Bisimulation and its Logical Characterization

Prakash Panangaden

1 Bisimulation: three definitions

We fix a labelled transition system

$$\mathcal{S} = (S, \mathcal{A}, \longrightarrow \subseteq S \times \mathcal{A} \times S)$$

which we assume to be *image finite*. This means that for any $a \in \mathcal{A}$ and any $s \in S$ the set $\{s' | s \xrightarrow{a} s'\}$ is finite.

Definition 1 *A* ***dynamic relation*** *on $\mathcal{S}$ is a binary relation $R \subseteq S \times S$ such that whenever sRt then $\forall a \in \mathcal{A}, s' \in S$ such that $s \xrightarrow{a} s'$, $\exists t'$ such that $t \xrightarrow{a} t'$ and $s'Rt'$ and, conversely, $\forall t'$ such that $t \xrightarrow{a} t'$, $\exists s'$ such that $s \xrightarrow{a} s'$ with $s'Rt'$.*

Given the complete lattice of relations, $\mathfrak{R}$ on S we define a function $\mathcal{F} : \mathfrak{R} \longrightarrow \mathfrak{R}$ as follows. If R is a relation, we define $\mathcal{F}(R)$ as $(s,t) \in \mathcal{F}(R)$ if, $\forall a \in \mathcal{A}, s' \in S$, such that if $s \xrightarrow{a} s'$, then $\exists t' \in S$ with $t \xrightarrow{a} t'$ and $(s',t') \in R$ and if $t \xrightarrow{a} t'$, then $\exists s' \in S$ with $s \xrightarrow{a} s'$ and $(s',t') \in R$.

The following important proposition is easy to prove.

Proposition 2 *The function $\mathcal{F}$ is monotone on $\mathfrak{R}$ with the inclusion order.*

It follows that it has a *greatest* fixed point.

We now define three equivalence relations on S.

Definition 3 (Milner) *We first define, by induction, a family of equivalence relations indexed by the integers. Let $\sim_0$ be the universal relation. Given a relation $\sim_n$ we define $\sim_{(n+1)}$ as $\mathcal{F}(\sim_n)$. Finally we define $\sim_M$ to be the intersection of all the $\sim_n$.*

Definition 4 (Park) *We define the relation $\sim_P$ to be the greatest fixed point of $\mathcal{F}$.*

Definition 5 (Milner2) *We define the relation $\sim$, called bisimulation, by saying that $s \sim t$ if there exists* any *dynamic relation R with sRt.*

These three definitions are equivalent for image-finite systems. In fact the last two are always equivalent; this is the really important connection.

There is an intimate relation between prefixed points of $\mathcal{F}$ and dynamic relations.

Proposition 6 *A relation R is a dynamic relation if and only if it is a prefixed point of $\mathcal{F}$.*

Proof . Suppose that R is a dynamic relation. Let sRt. I claim that $s\mathcal{F}(R)t$. To check this we must show that whenever $s \xrightarrow{a} s'$, there exists t' with $t \xrightarrow{a} t'$ and $s'Rt'$ (and vice versa). But this is immediate from the definition of a dynamic relation. Thus $R \subseteq \mathcal{F}(R)$. Conversely, $R \subseteq \mathcal{F}(R)$ is the definition of being a dynamic relation. ∎

We need another simple fact.

Proposition 7 *The union of any family of dynamic relations is again a dynamic relation.*

Proof . Suppose that $\{R_i | i \in I\}$ is a family of dynamic relations. Let $R = \bigcup_i R_i$. Suppose that sRt, then, for some $j \in I$, sR_jt. If $s \xrightarrow{a} s'$ then, for some t', $t \xrightarrow{a} t'$ with $s'R_jt'$ and vice versa. Clearly $s'Rt'$ so we have that R is a dynamic relation. ∎

Note that the last proof is almost too trivial to write down.

Theorem 8 *The relations $\sim$ and $\sim_P$ are the same.*

Proof . The relation $\sim$ is, by definition, the union of all dynamic relations. By Prop. 6, this says that $\sim$ is the union (least upper bound) of all the prefixed points of $\mathcal{F}$. By the fixed-point theorem Thm. 16 it follows that $\sim$ is the greatest fixed point of $\mathcal{F}$. ∎

We note some important properties of dynamic relations without proof.

Proposition 9 *If R is a dynamic relation then so is R^{-1}, the relational converse. If R_1 and R_2 are dynamic relations then so is $R_1 \circ R_2$.*

In order to see that $\sim_M$ is the same as $\sim$ we will first *assume* a very important property of $\mathcal{F}$; later we will show that the assumption is justified.

Definition 10 *In a poset $(S, \leq)$ we say that a non-empty subset X is **filtered**, if whenever $x, y \in X$, there is a z with $z \leq x$ and $z \leq y$.*

A decreasing chain is obviously filtered. We will only need to deal with decreasing chains, but the general concept is worth knowing.

Definition 11 *We say that $f : L \longrightarrow L$ is **co-continuous** if whenever we have a filtered family $X \subseteq L$ then $f(\bigwedge X) = \bigwedge f(X)$.*

Proposition 12 *In an image-finite system $\mathcal{F}$ is co-continuous.*

We will prove this later. For the moment we note that it gives us the equivalence of the first two definitions of bisimulation immediately.

Theorem 13 *The relation $\sim_M$ is the greatest fixed point of $\mathcal{F}$.*

Proof . From the definition of the relations $\sim_n$ we have that $\sim_{n+1} = \mathcal{F}(\sim_n)$. Now we have

$$\mathcal{F}(\sim_M) = \mathcal{F}(\bigcap_n \sim_n) = \bigcap_n \mathcal{F}(\sim_n) = \bigcap_n \sim_{n+1} = \sim_M .$$

This shows that $\sim_M$ is a fixed point of $\mathcal{F}$. Let K be any other fixed point. Then clearly $K \subseteq \sim_0$. Now, by an obvious induction proof, $K \subseteq \sim_n$ for all n. Thus $K \subseteq \bigcap_n \sim_n = \sim_M$. Thus, $\sim_M$ is the greatest fixed point of $\mathcal{F}$. ∎

Thus all three definitions coincide. We need to complete the proof of co-continuity. This will be very close to the proof of the Hennessy-Milner theorem.

Proof (Of cocontinuity). In this proof each argument comes in identical pairs, one where $s \xrightarrow{a} s'$ and then we have to find a matching t' and vice versa as well. I will only show one case as the other is identical.

Suppose that $\{R_i | i \in I\}$ is a filtered family of relations. We write $R = \bigcap_i R_I$, $K_i = \mathcal{F}(R_i)$ and $K = \bigcap_i K_i$. We want to show that $K = \mathcal{F}(R)$. First we show that $\mathcal{F}(R) \subseteq K$. Suppose that $s\mathcal{F}(R)t$. Suppose further that $s \xrightarrow{a} s'$, then, by the definition of $\mathcal{F}(R)$ we have that there is some t' such that $t \xrightarrow{a} t'$ and $s'Rt'$. This means that $\forall i \in I.s'R_it'$ so (arguing similarly for the other case) we have $\forall i \in I.s\mathcal{F}(R_i)t$ or $\forall i \in I.(s,t) \in K_i$ and hence $(s,t) \in K$.

Now we assume that $\neg s\mathcal{F}(R)t$. Once again we have that there is some a, s' with $s \xrightarrow{a} s'$ and $\forall t'$, $t \xrightarrow{a} t' \Rightarrow \neg(s'Rt')$, i.e. $\exists R_j$ such that $\neg s'R_jt'$. Note, however, that the R_j can be different for each t' so we cannot immediately say that we are done. There are, however, only finitely many possible t' (image-finiteness), call them $t_1, \ldots, t_k$ and call the associated relations $R_1, \ldots, R_k$. Thus for each $j \in \{1, \ldots, k\}$, we have $t \xrightarrow{a} t_j$ and $\neg s'R_jt_j$. Of course, it could be that, for example, $s'R_7t_3$ so we cannot conclude anything just yet. However, the family of relations is filtered, by assumption, and the number of t_j is finite, so there has to be *one* relation, call it T, such that $\neg s'Tt_j$ for all the j. Thus we have that $\neg s\mathcal{F}(T)t$, but this means that there is some $R_l = T$ such that $(s,t) \notin K_l$, hence $(s,t) \notin K$. Thus, $K \subseteq \mathcal{F}(R)$. This concludes the proof of cocontinuity ∎

2 The Logical Characterization of Bisimulation

Consider the modal logic

$$\Phi ::== \mathsf{T} | \neg\phi | \phi_1 \wedge \phi_2 | \langle a \rangle \phi.$$

The meaning of $\langle a \rangle \phi$ is, $s \models \langle a \rangle \phi$ if there exists an s' such that $s \xrightarrow{a} s'$ with $s' \models \phi$.

Definition 14 *We define the relation of logical equivalence between states by*

$$s \approx t if \forall \phi \in \Phi,\ s \models \phi \Leftrightarrow t \models \phi.$$

The following important theorem is often called the Hennessy-Milner theorem. It was independently discovered by van Benthem slightly before Hennessy and Milner.

Theorem 15 *The relations $\sim$ and $\approx$ are the same.*

Proof . Suppose that $s \sim t$. We prove $s \approx t$ by induction on the structure of formulas. The base case is trivial. The boolean cases are almost trivial. Consider a formula of the form $\langle a \rangle \phi$ and suppose that we have proved the theorem for all formulas of lower complexity. Suppose that $s \models \langle a \rangle \phi$. Then there is an s' such that $s \xrightarrow{a} s'$ and $s' \models \phi$. Since $s \sim t$ we have that there is a t' with $t \xrightarrow{a} t'$ and $s' \sim t'$. By the induction hypothesis s', t' agree on all formulas of lower complexity. This implies that $t' \models \phi$ or, $t \models \langle a \rangle \phi$. This completes the induction.

For the other direction we will show that $\approx$ is a dynamic relation. Suppose that $s \approx t$ and that $s \xrightarrow{a} s'$. Suppose, for the sake of deriving a contradiction, that for all the t' such that $t \xrightarrow{a} t'$ that $s' \not\approx t'$. There are only finitely many such t'; call them t_i'. For each such t_i' there is a formula ϕ_i such that $s' \models \phi_i$ but $t_i' \not\models \phi_i$. Note that we really need the logic to include negation in order to claim this. Without negation, it might be the case that for some t_i' we have $t_i' \models \phi_i$ and $s' \not\models \phi_i$. Using negation we can replace ϕ_i by $\neg\phi_i$ and establish the claim that for each t_i' there is a formula ϕ_i such that $s' \models \phi_i$ and $t_i' \models \phi_i$.

Consider the formula $\phi \stackrel{def}{=} \bigwedge_i \phi_i$. We have $s' \models \phi$ but for any t_i' we have $t_i' \not\models \phi$. This means that $s \models \langle a \rangle \phi$ but $t \not\models \langle a \rangle \phi$. This contradicts the assumption that $s \approx t$. Thus there must be a t' with $s' \approx t'$. We have proved that $\approx$ is a dynamic relation so $s \sim t$. ∎

A Basic Fixed-Point Theory for Complete Lattices

Let L be a complete lattice: this means that *every* subset of L has a least upper bound. From this it follows that every subset has a greatest lower bound as well.

To see that every subset has a greatest lower bound we proceed as follows. Let L be a complete lattice and let $Q \subseteq L$. Let $P \subseteq L$ be the set of lower bounds of Q and let g be the least upper bound of P. Now every element of $q \in Q$ is an upper bound for P so $g \leq q$; thus, g is itself a lower bound of Q. By construction it is greater than any other lower bound of Q so it is the *greatest* lower bound of Q.

Note that "every" includes the empty set, so every complete lattice has a least and a greatest element. Of course, this by itself is not enough for a lattice to be a complete lattice.

Let $f : L \longrightarrow L$ be a monotone function. An element, x, of L such that $x \leq f(x)$ is called a *pre-fixed point* of f. We will show that the supremum of the pre-fixed points of f give the greatest fixed point of f.

Theorem 16 *There are greatest fixed points and least fixed points for f.*[1] *Furthermore the greatest fixed point is the supremum of all the prefixed points of f.*

Proof . Define $G = \{x | x \leq f(x)\}$ and $g = \bigvee G$; we know that g exists because L is a complete lattice. Now $\forall x \in G,\ x \leq g$, so, by monotonicity of f, $f(x) \leq f(g)$. Since $x \leq f(x) \leq f(g)$ it follows that $f(g)$ is an upper bound of G, hence it is bigger than the least upper bound, g: i.e. $g \leq f(g)$. Then, again by monotonicity of f, $f(g) \leq f(f(g))$. This means that $f(g) \in G$, hence $f(g) \leq g$. Thus, we have $g = f(g)$; g is a fixed point of f. Now if h is any fixed point of h we have $h \leq f(h)$ so $h \in G$. Thus $h \leq g$, i.e. g is the greatest fixed point of f. The obvious dualization of this argument shows that f has a least fixed point. ∎

[1] Contrary to what you may read in textbooks, this is **not** the Knaester-Tarski fixed point theorem. That theorem says that the fixed points of f form a complete lattice.