Terence Sim

# Interesting Theorem

All positive integers are interesting.

### Proof:

- 1. Suppose not.
- 2. Then by the Well Ordering Principle, there exists a smallest positive integer that is non-interesting.
- 3. But, hey, that's pretty interesting!
- 4. Contradiction.
- 5. Therefore all positive integers are interesting.



## Reading

Chapter 8.1 — 8.5 of Epp.

### Definition 8.2.7

Basics

Let  $S_i$ , for i=1 to n, be n sets. An n-ary relation on the sets  $S_i$ , denoted  $\mathcal{R}$ , is a subset of the Cartesian product  $\prod_{i=1}^n S_i$ . We call n the arity or degree of the relation.

This is the generalization of the binary relation. It forms the mathematical basis for Relational Calculus and Relational Databases, such as mySQL and SQL Server, commonly used in web applications.

For CS1231, we will focus on binary relations.

# Definition 8.2.8

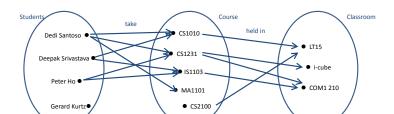
Let S, T and U be sets. Let  $\mathcal{R} \subseteq S \times T$  be a relation. Let  $\mathcal{R}' \subseteq T \times U$  be a relation. The composition of  $\mathcal{R}$  with  $\mathcal{R}'$ , denoted  $\mathcal{R}' \circ \mathcal{R}$ , is the relation from S to U such that:

$$\forall x \in S, \ \forall z \in U \ (x \ \mathcal{R}' \circ \mathcal{R} \ z \leftrightarrow (\exists y \in T \ (x \ \mathcal{R} \ y \land y \ \mathcal{R}' \ z))).$$

In other words,  $x \in S$  and  $z \in U$  are related iff there is a "path" from x to z via some intermediate element  $y \in T$ .

**Basics** 

0000



Dedi Santoso Dedi Santoso Ultis

Deepak Srivastava

Peter Ho

Gerard Kurtz

Gerard Kurtz

# Proposition 8.2.9 (Composition is Associative)

Let S, T, U, V be sets. Let  $\mathcal{R} \subseteq S \times T$  be a relation. Let  $\mathcal{R}' \subseteq T \times U$  be a relation. Let  $\mathcal{R}'' \subseteq U \times V$  be a relation.

$$\mathcal{R}''\circ(\mathcal{R}'\circ\mathcal{R})=(\mathcal{R}''\circ\mathcal{R}')\circ\mathcal{R}=\mathcal{R}''\circ\mathcal{R}'\circ\mathcal{R}.$$

### Proposition 8.2.10

Let S, T and U be sets. Let  $\mathcal{R} \subseteq S \times T$  be a relation. Let  $\mathcal{R}' \subseteq T \times U$  be a relation.

$$(\mathcal{R}' \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{R}'^{-1}$$

Proofs omitted.

# 8.3. Properties of Relations on a Set

Let A be a set, and  $\mathcal{R} \subseteq A \times A$  be a relation. We say that  $\mathcal{R}$  is a relation on A.

### Definition 8.3.1

 $\mathcal{R}$  is said to be reflexive iff  $\forall x \in A \ (x \ \mathcal{R} \ x)$ .

### Definition 8.3.2

 $\mathcal{R}$  is said to be symmetric iff  $\forall x, y \in A \ (x \mathcal{R} \ y \to y \mathcal{R} \ x)$ .

### Definition 8.3.3

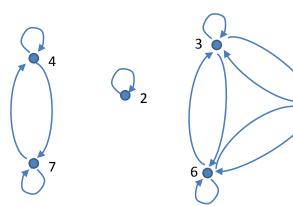
 $\mathcal{R}$  is said to be transitive iff

 $\forall x, y, z \in A ((x \mathcal{R} y \land y \mathcal{R} z) \rightarrow x \mathcal{R} z).$ 

# Example

Let  $A = \{2, 3, 4, 6, 7, 9\}$  and define a relation  $\mathcal{R}$  on A by:

$$\forall x, y \in A \ (x \mathcal{R} \ y \leftrightarrow (x - y) \text{ is divisible by 3}).$$

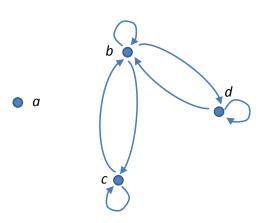


# Drawing it out

- Denote each element by a dot.
- Draw an arrow from x to y whenever  $x \mathcal{R} y$ .

- Reflexive means that all dots must have a self-loop.
- Symmetric means that every outgoing arrow to a dot must have an incoming arrow from that same dot.
- Transitive means that if an arrow goes from one dot to a second dot, and another arrow goes from the second to a third, then there must be an arrow going from the first to the third dot.

Is this relation reflexive? symmetric? transitive?



### Definition 8.3.4

Let  $\mathcal{R}$  be a relation on a set A.

 ${\cal R}$  is called an equivalence relation iff  ${\cal R}$  is reflexive, symmetric, and transitive.

The example on slide 8 was an equivalence relation.

Please verify that it is reflexive, symmetric and transitive.

Let  $\mathcal{R}$  be an equivalence relation on a set A.

### Definition 8.3.5

Let  $x \in A$ . The equivalence class of x, denoted [x], is the set of all elements  $y \in A$  that are in relation with x.

$$[x] = \{ y \in A \mid x \mathcal{R} y \}$$

### For the example on slide 8,

- The equivalence class of 2 is:  $[2] = \{2\}$ .
- The equivalence class of 4 is:  $[4] = [7] = \{4, 7\}.$
- The set of distinct equivalence classes is:

$$\{ [2], [3], [4] \} = \{ \{2\}, \{3, 6, 9\}, \{4, 7\} \}$$

# Example: Congruence modulo n

Given a positive integer n, define a binary relation  $\mathcal R$  on the set of integers  $\mathbb Z$  as follows:

$$\forall x, y \in \mathbb{Z} (x \mathcal{R} y \leftrightarrow n \mid (x - y))$$

This relation is called *congruence modulo n*.

It is easy to prove that R is an equivalence relation.

### Proof

- 1. Reflexive: Clearly,  $\forall x \in \mathbb{Z}$ ,  $n \mid (x x)$ . Thus  $x \in \mathbb{R}$  x.
- 2. Symmetric: Again, it is obvious that  $\forall x, y \in \mathbb{Z}$ , if  $n \mid (x - y)$  then  $n \mid (y - x)$ . Thus  $x \mathcal{R} y \to y \mathcal{R} x$ .
- 3. Transitive: Given any  $x, y, z \in \mathbb{Z}$ , if  $n \mid (x y) \land n \mid (y z)$ , then  $\exists k_1, k_2 \in \mathbb{Z}$  such that  $x - y = k_1 n$  and  $y - z = k_2 n$ .
- 4. Thus  $(x y) + (y z) = k_1 n + k_2 n$ , which simplifies to  $x-z=(k_1+k_2)n$ . This means  $n\mid (x-z)$  since  $k_1+k_2$  is an integer. Thus  $x \mathcal{R} z$  whenever  $x \mathcal{R} y \wedge y \mathcal{R} z$ .
- 5. Hence,  $\mathcal{R}$  is an equivalence relation.

# Equivalence classes of congruence modulo n

Since  $n \mid (x - y) \rightarrow \exists k \in \mathbb{Z}, x - y = kn$ , we may re-write:

$$x = kn + y$$

Let's write y = qn + r, where q is the quotient, and r is the remainder when y is divided by n. Note that  $0 \le r < n$ .

Thus, 
$$x = kn + qn + r$$
  
=  $(k + q)n + r$ 

This shows that x and y have the same remainder r. The distinct equivalence classes are those formed by all the possible values of r:

$$\{ [0], [1], [2], \ldots, [n-1] \}$$

Let  $\mathcal{R}$  be an equivalence relation on a set A. Then the set of distinct equivalence classes form a partition of A.

### **Proof Sketch**

Our proof will require three steps:

- 1. Two elements that are related are in the same equivalence class.
- 2. Two equivalence classes are either disjoint, or they are equal.
- 3. The union of all equivalence classes is A.

Let  $\mathcal{R}$  be an equivalence relation on a set A, and let a, b be two elements in A. If  $a \mathcal{R} b$  then [a] = [b].

Proof: see page 468 of Epp.

# Lemma 8.3.3 (Epp)

If  $\mathcal{R}$  is an equivalence relation on a set A, and a, b are elements in A, then either  $[a] \cap [b] = \emptyset$  or [a] = [b].

### **Proof Sketch**

The statement to be proven has the form:

if 
$$p$$
 then  $(q \lor r)$ .

We will prove the logically equivalent statement (why?):

if 
$$p \wedge (\sim q)$$
 then  $r$ .

That is, we will prove:

If  $\mathcal{R}$  is an equivalence relation on a set A, and a, b are elements in A, and  $[a] \cap [b] \neq \emptyset$ , then [a] = [b].

- 1. Given any set A and an equivalence relation  $\mathcal{R}$  on A:
- 2. If  $[a] \cap [b] \neq \emptyset$ :
- $\exists x \ (x \in [a] \cap [b])$ , since the intersection is not empty. 3.
- $\exists x \ (x \in [a] \land x \in [b])$  by definition of intersection. 4.
- 5. So  $a \mathcal{R} \times \wedge b \mathcal{R} \times$ , by def. of equiv. class.
- 6. Now,  $\times \mathcal{R}$  b, because  $\mathcal{R}$  is symmetric.
- 7. So a  $\mathcal{R}$  b, by Lines 5, 6 and because  $\mathcal{R}$  is transitive.
- Hence [a] = [b], by Lemma 8.3.2 (Epp). 8.

Let E denote the set of distinct equivalence classes of A given binary relation  $\mathcal R$  on A.

(We need to prove that  $A = \bigcup E$ .)

- 1. For any element x in A:
- 2. Clearly,  $x \mathcal{R} x$ , because  $\mathcal{R}$  is reflexive.
- 3. Then  $x \in [x]$ , by definition of equiv. class.
- 4. Thus  $[x] \in E$ , by definition of E.
- 5. Thus  $x \in \bigcup E$ , by definition of union.
- 6. So  $A \subseteq \bigcup E$ , by definition of subset.

. . .

- 7. For any element x in  $\bigcup E$ :
- 8.  $\exists S \in E \ (x \in S)$ , by definition of union.
- 9. (That is, x must belong to one of the sets being unioned.)
- 10. Thus  $\exists y \in A \ (S = [y])$ , by def. of equiv. class.
- 11. But  $[y] \subseteq A$ , because an equiv. class is a subset of A.
- 12. So  $x \in [y] \rightarrow x \in A$ .
- 13. Thus  $\bigcup E \subseteq A$ , by definition of subset.
- 14. Hence  $A = \bigcup E$ .

. . .

### Proof cont'd

(We need to prove that distinct equiv. classes are mutually disjoint.)

- 15. Take any two distinct equivalence classes, [u], [v].
- 16. Then  $\exists u, v \in A \ (u \in [u] \land v \in [v])$ , by def. of equiv. class.
- 17. Hence either  $[u] \cap [v] = \emptyset$  or [u] = [v], by Lemma 8.3.3 (Epp).
- 18. Since  $[u] \neq [v]$  (they are distinct), we conclude that  $[u] \cap [v] = \varnothing$ .

# Theorem 8.3.1 (Epp) Equivalence relation induced by a partition

Given a partition  $S_1, S_2, \ldots$  of a set A, there exists an equivalence relation  $\mathcal{R}$  on A whose equivalence classes make up precisely that partition.

### **Proof Sketch**

Proof by Construction: we create the relation that satisfies the necessary property, and then show that it is an equivalennce relation.

Define  $\mathcal{R}$  as:

 $\forall x, y \in A \ (x \ \mathcal{R} \ y \leftrightarrow \text{there is a set } S_i \text{ in the partition}$ such that  $x \in S_i \land y \in S_i$ ).

. . .

### Proof Sketch cont'd

Then  $\mathcal{R}$  is an equivalence relation. Furthermore, the set of distinct equivalence classes  $= \{S_1, S_2, \ldots\}$ .

It is straightforward to show that  $\mathcal{R}$  is reflexive, symmetric and transitive, i.e. it is indeed an equivalence relation. Moreover, each  $S_i$  is indeed an equivalence class of those elements it contains.

For the detailed proof, see pages 461 and 462 of Epp.

Taken together, Theorems 8.3.1 (Epp) and 8.3.4 (Epp) say that every time you see an equivalence relation on a set, that set is partitioned (by the equivalence classes), and every time you see a partition of a set, an equivalence relation is implied.

Real-life examples of partitions (and therefore equivalence relations) are not hard to find. Examples:

- NUS has 16 Faculties (some are called Schools), e.g. SOC, FoE, FASS, SDE, that partition all its students.
- When buying a laptop, the salesperson may ask you to choose from: notebook, ultrabook, business model, gaming machine, high performance laptop.
- Human languages may be categorized (partitioned) into families: e.g. Indo-European, Sino-Tibetan, Niger-Congo.

### Definition 8.5.1

Let A be a set. Let  $\mathcal{R}$  be a relation on A. The transitive closure of  $\mathcal{R}$ , denoted  $\mathcal{R}^t$ , is a relation that satisfies these three properties:

- (1)  $\mathcal{R}^t$  is transitive.
- (2)  $\mathcal{R} \subseteq \mathcal{R}^t$ .
- (3) If S is any other transitive relation such that  $R \subseteq S$ , then  $R^t \subset S$ .

- Thus we can say that the transitive closure is the smallest superset that is transitive, where "smallest" is in the subset sense as defined above.
- Similar definitions can be made for reflexive closure and symmetric closure of a relation.

# Repeated compositions

Let  $\mathcal R$  be a relation on a set A. We adopt the following notation for the composition of  $\mathcal R$  with itself.

- We define  $\mathcal{R}^1 \triangleq \mathcal{R}$ .
- We define  $\mathcal{R}^2 \triangleq \mathcal{R} \circ \mathcal{R}$ .
- We define  $\mathcal{R}^n \triangleq \underbrace{\mathcal{R} \circ ... \circ \mathcal{R}}_{n} = \bigodot_{i=1 \ to \ n} \mathcal{R}$ .

# Proposition 8.5.2

Let R be a relation on a set A. Then,

$$\mathcal{R}^t = \bigcup_{i=1}^{\infty} \mathcal{R}^i$$

Proof omitted.

Let  $\mathcal{R}$  be a relation on a set A.

### Definition 8.6.1

 $\mathcal{R}$  is said to be anti-symmetric iff

$$\forall x \in A, \ \forall y \in A \ ((x \ \mathcal{R} \ y \land y \ \mathcal{R} \ x) \rightarrow x = y).$$

### Definition 8.6.2

 $\mathcal{R}$  is said to be a partial order iff it is reflexive, anti-symmetric, and transitive.

We usually denote a partial order by the symbol " $\leq$ ". A set A is called a partially ordered set (or poset) with respect to a relation  $\leq$  iff  $\leq$  is a partial order relation on A.

### Example 1

The subset relation " $\subseteq$ " between two sets is a partial order.

### **Proof Sketch**

- 1. For any set S, clearly  $S \subseteq S$ , so it is reflexive.
- 2. For any sets S, T, if  $S \subseteq T$  and  $T \subseteq S$ , then S = T by Proposition 6.3.3. But this is exactly what it means to be anti-symmetric.
- 3. For any sets S, T, U, it is easy to show that  $(S \subseteq T \land T \subseteq U) \rightarrow S \subseteq U$ . Thus " $\subseteq$ " is transitive.
- 4. Hence "⊆" is a partial order.

Consider the usual "less than or equal to" relation,  $\leq$ , on the set of real numbers,  $\mathbb{R}$ . Its usual definition is:

$$\forall x, y \in \mathbb{R}, \ (x \le y \leftrightarrow x < y \text{ or } x = y)$$

Show that " $\leq$ " is a partial order.

Proof omitted. You try!

# Example 3

The English dictionary lists words in a certain order, called the lexicographic order. Examples:

- "chicken" appears before "dog"
- "runner" appears after "run" but before "runway"

This lexicographic order is really a partial order on the set of strings defined over the English alphabet.

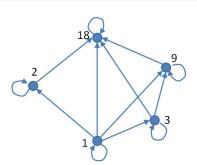
Of course, the lexicographic order owes its property to another partial order, i.e. the one that defines the order of letters in the alphabet.

# Hasse Diagrams

Let  $A = \{1, 2, 3, 9, 18\}$ , and consider the "divides" relation on A:

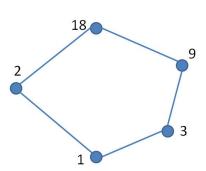
$$\forall a, b \in A, (a \mid b \leftrightarrow \exists k \in \mathbb{Z} (b = ka))$$

The "|" relation can be shown to be a partial order. (You try.) Its diagram is:



- Draw the directed graph so that all arrows point upwards.
- 2. Eliminate all self-loops.
- Eliminate all arrows implied by the transitive property.
- 4. Remove the direction of the arrows.

This is called a Hasse diagram.



Let  $\leq$  be a partial order on a set A. Elements a, b of A are said to be comparable iff either  $a \leq b$  or  $b \leq a$ . Otherwise, a and b are called noncomparable.

# Definition 8.6.4 (Total Order)

Let  $\leq$  be a partial order on a set A.  $\leq$  is said to be a total order iff

$$\forall x, y \in A \ (x \leq y \ \lor \ y \leq x)$$

In other words,  $\leq$  is a total order if  $\leq$  is a partial order and all x, y are comparable.

### **Examples**

 $(\mathbb{Z}, \leq)$  is a total order.

The Hasse diagram on slide 36 is not a total order. (Why?)

Let  $\leq$  be a partial order on a set A.

# Definition 8.6.5 (Maximal)

An element x is a maximal element iff

$$\forall y \in A \ (x \leq y \to x = y).$$

# Definition 8.6.6 (Maximum)

An element, usually noted  $\top$ , is the maximum element (or the maximum<sup>1</sup>) iff

$$\forall x \in A \ (x \leq \top).$$

<sup>&</sup>lt;sup>1</sup>Some authors say greatest element.

Let  $\leq$  be a partial order on a set A.

# Definition 8.6.7 (Minimal)

An element x is a minimal element iff

$$\forall y \in A \ (y \leq x \to x = y).$$

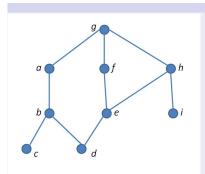
# Definition 8.6.8 (Minimum)

An element, usually noted  $\perp$ , is the minimum element (or the minimum<sup>2</sup>) iff

$$\forall x \in A \ (\bot \leq x).$$

<sup>&</sup>lt;sup>2</sup>Some authors say least element.

For the example shown in slide 36, there is only one maximal element, 18, which is also the maximum. The only minimal element is 1, which is also the minimum.



For the Hasse diagram on the left, the only maximal element is g, which is also the maximum. The minimal elements are: c, d, i, and there is no minimum element.

Let  $\leq$  be a total order on a set A. A is well ordered iff every non-empty subset of A contains a minimum element, formally:

$$\forall S \in \mathcal{P}(A) \ (S \neq \varnothing \to (\exists x \in S \ \forall y \in S \ (x \leq y))).$$

# **Examples**

 $(\mathbb{N}, \leq)$  is well-ordered.

 $(\mathbb{Z}, \leq)$  is not well-ordered.

# 8.7. Summary

- Relations allow us to model and study many real-world relationships.
- Relations may be inverted and composited.
- Important properties are: reflexivity, symmetry, transitivity, anti-symmetry.
- An Equivalence Relation is the generalization of the notion of "equality".
- A partition of a set and an equivalence relation are two sides of the same coin.
- A Partial Order is the generalization of the notion of "less than or equal to".
- Maximal and minimal elements are generalizations of upper and lower bounds.