Reachability has a last step

Rajeev Joshi and K. Rustan M. Leino

13 June 1997

Digital Equipment Corporation Systems Research Center
130 Lytton Ave., Palo Alto, CA 94301, U.S.A.
{rjoshi, rustan}@pa.dec.com

Greg Nelson defined a *reachability predicate* and gave eight axioms about it [0]. He proved the axioms sound with respect to a model, but it is not known whether the axioms are complete. In working with the reachability predicate, we noticed we were making use of a ninth property. If the eight axioms were complete, the ninth property would follow from the eight axioms. We have not shown this to be the case in general, but we show in this note that, for *finite* domains, the ninth property follows from the eight axioms and mathematical induction.

The reachability predicate is written

$$x \xrightarrow[z]{f} y$$

where f is a function and x, y, and z are elements in the domain of f. The predicate is pronounced "x reaches y via f avoiding z". Its standard model of interpretation is that some number of applications of f to x, none of which is applied to z, yields y; in symbols,

$$\langle \exists n \rhd f^n.x = y \wedge \langle \forall m \mid m < n \rhd f^m.x \neq z \rangle \rangle \quad ,$$

where m and n range over the natural numbers. However, we will not appeal to this model directly. Instead, we will confine our attention to eight axioms, given below.

The "ninth property" to which we alluded is:

$$x \xrightarrow[z]{f} y \;\equiv\; x = y \vee \langle \exists u \rhd x \xrightarrow[z]{f} u \wedge u \neq z \wedge f.u = y \rangle \quad . \tag{0}$$

The right-hand side of this property says that either x and y are equal, or there is a last hop in the path from x to y. As we will show in this note, the $\Leftarrow$ direction of the equivalence (0) follows from Greg Nelson's eight axioms. We will also show that the $\Rightarrow$ direction follows from the axioms if the domain of f is finite. We do not know if the $\Rightarrow$ direction follows from the eight axioms if the domain of f is infinite.

Although it's a pity we haven't proved anything about the $\Rightarrow$ direction of (0) for infinite domains, the restriction to finite domains is for our purposes not totally unreasonable. The primary application of the reachability predicate that we have in mind (as did Greg Nelson in 1983) is reasoning about whether or not an object y can be reached from an object x by applications of an object field f, which is really a map from objects to objects. (For this application, z is usually the special object **nil**.) At any time in the execution of a program, the number of allocated objects is finite; hence, so is the domain of f.

Greg Nelson's eight axioms are:

$$u \xrightarrow[x]{f} v \;\equiv\; u = v \vee (u \neq x \wedge f.u \xrightarrow[x]{f} v) \tag{1}$$

$$u \xrightarrow[x]{f} v \wedge v \xrightarrow[x]{f} w \;\Rightarrow\; u \xrightarrow[x]{f} w \tag{2}$$

$$u \xrightarrow[x]{f} v \;\Rightarrow\; u \xrightarrow{f} v \tag{3}$$

$$u \xrightarrow[y]{f} x \wedge u \xrightarrow[z]{f} y \;\Rightarrow\; u \xrightarrow[z]{f} x \tag{4}$$

$$u \xrightarrow{f} x \vee u \xrightarrow{f} y \;\Rightarrow\; u \xrightarrow[y]{f} x \vee u \xrightarrow[x]{f} y \tag{5}$$

$$u \xrightarrow[y]{f} x \wedge u \xrightarrow[z]{f} y \;\Rightarrow\; x \xrightarrow[z]{f} y \tag{6}$$

$$f.u \xrightarrow{f} v \;\equiv\; f.u \xrightarrow[u]{f} v \tag{7}$$

$$u \xrightarrow[x,p]{f(p:=q)} v \;\equiv\; u \xrightarrow[x,p]{f} v \tag{8}$$

Each axiom is implicitly universally quantified over all alphabetical symbols occurring in it. The axioms make use of two shorthands for the reachability predicate. First, leaving out the element under the arrow is a shorthand for putting the right-hand side of the arrow there:

$$x \xrightarrow{f} y \;\equiv\; x \xrightarrow[y]{f} y \qquad . \tag{9}$$

Second, writing more than one element under the arrow is a shorthand for writing a conjunction of reachability predicates:

$$x \xrightarrow[z,w]{f} y \;\equiv\; x \xrightarrow[z]{f} y \;\wedge\; x \xrightarrow[w]{f} y \qquad . \tag{10}$$

The axioms also mention the *function update operator*, written $f(x := y)$, where f is a function and x and y are elements. Function $f(x := y)$ is like f, except at x where it yields y. Formally,

$$f(u := v).u = v \;\wedge\; \langle\, \forall x \;|\; x \neq u \;\triangleright\; f(u := v).x = f.x \,\rangle \qquad . \tag{11}$$

Let us now prove the following theorem, the $\Leftarrow$ direction of property (0):

Theorem. For any f, x, y, and z,

$$x \xrightarrow[z]{f} y \;\Leftarrow\; x = y \;\vee\; \langle\, \exists u \;\triangleright\; x \xrightarrow[z]{f} u \;\wedge\; u \neq z \;\wedge\; f.u = y \,\rangle \tag{12}$$

Proof. First, note that by axiom (1), the relation $\xrightarrow[z]{f}$ is reflexive. Thus, the left-hand side of (12) follows from the disjunct $x = y$. Focusing now on the other disjunct, we calculate, for any u,

$$\begin{array}{ll}
 & x \xrightarrow[z]{f} u \;\wedge\; u \neq z \;\wedge\; f.u = y \\
\Rightarrow & \quad \{\; \text{axiom (1): } \xrightarrow[z]{f} \text{ is reflexive} \;\} \\
 & x \xrightarrow[z]{f} u \;\wedge\; u \neq z \;\wedge\; f.u \xrightarrow[z]{f} y \\
\Rightarrow & \quad \{\; \text{axiom (1): } u \neq z \;\wedge\; f.u \xrightarrow[z]{f} y \;\Rightarrow\; u \xrightarrow[z]{f} y \;\} \\
 & x \xrightarrow[z]{f} u \;\wedge\; u \xrightarrow[z]{f} y \\
\Rightarrow & \quad \{\; \text{axiom (2): transitivity of } \xrightarrow[z]{f} \;\} \\
 & x \xrightarrow[z]{f} y \qquad .
\end{array}$$

□

Before getting to the $\Rightarrow$ direction of (0), it will be useful to prove three lemmas.

Lemma. For any f, x, y, and z,

$$x \neq y \;\Rightarrow\; (x \xrightarrow[z]{f} y \;\equiv\; x \neq z \;\wedge\; f.x \xrightarrow[z]{f} y) \qquad . \tag{13}$$

Proof. Under the antecedent, we calculate,

$$
\begin{array}{ll}
 & x \xrightarrow[z]{f} y \\
\equiv & \quad \{ \text{ axiom (1) } \} \\
 & x = y \ \vee \ (x \neq z \ \wedge \ f.x \xrightarrow[z]{f} y) \\
\equiv & \quad \{ \ x \neq y \ \} \\
 & x \neq z \ \wedge \ f.x \xrightarrow[z]{f} y \qquad .
\end{array}
$$

□

The next two lemmas are in some sense generalizations of axioms (7) and (8), respectively.

Lemma. For any f, b, x, and w,

$$f.b = x \ \wedge \ x \neq w \ \Rightarrow \ (f.x \xrightarrow{f} w \ \equiv \ f.x \xrightarrow[b]{f} w) \qquad . \tag{14}$$

Proof. Under the antecedent, we calculate,

$$
\begin{array}{ll}
 & f.x \xrightarrow[b]{f} w \\
\Rightarrow & \quad \{ \text{ axiom (3) } \} \\
 & f.x \xrightarrow{f} w \\
\equiv & \quad \{ \ x \neq w \ \} \\
 & x = w \ \vee \ (x \neq w \ \wedge \ f.x \xrightarrow{f} w) \\
\equiv & \quad \{ \text{ axiom (1) and shorthand (9) } \} \\
 & x \xrightarrow{f} w \\
\equiv & \quad \{ \text{ axiom (7), since } x = f.b \ \} \\
 & x \xrightarrow[b]{f} w \\
\equiv & \quad \{ \text{ lemma (13), since } x \neq w \ \} \\
 & x \neq b \ \wedge \ f.x \xrightarrow[b]{f} w \\
\Rightarrow & \\
 & f.x \xrightarrow[b]{f} w \qquad .
\end{array}
$$

□

Lemma. For any f, b, x, w, and z,

$$f.b = x \ \wedge \ x \neq w \ \Rightarrow \ (f.x \xrightarrow[z]{f} w \ \equiv \ f.x \xrightarrow[z]{f(b:=f.x)} w) \tag{15}$$

Proof. Under the antecedent, we calculate,

$$
\begin{array}{ll}
 & f.x \xrightarrow[z]{f} w \\
\equiv & \quad \{ \text{ shorthand (10); and lemma (14), since } f.b = x \ \wedge \ x \neq w \ \} \\
 & f.x \xrightarrow[z,b]{f} w \\
\equiv & \quad \{ \text{ axiom (8) } \} \\
 & f.x \xrightarrow[z,b]{f(b:=f.x)} w \\
\equiv & \quad \{ \text{ shorthand (10); and axiom (7), since } f(b := f.x).b = f.x \ \} \\
 & f.x \xrightarrow[z]{f(b:=f.x)} w \qquad .
\end{array}
$$

□

The rest of this note concerns the proof of the $\Rightarrow$ direction of property (0) for finite domains:

Theorem. For any f, x, y, and z, where the size of the domain of f is finite,

$$x \xrightarrow[z]{f} y \ \Rightarrow \ x = y \ \vee \ \langle \exists u \triangleright x \xrightarrow[z]{f} u \ \wedge \ u \neq z \ \wedge \ f.u = y \rangle \qquad . \tag{16}$$

Proof. The proof is by induction on the size of the domain of f.

If the size of the domain of f is 0, the theorem holds vacuously. If the size of the domain is 1, the disjunct $x = y$ in the consequent holds trivially, and thus so does the theorem.

From now on, we consider an f with a domain with at least 2 elements; call it S. We will prove the induction step by proving

$$\langle \exists u \triangleright x \xrightarrow[z]{f} u \ \wedge \ u \neq z \ \wedge \ f.u = y \rangle \tag{17}$$

under the assumptions

$$x \xrightarrow[z]{f} y \tag{18}$$

and

$$x \neq y \qquad . \tag{19}$$

Let's start with an observation: From the givens (18) and (19) and lemma (13), we have

$$x \neq z \ \wedge \ f.x \xrightarrow[z]{f} y \qquad . \tag{20}$$

From (20), we see that we're done if $f.x = y$, for then (17) holds with x for u. Hence, let's assume

$$f.x \neq y \qquad . \tag{21}$$

So that we can apply the induction hypothesis, we define a smaller domain, a function on that domain, and a mapping from S to the smaller domain. Let S' denote $S \setminus \{x\}$. As the mapping of elements, we define a function $\overline{\ } : S \to S'$ as follows: for any element $e \in S$,

$$\overline{e} \;=\; \begin{cases} e & \text{if } e \neq x \\ f.x & \text{if } e = x \end{cases} \tag{22}$$

To show that $\overline{e}$ is indeed in S', we must show $f.x \in S'$. We calculate, beginning from the second conjunct of (20),

$$\begin{array}{ll} & f.x \xrightarrow[z]{f} y \\ \Rightarrow & \quad \{ \text{ axiom (3) } \} \\ & f.x \xrightarrow{f} y \\ \equiv & \quad \{ \text{ axiom (7) } \} \\ & f.x \xrightarrow[x]{f} y \\ \equiv & \quad \{ \text{ lemma (13), since (21): } f.x \neq y \ \} \\ & f.x \neq x \ \wedge \ f.(f.x) \xrightarrow[x]{f} y \\ \Rightarrow & \\ & f.x \neq x \qquad . \end{array} \tag{23}$$

From (19) and (20) and definition (22), we have

$$\overline{x} = f.x \ \wedge \ \overline{y} = y \ \wedge \ \overline{z} = z \qquad . \tag{24}$$

Consequently, from (21), we also have

$$\overline{x} \neq \overline{y} \qquad . \tag{25}$$

Finally, for every element $e \in S'$, we define function $f' : S' \to S'$ by

$$f'.e \;=\; \overline{f.e} \qquad . \tag{26}$$

From the induction hypothesis, we have

$$\overline{x} \xrightarrow[\overline{z}]{f'} \overline{y} \;\Rightarrow\; \overline{x} = \overline{y} \;\vee\; \langle\, \exists\, u \;\mid\; u \in S' \;\triangleright\; \overline{x} \xrightarrow[\overline{z}]{f'} u \;\wedge\; u \neq \overline{z} \;\wedge\; f'.u = \overline{y} \,\rangle \quad . \tag{27}$$

Our plan is to show the antecedent of (27). By (25), we then have the existential quantification, from which we will later dismiss our proof obligation (17). We will make use of the following lemma, which we will prove later: for any w,

$$x \neq w \;\Rightarrow\; (f.x \xrightarrow[z]{f'} w \;\equiv\; x \xrightarrow[z]{f} w) \qquad . \tag{28}$$

Here's the proof of the antecedent of (27):

$$\begin{array}{ll} & \overline{x} \xrightarrow[\overline{z}]{f'} \overline{y} \\ \equiv & \quad \{ \quad (24) \quad \} \\ & f.x \xrightarrow[z]{f'} y \\ \equiv & \quad \{ \quad \text{lemma (28), since (19): } x \neq y \quad \} \\ & x \xrightarrow[z]{f} y \\ \equiv & \quad \{ \quad (18) \quad \} \\ & true \qquad . \end{array}$$

Having established the antecedent of (27), the consequent of (27) and (25) gives us:

$$\langle\, \exists\, u \;\mid\; u \in S' \;\triangleright\; \overline{x} \xrightarrow[\overline{z}]{f'} u \;\wedge\; u \neq \overline{z} \;\wedge\; f'.u = \overline{y} \,\rangle \qquad . \tag{29}$$

Before massaging this formula, we do a little calculation, from which we will conclude, for any $e \in S'$,

$$f'.e = y \;\Rightarrow\; f.e = y \qquad . \tag{30}$$

Here's the calculation: for any $e \in S'$,

$$\begin{array}{ll} & f'.e = y \\ \equiv & \quad \{ \quad (26)\text{: definition of } f' \quad \} \\ & \overline{f.e} = y \\ \equiv & \quad \{ \quad (22)\text{: definition of } {}^{-} \quad \} \\ & (f.e \neq x \;\wedge\; f.e = y) \;\vee\; (f.e = x \;\wedge\; f.x = y) \\ \equiv & \quad \{ \quad (21)\text{: } f.x \neq y \quad \} \\ & f.e \neq x \;\wedge\; f.e = y \\ \Rightarrow & \\ & f.e = y \qquad . \end{array}$$

Now we are ready to massage (29):

$$
\begin{array}{ll}
 & \langle\, \exists\, u \;\mid\; u \in S' \;\triangleright\; \overline{x} \xrightarrow[\overline{z}]{f'} u \;\wedge\; u \neq \overline{z} \;\wedge\; f'.u = \overline{y} \,\rangle \\
\equiv & \quad \{\;\; (24) \;\;\} \\
 & \langle\, \exists\, u \;\mid\; u \in S' \;\triangleright\; f.x \xrightarrow[z]{f'} u \;\wedge\; u \neq z \;\wedge\; f'.u = y \,\rangle \\
\Rightarrow & \quad \{\;\; (30) \;\;\} \\
 & \langle\, \exists\, u \;\mid\; u \in S' \;\triangleright\; f.x \xrightarrow[z]{f'} u \;\wedge\; u \neq z \;\wedge\; f.u = y \,\rangle \\
\equiv & \quad \{\;\; \text{lemma (28), since } (u \in S' \;\wedge\; x \notin S' \text{ which implies) } u \neq x \;\;\} \\
 & \langle\, \exists\, u \;\mid\; u \in S' \;\triangleright\; x \xrightarrow[z]{f} u \;\wedge\; u \neq z \;\wedge\; f.u = y \,\rangle \\
\Rightarrow & \\
 & \langle\, \exists\, u \;\triangleright\; x \xrightarrow[z]{f} u \;\wedge\; u \neq z \;\wedge\; f.u = y \,\rangle \qquad .
\end{array}
$$

We have now arrived at our proof obligation (17), but during our journey we incurred an obligation to establish lemma (28). Hence, for any w that satisfies

$$x \neq w \qquad , \tag{31}$$

we calculate,

$$
\begin{array}{ll}
 & x \xrightarrow[z]{f} w \\
\equiv & \quad \{\;\; \text{lemma (13), since (31): } x \neq w \;\;\} \\
 & x \neq z \;\wedge\; f.x \xrightarrow[z]{f} w \\
\equiv & \quad \{\;\; (20)\text{: } x \neq z \;\;\} \\
 & f.x \xrightarrow[z]{f} w \qquad .
\end{array}
$$

This calculation reduces the proof of lemma (28) to the proof of:

$$f.x \xrightarrow[z]{f} w \;\equiv\; f.x \xrightarrow[z]{f'} w \qquad . \tag{32}$$

The function update operator gives us a way to write f' in term of f. An inspection of the definition of f' (26) and $\overline{}$ (22) leads us to the assertion

$$f' \;=\; f(b_0 := f.x)(b_1 := f.x) \cdots (b_{n-1} := f.x) \qquad , \tag{33}$$

where $b_0, b_1, \ldots, b_{n-1}$ are the "f-predecessors" of x, that is, the values from which one application of f yields x. Using formulation (33), equation (32) can be written as

$$f.x \xrightarrow[z]{f} w \;\equiv\; f.x \xrightarrow[z]{f(b_0:=f.x)(b_1:=f.x)\cdots(b_{n-1}:=f.x)} w \qquad . \tag{34}$$

We define a function g_j for every j satisfying $0 \leq j \leq n$:

$$\begin{array}{lcl} g_0 & = & f \\ g_{j+1} & = & g_j(b_j := f.x) \quad \text{for } j : 0 \leq j < n \end{array} \quad .$$

Thus, $g_0 = f$ and $g_n = f'$, and for each j satisfying $0 \leq j < n$,

$$g_j.x = f.x \ \wedge \ g_j.b_j = f.b_j = x \quad . \tag{35}$$

The first conjunct of (35) holds because x is not an f-predecessor of itself (23).

Equation (34) now follows from n applications of lemma (15): For each j satisfying $0 \leq j < n$, lemma (15) yields

$$f.x \xrightarrow[z]{g_j} w \ \equiv \ f.x \xrightarrow[z]{g_{j+1}} w \quad ,$$

because of the properties about g_j (35) and $x \neq w$ (31).

This concludes the proof.

□

We can actually strengthen the term of the existential quantification of property (0):

Corollary. For any f, x, y, and z, where the size of the domain of f is finite,

$$x \xrightarrow[z]{f} y \ \equiv \ x = y \vee \langle \exists u \triangleright x \xrightarrow[y,z]{f} u \wedge u \neq z \wedge u \neq y \wedge f.u = y \rangle \quad . \tag{36}$$

Proof. The $\Leftarrow$ direction of (36) follows directly from theorem (12), since the right-hand side of (36) is stronger than the right-hand side of (12).

For the $\Rightarrow$ direction, it suffices to show

$$\langle \exists u \triangleright x \xrightarrow[y,z]{f} u \wedge u \neq z \wedge u \neq y \wedge f.u = y \rangle \tag{37}$$

under the assumption

$$x \xrightarrow[z]{f} y \wedge x \neq y \quad . \tag{38}$$

From the first conjunct of (38), we calculate,

$$\begin{array}{ll} & x \xrightarrow[z]{f} y \\ \Rightarrow & \quad \{ \ \text{axiom (3); and shorthand (9)} \ \} \end{array}$$

$$
\begin{array}{ll}
 & x \xrightarrow[y]{f} y \\
\Rightarrow & \quad \{ \ \text{theorem (16), with } z := y \ \} \\
 & x = y \ \vee \ \langle \exists u \rhd x \xrightarrow[y]{f} u \ \wedge \ u \neq y \ \wedge \ f.u = y \rangle \\
\equiv & \quad \{ \ (38)\text{: } x \neq y \ \} \\
 & \langle \exists u \rhd x \xrightarrow[y]{f} u \ \wedge \ u \neq y \ \wedge \ f.u = y \rangle \qquad . \qquad (39)
\end{array}
$$

Our proof obligation (37) follows from (39) and

$$\langle \forall u \rhd x \xrightarrow[y]{f} u \ \wedge \ u \neq y \ \wedge \ f.u = y \ \Rightarrow \ x \xrightarrow[z]{f} u \ \wedge \ u \neq z \rangle \qquad .$$

To take care of this last proof obligation, we calculate, for any u,

$$
\begin{array}{ll}
 & x \xrightarrow[y]{f} u \ \wedge \ u \neq y \ \wedge \ f.u = y \\
\Rightarrow & \quad \{ \ \text{drop third conjunct; and (38): } x \xrightarrow[z]{f} y \ \} \\
 & x \xrightarrow[y]{f} u \ \wedge \ x \xrightarrow[z]{f} y \ \wedge \ u \neq y \\
\Rightarrow & \quad \{ \ \text{axioms (4) and (6)} \ \} \\
 & x \xrightarrow[z]{f} u \ \wedge \ u \xrightarrow[z]{f} y \ \wedge \ u \neq y \\
\equiv & \quad \{ \ \text{lemma (13), since } u \neq y \ \} \\
 & x \xrightarrow[z]{f} u \ \wedge \ u \neq z \ \wedge \ f.u \xrightarrow[z]{f} y \ \wedge \ u \neq y \\
\Rightarrow & \\
 & x \xrightarrow[z]{f} u \ \wedge \ u \neq z \qquad .
\end{array}
$$

□

Acknowledgements. Jim Saxe proved lemma (14).

References

[0] Greg Nelson. Verifying reachability invariants of linked structures. *Conference Record of the Tenth Annual ACM Symposium on Principles of Programming Languages, Austin, Texas, January 1983*, pages 38–47, January 1983.