] \Leftrightarrow x \, R \, a$$

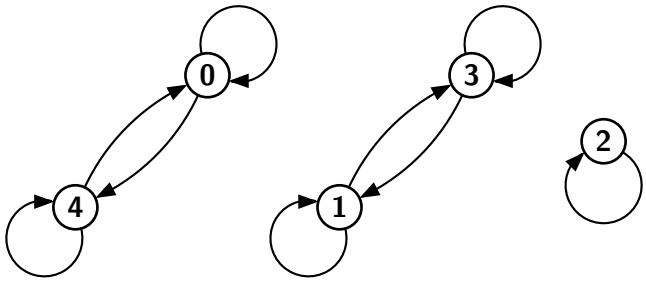
- The notation $[a]_R$ may be used to specify an equivalence class of a for a particular relation R.
- Additionally, for any equivalence class $[a]$, a is the **representative** for the class.
  - However, equivalence classes may be equal even if they have different representatives.

Example: Equivalence Classes of a Relation Given as a Set of Ordered Pairs

Let $A = \{0, 1, 2, 3, 4\}$ and define relation R on A as follows:

$$R = \{(0,0), (0,4), (1,1), (1,3), (2,2), (3,1), (3,3), (4,0), (4,4)\}$$

Additionally, the directed graph is as follows:



What are the distinct equivalence classes of R?

$$[0] = \{x \in A \mid x \, R \, 0\} = \{0, 4\}$$
$$[1] = \{x \in A \mid x \, R \, 1\} = \{1, 3\}$$
$$[2] = \{x \in A \mid x \, R \, 2\} = \{2\}$$
$$[3] = \{x \in A \mid x \, R \, 3\} = \{1, 3\}$$
$$[4] = \{x \in A \mid x \, R \, 4\} = \{0, 4\}$$

- Removing duplicate sets, the distinct equivalence classes are as follows:

$$\{0, 4\}, \{1, 3\}, \{2\}$$

Example: Equivalent Classes of the Identity Relation

Let A be any set and define a relation R on A as follows:

$$\textit{For every } x, y \in A,$$

$$x \, R \, y \Leftrightarrow x = y$$

R is also an equivalence relation.

What are the distinct equivalence classes of R?

$$[a] = \{x \in A \mid x \, R \, a\}$$
$$[a] = \{x \in A \mid x = a\} \text{ by definition of } R$$
$$[a] = \{a\}$$

- Given this definition, the classes for all elements in A are all distinct equivalence classes of R.

Lemma 8.3.2:
Suppose R is an equivalence relation on set A, and a and b are elements of A.

$$a\,R\,b \Rightarrow [a] = [b]$$

Lemma 8.3.3:
If R is an equivalence relation on set A, and a and b are elements of A, then

$$[a] \cap [b] = \emptyset \text{ or } [a] = [b]$$

Theorem 8.3.4:
Given equivalence relation R on set A, the distinct equivalence classes of R altogether are equivalent to A's partition.

Congruence Modulo n

Example: Equivalence Classes of Congruence Modulo 3
Let R be the congruence modulo 3 relation on $\mathbb{Z}$, or

$$m\,R\,n \Leftrightarrow 3 \mid (m - n)$$

What are the equivalence classes of R?

- For each integer a,

$$[a] = \{x \in \mathbb{Z} \mid x\,R\,a\}$$
$$[a] = \{x \in \mathbb{Z} \mid 3 \mid (x - a)\} \text{ by definition of } R$$
$$[a] = \{x \in \mathbb{Z} \mid (x - a) = 3k \text{ for some integer } k\} \text{ by definition of divisibility}$$
$$[a] = \{x \in \mathbb{Z} \mid x = 3k + a\}$$

- It should follow that there are three equivalence classes of R.

$$[0] = \{x \in \mathbb{Z} \mid x = 3k \text{ for some integer } k\}$$
$$[1] = \{x \in \mathbb{Z} \mid x = 3k + 1 \text{ for some integer } k\}$$
$$[2] = \{x \in \mathbb{Z} \mid x = 3k + 2 \text{ for some integer } k\}$$

This is an instance of a relation where equivalence classes can take on different names. Since the relation in based on remainders, $[0]$ is the same equivalence class as $[3]$ or $[6]$.

Definition:
Let m and n be integers and let d be a positive integer. m is said to be **congruent to n modulo d**, shown as

$$m \equiv n (\text{mod}\, d) \Leftrightarrow d \mid (m - n)$$

Example: Evaluating Congruencies

Determine the truth values of the following congruencies:

$$12 \equiv 7 (\mathrm{mod}\, 5)$$
$$6 \equiv -8 (\mathrm{mod}\, 4)$$
$$3 \equiv 3 (\mathrm{mod}\, 7)$$

- The first congruency is true.

$$\begin{aligned} 12 - 7 &= 5 \\ &= 5 \cdot 1 \\ \therefore 5 &\mid (12 - 7) \end{aligned}$$

- The second congruency is false.

$$\begin{aligned} 6 - (-8) &= 14 \\ \therefore 5 &\nmid (6 - (-8)) \end{aligned}$$

- The third congruency is true.

$$\begin{aligned} 3 - 3 &= 0 \\ &= 7 \cdot 0 \\ \therefore 7 &\mid (3 - 3) \end{aligned}$$

A Definition for Rational Numbers

- When expressed as fractions, the same rational number can be expressed using different numerators and denominators

$$\frac{6}{7} = \frac{12}{14}$$

  - Yet, they could represent the different tuples $(6,7)$ and $(12,14)$.
- Algebraically, it follows that

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

Example: Rational Numbers As Equivalence Classes

Let A be the set of all ordered pairs of integers excluding pairs whose second element is zero.

$$A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$$

Additionally, let R be a relation on A as follows:

For all pairs (a,b) *and* $(c,d) \in A$,

$$(a,b)\,R\,(c,d) \Leftrightarrow ad = bc$$

Continued on next page

Example: *Rational Numbers as Equivalence Classes continued*

Prove that R is transitive.

- Suppose (a,b), (c,d), and (e,f) are *particular but arbitrarily chosen* elements of A such that

$$(a,b)\,R(c,d) \text{ and } (c,d)\,R(e,f)$$

- By definition of R,

$$(1)\ ad = bc$$
$$(2)\ cf = de$$

- Because the second elements for all tuples in A are nonzero, both sides of (1) and (2) may be multiplied by f and b, respectively.

$$(1')\ adf = bcf$$
$$(2')\ bcf = bde$$

- Now, $(1')$ and $(2')$ are equal to the same thing. Thus,

$$adf = bde$$
$$af = be \text{ because } d \neq 0$$

- Therefore, by definition of R, $(a,b)\,R(e,f)$.

R is transitive.

What are the equivalence classes of R?

- Every unique rational number may represent an equivalence class for R. Meanwhile, equivalent rational numbers are stored in each equivalence class because the rule for R follows the same logic as the equality of rational numbers.

$$[(1,2)] = \{(1,2),(-1,-2),(2,4),(-2,-4),\ldots(n,2n)\} \text{ for each } n \in \mathbb{Z} - \{0\}$$

8.4 Modular Arithmetic with Applications to Cryptography

Cryptography refers to study of learning techniques to mask messages. **Encryption** transforms **plaintext** into **ciphertext**, which is largely unreadable without using **decryption**. Methods of encryption are known as **ciphers**.

- For example, the **Caesar cipher** encrypts messages by doing an alphanumeric shift that wraps back to the beginning.
  - Thus, given numerical represents of ciphertext C and plaintext M:

$$C = (M + 3) \bmod 26$$

  - *Each letter in the Latin alphabet may be associated with a number according to their position.*
- Simple ciphers like the Caesar cipher can be very unsecure, especially with larger plaintext where patterns are accentuated.
- Meanwhile, public-key cryptography systems, including the **RSA cipher**, use properties of congruence modulo n, making them very difficult to decrypt.

Properties of Congruence Modulo n

Theorem 8.4.1:

Let a, b, and n be any integers for $n > 1$. These statements are all equivalent to each other:

- $n \mid (a - b)$.
- $a \equiv b \pmod{n}$.
- $a = b + kn$ for some integer k.
- a and b have the same nonnegative remainder when divided by n.
- $a \bmod n = b \bmod n$.

- Essentially, two numbers are congruent modulo n, if, and only if, they share the remainder n.
- Recall the quotient-remainder theorem

$$a = nq + r \text{ for } 0 \leq r < n$$

- Consequently, there are exactly n integers that satisfy the constraint, and, by extension, n possible remainders.

Definition:

Given integers a and n for $n > 1$, **the residue of $a \bmod n$** is the remainder r as denoted by quotient-remainder theorem. Thus, the **complete set of residues modulo n** is the sequence, $0, 1, 2, \ldots, n - 1$.

- Thus, by evaluating the modulo equation, we are finding the residue, which is known as **reducing a number modulo n**.
- When n is fixed, the shorthand phrase, **the residue of a**, is often used.

Theorem 8.4.2:
Given an integer n for $n > 1$, congruence modulo n is an equivalence relation on $\mathbb{Z}$. The distinct equivalence classes of the set are

$$[a] = \{m \in Z \mid m \equiv a (\mathrm{mod}\, n)\}$$

for each $a = 0, 1, 2, ..., n - 1$.

Modular Arithmetic

A core principle of congruence modulo n is that performing operations closed under $\mathbb{Z}$ before reducing via modulo n is the exact same as performing modulo n on the operands.

Theorem 8.4.3:
Given integers a, b, c, d, and n for $n > 1$, suppose that

$$a \equiv c \bmod n \text{ and } b \equiv d (\mathrm{mod}\, n)$$

The following equivalencies must hold:

- $(a + b) \equiv (c + d) (\mathrm{mod}\, n)$.
- $(a - b) \equiv (c - d) (\mathrm{mod}\, n)$.
- $ab \equiv cd (\mathrm{mod}\, n)$.
- $a^m \equiv c^m (\mathrm{mod}\, n) \forall$ integer m.

Example: Modular Arithmetic Basics
Modular arithmetic's main application is reducing large computations.

- $55 + 26 \equiv (3 + 2) (\mathrm{mod}\, 4)$

$$\begin{aligned} 81 &\equiv 5 (\mathrm{mod}\, 4) \\ 81 - 5 &= 76 \\ &= 4 \cdot 19 \\ \therefore 5 &\mid (81 - 5) \end{aligned}$$

- $55 - 26 \equiv (3 - 2) (\mathrm{mod}\, 4)$

$$\begin{aligned} 29 &\equiv 1 (\mathrm{mod}\, 4) \\ 29 - 1 &= 28 \\ &= 4 \cdot 9 \\ \therefore 5 &\mid (29 - 1) \end{aligned}$$

- $55 \cdot 26 \equiv (3 \cdot 2) (\mathrm{mod}\, 4)$

$$\begin{aligned} 1430 &\equiv 6 (\mathrm{mod}\, 4) \\ 1430 - 6 &= 1424 \\ &= 4 \cdot 356 \\ \therefore 5 &\mid (1430 - 6) \end{aligned}$$

Continued on next page

Example: *Modular Arithmetic Basics continued*

- $55^2 \equiv (3^2) \pmod 4$

$$3025 \equiv 9 \pmod 4$$
$$3025 - 9 = 3016$$
$$= 4 \cdot 754$$
$$\therefore 5 \mid (3025 - 9)$$

Corollary 8.4.4:

Given integers a, b, and n for $n > 1$,

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod n$$
$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n$$

Additionally, for any positive integer m:

$$a^m \equiv \left[(a \bmod n)^m\right] \pmod n$$

- When modular arithmetic is applied to large numbers, *such as in RSA cryptography*, computations use two particular properties of exponents:

$$x^{2a} = \left(x^2\right)^a \text{ for all real numbers } x \text{ and } a \text{ for } x \geq 0.$$
$$x^{a+b} = x^a x^b \text{ for all real numbers } x, a \text{ and } b \text{ for } x \geq 0.$$

Example: Modulo n with powers of 2

Find the residue of $144^4 \bmod 713$.

$$144^4 \bmod 713 = \left(144^2\right)^2 \bmod 713$$
$$= \left(144^2 \bmod 713\right)^2 \bmod 713$$
$$= (20736 \bmod 713)^2 \bmod 713$$
$$= 59^2 \bmod 713$$
$$= 3481 \bmod 713$$
$$= 629$$

Example: Modulo n without powers of 2

Find the residue of $12^{43} \bmod 713$.

- *Recalling the second property, 43 can be split into multiple exponents to simplify the problem.*

$$43 = 2^5 + 2^3 + 2^1 + 2^0$$
$$= 32 + 8 + 2 + 1$$
$$12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12$$

Continued on next page

Example: *Modulo n without powers of 2 continued*

- By **Corollary 8.4.4.**, we can split products modulo n into the product of the operands modulo n, modulo n.
- We can start by evaluating them separately.

$$\begin{aligned} 12 \bmod 713 &= 12 \\ 12^2 \bmod 713 &= 144 \\ 12^4 \bmod 713 &= 144^2 \bmod 713 \\ &= 59 \\ 12^8 \bmod 713 &= 59^2 \bmod 713 \\ &= 629 \\ 12^{32} \bmod 713 &= 629^2 \bmod 713 \\ &= 485 \end{aligned}$$

- Thus,

$$\begin{aligned} 12^{43} \bmod 713 &= \left[(12^{32} \bmod 713) \cdot (12^8 \bmod 713) \cdot (12^2 \bmod 713) \cdot (12^1 \bmod 713)\right] \bmod 713 \\ &= (485 \cdot 629 \cdot 59 \cdot 144 \cdot 12) \bmod 713 \text{ by substitution} \\ &= 527152320 \bmod 713 \\ &= 48 \end{aligned}$$

Note that finding the residue is difficult regardless of what you do, as the exponents are still large after being split.

Extending the Euclidean Algorithm

- Recall the process for the euclidean algorithm:

```
'''
For a >= b >= 0, calculate the greatest common divisor between a and b.
Continuously apply the quotient remainder theorem until a remainder of 0 is reached.
'''
def euclidean(a: int, b: int) -> int:
  if b == 0:
    return a
  return euclidean(b, a % b)
```

Definition:
An integer d is a **linear combination of integers** a and b if, and only if, there exist integers s and t such that $as + bt = d$.

Theorem 8.4.5:
For all nonzero integers a and b, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Example: Expressing a GCD as a Linear Combination

Express $\gcd(330, 156)$ as the linear combination of 330 and 156 using the Euclidean algorithm.

- Using Euclidean's algorithm:

$$\begin{aligned} 330 &= 156 \cdot 2 + 18 \\ 156 &= 18 \cdot 8 + 12 \\ 18 &= 12 \cdot 1 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

- This implies that $\gcd(330, 156) = 6$.
- *Defining each remainder in terms of everything else:*

$$\begin{aligned} 18 &= 330 - 156 \cdot 2 \\ 12 &= 156 - 18 \cdot 8 \\ 6 &= 18 - 12 \cdot 1 \end{aligned}$$

- Now, we can backtrack through each step through continuous substitutions, making sure to keep multiples of 330 and 156 intact.

$$\begin{aligned} \gcd(330, 156) &= 6 \\ &= 18 - 12 \cdot 1 \\ &= 18 - (156 - 18 \cdot 8) \cdot 1 \text{ by substitution} \\ &= 18 \cdot 9 - 156 \\ &= (330 - 156 \cdot 2) \cdot 9 - 156 \text{ by substitution} \\ &= 330 \cdot 9 - 156 \cdot 18 - 156 \\ &= \underbrace{330 \cdot 9 + 156 \cdot (-19)}_{\text{Linear Combination}} \end{aligned}$$

Logically, the linear combination of 330 and 156 reduces to 6.

Finding an Inverse Modulo n

- Consider the following congruence:

$$2x \equiv 3 \pmod 5$$

- Here, we have to evaluate a value of x that satisfies the congruence.
- Notice that for $x = 3$, 2 is related to 1 by modulo 5.

$$6 \equiv 1 \pmod 5$$

- Thus, we can see the number 3 as an **inverse for $2 \bmod 5$**. Now, we can try multiplying both sides by the inverse to see if it will help solve for x.

$$\begin{aligned} 3 \cdot 2x &\equiv 3 \cdot 3 \pmod 5 \\ 6x &\equiv 9 \pmod 5 \\ 6x &\equiv 4 \pmod 5 \text{ by quotient-remainder theorem} \end{aligned}$$

- Now, because $6 \equiv 1 (\mathrm{mod}\, 5)$, we can say that $6x \equiv 1 \cdot x (\mathrm{mod}\, 5)$.
- Additionally, because we've established that modular congruence is symmetric and transitive:

$$6x \equiv 4 (\mathrm{mod}\, 5) \equiv 4 \equiv x (\mathrm{mod}\, 5) \equiv x \Rightarrow x \equiv (4 \bmod 5)$$

- Thus, a valid solution to the congruency is $x = 4$.

Definition:
Given any integer a and positive integer n, if there exists an integer s such that $as \equiv 1 (\mathrm{mod}\, n)$, then s is **an inverse for a modulo n**.

Definition:
Integers a and b are **relatively prime**, if and only if, $\gcd(a, b) = 1$.
Additionally, a sequence of integers $a_1, a_2, ..., a_n$ may be **pairwise relatively prime** for all integers $i \geq 1$ and $j \leq n$ given that $i \neq j$.

Corollary 8.4.6:
Given relatively prime integers a and b, there must exist integers s and t such that $as + bt = 1$.

Example: Expressing 1 as a Linear Combination of Relatively Prime Integers

Show that 660 and 43 are relatively prime. Additionally, find a corresponding linear combination equal to 1.

- Again, we will use use Euclidean's algorithm:

$$\begin{aligned} 660 &= 43 \cdot 15 + 15 \\ 43 &= 15 \cdot 2 + 13 \\ 15 &= 13 \cdot 1 + 2 \\ 13 &= 2 \cdot 6 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

- Thus, $\gcd(660, 43) = 1$.
- **Therefore, 660 and 43 are relatively prime.**
- Because the greatest common divisor is 1, then it follows that backtracking through the algorithm should yield a Linear Combination equal to 1.
- *Defining each remainder in terms of everything else:*

$$\begin{aligned} 15 &= 660 - 43 \cdot 15 \\ 13 &= 43 - 15 \cdot 2 \\ 2 &= 15 - 13 \cdot 1 \\ 1 &= 13 - 2 \cdot 6 \end{aligned}$$

Continued on next page

Example: *Expressing 1 as a Linear Combination of Relatively Prime Integers continued*

- Like the last example, we can now use continuous substitutions to find the Linear Combination:

$$\begin{aligned}\gcd(660,43) &= 1\\ &= 13 - 2\cdot 6 \text{ by substitution}\\ &= 13 - (15-13)\cdot 6 \text{ by substitution}\\ &= 13 - 15\cdot 6 + 13\cdot 6\\ &= 13\cdot 7 - 15\cdot 6\\ &= (43 - 15\cdot 2)\cdot 7 - 15\cdot 6 \text{ by substitution}\\ &= 43\cdot 7 - 15\cdot 14 - 15\cdot 6\\ &= 43\cdot 7 - 15\cdot 20\\ &= 43\cdot 7 - (660 - 43\cdot 15)\cdot 20 \text{ by substitution}\\ &= 43\cdot 7 - 660\cdot 20 + 43\cdot 300\\ &= \underbrace{43\cdot 307 + 660\cdot(-20)}_{\text{Linear Combination}}\end{aligned}$$

Corollary 8.4.7:

For all integers a and n, if $\gcd(a,n) = 1$, then there exists an integer s such that $as \equiv 1 \pmod{n}$, that is, an inverse for a modulo n.

RSA Cryptography

- **RSA ciphers** encrypt messages using a product of two distinct prime numbers pq and some integer e relatively prime to the number of distinct prime factors of pq.
  - This ensures that the **public key** and the **private key** are distinct.
- Thus, for very large values of p and q, it is difficult to ascertain them from just the product.
- Thus, all messages can be easily encrypted by the accessible **public key**, then decrypted by the cipher using the **private key**.

Example: Simple RSA Cipher

First, we can choose the values of p and q.

- To minimize key overlapping, we can choose $p = 5$ and $q = 11$.
- Thus, $pq = 55$.

Now, we can choose an integer e, and we want it to be relatively prime to the number of distinct prime factors of pq to ensure that the private key's modular inverse is unique.

- Euler's totient function gives the number of distinct prime numbers up to a given integer, and it can be used to find the total factors of pq:

$$\begin{aligned}\Phi(pq) &= \Phi(p)\Phi(q)\\ &= (p-1)(q-1)\end{aligned}$$

- Now, since $(p-1)(q-1) = 40$, we can let $e = 3$, which is relatively prime to 40.

Continued on next page

Example: *Simple RSA Cipher continued*

With these two values, we have a **public key**:

$$(pq, e) = (55, 3)$$

Thus, for each letter in a message, the following formula may be used to encrypt plaintext M into ciphertext C:

$$C = M^e \bmod pq$$

- Each letter in the alphabet we be associated with their nth place in the alphabet.
- For instance, to send the message, "HI", it could be encrypted as:

$$\begin{aligned} C_1 &= \mathrm{H}^e \bmod pq \\ &= 8^3 \bmod 55 \\ &= 512 \bmod 55 \\ &= 17 \end{aligned} \qquad \begin{aligned} C_2 &= \mathrm{I}^e \bmod pq \\ &= 9^3 \bmod 55 \\ &= 729 \bmod 55 \\ &= 14 \end{aligned}$$

$$\boxed{17\ 14}$$

To create a **private/decryption key**, we need an additional integer that is the positive inverse to $e \bmod (p-1)(q-1)$. We can refer to this integer as d, and is the last part of the private key:

$$(pq, d)$$

This private key may be used in the following decryption formula:

$$M = C^d \bmod pq$$

Keep in mind that real RSA cryptography would use values far larger than this.

Euclid's Lemma

Theorem 8.4.8:

$\forall$ integers a, b, and c,

$$\gcd(a, b) = 1 \text{ and } a \mid bc \Rightarrow a \mid b$$

8.5 Partial Order Relations

Antisymmetry

- As opposed to symmetric relations showing two-way connections between connected elements in an arrow diagram, antisymmetric

Definition:
Let R be a relation on a set A. R is **antisymmetric**, if and only if, for every a and $b \in A$, if $a\,R\,b$ and $b\,R\,a$, then $a = b$.

- Thus, to disprove that a relation is antisymmetric,

$$\exists a \text{ and } b \text{ such that } a\,R\,b \text{ and } b\,R\,a \text{ but } a \neq b$$

Example: Testing Antisymmetry for Finite Relations
Let R_1 and R_2 be relations on $\{0, 1, 2\}$ defined as follows:

$$R_1 = \{(0, 2), (1, 2), (2, 0)\}$$
$$R_2 = \{(0, 0), (0, 1), (0, 2), (1, 1), (1, 2)\}$$

Are any of the relations antisymmetric?

- R_1 is not antisymmetric. When drawing out its directed graph, there are two parallel edges between vertex 0 and 2.

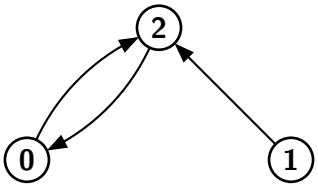


Diagram 8.5.22: The directed graph for R_1.

- R_2 is antisymmetric. All connections between different vertices are only through one edge.

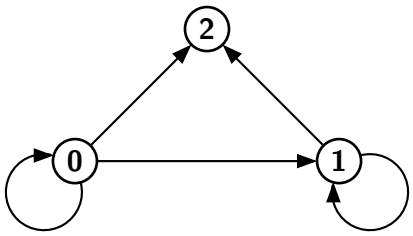


Diagram 8.5.23: The directed graph for R_2.

Antisymmetry with Partial Order Relations

Definition:
Let R be a relation defined on set A. R is a **partial order relation**, if, and only if, R is reflexive, antisymmetric, and transitive.

- The first fundamental partial order relation is the **less than or equal to** relation on $\mathbb{R}$.

For all integers a and b,

$$a \mathrel{R} b \Leftrightarrow a \preceq b$$

- The second fundamental partial order relation is the **subset** relation on a set of sets.

For any sets A and $B \in C$,

$$A \mathrel{R} B \Leftrightarrow A \subseteq B$$

- Due to the commonality of the *less than or equal to* relation, the symbol $\preceq$ is used to denote it as a general partial order relation.
  - Consequently, $x \preceq y$ may be read as the same as "$x \leq y$."

Example: Divides Relation

Let $\mid$ be the divides relation on set of positive integers A. It is defined as follows:

For all positive integers a and $b \in A$

$$a \mid b \Leftrightarrow b = ka \text{ for some integer } k$$

Prove that $\mid$ is a partial order relation on A.

Prove that $\mid$ is reflexive:

- Suppose there exists some positive integer $a \in A$.

$$a = 1 \cdot a$$

- By definition of divisibility, $a \mid a$.
- Thus, $\mid$ is reflexive.

Prove that $\mid$ is antisymmetric:

- Suppose there exists some positive integers a and $b \in A$ such that $a \mid b$ and $b \mid a$.
- By definition of divisibility, $a = k_1 b$ and $b = k_2 a$ for some integers k_1 and k_2.

$$\begin{aligned} a &= k_1 b \\ a &= k_1 k_2 a \text{ by substitution} \\ 1 &= k_1 k_2 \text{ by algebra} \end{aligned}$$

- Because a and b are both positive integers, it follows that k_1 and k_2 are also positive integers.
- The only product of two positive integers that equates to 1 is $1 \cdot 1$.
- Therefore, $k_1 = k_2 = 1$.
- By substitution, $a = b$ and $b = a$.
- Thus, $\mid$ is antisymmetric.

Prove that $\mid$ is transitive:

- Suppose there exists some positive integers a, b, and $c \in A$ such that $a \mid b$ and $b \mid c$.
- By definition of divisibility, $a = rb$ and $b = sc$ for some integers r and s.

$$\begin{aligned} a &= rb \\ a &= rsc \end{aligned}$$

- Because $\mathbb{Z}$ is closed under multiplication, rs is an integer.
- By definition of divisibility, $a \mid c$, so $\mid$ is transitive.

Because $\mid$ is reflexive, antisymmetric, and transitive, it is a partial order relation.

Lexicographic Order

- In programming languages, strings are generally sorted **lexicographically**.

Theorem 8.5.1:
Let A be a set with a partial order relation R, and let S be a set of strings over A. Define a relation $\preceq$ on S as follows:

For any strings s and t of positive integer lengths m and n, respectively, let s_m and t_m be the characters at the mth position of s and t, respectively. Thus, the following conditions hold:

1. If $m \leq n$ and the first m characters are the same between s and t, then $s \preceq t$.
2. If the first $m-1$ characters are the same between s and t, $s_m \, R \, t_m$, and $s_m \neq t_m$, then $s \preceq t$.
3. Null string $\lambda \preceq s$.

If no strings are related by $\preceq$ other than the aforementioned conditions, then $\preceq$ is a partial order relation on S.

- Essentially, $\preceq$ defines a sorting order for the strings depending on the comparative values of each character in the strings.
- For instance, `"flag"` is related to `"flagged"` by $\preceq$ according to the first condition, and `"flagged"` is related to `"flagger"` by $\preceq$ by the second condition.
  - Thus, the resulting order would be `{"flag", "flagged", "flagger"}`
- Additionally, notice how the set A has another partial relation R. This means that $\preceq$ may only sort comparable elements, that is, when each character being related to each other by R.

Definition:
The partial order relation, $\preceq$, outlined in **Theorem 8.5.1.**, is the **lexicographic order for S** that corresponds to the partial order R on A.

Hasse Diagrams

- A **Hasse diagram** is a *simplified* arrow diagram that may be associated with a partial order relation defined on a finite set.
- It is oriented upward, that is, all arrows aside from loops will point upward.
- Loops, transitive-implied edges, and direction indicators are all omitted.
- Suppose we let set $A = \{1, 2, 3, 9, 18\}$, and define the following *divides* relation on A:

$$\text{For all } a \text{ and } b \in A,$$

$$a \mid b \Leftrightarrow b = ka \text{ for some integer } k$$

- This results in the following directed graph:

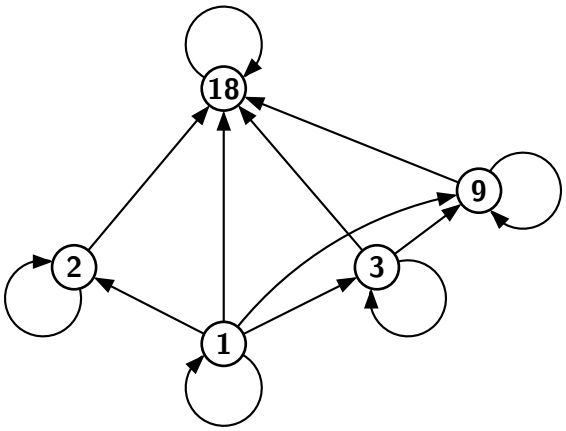


Diagram 8.5.24: The directed graph for the *divides* relation.

- However, this graph is very messy, and we already *know* that it is a partial order relation.
- Thus, we can use the following Hasse diagram to visually express it more clearly:

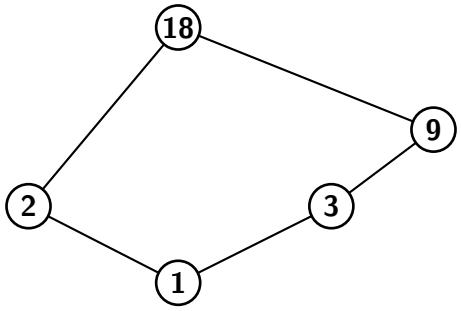


Diagram 8.5.25: The Hasse diagram for the *divides* relation.

- By recalling the properties of partial order relations, we can still construct the original direct graph from this alone.
  - Because the relation is reflexive, we can imagine a loop on every single loop.
  - Because it is oriented upwards, and the relation is antisymmetric, we know that relations between elements will be directed upwards.
  - Because it is oriented upwards, and the relation is transitive, we can imagine extra directed arrows from elements at the bottom to elements higher up on the diagram.

Partially and Totally Ordered Sets

- Given two real numbers x and y such that $x \leq y$ or $y \leq x$, then x and y are known to be **comparable**.
- Meanwhile, given two subsets $A = \{1, 2\}$ and $B = \{2, 3\}$ of $\{1, 2, 3\}$, $A \not\subseteq B$ and $B \not\subseteq A$, so A and B are known to be **noncomparable**.

Definition:
Given a and $b \in A$ and $\preceq$ on A, a and b are **comparable** if, and only if, either $a \preceq b$ or $b \preceq a$. Otherwise, a and b are **noncomparable**.

- All elements in a **total order relation** are comparable.

Definition:
If R is a partial order relation on set A, and for any two elements a and b, $a\,R\,b$ or $b\,R\,a$, then R is a **total order relation**.

- Sets also have special names with respect to particular partial order relations.
  - A set is a **partially ordered set** or **poset** with respect to $\preceq$ if, and only if, $\preceq$ is a partial order relation on it.
  - A set is a **totally ordered set** with respect to $\preceq$ if, and only if, $\preceq$ is a total order relation on it.
- Even then, subsets of posets may still be totally ordered sets, known as chains.

Definition:
Given A, a poset with respect to $\preceq$, subset B of A is a **chain** if, and only if, each pair in B is comparable.
The **length of a chain** is the number of elements in the chain minus one.

Example: A Chain of Subsets
Let set $P(\{a,b,c\})$ be a partially ordered relation with respect to the subset relation. Find a chain of length $3 \in P(\{a,b,c\})$.
- By definition of the subset relation:

$$\emptyset \subseteq \{a\} \subseteq \{a,b\} \subseteq \{a,b,c\}$$

Thus, the set $\{\emptyset,\{a\},\{a,b\},\{a,b,c\}\}$ is the chain of length $3 \in P(\{a,b,c\})$.

- Additionally, partially ordered sets may have extrema. However, there are four rather than two, as it is dependent on the comparability between elements in a set.

Definition:
Let set A be partially ordered with respect to $\preceq$.
1. $a \in A$ is a **maximal element** of $A \Leftrightarrow$ for each $b \in A$, either $b \preceq a$ or b and a are not comparable.
2. $a \in A$ is a **greatest element** of $A \Leftrightarrow$ for each $b \in A$, $b \preceq a$.
3. $a \in A$ is a **minimal element** of $A \Leftrightarrow$ for each $b \in A$, either $a \preceq b$ or a and b are not comparable.
4. $a \in A$ is a **least element** of $A \Leftrightarrow$ for each $b \in A$, $a \preceq b$.

- Following a Hasse diagram, the greatest element should be at the very top, while the least element is at the very bottom.
- Because maximal and minimal elements are only relative to comparable elements, this should only hold true for their respective **chains**.

Example: Maximal, Minimal, Greatest, and Least Elements

Given set $A = \{a, b, c, d, e, f, g, h, i\}$ and the partial order relation defined by the Hasse diagram below, find the maximal, minimal, greatest, and least elements of A.

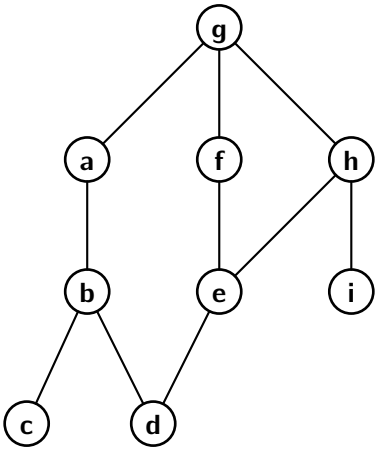


Diagram 8.5.26: The Hasse diagram for A.

- g is the only maximal element.
- g is also the only greatest element.
- c, d, and i are the minimal elements.
- There is no least element.

Topological Sorting

- The basis of topological sorting is that inputs considered *lesser* than another must be inputted before it.

Definition:

Given $\preceq$ and $\preceq'$ on set A, $\preceq'$ is **compatible** with $\preceq$ if, and only if, for every a and $b \in A$, $a \preceq b \Rightarrow a \preceq' b$.

Definition:

Given partial order relations $\preceq$ and $\preceq'$ on set A, $\preceq'$ is a **topological sorting** for $\preceq$, if, and only if, $\preceq'$ is a total order compatible with $\preceq$.

- Formally, the algorithm for constructing a toplogical sorting is as follows:
  1. Pick any minimal element $a \in A$, *given that* $A \neq \emptyset$.
  2. $A' := A - \{a\}$.
  3. Repeat the following steps while $A' \neq \emptyset$:
     - Pick any minimal element $b \in A'$.
     - Define $a \preceq' b$.
     - Set $A' := A' - \{b\}$ and $a := b$.

Example: Topological Sorting Steps

Extra Examples

Example: The Extended Euclidean Algorithm

Use the extended Euclidean algorithm to find the GCD and the Linear Combination of **5590** and **637**.

- *Finding the GCD:*

$$\begin{aligned} 5590 &= 637 \cdot 8 + 494 \\ 637 &= 494 \cdot 1 + 143 \\ 494 &= 143 \cdot 3 + 65 \\ 143 &= 65 \cdot 2 + 13 \\ 65 &= 13 \cdot 5 + 0 \end{aligned}$$

- Thus, $\gcd(5590, 637) = 13$.
- *Defining each remainder in terms of everything else:*

$$\begin{aligned} 494 &= 5590 - 637 \cdot 8 \\ 143 &= 637 - 494 \cdot 1 \\ 65 &= 494 - 143 \cdot 3 \\ 13 &= 143 - 65 \cdot 2 \end{aligned}$$

- *Finding the Linear Combination:*

$$\begin{aligned} \gcd(5590, 637) &= 13 \\ &= 143 - 65 \cdot 2 \text{ by substitution} \\ &= 143 - (494 - 143 \cdot 3) \cdot 2 \text{ by substitution} \\ &= 143 - 494 \cdot 2 + 143 \cdot 6 \\ &= 143 \cdot 7 - 494 \cdot 2 \\ &= (637 - 494) \cdot 7 - 494 \cdot 2 \text{ by substitution} \\ &= 637 \cdot 7 - 494 \cdot 7 - 494 \cdot 2 \\ &= 637 \cdot 7 - 494 \cdot 9 \\ &= 637 \cdot 7 - (5590 - 637 \cdot 8) \cdot 9 \text{ by substitution} \\ &= 637 \cdot 7 - 5590 \cdot 9 + 637 \cdot 72 \\ &= \underbrace{637 \cdot 79 + 5590 \cdot (-9)}_{\text{Linear Combination}} \end{aligned}$$