Generalization of postconditions to relations

When postconditions are viewed as relations (subsets of **D**×**D**) instead of as subsets of **D**, the lemmata for the several kinds of preconditions change to the forms given below.

In the following expressions,

- V is a set of data environments (**D**, states of program execution),
- S is a *function* mapping a data environment to a data environment, i.e. is a relation on **D** (a subset of **D**×**D**), and
- P is a relation on **D** (a subset of **D**×**D**).

$\{V\}\ S\ \{P\}$ = $(V \cap \mathrm{dom}(S) \subseteq \mathrm{dom}(S \cap P))$

$\{V\}\ S\ \{P\}$ strictly = $(V \subseteq \mathrm{dom}(S \cap P))$

$\{V\}\ S\ \{P\}$ completely = $(V \cap \mathrm{dom}(S) = \mathrm{dom}(S \cap P))$

$\{V\}\ S\ \{P\}$ strictly and completely = $(V = \mathrm{dom}(S \cap P))$

The expressions above are based on the identity

$$S^{-1}.P = \mathrm{dom}(S \cap P)$$

of which

$$S^{-1}.(\mathbf{D} \times \mathbf{D}) = \mathrm{dom}(S)$$

is a special case.

Then the lemmata for $\{V\}\ S\ \{P\}$ for the several types of preconditions are given in the following table:

	not (necessarily) strict	strict
not (necessarily) complete	$V \cap \mathrm{dom}(S) \subseteq \mathrm{dom}(S \cap P)$	$V \subseteq \mathrm{dom}(S \cap P)$
complete	$V \cap \mathrm{dom}(S) = \mathrm{dom}(S \cap P)$	$V = \mathrm{dom}(S \cap P)$

Generalizing the definition of {V} S {P} when P is a relation and contains references to the initial values of variables

The MRSD lecture notes dated 2002 September 9, section 3.6 give a definition for {V} S {P} when the postcondition P contains references to the initial values of variables. When the postcondition P is viewed as a relation (possibly containing references to the initial values of variables), this definition generalizes to

$(A\ d0 : d0 \in \mathbf{D} : \{V \wedge d=d0\}\ S\ \{Pi.d0\})$ [definition of {V} S {P} in specified case]

where d0 is the "specification variable", Pi.d0 is the image of d0 under the relation P, and d is the initial data environment (state).

I.e., d0 is a parameter of the correctness proposition {V} S {P}. Note that Pi.d0 is a subset of **D**, the set of all data environments. Pi.d0 in the relational view is the postcondition P in the traditional view of P as a subset of **D**.

Then the above definition

$(A\ d0 : d0 \in \mathbf{D} : \{V \wedge d=d0\}\ S\ \{Pi.d0\})$

= [definition of {V} S {P} in the MRSD lecture notes dated 2002 September 9, section 3.1]

$(A\ d0 : d0 \in \mathbf{D} : (A\ d:\ d \in V \cap S^{-1}.\mathbf{D} \wedge d=d0 : S.d \in Pi.d0)\ )$

= [property of the for all quantification]

$(A\ d0 : d0 \in \mathbf{D} : (A\ d:\ d=d0 : d \in V \cap S^{-1}.\mathbf{D} \Rightarrow S.d \in Pi.d0)\ )$

= [singleton range of quantification]

$(A\ d0 : d0 \in \mathbf{D} : d0 \in V \cap S^{-1}.\mathbf{D} \Rightarrow S.d0 \in Pi.d0\ )$

= [property of the for all quantification]

$(A\ d0 : d0 \in \mathbf{D} \wedge d0 \in V \cap S^{-1}.\mathbf{D} : S.d0 \in Pi.d0\ )$

= [$S^{-1}.\mathbf{D}$, and hence $V \cap S^{-1}.\mathbf{D}$, is a subset of **D**]

$(A\ d0 : d0 \in V \cap S^{-1}.\mathbf{D} : S.d0 \in Pi.d0\ )$

= [definition of an image under a relation]

$(A\ d0 : d0 \in V \cap S^{-1}.\mathbf{D} : (d0, S.d0) \in P\ )$

= [renaming the quantified variable]

$(A\ d : d \in V \cap S^{-1}.\mathbf{D} : (d, S.d) \in P\ )$ [generalized definition of {V} S {P}]

The last line above is a suitable definition of {V} S {P} for a postcondition P viewed as a relation and which may, therefore, contain references to the initial values of program variables. See also Baber, Robert L., *Praktische Anwendbarkeit* ..., section 3.1.6 (1), page 38.

See also the file *TheoremPPeqvLD.pdf*., which contains a theorem regarding the equivalence of a specification consisting of a strict precondition and postcondition and a specification consisting of an LD-relation.