Part 3: Relations

Contents [DOCUMENT FINALIZED]

Relations

After introducing sets that contain items with certain properties, we may be interested to model relations between elements.

Examples

– We might say that integers a and b are related if a divides b, or $a = b + 1$.

– Two people may be related if they have the same blood type or like the same food.

In this part we will study "is related to" in precise terms by introducing the concept of relations and their properties.

We begin by considering **ordered pairs** of two objects a and b, symbolized by (a, b), which has the property that if either of the **coordinates** a and b change, then the ordered pair changes. I.e., two ordered pairs (a, b) and (x, y) are equal iff $x = a$ and $y = b$.

What makes such pairs ordered is the fact that $(a, b) \neq (b, a)$, i.e. the order of objects matters.

Generalizing this concept we say that the **ordered n-tuples** $(a_1, a_2, \ldots, a_n)$ and $(x_1, x_2, \ldots, x_n)$ are equal iff $a_i = x_i$ for all $i \in \{1 \ldots n\}$.

Thus, the 5-tuples $(1, 2, 3, 4, 5)$, $(5, 4, 3, 2, 1)$, and $(1, 5, 2, 4, 3)$ are all different.

An ordered 2-tuple is an ordered pair, and ordered 3-tuples are called **ordered triples**.

Definition: Let A and B be sets. The set of all ordered pairs having the first coordinate in A and the second in B is called the **Cartesian product** (or **cross product**) of A and B and is written $A \times B$. Thus,

$$A \times B := \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Example

Let $A = \{1, 2\}$ and $B = \{2, 3, 4\}$. Then

$$A \times B = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\},$$

but

$$B \times A = \{(2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)\}$$

What is $A \times A$?

$$A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$

Constructing a list of pairs in a Cartesian product of finite sets requires two tasks: selecting an element from A and then selecting an element from B. The Product Rule says that if A had m elements and B has n, then $A \times B$ has mn elements.

Generalizing the Cartesian product to more than two sets is straight-forward:

$$A_1 \times A_2 \times \cdots A_n := \{(a_1, \ldots, a_n) \mid a_1 \in A_1 \wedge \cdots \wedge a_n \in A_n\}$$

If all A_i are the same we write $A^n = \underbrace{A \times A \cdots \times A}_{A\ n \text{ times}}$.

For example,

$$A \times B \times C = \{(a, b, c) \mid a \in A \wedge b \in B \wedge c \in C\}$$

$A \times B \times C$ and $(A \times B) \times C$ and $A \times (B \times C)$ are all different. Why?

What is $|A_1 \times A_2 \times \cdots A_n|$?

Theorem: If A, B, C, and D are sets, then

1. $A \times \emptyset = \emptyset \times A = \emptyset$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
4. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
5. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

Proof:

2. $(x, y) \in A \times (B \cup C)$

$\Leftrightarrow x \in A \;\wedge\; y \in (B \cup C)$ (Definition)

$\Leftrightarrow x \in A \;\wedge\; (y \in B \vee y \in C)$ (Definition)

$\Leftrightarrow (x \in A \wedge y \in B) \;\vee\; (x \in A \wedge y \in C)$ (Distr. Law)

$\Leftrightarrow (x, y) \in A \times B \;\vee\; (x, y) \in A \times C$ (Definition)

$\Leftrightarrow (x, y) \in (A \times B) \cup (A \times C)$ (Definition)

Rest: exercise $\square$

Relating two objects a and b can be indicated by an ordered pair (a, b) being an element of a set, which is called relation:

Definition: Let A and B be sets. R is a **(binary) relation from $\mathbf{A}$ to $\mathbf{B}$** iff R is a subset of $A \times B$. If $(a, b) \in R$ we write aRb. If $(a, b) \notin R$ we write $a \not R b$. A relation from A to A is called a **relation on $\mathbf{A}$**.

Example 1

Let $A = \{1, 2, 3, 4\}$ and $R = \{(a, b) \mid a \text{ divides } b\}$.

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

Example 2

$R_1 = \{(a, b) \mid a \le b\}$ $\quad R_5 = \{(a, b) \mid a + b \le 3\}$

$R_2 = \{(a, b) \mid a + 2 > b\}$

$R_3 = \{(a, b) \mid a = b \vee a = -b\}$

$R_4 = \{(a, b) \mid a = b\}$

Which relations contain the pairs $(1,1), (1,2), (2,1), (1,-1)$?

Example 3

Let $G = \{(x, y) \in \mathbb{R}^2 \mid x \ge y\}$. Then $(5, 2) \in G$ because $5 \ge 2$. We can also write $5\ G\ 2$. The notation $x\ G\ y$ is consistent with $x \ge y$.

Representations of Relations

There are several ways to present a relation in a usable form. We can list the ordered pairs, present them in a table, find a corresponding predicate, or give a pictorial representation of the ordered pairs by using a rectangular coordinate system to graph the relation.

Example

Let $A = \{1, 2, 3, 4\}$, $B = \{-1, 1, 2, 4, 5\}$, and

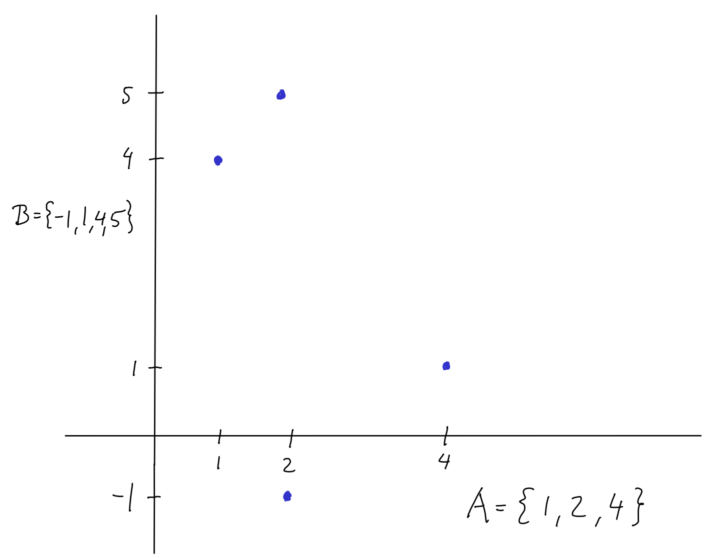
$$R = \{(1, 4), (2, 5), (2, -1), (4, 1)\}$$

Table format:

1	4
2	5
2	−1
4	1

Predicate: $R = \{(x, y) \in A \times B \mid |x - y| = 3\}$

Graph:



In general there are many relations from a set A to a set B, because every subset of $A \times B$ is a relation from A to B, including $\emptyset$ and $A \times B$. If A has m elements and B had n elements, then there are 2^{mn} different relations from A to B (why?)

Definition:

The **domain** of a relation R from A to B is the set

$$\text{Dom}(R) := \{x \in A \mid \exists y \in B : \; x \; R \; y\}$$

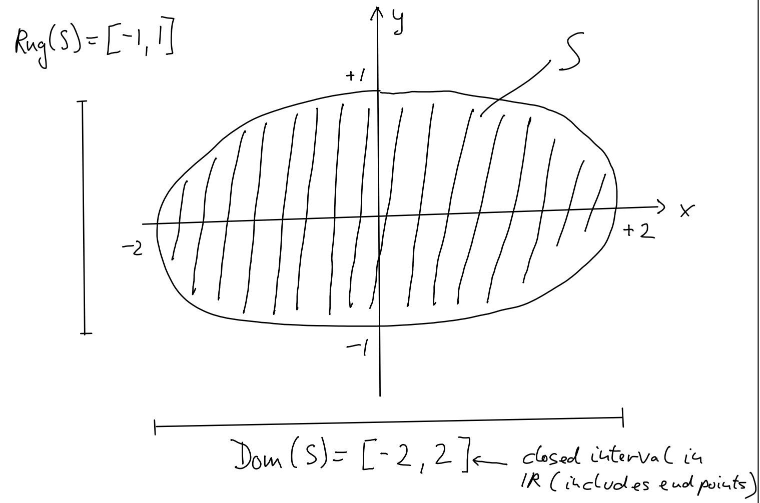
The **range** of relation R is the set

$$\text{Rng}(R) := \{y \in B \mid \exists x \in A : \; x \; R \; y\}$$

Thus, the domain of R is the set of all first coordinates of ordered pairs in R, and the range of R is the set of all second coordinates. By definition $\text{Dom}(R) \subseteq A$ and $\text{Rng}(R) \subseteq B$

Example 1

Let $S = \{(x, y) \in \mathbb{R}^2 \mid \frac{x^2}{4} + y^2 \leq 1\}$



Here we use the interval notation for $\mathbb{R}$:

$$[a, b] := \{x \in \mathbb{R} \mid a \leq x \; \wedge \; x \leq b\}$$

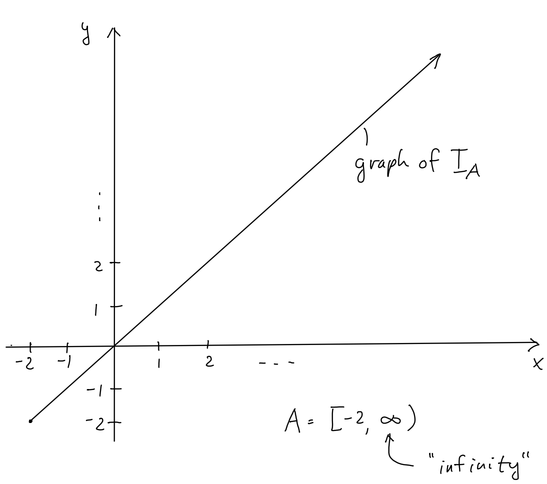
Example 2 Lecture 14

Let A be any set. The set $I_A := \{(x, x) \mid x \in A\}$ is called the **identity relation** on A.

For $A = \{1, 2\}$, $I_A = \{(1, 1), (2, 2)\}$.

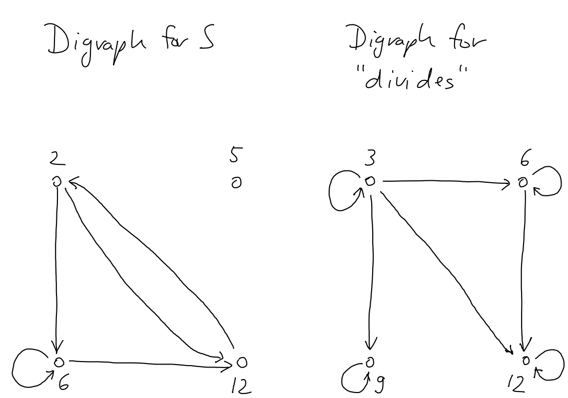
Obviously, for any A, $\text{Dom}(I_A) = \text{Rng}(I_A) = A$.

The graph of I_A is the "main diagonal" of $A \times A$. For $A = [-2, \infty) = \{x \in \mathbb{R} \mid -2 \leq x < \infty\}$ it looks like this:



Another important kind of graphical representation of a relation on a set A is the **directed graph** (or **digraph**). We represent each element of A as a vertex. Relation R is then telling us which vertices to connect by edges. The edges are directed like arrows pointing from vertex x to vertex y iff $(x, y) \in R$.

Examples: The following digraphs represent relations $S = \{(6, 12), (2, 6), (2, 12), (6, 6), (12, 2)\}$ on the set $V = \{2, 5, 6, 12\}$ and the relation "divides" on set $\{3, 6, 9, 12\}$.



Constructing New Relations

The two most fundamental methods for constructing new relations from given ones are **inversion** and **composition**.

Definition: If R is a relation from A to B, then the **inverse** of R is

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

Inversion switches the order of each pair in a relation.

Examples

The inverse of $\{(1,a),(2,b)\}$ is $\{(a,1),(b,2)\}$

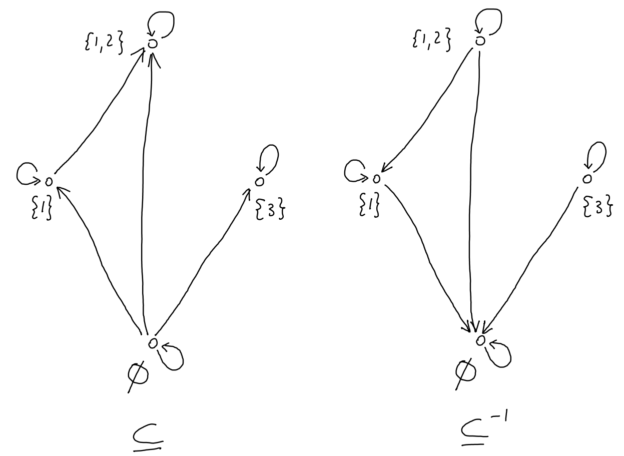
$I_A^{-1} = I_A$ for all sets A

For the real numbers, the inverse of "less than" is "greater than" because $x < y \;\Leftrightarrow\; y > x$.

The digraph of the inverse of a relation on a set differs from the digraph of the relation only in that the directions of the arrows are reversed.

Example

Subset relation $\subseteq$ on the set $\{\emptyset, \{1\}, \{3\}, \{1,2\}\}$ and its reverse:



Another Example

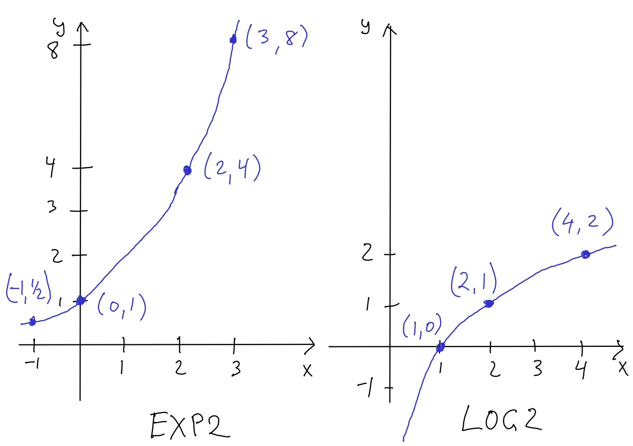
Let EXP2 ("exponential, base 2") be the relation on $\mathbb{R}$ given by

$$x \text{ EXP2 } y \;\Leftrightarrow\; y = 2^x$$

LOG2 ("logarithm, base 2") is the inverse of EXP2

$$x \text{ LOG2 } y \;\Leftrightarrow\; y \text{ EXP2 } x$$

Here are their graphs in the Cartesian plane:



You can create one from the other by mirroring the graphs with respect to the $y = x$ line.

Theorem: Let R be a relation from A to B. Then

1. R^{-1} is a relation from B to A
2. Dom(R^{-1}) = Rng(R)
3. Rng(R^{-1}) = Dom(R)
4. $(R^{-1})^{-1} = R$

Proof:

1. Suppose $(y,x) \in R^{-1}$ (we want to show $(y,x) \in B \times A$).

   Then $(x,y) \in R$, which means $(x,y) \in A \times B$.

   Therefore, $x \in A$ and $y \in B$ and $(y,x) \in B \times A$, which proves $R^{-1} \subseteq B \times A$.

2. $x \in$ Dom(R^{-1})

   iff there exists $y \in A$ with $(x,y) \in R^{-1}$

   iff there exists $y \in A$ with $(y,x) \in R$

   iff $x \in$ Rng(R)

3.+4.: exercise $\square$

Given a relation from A to B and another from B to C, composition is a method of constructing a relation from A to C.

Definition: Let R be a relation from A to B and S be a relation from B to C. The **composite** of R and T is

$$S \circ R := \{(a, c) \mid \exists b \in B : (a, b) \in R \wedge (b, c) \in S\}$$

$S \circ R$ is a relation from A to C because $S \circ R \subseteq A \times C$.

Note the right-to-left procedure for checking whether $(a, c) \in S \circ R$:

– we FIRST consider R by finding a $b \in B$ for the given a with $(a, b) \in R$

– and THEN we consider S when checking $(b, c) \in S$ for the given $c \in C$.

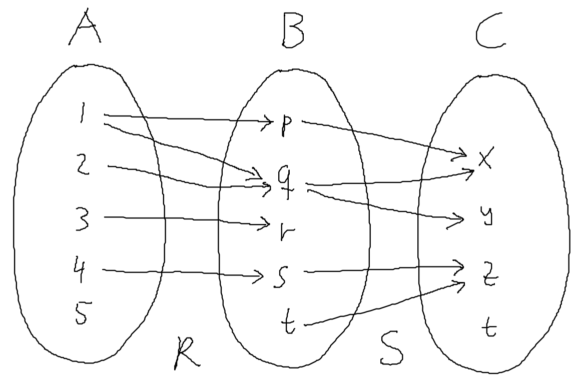
Example

Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{p, q, r, s, t\}$ and $C = \{x, y, z, w\}$ and R be the following relation from A to B:

$$R = \{(1, p), (1, q), (2, q), (3, r), (4, s)\}$$

and S be the following relation from B to C:

$$S = \{(p, x), (q, x), (q, y), (s, z), (t, z)\}$$



What is $S \circ R$?

$$S \circ R = \{\underbrace{(1, x)}_{\text{via } p}, \underbrace{(1, y)}_{\text{via } q}, \underbrace{(2, x)}_{\text{via } q}, \underbrace{(2, y)}_{\text{via } q}, \underbrace{(4, z)}_{\text{via } s}\}$$

Is the composition of relations commutative, i.e. does

$$S \circ R = R \circ S$$

hold in general?

No, not even in the case $R \subseteq A \times A$ and $S \subseteq A \times A$.

Example

$$R := \{(x, y) \in \mathbb{R}^2 \mid y = x + 1\}$$
$$S := \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$$

$$\begin{aligned} S \circ R &= \{(x, y) \mid \exists z \in \mathbb{R} : (x, z) \in R \wedge (z, y) \in S\} \\ &= \{(x, y) \mid \exists z \in \mathbb{R} : z = x + 1 \wedge y = z^2\} \\ &= \{(x, y) \mid y = (x + 1)^2\} \end{aligned}$$

$$\begin{aligned} R \circ S &= \{(x, y) \mid \exists z \in \mathbb{R} : (x, z) \in S \wedge (z, y) \in R\} \\ &= \{(x, y) \mid \exists z \in \mathbb{R} : z = x^2 \wedge y = z + 1\} \\ &= \{(x, y) \mid y = x^2 + 1\} \end{aligned}$$

These are different. One witness is $(1, 4)$: $(1, 4) \in S \circ R$ but $(1, 4) \notin R \circ S$

The following theorem collects serveral results about inversion, composition, and the identity relation.

Theorem: Let A, B, C, D be sets, R a relation from A to B, S a relation from B to C, and T a relation from C to D.

1. $I_B \circ R = R \circ I_A = R$
2. $T \circ (S \circ R) = (T \circ S) \circ R$,
   i.e. relation composition is associative
3. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Proof:

1. We first show $I_B \circ R \subseteq R$. Suppose $(x, y) \in I_B \circ R$.

   Then there exists $z \in B$ such that $(x, z) \in R$ and $(z, y) \in I_B$.

   Since $(z, y) \in I_B$ we know $z = y$. This means $(x, y) \in R$, because $(x, z) \in R$.

   Conversely, suppose $(p, q) \in R$.

   Then, with $(q, q) \in I_B$, we have $(p, q) \in I_B \circ R$.

   Thus, $I_B \circ R = R$. $R \circ I_A = R$ analogous.

2. Lecture 15 Plan: use definitions of $\circ$ to flatten logical description, switch quantifiers, and then undo flattening.
The pair (a,d) is in $T \circ (S \circ R)$

$\Leftrightarrow\ \exists c \in C : \big[(a,c) \in S \circ R \wedge (c,d) \in T\big]$

[definition of $\circ$]

$\Leftrightarrow\ \exists c \in C :$
$\Big[\big(\exists b \in B : (a,b) \in R \wedge (b,c) \in S\big) \wedge (c,d) \in T\Big]$

[cover $(c,d) \in T$ by $\exists b$:]
[$\exists x\big[\big(\exists y\ P(x,y)\big) \wedge Q(x)\big] \equiv$]
[$\exists x\ \exists y\big[P(x,y) \wedge Q(x)\big]$]

$\Leftrightarrow\ \exists c \in C\ \exists b \in B :$
$\big[(a,b) \in R\ \wedge\ (b,c) \in S\ \wedge\ (c,d) \in T\big]$

[switch quantifiers: $\exists c\ \exists b : \varphi \equiv \exists b\ \exists c : \varphi$]

$\Leftrightarrow\ \exists b \in B\ \exists c \in C :$
$\big[(a,b) \in R\ \wedge\ (b,c) \in S\ \wedge\ (c,d) \in T\big]$

$\Leftrightarrow\ \exists b \in B :$
$\Big[(a,b) \in R \wedge \exists c \in C : \big((b,c) \in S\ \wedge\ (c,d) \in T\big)\Big]$

$\Leftrightarrow\ \exists b \in B : \big[(a,b) \in R\ \wedge\ (b,d) \in T \circ S\big]$

$\Leftrightarrow (a,d) \in (T \circ S) \circ R$

3. Exercise. □

The relations we have seen in this section consisted of pairs.

Generalizing the relation definition to more than two variables is straightforward — we just need to consider subsets of $A_1 \times A_2 \cdots \times A_n$.

Using tables that represent multi-dimensional relations is the basis of an important field of computer science called **relational databases**. Currently, most large data sets are organized in such relational databases, which allow to answer queries, such as listing all employees with salary >\$100,000 and age <40, quickly.

Example : relational table representing employee data

First	Last	Age	Salary
Krista	Maire	23	60,000
Adam	Powell	35	85,000
Kim	Martinez	45	104,000

Equivalence Relations

Each of the following three properties is important in its own right, and relations that posses all three properties are particularly interesting:

Definition: Let A be a set and R be a relation on A.

- R is **reflexive on A** iff $\forall x \in A : xRx$
- R is **symmetric** iff
  $\forall x \in A\ \forall y \in A : (xRy \Rightarrow yRx)$
- R is **transitive** iff
  $\forall x \in A\ \forall y \in A\ \forall z \in A : \big[(xRy \wedge yRz) \Rightarrow xRz\big]$

For a relation $R \neq \emptyset$, R being reflexive asserts that some ordered pairs belong to R.

To prove R is reflexive one has to show that xRx for all $x \in A$, i.e. $I_A \subseteq R$.

To show that R is not reflexive one needs to find an $x \in A$ for which $x \not R\, x$.

$\emptyset$ is not reflexive on A except when A is empty.

Because symmetry or transitivity are defined by conditional sentences, proofs of these properties are usually direct.

$\emptyset$ is both symmetric and transitive on any set A.

To prove that a relation is not transitive or symmetric a counterexample suffices.

Example 1

For set $B = \{1,2,3,4\}$, let

$$\begin{aligned} S_1 &= \{(1,2),(2,3),(1,3)\} \\ S_2 &= \{(1,2),(2,3),(3,1)\} \\ S_3 &= \{(1,1),(1,2)\} \\ S_4 &= \{(1,2),(2,1),(1,1),(2,2),(3,3),(4,4)\} \end{aligned}$$

All S_i but S_2 are transitive. The only symmetric relation is S_4. S_4 is also the only reflexive relation.

Example 2

Let R be the subset relation on $\mathcal{P}(\mathbb{Z})$.

R is reflexive because $A \subseteq A$ for every set A.

R is also transitive because $\subseteq$ is transitive, as we have seen before.

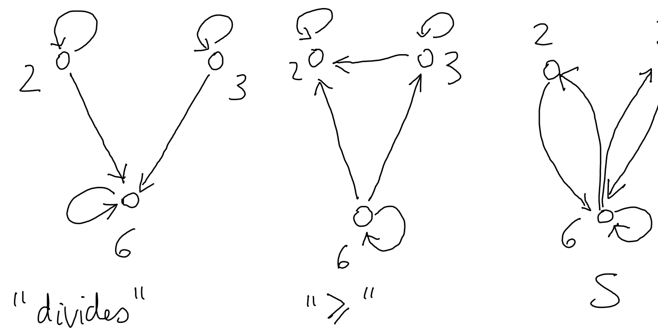
R is not symmetric because $\{1\} \subseteq \{1, 2\}$, but $\{1, 2\} \not\subseteq \{1\}$

Reflexivity, symmetry, and transitivity can be characterized by properties of digraphs:

- A relation is reflexive iff every vertex of the digraph has a loop, i.e. an edge from a vertex to itself.
- A relation is symmetric iff between any two vertices of the digraph there are either no edges or an edge in both directions.
- A relation is transitive iff whenever there is an edge from x to y and an edge from y to z, there must be an edge from x to z.

Examples

Three relations on $A = \{2, 3, 6\}$: "divides", "$\geq$", and relation S where $x\ S\ y$ iff $x + y > 7$.



"Divides" is reflexive on A because every integer divides itself. Likewise, "$\geq$" is reflexive on A. But S is not reflexive.

Only the digraph for S contains edges and their twin edges that point back. Thus, S is symmetric.

Both "divides" and "$\geq$" are transitive, but S is not, because $2\ S\ 6$ and $6\ S\ 3$, but $2 \not S\ 3$

The identity relation I_A on any set A has all three properties.

It is in fact the relation "equals", because

$$x\ I_A\ y \ \Leftrightarrow x = y$$

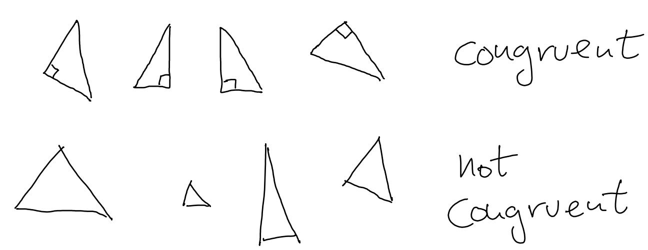
Equality is a way of comparing objects according to whether they are the same.

Equivalence relations are more general: they group objects according to whether they share a common trait.

For instance, if T is the set of all triangles, we might say two triangles are "equivalent" if they are congruent (i.e. a sequence of translations, rotations, and reflections make them identical).

This generates the relation

$$R = \{(x, y) \in T^2 \mid x \text{ congruent to } y\}$$



The notion of "equivalence" is expressed by these three properties.

Definition: A relation R on A is an **equivalence relation** iff R is reflexive on A, symmetric, and transitive.

Example

For the set P of all people, let L be the relation on P given by xLy iff x and y have the same last name.

Then L is an equivalence relation, assuming that everyone has a last name.

Luci Brown L Charlie Brown

James Madison L Dolly Madison

...

The subset of P consisting of all people who are L-related to Charlie Brown is the set of all people whose last name is Brown.

This set contains Charlie Brown, by reflexivity. It also contains Sally Brown, James Brown, and Leroy Brown and all other Browns.

This insight leads to the following:

Definition: Let R be an equivalence relation on A. For $x \in A$, the **equivalence class** of x determined by R is the set

$$x/R := \{y \in A \mid x \; R \; y\}$$

This is read **"the class of $\mathbf{x}$ modulo $\mathbf{R}$"** or "x mod R". The set of all equivalence classes is called **$\mathbf{A}$ modulo $\mathbf{R}$** and is denoted $A/R := \{x/R \mid x \in A\}$.

Example 1

The equivalence class of Charlie Brown modulo L is the set of all people whose last name is Brown. Furthermore, Buster Brown/L is the same as Charly Brown/L.

Lecture 16 Example 2

Relation $H = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ is an equivalence relation on set $A = \{1,2,3\}$.

$1/H = 2/H = \{1,2\}$ and $3/H = \{3\}$

Thus, $A/H = \{\{3\},\{1,2\}\}$

Example 3

The relation $\Box$ on $\mathbb{R}$ given by $x \Box y$ iff $x^2 = y^2$ is an equivalence relation on $\mathbb{R}$.

$2/\Box = \{-2, 2\}$ and $-\pi/\Box = \{-\pi, \pi\}$

For any $x \in \mathbb{R}$, $x/\Box = \{-x, x\}$

$\mathbb{R}/\Box = \{\{-x, x\} \mid x \in \mathbb{R}\}$

Example 4

Two integers have the same **parity** iff they are either both even or both odd. Let

$$R = \{(x,y) \in \mathbb{Z}^2 \mid x \text{ and } y \text{ have the same parity}\}$$

R is an equivalence relation on $\mathbb{Z}$ with two equivalence classes: the even integers E and the odd integers D.

If x is even, then $x/R = E$. Otherwise, $x/R = D$.

Thus, $\mathbb{Z}/R = \{E, D\}$

Equivalence Relations on Integers Based on Divisibility

For a fixed integer $m \neq 0$, let $\equiv_m$ be the relation on $\mathbb{Z}$ given by

$$x \equiv_m y \;\Leftrightarrow\; m \text{ divides } x - y$$

The expression $x \equiv_m y$ is also written as

$$x \equiv y \pmod{m}$$

and read "x is congruent to y modulo m".

For example, $4 \equiv 1 \pmod 3$, because 3 divides $4-1$, and $10 \equiv_3 16$ because 3 divides $10 - 16 = -6$.

But $5 \not\equiv_3 -9$, because 3 does not divide $5-(-9) = 14$.

It is easy to see that 0 is congruent to $0, -3, 3, -6, 6,$ and in fact every multiple of 3.

What is $\mathbb{Z}/{\equiv_3}$, which we call $\mathbb{Z}_3$?

For $x \in \mathbb{Z}$, $x/{\equiv_3} = \{y \in \mathbb{Z} \mid x \equiv_3 y\}$.

We use $\bar{x}$ to denote $x/{\equiv_3}$. Because the intergers congruent to 0 mod 3 are exactly the multiples of 3, we have

$$\bar{0} = \{3k \mid k \in \mathbb{Z}\}$$

What is $\bar{1}$?

$1, 4, 7, 10, ...$ is in the set, as well as $-2, -5, -8, ...$, i.e.

$$\bar{1} = \{3k + 1 \mid k \in \mathbb{Z}\}$$

Similarly, we obtain

$$\bar{2} = \{3k + 2 \mid k \in \mathbb{Z}\}$$

What about $\bar{3}$? It is the same as $\bar{0}$. In fact $\bar{4} = \bar{1},\ \bar{5} = \bar{2},\ \bar{6} = \bar{0}$, etc.

Thus, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

In general, it can be proved that there are always m distinct equivalence classes for the relation $\equiv_m$ and $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$.

It his helpful to note that $0, 1, 2, \ldots, m-1$ are exactly all the possible remainders when integers are divided by m. For this reason the elements of $\mathbb{Z}_m$ are sometimes called the risidue (or remainder) classes modulo m.

As an application consider how you tell time. Rather than talking about hours beyond 12 o'clock, we start over again with 1 o'clock instead of 13 o'clock (13 $\equiv_{12}$ 1).

We routinely even do modular hour arithmetic: e.g. 9 hours after 8 o'clock is 5 o'clock, because 8+9=17 and 17 $\equiv_{12}$ 5, and 4 hours before 3 o'clock is 11 o'clock, because 3-4 = -1 and -1 $\equiv_{12}$ 11.

Theorem:
The relation $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

Proof: $\equiv_m$ is a set of ordered pairs of integers. Therefore, $\equiv_m$ is a relation on $\mathbb{Z}$. We need to prove three properties:

1. $\equiv_m$ is reflexive on $\mathbb{Z}$: for all $x \in \mathbb{Z}$, $x \equiv_m x$, because $x - x = 0$ is divisible by m.
2. $\equiv_m$ is symmetric: suppose $x \equiv_m y$. Then m divides $x - y$, i.e. $\exists k \in \mathbb{Z} : x - y = km$.
   This means $y - x = -km$. Hence, $y \equiv_m x$.

3. $\equiv_m$ is transitive: suppose $x \equiv_m y$ and $y \equiv_m z$. Then m divides both $x - y$ and $y - z$, i.e.

   $$\exists k, l \in \mathbb{Z} :\ x - y = km \ \text{ and } \ y - z = lm$$

   Now,

   $$x - z = (x - y) + (y - z) = km + lm = (k + l)m$$

   This means that $x - z$ is divisible by m, i.e. $x \equiv_m z$

$\square$

Partitions

Partitioning is frequently used to organize the world around us. For example, countries are partitioned in several ways: states, postal code areas, phone area code regions, etc.

In each case non-empty subsets that do not overlap together form a set. In this section we introduce the concept of partitioning sets and show how it relates to equivalence relations.

Definition: Let A be a non-empty set, $\mathcal{A}$ is a **partition of A** iff $\mathcal{A}$ is a set of subsets of A such that:

1. If $X \in \mathcal{A}$, then $X \neq \emptyset$
2. If $X \in \mathcal{A}$ and $Y \in \mathcal{A}$ then $X = Y$ or $X \cap Y = \emptyset$
3. $\displaystyle\dot{\bigcup_{X \in \mathcal{A}}} X = A$

In part 3 we look at all elements X of $\mathcal{A}$ (which are sets) and take their union. We can use the disjoint set union operator because we know that all elements of $\mathcal{A}$ are pairwise disjoint (part 2).

Example 1

Let $A = \{1,2,3,4,5,6\}$ and $\mathcal{A} = \{\{1,2,3\},\{4,5\},\{6\}\}$

To prove that $\mathcal{A}$ is a partition of A we need to check

1. that all elements of $\mathcal{A}$ are non-empty:
   $\{1,2,3\} \neq \emptyset$
   $\{4,5\} \neq \emptyset$
   $\{6\} \neq \emptyset$ — OK
2. that all elements of $\mathcal{A}$ are pairwise disjoint:
   $\{1,2,3\} \cap \{4,5\} = \emptyset$
   $\{1,2,3\} \cap \{6\} = \emptyset$
   $\{4,5\} \cap \{6\} = \emptyset$ — OK
3. and that the union of all elements of $\mathcal{A}$ is A
   $\{1,2,3\} \cup \{4,5\} \cup \{6\} = A$ — OK

Example 2

Here are five different partitions of $\mathbb{Z}$:

1. $\{\{0\},\{-1,1\},\{-2,2\},\{-3,3\},\dots\}$
2. $\{E,D\}$ where E is the set of even integers and D is the set of odd integers
3. $\{\{x \in \mathbb{Z} \mid x < 0\},\ \{x \in \mathbb{Z} \mid x \geq 0\}\}$
4. $\{...,\{-3\},\{-2\},\{-1\},\{0\},\{1\},\{2\}...\}$
5. $\{\mathbb{Z}\}$

The last two examples are extremes in terms of number of elements in the partition.

Generally, for any non-empty set A, $\{\{x\} \mid x \in A\}$ and $\{A\}$ are partitions.

Example 3

The set $\mathbb{R}$ of real numbers may be partitioned into

$$\{\mathbb{Q}, \mathbb{R} - \mathbb{Q}\}$$

where $\mathbb{Q}$ is the set of rational numbers and $\mathbb{R} - \mathbb{Q}$ is the set of irrational numbers.

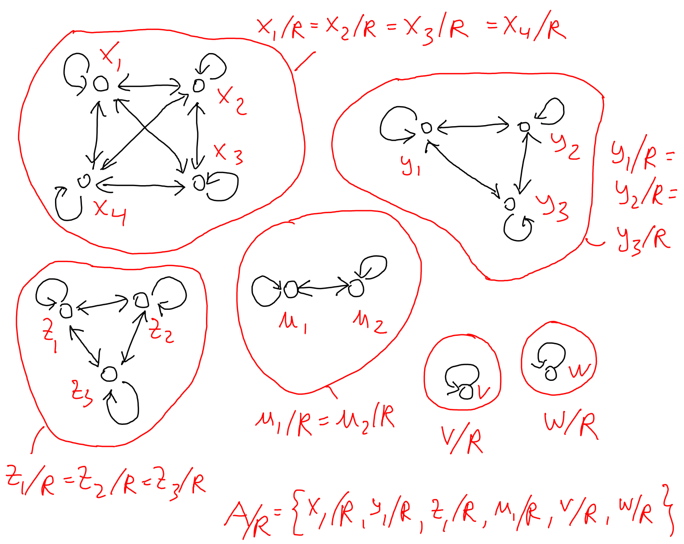
Alternatively, we can partition $\mathbb{R}$ into a set of intervals:

$$\{[k, k+1) \mid k \in \mathbb{Z}\}$$

Here, $[k, k+1)$ denotes the half-open interval from k to $k+1$ (excluding), i.e.

$$[k, k+1) = \{x \in \mathbb{R} \mid k \leq x < k+1\}$$

Looking back at the examples of equivalence classes we see that for an equivalence relation on A every equivalence class is a non-empty subset of A, equivalence classes for elements x and y are either equal or disjoint, and every element is in some equivalence class.



(The equivalence classes (red) partition A)

The following theorem formalizes this observation:

Theorem: Let R be an equivalence relation on a non-empty set A. Then

1. For all $x \in A : x/R \subseteq A$ and $x \in x/R$
   Thus, $x/R \neq \emptyset$
2. $\bigcup\limits_{x \in A} x/R = A$
3. $x\ R\ y \;\Leftrightarrow\; x/R = y/R$
4. $x \not R\ y \;\Leftrightarrow\; x/R \cap y/R = \emptyset$ $\square$

1. says that no x/R is empty.

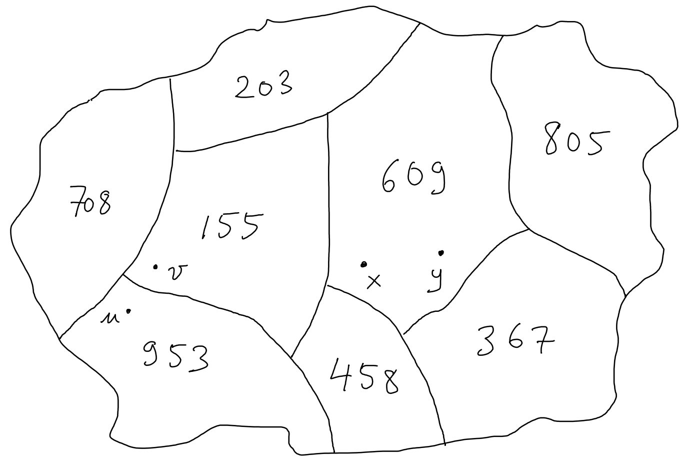
2. states that each $y \in A$ is covered by an x/R.

3.+4. imply that equivalence classes of elements of A are either identical or disjoint.

Therefore, the set $\{x/R \mid x \in A\}$ of equivalence classes is a partition of A.

Now that we know that every equivalence relation on A induces a partition of A, the remaining question is whether for every partition we can find an equivalence relation that defines it.

Consider for instance a country being partitioned according to phone area codes. Can this partition be created by an equivalence relation? Yes: define two locations are equivalent iff they share the same area code.



x and y are related, but u and v are not.

The following theorem, which we present without proof, formalizes this idea:

Lecture 17

Theorem: Let $\mathcal{B}$ be a partition of the non-empty set A. For $x, y \in A$, define xQy iff there exists $C \in \mathcal{B}$, such that $x \in C$ and $y \in C$. Then

1. Q is an equivalence relation
2. $A/Q = \mathcal{B}$ (recall: $A/Q = \{t/Q \mid t \in A\}$) $\square$

Example 1

In the area code example we just saw locations may be given by longitude – latitude pairs. For two locations u and v, $(u, v) \in Q$ iff u and v share the same area code.

Example 2

Let $A = \{1, 2, 3, 4\}$ and $\mathcal{B} = \{\{1\}, \{2, 3\}, \{4\}\}$.

The equivalence relation Q associated with $\mathcal{B}$ is

$$\{(1, 1), (2, 2), (3, 3), (4, 4), (2, 3), (3, 2)\}$$

The three equivalence classes are

$1/Q = \{1\}$

$2/Q = 3/Q = \{2, 3\}$

$4/Q = \{4\}$

and the set of all equivalence classes is exactly $\mathcal{B}$.

Example 3

The set $\mathcal{A} = \{A_0, A_1, A_2, A_3, A_4\}$ is a partition of $\mathbb{Z}$, where

$A_0 = \{5k + 0 \mid k \in \mathbb{Z}\}$

$A_1 = \{5k + 1 \mid k \in \mathbb{Z}\}$

$A_2 = \{5k + 2 \mid k \in \mathbb{Z}\}$

$A_3 = \{5k + 3 \mid k \in \mathbb{Z}\}$

$A_4 = \{5k + 4 \mid k \in \mathbb{Z}\}$

Then integers x and y are in the same set A_i iff $x = 5n + i$ and $y = 5m + i$ for some integers n, m.

This is equivalent to $x - y$ being a multiple of 5.

Thus, the equivalence relation induced by $\mathcal{A}$ is $\equiv_5$.

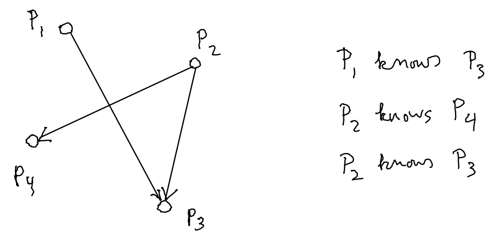
Graph Introduction

This section introduces the concept of graphs which are among the most ubiquitous models used in science.

Graphs model binary relations $R \subseteq V \times V$

- Objects are represented by vertices
- Related objects are connected by edges

Example: Relation R with



Relations are not necessarily symmetric:

$$(x, y) \in R \not\Rightarrow (y, x) \in R$$

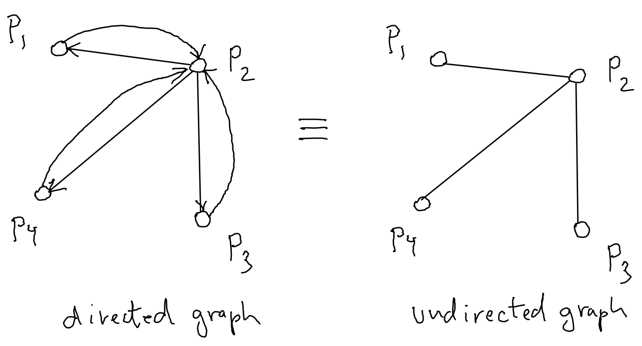
Therefore we need directed edges ("arcs")

For symmetric relations undirected edges suffice

Example:

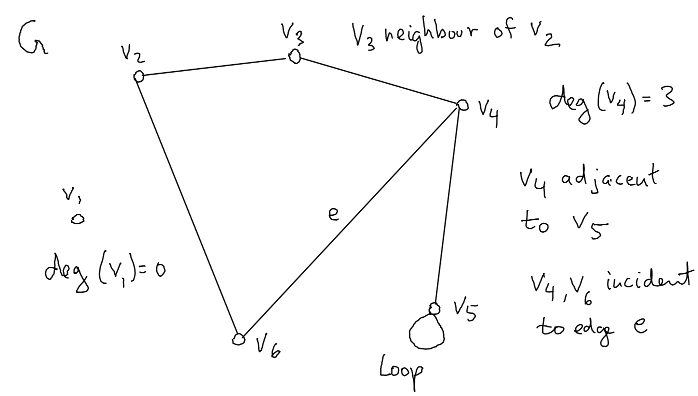
$$(x, y) \in F \;\Leftrightarrow\; x \text{ is a friend of } y$$

Then (usually) $(x, y) \in F \Leftrightarrow (y, x) \in F$



Definition:

An **(undirected) graph** is a pair $G = (V, E)$ that is composed of a non-empty vertex (or node) set V and an edge set E, so that for each edge $e \in E$, $1 \leq |e| \leq 2$, i.e. each edge contains one or two vertices.



$G = (V, E) \quad V = \{v_1 \ldots v_6\}$

$E = \{\ \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5\}, \{v_4, v_6\}, \{v_2, v_6\}\ \}$

The order of G is 6 (number of nodes), and so is its size (number of edges)

The **order** of $G = (V, E)$ is $|V|$.

The **size** of $G = (V, E)$ is $|E|$.

We say that edge $e = \{u, v\}$ **connects** node u with node v. In case $e = \{u\}$, vertex u is connected to itself and forms a **loop**.

A graph is called **simple** if it does not contain loops.

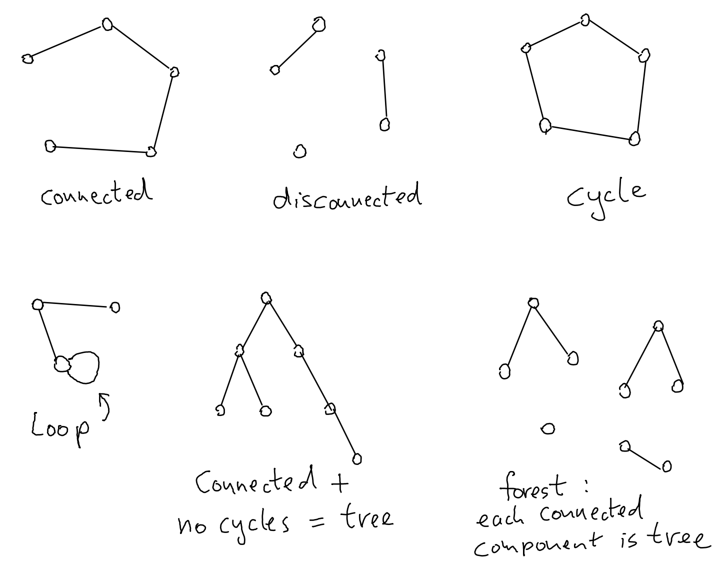
A vertex u is called a **neighbour** of vertex v iff $\{u, v\} \in E$.

The number of neighbours of a vertex u is called its **degree**, denoted deg(u). A loop contributes twice to the degree.

$u, v \in V$ are **adjacent** iff $\{u, v\} \in E$

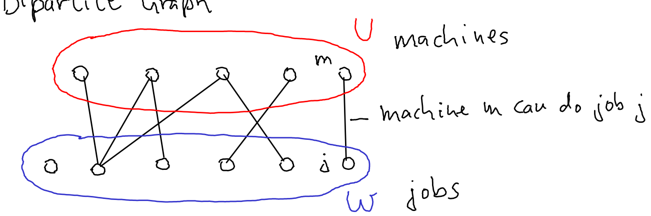
$u, v \in V$ are **incident** to edge $e \in E$ iff $e = \{u, v\}$

Some Fundamental Graph Classes and Properties



Will formally define these in a moment.

Bipartite Graph



$V = U \cup W$ and $U \cap W = \emptyset$ (node partition)

All edges of form $e = \{u, w\}$ with $u \in U$ and $w \in W$

Definition:

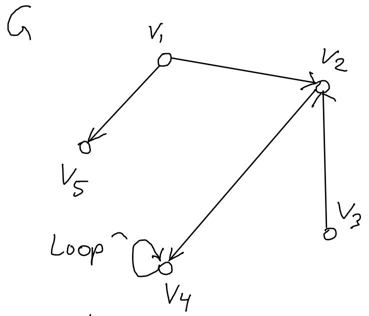
A **directed graph** is a pair $G = (V, E)$ that is composed of a non-empty vertex set V and an edge set $E \subseteq V \times V$.

Edge $e = (u, v)$ connects vertex u with vertex v (u is said to be adjacent to v, and v is adjacent from u). u is called the **initial vertex** of e, and v is called the **terminal vertex** of e.

The **in-degree** of a vertex v, denoted deg$^-(v)$, is the number of edges with v as their terminal vertex.

The **out-degree** of a vertex v, denoted deg$^+(v)$, is the number of edges with v as their initial vertex.

Loops contribute 1 to both the in- and out-degree.



$deg^+(v_2) = 1$

$deg^-(v_2) = 2$

v_2 adjacent to v_4

v_4 adjacent from v_2

$deg^+(v_4) = 1$

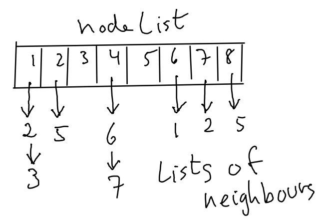
$deg^-(v_4) = 2$

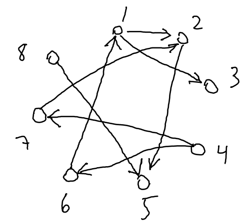
$G = (V, E), \ V = \{v_1 \dots v_6\}$

$E = \{(v_1, v_2), (v_1, v_5), (v_2, v_4), (v_3, v_2), (v_4, v_4)\}$

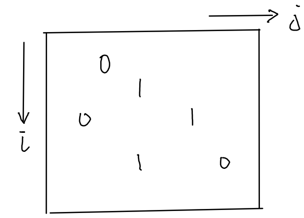
Graph Data Structures

Adjacency Lists





Adjacency Matrix



$V = \{v_1, \dots, v_m\}$

Boolean $m \times m$ matrix A

$A[i,j] = 1 \iff (v_i, v_j) \in E$

Adjacency lists are smaller if G is **sparse** ($|E|$ much smaller than $|V|^2$). If G is **dense** ($|E|$ quadratic in $|V|$), adjacency matrices save space and allow direct access to edge information.

Which representation is better depends on algorithm used

Connectivity

Lecture 18

Problems of efficiently planning routes for mail delivery, garbage pickup, diagnostics in computer networks, etc. can be solved using models that involve paths in graphs.

Informally, a path is a sequence of edges that begins at a vertex of a graph and travels from vertex to vertex along edges of the graph.

Definition

Let $n \in \mathbb{N} - \{0\}$ and $G = (V, E)$ a graph. A **path** of length n from u to v in G is a sequence of n edges

$$(e_1, e_2, \dots, e_n)$$

– written as $(e_i)_{i=1}^n$ – such that $e_i = \{x_{i-1}, x_i\} \in E$ for all i, with $u = x_0$ and $x_n = v$.

In case of directed graphs, $e_i = (x_{i-1}, x_i) \in E$.

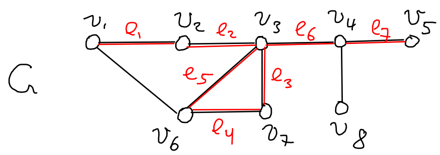
Sometimes it is convenient to define a path just by the sequence of visited vertices, which implies the edges:

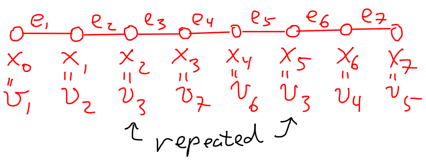
$$(x_0, x_1, \dots x_n)$$

A path is a **cycle** (or circuit) iff $x_0 = x_n$ and $n > 0$.

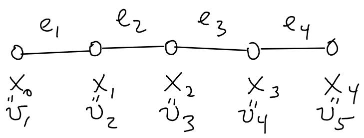
A path or cycle is **simple** iff it does not contain the same node more than once (except for the necessary repetition of the start and end vertex in the case of cycles).

Examples



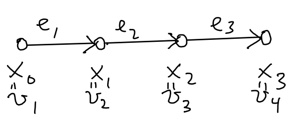


Path from v_1 to v_5

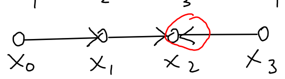


Simple path from v_1 to v_5

Directed path examples:



Simple directed path



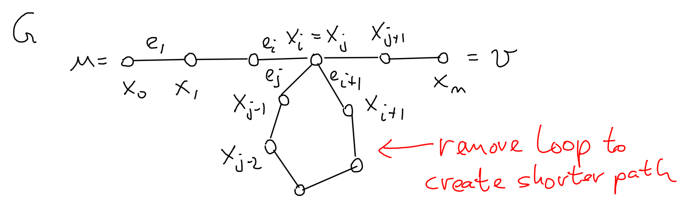
Not a directed path!

A graph is called **connected** iff there is a path between every pair of distinct vertices of the graph.

Theorem
There is a simple path between every pair of distinct vertices of a connected graph.

Proof
Let $G = (V, E)$ be a connected graph and $u, v \in V$. Then there exists a path $P_0 = (e_i)_{i=1}^n$ that connects u to v, with $e_i = \{x_{i-1}, x_i\} \in E$ for all i, with $u = x_0$ and $x_n = v$.

If no vertex is repeated, then P_0 is a simple path and we are done. Otherwise, let i, j be distinct integers with $i < j$ and $x_i = x_j$, i.e. vertex x_i is repeated.



If we delete the edges $e_{i+1}, \ldots, e_j$ from P_0 we obtain

a shorter path P_1 from u to v and has fewer repeated nodes. If P_1 is a path we are done. Otherwise, we repeat the process.

Since P_0 is a finite sequence and we decrease its length in every step, eventually we must reach stage k where no vertices are repeated and the resulting path P_k is simple. □

Given a graph $G = (V, E)$, being reachable defines a relation C on V:

$(u, v) \in C \Leftrightarrow u = v$ or there is a path from u to v in G

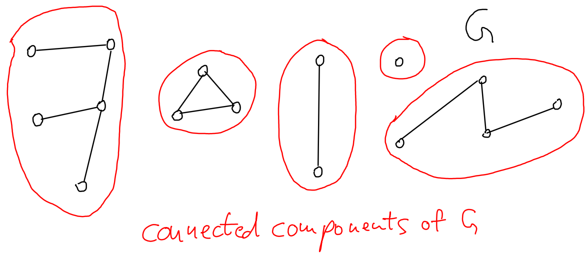
Then, C is

- reflexive: $\forall v \in V : (v, v) \in C$
- symmetric: $\forall u, v \in V : (u, v) \in C \Rightarrow (v, u) \in C$
- and transitive $\forall x, y, z \in V :$
$$[(x, y) \in C \wedge (y, z) \in C] \Rightarrow (x, z) \in C$$

(Why?)

This means that C is an equivalence relation, and as such the set of all element equivalence classes forms a partition of V.

Each such equivalence class v/C together with the set of edges that are incident to those vertices is called **connected component**.



Observations:

Connected components of graph G are connected subgraphs of G that contain vertices and all incident edges of G, such that no other vertex can be added to create larger connected subgraphs.

[Graph $H = (W, F)$ is a **subgraph** of $G = (V, E)$ iff $W \subseteq V$ and $F \subseteq E$]

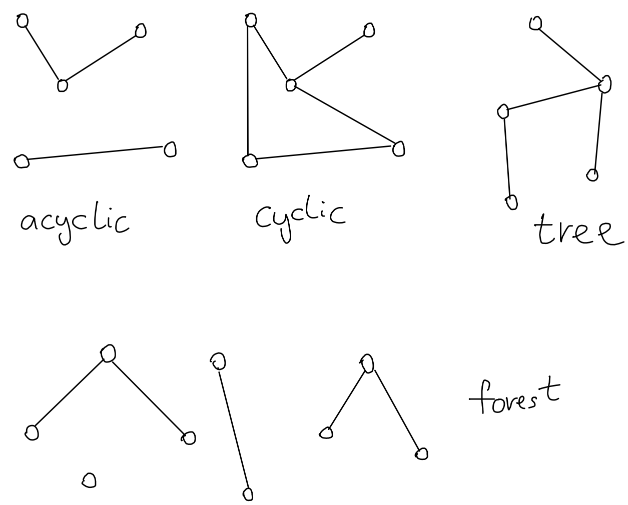
A graph is connected iff it has one connected component.

Definition

A graph is called **acyclic** iff it does not contain a cycle.

A connected acyclic graph is called a **tree**.

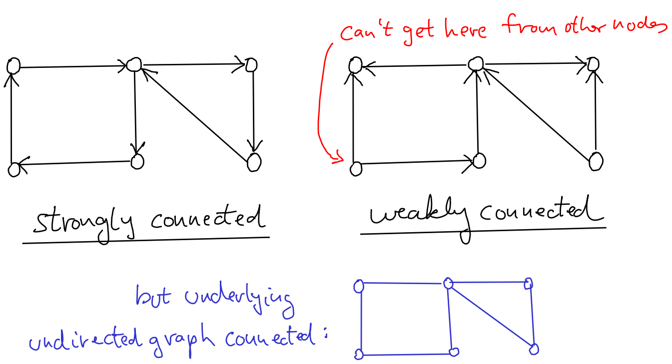
An acyclic graph is also called **forest**.



Connectivity in Directed Graphs

There are two notions of connectedness in directed graphs, depending on whether the directions of the edges are considered.

Definition
A directed graph (V, E) is **strongly connected** iff for all distinct vertices $u, v \in V$ there is a path from u to v and from v to u.



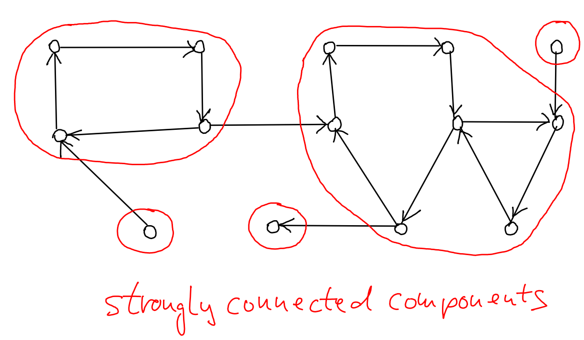
A directed graph is **weakly connected** iff the underlying undirected graph, that is constructed by turning every directed edge into an undirected edge, is connected.

Similar to the reachability relation on graphs, the reachability relation C on digraphs given by

$$(u, v) \in C \Leftrightarrow$$

$u = v$ or there is a path from u to v and from v to u

is an equivalence relation and therefore induces a vertex partition. The subgraphs induced by the equivalence classes are called **strongly connected components** (SCCs).

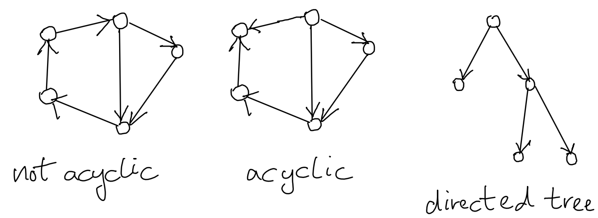


In each SCC, every node can be reached from any other by a directed path, and like connected components in graphs, they can't be enlarged by adding a node.

Definition

A directed graph is **acyclic** iff it does not contain a directed cycle.

A directed graph is a **directed tree** iff it would be a tree if all directed edges are turned into undirected edges and in-degree $\deg^{-}(v) \leq 1$ for all vertices.

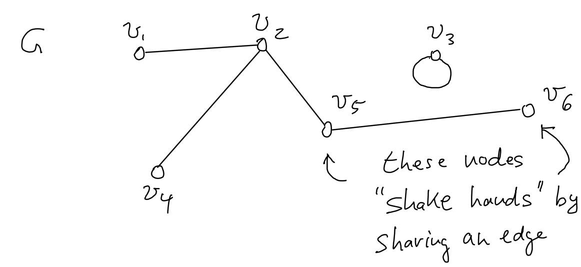


Some Fundamental Graph Properties

The Handshake Lemma (Euler 1736):
Let $G = (V, E)$ be a graph with $V = \{v_1, \ldots, v_n\}$. Then

$$\sum_{i=1}^{n} \mathsf{deg}(v_i) = 2|E|$$

Example



$$\sum_{i=1}^{n} \mathsf{deg}(v_i) = 1 + 3 + 2 + 1 + 2 + 1 = 10$$

$$|E| = 5$$

Corollary: Any graph contains an even number of vertices of odd degree.

Proof: Suppose the number of vertices of odd degree is odd – say l. Then – assuming the first l nodes have odd degree:

$$\sum_{i=1}^{n} \mathsf{deg}(v_i) = \underbrace{\sum_{i=1}^{l} (2 \cdot a_i + 1)}_{\text{odd degrees}} + \underbrace{\sum_{i=l+1}^{n} 2 \cdot a_i}_{\text{even degrees}}$$

for some integers a_i. This means

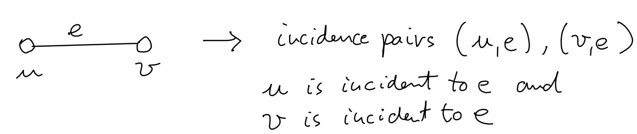
$$\sum_{i=1}^{n} \mathsf{deg}(v_i) = l + 2 \sum_{i=1}^{n} a_i$$

which is an odd number. This contradicts the Handshake Lemma. $\square$

Proof of the Handshake Lemma:

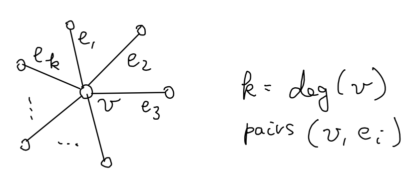
We first prove the result for simple (loop-free) graphs:

We count the number I of incidence pairs (v, e) (also called "half-handshakes"), where $v \in V, e \in E$, and $e = \{v, u\}$ for some $u \in V$ (i.e. v is incident to e), in two ways.



Because each edge has two incident vertices we know $I = 2|E|$.

Incidence pairs for a fixed node v:



On the other hand, node v belongs to $\mathsf{deg}(v)$ incidence pairs: namely all (v, e) for which $e = \{v, u\} \in E$ for some $u \in V$.

Therefore, $I = \sum_{i=1}^{n} \deg(v_i)$, and

$$\sum_{i=1}^{n} \deg(v_i) = 2|E|$$

holds for simple graphs.

If we now add an arbitrary number l of loop edges to a simple graph, the equation still holds because each loop adds 2 to the vertex degree, i.e. both sides are increased by $2l$. $\square$

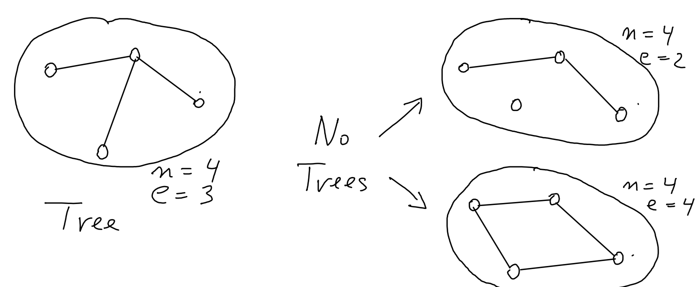
Characterizations of Trees

Trees are everywhere – not just around us. When talking about graphs, trees have many uses in science. For instance, they can describe hierarchical object relationships and are at the core of many efficient data structures (e.g. heaps).

Here we will present and prove a series of tree characterizations which are useful for proving properties of tree-based algorithms. Moreover, the proofs we will see make use of various proof techniques we have seen earlier.

Theorem: Let G be a simple graph with n nodes and e edges. Then the following statements are equivalent:

1. G is a tree (connected and acyclic).
2. Every two distinct nodes of G are joined by a unique path.
3. G is connected and $n = e + 1$.
4. G is acyclic and $n = e + 1$.
5. G is acyclic and if any two non-adjacent nodes are joined by an edge, the resulting graph has exactly one simple cycle.



✓ 1. acyclic + connected ✗

✓ 2. unique paths for all pairs ✗

✓ 3. connected + n = e + 1 ✗

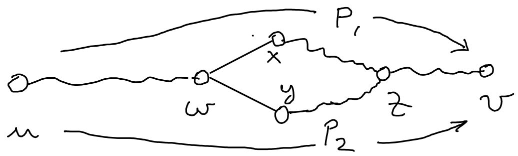
✓ 4. acyclic + n = e + 1 ✗

✓ 5. acyclic + adding edge creates single simple cycle ✗

Lecture 19

Proof:
We show $1. \Rightarrow 2. \Rightarrow 3. \Rightarrow 4. \Rightarrow 5. \Rightarrow 1.$, which establishes the equivalence of each pair of properties.

$\underline{1 \Rightarrow 2}$:
If G is a tree (i.e. acyclic and connected) then every two distinct nodes are joined by a unique path.



Suppose that there are two paths P_1 and P_2 from node u to node v. Tracing the two paths simultaneously from u to v, let w be the first point that is on both paths, but for which the successor nodes x and y are on different paths.

Also, let z be the next node after w that is on both paths. Note that such vertex exists, because the paths share vertex v.

Then the paths from w to z along P_1 and from z to w along P_2 reversed together create a cycle. But this can't happen if G is acyclic. This is a contradiction to the premise, and therefore every node pair is connected by a unique path. $\square$

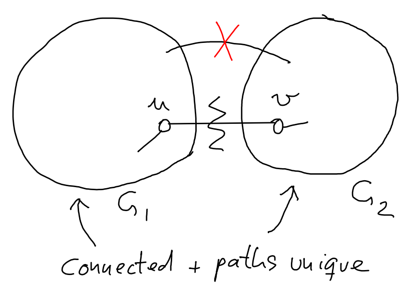
$\underline{2 \Rightarrow 3}$:
If every two nodes of G are joined by a unique path, then G is connected and $n = e + 1$.

G is connected because any two nodes are joined by a path.

To show $n = e + 1$, we use induction.

The statement is true for $n = 1$ because there can't be any edges in G which is assumed to be simple.

Now assume it's true for $< n$ nodes. Removing any edge from G breaks G into two connected components G_1 and G_2, because paths are unique.



Suppose their orders are n_1 and n_2, respectively, with

$$n_1 + n_2 = n$$

By the induction hypothesis, which applies to G_1, G_2:

$$n_1 = e_1 + 1 \text{ and } n_2 = e_2 + 1$$

But then

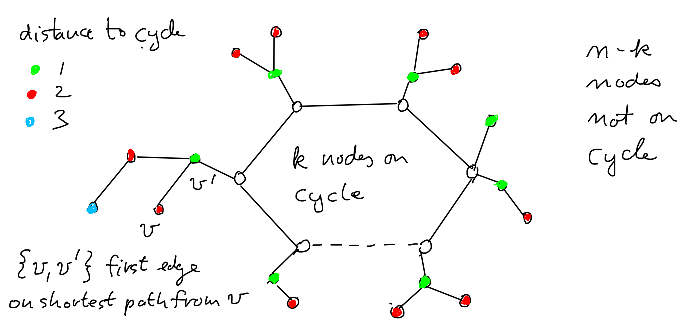
$$\begin{aligned} n &= n_1 + n_2 \\ &= (e_1 + 1) + (e_2 + 1) \\ &= (e_1 + e_2) + 2 \\ &= (e - 1) + 2 \\ &= e + 1 \end{aligned}$$

$\square$

$\underline{3 \Rightarrow 4}$:
If G is connected and $n = e + 1$, then G is acyclic.

Suppose G has a simple cycle of length k. Then there are k nodes and k edges on this cycle.

Since G is connected, for each node v not on the cycle, there is a shortest path from v to a node on the cycle.



On these shortest paths, the first edge $\{v, v'\}$ is not contained in shorter shortest paths from any other node outside the cycle.

If it were, then the current path from v to the cycle would not be the shortest possible.

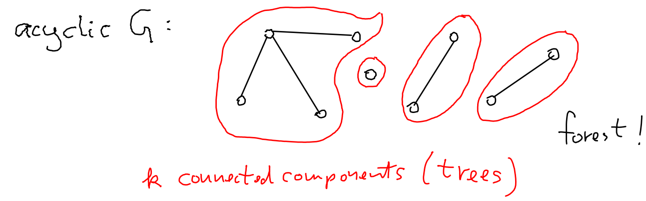
Thus, we see by sorting the $n-k$ non-cycle nodes by increasing distance to the cycle, that for any such node there is at least one edge in G.

Therefore, $e \geq (n-k)+k = n$, which contradicts the assumption $n = e+1$, i.e. $e = n-1$.

So, G can't have any cycles. $\square$

<u>$4 \Rightarrow 5$:</u>
If G is acyclic and $n = e+1$, then if any two non-adjacent nodes are joined by an edge, the resulting graph has exactly one simple cycle.

Since G doesn't have cycles, each connected component of G is a tree. Suppose there are k components of order n_i and size e_i, respectively.



Then, by $(1. \Rightarrow 3.)$, $n_i = e_i + 1$, and therefore $n = e + k$.

It follows that $k = 1$, so G is in fact connected, and therefore a tree.

By $(1. \Rightarrow 2.)$, for any pair of non-adjacent nodes u and v, there is a unique path between them. Adding edge $\{u, v\}$ thus results in exactly one simple cycle. $\square$

<u>$5 \Rightarrow 1$:</u>
If G is acyclic joining any non-adjacent points results in a single simple cycle, then G is a tree.

Since joining any pair of non-adjacent nodes gives a cycle, the points must be connected by a path. Thus G is connected and acyclic, and therefore a tree. $\square$