MFCS

Special Relations

KLAUS SUTNER

CARNEGIE MELLON UNIVERSITY

FALL 2022

Generalizing Equality

Equality is one of the most important relations. Clearly, equality is reflexive, symmetric and transitive:

- $x = x$,
- $x = y$ implies $y = x$, and
- $x = y$, $y = z$ implies $x = z$.

It is natural to consider weaker versions of equality: coarser relations that maintain these three properties.

These relations formalize the notion of two objects being “the same” in some sense – without necessarily being identical.

Equivalence Relations

Definition

A square relation ρ on A is an equivalence relation if ρ is symmetric, reflexive, and transitive.
Suppose ρ equivalence relation. The equivalence class of $a \in A$ is:

$$[a]_\rho = \{\, x \in A \mid a \; \rho \; x \,\}.$$

$A/\rho = \{\, [a]_\rho \mid a \in A \,\}$ is the collection of all such classes, the quotient of A by ρ. The cardinality of A/ρ is the index of ρ.

Recall that for a binary relation ρ on some set A we have

property	$\forall\, x\,, y, z \in A$
reflexive	$x \; \rho \; x$
symmetric	$x \; \rho \; y \Rightarrow y \; \rho \; x$
transitive	$x \; \rho \; y \wedge y \; \rho \; z \Rightarrow x \; \rho \; z$

Examples

Here is a list of equivalence relations together with their domains.

- equality, any set A
- same weight, dumbbells
- same parents, humans
- same cardinality, sets
- same prime factors, naturals
- same dimension, matrices
- equidecomposability, polygons
- same-input-output is an equivalence relation on programs

Equidecomposability is also called scissor equivalence: cut up a polygon into finitely mnay pieces (wlog triangles), reassemble them to form a new polygon. See below for a discussion.

The Classic Example

Congruence modulo m on the integers.

$$x = y \pmod{m} \iff m \text{ divides } x - y$$

Is an equivalence relation on $\mathbb{Z}$ where

$$[a] = \ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots$$

Note that the equivalence relation $\pmod{m}$ has index m.

This simple equivalence is the foundation for a lot of cryptographic schemes, including RSA.

Was first studied in great detail by C. F. Gauss (1777–1855) in his work on number theory.

Equivalence Classes

What can we say about equivalence classes?

The equivalence classes of I_A and U_A are trivial:

$$\{a\} = [a]_= \quad \text{and} \quad A = [a]_{U_A}$$

In general, we always have

$$a \in [a]_\rho$$

by reflexivity.

Usually write $[a]$ instead of $[a]_\rho$ unless there is any danger of confusion.

Disjoint Classes

The following dichotomy is the single-most important property of equivalence classes.

Lemma

Let ρ be an equivalence relation on A. For all $a, b \in A$:

$$[a] = [b] \quad \textit{or} \quad [a] \cap [b] = \emptyset.$$

Proof.

If $c \in [a] \cap [b]$, then by symmetry for any $z \in [a]$:

$$z \;\rho\; a \;\rho\; c \;\rho\; b$$

Hence $z \in [b]$ by transitivity. But then $[a] \subseteq [b]$.

By a symmetric argument, $[b] \subseteq [a]$, done. □

Partitions

Definition

A partition of a set A is a set $P \subseteq \mathfrak{P}(A)$ of subsets of A such that

- $X \neq \emptyset$ for all $X \in P$,
- $\bigcup P = A$, and
- $X \neq Y \in P \Rightarrow X \cap Y = \emptyset$.

The sets $X \in P$ are called the blocks of the partition.

This is really just different terminology, not a new idea: a block is nothing but an equivalence class.

By the lemma, the classes form a partition.

Same Idea

Lemma

Equivalence relations correspond exactly to partitions.

Proof.

If ρ is an equivalence relation on A the equivalence classes $[a]$ of ρ produce a partition by the last lemma.

Now let P be a partition of A. Define

$$x \; \rho \; y \iff \exists \, X \in P \, (x, y \in X).$$

Clearly ρ is reflexive and symmetric.

Transitivity follows from the lemma. $\square$

Functions and Equivalence Relations

A closer look at the list of examples above shows that almost all our equivalence relations are based on measuring some particular aspect of an object, and declaring two objects to be equivalent if the measurements come out the same.

In other words, they are of the form

$$x \, \rho \, y \iff f(x) = f(y)$$

for some suitable function $f : A \to B$.

Kernels

Definition

Let $f : A \to B$ be a function. Define the kernel relation of f by

$$x \; \rho \; y \iff f(x) = f(y)$$

The kernel relation is usually written K_f or $\ker(f)$.

It is easy to check that ρ is an equivalence relation on A.

Example

Let $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x \bmod m$. Then K_f is congruence modulo m.

Kernels Everywhere

Question:
Could every equivalence relation already be a kernel relation?

In other words, given an arbitrary equivalence relation ρ on A, can we produce a function $f : A \to B$ such that $\rho = K_f$.

If we don't care much about the codomain this is easy:

$$\begin{array}{rccc} f : & A & \longrightarrow & \mathfrak{P}(A) \\ & x & \longmapsto & [x] \end{array}$$

Correct, but uncomfortable. Power sets are huge, and should be avoided whenever possible.

Better Kernels

Theorem

Every equivalence relation ρ on A is a kernel relation.
In fact, we can choose a function $f : A \to A$ such that $K_f = \rho$.

Proof.

We have to produce a function $f : A \to A$ such that $\rho = K_f$.

For each equivalence class $[x]_\rho$ pick one representative $x_0 \in [x]_\rho$.

Set $f(z) = x_0$ for all $z \in [x]_\rho$.

$\square$

A Minor Foundational Problem

But, there is a small problem: how do we actually pick $x_0 \in [x]$?

If $[x] \subseteq A$ is just an abstract set, there is no mechanism to select x_0.

As B. Russell pointed out, given an infinite collection of pairs of shoes one can select one from each pair; given an infinite collection of socks one is stumped.

Choice

But, we have the celebrated Axiom of Choice.

Consider the partition $P \subseteq \mathfrak{P}(A)$ corresponding to ρ.

By (AC), there is a choice set C:

$$\forall\, X \in P\, (|X \cap C| = 1).$$

Hence we can define

$$f(x) = y \qquad \text{iff} \qquad x \; \rho \; y \wedge y \in C$$

It is easy to check that f really is a function and that $\rho = K_f$.

Data Structure Angle

For computational purposes, we may as well assume that $A = [n]$.

By the theorem, we can represent any equivalence relation on A as a map $f : A \to A$: in other words, by a plain array.

And there is an obvious answer on how we should pick the representative:

$$f(x) = \min\big(z \in [n] \mid x \; \rho \; z \big)$$

This is representation is used in a number of algorithms, in particular minimization of finite state machines.

Chess

Consider the chess board $C = [8] \times [8]$.

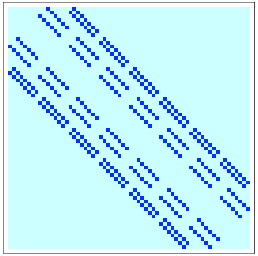
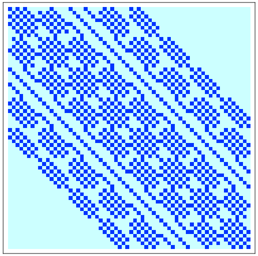
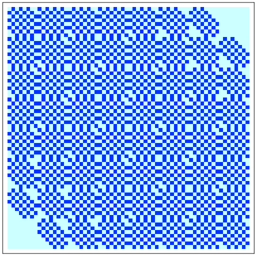
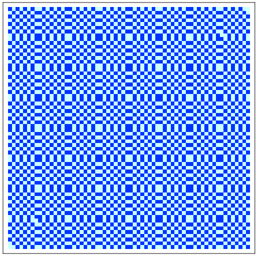
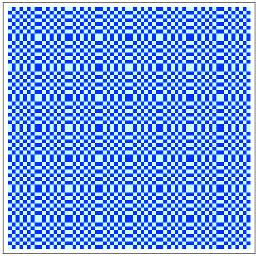
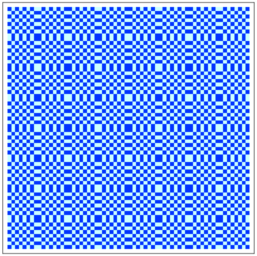
For each piece, we can define a move relation ρ on C by:

$(x, y)\ \rho\ (x', y')$ iff the piece can move from square (x, y) to (x', y') in a single move. We write $\rho^\star$ for the relation: can move in a sequence of single moves.

For example, for a knight the relation can be defined like so:

$$\begin{aligned}(x, y)\ \rho\ (x', y') \iff \big(|x - x'| = 1 \land |y - y'| = 2\big) \lor \\ \big(|x - x'| = 2 \land |y - y'| = 1\big)\end{aligned}$$

Knights

Reachable Squares

From the pictures, one can "see" that $\rho^\star = \bigcup_{i \leq 6} \rho^i$.

Claim

$\rho^\star$ is an equivalence relation and has exactly one equivalence class. .

The same for a rook, king or queen.

But for a bishop there are two equivalence classes: the black squares and the white squares.

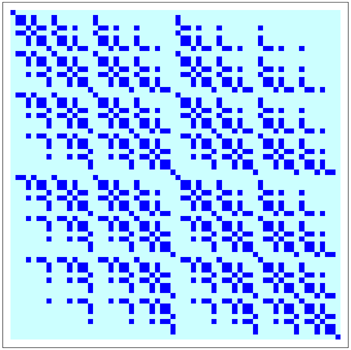
Exercise

How many equivalence classes for a pawn? Only consider the basic move $(i, j) \to (i, j + 1)$, no conversion. What's wrong?

Boolean Matrices

Consider as carrier set the collection of all binary lists of length 6 (organized in natural order). Here is a picture of the relation “list x has the same number of 1’s as list y.

Note that by definition this is an equivalence relation.

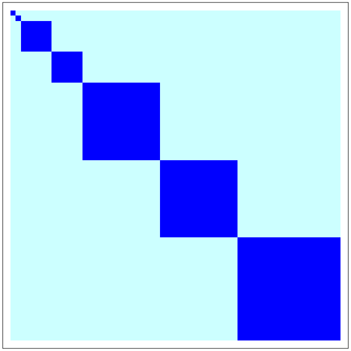


The picture clearly shows reflexivity and symmetry. But how about transitivity?

Reordering the Carrier Set

Transitivity is just about impossible to see from the last picture.

But, if we reorder the carrier set so that equivalent elements are all consecutive, the picture becomes very clear.



Exercise

What are the sizes of these blocks?

Reordering

Picture 1 uses the carrier set in natural order, but in picture 2 the carrier set is reordered so all elements of a block in the equivalence relation are contiguous.

natural	reordered
000000	000000
000001	111111
000010	000001
000011	000010
000100	000100
000101	001000
...	...
111101	110010
111110	110100
111111	111000

The important point here is that the relation is unchanged, only its representation in terms of the Boolean matrix has changed.

Equidecomposability

Here is a much more interesting equivalence relation.

Definition

Two polygons P and Q are equidecomposable if P can be cut up into finitely many triangles which can be reassembled to form Q.

We will not give a precise definition of what we mean by reassemble and appeal to common (geometric) sense.

Equidecomposability is also called scissor equivalence.

It's an Equivalence

Lemma

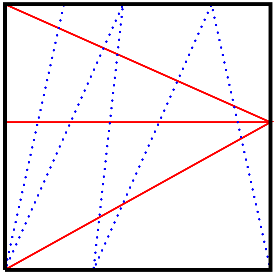
Equidecomposability is an equivalence relation.

Reflexivity and symmetry is obvious, but transitivity is not.

Suppose we can cut up P to obtain Q, and we can cut up Q to obtain R.

Why should we be able to cut up P to obtain R directly?

Picture Proof



Given two triangulations of a polygon, construct a finer one: triangulate the polygonal regions produced by intersection.

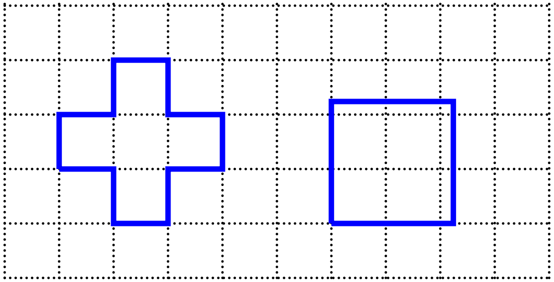
And Kernels???

We have shown that any equivalence relation is already a kernel relation.

What is the natural kernel function for equidecomposability?

It turns out to be area, but that is far from obvious.

A Challenge



The square on the right is $\sqrt{5}$ by $\sqrt{5}$, so both polygons have area 5.

Exercise

Show that the two polygons are equidecomposable.
What is the least possible number of cuts?

Wallace-Bolyai-Gerwien

It is clear that any two equidecomposable polygons must have the same area: cutting them up and reassembling the pieces does not change the area[†]. But it is somewhat surprising that the opposite direction also holds[‡].

Theorem (Wallace-Bolyai-Gerwien Theorem)

Let P and Q be two polygons of equal area. Then P and Q are equidecomposable.

We sketch the proof below. It is an excellent exercise to turn this into a real proof.

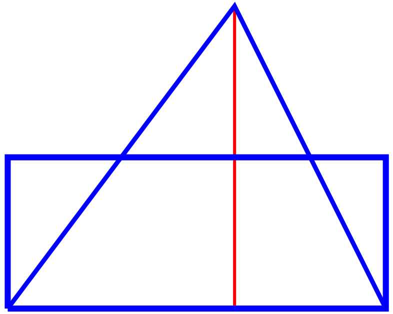
[†] But consider the Banach-Tarski construction to double a sphere.

[‡] In other words, area is a kernel function

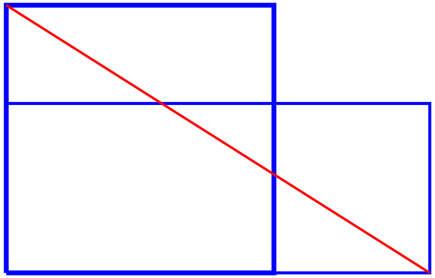
Step 1

To prove the Wallace-Bolyai-Gerwien theorem it suffices to show that every polygon P is equidecomposable with a square: there is exactly one square for each area. Since we can triangulate any polynomial, we start with triangles.

Here is a method to convert triangles to rectangles of equal area:



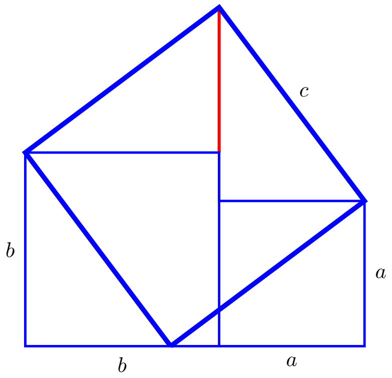
Step 2



In the second step we convert rectangles to squares.

This requires that the longer side of the rectangles is ≤ 4 times the shorter one. What if not?

Step 3



Lastly, we have to add squares and produce new squares. We exploit Pythagoras's theorem: $a^2 + b^2 = c^2$.

Orders

The relations $\leq$ on $\mathbb{N}$, $\leq$ on $\mathbb{R}$ and $\subseteq$ on $\mathfrak{P}(\mathbb{N})$ are similar in a sense, they organize the elements of the domain into “smaller” versus “larger” elements.

What are the crucial properties that make them similar?

Definition

Let ρ be a relation on A.
ρ is a preorder (or quasi-order) if it is both reflexive and transitive.
ρ is a partial order if it is a preorder and antisymmetric.
ρ is an order (or total order or linear order) if it is a partial order and all elements of A are comparable with respect to ρ:

$$\forall x, y \in A \, (x \; \rho \; y \vee y \; \rho \; x).$$

Strict versus Reflexive

Often it is more convenient to consider the strict (i.e. irreflexive) version of an order, obtained by setting

$$x \; \rho' \; y \iff x \neq y \wedge x \; \rho \; y.$$

Notation: $\leq$ versus $<$, $\subseteq$ versus $\subset$. One sometimes refers to the reflexive versions as weak orders. Similarly we denote the converse of an order by flipping the symbol around: $\geq$ and $>$ versus $\leq$ and $<$.

Thus, a strict preorder is any irreflexive and transitive relation. Note that any such relation is automatically asymmetric.

A strict total order has the additional trichotomy property:

$$\forall \, x, y \in A \, (x \; \rho \; y \vee x = y \vee y \; \rho \; x)$$

Posets

Another piece of terminology: a structure

$$\langle A, < \rangle$$

consisting of a set A and a strict partial order $<$ (or a weak version) is often called a poset.

This is mostly an acknowledgment that partial orders are so important that one should have a nice, compact, generally accepted name for them (just like groups or fields).

The study of posets has turned out to be of major importance for the semantics of programming languages.

Examples

- The usual order relations on numbers are total orders.
- Subset-of and divides are partial orders.
- Ordering polynomials by their degree produces a preorder.
- Cardinality of a set is a preorder (and has full comparability).
- Lies-north-east-of in the plane is a partial order.
- Lexicographic order on words is a total order.
- The substring order is a partial order on strings:
  $x \preceq y \iff \exists\, u, v\, (y = uxv)$.
- The element relation $\in$ is a total order on the class of ordinals but only a partial order on the class of all sets.

Ordering Pairs

A standard problem is to lift a given order $\leq$ on A to $A \times A$. One plausible definition is

Definition

The product order of $\leq$ with itself is defined by

$$(x, y) \leq_2 (x', y') \iff x \leq x' \wedge y \leq y'.$$

On the plane $\mathbb{R} \times \mathbb{R}$ this is the "north-east-of" relation. Thus, the product order is partial, even though $\langle \mathbb{R}; \leq \rangle$ is a total order. Can we manufacture a total order? How about

$$(x, y) \trianglelefteq (x', y') \iff x \leq x' \vee (x = x' \wedge y \leq y').$$

Exercise

Show that $\trianglelefteq$ is indeed a total order.

Ordering Sequences

It is slightly harder to order all sequences over A, not just pairs.

The usual order on characters $a < b < c < \ldots < y < z$ can be lifted to words over this alphabet.

Recall that we write $|u|$ for the length of a sequence u.

Definition

Consider two sequences u and v over A.

1. Lexicographic Order (Dictionary Order)
   $u \prec v$ lexicographically if u is a proper prefix of v or if $u = xay$, $v = xbz$ and $a < b$, where x, y, z are sequences, $a, b \in A$.
2. Length-Lex Order
   $u \prec v$ in the length-lex order if $|u| < |v|$ or $|u| = |v|$ and u precedes v lexicographically.
3. Length Order
   $u \prec v$ in the length order if $|u| < |v|$.

Lex Orderings

Lexicographic order and length-lex order are bonified total orders on finite sequences, but length order is only a preorder.

On words over the alphabet $\{0, 1\}$, length-lex order produces

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots$$

This is crucially important for induction arguments: we finish off all words of length k before working on length $k + 1$.

But lexicographic order for these few words would be

$$\varepsilon, 0, 00, 000, 001, 010, 011, 1, 11$$

This is much less natural if one tries to systematically work through these words.

Lexicographic order is used in the $\mathrm{C}{+}{+}$ library STL to overload `operator<` for stacks.