Lecture 4.2: Equivalence relations and equivalence classes

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

Recall the basic concepts

Definition

An equivalence relation on a set A is a relation that is

(i) reflexive,

(ii) transitive,

(iii) symmetric.

We can always visualize a relation R on a finite set A with a directed graph (digraph):

- the vertex set is A;
- include a directed edge $a \to b$ if $(a, b) \in R$.

The digraph of an equivalence relation will be bidirected.

For convenience, we usually drop:

- all arrow tips, so all edges are undirected;
- all self-loops.

Equivalence classes

Definition

Given an equivalence relation R on A (write $a \equiv b$ for $(a,b) \in R$), the equivalence class containing $a \in A$ is the set

$$[a] := \{b \in A \mid (a,b) \in R\} = \{b \in A \mid a \equiv b\}.$$

We denote the set of equivalence classes by A/R, or $A/\equiv$, and say "*A modulo R*."

Example 1

Let A be the set of all people.

1. Say that two people are equivalent iff they were born in the same year.
2. Say that two people are equivalent iff they have the same last name.

Proposition

Let R be an equivalence relation on A.

(i) If $b \in [a]$, then $[a] = [b]$.

(ii) If $b \notin [a]$, then $[a] \cap [b] = \emptyset$.

In other words, the set of equivalence classes forms a partition of A.

Examples of equivalence classes

Example 2: isomorphic graphs

Let S be the following graphs, under the equivalence relation of isomorphism.

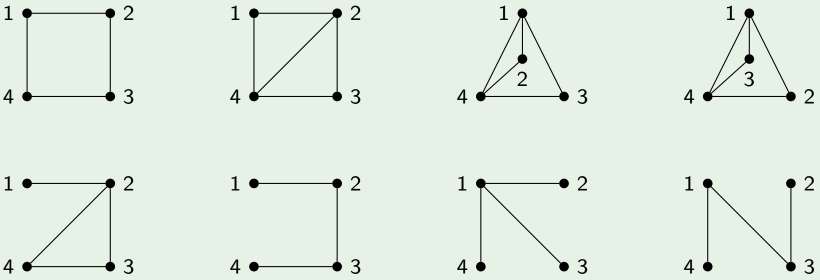


Figure: These 8 graphs fall into 6 equivalence classes.

Example 3: similar matrices

Let $M_n(\mathbb{C})$ be the set of $n \times n$ matrices, where the equivalence is similarity.

The equivalence classes are the similarity classes.

Examples of equivalence classes

Example 4: equivalence relation from partitions

Let V be a finite set. Every undirected graph on V defines an equivalence relation, where $v \equiv w$ iff v and w lie on the same connected component.

Moreover, *any* arbitrary partition of V defines an equivalence relation.

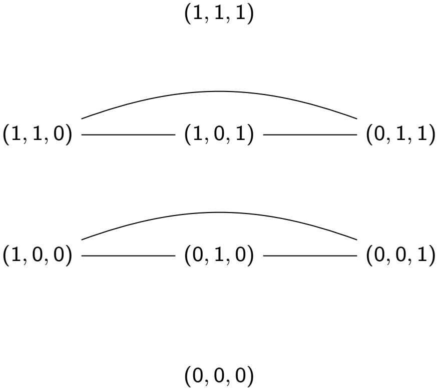
Example 5: Bitstrings

Given a length-n Boolean vector x, its Hamming weight $H(x)$ is the number of 1 bits in it.

Consider the equivalence on the set of length-3 Boolean vectors (or strings), where

$$x \equiv y \quad \text{iff} \quad H(x) = H(y).$$

The equivalence classes are the connected components in the graph below:



Example 6: Digital logic circuits

There are infinitely many possible digital logic circuits with n inputs.

However, there are only 2^{2^n} Boolean functions with n inputs.

Declare two digital logic circuits to be equivalent iff they give the same output on all inputs.

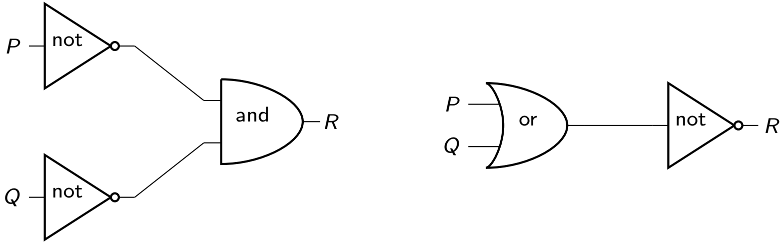


Figure: Two equivalent digital circuits

Example 7: Modular arithmetic

Let $A = \mathbb{Z}$, and fix $n > 1$.

Say that $a \equiv b$ iff $n \mid (a - b)$. We say that a and b are equivalent modulo n, and write

$$a \equiv b \pmod{n}, \qquad \text{or} \qquad a \equiv_n b.$$

This equivalence relation is sometimes called congruence modulo n.

Proposition

Let $a, b, c \in \mathbb{N}$, $n > 1$ and suppose that $a \equiv b \pmod{n}$. Then

1. $a + c \equiv b + c \pmod{n}$,
2. $ac \equiv bc \pmod{n}$,
3. $a^c \equiv b^c \pmod{n}$.

Corollary

Reducing modulo n can be done *before or after* doing arithmetic, i.e.,

1. $(a + b) \pmod{n} \equiv a \pmod{n} + b \pmod{n}$,
2. $(ab) \pmod{n} \equiv (a \pmod{n})(b \pmod{n})$.

We say that addition and multiplication is well-defined with respect to $\equiv_n$.

Example 7: Modular arithmetic

Let $n = 12$. The equivalence classes of $\mathbb{Z}$ modulo n are

$$\begin{aligned}
[0] &= \{\dots, -36, -24, -12, 0, 12, 24, 36, \dots\} \\
[1] &= \{\dots, -35, -23, -11, 1, 13, 25, 37, \dots\} \\
[2] &= \{\dots, -34, -22, -10, 2, 14, 26, 38, \dots\} \\
&\vdots \\
[11] &= \{\dots, -25, -13, -1, 11, 23, 35, 47, \dots\}
\end{aligned}$$

The fact that addition and multiplication is well-defined with respect to $\equiv_n$ means that it does not depend on choice of representative, i.e.,

$$\text{if } [a] = [b] \text{ and } [c] = [d], \text{ then } [a+c] = [b+d] \text{ and } [ac] = [bd].$$

Equivalently,

$$\text{if } a \equiv_n b \quad \text{and} \quad c \equiv_n d, \quad \text{then} \quad (a+c) \equiv_n (b+d) \text{ and } \quad ac \equiv_n bd.$$

Example 8: the rational numbers

"*God created the integers; all else is the work of man.*"
–Leopold Kronecker (1880s)

Let $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Define a relation on A by

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

We need to check that $\sim$ is:

(i) Reflexive: $(a, b) \sim (a, b)$,
(ii) Symmetric: $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$,
(iii) Transitive: $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$.

[We need the *cancellation law* in $\mathbb{Z}$: if $ab = ac$ and $a \neq 0$, then $b = c$.]

The equivalence class containing (a, b), denoted a/b or $\frac{a}{b}$, is

$$\tfrac{a}{b} := \big[(a, b)\big] = \big\{(p, q) \mid (a, b) \sim (p, q)\big\}.$$

Definition

We can define addition and multiplication of equivalence classes as follows:

(i) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$,
(ii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Example 8: the rational numbers

Exercise

Check that addition and multiplication of equivalence classes, defined as

(i) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$,

(ii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$,

is well-defined.

This means checking that if $[(a,b)] = [(c,d)]$ and $[(p,q)] = [(r,s)]$, then

1. $[(a,b)] + [(p,q)] = [(c,d)] + [(r,s)]$,

2. $[(a,b)] \cdot [(p,q)] = [(c,d)] \cdot [(r,s)]$.