Methodological Hints About Constructing *unless* Properties

Notes on UNITY: 27-91

Jayadev Misra*

Department of Computer Sciences

The University of Texas at Austin

Austin, Texas 78712

(512) 471-9547

misra@cs.utexas.edu

12/19/91

A typical informal description from which an *unless* property is to be constructed is the following: If process x and process y are both waiting then both will continue waiting until y stops waiting. Denoting by xw and yw that x, y are waiting, respectively, the above requirement can be translated to Hoare-triples,

for any transition S : $\{xw \wedge yw\}\ S\ \{xw\}$

Note: The informal description is confusing. A possible interpretation is to allow the postcondition, $xw \vee \neg yw$, i.e., allow for both processes to stop waiting simultaneously. □

An unless property can be constructed from the above triple as follows (see Exercise 3.8 in [**?**]). Given that

$(\forall\ S\ ::\ \{u\}\ S\ \{v\})$

We can assert p *unless* q for *any* p, q satisfying:

- $u \Rightarrow p \Rightarrow v$,
- $q \equiv \neg u \wedge v$

These observations are justified by solving

$u \equiv p \wedge \neg q$ and $v \equiv p \vee q$

for p, q.

Note: The given conditions show that we cannot deal with a triple $\{u\}\ S\ \{v\}$ where u does not imply v. □

Applying to the given example, obtain from $\{xw \wedge yw\}\ S\ \{xw\}$

$$xw \wedge yw \Rightarrow p \Rightarrow xw$$

and $q \equiv \neg(xw \wedge yw) \wedge xw$
$\equiv \neg yw \wedge xw$

*This material is based in part upon work supported by the Texas Advanced Research Program under Grant No. 003658–065, by the Office of Naval Research Contract N00014-90-J-1640 and by the National Science Foundation Award CCR–9111912.

A simple choice for p is, xw.

Similarly, $\{xw \ \wedge \ yw\}$ S $\{xw \ \vee \ \neg yw\}$ can be translated to

$$xw \textit{ unless } \neg(xw \ \wedge \ yw) \ \wedge \ (xw \ \vee \ \neg yw)$$
$$\text{i.e., } xw \textit{ unless } \neg yw$$

Two Simplifications:

The following identities (see Exercise 3.7.2 in [**?**]) are often useful for simplifications.

$$p \textit{ unless } q \quad \equiv \quad p \ \wedge \ \neg q \ \ \textit{unless } q$$
$$p \textit{ unless } q \quad \equiv \quad p \ \vee \ q \ \ \textit{unless } q$$

The first identity suggests that we may start by defining an *unless* whose left and right sides are disjoint (i.e., $p \ \wedge \ \neg q$ and q); then, manipulate it to a simpler form. Since the informal meaning of p *unless* q is that, once p holds it continues to hold until q holds, it may be simpler to translate informally stated properties to an *unless* when p, q do not hold simultaneously.