General Conjunction and Disjunction Rules for *unless*

Notes on UNITY: 01-88

Jayadev Misra*
Department of Computer Sciences
The University of Texas at Austin
Austin, Texas 78712
(512) 471-9547
misra@cs.utexas.edu

9/14/88

1 The Rules

The conjunction and disjunction rules for *unless*, as given in [1], are as follows.

$$\frac{p \text{ unless } q \ , \ p' \text{ unless } q'}{\begin{array}{llll} p \wedge p' & \text{unless} & (p \wedge q') \vee (p' \wedge q) \vee (q \wedge q') & \{\text{conjunction}\} \\ p \vee p' & \text{unless} & (\neg p \wedge q') \vee (\neg p' \wedge q) \vee (q \wedge q') & \{\text{disjunction}\} \end{array}}$$

The generalizations of these rules to arbitrary—possibly infinite—sets of *unless* properties is the subject of this note. These generalizations were discovered independently by Ernie Cohen [2] and Carel S. Scholten [4]. In the following, i is a dummy variable that takes on values from an arbitrary set and $p.i, q.i$ are predicates in which i is free.

$$\frac{\langle \forall\ i\ ::\ p.i \text{ unless } q.i \rangle}{\begin{array}{llll} \langle \forall\ i\ ::\ p.i \rangle & \text{unless} & \langle \forall\ i\ ::\ p.i \vee q.i \rangle \ \wedge\ \langle \exists\ i\ ::\ q.i \rangle & \{\text{conjunction}\}, \\ \langle \exists\ i\ ::\ p.i \rangle & \text{unless} & \langle \forall\ i\ ::\ \neg p.i \vee q.i \rangle \ \wedge\ \langle \exists\ i\ ::\ q.i \rangle & \{\text{disjunction}\} \end{array}}$$

2 Proofs of the Rules

In a program we have the restriction that every statement is deterministic and execution of any statement in any program state terminates. Then we have,

$$\frac{\langle \forall\ i\ ::\ \{p.i\}\ \ s\ \ \{q.i\} \rangle}{\begin{array}{lll} \{\langle \forall\ i\ ::\ p.i \rangle\} & s & \{\langle \forall\ i\ ::\ q.i \rangle\}\ , \\ \{\langle \exists\ i\ ::\ p.i \rangle\} & s & \{\langle \exists\ i\ ::\ q.i \rangle\} \end{array}} \tag{1}$$

(These facts can be justified by observing that for any s, the weakest precondition function, $wp.s$, is positively conjunctive, and for deterministic s, $wp.s$ is universally disjunctive. For details see Dijkstra and Scholten [3].)

Furthermore, we have

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

$$\frac{p \;\Rightarrow\; p' \;,\; \{p'\} \;\; s \;\; \{q'\} \;,\; q' \;\Rightarrow\; q}{\{p\} \;\; s \;\; \{q\}} \tag{2}$$

2.1 Proof of the Conjunction Rule

We are given,

$\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ q.i \rangle$

i.e., $\langle \forall\ i\ ::$
$\quad\langle \forall\ s\ ::\ \{p.i\ \wedge\ \neg q.i\}\ \ s\ \ \{p.i\ \vee\ q.i\}\rangle$
$\rangle$

We consider an arbitrary statement s in the following proof. Applying (1) we deduce,

$$\{\langle \forall\ i\ ::\ p.i\ \wedge\ \neg q.i\rangle\}\ \ s\ \ \{\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\}$$

We are required to show

$$\langle \forall\ i\ ::\ p.i\rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\ \wedge\ \langle \exists\ i\ ::\ q.i\rangle$$

That is, for statement s,

$$\begin{array}{l} \{\langle \forall\ i\ ::\ p.i\rangle \wedge \neg[\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\ \wedge\ \langle \exists\ i\ ::\ q.i\rangle]\} \\ \qquad\qquad s \\ \{\langle \forall\ i\ ::\ p.i\rangle\ \vee\ [\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\ \wedge\ \langle \exists\ i\ ::\ q.i\rangle]\} \end{array}$$

Using (2), it is sufficient to show

$$\begin{array}{ll} & \langle \forall\ i\ ::\ p.i\rangle\ \wedge\ \neg[\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\ \wedge\ \langle \exists\ i\ ::\ q.i\rangle] \\ \Rightarrow & \langle \forall\ i\ ::\ p.i\ \wedge\ \neg q.i\rangle \end{array} \tag{3}$$

and,

$$\begin{array}{ll} & \langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle \\ \Rightarrow & \langle \forall\ i\ ::\ p.i\rangle\ \vee\ [\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\ \wedge\ \langle \exists\ i\ ::\ q.i\rangle] \end{array} \tag{4}$$

Proof of (3)

$$\begin{array}{ll} & \text{antecedent of (3)} \\ = & \{\text{using deMorgan}\} \\ & \langle \forall\ i\ ::\ p.i\rangle\ \wedge\ [\neg\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle\ \vee\ \langle \forall\ i\ ::\ \neg q.i\rangle] \\ = & \{\text{distributing} \wedge \text{over} \vee\} \\ & [\langle \forall\ i\ ::\ p.i\rangle\ \wedge\ \neg\langle \forall\ i\ ::\ p.i\ \vee\ q.i\rangle]\ \vee\ [\langle \forall\ i\ ::\ p.i\rangle\ \wedge\ \langle \forall\ i\ ::\ \neg q.i\rangle] \\ = & \{\text{the first term is } \mathit{false}\text{; combining the conjuncts in the second term}\} \\ & \langle \forall\ i\ ::\ p.i\ \wedge\ \neg q.i\rangle \end{array}$$

Proof of (4)

$$
\begin{array}{ll}
& \text{antecedent of (4)} \\
= & \{\text{idempotence of } \wedge\} \\
& \langle \forall\ i\ ::\ p.i\ \vee\ q.i \rangle\ \wedge\ \langle \forall\ i\ ::\ p.i\ \vee\ q.i \rangle \\
\Rightarrow & \{\text{weakening the second term}\} \\
& \langle \forall\ i\ ::\ p.i\ \vee\ q.i \rangle\ \wedge\ [\langle \forall\ i\ ::\ p.i \rangle\ \vee\ \langle \exists\ i\ ::\ q.i \rangle] \\
= & \{\text{distributing } \wedge \text{ over } \vee\} \\
& [\langle \forall\ i\ ::\ p.i\ \vee\ q.i \rangle\ \wedge\ \langle \forall\ i\ ::\ p.i \rangle]\ \vee\ [\langle \forall\ i\ ::\ p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle] \\
= & \{\text{simplifying the first term}\} \\
& \langle \forall\ i\ ::\ p.i \rangle\ \vee\ [\langle \forall\ i ::\ p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]
\end{array}
$$

2.2 Proof of the Disjunction Rule

The structure of the proof is similar to that for the conjunction rule. For any statement s, from

$$\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ q.i \rangle$$

we have

$$\langle \forall\ i\ ::\ \{p.i\ \wedge\ \neg q.i\}\ \ s\ \ \{p.i\ \vee\ q.i\} \rangle\ .$$

Using the disjunctive form of (1) we get, from the above,

$$\{\langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle\}\ \ s\ \ \{\langle \exists\ i\ ::\ p.i\ \vee\ q.i \rangle\}\ .$$

Our goal is to prove,

$$\langle \exists\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ \neg p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle$$

i.e., for statement s

$$
\begin{array}{l}
\{\langle \exists\ i\ ::\ p.i \rangle \wedge \neg[\langle \forall\ i\ ::\ \neg p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]\} \\
\qquad\qquad s \\
\{\langle \exists\ i\ ::\ p.i \rangle\ \vee\ [\langle \forall\ i\ ::\ \neg p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]\}
\end{array}
$$

Using (2), it is sufficient to show that

$$
\begin{array}{ll}
& \langle \exists\ i\ ::\ p.i \rangle\ \wedge\ \neg[\langle \forall\ i\ ::\ \neg p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle] \\
\Rightarrow & \langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle
\end{array}
\tag{5}
$$

and,

$$
\begin{array}{ll}
& \langle \exists\ i\ ::\ p.i\ \vee\ q.i \rangle \\
\Rightarrow & \langle \exists\ i\ ::\ p.i \rangle\ \vee\ [\langle \forall\ i\ ::\ \neg p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]
\end{array}
\tag{6}
$$

Proof of (5)

antecedent of (5)
$= \{\text{deMorgan}\}$
$\langle \exists\ i\ ::\ p.i \rangle \ \wedge\ [\langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle\ \vee\ \langle \forall\ i\ ::\ \neg q.i \rangle]$
$= \{\text{distributing } \wedge \text{ over } \vee\}$
$[\langle \exists\ i\ ::\ p.i \rangle\ \wedge\ \langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle]\ \vee\ [\langle \exists\ i\ ::\ p.i \rangle\ \wedge\ \langle \forall\ i\ ::\ \neg q.i \rangle]$
$\Rightarrow$ {the first conjunct in the first term is implied by the second conjunct; weaken the second term}
$\langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle\ \vee\ \langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle$
$= \{\text{idempotence of } \vee\}$
$\langle \exists\ i\ ::\ p.i\ \wedge\ \neg q.i \rangle$

Proof of (6)

antecedent of (6)
$= \{\text{distributing } \exists \text{ over } \vee\}$
$\langle \exists\ i\ ::\ p.i \rangle\ \vee\ \langle \exists\ i\ ::\ q.i \rangle$
$= \{\text{absorption law}\}$
$\langle \exists\ i\ ::\ p.i \rangle\ \vee\ [\neg\langle \exists\ i\ ::\ p.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]$
$= \{\text{deMorgan}\}$
$\langle \exists\ i\ ::\ p.i \rangle\ \vee\ [\langle \forall\ i\ ::\ \neg p.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]$
$\Rightarrow$ {weakening the first conjunct in the second term}
$\langle \exists\ i\ ::\ p.i \rangle\ \vee\ [\langle \forall\ i\ ::\ \neg p.i\ \vee\ q.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle]$

3 Some Derived Results

• The following result generalizes Corollary 5 in Section 3.6.1 in [1]. Its special cases appear several times in [1], in particular in Sections 16.3.2 and 16.5.3.

$$\frac{\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ p.i\ \wedge\ q.i \rangle}{\langle \forall\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle}$$

Proof:
$\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ p.i\ \wedge\ q.i \rangle$
, given
$\langle \forall\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i\ \vee\ (p.i \wedge q.i) \rangle\ \wedge\ \langle \exists\ i\ ::\ p.i \wedge q.i \rangle$
, conjunction rule
$\langle \forall\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i \rangle\ \wedge\ \langle \exists\ i\ ::\ p.i\ \wedge\ q.i \rangle$
, simplifying the first term in the right side
$\langle \forall\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i \rangle\ \wedge\ \langle \exists\ i\ ::\ q.i \rangle$
, weakening the second term in the right side ▽

• A dual of the above rule, discovered by Mark Staskauskas, is called *unless*-refinement rule in [5]. Its proof follows by applying the disjunction rule.

$$\frac{\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ \neg p.i \wedge q.i \rangle}{\langle \exists\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ \neg p.i \rangle\ \vee\ \langle \exists\ i\ ::\ q.i \rangle}$$

• The following result is the subject of exercise 14.3 in [1]. Let i satisfy $0 \leq i < N$, and let $\oplus$ denote addition mod N.

$$\frac{\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ p.(i \oplus 1) \rangle}{\langle \exists\ i\ ::\ p.i \rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i \rangle}$$

Proof:
$\langle \forall\ i\ ::\ p.i\ \mathit{unless}\ p.(i \oplus 1)\rangle$
, given
$\langle \exists\ i\ ::\ p.i\rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ \neg p.i\ \vee\ p.(i \oplus 1)\rangle\ \wedge\ \langle \exists\ i\ ::\ p.(i \oplus 1)\rangle$
, disjunction rule
$\langle \exists\ i\ ::\ p.i\rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ \neg p.i\ \vee\ p.(i \oplus 1)\rangle\ \wedge\ \langle \exists\ i\ ::\ p.i\rangle$
, simplifying the second term
$\langle \exists\ i\ ::\ p.i\rangle\ \mathit{unless}\ \langle \forall\ i\ ::\ p.i\rangle$
, using induction to simplify the right side ▽

In a similar manner, exercise 11.3 of [1] may be proven without using explicit induction:

$$\frac{\langle \forall\ i\ :\ 0 \le i < N\ ::\ p.i\ \wedge\ p.(i+1)\ \mathit{unless}\ p.i\ \wedge\ \neg p.(i+1)\rangle}{\langle \wedge\ i\ :\ 0 \le i \le N\ ::\ p.i\rangle\ \mathit{unless}\ \langle \wedge\ i\ :\ 0 \le i < N\ ::\ p.i\rangle\ \wedge\ \neg p.N}$$

- Let x denote a set of variables of a given program. Suppose p, q do not name k as a free variable.

$$\frac{\langle \forall\ k\ ::\ p\ \wedge\ x = k\ \mathit{unless}\ (p\ \wedge\ x \ne k)\ \vee\ q\rangle}{p\ \mathit{unless}\ q}$$

Proof
$\langle \forall\ k\ ::\ p\ \wedge\ x = k\ \mathit{unless}\ (p\ \wedge\ x \ne k)\ \vee\ q\rangle$
, given
$\langle \exists\ k\ ::\ p\ \wedge\ x = k\rangle\ \mathit{unless}\ \langle \forall\ k\ ::\ \neg(p\ \wedge\ x = k)\ \vee\ (p\ \wedge\ x \ne k)\ \vee\ q\rangle$
$\wedge\ \langle \exists\ k\ ::\ (p\ \wedge\ x \ne k)\ \vee\ q\rangle$
, disjunction rule
$p\ \mathit{unless}\ \langle \forall\ k\ ::\ \neg p\ \vee\ x \ne k\ \vee\ q\rangle\ \wedge\ \langle \exists\ k\ ::\ (p\ \wedge\ x \ne k)\ \vee\ q\rangle$
, in the left side $\langle \exists\ k\ ::\ x = k\rangle$ is replaced by *true*
$p\ \mathit{unless}\ [\neg p\ \vee\ q\ \vee\ \langle \forall\ k\ ::\ x \ne k\rangle]\ \ \wedge\ \ [\langle \exists\ k\ ::\ (p\ \wedge\ x \ne k)\rangle\ \vee\ q]$
, rewriting both terms in the right side
$p\ \mathit{unless}\ [\neg p\ \vee\ q]\ \ \wedge\ \ [p\ \vee\ q]$
, replacing $\langle \forall\ k\ ::\ x \ne k\rangle$ by *false* in the first term and weakening the second term in the right side
$p\ \mathit{unless}\ q$
, simplifying the right side ▽

- Let R be a transitive relation and x be a program variable.

$$\frac{\langle \forall\ k\ ::\ x = k\ \mathit{unless}\ x \ne k\ \wedge\ x\ R\ k\rangle}{\langle \forall\ m\ ::\ x\ R\ m \text{ is stable}\rangle}$$

Proof: Consider any arbitrary constant m.
$\langle \forall\ k\ :\ k\ R\ m\ ::\ x = k\ \mathit{unless}\ x \ne k\ \wedge\ x\ R\ k\rangle$
, from the antecedent, restricting k for which $k\ R\ m$ holds
$\langle \exists\ k\ :\ k\ R\ m\ ::\ x = k\rangle\ \mathit{unless}\ \langle \forall\ k\ :\ k\ R\ m\ ::\ x \ne k\ \vee\ (x \ne k\ \wedge\ x\ R\ k)\rangle\ \wedge$
$\langle \exists\ k\ :\ k\ R\ m\ ::\ x \ne k\ \wedge\ x\ R\ k\rangle$
, disjunction rule
$x\ R\ m\ \mathit{unless}\ \langle \forall\ k\ :\ k\ R\ m\ ::\ x \ne k\rangle\ \wedge\ \langle \exists\ k\ :\ k\ R\ m\ ::\ x\ R\ k\rangle$
, simplifying left side and first term in the right side and weakening the second term in the right side
$x\ R\ m\ \mathit{unless}\ \neg x\ R\ m\ \wedge\ x\ R\ m$
, simplifying the first term in the right side using predicate calculus (Leibniz) and the

second term using the transitivity of R

$x\ R\ m$ is stable

, definition of stable $\bigtriangledown$

- A corollary of the above result is, for any partial ordering relation $>$,

$$\frac{\langle \forall\ k\ ::\ x = k\ \textit{unless}\ x > k \rangle}{\langle \forall\ k\ ::\ x > k \text{ is stable} \rangle}$$

- A similar result is, for any function f,

$$\frac{\langle \forall\ k\ ::\ x = k\ \textit{unless}\ x \neq k\ \wedge\ f(x) = f(k) \rangle}{\langle \forall\ m\ ::\ f(x) = m \text{ is stable} \rangle}$$

4 References

1. K. M. Chandy and J. Misra, *Parallel Program Design: A Foundation*, Addison-Wesley, 1988.

2. E. Cohen, personal communication, June 1988.

3. E. W. Dijkstra and C. S. Scholten, *Predicate Calculus and Programming Semantics*, Chapter 7, (Semantics of Straightline Programs), Springer-Verlag (to be published), 1989.

4. C. S. Scholten, "Unless and Junctions," CSS 141, July 1988, Beekbergen, The Netherlands.

5. M. Staskauskas, "The Formal Specification and Design of a Distributed Electronic Funds-Transfer System," (to appear in the special issue of *IEEE Transactions on Computers, on Parallel and Distributed Algorithms*).