COMP30026 Models of Computation

Binary Relations, and Functions

Harald Søndergaard

Lecture 12

Semester 2, 2017

Binary Relations

An binary relation is a set of pairs, or 2-tuples.

"Being unifiable", "$<$", "$\subseteq$", "divides" are all binary relations.

For small relations we can tabulate:

Beats	Paper	Scissors	Rock
Paper	0	0	1
Scissors	1	0	0
Rock	0	1	0

We can express membership of a relation in many ways:
$Beats(x, y)$, $(x, y) \in Beats$, or x $Beats$ y.

Domain and Range of a Relation

The domain of R is $dom(R) = \{x \mid \exists y\ R(x, y)\}$.

The range of R is $ran(R) = \{y \mid \exists x\ R(x, y)\}$.

We say that R is a relation from A to B if $dom(R) \subseteq A$ and $ran(R) \subseteq B$. Or, R is a relation between A and B.

A relation from A to A is a relation on A.

"Being unifiable" is a relation on *Term*.

"$<$" is a relation on integers.

"$\subseteq$" is a relation on $\mathcal{P}(A)$.

"Acted in" is a relation between actors and films.

Identity and Inverse

$A \times B$ is a relation—the full relation from A to B.

$\emptyset$ is a relation.

$\Delta_A = \{(x, x) \mid x \in A\}$ is a relation on A—the identity relation.

If R is a relation from A to B then $R^{-1} = \{(b, a) \mid R(a, b)\}$ is a relation from B to A, called the inverse of R.

Clearly $(R^{-1})^{-1} = R$.

Since relations are sets, all the set operations, such as $\cap$ and $\cup$, are applicable to relations.

Properties of Relations

Let A be a non-empty set and let R be a relation on A.

R is reflexive iff $R(x, x)$ for all x in A.

R is irreflexive iff $R(x, x)$ holds for no x in A.

R is symmetric iff $R(x, y) \Rightarrow R(y, x)$ for all x, y in A.

R is asymmetric iff $R(x, y) \Rightarrow \neg R(y, x)$ for all x, y in A.

R is antisymmetric iff $R(x, y) \wedge R(y, x) \Rightarrow x = y$ for all x, y in A.

R is transitive iff $R(x, y) \wedge R(y, z) \Rightarrow R(x, z)$ for all x, y, z in A.

Reflexive, Symmetric, Transitive Closures

The full relation is transitive, and transitive relations are closed under intersection. That is, if R_1 and R_2 are transitive then so is $R_1 \cap R_2$.

This means that for any binary relation R, there is a smallest transitive relation R^+ which includes R.

We call R^+ the transitive closure of R.

Similarly we have the (unique) reflexive closure and the (unique) symmetric closure of R.

Closures Quiz

What is the reflexive, transitive closure of $R = \{(n, n+1) \mid n \in \mathbb{N}\}$?

Closures Quiz

What is the reflexive, transitive closure of $R = \{(n, n+1) \mid n \in \mathbb{N}\}$?

What is the symmetric closure of $<$ on $\mathbb{Z}$?

Composing Relations

Let R_1 and R_2 be relations on A. The composition $R_1 \circ R_2$ is the relation on A defined by

$$(x, z) \in (R_1 \circ R_2) \text{ iff } \exists y \; (R_1(x, y) \wedge R_2(y, z))$$

The n-fold composition R^n is defined by

$$\begin{array}{rcl} R^1 & = & R \\ R^{n+1} & = & R^n \circ R \end{array}$$

Composition Quiz

If R is $\{(0,2),(0,3),(1,0),(1,3),(2,0),(2,3)\}$, what is R^2?

Composition Quiz

If R is $\{(0,2),(0,3),(1,0),(1,3),(2,0),(2,3)\}$, what is R^2?

What is R^3?

Composition Quiz

If R is $\{(0,2),(0,3),(1,0),(1,3),(2,0),(2,3)\}$, what is R^2?

What is R^3?

If R is $<$ on $\mathbb{N}$, what is R^2?

Transitive Closure Again

The transitive closure of R can be defined in terms of composition:

$$R^+ = \bigcup_{n \geq 1} R^n$$

The reflexive, transitive closure is

$$R^* = \bigcup_{n \geq 0} R^n = R^+ \cup \Delta_A$$

Equivalence Relations

A binary relation which is reflexive, symmetric and transitive is an equivalence relation.

The identity relation Δ_A is the smallest equivalence relation on a set A. The full relation A^2 is the largest equivalence relation on A.

Quiz: Equivalence Relations?

Which of these binary relations are equivalence relations?

- $\leq$ on $\mathbb{Z}$?

Quiz: Equivalence Relations?

Which of these binary relations are equivalence relations?

- $\leq$ on $\mathbb{Z}$?
- $\equiv_m$ on $\mathbb{Z}$, where $a \equiv_m b$ iff $a \ mod \ m = b \ mod \ m$?

Quiz: Equivalence Relations?

Which of these binary relations are equivalence relations?

- $\leq$ on $\mathbb{Z}$?
- $\equiv_m$ on $\mathbb{Z}$, where $a \equiv_m b$ iff $a\ mod\ m = b\ mod\ m$?
- "are unifiable" on the set of terms (over some alphabet)?

Quiz: Equivalence Relations?

Which of these binary relations are equivalence relations?

- $\leq$ on $\mathbb{Z}$?
- $\equiv_m$ on $\mathbb{Z}$, where $a \equiv_m b$ iff $a \ mod \ m = b \ mod \ m$?
- "are unifiable" on the set of terms (over some alphabet)?
- $\{(a, b) \mid |a - b| \leq 3\}$?

Quiz: Equivalence Relations?

Which of these binary relations are equivalence relations?

- $\leq$ on $\mathbb{Z}$?
- $\equiv_m$ on $\mathbb{Z}$, where $a \equiv_m b$ iff $a \; mod \; m = b \; mod \; m$?
- "are unifiable" on the set of terms (over some alphabet)?
- $\{(a, b) \mid |a - b| \leq 3\}$?
- "are compatriots" on the set of all people?

Quiz: Equivalence Relations?

Which of these binary relations are equivalence relations?

- $\leq$ on $\mathbb{Z}$?
- $\equiv_m$ on $\mathbb{Z}$, where $a \equiv_m b$ iff $a\ mod\ m = b\ mod\ m$?
- "are unifiable" on the set of terms (over some alphabet)?
- $\{(a, b) \mid |a - b| \leq 3\}$?
- "are compatriots" on the set of all people?
- "are logically equivalent" on the set of propositional formulas?

Partial Orders

R is a pre-order iff R is transitive and reflexive.

R is a strict partial order iff R is transitive and irreflexive.

R is a partial order iff R is an antisymmetric preorder.

R is linear iff $R(x, y) \vee R(y, x) \vee x = y$ for all x, y in A.

A linear partial order is also called a total order.

In a total order, every two elements from A are comparable.

Quiz: Partial Orders?

Which of these binary relations are partial orders?

- The relation $\leq$ on $\mathbb{N}$?

Quiz: Partial Orders?

Which of these binary relations are partial orders?

- The relation $\leq$ on $\mathbb{N}$?
- The relation $\subseteq$ on $\mathcal{P}(\mathbb{N})$?

Quiz: Partial Orders?

Which of these binary relations are partial orders?

- The relation $\leq$ on $\mathbb{N}$?
- The relation $\subseteq$ on $\mathcal{P}(\mathbb{N})$?
- The relation "divides" on $\mathbb{N}$?

Functions

- **Mathematically:** A function f is a relation with the property that $(x, y) \in f \land (x, z) \in f \Rightarrow y = z$. That is, for $x \in dom(f)$, there is exactly one $y \in ran(f)$ such that $(x, y) \in f$. We write this: $f(x) = y$.
- **Computationally:** A prescription (an algorithm) for how to calculate output values from input values.

Note that a function-as-a-relation may be infinite, but we assume that an "algorithm" is finite.

The question of how to define "algorithm" is central to computability theory—we won't venture into that territory just yet.

The Two Views Contrasted

The three Haskell functions defined by

```
f0 n = n^2 + n
f1 n = n * (n+1)
f2 n = if n == 0 then 0 else 2*n + f2 (n-1)
```

all prescribe calculations of the (mathematical) function

$$\{(0,0),(1,2),(2,6),(3,12),\ldots\} = \{(n, n^2+n) \mid n \in \mathbb{N}\}$$

But note that there is no Haskell type corresponding to $\mathbb{N}$, and the functions do not behave identically if applied to a negative integer.

Domains and Co-Domains

We say that the function f is from X to Y, or

$$f : X \to Y$$

if $dom(f) = X$ and $ran(f) \subseteq Y$. We call Y the co-domain of f.

Example: The range of the factorial function is $\{1, 2, 6, 24, 120, \ldots\}$, but we normally define it as having co-domain $\mathbb{N}$.

The domain/co-domain specification is integral to the function definition, as we define functions $f : X \to Y$ and $f' : X' \to Y'$ to be equal iff $X = X'$, $Y = Y'$, and for all $x \in X, f(x) = f'(x)$.

Recurrences versus Closed Forms

The definition of `f2` above is given as a recurrence formula—to define `f2`, we refer back to `f2` itself!

The definition of (the equivalent) `f1` does not depend (directly or indirectly) on `f1` itself. We say that the definition is in closed form.

Computationally, and also for readability, a closed form definition is usually preferable—though not always possible to find.

Images and Co-Images

Let $A \subseteq X$, $B \subseteq Y$, and consider $f : X \to Y$.

$f[A] = \{f(x) \mid x \in A\}$ is the image of A under f.

$f^{-1}[B] = \{x \in X \mid f(x) \in B\}$ is the co-image of B under f.

Consider the relation $f = \{(1,2),(2,3),(3,5),(4,3),(5,2)\}$.

f is a function with domain $D = \{1,2,3,4,5\}$ and range $\{2,3,5\}$.

We could take $\mathbb{N}$ to be the co-domain and write $f : D \to \mathbb{N}$.

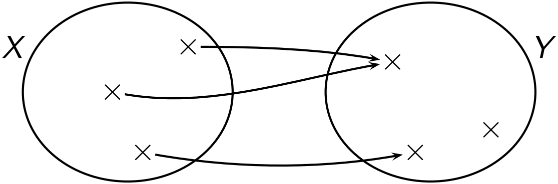
Let $A = \{2,5\}$. We have:

- $f[A] = \{2,3\}$
- $f^{-1}[A] = \{1,3,5\}$

Injections, Surjections and Bijections

A function $f : X \to Y$ is

- surjective (or onto) iff $f[X] = Y$.
- injective (or one-to-one) iff $f(x) = f(y) \Rightarrow x = y$.
- bijective iff it is both surjective and injective.



Examples

$f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2$ is neither surjective nor injective.

$g : \mathbb{Z} \to \mathbb{N}$ defined by $g(n) = |n|$ is surjective but not injective.

$s : \mathbb{N} \to \mathbb{N}$ defined by $s(n) = n + 1$ is injective but not surjective.

$d : \mathbb{Z} \to \mathbb{N}$ defined by

$$d(n) = \begin{cases} 2n - 1 & \text{if } n > 0 \\ -2n & \text{if } n \leq 0 \end{cases}$$

is bijective. It establishes a one-to-one mapping between $\mathbb{Z}$ and $\mathbb{N}$.

Examples

$h : \mathbb{N}^2 \to \mathbb{N}$ defined by

$$h(m, n) = \frac{(m+n)^2 + 3m + n}{2}$$

is bijective. It establishes a one-to-one mapping between $\mathbb{N}^2$ and $\mathbb{N}$.

The last two examples are interesting, because they show that, in a precise sense, there are no more integers than there are natural numbers, and similarly there are no more pairs of natural numbers than there are natural numbers.

Bijections will play a central role when we get to computability theory.

Function Composition

The composition of $f : X \to Y$ and $g : Y \to Z$ is the function $g \circ f : X \to Z$ defined by

$$(g \circ f)(x) = g(f(x))$$

We assume that g's domain coincides with f's co-domain, although the composition makes sense as long as $ran(f) \subseteq dom(g)$.

Note the unfortunate inconsistency with the use of $\circ$ for composing relations. For functions, $g \circ f$ is best read as "g after f."

$\circ$ is associative, and for $f : X \to Y$, $f \circ 1_X = 1_Y \circ f = f$, where $1_X : X \to X$ is the identity function on X.

Function Composition

Let $f : X \to Y$ and $g : Y \to Z$. It is easy to show that

- $g \circ f$ injective $\Rightarrow$ f injective;
- $g \circ f$ surjective $\Rightarrow$ g surjective;
- g, f injective $\Rightarrow$ $g \circ f$ injective;
- g, f surjective $\Rightarrow$ $g \circ f$ surjective.

Partial Functions

So far we have assumed that the domain of a function is known, so that $f : X \to Y$ means that $f(x)$ is defined for each $x \in X$.

In computer science, however, it is often more appropriate to deal with functions that are partial.

We write $f : X \hookrightarrow Y$ to say that f has a domain which is a subset of X, but $f(x)$ may be undefined for some $x \in X$.

Note that a total function $f : X \to Y$ is by definition also partial: $f : X \hookrightarrow Y$.

Partial Functions: Example 1

The function f defined by

$$f(n) = \begin{cases} 42 & \text{if } n = 0 \\ f(n-2) & \text{if } n \neq 0 \end{cases}$$

is a partial function $f : \mathbb{Z} \hookrightarrow \mathbb{Z}$.

In a natural interpretation, it is undefined if n is odd and/or negative. Its range is $\{42\}$.

In this case, it is not too hard to determine the set of values for which f is defined. So we could also choose to say that f is a total function $X \to \mathbb{Z}$, where $X = \{n \in \mathbb{Z} \mid n \geq 0 \land n \text{ is even}\}$.

However, it is not always easy, or even possible, to determine a function's domain.

Partial Functions: Example 2

The function c defined by

$$c(n) = \begin{cases} 1 & \text{if } n = 0 \text{ or } n = 1 \\ c(n/2) & \text{if } n \text{ is even and } n > 1 \\ c(3n+1) & \text{if } n \text{ is odd and } n > 1 \end{cases}$$

is a partial function $c : \mathbb{N} \hookrightarrow \mathbb{N}$ with range $\{1\}$.

It is not known whether c is total.

This is the so-called $3n + 1$ problem, or Collatz's problem.