# The calculus of boolean structures (Part 1)

Universal quantification is a generalization of the conjunction. Its format is

$$(\underline{A}\ \text{dummies} : \text{range} : \text{term})$$

Here, "dummies" stands for an unordered list of local variables, whose scope is delineated by the outer parenthesis pair. In what follows, $x$ and $y$ will be used to denote dummies; they may be of any understood type. Components "range" and "term" are in general expressions of type "boolean structure"; their potential dependence on the dummies will be indicated explicitly by using a functional notation, i.e. if a range has the form $r.x \wedge s.y$, it is a conjunction of $r.x$, which does not depend on $y$, and $s.y$, which does not depend on $x$; similarly, $Q$ would stand for a predicate that depends on none of the dummies. In the following, we shall use $r$, $s$, $f$ and $g$ to denote functions from (the types of) the dummies to boolean structures on the implicitly understood space or on the trivial one. (In the latter case, they are just boolean functions.) If range and term are boolean expressions, the whole quantification is a boolean expression, otherwise it is a boolean structure.

For the sake of brevity, the range true will be omitted. The following axiom tells us how ranges different from true can be eliminated

(59) $[(\underline{A}x : r.x : f.x) \equiv (\underline{A}x :: \neg r.x \vee f.x)]$ .

(Appeals to this axiom will be given by the catchword "trading", being short for "trading between range and term".)

Disjunction distributes in the same way over universal quantification as it does over conjunction, i.e. we postulate

(60) $[Q \vee (\underline{A}x :: f.x) \equiv (\underline{A}x :: Q \vee f.x)]$ .

But now we observe for any $Q, r, f$

$$\begin{array}{ll} & Q \vee (\underline{A}x : r.x : f.x) \\ = & \{\text{trading}\} \\ & Q \vee (\underline{A}x :: \neg r.x \vee f.x) \\ = & \{(60)\} \\ & (\underline{A}x :: Q \vee \neg r.x \vee f.x) \\ = & \{\text{trading}\} \\ & (\underline{A}x : r.x : Q \vee f.x) \quad . \end{array}$$

Hence we have the more general

(61) $[Q \vee (\underline{A}x : r.x : f.x) \equiv (\underline{A}x : r.x : Q \vee f.x)]$ .

An analogue of conjunction's associativity and symmetry is introduced by postulating

(62) $[(\underline{A}x:: f.x) \land (\underline{A}x:: g.x) \equiv (\underline{A}x:: f.x \land g.x)]$

which invites us to observe for any $r, f, g$

$$\begin{array}{ll}
 & (\underline{A}x: r.x: f.x) \land (\underline{A}x: r.x: g.x) \\
= & \{\text{trading, twice}\} \\
 & (\underline{A}x:: \neg r.x \lor f.x) \land (\underline{A}x:: \neg r.x \lor g.x) \\
= & \{(62)\} \\
 & (\underline{A}x:: (\neg r.x \lor f.x) \land (\neg r.x \lor g.x)) \\
= & \{\text{pred. calc}\} \\
 & (\underline{A}x:: \neg r.x \lor (f.x \land g.x)) \\
= & \{\text{trading}\} \\
 & (\underline{A}x: r.x: f.x \land g.x) \quad .
\end{array}$$

Hence we have the more general

(63) $[(\underline{A}x: r.x: f.x) \land (\underline{A}x: r.x: g.x) \equiv$
$(\underline{A}x: r.x: f.x \land g.x)]$ .

Formula (61) relates two quantifications with the same range, (63) relates three quantifications with the same range. It is, in fact, not uncommon that all through a longer manipulation a given dummy has always the same range; for brevity's sake, such constant ranges are stated once and for all and subsequently not repeated over and over again. (This opportunity for abbreviation was, in fact, one of the reasons for introducing the notion of the range in the first place.)

This last formula has a partner, in hints referred to as "splitting the range"

(64) $$[(\underline{A}x: r.x: f.x) \wedge (\underline{A}x: s.x: f.x) \equiv (\underline{A}x: r.x \vee s.x: f.x)]$$ .

<u>Proof</u> We observe for any $r, s, f$

$$(\underline{A}x: r.x: f.x) \wedge (\underline{A}x: s.x: f.x)$$
$=$ { trading, 4 times }
$$(\underline{A}x: \neg f.x: \neg r.x) \wedge (\underline{A}x: \neg f.x: \neg s.x)$$
$=$ { (63) with $r, f, g := \neg f, \neg r, \neg s$ }
$$(\underline{A}x: \neg f.x: \neg r.x \wedge \neg s.x)$$
$=$ { trading, twice }
$$(\underline{A}x: \neg(\neg r.x \wedge \neg s.x): f.x)$$
$=$ { de Morgan }
$$(\underline{A}x: r.x \vee s.x: f.x)$$ .

(End of Proof.)

Another manifestation of associativity and symmetry is the postulate

(65) $$[(\underline{A}x:: (\underline{A}y:: f.x.y)) \equiv (\underline{A}y:: (\underline{A}x:: f.x.y))]$$ ,

which invites us to observe for any $r, s, f$

$$(\underline{A}x: r.x: (\underline{A}y: s.y: f.x.y))$$
$=$ { trading, twice }
$$(\underline{A}x:: \neg r.x \vee (\underline{A}y:: \neg s.y \vee f.x.y))$$
$=$ { $\vee$ distributes over $\underline{A}$ }
$$(\underline{A}x:: (\underline{A}y:: \neg r.x \vee \neg s.y \vee f.x.y))$$
$=$ { (65) }

$$\begin{array}{ll} & (\underline{A}y::\ (\underline{A}x::\ \neg r.x \vee \neg s.y \vee f.x.y)) \\ = & \quad \{ \vee \text{ distributes over } \underline{A} \} \\ & (\underline{A}y::\ \neg s.y \vee (\underline{A}x::\ \neg r.x \vee f.x.y)) \\ = & \quad \{ \text{trading, twice} \} \\ & (\underline{A}y:\ s.y:\ (\underline{A}x:\ r.x:\ f.x.y) \quad . \end{array}$$

Hence, we have the more general

(66) $$[(\underline{A}x:\ r.x :\ (\underline{A}y:\ s.y:\ f.x.y) \equiv (\underline{A}y:\ s.y :\ (\underline{A}x:\ r.x:\ f.x.y) ]$$

In hints, these formulae are referenced by "interchange of quantifications". Notice that in (66) each dummy carries with it its own range; hence we don't run into trouble here when we leave ranges unmentioned.

Often we don't care which is the outer and which is the inner quantification. We cater to that by admitting a list of dummies following the $\underline{A}$ . By definition

(67) $$[(\underline{A}x,y ::\ f.x.y) \equiv (\underline{A}x::\ (\underline{A}y::\ f.x.y))] \quad ,$$

which admits the analogous generalization

(68) $$[(\underline{A}x,y:\ r.x \wedge s.y:\ f.x.y) \equiv (\underline{A}x:\ r.x:\ (\underline{A}y:\ s.y:\ f.x.y))] \quad .$$

In hints we refer to these transformations by "nesting" or "unnesting". The proof of (68) is left to the reader.

Finally we mention a special case of interchange of universal quantification

(69) $[(\underline{A}x: [r.x]: f.x)] \equiv (\underline{A}x: [r.x]: [f.x])$ ;

note that in this case, the range is not allowed to be a full-blown boolean structure.

From (61) we derive with $Q:=$ true

(70) $[\text{true} \equiv (\underline{A}x: r.x: \text{true})]$

and from that with $r:=\neg f$ and trading

(71) $[\text{true} \equiv (\underline{A}x: \text{false}: f.x)]$ .

From our formalization of the universal quantification, something is still lacking: all our postulates would be satisfied if each quantification were equivalent to true! This is remedied by the postulation of what is known as the "one-point rule", viz. that we have for any $f$ and $y$

(72) $[(\underline{A}x: [x=y]: f.x) \equiv f.y]$ .

Substituting in the above for $f$ the constant function false, we get

(73) $(\underline{A}x: [x=y]: \text{false}) \equiv \text{false}$ .

<u>Remark</u> An alternative would have been to postulate (73) and then to derive (72). The exercise

is left to the reader. He may also wish to verify that another possibility would have been to postulate

(74) $(\underline{A}x :: \neg(x \in V)) \equiv V = \emptyset$ .

(End of Remark.)

Next we observe for any $y$

$$\begin{array}{ll} & (\underline{A}x :: f.x) \wedge f.y \\ = & \{\text{one-point rule}\} \\ & (\underline{A}x :: f.x) \wedge (\underline{A}x : [x=y] : f.x) \\ = & \{\text{range splitting}\} \\ & (\underline{A}x : \text{true} \vee [x=y] : f.x) \\ = & \{\text{predicate calculus}\} \\ & (\underline{A}x :: f.x) \quad . \end{array}$$

Hence we have for any $y$

(75) $[(\underline{A}x :: f.x) \Rightarrow f.y]$

and, because of [ ]'s monotonicity and (69),

(76) $(\underline{A}x :: [f.x]) \Rightarrow [f.y]$ .

It is this formula that allows us to identify the phrase "We have, for any $x$, $[f.x]$" with "We have $(\underline{A}x :: [f.x])$": both allow us to conclude, for any $y$, that we have $[f.y]$ . From an operational point, the two phrases are equivalent. The reader may generalize (76) into

(77) $(\underline{A}x : [r.x] : [f.x]) \Rightarrow ([r.y] \Rightarrow [f.y])$ .

We have for any $f, g, h$

(78) $(\underline{A}x :: [f.x = g.x]) \Rightarrow [(\underline{A}x :: h.(f.x)) \equiv (\underline{A}x :: h.(g.x))]$ .

This formula is of importance because it shows how Leibniz's principle can be applied to quantified terms.

<u>Proof</u> To begin with we observe for any $f, g, h$

$$
\begin{array}{ll}
 & (78) \\
= & \{(44); (58)\} \\
 & [(\underline{A}x :: [f.x = g.x]) \Rightarrow ((\underline{A}x :: h.(f.x)) \equiv (\underline{A}x :: h.(g.x)))] \\
= & \{[X \Rightarrow (Y \equiv Z) \ \equiv \ X \wedge Y \ \equiv \ X \wedge Z]; (62)\} \\
 & [(\underline{A}x :: [f.x = g.x] \wedge h.(f.x)) \equiv \\
 & \quad (\underline{A}x :: [f.x = g.x] \wedge h.(g.x))\ ] \\
= & \{[[a=b] \wedge h.a \equiv [a=b] \wedge h.b] \text{ with } a, b := f.x, g.x\} \\
 & [(\underline{A}x :: [f.x = g.x] \wedge h.(f.x)) \equiv \\
 & \quad (\underline{A}x :: [f.x = g.x] \wedge h.(f.x))] \\
= & \{\text{pred. calc}\} \\
 & \mathit{true}
\end{array}
$$

(End of Proof.)

And now we should be ready to show that universal quantification is monotonic, i.e.

(79) $(\underline{A}x :: [f.x \Rightarrow g.x]) \Rightarrow [(\underline{A}x :: f.x) \Rightarrow (\underline{A}x :: g.x)]$

<u>Proof</u> We observe for any $f, g$

$$
\begin{array}{ll}
 & [(\underline{A}x :: f.x) \Rightarrow (\underline{A}x :: g.x)] \\
= & \{\text{pred. calc.}\} \\
 & [(\underline{A}x :: f.x) \wedge (\underline{A}x :: g.x) \equiv (\underline{A}x :: f.x)] \\
= & \{(62)\}
\end{array}
$$

$$
\begin{array}{ll}
 & [(\underline{A}x{::}\ f.x \wedge g.x) \equiv (\underline{A}x{::}\ f.x)] \\
\Leftarrow & \{(78)\} \\
 & (\underline{A}x{::}\ [f.x \wedge g.x \ \equiv\ f.x]) \\
= & \{\text{pred. calc.}\} \\
 & (\underline{A}x{::}\ [f.x \Rightarrow g.x]) \quad .
\end{array}
$$

(End of Proof.)

An important manipulation relies on

(80) for any invertible function $t$

$$[(\underline{A}x{:}\ r.x{:}\ f.x) \equiv (\underline{A}y{:}\ r.(t.y){:}\ f.(t.y))] \quad .$$

In hints, we refer to this manipulation as "transforming the dummy"; in the special case that $t$ is the identity function, "renaming the dummy" is the usual hint.

We prove (80) by mutual implication from the fact that we have for any -not necessarily invertible- $t$

(81) $[(\underline{A}x{:}\ r.x{:}\ f.x) \Rightarrow (\underline{A}y{:}\ r.(t.y){:}\ f.(t.y))]$ ,

which we shall prove subsequently. Using trading we see that it suffices to prove these formulae with the range $true$ .

<u>Proof of (80)</u> We prove (80) by mutual implication. In the one direction the implication is stated by (81). For the implication in the other direction, we observe for any $f$ and invertible $t$

$$(\underline{A}y :: f.(t.y))$$

$$\Rightarrow \quad \{ (81) \text{ with } x, y, f, t := y, x, f \circ t, t^{-1} \}$$

$$(\underline{A}x :: f.(t.(t^{-1}.x)))$$

$$= \quad \{ t \circ t^{-1} \text{ is the identity function} \}$$

$$(\underline{A}x :: f.x) \quad .$$

(End of Proof of (80).)

Proof of (81) We observe for any $f, t$

$$[(\underline{A}x :: f.x) \Rightarrow (\underline{A}y :: f.(t.y))]$$

$$= \quad \{ \text{"}Q \Rightarrow\text{" distributes over } \underline{A} \}$$

$$[(\underline{A}y :: (\underline{A}x :: f.x) \Rightarrow f.(t.y))]$$

$$= \quad \{ (75) \text{ with } y := t.y \}$$

$$[(\underline{A}y :: true)]$$

$$= \quad \{ (70) \}$$

$$true \quad .$$

(End of Proof of (81).)

We close our discussion of the universal quantification with two monotonicity theorems.

We have for any monotonic predicate transformer $f$ and any bag $V$ of predicates

(82) $\quad [f.(\underline{A}X : X \in V : X) \Rightarrow (\underline{A}X : X \in V : f.X)]$ .

Proof We observe for any monotonic $f$ and any $V$, the range $X \in V$ being understood

$$[f.(\underline{A}X :: X) \Rightarrow (\underline{A}X :: f.X)]$$

$$= \quad \{ \text{"}Q \Rightarrow\text{" distributes over } \underline{A} \}$$

$$[(\underline{A}X :: f.(\underline{A}X :: X) \Rightarrow f.X)]$$

$=$ $\{$interchange of quantifications$\}$

$(\underline{A}X:: [f.(\underline{A}X::X) \Rightarrow f.X])$

$\Leftarrow$ $\{f$ is monotonic; so is $\underline{A}\}$

$(\underline{A}X:: [(\underline{A}X::X) \Rightarrow X])$

$=$ $\{(75)\,;\,(70)\}$

true .

(End of Proof.)

For an $f$ with a natural argument "the $f.i$ form a strengthening sequence" means

$$(\underline{A}\, i,j : 0 \leq i < j : [f.i \Leftarrow f.j]) \quad .$$

For $f$ and $g$ such that the $f.i$ and $g.j$ form strengthening sequences, we have

(83) $$[(\underline{A}\, i : 0 \leq i : f.i) \vee (\underline{A}\, j : 0 \leq j : g.j) \equiv (\underline{A}\, i : 0 \leq i : f.i \vee g.i)]$$

<u>Proof</u> To begin with we observe for any $f$ and $g$

$(\underline{A}\, i : 0 \leq i : f.i) \vee (\underline{A}\, j : 0 \leq j : g.j)$

$=$ $\{\vee$ distributes over $\underline{A}\}$

$(\underline{A}\, i : 0 \leq i : f.i \vee (\underline{A}\, j : 0 \leq j : g.j))$

$=$ $\{\vee$ distributes over $\underline{A}\}$

$(\underline{A}\, i : 0 \leq i : (\underline{A}\, j : 0 \leq j : f.i \vee g.j))$

$=$ $\{$unnesting$\}$

$(\underline{A}\, i,j : 0 \leq i \wedge 0 \leq j : f.i \vee g.j)$

$=$ $\{$predicate calculus$\}$

$(\underline{A}\, i,j : 0 \leq i \leq j \vee 0 \leq j \leq i : f.i \vee g.j)$

$=$ $\{$splitting the range$\}$

$(\underline{A}\, i,j : 0 \leq i \leq j : f.i \vee g.j) \wedge (\underline{A}\, i,j : 0 \leq j \leq i : f.i \vee g.j)$

Focussing our attention on the left conjunct we observe

left conjunct above<br>
$=$ {predicate calculus}<br>
$(\underline{A}i,j: 0 \leq i \leq j \wedge 0 \leq j: f.i \vee g.j)$<br>
$=$ {nesting the quantifications}<br>
$(\underline{A}j: 0 \leq j: (\underline{A}i: 0 \leq i \leq j: f.i \vee g.j))$<br>
$=$ {$\vee$ distributes over $\underline{A}$}<br>
$(\underline{A}j: 0 \leq j: (\underline{A}i: 0 \leq i \leq j: f.i) \vee g.j)$<br>
$=$ {f strengthening}<br>
$(\underline{A}j: 0 \leq j: f.j \vee g.j)$

For reasons of symmetry, the other conjunct has the same value, which combined observations — the conjunction being idempotent — conclude the proof.

(End of Proof.)

Existential quantification is the generalization of the disjunction and can now be defined by the analogue of de Morgan's Law:

(84) $[(\underline{E}x: r.x: f.x) \equiv \neg(\underline{A}x: r.x: \neg f.x)]$ .

It has all the properties you would expect it to have. The derivation of the formulae that are the dual of the ones we gave for universal quantification is left to the reader.

Austin, 1 March 1987

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