A universal quantification revisited

by C.S. Scholten and Edsger W. Dijkstra

For any bag B and any boolean function b defined on the elements of B we deem $(\underline{A}X: X\ \underline{in}\ B: bX)$ defined as usual. Our first purpose is to define as a predicate

(0) $$(\underline{A}X: X\ \underline{in}\ B: fX)$$

where f is a function from the elements of B to predicates on some space. (If the elements of B are predicates on that same space, f is traditionally known as a predicate transformer.)

A traditional way of defining the predicate (0) is by point-wise definition: in each point of state space the fX stand for boolean values for which universal quantification over B is defined. We should like to develop a predicate calculus as far as possible without explicit reference to points of the space; we would like to define it by means of a set of rules for the manipulation of formulae.

We postulate expressions of form (0) to satisfy the following two rules — where a pair of square brackets, if so desired, may be interpreted as universal quantification over the points of space —

(1) $$(\underline{A}X: X\ \underline{in}\ B: [fX]) \equiv [(\underline{A}X: X\ \underline{in}\ B: fX)]$$

(2) $$[(\underline{A}X: X\ \underline{in}\ B: Q \vee fX) \equiv Q \vee (\underline{A}X: X\ \underline{in}\ B: fX)]$$ for

any predicate Q.

Note that in the case of a finite bag B, (1) and (2) are consistent with the interpretation of (0) as the conjunction of fX over the elements of B.

For the sake of brevity, the range "X in B" will be omitted in the sequel.

We observe for any Z

$$\begin{array}{ll} & true \\ = & \{\text{substitution of } \neg Z \text{ for } Q \text{ in } (2)\} \\ & [(\underline{A}X :: \neg Z \vee fX) \equiv \neg Z \vee (\underline{A}X :: fX)] \\ \Rightarrow & \{\text{Leibniz's Rule}\} \\ & [(\underline{A}X :: \neg Z \vee fX)] \equiv [\neg Z \vee (\underline{A}X :: fX)] \\ = & \{(1) \text{ and the definition of } \Rightarrow\} \\ (3) & (\underline{A}X :: [Z \Rightarrow fX]) \equiv [Z \Rightarrow (\underline{A}X :: fX)] \end{array}$$

.

One of the consequences of (3) is that (0) is the weakest solution of

(4) $\qquad Z : (\underline{A}X :: [Z \Rightarrow fX])$,

because, firstly, any solution of (4) substituded for Z in (3) reduces its left-hand side to true and, hence, implies (0), and, secondly, (0) substituded for Z in (3) reduces its right-hand side to true and, hence, is a solution of (4).

Consider in addition to B a bag of elements Y and let g be a predicate-valued on the Cartesian product of B and C. For any Z

$$\begin{array}{l}
\quad true \\
= \{\text{substitution of } g\,X\,Y \text{ for } f\,X \text{ in (3)}\} \\
\quad (\underline{A}Y :: (\underline{A}X :: [Z \Rrightarrow g\,X\,Y]) \equiv [Z \Rrightarrow (\underline{A}X :: g\,X\,Y)]) \\
\Rrightarrow \{\text{predicate calculus}\} \\
\quad (\underline{A}Y :: (\underline{A}X :: [Z \Rrightarrow g\,X\,Y])) \equiv (\underline{A}Y :: [Z \Rrightarrow (\underline{A}X :: g\,X\,Y)]) \\
= \{\text{predicate calculus}\} \\
\quad (\underline{A}X :: (\underline{A}Y :: [Z \Rrightarrow g\,X\,Y])) \equiv (\underline{A}Y :: [Z \Rrightarrow (\underline{A}X :: g\,X\,Y)]) \\
= \{(3)\} \\
\quad (\underline{A}X :: [Z \Rrightarrow (\underline{A}Y :: g\,X\,Y)]) \equiv (\underline{A}Y :: [Z \Rrightarrow (\underline{A}X :: g\,X\,Y)]) \\
= \{\text{(3) applied to both sides}\} \\
\quad [Z \Rrightarrow (\underline{A}X :: (\underline{A}Y :: g\,X\,Y))] \equiv [Z \Rrightarrow (\underline{A}Y :: (\underline{A}X :: g\,X\,Y))]
\end{array}$$

Hence

(5) $\quad [(\underline{A}X :: (\underline{A}Y :: g\,X\,Y)) \equiv (\underline{A}Y :: (\underline{A}X :: g\,X\,Y))]$,

i.e. also when the terms are predicates, the order of universal quantifications is immaterial.

<u>Corollary</u> of (5)

$$[(\underline{A}X :: f\,X \wedge g\,X) \equiv (\underline{A}X :: f\,X) \wedge (\underline{A}X :: g\,X)] \quad .$$

Note that from this corollary the monotonicity of universal quantification over X follows.

* * *

Slightly shifting notational gears we consider (0) with for f the identity function and for $\mathbb{B}$ the bag of solutions of the equation

(6) $\qquad X : [g\,X]$,

where g is some predicate transformer, i.e X and $g\,X$ are predicates on the same space. For the sake of reference, the resulting expression is denoted by Q, i.e.

(7) $\quad [Q \equiv (\underline{A}X{:}[gX]{:}\ X)]$.

Rewriting (3) we observe for any Z

(8) $\quad (\underline{A}X{:}[gX]{:}[Z \Rrightarrow X]) \equiv [Z \Rrightarrow Q]$

with the corollary

(9) $\quad (\underline{A}X{:}[gX]{:}[Q \Rrightarrow X])$.

We are now ready to prove

<u>Lemma 0</u>. In terms of (6) and (7) the following three assertions are equivalent

(i) Q is a solution of (6)
(ii) Q is the strongest solution of (6)
(iii) a strongest solution of (6) exists .

<u>Proof</u>. Formally expressed the assertions are

(i) $[gQ]$
(ii) $[gQ] \wedge (\underline{A}X{:}[gX]{:}[Q \Rrightarrow X])$
(iii) $(\underline{E}P{:}[gP]{:}(\underline{A}X{:}[gX]{:}[P \Rrightarrow X]))$.

The equivalence (i)$\equiv$(ii) follows immediately from (9). Further we observe

$\quad$ (iii)
$= \{$definition of (iii) and (8) with P for $Z\}$
$\quad (\underline{E}P{:}[gP]{:}\ [P \Rrightarrow Q])$
$= \{$on account of (9)$\}$
$\quad (\underline{E}P{:}[gP]{:}\ [P \Rrightarrow Q] \wedge [Q \Rrightarrow P])$

$= \{\text{predicate calculus}\}$
$(\underline{E}P: [gP]: [P \equiv Q])$
$= \{\text{predicate calculus}\}$
$[gQ]$
$= \{\text{definition of (i)}\}$
(i)

(End of Proof.)

<u>Remark 0</u>. Note that Lemma 0 holds without <u>any</u> further assumptions about predicate transformer g. (End of Remark 0.)

We mention a special consequence of Lemma 0. In order to prove that (6) has a strongest solution, one shows for instance that Q — the conjunction of <u>all</u> solutions of (6) — is a solution of (6). Sometimes one can prove a somewhat stronger property of g, viz. that the conjunction of any bag of solutions of (6) is again a solution of (6). Such is the case in the following two examples.

<u>Example 0</u>. For monotonic h, the equation

(10) $\qquad X: [hX \Rrightarrow X]$

has a strongest solution.

<u>Proof</u>. In view of the above it suffices to show that $(\underline{A}X: X \underline{\text{in}}\, \mathcal{B}: X)$ solves (10) for $\mathcal{B}$ any bag of solutions of (10).

true
$= \{\text{definition of } \mathcal{B}\}$
$(\underline{A}X: X \underline{\text{in}}\, \mathcal{B}: [hX \Rrightarrow X])$

$\Rightarrow$ {monotonicity of universal quantification}
$[(\underline{A}X : X \ \underline{in}\ B : \ h X) \Rightarrow (\underline{A} X : X \ \underline{in}\ B : X)]$
$\Rightarrow$ {monotonicity of h, see next page}
$[h(\underline{A}X : X \ \underline{in}\ B : X) \Rightarrow (\underline{A}X : X \ \underline{in}\ B : X)]$

(End of Proof.)

(Note that Example 0 states "half" of the Theorem of Knaster-Tarski.)

<u>Example 1</u>. For universally conjunctive h, the equation

(11) $\qquad X : [P \vee h X]$

has a strongest solution for any predicate P.

<u>Proof</u>. For any bag B of solutions of (11) we have

true
= {definition of B}
$(\underline{A}X : X \ \underline{in}\ B : [P \vee h X])$
= {predicate calculus}
$[(\underline{A}X : X \ \underline{in}\ B : P \vee h X)]$
= {on account of (2)}
$[P \vee (\underline{A}X : X \ \underline{in}\ B : h X)]$
= {universal conjunctivity of h}
$[P \vee h(\underline{A}X : X \ \underline{in}\ B : X)]$.

(End of Proof.)

The last transition in the proof of Example 0 relies on

(11) For monotonic h and any bag B
$$[h(\underline{A}X: X \underline{\text{in}}\ B: X) \Rightarrow (\underline{A}X: X \underline{\text{in}}\ B: hX)]$$

<u>Proof</u>

$$\begin{array}{l} \quad \text{true} \\ = \{(3) \text{ with } f \text{ the identity and } (\underline{A}Y: Y \underline{\text{in}}\ B: Y) \text{ for } Z\} \\ \quad (\underline{A}X: X \underline{\text{in}}\ B: [(\underline{A}Y: Y \underline{\text{in}}\ B: Y) \Rightarrow X]) \\ \Rightarrow \{\text{monotonicity of } h\} \\ \quad (\underline{A}X: X \underline{\text{in}}\ B: [h(\underline{A}Y: Y \underline{\text{in}}\ B: Y) \Rightarrow hX]) \\ = \{(3)\} \\ \quad [h(\underline{A}Y: Y \underline{\text{in}}\ B: Y) \Rightarrow (\underline{A}X: X \underline{\text{in}}\ B: hX)] \\ = \{\text{renaming the dummy}\} \\ \quad (11) \end{array}$$

(End of Proof.)

* * *

The conclusion we drew from the Corollary of (5), viz. the monotonicity of universal quantification, was a bit rash. The statement of the monotonicity —and in this version we used it in the proof of Example 0— is

(12) $(\underline{A}X: X \underline{\text{in}}\ B: [fX \Rightarrow gX]) \Rightarrow [(\underline{A}X: X \underline{\text{in}}\ B: fX) \Rightarrow (\underline{A}X: X \underline{\text{in}}\ B: gX)]$.

For the formal proof of (12) we need an extension of Leibniz's Rule, viz.

(13) $(\underline{A}X: X \underline{\text{in}}\ B: [fX \equiv gX]) \Rightarrow [(\underline{A}X: X \underline{\text{in}}\ B: fX) \equiv (\underline{A}X: X \underline{\text{in}}\ B: gX)]$.

The proof of (12) is then as follows —for the sake of brevity under omission of the range—

Proof

$$
\begin{array}{l}
\quad (\underline{A} X :: [fX \Rightarrow gX]) \\
= \{\text{predicate calculus}\} \\
\quad (\underline{A} X :: [fX \equiv fX \wedge gX]) \\
\Rightarrow \{(13)\} \\
\quad [(\underline{A} X :: fX) \equiv (\underline{A} X :: fX \wedge gX)] \\
= \{\text{Corollary of (5)}\} \\
\quad [(\underline{A} X :: fX) \equiv (\underline{A} X :: fX) \wedge (\underline{A} X :: gX)] \\
= \{\text{predicate calculus}\} \\
\quad [(\underline{A} X :: fX) \Rightarrow (\underline{A} X :: gX)]
\end{array}
$$

(End of Proof.)

26 November 1982

drs. C.S. Scholten
Scientific Advisor
Philips Research Laboratories
5600 JA EINDHOVEN
The Netherlands

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow
Plataanstraat 5
5671 AL NUENEN
The Netherlands.