Partitioning predicates and substitution; diabolical and angelical nondeterminism.

Anyone involved with the formal semantics of

if B **then** $S0$ **else** $S1$ **fi**

has encountered the tautology

(0) $(B \wedge P0) \vee (\neg B \wedge P1) \equiv (\neg B \vee P0) \wedge (B \vee P1)$.

This little note primarily deals with a generalisation of the latter formula.

Some nomenclature and notation

- We call X a "predicate" (or "boolean structure") on some space if it is a boolean expression in (or a boolean function applied to) the coordinates of (or the variables spanning) that space. (End of •.)

- Let X be a predicate on some space; with $[X]$ we then denote X universally quantified over (the coordinates of) that space. (End of •.)

- Functional application is denoted by an infix period, left-associative and with the highest binding power of all operators. (End of •.)

- With B and R boolean functions of some (understood) type, and x a dummy of that type, the "numerical quantifier" $\underline{N}$ is given by

$(\underline{N}x: B.x: R.x)$ = the number of distinct solutions of $B.x \wedge R.x$, viewed as equation in x .

(End of •.)

The connection between existential and numerical quantification is

(1) $(\underline{E}x: B.x: R.x) \equiv (\underline{N}x: B.x: R.x) \neq 0$;

that between universal and numerical quantification is

(2) $(\underline{A}x: B.x: R.x) \equiv (\underline{N}x: B.x: \neg R.x) = 0$.

(End of Some nomenclature and notation.)

In the following "chosen" is the name of some type (e.g. integer, or the colours of the spectrum) independent of the space that will be introduced in the next sentence.

Let B be a function that, applied to a chosen argument, yields as value a predicate on some space, and let c be a chosen dummy.

Then

$$(\underline{N}c: B.c: true)$$

denotes a natural structure on that same space, and

$$(\underline{N}c: B.c: true) = 1$$

denotes a predicate on that space.

We now define "the B.c's are a set of partitioning predicates" to mean $[(\underline{N}c: B.c: true) = 1]$, i.e. in each point of the space under consideration, precisely one of the B.c's holds.

With R a function of the same type as B and the B.c's being a set of partitioning predicates, we have

(4) $[(\underline{E}c: B.c: R.c) \equiv (\underline{A}c: B.c: R.c)]$.

<u>Proof</u> $[(\underline{N}c: B.c: true) = 1]$

$=$ {Law of the Excluded Middle}

$[(\underline{N}c: B.c: R.c \vee \neg R.c) = 1]$

$=$ {Properties of $\underline{N}$}

$[(\underline{N}c: B.c: R.c) + (\underline{N}c: B.c: \neg R.c) = 1]$

$\Rightarrow$ {$(\underline{N} \ldots)$ yields a natural value, hence precisely 1 of the addenda equals 0}

$[(\underline{N}c: B.c: R.c) \neq 0 \equiv (\underline{N}c: B.c: \neg R.c) = 0]$

$=$ {(1) and (2)}

$[(\underline{E}c: B.c: R.c) \equiv (\underline{A}c: B.c: R.c)]$.

(End of Proof.)

Alternatively, the B.c's being a set of partitioning predicates, we could have associated with them a chosen structure C on the space in question, satisfying

(5) $(\underline{A}c: true: [B.c \equiv c = C])$.

Then, (4) can be established by observing

$[(\underline{E}c: B.c: R.c) \equiv (\underline{A}c: B.c: R.c)]$

$=$ {(5)}

$[(\underline{E}c: c = C: R.c) \equiv (\underline{A}c: c = C: R.c)]$

$=$ {one-point rules}

$[R.C \equiv R.C]$

$=$ {predicate calculus}

true,

and it is the latter argument that connects partitioning predicates to substitution.

Remark Note that, as a special consequence, with S a function from booleans to statements,

$$\underline{\mathbf{if}}\ B\ \underline{\mathbf{then}}\ S.true\ \underline{\mathbf{else}}\ S.false\ \underline{\mathbf{fi}}$$

can (at least symbolically) be rendered by $S.B$. (End of Remark.)

The generalization from (0) to (4) corresponds to the transition from the alternative clause to the case statement that, with S a statement-valued function of a chosen argument could be rendered by — with "::" short for ":true:" —

(6) $\underline{\mathbf{if}}([\!]c{::}\ B.c \rightarrow S.c)\ \underline{\mathbf{fi}}$.

Remark. (6) is a generalization of the guarded-command notation in which our original conditional statement is written as

$$\underline{\mathbf{if}}\ B \rightarrow S0\ [\!]\ \neg B \rightarrow S1\ \underline{\mathbf{fi}} \quad .$$

(End of Remark.)

In terms of weakest preconditions, two definitions of the semantics of (6) now present themselves:

(7) $[wp(\text{"}\underline{\mathbf{if}}([\!]c{::}\ B.c \rightarrow S.c\underline{\mathbf{fi}}\text{"}, X) \equiv (\underline{\mathbf{E}}c{:}\ B.c{:}\ wp(S.c, X))]$

(8) $[wp(\text{"}\underline{\mathbf{if}}([\!]c{::}\ B.c \rightarrow S.c\underline{\mathbf{fi}}\text{"}, X) \equiv (\underline{\mathbf{A}}c{:}\ B.c{:}\ wp(S.c, X))]$,

which, in view of (4), are equivalent for $B.c$'s that form a partitioning set of predicates.

In the case statement, nondeterminism is introduced if its guards don't necessarily exclude each other, e.g. admitting a B that satisfies

(9) $[(\underline{N}c: B.c: true) \geq 1]$

In view of (1), (9) is equivalent to $[(\underline{E}c: B.c.true)]$; it excludes points in space where none of the guards holds. If B satisfies (9) we have

(10) $[(\underline{E}c: B.c: R.c) \Leftarrow (\underline{A}c: B.c: R.c)]$.

<u>Proof</u> $[(\underline{N}c: B.c: true) \geq 1]$

$= \{$Excluded Middle and Properties of $\underline{N}\}$

$[(\underline{N}c: B.c: R.c) + (\underline{N}c: B.c: \neg R.c) \geq 1]$

$\Rightarrow \{$at most one of the addenda equals 0$\}$

$[(\underline{N}c: B.c: R.c) \neq 0 \Leftarrow (\underline{N}c: B.c: \neg R.c) = 0]$

$= \{(1)$ and $(2)\}$

$[(\underline{E}c: B.c: R.c) \Leftarrow (\underline{A}c: B.c: R.c)]$

(End of Proof.)

C.A.R. Hoare dubbed definitions (7) and (8) "angelical" and "diabolical" nondeterminism. Definition (7) gives the precondition under which the case statement establishes X provided the nondeterminism is resolved by a most cooperative daemon; (8) gives that precondition, no matter how uncooperative the daemon. The latter implies the former.

Pasadena, 21 March 1986

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
United States of America.

PS. The above is mostly a synthesis of EWD 834 and EWD 894 (which I had largely forgotten).