Proving Unless Properties by Parts

Notes on UNITY: 09-89

Jayadev Misra*

Department of Computer Sciences

The University of Texas at Austin

Austin, Texas 78712

(512) 471-9547

misra@cs.utexas.edu

6/19/89

Consider a property of the form

$$p(x,y) \text{ unless } q(x,y) \tag{1}$$

where x, y are program variables.

We show that if the values of x, y are not simultaneously changed—this property is stated formally below—then (1) can be proven in two parts, replacing x by a free variable and replacing y by a free variable, i.e., by proving

$$p(m,y) \text{ unless } q(m,y) \tag{2}$$

and

$$p(x,n) \text{ unless } q(x,n) \tag{3}$$

where m is free in (2) and n is free in (3).

The fact that x, y are not simultaneously changed can be written as,

$$(x,y) = (m,n) \text{ unless } (x \neq m \ \wedge \ y = n) \ \vee \ (x = m \ \wedge \ y \neq n) \tag{4}$$

Now we show that (1) can be deduced from (2,3,4). Conjunction of (3,4) yields

$$\begin{array}{l} p(x,n) \wedge (x,y) = (m,n) \text{ unless} \\ \qquad (p(x,n) \ \wedge \ x \neq m \ \wedge \ y = n) \vee \\ \qquad (p(x,n) \ \wedge \ x = m \ \wedge \ y \neq n) \vee \\ \qquad (q(x,n) \ \wedge \ x = m \ \wedge \ y = n) \vee \\ \qquad (q(x,n) \ \wedge \ x \neq m \ \wedge \ y = n) \vee \\ \qquad (q(x,n) \ \wedge \ x = m \ \wedge \ y \neq n) \end{array}$$

The lhs is equivalent to

$$p(x,y) \ \wedge \ (x,y) = (m,n)$$

*This work was partially supported by ONR Contracts N00014-87-K-0510 and N00014-86-0763 and by a grant from the John Simon Guggenheim Foundation.

The rhs implies

$$\begin{aligned}&(p(x,y)\ \wedge\ (x,y)\neq(m,n))\ \vee\\&([p(x,n)\ \vee\ q(x,n)]\ \wedge\ x=m\ \wedge\ y\neq n)\ \vee\\&q(x,y)\end{aligned}$$

So we deduce

$$\begin{aligned}&p(x,y)\ \wedge\ (x,y)=(m,n)\ \textit{unless}\\&\qquad(p(x,y)\ \wedge\ (x,y)\neq(m,n))\ \vee\\&\qquad([p(x,n)\ \vee\ q(x,n)]\ \wedge\ x=m\ \wedge\ y\neq n)\ \vee\\&\qquad q(x,y)\end{aligned}\tag{5}$$

Working with (2,4), we similarly deduce

$$\begin{aligned}&p(x,y)\ \wedge\ (x,y)=(m,n)\ \textit{unless}\\&\qquad(p(x,y)\ \wedge\ (x,y)\neq(m,n))\ \vee\\&\qquad([p(m,y)\ \vee\ q(m,y)]\ \wedge\ x\neq m\ \wedge\ y=n)\ \vee\\&\qquad q(x,y)\end{aligned}\tag{6}$$

Taking conjunction of (5,6) and simplifying

$$p(x,y)\ \wedge\ (x,y)=(m,n)\ \textit{unless}\ [p(x,y)\ \wedge\ (x,y)\neq(m,n)]\ \vee\ q(x,y)$$

Taking disjunction of the above over all m, n (see *Notes on Unity 01-88* for the general disjunction rule) yields

$$\begin{aligned}&p(x,y)\ \textit{unless}\\&\qquad\langle\forall\ m,n\ ::\ \neg p(x,y)\ \vee\ (x,y)\neq(m,n)\ \vee\\&\qquad\qquad\qquad[p(x,y)\ \wedge\ (x,y)\neq(m,n)]\ \vee q(x,y)\\&\qquad\rangle\\&\quad\wedge\ \langle\exists\ m,n\ ::\ [p(x,y)\ \wedge\ (x,y)\neq(m,n)]\vee q(x,y)\rangle\end{aligned}$$

Simplifying the first term in the rhs and weakening the second term—by removing $(x,y)\neq(m,n)$ from it—we obtain

$$\begin{aligned}&p(x,y)\ \textit{unless}\\&\langle\forall\ m,n\ ::\ \neg p(x,y)\ \vee\ (x,y)\neq(m,n)\ \vee\ q(x,y)\rangle\ \wedge\\&\langle\exists\ m,n\ ::\ p(x,y)\ \vee\ q(x,y)\rangle\end{aligned}$$

Simplifying the terms in the rhs,

$$\begin{aligned}&p(x,y)\ \textit{unless}\\&\qquad[\neg p(x,y)\ \vee\ q(x,y)\ \vee\ \langle\forall\ m,n\ ::\ (x,y)\neq(m,n)\rangle]\ \wedge\ [p(x,y)\ \vee\ q(x,y)]\end{aligned}$$

We have as an axiom $\langle\exists\ m,n\ ::\ (x,y)=(m,n)\rangle$. Hence the rhs can be simplified.

$$\begin{aligned}&p(x,y)\ \textit{unless}\ [\neg p(x,y)\ \vee\ q(x,y)]\ \wedge\ [p(x,y)\ \vee\ q(x,y)]\\\text{i.e.,}\ \ &p(x,y)\ \textit{unless}\ q(x,y)\end{aligned}$$

□