The algebraic core of a propositional logic

This note deals with the following theorem.

For a nonempty domain E, there exist the operators $\rightsquigarrow$ of type $E^2 \to E$, $\bullet$ of type $E \to E$, and $[\ldots]$ of type $E \to bool$. The prefix operator $\bullet$ is given a higher syntactic binding power than the infix $\rightsquigarrow$.

Universal quantification over a, b, c is often left implicit. The operators satisfy

(0, W) $\quad [a \rightsquigarrow (b \rightsquigarrow a)]$

(0, D) $\quad [(a \rightsquigarrow (b \rightsquigarrow c)) \rightsquigarrow ((a \rightsquigarrow b) \rightsquigarrow (a \rightsquigarrow c))]$

(0, C) $\quad [(\bullet a \rightsquigarrow b) \rightsquigarrow ((\bullet a \rightsquigarrow \bullet b) \rightsquigarrow a)]$

(0, MP) $\quad [a] \wedge [a \rightsquigarrow b] \Rightarrow [b]$.

(The four names are short for Weakening, Distribution, Contradiction and Modus Ponens respectively.)

In terms of the above we now define the relations $\sqsubseteq$ and $\simeq$, both of type $E^2 \to bool$:

(1) $\quad a \sqsubseteq b \equiv [a \rightsquigarrow b]$

(2) $\quad a \simeq b \equiv a \sqsubseteq b \wedge b \sqsubseteq a$.

(In view of the types, no further binding powers need to be defined.)

Then

(i) $\sqsubseteq$ is a preorder (i.e. is reflexive and transitive)

(ii) $\rightsquigarrow$ and $\bullet$ "preserve $\simeq$" (see later)

(iii) $(E/\simeq, \sqsubseteq)$ is a boolean lattice, i.e. there exist

operators $\uparrow, \downarrow, \sim$ which "preserve $\simeq$" and satisfy

(iii, supremum) $\quad a \uparrow b \sqsubseteq c \;\equiv\; a \sqsubseteq c \wedge b \sqsubseteq c$

(iii, infimum) $\quad a \sqsubseteq b \downarrow c \;\equiv\; a \sqsubseteq b \wedge a \sqsubseteq c$

(iii, shunting) $\quad a \downarrow b \sqsubseteq c \;\equiv\; b \sqsubseteq \sim a \uparrow c$

* * *

To begin with we rewrite the properties (0), introducing $\sqsubseteq$ via (1):

(3, W) $\quad a \sqsubseteq b \rightsquigarrow a$

(3, D) $\quad a \rightsquigarrow (b \rightsquigarrow c) \sqsubseteq (a \rightsquigarrow b) \rightsquigarrow (a \rightsquigarrow c)$

(3, C) $\quad \cdot a \rightsquigarrow b \sqsubseteq (\cdot a \rightsquigarrow \cdot b) \rightsquigarrow a$

(3, MP) $\quad a \sqsubseteq b \;\Rightarrow\; ([a] \Rightarrow [b])$

Note that in deriving (3, MP) we have also applied shunting from the predicate calculus; we have done so in order to express clearly that MP is a monotonicity property of $[\ldots]$. Note also that the above was just a rewriting: formulae (3) are equivalent to formulae (0).

Matching the $\sqsubseteq$ of (3, MP) with the $\sqsubseteq$'s in the preceding 3 properties, we derive, again via (1)

(4, W) $\quad [a] \Rightarrow b \sqsubseteq a$

(4, D) $\quad a \sqsubseteq b \rightsquigarrow c \;\Rightarrow\; a \rightsquigarrow b \sqsubseteq a \rightsquigarrow c$

(4, C) $\quad \cdot a \sqsubseteq b \;\Rightarrow\; \cdot a \rightsquigarrow \cdot b \sqsubseteq a$.

(Because (3, MP) is an implication, formulae (4) are weaker than the corresponding formulae (3).)

The consequents of formulae (4) have all the form of the antecedent of (3,MP), so we can use the latter again. Thus we derive (with shunting from the predicate calculus)

(5,W) $\quad [a] \wedge [b] \Rightarrow [a]$

(5,D) $\quad a \sqsubseteq b \rightsquigarrow c \;\wedge\; a \sqsubseteq b \;\Rightarrow\; a \sqsubseteq c$

(5,C) $\quad \cdot a \sqsubseteq b \;\wedge\; \cdot a \sqsubseteq \cdot b \;\Rightarrow\; [a]$

Conclusion (5,W) gives us nothing new, (5,D) will be used in a moment, and (5,C) nicely reflects the Reductio ad Absurdum.

* * *

After the above explorations we are ready to tackle section (i) of our proof obligation.

$\sqsubseteq$ is reflexive, i.e. for any a

(6) $\quad a \sqsubseteq a$

Proof We observe

$$
\begin{array}{ll}
 & a \sqsubseteq a \\
\Leftarrow & \quad \{ (5,D) \text{ with } c := a \} \\
 & \langle \exists b :: a \sqsubseteq b \rightsquigarrow a \;\wedge\; a \sqsubseteq b \rangle \\
\equiv & \quad \{ (3,W) \} \\
 & \langle \exists b :: a \sqsubseteq b \rangle \\
\Leftarrow & \quad \{ \text{instantiation } b := c \rightsquigarrow a \} \\
 & \langle \exists c :: a \sqsubseteq c \rightsquigarrow a \rangle \\
\equiv & \quad \{ (3,W) \text{ and } E \text{ nonempty} \} \\
 & \text{true}
\end{array}
$$

(End of Proof.)

$\sqsubseteq$ is transitive, i.e. for any a,b,c

(7) $\quad a \sqsubseteq b \wedge b \sqsubseteq c \Rightarrow a \sqsubseteq c$

Proof We observe for any a,b,c

$$
\begin{array}{ll}
 & a \sqsubseteq c \\
\Leftarrow & \quad \{ (5,\mathbb{D}) \} \\
 & a \sqsubseteq b \wedge a \sqsubseteq b \rightarrow c \\
\Leftarrow & \quad \{ (8), \text{ see below} \} \\
 & a \sqsubseteq b \wedge b \sqsubseteq c \quad .
\end{array}
$$

(End of Proof.)

Above we have used

(8) $\quad b \sqsubseteq c \Rightarrow a \sqsubseteq b \rightarrow c$

(which could deserve a number in its own right).

Proof We observe for any a,b,c

$$
\begin{array}{ll}
 & a \sqsubseteq b \rightarrow c \\
\Leftarrow & \quad \{ (4,W) \text{ with } a,b := b \rightarrow c, a \} \\
 & [b \rightarrow c] \\
\equiv & \quad \{ (1) \} \\
 & b \sqsubseteq c
\end{array}
$$

(End of Proof.)

Thanks to the reflexivity of $\sqsubseteq$ we derive from $(4,\mathbb{D})$ with $a := b \rightarrow c$

(9) $\quad (b \rightarrow c) \rightarrow b \sqsubseteq (b \rightarrow c) \rightarrow c \quad .$

The transitivity of $\sqsubseteq$ will be exploited by admitting $\sqsubseteq$ in the left column of our proof

format.

Finally we conclude from (2), (6) & (7):

(10) $a \simeq a$ i.e. $\simeq$ is reflexive
$a \simeq b \equiv b \simeq a$ i.e. $\simeq$ is symmetric
$a \simeq b \wedge b \simeq c \Rightarrow a \simeq c$ i.e. $\simeq$ is transitive,

hence $\simeq$ is an equivalence relation (as already suggested by the symbol chosen). Because of the transitivity, also $\simeq$ can be admitted in the left column of our proof format.

This concludes the proof of (i) and our discussion of its immediate consequences.

* * *

The time has come to turn to proof obligation (ii) and we shall start with "$\rightsquigarrow$ preserves $\simeq$", which is short for "the prefix operator $a \rightsquigarrow$ preserves $\simeq$", i.e.

(11) $b \simeq c \Rightarrow a \rightsquigarrow b \simeq a \rightsquigarrow c$

and "the postfix operator $\rightsquigarrow c$ preserves $\simeq$", i.e.

(12) $a \simeq b \Rightarrow a \rightsquigarrow c \simeq b \rightsquigarrow c$.

By virtue of definition (2) of $\simeq$, predicate calculus and symmetry, (11) follows from

(13,M) $b \sqsubseteq c \Rightarrow a \rightsquigarrow b \sqsubseteq a \rightsquigarrow c$,

while, similarly, (12) follows from

(13,AM) $\quad a \sqsubseteq b \;\Rightarrow\; b \rightsquigarrow c \sqsubseteq a \rightsquigarrow c$.

(Here M and AM are short for Monotonicity and Anti-Monotonicity respectively.) Formulae (13) follow via (3,MP) and definition (1) of $\sqsubseteq$, directly from

(14, M) $\quad b \rightsquigarrow c \sqsubseteq (a \rightsquigarrow b) \rightsquigarrow (a \rightsquigarrow c)$ and
(14,AM) $\quad a \rightsquigarrow b \sqsubseteq (b \rightsquigarrow c) \rightsquigarrow (a \rightsquigarrow c)$ respectively.

For the proof of (14,M) we observe

$$
\begin{array}{ll}
 & b \rightsquigarrow c \\
\sqsubseteq & \quad \{(3,W) \text{ with } a,b := b \rightsquigarrow c,\ a\} \\
 & a \rightsquigarrow (b \rightsquigarrow c) \\
\sqsubseteq & \quad \{(3,D)\} \\
 & (a \rightsquigarrow b) \rightsquigarrow (a \rightsquigarrow c) \quad ;
\end{array}
$$

the transitivity of $\sqsubseteq$ then completes the proof.

For the proof of (14,AM) we observe

$$
\begin{array}{ll}
 & a \rightsquigarrow b \sqsubseteq (b \rightsquigarrow c) \rightsquigarrow (a \rightsquigarrow c) \\
\Leftarrow & \quad \{(3,W) \text{ and transitivity of } \sqsubseteq\} \\
 & (b \rightsquigarrow c) \rightsquigarrow (a \rightsquigarrow b) \sqsubseteq (b \rightsquigarrow c) \rightsquigarrow (a \rightsquigarrow c) \\
\Leftarrow & \quad \{(4,D)\} \\
 & b \rightsquigarrow c \sqsubseteq (a \rightsquigarrow b) \rightsquigarrow (a \rightsquigarrow c) \\
\equiv & \quad \{(14,M)\} \\
 & \text{true} \quad ,
\end{array}
$$

and this completes the proof that $\rightsquigarrow$ preserves $\simeq$.

The antimonotonicity enables us to prove the useful shunting rules

(15, S) $\quad a \rightsquigarrow (b \rightsquigarrow c) \simeq b \rightsquigarrow (a \rightsquigarrow c)$

(16, S) $\quad a \sqsubseteq b \rightsquigarrow c \equiv b \sqsubseteq a \rightsquigarrow c$.

The above two lemmata follow from the symmetry in a, b, definitions (1) and (2), (3, MP) and

$$a \rightsquigarrow (b \rightsquigarrow c) \sqsubseteq b \rightsquigarrow (a \rightsquigarrow c) \quad ,$$

which is proved by observing

$$\begin{array}{ll} & a \rightsquigarrow (b \rightsquigarrow c) \\ \sqsubseteq & \quad \{(3, D)\} \\ & (a \rightsquigarrow b) \rightsquigarrow (a \rightsquigarrow c) \\ \sqsubseteq & \quad \{\text{from } (3, W)\ b \sqsubseteq a \rightsquigarrow b\ ;\ (13, AM)\} \\ & b \rightsquigarrow (a \rightsquigarrow c) \end{array} \quad .$$

We now turn to the remainder of proof obligation (ii), viz. that "$\bullet$ preserves $\simeq$", or formally

$$a \simeq b \Rightarrow \bullet a \simeq \bullet b \quad .$$

This means that we have to use what has been given about $\bullet$, i.e. (0, C) or $\sqsubseteq$-equivalent and probably more convenient — (3, C). (It is probably unwise to found our further study of $\bullet$ on (4, C), as that is intrinsically weaker.) Our recent result (16, S) about shunting allows us to rewrite

(3,C) $\quad \bullet a \rightarrow b \sqsubseteq (\bullet a \rightarrow \bullet b) \rightarrow a$

as

(17,C) $\quad \bullet a \rightarrow \bullet b \sqsubseteq (a \rightarrow b) \rightarrow a$,

i.e. the fundamental property of $\bullet$ is symmetric in b and $\bullet b$. (Since we hope to show that $\bullet$ is its own inverse, this is very encouraging.)

We now observe for any a, b

true

$\equiv$ {(3,C)}

$\bullet a \rightarrow b \sqsubseteq (\bullet a \rightarrow \bullet b) \rightarrow a$

$\Rightarrow$ {from (3,W) $b \sqsubseteq \bullet a \rightarrow b$ and $\sqsubseteq$ transitive}

$b \sqsubseteq (\bullet a \rightarrow \bullet b) \rightarrow a$

$\equiv$ {(16,S)}

(18) $\quad \bullet a \rightarrow \bullet b \sqsubseteq b \rightarrow a$

Similarly one derives from (17,C)

(19) $\quad \bullet a \rightarrow b \sqsubseteq \bullet b \rightarrow a$.

Combining (19) with its instantiation $a, b := b, a$ yields (because of definition (2) of $\simeq$) the important

(20) $\quad \bullet a \rightarrow b \simeq \bullet b \rightarrow a$;

it is important because it expresses that (but for equivalence) $\bullet a \rightarrow b$ is a symmetric

expression in a, b .

Instantiating (19) with $b := \cdot a$ yields (via (3, MP), (1) and reflexivity of $\sqsubseteq$)

(21) $\quad \cdot\cdot a \sqsubseteq a$.

Furthermore we observe

$$
\begin{array}{ll}
 & \cdot\cdot a \rightsquigarrow b \\
\sqsubseteq & \quad \{ \text{(19) with } a := \cdot a \} \\
 & \cdot b \rightsquigarrow \cdot a \\
\sqsubseteq & \quad \{ \text{(18) with } a, b := b, a \} \\
 & a \rightsquigarrow b \qquad ;
\end{array}
$$

instantiating the above result with $b := \cdot\cdot a$ yields (again via (3, MP), (1) and reflexivity of $\sqsubseteq$)

$$a \sqsubseteq \cdot\cdot a \quad ,$$

and in combination with (21)

(22) $\quad \cdot\cdot a \simeq a \quad ,$

i.e. but for equivalence, $\cdot$ is its own inverse. We immediately use this result by observing for any a, b

$$
\begin{array}{ll}
 & a \rightsquigarrow b \\
\simeq & \quad \{ \text{(22) and (12)} \} \\
 & \cdot\cdot a \rightsquigarrow b \\
\sqsubseteq & \quad \{ \text{(19) with } a := \cdot a \} \\
 & \cdot b \rightsquigarrow \cdot a \qquad ,
\end{array}
$$

thus establishing

$$a \rightsquigarrow b \;\sqsubseteq\; \cdot b \rightsquigarrow \cdot a \quad .$$

from which we conclude via (3, MP)

(23) $\quad a \sqsubseteq b \;\Rightarrow\; \cdot b \sqsubseteq \cdot a \quad .$

Combining finally (23) with its instantiation $a,b := b,a$ yields (with predicate calculus and definition (2) of $\simeq$)

(24) $\quad a \simeq b \;\Rightarrow\; \cdot a \simeq \cdot b \quad ,$

i.e. "$\cdot$ preserves $\simeq$", as we had set out to prove.

* * *

We now turn to section (iii) of our proof obligations, which asks us to show the existence of 3 operators that preserve $\simeq$ and enjoy further properties. The preservation of $\simeq$ by our new operators is a direct consequence of the fact that the latter are defined in terms of $\rightsquigarrow$ and $\cdot$, which —see (ii)— preserve $\simeq$; with this remark we consider the preservation of $\simeq$ by the new operators dealt with.

(iii, supremum) For any a, b we define

(25) $\quad a \uparrow b \;=\; \cdot a \rightsquigarrow b$

and shall prove that $\uparrow$ thus defined has the

desired property; on our way we shall prove a few things more.

But for equivalence, $\uparrow$ is symmetric. To demonstrate this, we observe for any a, b

$$
\begin{array}{lll}
(26) & & a \uparrow b \simeq b \uparrow a \\
& \equiv & \quad \{ (25) \text{ twice} \} \\
& & \cdot a \rightsquigarrow b \simeq \cdot b \rightsquigarrow a \\
& \equiv & \quad \{ (20) \} \\
& & \text{true} \quad .
\end{array}
$$

Moreover, $\uparrow$ is but for equivalence associative. To demonstrate this we observe for any a, b, c

$$
\begin{array}{lll}
(27) & & a \uparrow (b \uparrow c) \simeq (a \uparrow b) \uparrow c \\
& \equiv & \quad \{ (26) \text{ twice} \} \\
& & a \uparrow (c \uparrow b) \simeq c \uparrow (a \uparrow b) \\
& \equiv & \quad \{ (25), \text{ four times} \} \\
& & \cdot a \rightsquigarrow (\cdot c \rightsquigarrow b) \simeq \cdot c \rightsquigarrow (\cdot a \rightsquigarrow b) \\
& \equiv & \quad \{ (15, 5) \} \\
& & \text{true}
\end{array}
$$

That $a \uparrow b$ is an upper bound is expressed by

$$
(28) \qquad a \sqsubseteq a \uparrow b \quad \wedge \quad b \sqsubseteq a \uparrow b \qquad ;
$$

it suffices to prove, say, the second conjunct, which we do by observing

$$
\begin{array}{ll}
 & b \\
\sqsubseteq & \quad \{ (3, W) \} \\
 & \bullet a \rightsquigarrow b \\
\simeq & \quad \{ (25) \} \\
 & a \uparrow b \qquad ,
\end{array}
$$

which we immediately use to equate

$$
\begin{array}{ll}
(29) & b \simeq a \uparrow b \equiv a \sqsubseteq b \\
 & \equiv \quad \{ (2) \text{ and } (28) \} \\
(30) & a \uparrow b \sqsubseteq b \equiv a \sqsubseteq b \qquad ,
\end{array}
$$

after which we prove the latter by mutual implication

Proof We observe for ping

$$
\begin{array}{ll}
 & a \uparrow b \sqsubseteq b \\
\equiv & \quad \{ (28) \} \\
 & a \sqsubseteq a \uparrow b \ \wedge \ a \uparrow b \sqsubseteq b \\
\Rightarrow & \quad \{ \text{transitivity } \sqsubseteq \} \\
 & a \sqsubseteq b \qquad .
\end{array}
$$

We observe for pong

$$
\begin{array}{ll}
 & a \uparrow b \sqsubseteq b \\
\equiv & \quad \{ (25), (26) \} \\
 & \bullet b \rightsquigarrow a \sqsubseteq b \\
\equiv & \quad \{ (22) \} \\
 & \bullet b \rightsquigarrow \cdot\cdot a \sqsubseteq b \\
\Leftarrow & \quad \{ (4C) \text{ with } a, b := b, \cdot a \} \\
 & \cdot b \sqsubseteq \cdot a \\
\Leftarrow & \quad \{ (23) \}
\end{array}
$$

$a \sqsubseteq b$.

(End of Proof.)

And now we are ready to meet our final proof obligation for (iii, supremum)

(31) $\quad a \uparrow b \sqsubseteq c \;\equiv\; a \sqsubseteq c \wedge b \sqsubseteq c$.

To this end we observe for any a, b, c

$$
\begin{array}{ll}
 & a \uparrow b \sqsubseteq c \\
\equiv & \quad \{ \text{(28) } b \sqsubseteq a \uparrow b \text{ and transitivity } \sqsubseteq \} \\
 & a \uparrow b \sqsubseteq c \;\wedge\; b \sqsubseteq c \\
\equiv & \quad \{ \text{(29) twice} \} \\
 & c \simeq a \uparrow b \uparrow c \;\wedge\; c \simeq b \uparrow c \\
\equiv & \quad \{ \text{Leibniz: } \uparrow \text{ and } \simeq \text{ preserve } \simeq \text{ !} \} \\
 & c \simeq a \uparrow c \;\wedge\; c \simeq b \uparrow c \\
\equiv & \quad \{ \text{(29) twice} \} \\
 & a \sqsubseteq c \;\wedge\; b \sqsubseteq c \quad .
\end{array}
$$

And this concludes our treatment of (iii, supremum).

(iii, infimum) After we define $\downarrow$ by

(32) $\quad a \downarrow b = \bullet(\bullet a \uparrow \bullet b)$

– in which the reader is welcome to recognize a Law of De Morgan –, our proof obligation

(33) $\quad a \sqsubseteq b \downarrow c \;\equiv\; a \sqsubseteq b \wedge a \sqsubseteq c$

is now a walk-over: we oberve for any a, b, c

$$
\begin{array}{ll}
 & a \sqsubseteq b \downarrow c \\
\equiv & \quad \{(32)\} \\
 & a \sqsubseteq \bullet(\bullet b \uparrow \bullet c) \\
\equiv & \quad \{(22)\ \&\ (23)\} \\
 & \bullet b \uparrow \bullet c \sqsubseteq \bullet a \\
\equiv & \quad \{(31)\} \\
 & \bullet b \sqsubseteq \bullet a \ \wedge\ \bullet c \sqsubseteq \bullet a \\
\equiv & \quad \{(22)\ \&\ (23)\} \\
 & a \sqsubseteq b \ \wedge\ a \sqsubseteq c \ .
\end{array}
$$

And this concludes our treatment of (iii, infimum).

(iii, shunting) We define our unary operator by stating that for all a

$$\sim a = \bullet a \quad , \tag{34}$$

which turns our last proof obligation into

$$a \downarrow b \sqsubseteq c \ \equiv\ b \sqsubseteq \bullet a \uparrow c \ . \tag{35}$$

Proof: We observe for any a, b, c

$$
\begin{array}{ll}
 & b \sqsubseteq \bullet a \uparrow c \\
\equiv & \quad \{(25)\ \&\ (26)\} \\
 & b \sqsubseteq \bullet c \rightsquigarrow \bullet a \\
\equiv & \quad \{(16, 5)\} \\
 & \bullet c \sqsubseteq b \rightsquigarrow \bullet a \\
\equiv & \quad \{(22)\} \\
 & \bullet c \sqsubseteq \bullet\bullet b \rightsquigarrow \bullet a \\
\equiv & \quad \{(25)\ \&\ (26)\}
\end{array}
$$

$$
\begin{array}{ll}
 & \bullet c \sqsubseteq \bullet a \uparrow \bullet b \\
\equiv & \quad \{(22)\ \&\ (23)\} \\
 & \bullet(\bullet a \uparrow \bullet b) \sqsubseteq c \\
\equiv & \quad \{(32)\} \\
 & a \downarrow b \sqsubseteq c
\end{array}
$$

(End of Proof?)

* * *

Coda Rutger is not responsible for this text which was written by me (i.e. Edsger) in his absence. He is mentioned as co-author because he conceived the theorem and helped me out when I got stuck in my proof effort. (That was in my effort to prove the Anti-Monotonicity.) He can explain better than I why he thought it worthwhile to design this theorem.

Nuenen, 22 July 1998

Rutger M. Dijkstra
Department of Computing Science
University of Groningen,
P.O. Box 800
9700 AV Groningen, The Netherlands
e-Mail rutger@cs.rug.nl

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