Equivalence Relations

Siddhartha Chaudhuri

CS 2800, Spring 2015

Definition 1. The *cartesian product* $A \times B$ of sets A and B is the set of all possible ordered pairs with the first element drawn from A and the second from B. That is, it is the set

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

Definition 2. A *relation* with domain A and codomain B is a subset of $A \times B$.

For instance, $R = \{(a, 1), (a, 2), (b, 1)\}$ is a relation from set $\{a, b, c\}$ to set $\{1, 2, 3\}$. Note that R relates a to two different numbers, and does not cover either the entire domain or the entire codomain. In this, a relation is different from a *function*, which is a special type of relation that maps each element of the domain to a single (not necessarily unique) element of the codomain.

When specifying a particular relation, it is often useful to write it as a rule connecting pairs of elements, rather than as a set of pairs. Indeed, the latter is often infeasible when large or infinite sets are concerned. For example, here is a relation P between people:

$$x\ P\ y \text{ if and only if } x \text{ is the parent of } y$$

$x\ P\ y$ is read as "x is related (by P, in this case parenthood) to y". Remember that this relation is still just a set of pairs, of the form $(parent, child)$, and can be rewritten in that style! This is just a different notation, not a different definition.

Note also that a relation need not be symmetric. It's perfectly possible that, as in this example, $x\ P\ y$ but not $y\ P\ x$.

Definition 3. An *equivalence relation* R on a set A is a relation from A to itself (that is a, subset of $A \times A$) that satisfies three properties:

1. **Reflexivity:** For all $x \in A$, $x\ R\ x$.
2. **Symmetry:** For all $x, y \in A$, if $x\ R\ y$ then $y\ R\ x$.
3. **Transitivity:** For all $x, y, z \in A$, if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$.

Make sure you correctly interpret these three properties! Reflexivity, for instance, says that every element must be related to itself. Transitivity says that the relation "short-circuits" chains of related pairs.

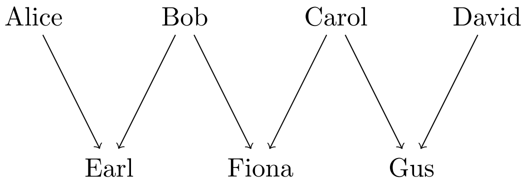
It can be useful to draw the relation as a graph. Plot a point for every element of A, and draw an arrow from x to y if x is related to y. Then reflexivity says that every point has a self loop (an arrow pointing to itself). Symmetry says that every arrow is bidirectional. And transitivity says that if there is a (directed) path between two points, then there is a direct arrow between them as well.

We observe right at the outset that any reasonable definition of equality (the "is equal to" sign '=', in the context of numbers, or sets, or matrices …) that you might see is almost certainly an equivalence relation, else there would be severe cognitive dissonance. Here are some more examples.

Example 1. Let R be the following relation on the set of all people in the world: x is related to y if and only if x and y have the same set of parents. This is an equivalence relation, which we can prove by arguing that it is reflexive, symmetric and transitive. It is clearly reflexive, since one has the same set of parents as oneself. It is also symmetric, since if I have the same parents as another person, that other person has the same parents as me. And it is transitive, because if I have the same parents as a second person, and that person has the same parents as a third person, then all three of us clearly share the same set of parents.

This can also be stated slightly more "mathily", though plain English works just fine here: let $\pi(x)$ denote the set of parents of x. The relation is reflexive since $\pi(x) = \pi(x)$, symmetric since $\pi(x) = \pi(y) \implies \pi(y) = \pi(x)$, and transitive since $(\pi(x) = \pi(y) \wedge \pi(y) = \pi(z)) \implies \pi(x) = \pi(z)$. In other words, the result follows from set equality being reflexive, symmetric and transitive, i.e. an equivalence relation.

Note that if we had instead defined two people to be related if they shared *at least one* parent, this would no longer be an equivalence relation! For example, if Alice, Bob, Carol and David pair up as illustrated below to produce children Earl, Fiona and Gus, then transitivity is broken: Earl is related to Fiona and Fiona is related to Gus, but Earl is not related to Gus since they don't share any parents.



Note also that if we had instead defined the relation as "x is related to y if they are siblings", the question of this being an equivalence would hinge upon whether you consider yourself to be your own sibling.

Example 2. For a given integer $m > 1$, let $\sim_m$ be the following relation on the set of all integers: $x \sim_m y$ if and only if $x - y$ is exactly divisible by m. That is, x and y leave the same remainder upon division by m (the remainder needs to be suitably defined when dividing negative numbers). This relation is important enough in both theoretical and practical (e.g. cryptography) settings to have a special name: "congruence modulo m".

This is an equivalence relation. It is reflexive: $x - x = 0$, which is divisible by m. It is symmetric: if $x - y$ is divisible by m, so is $y - x = -(x - y)$. It is transitive: if $x - y = am$ and $y - z = bm$, for integers a and b, then $x - z = (a + b)m$, which is divisible by m.

A specific example: if $m = 10$, then this relation says that $\ldots - 15, -5, 5, 15, 25, 35 \ldots$ are all equivalent, as are $\ldots - 19, -9, 1, 11, 21, 31 \ldots$, etc. The first set of numbers all leave 5 as a remainder when divided by 10; the second set leaves 1 as a remainder. We can devise a way to to do arithmetic only in the space of remainders $\{0, 1, \ldots, m-1\}$: this is called modular arithmetic. For $m = 2$, this is just 1-bit binary arithmetic, which is the foundation of modern digital computers. For certain very large values of m, this arithmetic is crucial to constructing secure cryptosystems, as we will see later in this course.

An equivalence relation induces a very neat structure on a set. This is expressed via the notion of an equivalence class.

Definition 4. The *equivalence class*, denoted $[x]$, of an element x of set A with respect to an equivalence relation $\sim$ defined on A, is the set of all elements that are equivalent to x. That is,

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

The set of all equivalence classes of $\sim$ on A, denoted $A/{\sim}$, is called the *quotient* (or *quotient set*) of the relation. It is by definition a subset of the power set 2^A.

Theorem 1. The quotient of an equivalence relation is a partition of the underlying set. That is, the elements of $A/{\sim}$ are disjoint, and their union is A.

Proof. We will first show that the elements of $A/{\sim}$ are disjoint. To do this, it is sufficient to prove that the equivalence classes $[x]$ and $[y]$ of two arbitrary elements $x, y \in A$ are either disjoint or identical: they cannot partially overlap. Assume $[x]$ and $[y]$ are not, in fact, disjoint. Then they have a non-zero intersection $[x] \cap [y]$, from which we can select some arbitrary representative z. Our strategy will be to "chain" the relation through z. Consider any element $a \in [y]$. By definition, $y \sim a$. Also, $y \sim z$ (since $z \in [y]$), from which we conclude that $z \sim y$ (by symmetry). By transitivity, $z \sim a$. But z is also in $[x]$, so $x \sim z$! Again applying transitivity, we obtain $x \sim a$, which implies that $a \in [x]$. Since a was an arbitrary element of $[y]$, we conclude that $[y] \subseteq [x]$. By a symmetric argument, we can also show that $[x] \subseteq [y]$. Hence, $[x] = [y]$.

To complete the proof, we must show that the union of the equivalence classes is A. But this is easy: every element of A is related to itself by reflexivity, so it must be in its own equivalence class: $x \in [x]$! Hence every element of A is covered by some equivalence class. □

To wrap this up, here's a little exercise that uses equivalence relations to study the structure induced by a function on its domain.

Exercise 1. For a function f with domain A (and arbitrary codomain), define two elements $x, y \in A$ to be related if and only if $f(x) = f(y)$. Show that this is an equivalence relation, and moreover, that the quotient set has a bijective mapping to the image of the function.