# Progress–Safety–Safety
Notes on UNITY: 05-89

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

4/20/89

The PSP rule (PSP is an abbreviation for Progress–Safety–Progress) is a fundamental rule for deriving a progress property from a progress and a safety property. We had no analogous rule for deriving a nontrivial safety property from a progress and a safety propety. This note contains such a rule.

Theorem:

$$\frac{p \mapsto q\ ,\ \neg r \wedge \neg q \text{ is stable}}{\begin{array}{c} p \Rightarrow q \vee r\ , \\ p \textit{ unless } (\neg p \wedge r) \vee q \end{array}}$$

Proof of $p \Rightarrow q \vee r$

| | |
|---|---|
| $p \mapsto q$ | , antecedent |
| $\neg r \wedge \neg q$ is stable | , antecedent |
| $p \wedge \neg r \wedge \neg q \mapsto \textit{false}$ | , PSP rule on the above two |
| $\neg(p \wedge \neg r \wedge \neg q)$ | , impossibility rule on the above |
| $p \Rightarrow q \vee r$ | , rewriting the above |

Proof of $p \textit{ unless } (\neg p \wedge r) \vee q$:

Crucial to this proof is a recent result due to Ambuj Singh [1] which says that given $p \mapsto q$ there is a predicate $s$ such that

$$p \Rightarrow s, \quad (1)$$
$$s \textit{ unless } q \quad (2)$$
$$s \mapsto q \quad (3)$$

Also we have from the antecedent

$$\neg r \wedge \neg q \text{ is stable} \quad (4)$$

Now

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

$s \wedge \neg r \wedge \neg q \mapsto \mathit{false}$
, PSP on (3) and (4)
$s \Rightarrow q \vee r$
, impossibility theorem on the above and then rewriting (5)
$p$ *unless* $\neg p$
, property of *unless*
$s$ *unless* $q$
, repeating (2)
$p \wedge s$ *unless* $(p \wedge q) \vee (\neg p \wedge s) \vee (\neg p \wedge q)$
, conjunction of the above two
$p \wedge s$ *unless* $(\neg p \wedge s) \vee q$
, rewriting the rhs of the above
$p$ *unless* $(\neg p \wedge s) \vee q$
, simplifying the lhs using (1)
$p$ *unless* $[\neg p \wedge (q \vee r)] \vee q$
, weakening the rhs using (5)
$p$ *unless* $(\neg p \wedge r) \vee q$
, simplifying the rhs □

The following corollary was proven in [1]. Now we have a trivial proof.

Corollary 1:

$$\frac{p \mapsto q \text{ , } \neg p \wedge \neg q \text{ is stable}}{p \textit{ unless } q}$$

Proof: Replace $r$ by $p$ in the second consequent of the theorem. □

Corollary 2:

$$\frac{\begin{array}{c} p \mapsto q \text{ ,} \\ \neg r \wedge \neg q \text{ is stable ,} \\ p \textit{ unless } \neg r \end{array}}{p \textit{ unless } q}$$

Proof:

$p$ *unless* $(\neg p \wedge r) \vee q$
, from the second consequent of the theorem
$p$ *unless* $\neg r$
, from the antecedent of the corollary
$p$ *unless* $(p \wedge \neg r) \vee (p \wedge q) \vee (q \wedge \neg r)$
, conjunction of the above two
$p$ *unless* $(p \wedge \neg r) \vee q$
, weakening the rhs of the above
$p$ *unless* $q$
, weakening the rhs using $p \wedge \neg r \Rightarrow q$
(from the first consequent of the theorem) □

# References


1. Jayadev Misra, "A Theorem Relating *leads-to* and *unless*," *Notes on UNITY: 04-88*, The University of Texas, Austin, Texas, December 1988.