Copyright Notice

The calculus of boolean structures (Part 0)

We refer by the catchword "Leibniz" to the principle enunciated by Leibniz that a function applied to equal arguments yields equal values. This is usually expressed by the formula

$$x = y \Rightarrow f.x = f.y \quad .$$

Legenda It is generally understood that this formula holds for any function f and to any arguments x and y to which f is applicable. We have used an infix period to denote functional application; it has the highest binding power of all infix operators. The equality $=$ has a higher binding power than the implication $\Rightarrow$. Hence the above formula is a shorthand for

$$(x = y) \Rightarrow ((f.x) = (f.y)) \quad .$$

(End of Legenda.)

We shall appeal to the principle of Leibniz for named functions; most frequently, however, our appeal to it will be justified by the fact that all expressions we write down are functions of their subexpressions.

We recall our convention that, for x and y structures of some shape, $x = y$ stands for a boolean structure of that same shape; also, f

could be a structure-valued function. In order to adapt the principle of Leibniz to that convention we rewrite it as

$$[x = y] \Rightarrow [f.x = f.y] \quad .$$

(Since a non-structure can always be viewed as a structure on the trivial space consisting of the one anonymous point, our first formulation is a special instance of the above.)

In the following, we shall use the capital letters of the end of the alphabet - primarily X, Y, and Z - as variables of type boolean structure. For the equality between boolean operands we introduce the alternative symbol $\equiv$, which from a syntactical point of view distinguishes itself from $=$ only by the fact that (for reasons of convenience) it has been given a much lower binding power than $=$. An expression of the form $X \equiv Y$ is called "an equivalence" and is read as "X equivalent Y" or as "X equivales Y". The justification for a special symbol and a special name in the case of boolean operands is to be found in the circumstance that equivalence enjoys a property not enjoyed by the equality in general: equivalence is associative, i.e. we have for any X, Y, and Z

(0) $\quad [(X \equiv (Y \equiv Z)) \equiv ((X \equiv Y) \equiv Z)] \quad .$

Together with Leibniz's principle, (0) indeed expresses

associativity: it implies that wherever we have a sub-expression parenthesized as at the left-hand side of (0)'s central ≡-sign, the parentheses may be rearranged as at its right-hand side without changing the value of the total expression. For brevity's sake we shall never carry out these shunting operations in detail, justifying each step by an explicit appeal to (0). Instead, we shall feel free to insert into or remove from such continued equivalences parenthesis pairs as we see fit.

The other important property of the equivalence - remember that ≡ is only an alternative for = - is that it is symmetric; under the convention of omitting redundant parentheses we can state this by

(1) $\quad [X \equiv Y \equiv Y \equiv X]$.

In combination with the associativity of the equivalence, (1) is a rich formula:

- parenthesized as $[(X \equiv Y) \equiv (Y \equiv X)]$ it expresses the symmetry of the equivalence
- parenthesized as $[X \equiv (Y \equiv Y \equiv X)]$ it expresses that $Y \equiv Y$ is a left-identity element of the equivalence
- parenthesized as $[(X \equiv Y \equiv Y) \equiv X]$ it expresses that $Y \equiv Y$ is a right-identity element of the equivalence.

Since for an infix operator that has a left- and a right-hand identity element, the identity element is unique, we can give it a name. In the case of the equivalence, its customary name is "true", a convention properly captured by

(2) $[X \equiv true \equiv X]$.

Remark Here one could have the lurking suspicion that the equivalence has as many distinct identity elements as we can have spaces on which to define structures. Fortunately, we can also read the above introduction of true as stating that it is the identity element of the equivalence, whatever the underlying space (including the trivial one). The constant true is as unique as the zeroes in $0 + \sin.x$ and in $0 + \cos.y$ are the same zero ; the constant true is, in fact, as unique as the equivalence and the square brackets themselves. (End of Remark.)

The square brackets denote a unary operator operating on the enclosed, more precisely a function from boolean structures to the traditional boolean domain. Hence (0), (1), and (2) are normal boolean expressions, and, true being the identity element of the equivalence, we could have written instead of (2)

(2') $[X \equiv true \equiv X] \equiv true$;

for brevity's sake, we prefer (2).

Furthermore we equate a boolean value with a boolean structure on the trivial space consisting of the one anonymous point. Because the square brackets have all the properties of universal quantification over the underlying space, they reduce to the identity function when applied to a boolean expression. So we could have written as further alternatives to (2)

$$[[X \equiv true \equiv X]] \qquad \text{or}$$

$$[[X \equiv true \equiv X] \equiv true] \quad ;$$

again, we don't regard these as an improvement over (2).

Because $[X]$ is a boolean expression and, applied to a boolean expression, the square brackets reduce to the identity function, we have

(3) $$[[X]] \equiv [X] \quad ,$$

the square bracketing is idempotent.

Formulae (0) through (3) state properties of $\equiv$, true, and $[\,]$. We use them as axioms – later, when we introduce more connectives, we shall give more axioms –. We use them to compute values as implied by their truth, as illustrated by the following (simple) proof.

Theorem. Equivalence is reflexive, i.e. we have for any boolean structure X

(4) $[X \equiv X]$.

Proof We observe for any X

$[X \equiv X]$
$=$ { (2), parenthesized $[X \equiv (\text{true} \equiv X)]$
$[X \equiv \text{true} \equiv X]$
$=$ { (2), or (2'), if you prefer }
true .

(End of Proof.)

Remark Note how, in the first hint, we did not need to identify the subexpression being replaced. (End of Remark).

Finally we derive for the identity element of the equivalence

(5) $[\text{true}]$

by calculating for some X

$[\text{true}]$
$=$ { (2), parsed $[\text{true} \equiv (X \equiv X)]$
$[X \equiv X]$
$=$ { (4) }
true ,

a result in accordance with an earlier announced property of square bracketing. So much for the equivalence.

* *
*

It is time to introduce our next infix operator; it is called the disjunction, it is written as "$\vee$" and read as "or". We give it a higher binding power than the equivalence.

The disjunction is postulated to be symmetric, i.e. we have for any X and Y

(6) $\quad [X \vee Y \equiv Y \vee X]$;

to be associative, i.e. we have for any X, Y, and Z

(7) $\quad [X \vee (Y \vee Z) \equiv (X \vee Y) \vee Z]$;

to be idempotent, i.e. we have for any X

(8) $\quad [X \vee X \equiv X]$;

to distribute over equivalence, i.e. we have for any X, Y, and Z

(9) $\quad [X \vee (Y \equiv Z) \equiv X \vee Y \equiv X \vee Z]$.

Theorem The constant true is the zero-element of the disjunction, i.e. we have for any X

(10) $\quad [X \vee \text{true} \equiv \text{true}]$.

Remark The shorter statement $[X \vee \text{true}]$ would have disguised the zero-element. (End of Remark.)

Proof We observe for any X and Y

$$\begin{aligned} & X \vee \text{true} \\ = \; & \{ (2) \text{ with } X := Y \} \end{aligned}$$

$$
\begin{array}{ll}
 & X \vee (Y \equiv Y) \\
= & \{(9) \text{ with } Z := Y\} \\
 & X \vee Y \equiv X \vee Y \\
= & \{(2) \text{ with } X := X \vee Y\} \\
 & \text{true} \quad .
\end{array}
$$

(End of Proof.)

At this stage we can use (6), (7), and (8) to show the following

Theorem The disjunction distributes over itself, i.e. we have for any X, Y, and Z

(11) $\quad [X \vee (Y \vee Z) \equiv (X \vee Y) \vee (X \vee Z)] \quad .$

Proof We observe for any X, Y, Z

$$
\begin{array}{ll}
 & (X \vee Y) \vee (X \vee Z) \\
= & \{(7), \text{i.e. } \vee \text{ is associative}\} \\
 & X \vee (Y \vee X) \vee Z \\
= & \{(6), \text{i.e. } \vee \text{ is symmetric}\} \\
 & X \vee (X \vee Y) \vee Z \\
= & \{(7), \text{i.e. } \vee \text{ is associative}\} \\
 & (X \vee X) \vee (Y \vee Z) \\
= & \{(8), \text{i.e. } \vee \text{ is idempotent}\} \\
 & X \vee (Y \vee Z)
\end{array}
$$

(End of Proof.)

Remark In the above we have written more parentheses than we shall do in the future. The "auto-distribution" holds for any operator that is symmetric, associative, and idempotent. (End of Remark.)

* * *

It is time to introduce a next operator. The shortest total argument would result from introducing the negation first and then defining the conjunction in terms of negation and disjunction (i.e. by postulating one of the Laws of de Morgan.) We shall not do so, firstly because it is the usual order -and it is always nice to show an alternative-, and secondly because it disguises the fact that conjunction can be introduced prior to the introduction of the negation.

Our next infix operator is called the conjunction; it is written as "$\wedge$" and read as "and". For reasons of symmetry (which will become apparent later) we give it the same binding power as the disjunction. The conjunction is defined by postulating for any X, Y

(12) $$[X \wedge Y \equiv X \equiv Y \equiv X \vee Y]$$

(also known as "The Golden Rule").

Theorem The conjunction is symmetric, i.e. we have for any X, Y

(13) $$[X \wedge Y \equiv Y \wedge X] \quad .$$

Proof We observe for any X, Y

$$\begin{array}{ll} & X \wedge Y \\ = & \{(12)\} \\ & X \equiv Y \equiv X \vee Y \end{array}$$

$=$ { associativity and symmetry of $\equiv$; symmetry of $\vee$ }

$Y \equiv X \equiv Y \vee X$

$=$ { (12) with $X, Y := Y, X$ }

$Y \wedge X$.

(End of Proof.)

Theorem The conjunction is associative, i.e. we have for any X, Y, Z

(14) $[X \wedge (Y \wedge Z) \equiv (X \wedge Y) \wedge Z]$.

Proof We observe for any X, Y, Z

$X \wedge (Y \wedge Z)$

$=$ { Golden Rule }

$X \equiv Y \wedge Z \equiv X \vee (Y \wedge Z)$

$=$ { Golden Rule }

$X \equiv Y \wedge Z \equiv X \vee (Y \equiv Z \equiv Y \vee Z)$

$=$ { Golden Rule; $\vee$ distributes over $\equiv$ }

$X \equiv Y \equiv Z \equiv Y \vee Z \equiv X \vee Y \equiv X \vee Z \equiv X \vee Y \vee Z$

which, thanks to the associativity and symmetry of $\equiv$ and $\vee$, is symmetric in X, Y, and Z; this last observation concludes the proof.

(End of Proof)

Theorem The conjunction is idempotent, i.e. we have for any X

(15) $[X \wedge X \equiv X]$.

Proof We observe for any X

$$
\begin{array}{ll}
 & X \wedge X \\
= & \quad \{(12) \text{ with } Y := X\} \\
 & X \equiv X \equiv X \vee X \\
= & \quad \{(2), \text{ i.e. identity element of } \equiv\} \\
 & X \vee X \\
= & \quad \{(8), \text{ i.e. idempotency of } \vee\} \\
 & X \quad .
\end{array}
$$

(End of Proof.)

Theorem The constant true is the identity element of the conjunction, i.e. we have for any X

$$[X \wedge \text{true} \equiv X] \qquad (16)$$

Proof We observe for any X

$$
\begin{array}{ll}
 & X \wedge \text{true} \\
= & \quad \{(12) \text{ with } Y := \text{true}\} \\
 & X \equiv \text{true} \equiv X \vee \text{true} \\
= & \quad \{(10), \text{ i.e. zero element of } \vee\} \\
 & X \equiv \text{true} \equiv \text{true} \\
= & \quad \{\text{identity element of } \equiv\} \\
 & X \quad .
\end{array}
$$

(End of Proof.)

Theorem We have for any X, Y the Laws of Absorption

$$[X \wedge (X \vee Y) \equiv X] \qquad (17)$$

$$[X \vee (X \wedge Y) \equiv X] \quad , \qquad (18)$$

Proof We observe for any X, Y

$$
\begin{array}{ll}
 & X \wedge (X \vee Y) \\
= & \{\text{Golden Rule}\} \\
 & X \equiv X \vee Y \equiv X \vee X \vee Y \\
= & \{\text{idempotence of } \vee\} \\
 & X \equiv X \vee Y \equiv X \vee Y \\
= & \{\text{identity element of } \equiv\} \\
 & X \qquad ;
\end{array}
$$

the other proof is like the above, but with $\vee$ and $\wedge$ interchanged.

(End of Proof.)

Theorem Disjunction distributes over conjunction, i.e. we have for any X, Y, Z

$$(19) \qquad [\, X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z) \,] \; .$$

Proof We observe for any X, Y, Z

$$
\begin{array}{ll}
 & (X \vee Y) \wedge (X \vee Z) \\
= & \{\text{Golden Rule}\} \\
 & X \vee Y \equiv X \vee Z \equiv X \vee Y \vee X \vee Z \\
= & \{\text{properties of } \vee\} \\
 & X \vee Y \equiv X \vee Z \equiv X \vee Y \vee Z \\
= & \{\vee \text{ distributes over } \equiv\} \\
 & X \vee (Y \equiv Z \equiv Y \vee Z) \\
= & \{\text{Golden Rule}\} \\
 & X \vee (Y \wedge Z) \; .
\end{array}
$$

(End of Proof.)

Theorem Conjunction distributes over disjunction, i.e.

(20) $[X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)]$

Proof We observe for any X, Y, Z

$$
\begin{aligned}
& (X \wedge Y) \vee (X \wedge Z) \\
= & \quad \{(19) \text{ with } X, Y := (X \wedge Y), X\} \\
& ((X \wedge Y) \vee X) \wedge ((X \wedge Y) \vee Z) \\
= & \quad \{(19) \text{ with } Z := X \ ; \ (19) \text{ with } X, Z := Z, X\} \\
& (X \vee X) \wedge (X \vee Y) \wedge (X \vee Z) \wedge (Y \vee Z) \\
= & \quad \{\vee \text{ is idempotent}\} \\
& X \wedge (X \vee Y) \wedge (X \vee Z) \wedge (Y \vee Z) \\
= & \quad \{(17), \text{ i.e. absorption}\} \\
& X \wedge (X \vee Z) \wedge (Y \vee Z) \\
= & \quad \{\text{absorption again}\} \\
& X \wedge (Y \vee Z) \quad .
\end{aligned}
$$

(End of Proof.)

Remark Whereas disjunction distributes over equivalence, conjunction, in general, does not. This is the reason why we have proved the last two theorems separately. In connection with the negation we shall discuss the extent to which conjunction distributes over equivalence; then we shall see that the last proof with $\vee$ and $\wedge$ interchanged demonstrates the preceding theorem. (End of Remark.)

* * *

It is time to introduce the prefix operator called negation; it is written "¬" and read as "non". We give it a higher binding power than ∨ and ∧. We postulate separately its properties with respect to the equivalence and the disjunction; its properties with respect to the conjunction will then be derived.

Negation and equivalence are connected in that we have for any X,Y

(21) $[\neg(X \equiv Y) \equiv \neg X \equiv Y]$.

Theorem We have for any X,Y

(22) $[\neg X \equiv Y \equiv X \equiv \neg Y]$.

Proof We observe for any X,Y

$$
\begin{aligned}
& \neg X \equiv Y \\
= & \quad \{(21)\} \\
& \neg(X \equiv Y) \\
= & \quad \{\text{symmetry of } \equiv\text{; (21) with } X,Y := Y,X\} \\
& X \equiv \neg Y \quad .
\end{aligned}
$$

(End of Proof)

Theorem Negation is its own inverse, i.e. we have for any X

$$[\neg\neg X \equiv X] \quad .$$

Proof We observe for any X

```
    ¬¬X ≡ X
=     { (22) with  Y:= ¬X }
    ¬X ≡ ¬X
=     { identity element of ≡ }
    true
```

(End of Proof.)

Negation and disjunction are connected by the famous Law of the Excluded Middle, i.e. we have for any X

(23) $[X \vee \neg X]$.

In order to investigate what we can derive from (21) and (23) together, we substitute in (23) $(X \equiv Y)$ for X, i.e.

we observe for any X, Y

```
    true
=     { (23) with  X:= (X≡Y) }
    [(X≡Y) ∨ ¬(X≡Y)]
=     { (21) }
    [(X≡Y) ∨ (¬X≡Y)]
=     { ∨ distributes over ≡ }
    [X∨¬X ≡ Y∨¬X ≡ X∨Y ≡ Y∨Y]
=     { (23); identity element of ≡ }
    [Y∨¬X ≡ X∨Y ≡ Y∨Y]
=     { idempotence of ∨ }
    [Y∨¬X ≡ X∨Y ≡ Y]
```

$$= \quad \{\text{Golden Rule}\}$$
$$[Y \vee \neg X \equiv X \wedge Y \equiv X] \quad .$$

Thus we have proved the
Theorem. We have for any X, Y

(24) $\quad [\neg X \vee Y \equiv X \vee Y \equiv Y]$
(25) $\quad [\neg X \vee Y \equiv X \wedge Y \equiv X]$.

Remark For the variation we have chosen to explore a calculational opportunity, just to see what theorems we would come up with. Platonists would say that we have "discovered" two new theorems. (End of Remark.)

Theorem We have for any X, Y

(26) $\quad [\neg X \vee \neg Y \equiv \neg(X \wedge Y)]$
(27) $\quad [\neg X \wedge \neg Y \equiv \neg(X \vee Y)]$,

known as the Laws of Augustus de Morgan (who, ironically, lacked a notation for the negation of an arbitrary expression: he had to name it with a single letter and the corresponding letter from the other – i.e. upper or lower- case would then stand for its negation).

Proof We observe for any X, Y

$$\neg X \vee \neg Y$$
$$= \quad \{(24) \text{ with } Y := \neg Y\}$$
$$X \vee \neg Y \equiv \neg Y$$
$$= \quad \{(24) \text{ with } X, Y := Y, X\}$$

$$
\begin{aligned}
& Y \vee X \equiv X \equiv \neg Y \\
= \quad & \{ (21) \} \\
& \neg (Y \vee X \equiv X \equiv Y) \\
= \quad & \{ \text{Golden Rule} \} \\
& \neg (X \wedge Y) \quad .
\end{aligned}
$$

With the aid of (22), (27) is easily calculated from (26).

(End of Proof.)

With the constant false defined by

(28) $[\text{false} \equiv \neg \text{true}]$,

we can formulate the

<u>Theorem</u> The constant false is the identity element of the disjunction and the zero element of the conjunction, i.e. we have for any X

(29) $[X \vee \text{false} \equiv X]$

(30) $[X \wedge \text{false} \equiv \text{false}]$.

We leave the proofs to the reader.

For the sake of completeness we mention yet another infix operator, called the discrepancy, written as "$\not\equiv$" and read "differs from". It is symmetric and associative; being mutually associative with the equivalence, it has been given the same low binding power. It is defined by

(31) $[X \not\equiv Y \equiv \neg (X \equiv Y)]$.

Theorem The constant false is the identity element of the discrepancy, i.e. we have for any X

(32) $[X \not\equiv \text{false} \equiv X]$.

Theorem The conjunction distributes over the discrepancy, i.e. we have for any X, Y, Z

(33) $[X \wedge (Y \not\equiv Z) \equiv X \wedge Y \not\equiv X \wedge Z]$.

The last theorem is about the only reason for mentioning the discrepancy at all. The proofs are left to the reader.

Remark Nothing in our axioms prevents us from choosing for the negation the identity operator. From the Excluded Middle we immediately derive for any X $[X]$ -or $[X \equiv \text{true}]$, if we wish to be more explicit-. The only thing wrong with the model in which true is essentially the one and only predicate is that it is void of interest. Hence our interest is restricted to those models in which $[X]$ holds only for X the predicate true and for none of the other predicates, of which at least one exists. The rejection of the noninteresting model is more than we care to formalize. (End of Remark.)

* * *

In the above we have gone in great detail

through about three dozen formulae. Some might even argue that we spent more pages than the topic deserves. This, however, is not confirmed by the general experience (of us and of others). In the teaching of this material, two handicaps are quite common.

The one handicap consists in an audience that has used boolean expressions in programming and therefore believes that it knows all these things already. Upon closer inspection, it usually knows the connectives -e.g. by way of a "truth table"- but has very few of their properties at its fingertips. And it is these properties, i.e. the rules of manipulation, that are the topic of this chapter and that we wish to convey.

The other handicap consists in an audience which has been introduced to logic by philosophers. Such an audience can become very uneasy about our use of the associativity of the equivalence, because that use does not reflect human reasoning, which, according to some philosophers, logic has to model. Without denying the associativity of the equivalence, some people argue against its use because it is "unnatural" or "counterintuitive".

We grant the latter in that (at least Western)

languages are rather poor at expressing equivalence. By all linguistic standards the sentence "Tom can see with both eyes if and only if Tom can see with only one eye if and only if Tom is blind." is - probably for its blatant syntactic ambiguity - total gibberish. But for us this is no reason to disqualify the equivalence. On the contrary, if our formalism allows simple calculations that are beyond the unaided mind because their verbal rendering would be too baffling, so much the better. In this respect we are totally pragmatic, and it was in that vein that we stressed the algebraic nature of the calculus.

It is here that we would like to make two remarks in connection with the Golden Rule. The first remark is concerned with set theory.

A possible model for our boolean structures is provided by the boolean functions defined on some space, with all logical operators to be applied point-wise. The next step is to associate with each boolean structure the subset of points of which it is the characteristic function. (Or, the other way round, we associate with each subset of points its membership function as its corresponding boolean structure.)

We can now try to translate our logical con-

nectives in set-theoretical notation. For the disjunction and the conjunction this is easy: disjunction corresponds to the union $\cup$ and conjunction to the intersection $\cap$. With the equivalence we have the problem that it would yield - for two operands - the set of points belonging to both sets or to neither, and set theory shuns operators that yield sets containing elements that don't belong to at least one of the operands. Fortunately, there is what is called "the symmetric set difference" $\div$ - known in electrical engineering as "the exclusive or" - : the elements belonging to one set but not to the other; it corresponds to our discrepancy $\neq$ and in set theory the associativity of the symmetric set difference is known.

In order to render the Golden Rule in standard set-theoretical notation, we have to replace two equivalences by discrepancies, whereas the last one is replaced by the equality sign that has to carry the burden of the square brackets. In books on set theory we may thus find the following "different" theorems

$$A = B \div (A \cap B) \div (A \cup B)$$
$$A \div B = (A \cap B) \div (A \cup B)$$
$$(A \cap B) = A \div B \div (A \cup B)$$
$$(A \cup B) = A \div B \div (A \cap B)$$

$$A \div (A \cup B) \;=\; B \div (A \cap B) \quad ,$$

in which we recognize five clumsy renderings of the Golden Rule. The above is a striking example of how inadequate notation can generate spurious diversification. We hope it reinforces our urgent recommendation not to translate our formulae into set-theoretical notation and concepts so as to make them "easier to understand".

Our second remark aims at removing some of the surprise that the Golden Rule usually evokes at first encounter. Remember the stage we were in when we had equivalence and disjunction, both symmetric and associative, and disjunction idempotent and distributing over equivalence. When we raise the question: "What nice new expressions can we now write down?", the distributivity tells us that we can confine ourselves to (continued) equivalences of (single variables and) disjunctions of single variables. In two variables X and Y, $X \equiv Y \equiv X \vee Y$ is the only new one that is symmetric, and this observation invites the study of that expression for which we introduce the short-hand notation $X \wedge Y$. So, whereas the introduction of the negation was the introduction of something really new, the introduction of the conjunction was in essence no more than a study of what we already

had.

The above is such a nice way of coming up with the conjunction that it immediately raises the question whether we can repeat the game. Given $\equiv$ and $\vee$, can we think of another nice expression? The remark that we can confine ourselves (continued) equivalences of (single variables and) disjunctions still holds, but we can forsake symmetry and consider $X \vee Y \equiv Y$. Is it nice? Apart from being asymmetric, it is nice, as follows from the little theory, given below. (We give the little theory in isolation because it is perfectly general. For simplicity's sake, we formulate it for non-structures, so we don't need to bother about square brackets.)

Little Theory We consider an infix operator $\bullet$ and a binary relation $\rightarrow$, defined in terms of $\bullet$ by

* $$x \rightarrow y \equiv x \bullet y = y$$

(Here the order of decreasing binding power of the operators is $\bullet$, $\rightarrow$ and $=$, $\wedge$ and $\vee$, $\equiv$.)

Theorem ($\bullet$ is idempotent) $\equiv$ ($\rightarrow$ is reflexive), i.e.

$$(\underline{A}x :: x \bullet x = x) \equiv (\underline{A}x :: x \rightarrow x) .$$

Proof We observe

$$
\begin{array}{ll}
 & (\underline{A}x::\ x\bullet x = x) \\
= & \quad \{ * \text{ with } y := x \} \\
 & (\underline{A}x::\ x \to x) \quad .
\end{array}
$$

(End of Proof)

Theorem ($\bullet$ is associative) $\Rightarrow$ ($\to$ is transitive) .

Proof We observe for any x, y, z

$$
\begin{array}{ll}
 & x \to y \ \wedge\ y \to z \\
= & \quad \{ *\ ;\ * \text{ with } x, y := y, z \} \\
 & x \bullet y = y \ \wedge\ y \bullet z = z \\
\Rightarrow & \quad \{ \text{Leibniz} \} \\
 & (x \bullet y) \bullet z = z \ \wedge\ y \bullet z = z \\
= & \quad \{ \bullet \text{ is associative} \} \\
 & x \bullet (y \bullet z) = z \ \wedge\ y \bullet z = z \\
\Rightarrow & \quad \{ \text{Leibniz} \} \\
 & x \bullet z = z \\
= & \quad \{ * \text{ with } y := z \} \\
 & x \to z \quad .
\end{array}
$$

(End of Proof.)

Theorem ($\bullet$ is symmetric) $\Rightarrow$ ($\to$ is antisymmetric)
(Antisymmetry of $\to$ means that for any x, y
$(x \to y \ \wedge\ y \to x) \Rightarrow (x = y)$.)

Proof. We observe for any x, y

$$
\begin{array}{ll}
 & x \to y \ \wedge\ y \to x \\
= & \quad \{ *\ ;\ * \text{ with } x, y := y, x \} \\
 & x \bullet y = y \ \wedge\ y \bullet x = x \\
= & \quad \{ \bullet \text{ is symmetric} \} \\
 & x \bullet y = y \ \wedge\ x \bullet y = x \\
\Rightarrow & \quad \{ \text{Leibniz} \} \\
 & x = y \quad .
\end{array}
$$

(End of Proof.)

Theorem With $\circ\!\!\!\!\circ$ a unary prefix operator
($\circ\!\!\!\!\circ$ distributes over $\bullet$) $\Rightarrow$
($\circ\!\!\!\!\circ$ is monotonic with respect to $\rightarrow$) .

Proof We observe for any x, y

$$
\begin{array}{ll}
 & \circ\!\!\!\!\circ x \rightarrow \circ\!\!\!\!\circ y \\
= & \quad \{ * \text{ with } x, y := \circ\!\!\!\!\circ x, \circ\!\!\!\!\circ y \} \\
 & \circ\!\!\!\!\circ x \bullet \circ\!\!\!\!\circ y = \circ\!\!\!\!\circ y \\
= & \quad \{ \circ\!\!\!\!\circ \text{ distributes over } \bullet \} \\
 & \circ\!\!\!\!\circ (x \bullet y) = \circ\!\!\!\!\circ y \\
\Leftarrow & \quad \{ \text{Leibniz} \} \\
 & x \bullet y = y \\
= & \quad \{ * \} \\
 & x \rightarrow y \quad .
\end{array}
$$

(End of Proof.)

Since -as we have seen in connection with $\vee$- $\bullet$ distributes over itself if $\bullet$ is associative, idempotent and symmetric, we have the

Corollary
($\bullet$ is associative, idempotent, and symmetric) $\Rightarrow$
($\bullet$ is monotonic with respect to $\rightarrow$) .

Theorem (1 is a left-hand unit element of $\bullet$) $\equiv$
(1 is a left-hand extreme of $\rightarrow$)

Proof
$$
\begin{array}{ll}
 & (\underline{A}\, y :: \; 1 \bullet y \equiv y) \\
= & \quad \{ * \text{ with } x := 1 \} \\
 & (\underline{A} y :: \; 1 \rightarrow y) \quad .
\end{array}
$$

(End of Proof.)

Theorem (0 is a right-hand zero element of $\bullet$) $\equiv$
(0 is a right-hand extreme of $\rightarrow$) .

Proof $(\underline{A}x :: x \bullet 0 = 0)$
$= \{ * \text{ with } y := 0 \}$
$(\underline{A}x :: x \rightarrow 0)$.

(End of Proof.)

This little theory, which, regrettably, is not widely known, is as beautiful as its proofs are simple. (End of Little Theory.)

Since $\vee$ is associative, symmetric, and idempotent, has zero element true and unit element false, the above little theory tells us that $X \vee Y \equiv Y$ is, indeed, a nice expression that begs the introduction of the asymmetric infix operator $\Rightarrow$, called "implication" and read as "implies", by postulating

(34) $[X \Rightarrow Y \equiv X \vee Y \equiv Y]$;

we give $\Rightarrow$ a higher binding power than $\equiv$, but a lower binding power than $\vee$ and $\wedge$. We identify it with the implication as we have used it all the time.

Our little theory tells us

(35) $[X \Rightarrow X]$

(36) $[(X \Rightarrow Y) \wedge (Y \Rightarrow Z) \Rightarrow (X \Rightarrow Z)]$

(37) $[(X \Rightarrow Y) \wedge (Y \Rightarrow X) \Rightarrow X \equiv Y]$

(38) $[(X \Rightarrow Y) \Rightarrow (X \vee Z \Rightarrow Y \vee Z)]$

(39) $[\text{false} \Rightarrow X]$

(40) $[X \Rightarrow \text{true}]$.

Since the properties of the disjunction that we used are shared by the conjunction, it stands to reason to introduce analogously the consequence, written as "$\Leftarrow$" and pronounced as "follows from" by

(41) $[X \Leftarrow Y \equiv X \wedge Y \equiv Y]$;

the consequence is given the same binding power as the implication. On account of (34), (41), and the Golden Rule we have

(42) $[X \Leftarrow Y \equiv Y \Rightarrow X]$;

for that reason we shall abstain from deriving the analogous formulae for the consequence with the exception of the analogue of (38):

(43) $[(X \Leftarrow Y) \Rightarrow (X \wedge Z \Leftarrow Y \wedge Z)]$.

Remark Note that the theorem "A conjunctive predicate transformer is monotonic", whose proof was used to illustrate our proof format, is a special case of the theorem about the unary operator ω from our Little Theory. (End of Remark.)

We shall close this section with a few further formulae about the implication; in view of (42), the analogous ones about the consequence are omitted.

(44) $[X \Rightarrow Y \equiv \neg X \vee Y]$

(45) $[\text{true} \Rightarrow X \equiv X]$

(46) $[X \Rightarrow \text{false} \equiv \neg X]$

(47) $[X \Rightarrow X \vee Y]$

(48) $[X \wedge Y \Rightarrow X]$

(49) $[(U \Rightarrow Y) \wedge (X \Rightarrow Z) \Rightarrow (U \wedge X \Rightarrow Y \wedge Z)]$

(50) $[(U \Rightarrow Y) \wedge (X \Rightarrow Z) \Rightarrow (U \vee X \Rightarrow Y \vee Z)]$

(51) $[(X \Rightarrow Y) \wedge (Y \Rightarrow X) \equiv X \equiv Y]$

(52) $[X \wedge Y \Rightarrow Z \equiv X \Rightarrow \neg Y \vee Z]$

We leave their proofs as exercises for the reader.

Being asymmetric and not associative, the implication is not pleasant to manipulate: there are too many formulae for the manipulation of the implication. The situation is aggravated by

(53) $[X \Rightarrow Y \equiv \neg X \Leftarrow \neg Y]$,

as follows immediately from (44). In our proofs, brevity is one goal; limitation of the repertoire of manipulations is another goal. For the sake of the latter, we are willing to add one or two steps if by doing so we can avoid appealing to a less attractive manipulation of the implication.

* * *

The unary operator denoted by square brackets is a function from boolean structures to the two-valued boolean domain {true, false}. It has all the properties of universal quantification over a non-empty range, i.e.

(54) $[\text{true}] \equiv \text{true}$

(55) $[\text{false}] \equiv \text{false}$

(56) $[[X]] \equiv [X]$ - i.e. it is idempotent -

(57) $[X \wedge Y] \equiv [X] \wedge [Y]$ - i.e. it distributes over $\wedge$ -

(58) $b \vee [X] \equiv [b \vee X]$ - with $b \in \{\text{true}, \text{false}\}$.

Austin, 16 February 1987

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