[3] P. Cousot and R. Cousot. Comparing the Galois Connection and Widening/Narrowing Approaches to Abstract Interpretation. Technical Report LIX/RR/92/09, École Polytechnique, 1992.

[4] A.C. Davis. A charcterization of complete lattices. *Pacific J. Mathematics*, 5:311–319, 1955.

[5] E.W. Dijkstra. On extreme solutions. EWD 1107, 1991.

[6] E.W. Dijkstra and C.S. Scholten. *Predicate calculus and program semantics.* Springer-Verlag, 1990.

[7] G. Grätzer. *General Lattice Theory.* Academic Press, 1978.

[8] J.A. Kalman. A two axiom definition for lattices. *Rev. Roumaine Math. Pures Appl.*, 13:669–670, 1968.

[9] J.J. Lukkien. An operational semantics for the guarded command language. In C.C. Morgan, editor, *Mathematics of Program Construction*, number 669 in Lecture Notes in Computer Science, page ? Springer-Verlag, 1993.

[10] R.N. McKenzie. Equational bases for lattice theories. *Math. Scand.*, 27:24–38, 1970.

[11] G. Nelson. A Generalization of Dijkstra's Calculus. *ACM Transactions on Programming Languages and Systems*, 11(4):517–561, 1989.

[12] A. Tarski. A lattice theoretical fixed point theorem and its applications. *Pacific J. Mathematics*, 5:285–309, 1955.

[13] J. von Wright. *A Lattice-theoretical Basis for Program Refinement.* PhD thesis, Åbo Akademi, 1990.

$$
\begin{array}{ll}
 & (b \to s)^*;\ (c \to t;\ (b \to s)^*)^*;\ [\neg b];\ [\neg c] \\
= & \qquad \{\ c\ =\ \neg b \wedge c\ \ \} \\
 & (b \to s)^*;\ (\neg b \wedge c \to t;\ (b \to s)^*)^*;\ [\neg b];\ [\neg c] \\
= & \\
 & (b \to s)^*;\ ([\neg b];\ \ c \to t;\ (b \to s)^*)^*;\ [\neg b];\ [\neg c] \\
= & \qquad \{\ \text{leapfrog; } [\neg b]\ \text{ is } \wedge\text{-distributive}\ \} \\
 & (b \to s)^*;\ [\neg b];\ (c \to t;\ (b \to s)^*;\ [\neg b])^*;\ [\neg c] \\
= & \\
 & \mathbf{do}\ b \to s\ \mathbf{od};\ (c \to t;\ \mathbf{do}\ b \to s\ \mathbf{od})^*;\ [\neg c] \\
= & \\
 & \mathbf{do}\ b \to s\ \mathbf{od};\ \mathbf{do}\ c \to t;\ \mathbf{do}\ b \to s\ \mathbf{od}\ \mathbf{od}
\end{array}
$$

19 Needs work

Invariance theorem(s).
Strongest postcondition.
Program inversion.

20 Appendix

Table of binding powers:

$$
\begin{array}{llll}
. & \circ & & \\
\uparrow & \downarrow & & \\
\leq & \geq & \subseteq & \supseteq \\
= & & & \\
\wedge & \vee & & \\
\Rightarrow & \Leftarrow & &
\end{array}
$$

References

[1] R.J.R. Back. *On the Correctness of Refinement Steps in Program Development.* PhD thesis, University of Helsinki, 1978. Report A-1978-4.

[2] G. Birkhoff. *Lattice Theory.* Colloquium Publications, Volume 25. American Mathematical Society, 1967.

Another interesting property of this loop is the so-called leapfrog rule. It holds for all B and for all finitely $\wedge$-distributive A.

$$A;\ (B;\ A)^* \ = \ (A;\ B)^*;\ A$$

$$\begin{array}{ll}
 & A;\ (B;\ A)^* \\
= & \\
 & A;\ \lfloor Y : Y \ = \ B;\ A;\ \ Y \ [\!]\ skip \rfloor \\
= & \\
 & A;\ \ \downarrow\{Y : Y \ = \ B;\ A;\ \ Y \ [\!]\ skip : Y\} \\
= & \qquad \{\ (46)\ \} \\
 & \downarrow\{Y : Y \ = \ B;\ A;\ \ Y \ [\!]\ skip : A;\ \ Y\} \\
= & \qquad \{\ \text{introduce } X\ \ \} \\
 & \downarrow\{X, Y : X \ = \ A;\ \ Y \quad \wedge \quad Y \ = \ B;\ X \ [\!]\ skip : X\} \\
= & \qquad \{\ \text{eliminate } Y\ \ \} \\
 & \downarrow\{X : X \ = \ A;\ (B;\ \ X \ [\!]\ skip) : X\} \\
= & \qquad \{\ \ A \text{ is finitely } \wedge\text{-distributive }\ \} \\
 & \downarrow\{X : X \ = \ A;\ B;\ \ X \ [\!]\ A : X\} \\
= & \qquad \{\ (172)\,[h.x.y := A; B; y [\!] x,\ \ g := A]\ \ \} \\
 & \downarrow\{X : X \ = \ A;\ B;\ \ X \ [\!]\ skip : X\};\ A \\
= & \\
 & (A;\ B)^*;\ A
\end{array}$$

From these two, we derive Greg Nelson's theorem that

$$\textbf{do } b \rightarrow s [\!] c \rightarrow t \textbf{ od} \ = \ \textbf{do } b \rightarrow s \textbf{ od};\ \textbf{do } c \rightarrow t;\ \textbf{do } b \rightarrow s \textbf{ od od}$$

provided $c \ \Rightarrow \ \neg b$.

$$\begin{array}{ll}
 & \textbf{do } b \rightarrow s [\!] c \rightarrow t \textbf{ od} \\
= & \\
 & (b \rightarrow s [\!] c \rightarrow t)^*;\ [\neg(b \vee c)] \\
= & \\
 & (b \rightarrow s [\!] c \rightarrow t)^*;\ [\neg b];\ [\neg c] \\
= &
\end{array}$$

$$(DO;\ DO').Q$$
$$=$$
$$DO.(DO'.Q)$$
$$= \qquad \{\ (234)\ \}$$
$$DO.(DO'.Q \wedge \neg b)$$
$$= \qquad \{\ (235)\ \}$$
$$DO.(\,Q \wedge \neg b)$$
$$= \qquad \{\ (234)\ \}$$
$$DO.Q$$

As a result, we have

$$DO;\ DO \ = \ DO$$

Also, we have

$$DO \ = \ \mathbf{do}\ b \rightarrow DO\ \mathbf{od}$$

A slightly simpler looping construct is sometimes written as

$$S^* \ = \ \lfloor Y : Y \ = \ S;\ \ Y \ \| \ skip \rfloor$$

and from

$$(b \rightarrow s)^*;\ [\neg b]$$
$$=$$
$$\lfloor Y : Y \ = \ b \rightarrow s;\ \ Y \ \| \ skip \rfloor;\ [\neg b]$$
$$= \qquad \{\ (172)\,[h.x.y := b \rightarrow s;\, y \| x,\ \ g := [\neg b]] \quad \}$$
$$\lfloor Y : Y \ = \ b \rightarrow s;\ \ Y \ \| \ [\neg b] \rfloor$$
$$=$$
$$\mathbf{do}\ b \rightarrow s\ \mathbf{od}$$

we have

$$\mathbf{do}\ b \rightarrow s\ \mathbf{od} \ = \ (b \rightarrow s)^*;\ [\neg b]$$

Observe that S^* is identical to the lowest $\uparrow$-closure $S \ {\uparrow\!\!\!\!\ast}$ of S. Hence, we have from (151),

$$(A \| B)^* \ = \ A^*;\ (B;\ A^*)^*$$

$$\begin{array}{ll} & \mathbf{if}\ [\!](i :: b_i \to S_i)\ \mathbf{fi};\ \ T \\ = & \\ & \{\exists(i :: b_i)\};\ [\!](i :: b_i \to S_i);\ \ T \\ = & \\ & \{\exists(i :: b_i)\};\ [\!](i :: (b_i \to S_i);\ \ T) \\ = & \\ & \{\exists(i :: b_i)\};\ [\!](i :: b_i \to S_i;\ \ T) \\ = & \\ & \mathbf{if}\ [\!](i :: b_i \to S_i)\ \mathbf{fi};\ \ T \end{array}$$

we have

$$\mathbf{if}\ [\!](i :: b_i \to S_i)\ \mathbf{fi};\ \ T \ = \ \mathbf{if}\ [\!](i :: b_i \to S_i;\ \ T)\ \mathbf{fi} \tag{233}$$

In general, we do not have

$$T;\ \mathbf{if}\ [\!](i :: b_i \to S_i)\ \mathbf{fi} \ = \ \mathbf{if}\ [\!](i :: b_i \to T;\ S_i)\ \mathbf{fi} \qquad ,$$

not even when T is $\wedge$-distributivity.

Let $DO \ = \mathbf{do}\ b \to S\ \mathbf{od}$ and $DO' \ = \mathbf{do}\ b' \to S'\ \mathbf{od}$. From (212) we conclude

$$DO.Q \ = \ DO.(Q \wedge \neg b) \tag{234}$$

and

$$(Q \ \Rightarrow \ \neg b) \ \Rightarrow \ (Q \ \Rightarrow \ (DO = skip)) \tag{235}$$

Given $(Q \Rightarrow \neg b)$ and Q, we have

$$\begin{array}{ll} & D.X \\ = & \qquad \{\ DO \text{ solves (212) } \} \\ & (b \ \wedge \ S.X) \ \vee \ (\neg b \ \wedge \ X) \\ = & \qquad \{\ \text{from } (Q \Rightarrow \neg b) \text{ and } Q, \text{ we have } \neg b \ \} \\ & X \end{array}$$

If $b' \Rightarrow b$ then

$$DO;\ DO' \ = \ DO$$

and hence we propose

$$\textbf{do } b \to s \textbf{ od} \;=\; \lfloor Y : Y \;=\; \textbf{if } b \to s;\;\; Y \,[\!]\, \neg b \to \mathit{skip} \textbf{ fi} \rfloor$$

which is equivalent to

$$\textbf{do } b \to s \textbf{ od} \;=\; \lfloor Y : Y \;=\; [b];\;\; s;\;\; Y \,[\!]\, [\neg b] \rfloor$$

and to

$$\textbf{do } b \to s \textbf{ od} \;=\; \lfloor Y : Y \;=\; \{b\};\;\; s;\;\; Y \quad \vee \quad \{\neg b\} \rfloor$$

Similar to the rejected attempt at defining $\textbf{if } S \textbf{ fi}$ one might try to introduce $\textbf{do } S \textbf{ od}$. In fact, this is done in [11] as follows.

$$\textbf{do } S \textbf{ od} \;=\; \lfloor Y : Y \;=\; S;\;\; Y \,[\!]\, [S.\mathit{false}] \rfloor$$

We refrain from doing so because this construct is not monotonic in S as shown by the following example. We have $\textbf{do } x \neq 0 \to x := 0 \textbf{ od} \;=\; x := 0$ and $\textbf{do } \mathit{magic} \textbf{ od} \;=\; \mathit{skip}$, and $x \neq 0 \to x := 0 \;\leq\; \mathit{magic}$ but not $x := 0 \;\leq\; \mathit{skip}$. We stick to our earlier definition of the loop $\textbf{do } b \to s \textbf{ od}$. According to (130), it is a monotonic function of s.

We now investigate some distribution properties of programs. From (71) we get

$$[\!]\{i :: S_i\};\;\; T \;=\; [\!]\{i :: S_i;\;\; T\} \tag{231}$$

but for

$$T;\;\; [\!]\{i :: S_i\} \;=\; [\!]\{i :: T;\;\; S_i\} \tag{232}$$

we need $\wedge$-distributivity of T. If T is universally $\wedge$-distributive, we have (232). If T is positively $\wedge$-distributive, we have (232) for nonempty set $\{i :: S_i\}$. If T is finitely $\wedge$-distributive, we have (232) for nonempty, finite set $\{i :: S_i\}$. We give the proof of the latter.

$$\begin{array}{ll}
 & (T;\, (U \,[\!]\, V)).Q \\
= & \qquad \{ \text{ definition of } [\!] \text{ and } ; \;\; \} \\
 & T.(U.Q \quad \wedge \quad V.Q) \\
= & \qquad \{ \;\; T \text{ is finitely } \wedge\text{-distributive } \} \\
 & T.(U.Q) \quad \wedge \quad T.(V.Q) \\
= & \qquad \{ \text{ definition of } [\!] \text{ and } ; \;\; \} \\
 & (T;\, U \,[\!]\, T;\, V).Q
\end{array}$$

From

Sequences of guard and assert statements can be combined.

$$\{P\};\ \{Q\} \ = \ \{P \wedge Q\} \tag{227}$$

$$[P];\ [Q] \ = \ [P \wedge Q] \tag{228}$$

We can now define the guarded command $P \rightarrow S$ as an abbreviation for $[P];\ S$. Since sequential composition is monotonic, $P \rightarrow S$ is monotonic with respect to S. The binding power of $\rightarrow$ is lower than that of ; and higher than that of $[\!]$. We have

$$[P];\ Q \rightarrow S \ = \ P \wedge Q \rightarrow S \tag{229}$$

and from the associativity of ; we have

$$(b \rightarrow S);\ T \ = \ b \rightarrow S;\ T \tag{230}$$

The if-command can be defined as

$$\textbf{if } [\!](i :: b_i \rightarrow S_i) \textbf{ fi} \ = \ \{\exists(i :: b_i)\};\ [\!](i :: b_i \rightarrow S_i) \qquad .$$

Since $[\!]$ and $\rightarrow$ are monotonic, the if-command is monotonic with respect to any of the commands S_i.

The shape of the formula suggests that we might define the if-command for any (partial) command S as

$$\textbf{if } S \textbf{ fi} \ = \ \{\neg S.\mathit{false}\};\ S$$

but we refrain from doing so because this construct is not monotonic with respect to S. For example, we have $\mathit{skip} \leq \mathit{magic}$ but not $\mathit{skip} \leq \mathit{abort}$, and yet $\textbf{if } \mathit{skip} \textbf{ fi} = \mathit{skip}$ and $\textbf{if } \mathit{magic} \textbf{ fi} = \mathit{abort}$.

We can rewrite the if-command as

$$\textbf{if } [\!](i :: b_i \rightarrow S_i) \textbf{ fi} \ = \ \{\exists(i :: b_i)\};\ [\!](i :: [b_i];\ S_i)$$

which suggest that we might also have another if-command, such as

$$\textbf{if } \diamond(i :: b_i \rightarrow S_i) \textbf{ fi} \ = \ [\exists(i :: b_i)];\ \ \vee(i :: \{b_i\};\ S_i)$$

or maybe

$$\textbf{if } \diamond(i :: b_i \rightarrow S_i) \textbf{ fi} \ = \ \vee(i :: \{b_i\};\ S_i)$$

The latter corresponds to angelic choice whereas the original one corresponds to demonic choice. When the b_i are mutually exclusive, the two commands coincide.

According to (214), DO is the lowest solution of

$$Y :\ Y = (b \ \wedge \ wp.s.Y) \ \vee \ (\neg b \ \wedge \ Q)$$

$$
\begin{array}{ll}
= & \\
& \forall(Q :: S.Q \Rightarrow T.Q) \\
= & \quad \{\ (7)\ \} \\
& \forall(P,Q :: (P \Rightarrow S.Q) \ \Rightarrow \ (P \Rightarrow T.Q)) \\
= & \quad \{\ \text{use Hoare triple } \{P\}S\{Q\} \text{ for } P \Rightarrow S.Q \ \ \} \\
& \forall(P,Q :: \{P\}S\{Q\} \ \Rightarrow \ \{P\}T\{Q\})
\end{array}
$$

The last line can be read as: T satisfies every specification that S satisfies, and hence, $S \leq T$ expresses that S can be refined by T. From (16) and (17) we conclude

$$S \leq S' \ \wedge \ T \leq T' \ \Rightarrow \ S;\, T \leq S';\, T'$$

which shows that a sequential composition of commands can be refined by refining its components. Given that we have a partial order $\leq$ on programs, we can derive the $\uparrow$ and $\downarrow$ on programs. They are usually written as $\vee$ and $[\!]$.

$$
\begin{array}{lll}
(S \vee T).Q & = & S.Q \quad \vee \quad T.Q \\
(S [\!] T).Q & = & S.Q \quad \wedge \quad T.Q
\end{array}
$$

If S and T are monotonic, then so are $S \vee T$ and $S [\!] T$. If S and T are positively $\wedge$-distributive, then so is $S [\!] T$ on account of (73), but $S \vee T$ need not be positively $\wedge$-distributive. Command *abort* is the unit element of $\vee$ and the zero element of $[\!]$, whereas *magic* is the unit element of $[\!]$ and the zero element of $\vee$. On account of (63), both $\vee$ and $[\!]$ are monotonic in S and T. They have a lower binding power than ; has. Of course, we have

$$(S \leq T) \ = \ (S [\!] T = S) \ = \ (S \vee T = T) \qquad .$$

We have seen the usefulness of $b?$ in the section on operational semantics. We introduce a similar construct in our program notation, and then add another one. They are called the assert and guard command respectively.

$$
\begin{array}{lll}
\{P\}.Q & = & P \quad \wedge \quad Q \\
[P].Q & = & P \Rightarrow Q
\end{array}
$$

Both are positively $\wedge$-distributive, and hence, also monotonic functions of Q. Both $\{P\}$ and $[P]$ act as *skip* if P holds. If P does not hold, then $\{P\}$ acts as *abort* whereas $[P]$ acts as *magic*. Notice

$$
\begin{array}{lll}
\{\mathit{false}\} & = & \mathit{abort} \\
[\mathit{false}] & = & \mathit{magic} \\
\{\mathit{true}\} & = & [\mathit{true}] \ = \ \mathit{skip}
\end{array}
$$

but, as its name suggests, its implementation may not be obvious. In fact, *magic* violates the Law of the Excluded Miracle, which implies that no operational semantics in the sense of the previous section exists for *magic*. A command that violates the Law of the Excluded Miracle is called a partial command. In our discussion of an axiomatic semantics, we do not assume that commands satisfy the Law of the Excluded Miracle, in fact we do not even assume that they are positively $\wedge$-distributive. Our only restriction is that every command be monotonic. In the sequel, a command can be any monotonic predicate transformer, and not only one for which we have given the syntactic representation as a program text. From (65) we know that these commands form a complete lattice, with bottom *abort* and top *magic*. Whenever we introduce a construct that composes commands, we have the proof obligation to show that the composite is monotonic given that the components are. For example,

$$S;\, T \;=\; S \circ T$$

and the monotonicity of $S;\, T$ follows from (13).

The positively $\wedge$-distributive predicate transformers do not form a complete lattice. However, from(73) we know that the highest lower bound of any set of positively $\wedge$-distributive predicate transformers is a positively $\wedge$-distributive itself. Most of our programs are positively $\wedge$-distributive, and some of them even universally $\wedge$-distributive, as noted when they are introduced. Both *skip* and *magic* are universally $\wedge$-distributive; *abort* is not universally but positively $\wedge$-distributive. From (102) we infer that $S;\; T$ has every distributivity property shared by S and T.

As a property of ; we have

$$\mathit{skip};\; S \;=\; S \;=\; S;\; \mathit{skip} \tag{221}$$

since id is the left and right identity element of function composition. Also, because function composition is associative, we have

$$;\ \text{is associative} \tag{222}$$

Combinations of ; with *abort* and *miracle* give

$$\mathit{miracle};\; S \;=\; \mathit{miracle} \tag{223}$$

$$(S;\; \mathit{miracle} \;=\; \mathit{miracle}) \;=\; (S.\mathit{true} \;=\; \mathit{true}) \tag{224}$$

$$\mathit{abort};\; S \;=\; \mathit{abort} \tag{225}$$

$$(S;\, \mathit{abort} \;=\; \mathit{abort}) \;=\; (S.\mathit{false} \;=\; \mathit{false}) \tag{226}$$

Before we proceed with the if- and do-commands, we see how the lifting of the ordering on predicates to predicate transformers can be interpreted.

$$S \leq T$$

$$
\begin{array}{ll}
 & true \\
= & \quad \{ \ (211) \ \} \\
 & wlp.DO.\neg X \ = \ \lceil Y : Y = (b \ \wedge \ wlp.s.Y) \ \vee \ (\neg b \ \wedge \ \neg X) \rceil \\
= & \quad \{ \ (91)\text{: De Morgan } \} \\
 & \neg wlp.DO.\neg X \ = \ \lfloor Y : \neg Y = (b \ \wedge \ wlp.s.\neg Y) \ \vee \ (\neg b \ \wedge \ \neg X) \rfloor \\
= & \quad \{ \ (91)\text{: De Morgan } \} \\
 & \neg wlp.DO.\neg X \ = \ \lfloor Y : Y = (\neg b \ \vee \ \neg wlp.s.\neg Y) \ \wedge \ (b \ \vee \ X) \rfloor \\
= & \quad \{ \ s \text{ is deterministic } \} \\
 & \neg wlp.DO.\neg X \ = \ \lfloor Y : Y = (\neg b \ \vee \ wp.s.Y) \ \wedge \ (b \ \vee \ X) \rfloor \\
= & \quad \{ \ (212) \ \} \\
 & \neg wlp.DO.\neg X \ = \ wp.DO.X \\
= & \\
 & DO \text{ is deterministic}
\end{array}
$$

□

18 Axiomatic semantics

In the preceding sections, we have identified a program with its set of traces, and we have derived its *wp* and *wlp* from this operational semantics. We might have followed an alternative path in which we state the *wp* and *wlp* of every program and never mention the operational semantics. This is referred to as axiomatic semantics. If one postulates, for example, each *wlp* then (198) can be proved by induction: first it is shown for the basic commands (*skip*, *abort*, and assignment) and then inductively for sequential, alternative, and repetitive compositions.

In the present section we forget about the operational semantics. Because a program's *wp* is of more practical importance than its *wlp*, we focus on the former. To emphasize this focus, we identify a program with its *wp*, so that we have $(v := e).Q = Q^v_e$ and $skip.Q = Q$, or, if we want to write it without Q,

$$
\begin{array}{ll}
skip & = \ id \\
abort & = \ false
\end{array}
$$

The definition of *abort* shows that it is the lifting of the constant predicate *false* (or $\perp$) to the level of predicate transformers. It suggests that we also introduce

$$
magic \quad = \ true
$$

$=$

$\exists(j :: false)$

$=$

$false$

However, we have the following result.

Theorem

If all $wlp.s_i$ are positively $\vee$-continuous and the range of i is finite,

$$wlp.\mathbf{if}\ [\!](i :: b_i \rightarrow s_i)\ \mathbf{fi} \text{ is positively } \vee-\text{continuous.} \qquad (218)$$

Proof

We have $wlp.\mathbf{if}\ [\!](i :: b_i \rightarrow s_i)\ \mathbf{fi}.Q \;=\; \forall(i :: \neg b_i \;\vee\; wlp.s_i.Q)$. Since every constant function is positively $\vee$-continuous, and because of (103), we have that $\neg b_i \;\vee\; wlp.s_i$ is positively $\vee$-continuous. Because of (139) and because the range of i is finite, we have that $\forall(i :: \neg b_i \;\vee\; wlp.s_i)$ and hence also that $wlp.\mathbf{if}\ [\!](i :: b_i \rightarrow s_i)\ \mathbf{fi}$ is positively $\vee$-continuous.

□

Theorem

$$\text{If } wlp.S \text{ is positively } \vee-\text{continuous, then so is } wp.S\ . \qquad (219)$$

Proof

Immediate from (199) and (105).

□

Weakest preconditions were originally studied in the context of programs whose nondeterminism is bounded. As a result, their wp is positively $\vee$-continuous and hence, according to (152), (212), and (214)

$$wp.\mathbf{do}\ b \rightarrow s\ \mathbf{od}.Q \;=\; \exists(i : i \geq 0 : f^i.false)$$

where

$$f.X \;=\; (\neg b \;\vee\; wp.s.X) \;\wedge\; (b \;\vee\; Q)$$

and this is then used as the definition of $wp.DO$. (Notice that f depends on b, s, and Q.) We prefer characterization (214). Programs whose nondeterminism is unbounded may not be easy to implement, but they are often interesting stepping stones in the development of programs from their specifications.

Theorem

$$\text{If } s \text{ is deterministic, then so is } \mathbf{do}\ b \rightarrow s\ \mathbf{od}\ . \qquad (220)$$

Proof

$$
\begin{array}{ll}
= & \quad \{ \text{ predicate calculus } \} \\
 & \neg wlp.S.\forall(Q : Q \in V : \neg Q) \\
= & \quad \{ \text{ (198) } \} \\
 & \neg\forall(Q : Q \in V : wlp.S.\neg Q) \\
= & \quad \{ \text{ (215) } \} \\
 & \neg\forall(Q : Q \in V : \neg wp.S.Q) \\
= & \quad \{ \text{ predicate calculus } \} \\
 & \exists(Q : Q \in V : wp.S.Q)
\end{array}
$$

□

It is easily checked that *skip*, *abort*, and $v := e$ are deterministic. Also, sequential composition of deterministic commands is deterministic. However, the if-command need not be deterministic. The nondeterminsim may even be unbounded, as shown by program UN, which assigns an arbitrary natural value to variable v.

$$UN \;=\; \mathbf{if}\ [\!](i : i \geq 0 : true \rightarrow v := i)\ \mathbf{fi}$$

We have

$$wp.UN.Q \;=\; wlp.UN.Q \;=\; \forall(i : i \geq 0 : Q^v_i)$$

and we show that $wlp.UN$ is not even $\vee$-continuous. In particular, we show that $wlp.UN$ does not $\vee$-distribute over set $\{j :: j \geq v\}$ which is a chain. We have

$$
\begin{array}{ll}
 & wlp.UN.\exists(j :: j \geq v) \\
= & \quad \{ \text{ take } j := v \ \} \\
 & wlp.UN.true \\
= & \\
 & true
\end{array}
$$

and

$$
\begin{array}{ll}
 & \exists(j :: wlp.UN.(j \geq v)) \\
= & \\
 & \exists(j :: \forall(i :: (j \geq v)^v_i)) \\
= & \quad \{ \text{ substitution } \} \\
 & \exists(j :: \forall(i :: j \geq i))
\end{array}
$$

$$
\begin{array}{ll}
\Rightarrow & \{\ \text{induction hypothesis}\ \} \\
& \forall(y,u :: t \in \{x\};\, b?;\, s;\, \{y\};\, u \ \ \wedge \ \ Y.y \ \ \wedge \ \ |t| < \infty) \\
\Rightarrow & \{\ \text{definition } wp\ \} \\
& b.x \ \ \wedge \ \ wp.s.Y.x \\
\Rightarrow & \{\ Y \text{ solves (212)}\ \} \\
& Y.x
\end{array}
$$

□

17 Nondeterminism

We say that a program is deterministic if every possible outcome of the program is unavoidable. With wp and wlp we express properties about the final state only, so "outcomes" are final states.

$$\text{Program } S \text{ is deterministic } = \forall(Q :: wp.S.\neg Q = \neg wlp.S.Q) \tag{215}$$

A rewrite of this expression reveals

$$
\begin{array}{ll}
& wp.S.\neg Q.x = \neg wlp.S.Q.x \\
= & \{\ \text{(197) and (196): definition of } wp \text{ and } wlp\ \} \\
& \forall(t : t \in \{x\};\, S : |t| < \infty \ \ \wedge \ \ \neg Q.(last.t)) \ = \ \neg\forall(t : t \in \{x\};\, S : |t| = \infty \ \ \vee \ \ Q.(last.t)) \\
= & \{\ \text{predicate calculus}\ \} \\
& \forall(t : t \in \{x\};\, S : |t| < \infty \ \ \wedge \ \ \neg Q.(last.t)) \ = \ \exists(t : t \in \{x\};\, S : |t| < \infty \ \ \wedge \ \ \neg Q.(last.t))
\end{array}
$$

and the latter line corresponds to our informal definition.

Theorem

If S is deterministic

$$wp.S \text{ is universally } \vee\text{-distributive} \tag{216}$$

$$wlp.S \text{ is positively } \vee\text{-distributive} \tag{217}$$

Proof

$$
\begin{array}{ll}
& wp.S.\exists(Q : Q \in V : Q) \\
= & \{\ (215)\ \} \\
& \neg wlp.S.\neg\exists(Q : Q \in V : Q)
\end{array}
$$

$\Rightarrow$

$Q.(last.t)$

□

Theorem

$wp.DO.Q$ is the lowest solution of (212). (214)

Proof

We need to show $wp.DO.Q \;\Rightarrow\; Y$ for any solution Y of (212), that is,

$$t \in \{x\};\, DO \;\;\wedge\;\; |t| < \infty \;\;\wedge\;\; Q.(last.t) \;\Rightarrow Y.x$$

for every trace t and state x. We have

$$\begin{array}{ll}
 & t \in \{x\};\, DO \quad \wedge \quad |t| < \infty \\
= & \qquad \{ \text{ definition of } DO \; \} \\
 & t \in \{x\};\, (b?;\, s)^{\omega};\, \neg b? \quad \wedge \quad |t| < \infty \\
= & \qquad \{ \text{ definition of } s^{\omega} \; \} \\
 & t \in \{x\};\, (loop.(b?;\, s) \cup \cup(n : n \geq 0 : (b?;\, s)^{n});\, \neg b? \quad \wedge \quad |t| < \infty \\
= & \qquad \{ \text{ all loop traces are infinite } \} \\
 & t \in \{x\};\; \cup\,(n : n \geq 0 : (b?;\, s)^{n});\, \neg b? \quad \wedge \quad |t| < \infty
\end{array}$$

and we prove by induction on n that the conjunction of $Q.(last.t)$ and the last line implies $Y.x$.

$n = 0$:

$$\begin{array}{ll}
 & t \in \{x\};\, \neg b?;\, skip \quad \wedge \quad |t| < \infty \quad \wedge \quad Q.(last.t) \\
= & \\
 & t = xx \quad \wedge \quad \neg b.x \quad \wedge \quad Q.x \\
\Rightarrow & \qquad \{ \;\; Y \text{ solves (212) } \} \\
 & Y.x
\end{array}$$

$n \geq 0$:

$$\begin{array}{ll}
 & t \in \{x\};\, (b?;\, s)^{n+1};\, \neg b? \quad \wedge \quad |t| < \infty \quad \wedge \quad Q.(last.t) \\
= & \\
 & \forall(y, u :: t \in \{x\};\, b?;\, s;\, \{y\};\, u \quad \wedge \quad u \in \{y\};\, (b?;\, s)^{n};\, \neg b? \quad \wedge \quad Q.(last.t) \quad \wedge \quad |t| < \infty)
\end{array}$$

$$t \in \{x\};\ (b?;\ s)^0$$
$=$
$$t = x$$
$\Rightarrow$ $\{\ Y.x\ \}$
$$Y.(last.t)$$

$n \geq 0:$

$$t \in \{x\};\ (b?;\ s)^{n+1}$$
$\Rightarrow$
$$\exists(u, v :: |u| < \infty \quad \wedge \quad u \in \{x\};\ (b?;\ s)^n \quad \wedge \quad v \in \{last.u\};\ b?;\ s \quad \wedge \quad t = u;\ v)$$
$\Rightarrow$ $\{$ induction hypothesis $\}$
$$\exists(u, v :: Y.(last.u) \quad \wedge \quad v \in \{last.u\};\ b?;\ s \quad \wedge \quad t = u;\ v)$$
$\Rightarrow$ $\{\ Y$ solves (211); $v \in \{last.u\};\ b?;\ s \ \Rightarrow\ b.(last.u)\ \}$
$$\exists(u, v :: wlp.s.Y.(last.u) \quad \wedge \quad v \in \{last.u\};\ b?;\ s \quad \wedge \quad t = u;\ v)$$
$\Rightarrow$ $\{\ last.u = v.0\ \}$
$$\exists(v :: wlp.s.Y.(v.0) \quad \wedge \quad v \in \{v.0\};\ s \quad \wedge \quad last.t = last.v)$$
$\Rightarrow$ $\{\ |v| < \infty\ \}$
$$\exists(v :: Y.(last.v) \quad \wedge \quad last.t = last.v)$$
$\Rightarrow$
$$Y.(last.t)$$

Next we prove the theorem.

$$Y.x \quad \wedge \quad |t| < \infty \quad \wedge \quad t \in \{x\};\ DO$$
$\Rightarrow$ $\{$ definition $DO\ \}$
$$\exists(n :: t \in \{x\};\ (b?;\ s)^n;\ \neg b?)$$
$=$
$$\exists(n, u, y :: t = uyy \quad \wedge \quad uy \in \{x\};\ (b?;\ s)^n \quad \wedge \quad \neg b.y)$$
$\Rightarrow$ $\{$ see result above $\}$
$$\exists(u, y :: t = uyy \quad \wedge \quad Y.y \quad \wedge \quad \neg b.y)$$
$\Rightarrow$ $\{\ Y$ solves (211) $\}$
$$\exists(u, y :: t = uyy \quad \wedge \quad Q.y)$$

$$
\begin{array}{ll}
 & wlp.DO.Q \\
= & \quad \{\ (189)\ \} \\
 & wlp.\mathbf{if}\ b \rightarrow s;\ DO [\!] \neg b \rightarrow skip\ \mathbf{fi}.Q \\
= & \quad \{\ \text{see result for}\ IF\ \} \\
 & (b \Rightarrow wlp.(s;\ DO).Q) \quad \wedge \quad (\neg b \Rightarrow wlp.skip.Q) \\
= & \quad \{\ (94)\ \} \\
 & (b \quad \wedge \quad wlp.(s;\ DO).Q) \quad \vee \quad (\neg b \quad \wedge \quad wlp.skip.Q) \\
= & \quad \{\ \text{see results for ; and}\ skip\ \} \\
 & (b \quad \wedge \quad wlp.s.(wlp.DO.Q)) \quad \vee \quad (\neg b \quad \wedge \quad Q)
\end{array}
$$

and hence $wlp.DO.Q$ is a solution of equation (Y is a predicate)

$$Y:\ Y = (b \quad \wedge \quad wlp.s.Y) \quad \vee \quad (\neg b \quad \wedge \quad Q) \tag{211}$$

$wp.DO.Q$ is a solution of

$$Y:\ Y = (b \quad \wedge \quad wp.s.Y) \quad \vee \quad (\neg b \quad \wedge \quad Q) \tag{212}$$

Theorem

$wlp.DO.Q$ is the highest solution of (211). (213)

Proof

Let Y be any solution of (211). We have to show $Y \Rightarrow wlp.DO.Q$, that is,

$$
\begin{array}{ll}
 & Y \Rightarrow wlp.DO.Q \\
= & \\
 & \forall(x :: Y.x \Rightarrow wlp.DO.Q.x) \\
= & \\
 & \forall(x :: Y.x \Rightarrow \forall(t : t \in \{x\};\ DO : |t| = \infty \quad \vee \quad Q.(last.t))) \\
= & \\
 & \forall(x, t : Y.x \quad \wedge \quad t \in \{x\};\ DO \quad \wedge \quad |t| < \infty : Q.(last.t))
\end{array}
$$

First, we prove by induction,

$$t \in \{x\};\ (b?;\ s)^n \quad \Rightarrow \quad Y.(last.t)$$

while assuming $Y.x \quad \wedge \quad |t| < \infty$.

$n = 0$:

$$
\begin{array}{ll}
 & \forall(t : t \in \{x\};\, S;\, U : |t| = \infty \;\;\vee\;\; Q.(last.t)) \\
= & \quad \{ \text{ change dummy } \; t := s;\, u \;\; \} \\
 & \forall(s, u : s \in \{x\};\, S \wedge u \in \{last.s\};\, U : |s;\, u| = \infty \;\;\vee\;\; Q.(last.(s;\, u))) \\
= & \\
 & \forall(s : s \in \{x\};\, S : |s| = \infty \;\;\vee\;\; \forall(u : u \in \{last.s\};\, U : |u| = \infty \;\;\vee\;\; Q.(last.u))) \\
= & \\
 & \forall(s : s \in \{x\};\, S : |s| = \infty \;\;\vee\;\; wlp.U.Q.(last.s)) \\
= & \quad \{ \text{ (196): definition of } \; wlp \;\; \} \\
 & wlp.S.(wlp.U.Q).x
\end{array}
$$

and hence

$$wlp.(S;\, U) \;=\; (wlp.S) \circ (wlp.U) \tag{207}$$

$$wp.(S;\, U) \;=\; (wp.S) \circ (wp.U) \tag{208}$$

$$
\begin{array}{ll}
 & wlp.\mathbf{if}\; [\![(i :: b_i \rightarrow s_i)\; \mathbf{fi}.Q.x \\
= & \quad \{ \text{ definitions of } \; IF \; \text{ and } \; wlp \;\; \} \\
 & \forall(t : t \in \{x\};\, (\cup(i :: b_i?;\, s_i) \cup \forall(i :: \neg b_i)?;\, abort) : |t| = \infty \;\;\vee\;\; Q.(last.t)) \\
= & \quad \{ \text{ all traces in } \; abort \; \text{ are infinite } \} \\
 & \forall(t : t \in \{x\};\, \cup\,(i :: b_i?;\, s_i) : |t| = \infty \;\;\vee\;\; Q.(last.t)) \\
= & \quad \{ \text{ (179) } \} \\
 & \forall(t : t \in \cup(i :: \{x\};\, b_i?;\, s_i) : |t| = \infty \;\;\vee\;\; Q.(last.t)) \\
= & \\
 & \forall(t : t \in \cup(i : b_i.x : \{x\};\, s_i) : |t| = \infty \;\;\vee\;\; Q.(last.t)) \\
= & \\
 & \forall(i : b_i.x : \forall(t : t \in \{x\};\, s_i : |t| = \infty \;\;\vee\;\; Q.(last.t))) \\
= & \quad \{ \text{ (196): definition of } \; wlp \;\; \} \\
 & \forall(i : b_i.x : wlp.s_i.Q.x)
\end{array}
$$

and hence

$$wlp.\mathbf{if}\; [\![(i :: b_i \rightarrow s_i)\; \mathbf{fi}.Q \;=\; \forall(i : b_i : wlp.s_i.Q) \tag{209}$$

$$wp.\mathbf{if}\; [\![(i :: b_i \rightarrow s_i)\; \mathbf{fi}.Q \;=\; \exists(i :: b_i) \;\wedge\; \forall(i : b_i : wp.s_i.Q) \tag{210}$$

$$wp.skip.Q \ = \ Q \tag{202}$$

The next command is *abort*.

$$\begin{array}{ll} & wlp.abort.Q.x \\ = & \qquad \{ \ (196)\text{: definition of } wlp \ \} \\ & \forall(t : t \in \{x\}; abort : |t| = \infty \quad \vee \quad Q.(last.t)) \\ = & \qquad \{ \ \text{definition of ; and } abort \ \} \\ & \forall(t : t \in \{x^\infty\} : |t| = \infty \quad \vee \quad Q.(last.t)) \\ = & \\ & true \end{array}$$

and hence

$$wlp.abort.Q \ = \ true \tag{203}$$

$$wp.abort.Q \ = \ false \tag{204}$$

The third command is the assignment $v := e$.

$$\begin{array}{ll} & wlp.(v := e).Q.x \\ = & \qquad \{ \ (196)\text{: definition of } wlp \ \} \\ & \forall(t : t \in \{x\}; v := e : |t| = \infty \quad \vee \quad Q.(last.t)) \\ = & \qquad \{ \ \text{definition of ; and } v := e \ \} \\ & \forall(t : t \in \{x \ x(v := e.x)\} : |t| = \infty \quad \vee \quad Q.(last.t)) \\ = & \\ & Q.(x(v := e.x)) \end{array}$$

and hence

$$wlp.(v := e).Q \ = \ Q^v_e \tag{205}$$

$$wp.(v := e).Q \ = \ Q^v_e \tag{206}$$

Next we look at the command constructors.

$$\begin{array}{ll} & wlp.(S;\ U).Q.x \\ = & \qquad \{ \ (196)\text{: definition of } wlp \ \} \end{array}$$

$$=\quad \{\ (67),\ \downarrow = \wedge\ \}$$

$$wlp.S.Q.x \quad \wedge \quad wp.S.true.x$$

$$=\quad \{\ (196) \text{ and } (197)\text{: definition of } wlp \text{ and } wp\ \}$$

$$\forall(t : t \in \{x\}; S : |t| = \infty \quad \vee \quad Q.(last.t)) \quad \wedge \quad \forall(t : t \in \{x\}; S : |t| < \infty \quad \wedge \quad true.(last.t))$$

$$=\quad \{\ \text{predicate calculus}\ \}$$

$$\forall(t : t \in \{x\}; S : |t| < \infty \quad \wedge \quad Q.(last.t))$$

$$=\quad \{\ (197)\text{: definition of } wp\ \}$$

$$wp.S.Q.x$$

□

Here is another property of wp.

Theorem *Law of the Excluded Miracle*

$$wp.S.false \ = \ false \tag{200}$$

Proof

$$wp.S.false.x$$

$$=\quad \{\ (197)\text{: definition of } wp\ \}$$

$$\forall(t : t \in \{x\}; S : |t| < \infty \quad \wedge \quad false.(last.t))$$

$$=\quad \{\ \text{predicate calculus}\ \}$$

$$false$$

□

Next, we calculate the wlp of some programs. The first one is $skip$.

$$wlp.skip.Q.x$$

$$=\quad \{\ (196)\text{: definition of } wlp\ \}$$

$$\forall(t : t \in \{x\}; skip : |t| = \infty \quad \vee \quad Q.(last.t))$$

$$=\quad \{\ (180)\text{: } skip \text{ is right unit of ; }\}$$

$$\forall(t : t \in \{x\} : |t| = \infty \quad \vee \quad Q.(last.t))$$

$$=$$

$$Q.x$$

and hence (and by a similar calculation for wp)

$$wlp.skip.Q \ = \ Q \tag{201}$$

We use some of the results of lattice theory in this exploration. To that end, observe that the booleans form a complete boolean lattice with

$$\begin{array}{lll} \bot & = & \mathit{false} \\ \top & = & \mathit{true} \\ \le & = & \Rightarrow \\ \uparrow & = & \vee, \quad \exists \\ \downarrow & = & \wedge, \quad \forall \end{array}$$

Theorem

$$wlp \text{ is universally } \wedge\text{-distributive.} \tag{198}$$

Proof
Let P be a set of predicates.

$$\begin{array}{ll}
 & wlp.S.\forall(p : p \in P : p).x \\
= & \quad \{ \text{ (196): definition } wlp \ \} \\
 & \forall(t : t \in \{x\}; S : |t| = \infty \ \vee \ \forall(p : p \in P : p).(last.t)) \\
= & \quad \{ \text{ (67), } \downarrow = \forall \ \} \\
 & \forall(t : t \in \{x\}; S : |t| = \infty \ \vee \ \forall(p : p \in P : p.(last.t))) \\
= & \quad \{ \text{ predicate calculus } \} \\
 & \forall(t : t \in \{x\}; S : \forall(p : p \in P : |t| = \infty \ \vee \ p.(last.t))) \\
= & \quad \{ \text{ predicate calculus } \} \\
 & \forall(p : p \in P : \forall(t : t \in \{x\}; S : |t| = \infty \ \vee \ p.(last.t))) \\
= & \quad \{ \text{ (196): definition } wlp \ \} \\
 & \forall(p : p \in P : wlp.S.p.x) \\
= & \quad \{ \text{ (67), } \downarrow = \forall \ \} \\
 & \forall(p : p \in P : wlp.S.p).x
\end{array}$$

□

Theorem

For all S and Q

$$wp.S.Q \ = \ wlp.S.Q \ \wedge \ wp.S.true \tag{199}$$

Proof

$$(wlp.S.Q \ \wedge \ wp.S.true).x$$

we observe $a \in A; B$ if a is infinite. Also, if a is finite, a trace $y\ s$ exists such that $y\ s \in B$ whose first element y equals a's last element since a is nonempty and B is a program for which the induction hypothesis holds. From the definition of ; it follows that $a\ s \in A; B$ The result now follows from $a \leq a\ s$. The theorem follows from this result plus the induction hypothesis that A contains a trace starting with x, for any $x \in X$.

Let $IF = \mathbf{if}\ b_i \rightarrow s_i\ \mathbf{fi}$. Notice that $b?; V$ is the subset of V whose traces start with a state in which b holds. Since for every state x we have $\forall(i :: \neg b_i.x) \ \vee\ \exists(i :: b_i.x)$, the fact that the theorem holds for IF follows from the induction hypothesis for s_i and the fact that the theorem holds for *abort*.

Let $DO = \mathbf{do}\ b \rightarrow s\ \mathbf{od}$. Suppose that for some state $x \in X$ we have no trace in DO starting with x. Since traces starting with x are present in $(b?;\ s)^n$ for all n, provided the induction hypothesis holds for s, but apparently not in $(b?;\ s)^\omega$, it follows that all those traces are finite and their last state satisfies b. Define a characterizing chain c as $c_0 = x$ and choose $c_{i+1} \in \{c_i\}; s$ arbitrarily. $\uparrow c$ starts with x and is a loop trace of $b?;\ s$ and hence it is in DO.

□

As a result, we have that programs are nonempty sets of traces.

Next, we look at properties of programs. A property may be viewed as a set of traces, and a program has a property if all its traces are in that set. We write *Prop* for the set of all properties $\mathcal{P}(T)$. We introduce the *weakest precondition* for a program and a property to be the condition on the initial state such that *all* traces with that initial state have the required property.

Function $w : Prog \times Prop \times X \rightarrow boolean$ is defined as

$$w.S.Q.x \ = \ \{x\}; S \subseteq Q \tag{191}$$

This allows us to the define the classical weakest precondition and weakest liberal precondition as

$$wlp.S.Q \ = \ w.S.(lt.Q) \tag{192}$$

$$wp.S.Q \ = \ w.S.(ct.Q) \tag{193}$$

where the liberal and conservative termination functions are defined by

$$lt.Q \ = \ \{t : t \in T \ \wedge\ (|t| = \infty \ \vee\ Q.(last.t)) : t\} \tag{194}$$

$$ct.Q \ = \ \{t : t \in T \ \wedge\ (|t| < \infty \ \wedge\ Q.(last.t)) : t\} \quad . \tag{195}$$

Substitution yields

$$wlp.S.Q.x \ = \ \forall(t : t \in \{x\}; S : |t| = \infty \ \vee\ Q.(last.t)) \tag{196}$$

$$wp.S.Q.x \ = \ \forall(t : t \in \{x\}; S : |t| < \infty \ \wedge\ Q.(last.t)) \tag{197}$$

Both wlp and wp are functions that, for fixed command S, map a predicate to a predicate. Such a function is sometimes called a predicate transformer. Next, we derive some properties of wlp and wp.

□

Theorem

$$DO \ = \ \textbf{if } b \rightarrow s;\, DO \,\|\, \neg b \rightarrow skip \textbf{ fi} \tag{189}$$

Proof

$$
\begin{array}{ll}
 & \textbf{if } b \rightarrow s;\, DO \,\|\, \neg b \rightarrow skip \textbf{ fi} \\
= & \quad \{ \text{ definition } \} \\
 & b?;\, s;\, DO \cup \neg b?;\, skip \cup false?;\, abort \\
= & \quad \{ \ false? = \emptyset;\ (180)\text{: } skip \text{ is right unit of ; } \} \\
 & b?;\, s;\, DO \cup \neg b? \\
= & \quad \{ \ (187) \ \} \\
 & b?;\, s;\, (b?;\, s)^{\omega};\, \neg b? \cup \neg b? \\
= & \quad \{ \ (180)\text{: } skip \text{ is left unit of ; } \} \\
 & b?;\, s;\, (b?;\, s)^{\omega};\, \neg b? \cup skip;\, \neg b? \\
= & \quad \{ \ (179) \ \} \\
 & (b?;\, s;\, (b?;\, s)^{\omega} \cup skip);\, \neg b? \\
= & \quad \{ \ 188) \ \} \\
 & (b?;\, s)^{\omega};\, \neg b? \\
= & \quad \{ \ (187) \ \} \\
 & DO
\end{array}
$$

□

16 Properties of programs

Theorem

For every program S and every state x, S contains a trace starting with x. (190)

Proof

The proof is by induction over the syntax of the program notation. The theorem is obviously true if S is one of *abort*, *skip*, or assignment.

If the theorem holds for A and B then we show that it holds for $A; B$ as well. To prove

$$\forall(a : a \in A : \exists(t : t \in A; B : a \leq t))$$

For $A \subseteq T$ we define A^ω as

$$A^\omega = loop.A \cup \cup(n : n \geq 0 : A^n) \tag{186}$$

Next, we define the semantics of a loop. We use the abbreviation $DO = \mathbf{do}\ b \rightarrow s\ \mathbf{od}$.

$$DO \ = \ (b?;\, s)^\omega;\, \neg b? \tag{187}$$

This definition of DO is rather complicated. And alternative way of defining DO starts with its first unfolding. A definition of DO is then obtained by solving equation

$$DO: \quad DO \ = \ \mathbf{if}\ b \rightarrow s;\, DO \,[\!]\, \neg b \rightarrow skip\ \mathbf{fi}$$

but it may have multiple solutions. One then introduces a topology, based on a metric, and shows that only one nonempty closed solution exists. Often, this requires that the nondeterminism be bounded to make certain functions continuous. Nondeterminism plays no role in our definition (and hence can be unbounded) and no metric or topology is needed. With our definition, we can prove that DO equals its first unfolding.

Theorem

$$A^\omega \ = \ skip \cup A;\, A^\omega \tag{188}$$

Proof

$$
\begin{array}{ll}
 & A^\omega \\
= & \quad \{\ (186)\ \} \\
 & loop.A \cup \cup(n : n \geq 0 : A^n) \\
= & \quad \{\ (185);\ inf.A \subseteq \cup(n : n \geq 0 : A^n)\ \ \} \\
 & A;\, loop.A \cup \cup(n : n \geq 0 : A^n) \\
= & \quad \{\ \text{range split}\ \} \\
 & A;\, loop.A \cup skip \cup \cup(n : n \geq 1 : A^n) \\
= & \quad \{\ \text{definition of}\ A^{n+1}\ \ \} \\
 & A;\, loop.A \cup skip \cup \cup(n : n \geq 0 : A;\, A^n) \\
= & \quad \{\ (179)\ \} \\
 & A;\, loop.A \cup skip \cup A;\ \cup\,(n : n \geq 0 : A^n) \\
= & \quad \{\ (179)\ \} \\
 & skip \cup A;\, (loop.A \cup \cup(n : n \geq 0 : A^n) \\
= & \quad \{\ (186)\ \} \\
 & skip \cup A;\, A^\omega
\end{array}
$$

$$
\begin{array}{ll}
= & \quad \{ \ c_i.i = d.i \ \} \\
& \forall(i, j : 0 \leq i < |c_j| : c_j.i = d.i) \\
= & \\
& \forall(j :: c_j \leq d)
\end{array}
$$

and hence d is an upper bound of c. Let e be an infinite trace different from d. We have

$$
\begin{array}{ll}
& d \neq e \\
\Rightarrow & \quad \{ \text{ both } d \text{ and } e \text{ are infinite } \} \\
& \exists(i :: d.i \neq e.i) \\
= & \\
& \exists(i :: c_i.i \neq e.i) \\
\Rightarrow & \\
& \exists(i :: \neg(c_i \leq e))
\end{array}
$$

which implies that e is not an upper bound of c. No finite trace is an upper bound of infinite chain c. Hence, d is the one and only upper bound of c . In particular $d = \uparrow c$.

□

Next, we do the "inverse": given an infinite trace t, we define a chain c to be a *characterizing chain* of t just when $t = \uparrow c$.

We say that trace t is a *loop trace* of trace set A if a characterizing chain c of t exists such that $c_i \in A^i$ for all $i \geq 0$. The set of all loop traces of A is denoted by $loop.A$.

Theorem

If $A \subseteq T$ then

$$loop.A \cup inf.A \ = \ A; loop.A \tag{185}$$

Proof

$\subseteq$:

Obviously, $inf.A = inf.A; loop.A \subseteq A; loop.A$, so it remains to show $loop.A \subseteq A; loop.A$. Let $t \in loop.A$ and let c be a characterizing chain of t. Since $c_1 \leq c_i$ for $i \geq 1$, we can define d as $c_i = c_1; d_{i-1}$ for $i \geq 1$. Since c is a chain, d is a chain. Because $c_1 \in A$ and $c_1; d_i \in A; A^i$ we have $d_i \in A^i$ for $i \geq 1$ and because $d_0 \in skip$ we have $\uparrow d \in loop.A$. Since $t = c_1; \uparrow d$ we have $t \in A; loop.A$.

$\supseteq$:

Let $a; t \in A; loop.A$. Either $a \in inf.A$ and we are done, or else $a \in fin.A$, $t \in loop.A$, and c is a characteristic chain of t. Define chain d as $d_0 = a.0$ and $d_{i+1} = a; c_i$. Since $c_i \in A^i$ we have $d_{i+1} \in A^{i+1}$ and since $d_0 \in true?$ we have $a; t = \uparrow d \in loop.A$.

□

We do not bother here with definedness of $e.x$. Next we define sequential composition for $U, V \subseteq T$.

$$U;\ V \ = \ \{u, x, v : ux \in U \wedge xv \in V : uxv\} \cup inf.U \tag{177}$$

Observe that term $inf.U$ can be omitted if V is nonempty. If V is empty, we have $U;\ V = inf.U$. When traces u and v satisfy $last.u = v.0$, we write $u;\ v$ for the the trace obtained by catenating u and the trace obtained by removing the leading element of v.

; is associative (178)

; is universally $\cup$ −distributive in both arguments (179)

skip is a left and right unit element of ; (180)

$$U;\ \ V \ = \ \{u : u \in U : \{u\};\ V\} \tag{181}$$

For predicate $b : X \rightarrow boolean$, we define $b?$ to be the construct that does not modify the state but restricts the state to those states for which b is *true*.

$$b? \ = \ \{x : x \in X \ \ \wedge \ \ b.x : x\ x\} \tag{182}$$

$$\textbf{if}\ [\!](i :: b_i \rightarrow s_i)\ \textbf{fi} \ = \ \cup(i :: b_i?;\ s_i) \cup \forall(i :: \neg b_i)?;\ abort \tag{183}$$

in which we assume that ; binds more strongly than $\cup$ does. For $V \subseteq T,$ we define V^n as

$V^0 = skip$

$V^{n+1} = V;\ V^n$ for $n \geq 0$

The prefix order $\leq$ on T is a partial order, but T is not a complete lattice, yet we need the lowest upper bound of certain sets.

Theorem

Every nonempty chain has a lowest upper bound (184)

Proof

Consider chain c and let c_i be the lowest-but- i trace of the chain, that is $c_i \leq c_{i+1}$. If c is finite, the highest trace in c is $\uparrow c$. If c is an infinite set, c_i is strictly rising with i. Let d be an infinite trace such that $d.i = c_i.i$ for all i. We have

c is a chain

$\Rightarrow$

$\forall(i, j : 0 \leq i < |c_j| : c_j.i = c_i.i)$

$=$ $\{$ definition of l $\}$

$\lfloor z : z = h.x.z \rfloor \leq \lfloor z : z = h.y.z \rfloor$

$=$ $\{$ Knaster Tarski $\}$

$\downarrow\{z : z \geq h.x.z : z\} \leq \downarrow\{z : z \geq h.y.z : z\}$

$\Leftarrow$ $\{$ (40) $\}$

$\forall(z :: z \geq h.x.z \;\Leftarrow\; z \geq h.y.z)$

$\Leftarrow$ $\{$ predicate calculus $\}$

$\forall(z :: h.x.z \leq h.y.z)$

$\Leftarrow$ $\{$ h is monotonic in its first argument $\}$

$x \leq y$

□

15 Operational Semantics

We define the semantics of a program to be the set of all traces (finite or infinite state sequences) that may result from executing the program.

X	the state space; a cartesian product with one coordinate per program variable
	the state space is nonempty
T	the set of all nonempty traces
$\vert t\vert$	the length of trace t
$t.i$	the first-but- i element of trace t; $0 \leq i < \vert t\vert$

We write $last.t$ for the last element of nonempty trace t. We write juxtaposition for catenation of strings. We write x^∞ for an infinite sequences of x's. We write $x(v := e.x)$ for the state which is a copy of x except the v coordinate is replaced with the value of e computed in state x. Relation $\leq$ is a partial order on traces; $s \leq t$ holds just when s is a prefix of t. For V a set of traces, $fin.V$ is the subset of V consisting of its finite traces, and $inf.V$ consists of the infinite traces.

We define the three basic constructs of our programming language. In the definition of $skip$, observe that we identify states and traces of length one.

$$abort \;=\; \{x : x \in X : x^\infty\} \tag{174}$$

$$skip \;=\; X \tag{175}$$

$$v := e \;=\; \{x : x \in X : x\; x(v := e.x)\} \tag{176}$$

□

Theorem

$$r \circ g = s \quad . \tag{172}$$

Proof

$$
\begin{array}{ll}
 & true \\
= & \{\ (120)\text{ for } r.x \ \} \\
 & \forall(x :: r.x = h.x.(r.x)) \\
\Rightarrow & \\
 & \forall(x :: r.(g.x) = h.(g.x).(r.(g.x))) \\
= & \\
 & \forall(x :: (r \circ g).x = h.(g.x).((r \circ g).x)) \\
\Rightarrow & \{\ (11)\text{: definition of } \circ\text{; definition of } s \ \} \\
 & s \leq r \circ g
\end{array}
$$

$$
\begin{array}{ll}
 & true \\
= & \{\ (120)\text{ for } s \ \} \\
 & \forall(x :: s.x = h.(g.x).(s.x)) \\
\Rightarrow & \{\ s.x \text{ solves defining equation of } l.(g.x) \ \} \\
 & \forall(x :: l.(g.x) \leq s.x) \\
= & \{\ (171)\text{: } l = r \ \} \\
 & \forall(x :: r.(g.x) \leq s.x) \\
= & \{\ (11)\text{: definition of } \circ \ \} \\
 & r \circ g \leq s
\end{array}
$$

□

Theorem *fixpoint is monotonic*

if h is monotonic in its first argument, l is monotonic (173)

Proof

$$l.x \leq l.y$$

14 More on fixpoints

Let f be a monotonic function (on a complete lattice), which implies that μf exists. Obviously,

$$\forall(y : y = f.y : y \geq \mu f) \qquad .$$

Let $h.x.y$ be a monotonic function of y. Define functions l, r, and s as follows.

$$\begin{array}{lcl} l.x & = & \lfloor y : y = h.x.y \rfloor \\ r & = & \lfloor f : \forall(x :: f.x = h.x.(f.x)) \rfloor \\ s & = & \lfloor f : \forall(x :: f.x = h.(g.x).(f.x)) \rfloor \end{array}$$

Notice that $\lambda(x :: h.x.(f.x))$ is a monotonic function of f :

$$\begin{array}{ll} & \forall(x :: h.x.(f.x) \leq h.x.(g.x)) \\ \Leftarrow & \qquad \{ \ h \text{ is monotonic in its last argument } \} \\ & \forall(x :: f.x \leq g.x) \\ = & \\ & f \leq g \end{array}$$

Theorem *range of fixpoint is pointwise*

$$l = r \qquad . \tag{171}$$

Proof

$$\begin{array}{ll} & true \\ = & \qquad \{ \ (120) \text{ for } l.x \ \} \\ & \forall(x :: l.x = h.x.(l.x)) \\ \Rightarrow & \qquad \{ \text{ definition of } r \ \} \\ & r \leq l \end{array}$$

$$\begin{array}{ll} & true \\ = & \qquad \{ \ (120) \text{ for } r \ \} \\ & \forall(x :: r.x = h.x.(r.x)) \\ \Rightarrow & \qquad \{ \text{ definition of } l.x \ \} \\ & \forall(x :: l.x \leq r.x) \\ = & \\ & l \leq r \end{array}$$

$\square$

Theorem

$$\uparrow(f.X)\uparrow\uparrow(g.X) \;=\; \uparrow((f\uparrow g).X) \tag{168}$$

$$\downarrow(f.X)\downarrow\downarrow(g.X) \;=\; \downarrow((f\downarrow g).X) \tag{169}$$

The following theorem is from [3].

Theorem *Lifting Galois connections*

Let $f : X \to Y$ and $g : Y \to X$. Define

$$\begin{aligned} f'.a &= f \circ a \circ g \\ g'.b &= g \circ b \circ f \end{aligned}$$

where $a : X \to X$ and $b : Y \to Y$. If a and b are monotonic, we have

$$Galois(f, g) \;\Rightarrow\; Galois(f', g') \tag{170}$$

Proof

$$\begin{array}{ll}
 & a \le g'.b \\
= & \quad \{ \text{ definition of } g' \; \} \\
 & a \le g \circ b \circ f \\
= & \quad \{ \text{ definition of } \le \; \} \\
 & \forall(x :: a.x \le g.(b.(f.x))) \\
= & \quad \{ \;\; Galois(f,g) \;\; \} \\
 & \forall(x :: f.(a.x) \le b.(f.x)) \\
\Rightarrow & \quad \{ \text{ instantiate } x := g.y \;\; \} \\
 & \forall(y :: f.(a.(g.y)) \le b.(f.(g.y))) \\
\Rightarrow & \quad \{ \;\; Galois(f,g) \;\Rightarrow\; f.(g.y) \le y\,;\; b \text{ is monotonic } \} \\
 & \forall(y :: f.(a.(g.y)) \le b.y) \\
= & \quad \{ \text{ definition of } f' \text{ and } \le \; \} \\
 & f'.a \le b \\
\Rightarrow & \quad \{ \text{ similarly } \} \\
 & a \le g'.b
\end{array}$$

$\square$

$$
\begin{array}{ll}
 & x \le g \downarrow^{*} .y \\
\Leftarrow & \quad \{ \ x \le f \uparrow^{*} .x \ \} \\
 & f \uparrow^{*} .x \le g \downarrow^{*} .y \\
\Leftarrow & \quad \{ \ z \le y \downarrow g.z \ \Rightarrow \ z \le g \downarrow^{*} .y \ \} \\
 & f \uparrow^{*} .x \le y \downarrow g.(f \uparrow^{*} .x) \\
= & \quad \{ \ (61) \ \} \\
 & f \uparrow^{*} .x \le y \quad \wedge \quad f \uparrow^{*} .x \le g.(f \uparrow^{*} .x) \\
= & \quad \{ \ Galois(f,g) \ \} \\
 & f \uparrow^{*} .x \le y \quad \wedge \quad f.(f \uparrow^{*} .x) \le f \uparrow^{*} .x \\
= & \quad \{ \ (144) \ \} \\
 & f \uparrow^{*} .x \le y \\
\Leftarrow & \quad \{ \ \text{similarly} \ \} \\
 & x \le g \downarrow^{*} .y
\end{array}
$$

$\Box$

13 Lifting

Theorem *μ is monotonic*

$$f \le g \ \Rightarrow \mu f \le \mu g \tag{167}$$

Proof

$$
\begin{array}{ll}
 & \mu f \\
= & \quad \{ \ \text{definition of } \mu \ \} \\
 & \downarrow\{x : x = f.x : x\} \\
= & \quad \{ \ (122) \ \} \\
 & \downarrow\{x : x \ge f.x : x\} \\
\le & \quad \{ \ (42) \text{ applies since } x = g.x \ \Rightarrow \ x \ge f.x \text{ because } f \le g \ \} \\
 & \downarrow\{x : x = g.x : x\} \\
= & \quad \{ \ \text{definition of } \mu \ \} \\
 & \mu g
\end{array}
$$

$$
\begin{array}{ll}
 & g.(f.x) = x \\
\Rightarrow & \qquad \{ \ f.x \in Y \ \ \} \\
 & x \in g.Y \\
\Rightarrow & \\
 & \exists(y : y \in Y : x = g.y) \\
= & \qquad \{ \ \ g.y = g.(f.(g.y)) \ \ \} \\
 & \exists(y : y \in Y : x = g.y \quad \wedge \quad x = g.(f.(g.y))) \\
\Rightarrow & \\
 & x = g.(f.x)
\end{array}
$$

□

Hence, the set of fixpoints of $g \circ f$ is $g.Y$ and the set of fixpoints of $f \circ g$ is $f.X$.

Theorem

If $Galois(f, g)$ then

$$(g.(f.x) \leq x) \ = \ (x \in g.Y) \tag{163}$$

$$(y \leq f.(g.y)) \ = \ (y \in f.X) \tag{164}$$

Theorem *Composition of Galois connections*

If $f0 : Y \to Z, \ \ g0 : Z \to Y, \ \ f1 : X \to Y, \ \ g1 : Y \to X,$

$$Galois(f0, g0) \wedge Galois(f1, g1) \ \Rightarrow \ Galois(f0 \circ f1, g1 \circ g0) \tag{165}$$

Proof

$$
\begin{array}{ll}
 & y \leq f0.(f1.x) \\
= & \qquad \{ \ \ Galois(f0, g0) \ \ \} \\
 & g0.y \leq f1.x \\
= & \qquad \{ \ \ Galois(f1, g1) \ \ \} \\
 & g1.(g0.y) \leq x
\end{array}
$$

□

Theorem *C.S. Scholten*

$$Galois(f, g) \ \Rightarrow \ Galois(f \, {\uparrow}\!\!\!\!{\ast}, g \, {\downarrow}\!\!\!\!{\ast}) \tag{166}$$

Proof

$$g.x \le g.y$$
$$f.(g.x) \le f.(g.y)$$
$$f.(g.x) \le y$$

are equivalent.

Proof

Immediate from previous result by instantiating with $x := g.x$.

□

Theorem

If $Galois(f,g)$ and $X = Y$ then conditions

$$f.x \le f.y$$
$$g.(f.x) \le g.(f.y)$$
$$x \le g.(f.y)$$

are equivalent.

Let V be a set of pairs of functions where each pair is a Galois connection. If $F.x = \uparrow\{f,g:(f,g) \in V : f.x\}$ and $G.y = \downarrow\{f,g:(f,g) \in V : g.y\}$ then $Galois(F,G)$.

$$\begin{array}{ll} & F.x \le y \\ = & \quad \{ \text{ definition of } F \ \} \\ & \uparrow\{f,g:(f,g) \in V : f.x\} \le y \\ = & \quad \{ \ (20) \ \} \\ & \forall(f,g:(f,g) \in V : f.x \le y) \\ = & \quad \{ \ Galois(f,g) \ \} \\ & \forall(f,g:(f,g) \in V : x \le g.y) \\ = & \quad \{ \ (21) \ \} \\ & x \le \downarrow\{f,g:(f,g) \in V : g.y\} \\ = & \quad \{ \text{ definition of } G \ \} \\ & x \le G.y \end{array}$$

Theorem

If $Galois(f,g)$ then

$$(g.(f.x) = x) \ = \ (x \in g.Y) \qquad (161)$$

$$(f.(g.y) = y) \ = \ (y \in f.X) \qquad (162)$$

Proof

The choice between the symmetric and asymmetric Galois connections seems to be no big deal when X and Y are different lattices (just switch from $\leq$ to $\geq$ in one of them). However, our main interest will be the case where $X = Y$, and in that case the choice does matter because it is inconvenient to having to work with two partial orders on the same set. In our application, we need the asymmetric Galois connection, and we will omit the arrows from now on.

For a Galois connection (f, g) we also have the following result.

$$
\begin{array}{ll}
& Galois(f,g) \\
\Rightarrow & \quad \{ \text{ (iv) above } \} \\
& \forall(x, y :: f.(g.y) \leq y \quad \wedge \quad x \leq g.(f.x)) \\
= & \quad \{ \text{ instantiate with } y := f.x \text{ and } x := g.y \ \} \\
& \forall(x, y :: f.(g.y) \leq y \quad \wedge \quad x \leq g.(f.x) \quad \wedge \quad f.(g.(f.x)) \leq f.x \quad \wedge \quad g.y \leq g.(f.(g.y))) \\
\Rightarrow & \quad \{ \text{ (iv): monotonicity of } f \text{ and } g \ \} \\
& \forall(x, y :: g.(f.(g.y)) \leq g.y \quad \wedge \quad f.x \leq f.(g.(f.x)) \quad \wedge \quad f.(g.(f.x)) \leq f.x \quad \wedge \quad g.y \leq g.(f.(g.y))) \\
= & \\
& \forall(x, y :: g.y = g.(f.(g.y)) \quad \wedge \quad f.(g.(f.x)) = f.x) \\
\Rightarrow & \\
& g \circ f = g \circ f \circ g \circ f \quad \wedge \quad f \circ g = f \circ g \circ f \circ g
\end{array}
$$

Hence $f \circ g$ is a $\downarrow$-closure and $g \circ f$ is an $\uparrow$-closure. From the universal distributivity properties of f and g we conclude

$$f.\bot = \bot \quad \wedge \quad g.\top = \top \tag{160}$$

Theorem

If $Galois(f, g)$ then conditions

$$x \leq g.y$$
$$f.x \leq f.(g.y)$$
$$f.x \leq y$$
$$g.(f.x) \leq y$$

are equivalent.

Proof

See proof of (iv) $\Rightarrow$ (i) above.

□

Theorem

If $Galois(f, g)$ and $X = Y$ then conditions

The second part of (iv) follows from

$$
\begin{array}{ll}
& \forall(y :: g.y = \lceil x : f.x \le y\rceil) \\
\Rightarrow & \quad \{\ (114)\ \} \\
& \forall(y :: f.(g.y) \le y \quad \wedge \quad \forall(x :: f.x \le y \ \Rightarrow \ x \le g.y)) \\
\Rightarrow & \quad \{\ \text{instantiate second term with } \ y := f.x \ \} \\
& \forall(y :: f.(g.y) \le y) \quad \wedge \quad \forall(x :: f.x \le f.x \ \Rightarrow \ x \le g.(f.x)) \\
= & \\
& \forall(y :: f.(g.y) \le y) \quad \wedge \quad \forall(x :: x \le g.(f.x))
\end{array}
$$

(iv) $\Rightarrow$ (i):

$$
\begin{array}{ll}
& x \le g.y \\
\Rightarrow & \quad \{\ f \ \text{is monotonic}\ \} \\
& f.x \le f.(g.y) \\
\Rightarrow & \quad \{\ f.(g.y) \le y \ \} \\
& f.x \le y \\
\Rightarrow & \quad \{\ g \ \text{is monotonic}\ \} \\
& g.(f.x) \le g.y \\
\Rightarrow & \quad \{\ x \le g.(f.x) \ \} \\
& x \le g.y
\end{array}
$$

Conditions (ii)b and (iii)b are dual to (ii)a and (iii)a.

□

We write $\downarrow\uparrow\text{-}\,Galois(f,g)$ to indicate the asymmetry in f and g. For any x, $f.x$ is the highest lower bound ($\downarrow$) of set $\{y : x \le g.y : y\}$, hence the $\downarrow$ in the first position. Since g is a lowest upper bound, we have an $\uparrow$ in the second position. The original definition of Galois connection (cf. [2]) is

$$\forall(x, y :: f.x \le y \ = \ g.y \le x)$$

which we would write as $\downarrow\downarrow\text{-}\,Galois(f,g)$. It is symmetric in f and g; both f and g are antimonotonic, and both $f \circ g$ and $g \circ f$ are contractions. For any set V, $\uparrow(f.V) = f.\!\downarrow V$. For any x, $f.x = \downarrow\{y : g.x \le y : y\}$. As an example of such a Galois connection, notice that in a boolean lattice we have

$$\forall(x, y :: \neg x \le y \ = \ \neg y \le x)$$

and, hence, $\downarrow\downarrow\text{-}\,Galois(\neg,\neg)$. Property $\uparrow(f.V) = f.\!\downarrow V$ immediately gives us De Morgan's rules.

$$
\begin{array}{ll}
 & f.\uparrow V \le y \\
= & \qquad \{\ (i); (158)\ \} \\
 & \uparrow V \le g.y \\
= & \qquad \{\ (20)\ \} \\
 & \forall(z : z \in V : z \le g.y) \\
= & \qquad \{\ (i); (158)\ \} \\
 & \forall(z : z \in V : f.z \le y) \\
= & \qquad \{\ (20)\ \} \\
 & \uparrow\{z : z \in V : f.z\} \le y \\
= & \\
 & \uparrow(f.V) \le y
\end{array}
$$

from which we conclude (using (8)) the first part of (ii)a. The second part follows from

$$
\begin{array}{ll}
 & \uparrow\{x : f.x \le y : x\} \\
= & \qquad \{\ (i); (158)\ \} \\
 & \uparrow\{x : x \le g.y : x\} \\
= & \qquad \{\ (28)\ \} \\
 & g.y \qquad .
\end{array}
$$

(ii)a $\Rightarrow$ (iii)a:
The monotonicity of f follows from the distributivity of f. On account of (116), the monotonicity of f implies that $\lceil x : f.x \le y \rceil$ exists, and on account of (112) it equals $\uparrow\{x : f.x \le y : x\}$.
(iii)a $\Rightarrow$ (iv):
Monotonicity of g follows from

$$
\begin{array}{ll}
 & g.y \le g.z \\
= & \qquad \{\ (iii)\ \} \\
 & \lceil x : f.x \le y \rceil \le \lceil x : f.x \le x \rceil \\
= & \\
 & \uparrow\{x : f.x \le y : x\} \le \uparrow\{x : f.x \le z : x\} \\
\Leftarrow & \qquad \{\ (39)\ \} \\
 & \forall(x :: f.x \le y \ \Rightarrow\ f.x \le z) \\
\Leftarrow & \\
 & y \le z \qquad .
\end{array}
$$

From

$$\begin{array}{ll} & \uparrow\{i : i \geq 0 : f^i.\bot\} \\ = & \quad \{ \text{ range split } \} \\ & \bot \uparrow \uparrow\{i : i \geq 1 : f^i.\bot\} \\ = & \\ & \uparrow\{i : i \geq 0 : f.(f^i.\bot)\} \\ = & \quad \{ \ \{i : i \geq 0 : f^i.\bot\} \text{ is a nonempty chain, and } f \text{ is positively } \uparrow\text{-continuous } \} \\ & f.\uparrow\{i : i \geq 0 : f^i.\bot\} \end{array}$$

we conclude that $\uparrow\{i : i \geq 0 : f^i.\bot\}$ is a fixpoint of f, and from (154) we conclude that it is below μf, the lowest fixpoint. Hence $\uparrow\{i : i \geq 0 : f^i.\bot\} = \mu f$.

□

12 Galois Connections

Let X and Y be partially ordered sets, and let $f : X \to Y$ and $g : Y \to X$. Functions f and g form a Galois connection just when $\downarrow\uparrow\text{-}\,Galois(f, g)$ holds.

$$\downarrow\uparrow - Galois(f, g) \;=\; \forall(x, y : x \in X \wedge y \in Y : f.x \leq y \;=\; x \leq g.y) \tag{158}$$

We are especially interested in Galois connections for the case where X and Y are complete lattices because the functions involved in Galois connections have strong distributivity properties. Throughout this section, x ranges over X and y ranges over Y. We have the following theorem.

Theorem

Properties (159)

(i) $\downarrow\uparrow\text{-}\,Galois(f, g)$

(ii)a f is universally $\uparrow$-distributive $\wedge$ $\forall(y :: g.y = \uparrow\{x : f.x \leq y : x\})$

(ii)b g is universally $\downarrow$-distributive $\wedge$ $\forall(x :: f.x = \downarrow\{y : x \leq g.y : y\})$

(iii)a f is monotonic $\wedge$ $\forall(y :: g.y = \lceil x : f.x \leq y\rceil)$

(iii)b g is monotonic $\wedge$ $\forall(x :: f.x = \lfloor y : x \leq g.y\rfloor)$

(iv) f and g are monotonic $\wedge$ $\forall(x, y :: x \leq g.(f.x) \;\wedge\; f.(g.y) \leq y)$,

are equivalent.

Proof

(i) $\Rightarrow$ (ii)a:

First, we calculate

$$
\begin{array}{ll}
 & \forall(y :: f.y \leq y \ \Rightarrow\ (\bot \leq y \ = \ f \ \uparrow\!\!\!\ast\ .\bot \leq y)) \\
= & \qquad \{ \ (147)\text{: no overshoot } \} \\
 & \mathit{true}
\end{array}
$$

□

From (149) and (152) we conclude

$$\mu f \ \geq \ \uparrow\{i : i \geq 0 : f^i.\bot\} \tag{154}$$

and, by duality

$$\nu f \ \leq \ \downarrow\{i : i \geq 0 : f^i.\top\} \tag{155}$$

Let us now see under which condition equality holds.

Theorem

$$\mu f \ = \ \uparrow\{i : i \geq 0 : f^i.\bot\} \qquad \text{if } f \text{ is positively } \uparrow\text{-continuous} \tag{156}$$

$$\nu f \ = \ \downarrow\{i : i \geq 0 : f^i.\top\} \qquad \text{if } f \text{ is positively } \downarrow\text{-continuous} \tag{157}$$

Proof

First, we show that $\{i : i \geq 0 : f^i.\bot\}$ is a chain if f is monotonic, a condition which is implied by f being continuous. We prove by induction $\forall(i : i \geq 0 : f^i.\bot \leq f^{i+1}.\bot)$.

$i = 0$:

$$
\begin{array}{ll}
 & f^0.\bot \leq f^1.\bot \\
= & \\
 & \bot \leq f^1.\bot \\
= & \\
 & \mathit{true}
\end{array}
$$

$i \geq 0$:

$$
\begin{array}{ll}
 & f^{i+1}.\bot \leq f^{i+2}.\bot \\
= & \\
 & f.(f^i.\bot) \leq f.(f^{i+1}.\bot) \\
\Leftarrow & \qquad \{ \ f \text{ is monotonic } \} \\
 & f^i.\bot \leq f^{i+1}.\bot \\
= & \qquad \{ \text{ induction hypothesis } \} \\
 & \mathit{true}
\end{array}
$$

$$
\begin{array}{ll}
& g.(f{\uparrow^{*}}.(s.x)) \le s.x \\
= & \\
& (t \circ t{\uparrow^{*}}).x \le t{\uparrow^{*}}.x \\
= & \qquad \{ \ (144) \ \} \\
& \mathit{true}
\end{array}
$$

Pong:

$$
\begin{array}{ll}
& f{\uparrow^{*}} \circ (g \circ f{\uparrow^{*}}){\uparrow^{*}} \\
\le & \qquad \{ \ \text{monotonicity} \ \} \\
& (f \uparrow g){\uparrow^{*}}.((f \uparrow g) \circ (f \uparrow g){\uparrow^{*}}){\uparrow^{*}} \\
= & \qquad \{ \ f{\uparrow^{*}} = f \circ f{\uparrow^{*}} \ \} \\
& (f \uparrow g){\uparrow^{*}}.(f \uparrow g){\uparrow^{*}}{\uparrow^{*}} \\
= & \qquad \{ \ f{\uparrow^{*}} = f \circ f{\uparrow^{*}} \ \} \\
& (f \uparrow g){\uparrow^{*}}{\uparrow^{*}} \\
= & \qquad \{ \ f{\uparrow^{*}}{\uparrow^{*}} = f{\uparrow^{*}} \ \} \\
& (f \uparrow g){\uparrow^{*}}
\end{array}
$$

□

Theorem

$$\mu f = f{\uparrow^{*}}.\bot \tag{152}$$

$$\nu f = f{\downarrow^{*}}.\top \tag{153}$$

Proof

From Knaster-Tarski we know that μf is the unique solution of

$$x : x = f.x \ \wedge \ \forall(y :: f.y \le y \ \Rightarrow \ x \le y) \qquad .$$

$$
\begin{array}{ll}
& \mu f = f{\uparrow^{*}}.\bot \\
= & \qquad \{ \ \mu f \ \text{solves the equation} \ \} \\
& f{\uparrow^{*}}.\bot = f.(f{\uparrow^{*}}.\bot) \ \wedge \ \forall(y :: f.y \le y \ \Rightarrow \ f{\uparrow^{*}}.\bot \le y) \\
= & \qquad \{ \ f{\uparrow^{*}}.x = x \uparrow f.(f{\uparrow^{*}}.x) \ \} \\
& \forall(y :: f.y \le y \ \Rightarrow \ f{\uparrow^{*}}.\bot \le y) \\
= & \qquad \{ \ \bot \le y \ \}
\end{array}
$$

(c):

$$
\begin{array}{ll}
 & f\ddagger .x \le g\ddagger .x \\
\Leftarrow & \qquad \{\ (143)\,[y := g\ddagger .x]\ \ \} \\
 & x \le g\ddagger .x \quad \wedge \quad f.(g\ddagger .x) \le g\ddagger .x \\
= & \qquad \{\ (143)\ \} \\
 & f.(g\ddagger .x) \le g\ddagger .x \\
\Leftarrow & \qquad \{\ (144)\ \} \\
 & f.(g\ddagger .x) \le g.(g\ddagger .x) \\
\Leftarrow & \\
 & f \le g
\end{array}
$$

□

Theorem $\ddagger$ *-decomposition*

For monotonic f and g,

$$(f\uparrow g)\ddagger = f\ddagger\circ(g\circ f\ddagger)\ddagger \tag{151}$$

Proof

Let $r = f\ddagger\circ s$, $s = t\ddagger$, and $t = g\circ f\ddagger$.

Ping:

$$
\begin{array}{ll}
 & (f\uparrow g)\ddagger .x \le r.x \\
\Leftarrow & \qquad \{\ (143)\,[f := f\uparrow g, y := r.x]\ \ \} \\
 & x \le r.x \quad \wedge \quad (f\uparrow g).(r.x) \le r.x \\
= & \qquad \{\ (60)\ \} \\
 & x \le r.x \quad \wedge \quad f.(r.x) \le r.x \quad \wedge \quad g.(r.x) \le r.x \\
= & \qquad \{\ (146)\,[x := r.x]\ \ \} \\
 & x \le r.x \quad \wedge \quad f\ddagger .(r.x) = r.x \quad \wedge \quad g.(r.x) \le r.x \\
= & \qquad \{\ \ r = f\ddagger\circ s;\ \ \text{hence } f\ddagger .(r.x) = r.x\ \ \} \\
 & x \le f\ddagger .(s.x) \quad \wedge \quad g.(f\ddagger .(s.x)) \le f\ddagger .(s.x) \\
\Leftarrow & \qquad \{\ \ y \le f\ddagger .y\,;\ \text{use with }\ y := s.x\ \ \} \\
 & x \le s.x \quad \wedge \quad g.(f\ddagger .(s.x)) \le s.x \\
= & \qquad \{\ \ s = t\ddagger\ \ \text{hence }\ x \le s.x\ \ \}
\end{array}
$$

$$f^0.x \leq f^{\ddagger}.x$$

$=$

$$x \leq f^{\ddagger}.x$$

$\Leftarrow$ $\quad \{ \ (141) \ \}$

$$true$$

$i \geq 0:$

$$f^{i+1}.x \leq f^{\ddagger}.x$$

$\Leftarrow$ $\quad \{ \ (144) \ \}$

$$f^{i+1}.x \leq f.(f^{\ddagger}.x)$$

$\Leftarrow$ $\quad \{ \ f \text{ is monotonic } \}$

$$f^{i}.x \leq f^{\ddagger}.x$$

Theorem $\ddagger$ *is an* $\uparrow$*-closure*

$$\ddagger \text{ is an } \uparrow -\text{closure} \tag{150}$$

Proof
We verify (a) through (c).
(a):

$$f \leq f^{\ddagger}$$

$\Leftarrow$ $\quad \{ \ f \circ f^{\ddagger} \leq f^{\ddagger} \ \}$

$$f \leq f \circ f^{\ddagger}$$

$=$ $\quad \{ \ (144) \ \}$

$$true$$

(b):

$$f^{\ddagger\ddagger}.x = f^{\ddagger}.x$$

$=$ $\quad \{ \ (149)[i := 1, f := f^{\ddagger}] \ \}$

$$f^{\ddagger\ddagger}.x \leq f^{\ddagger}.x$$

$\Leftarrow$ $\quad \{ \ (143)[f := f^{\ddagger}, y := f^{\ddagger}.x] \ \}$

$$x \leq f^{\ddagger}.x \quad \wedge \quad f^{\ddagger}.(f^{\ddagger}.x) \leq f^{\ddagger}.x$$

$=$ $\quad \{ \ (145) \ \}$

$$true$$

Proof

$\Rightarrow$:

Let $f.y \le y$.

$$\begin{array}{ll}
 & x \le y \\
\Rightarrow & \quad \{ \ f.y \le y \, ; (143) \ \} \\
 & f \uparrow\!\ast .x \le y \\
\Rightarrow & \quad \{ \ x \le f \uparrow\!\ast .x \ \} \\
 & x \le y
\end{array}$$

$\Leftarrow$:

$$\begin{array}{ll}
 & \forall(x :: x \le y \ = \ f \uparrow\!\ast .x \le y) \\
\Rightarrow & \quad \{ \ \text{instantiate with } x := y \ \} \\
 & f \uparrow\!\ast .y \le y \\
= & \quad \{ \ (141) \ \} \\
 & f \uparrow\!\ast .y = y \\
\Rightarrow & \quad \{ \ (141) \ \} \\
 & y \le y \ \ \wedge \ \ f.y \le y \\
= & \\
 & f.y \le y
\end{array}$$

□

Theorem

$$\forall(x :: f.x \le x \ = \ f \uparrow\!\ast .x = x) \tag{148}$$

Proof

Immediate from (147) and $f \uparrow\!\ast .x \ge x$.

□

Theorem

$$\forall(x, i : i \ge 0 : f^i.x \le f \uparrow\!\ast .x) \tag{149}$$

Proof

by induction;

$i = 0$:

From the definition of $f \ddagger$ we conclude

$$\forall(x, y :: x \leq y \wedge f.y \leq y \;\Rightarrow\; f \ddagger .x \leq y) \tag{143}$$

and

$$f \circ f \ddagger \leq f \ddagger \quad . \tag{144}$$

Theorem $f \ddagger$ *is an* $\uparrow$*-closure*

$$f \ddagger \text{ is an } \uparrow -\text{closure} \tag{145}$$

Proof
We check the three requirements (a) through (c).
(a): From the definition of $f \ddagger$ we conclude $x \leq f \ddagger .x$.
(b):

$$
\begin{array}{ll}
 & f \ddagger .(f \ddagger .x) = f \ddagger .x \\
= & \qquad \{ \text{ (a)} \, [x := f \ddagger .x] \ \} \\
 & f \ddagger .(f \ddagger .x) \leq f \ddagger .x \\
\Leftarrow & \qquad \{ \ (x \uparrow f.y \leq y \;\Rightarrow\; f \ddagger .x \leq y)[x := f \ddagger .x, y := f \ddagger .x] \ \} \\
 & f \ddagger .x \uparrow f.(f \ddagger .x) \leq f \ddagger .x \\
= & \\
 & f.(f \ddagger .x) \leq f \ddagger .x \\
= & \qquad \{ \ (144) \ \} \\
 & \mathit{true}
\end{array}
$$

(c): From (130) we conclude that $f \ddagger$ is a monotonic function.
□

Theorem

$$\forall(x, y :: y \leq f \ddagger .x \;=\; f \ddagger .y \leq f \ddagger .x) \tag{146}$$

Proof
Immediate from (145) and (140).
□

Theorem *no overshoot*

$$\forall(y :: f.y \leq y \;=\; \forall(x :: x \leq y \;=\; f \ddagger .x \leq y)) \tag{147}$$

$$\begin{array}{ll} \Rightarrow & \{\ (a)\ \} \\ & y \le f.x \end{array}$$

$\Leftarrow$:

(a):

$$\begin{array}{ll} & \forall(x,y :: y \le f.x \ = \ f.y \le f.x) \\ \Rightarrow & \{\ \text{instantiate with } y := x \ \} \\ & \forall(x :: x \le f.x) \end{array}$$

(b):

$$\begin{array}{ll} & \forall(x,y :: y \le f.x \ = \ f.y \le f.x) \\ \Rightarrow & \{\ \text{instantiate with } x,y := f.x,f.x \text{ and } x,y := x,f.x \ \} \\ & \forall(x :: f.x \le f.(f.x)) \ \wedge \ \forall(x :: f.(f.x) \le f.x) \\ = & \\ & \forall(x :: f.x = f.(f.x)) \end{array}$$

(c):

$$\begin{array}{ll} & f.x \le f.y \\ = & \{\ (y \le f.x \ = \ f.y \le f.x)[x := y, y := x] \ \} \\ & x \le f.y \\ \Leftarrow & \{\ (a)\,[x := y] \ \} \\ & x \le y \end{array}$$

□

For monotonic function f on a complete lattice, $f\,\ddagger$ is the lowest $\uparrow$-closure function above f. Stated pointwise, it is a function that, when applied to argument x, is the lowest value y above x and above $f.y$; that is

$$f\,\ddagger.x \ = \ \lfloor y : x \uparrow f.y \le y \rfloor \tag{141}$$

Since f and $\uparrow$ are monotonic, $x \uparrow f.y$ is a monotonic function of y. Hence, according to Knaster-Tarski, $f\,\ddagger.x$ exists and equals $\lfloor y : x \uparrow f.y = y \rfloor$. Similarly, the highest $\downarrow$-closure below f is

$$f\,\ddagger.x \ = \ \lceil y : y \le x \downarrow f.y \rceil \tag{142}$$

$$
\begin{array}{ll}
= & \quad \{ \ (85) \ \} \\
 & \uparrow\{i :: f.V_i \downarrow \uparrow\{j :: g.V_j\}\} \\
= & \quad \{ \ (85) \ \} \\
 & \uparrow\{i :: \uparrow\{j :: f.V_i \downarrow g.V_j\}\} \\
= & \quad \{ \ (47) \ \} \\
 & \uparrow\{i,j :: f.V_i \downarrow g.V_j\} \\
= & \quad \{ \ (137) \ \} \\
 & \uparrow\{i :: f.V_i \downarrow g.V_i\} \\
= & \quad \{ \ (69) \ \} \\
 & \uparrow\{i :: (f \downarrow g).V_i\} \\
= & \\
 & \uparrow((f \uparrow g).V)
\end{array}
$$

□

11 Closures

Function f is called an $\uparrow$-closure if it satisfies the following three conditions.

(a) $\forall(x :: x \leq f.x)$

(b) $\forall(x :: f.x = f.(f.x))$

(c) $\forall(x, y :: x \leq y \ \Rightarrow \ f.x \leq f.y)$

Theorem

$$f \text{ is an } \uparrow\!-\text{closure} \ = \ \forall(x, y :: y \leq f.x \ = \ f.y \leq f.x) \tag{140}$$

Proof

$\Rightarrow$:

$$
\begin{array}{ll}
 & y \leq f.x \\
\Rightarrow & \quad \{ \ (c) \ \} \\
 & f.y \leq f.(f.x) \\
= & \quad \{ \ (b) \ \} \\
 & f.y \leq f.x
\end{array}
$$

$$\uparrow\{x,y::f.x.y\}$$
$=$ { X is a chain }
$$\uparrow\{x,y:x\le y \quad\vee\quad y\le x:f.x.y\}$$
$=$ { (47) }
$$\uparrow\{x,y:x\le y:f.x.y\}\uparrow\uparrow\{x,y:y\le x:f.x.y\}$$
$=$ { (47) }
$$\uparrow\{y::\uparrow\{x:x\le y:f.x.y\}\}\uparrow\uparrow\{x::\uparrow\{y:y\le x:f.x.y\}\}$$
$=$ { f is monotonic }
$$\uparrow\{y::f.y.y\}\uparrow\{x::f.x.x\}$$
$=$
$$\{x::f.x.x\}$$

and

$$\downarrow\{x,y::f.x.y\}$$
$=$ { f is monotonic }
$$f.\downarrow X.\downarrow X$$
$=$ { f is monotonic }
$$\downarrow\{x::f.x.x\}$$

□

Theorem

If f and g are functions of one argument on a universally distributive lattice and they $\uparrow$-distribute over chain V then

$$f\downarrow g \quad \uparrow\text{–distributes over } V \tag{139}$$

Proof

Let V_i be the lowest-but- i element of chain V.

$$(f\downarrow g).\uparrow V$$
$=$ { (69) }
$$(f.\uparrow V)\downarrow(g.\uparrow V)$$
$=$ { f and g $\uparrow$-distribute over V }
$$\uparrow\{i::f.V_i\}\downarrow\uparrow\{j::g.V_j\}$$

$$
\begin{array}{ll}
= & \quad \{ \text{ dual of (129) } \} \\
 & f.(\neg h.y \uparrow l.(x \downarrow y)).x \downarrow f.(h.y).y \leq l.(x \downarrow y) \\
= & \quad \{ \; f \text{ is finitely } \downarrow\text{-distributive } \} \\
 & f.((\neg h.y \uparrow l.(x \downarrow y)) \downarrow h.y).(x \downarrow y) \leq l.(x \downarrow y) \\
= & \quad \{ \text{ (93): complement rule } \} \\
 & f.(l.(x \downarrow y) \downarrow h.y).(x \downarrow y) \leq l.(x \downarrow y) \\
= & \quad \{ \text{ see above: } l.(x \downarrow y) \leq h.y \; \} \\
 & f.(l.(x \downarrow y)).(x \downarrow y) \leq l.(x \downarrow y) \\
= & \quad \{ \text{ (129) } \} \\
 & true
\end{array}
$$

□

As a result hereof, we find

Theorem

Let the lattice be boolean.

$$l \text{ is finitely} \downarrow -\text{distributive if } f \text{ is} \tag{135}$$

$$h \text{ is finitely} \uparrow -\text{distributive if } f \text{ is} \tag{136}$$

Proof

$$
\begin{array}{ll}
 & l.(x \downarrow y) \\
= & \quad \{ \text{ (133) } \} \\
 & h.(x \downarrow y) \downarrow l.y \\
= & \quad \{ \text{ (132) } \} \\
 & h.x \downarrow h.y \downarrow l.y \\
= & \quad \{ \text{ (133) } \} \\
 & l.x \downarrow l.y
\end{array}
$$

□

Theorem

For any function $f.x.y$ that is monotonic in both arguments, and for chain X,

$$\uparrow\{x, y : x \in X \wedge y \in X : f.x.y\} \; = \; \uparrow\{x : x \in X : f.x.x\} \tag{137}$$

$$\downarrow\{x, y : x \in X \wedge y \in X : f.x.y\} \; = \; \downarrow\{x : x \in X : f.x.x\} \tag{138}$$

Proof

$$
\begin{array}{ll}
 & l.\uparrow V \le \uparrow(l.V) \\
\Leftarrow & \quad \{ \ (128) \ \} \\
 & f.\uparrow(l.V).\uparrow V \le \uparrow(l.V) \\
= & \quad \{ \ (129) \ \} \\
 & f.\uparrow(l.V).(\uparrow V) \le \uparrow(f.(l.V).V) \\
= & \quad \{ \ f \ \ \uparrow\text{-distributes over } \ l.V \times V \ \ \} \\
 & \mathit{true}
\end{array}
$$

□

Theorem

$$l.(x \downarrow y) \ = \ l.x \downarrow h.y \qquad \text{if } f \text{ is finitely} \downarrow -\text{distributive} \tag{133}$$

$$h.(x \uparrow y) \ = \ h.x \uparrow l.y \qquad \text{if } f \text{ is finitely} \uparrow -\text{distributive} \tag{134}$$

Proof

Ping:

$$
\begin{array}{ll}
 & l.(x \downarrow y) \le l.x \downarrow h.y \\
\Leftarrow & \quad \{ \ (128) \ \} \\
 & f.(l.x \downarrow h.y).(x \downarrow y) \le l.x \downarrow h.y \\
= & \quad \{ \ f \ \text{ is finitely } \downarrow\text{-distributive} \ \} \\
 & f.(l.x).x \downarrow f.(h.y).y \le l.x \downarrow h.y \\
= & \quad \{ \ (129) \text{ and its dual} \ \} \\
 & \mathit{true}
\end{array}
$$

Pong:

$$
\begin{array}{ll}
 & l.x \downarrow h.y \le l.(x \downarrow y) \\
= & \quad \{ \ (95)\text{: shunting} \ \} \\
 & l.x \le \neg h.y \uparrow l.(x \downarrow y) \\
\Leftarrow & \quad \{ \ (128) \ \} \\
 & f.(\neg h.y \uparrow l.(x \downarrow y)).x \le \neg h.y \uparrow l.(x \downarrow y) \\
= & \quad \{ \ (95)\text{: shunting} \ \} \\
 & f.(\neg h.y \uparrow l.(x \downarrow y)).x \downarrow h.y \le l.(x \downarrow y)
\end{array}
$$

$$h.y = \lceil x : x \le f.x.y \rceil \tag{127}$$

From (126) we have

$$f.x.y \le x \;\Rightarrow\; l.y \le x \tag{128}$$

and

$$f.(l.x).x = l.x \tag{129}$$

Theorem

l and h are monotonic functions (130)

Proof

$$\begin{array}{ll}
 & l.y \le l.z \\
= & \quad \{\ (126),(111)\ \} \\
 & \downarrow\{x : f.x.y \le x : x\} \le \downarrow\{x : f.x.z \le x : x\} \\
\Leftarrow & \quad \{\ (40)\ \} \\
 & \forall(x :: f.x.y \le x \;\Leftarrow\; f.x.z \le x) \\
= & \quad \{\ (6)\ \} \\
 & f.x.y \le f.x.z \\
\Leftarrow & \quad \{\ f \text{ is monotonic in its second argument }\} \\
 & y \le z
\end{array}$$

□

Theorem

l inherits all $\uparrow$−distributivity and $\uparrow$−continuity of f (131)

h inherits all $\downarrow$−distributivity and $\downarrow$−continuity of f (132)

Proof

We need to show that l is $\uparrow$-distributive over set V if f is $\uparrow$-distributive over a set of pairs of the same type as V. Since l is monotonic, the type of $l.V \times V$ is the same as the type of V.

$$\begin{array}{ll}
 & l.\!\uparrow V = \uparrow(l.V) \\
= & \quad \{\ (130) \text{ hence } (43)\ \}
\end{array}$$

$$
\begin{array}{ll}
 & \downarrow\{x : x = g.(f.x) : f.x\} \\
\leq & \qquad \{ \ (42) \text{ since } \ x = f.(g.x) \ \Rightarrow \ f.x = f.(g.(f.x)) \ \ \} \\
 & \downarrow\{x : f.x = f.(g.(f.x)) : f.x\} \\
= & \qquad \{ \ \text{renaming} \ \} \\
 & \downarrow\{y : y = f.(g.y) : y\} \\
= & \qquad \{ \ \text{definitions of } \ \mu \ \text{ and } \ \circ \ \ \} \\
 & \mu(f \circ g)
\end{array}
$$

we have $f.\mu(g \circ f) \ \leq \ \mu(f \circ g)$. We prove $\mu(f \circ g) \leq f.\mu(g \circ f)$ by showing that $f.\mu(g \circ f)$ is a fixpoint of $f \circ g$. The lowest fixpoint $\mu(f \circ g)$, which exists since $f \circ g$ is monotonic, is below any fixpoint.

$$
\begin{array}{ll}
 & (f \circ g).(f.\mu(g \circ f)) \\
= & \qquad \{ \ \text{definition of } \ \circ \ \ \} \\
 & f.(g.(f.\mu(g \circ f))) \\
= & \qquad \{ \ \text{definition of } \ \circ \ \ \} \\
 & f.((g \circ f).\mu(g \circ f)) \\
= & \qquad \{ \ (120) \ \} \\
 & f.\mu(g \circ f)
\end{array}
$$

□

Theorem

Let f be a monotonic function on a complete lattice, and let x, z be such that

$$x \leq f.x \leq f.z \leq z$$

then

$$\exists(y : x \leq y \leq z : f.y = y) \qquad . \tag{125}$$

10 Functions of two variables

Consider function f of two arguments on a complete lattice. We write $f.(x, y)$ when we want to emphasize that the ordering of f's arguments is as given by (49), and we write $f.x.y$ otherwise. One may view the latter as the curried version of the former. In this section, let f be monotonic. Define l and h by

$$l.y = \lfloor x : f.x.y \leq x \rfloor \tag{126}$$

$$
\begin{array}{ll}
\geq & \{\ (43)\ \} \\
 & \uparrow\{x : x \leq f.x : f.x\} \\
\geq & \{\ (41)\text{: } \uparrow \text{ is monotonic }\} \\
 & \uparrow\{x : x \leq f.x : x\} \\
= & \{\ \text{definition of } q\ \} \\
 & q
\end{array}
$$

$$
\begin{array}{ll}
 & f.q \leq q \\
\Leftarrow & \{\ (20)\ \} \\
 & f.q \in \{x : x \leq f.x : x\} \\
= & \\
 & f.q \leq f.(f.q) \\
\Leftarrow & \{\ f \text{ is monotonic }\} \\
 & q \leq f.q
\end{array}
$$

Hence, $f.q = q$. From (39) we conclude $q = \lceil x : x = f.x \rceil = \nu f$.

□

Observe that both $\downarrow\{x : x \leq f.x : x\}$ and $\uparrow\{x : x \geq f.x : x\}$ exist, and hence both μf and νf exist, if the lattice is complete.

The converse to Knaster-Tarski's theorem is due to [4].

Theorem *Davis*

If every monotonic function on a lattice has a fixpoint then the lattice is complete.

The following theorem is part of the folklore. Roland Backhouse dubbed it μ-fusion.

Theorem *μ-fusion*

For monotonic functions f and g on a complete lattice,

$$f.\mu(g \circ f) \ = \ \mu(f \circ g) \tag{124}$$

Proof

From

$$
\begin{array}{ll}
 & f.\mu(g \circ f) \\
= & \{\ \text{definitions of } \mu \text{ and } \circ\ \} \\
 & f.\downarrow\{x : x = g.(f.x) : x\} \\
\leq & \{\ (44) \text{ since } f \text{ is monotonic }\}
\end{array}
$$

□

Since the identity function is both $\downarrow$- and $\uparrow$-distributive over every set, and since $\uparrow V$ and $\downarrow V$ exist for every V in a complete lattice, we have the following result.

Theorem

In a complete lattice, $\lfloor x : f.x \leq x \rfloor$ and $\lceil x : x \leq f.x \rceil$ exist if f is monotonic. (117)

This theorem suggests that we also have a look at equation $x : x = f.x$ and this is what we do next.

9 Fixpoints

Let f be a function on Z. Element x of Z is called a fixpoint of f just when $f.x = x$. The lowest fixpoint of f is denoted by μf. The highest fixpoint of f is denoted by νf.

$$\mu f = \lfloor x : x = f.x \rfloor \tag{118}$$

$$\nu f = \lceil x : x = f.x \rceil \tag{119}$$

From (113) and (114), we have

$$f.\mu f \;=\; \mu f \tag{120}$$

$$f.\nu f \;=\; \nu f \tag{121}$$

If $x \leq f.x$ then x is called a prefixpoint of f. If $f.x \leq x$ then x is called a postfixpoint of f. The following theorem is due to Knaster and Tarski (cf. [12]). It relates extreme prefixpoints, postfixpoints, and fixpoints.

Theorem *Knaster-Tarski*

For monotonic f

if $\downarrow\{x : f.x \leq x : x\}$ exists then μf exists and the two are equal (122)

if $\uparrow\{x : x \leq f.x : x\}$ exists then νf exists and the two are equal (123)

Proof

Let $q = \uparrow\{x : x \leq f.x : x\}$.

$$\begin{array}{ll} & f.q \\ = & \quad \{ \text{ definition of } q \ \} \\ & f.\uparrow\{x : x \leq f.x : x\} \end{array}$$

$$
\begin{array}{ll}
= & \{ \text{ calculation above } \} \\
 & \forall(y :: (\lfloor x : b.x \rfloor \text{ exists and equals } y) \;=\; (b.q \;\;\wedge\;\; y = q)) \\
\Rightarrow & \{ \text{ existential quantification over } y \;\} \\
 & \lfloor x : b.x \rfloor \text{ exists } \;=\; \exists(y :: b.q \;\;\wedge\;\; y = q) \\
= & \\
 & \lfloor x : b.x \rfloor \text{ exists } \;=\; b.q
\end{array}
$$

□

Theorem

$$\lfloor x : b.x \rfloor \;=\; \downarrow\{x : b.x : x\} \tag{111}$$

$$\lceil x : b.x \rceil \;=\; \uparrow\{x : b.x : x\} \tag{112}$$

$$b.\lfloor x : b.x \rfloor \;\wedge\; \forall(y :: b.y \;\Rightarrow\; \lfloor x : b.x \rfloor \leq y) \tag{113}$$

$$b.\lceil x : b.x \rceil \;\wedge\; \forall(y :: b.y \;\Rightarrow\; y \leq \lceil x : b.x \rceil) \tag{114}$$

We now turn to equations of the form

$$x : f.x \leq g.x \qquad .$$

Theorem

$$\lfloor x : f.x \leq g.x \rfloor \text{ exists if } f \text{ is monotonic and } g \text{ is } \downarrow\text{-distributive over } \{x : f.x \leq g.x : x\} \tag{115}$$

$$\lceil x : f.x \leq g.x \rceil \text{ exists if } g \text{ is monotonic and } f \text{ is } \uparrow\text{-distributive over } \{x : f.x \leq g.x : x\} \tag{116}$$

Proof
Because of (110), $\lfloor x : f.x \leq g.x \rfloor$ exists just when $\downarrow\{y : f.y \leq g.y : y\}$ exists and solves $x : f.x \leq g.x$.

$$
\begin{array}{ll}
 & f.\downarrow\{y : f.y \leq g.y : y\} \\
\leq & \{ \; f \text{ is monotonic: (44) } \} \\
 & \downarrow\{y : f.y \leq g.y : f.y\} \\
\leq & \{ \text{ (42) } \} \\
 & \downarrow\{y : f.y \leq g.y : g.y\} \\
= & \{ \; g \text{ is } \downarrow\text{-distributive over } \{x : f.x \leq g.x : x\} \;\} \\
 & g.\downarrow\{y : f.y \leq g.y : y\}
\end{array}
$$

8 Extreme solutions of equations

We write

$$x : b.x \tag{107}$$

for an equation in variable x. The set of solutions of this equation is the set of values x such that $b.x$ holds. Consider also

$$x : b.x \wedge \forall(y : b.y : x \leq y) \tag{108}$$

which is a more restrictive equation, and define q as follows.

$$q = \downarrow\{y : b.y : y\} \tag{109}$$

Assuming that q exists, we calculate

$$\begin{array}{ll}
 & x \text{ solves } (108) \\
= & \\
 & b.x \quad \wedge \quad \forall(y : b.y : x \leq y) \\
= & \qquad \{ \ (21) \ \} \\
 & b.x \quad \wedge \quad x \leq \downarrow\{y : b.y : y\} \\
= & \qquad \{ \ (109) \ \} \\
 & b.x \quad \wedge \quad x \leq q \\
= & \qquad \{ \text{ from } (109) \ \ b.x \Rightarrow q \leq x \ \ \} \\
 & b.x \quad \wedge \quad x = q \\
= & \\
 & b.q \quad \wedge \quad x = q
\end{array}$$

and conclude that (108) has at most one solution, viz. q. If a solution exists, it solves (107) as well and is the lowest solution of (107). We write $\lfloor x : b.x \rfloor$ for the lowest solution, and $\lceil x : b.x \rceil$ for the highest solution.

Theorem

$$\lfloor x : b.x \rfloor \text{ exists} \ = \ b.q \tag{110}$$

Proof

$$\mathit{true}$$

We have

$$
\begin{array}{ccccc}
f \text{ is universally } \uparrow\text{-distributive} & \Rightarrow & f \text{ is universally } \uparrow\text{-continuous} & & \\
\Downarrow & & \Downarrow & & \\
f \text{ is positively } \uparrow\text{-distributive} & \Rightarrow & f \text{ is positively } \uparrow\text{-continuous} & & \\
\Downarrow & & \Downarrow & & \\
f \text{ is finitely } \uparrow\text{-distributive} & \Rightarrow & f \text{ is finitely } \uparrow\text{-continuous} & = & f \text{ is monotonic}
\end{array}
\quad .
$$

Similar definitions can be given for $\downarrow$. Notice that monotonicity does not distinguish between $\uparrow$-continuity and $\downarrow$-continuity. An interesting theorem, due to J.C.S.P. van der Woude, is the following.

Theorem

$$(f \text{ is finitely } \downarrow\text{-distributive} \wedge f \text{ is positively } \uparrow\text{-continuous}) \Rightarrow f \text{ is positively } \downarrow\text{-continuous}$$

A generalization of (13) is the following theorem. Let X, Y, and Z be posets, $f : Y \to Z$, g: $X \to Y$.

Theorem

$$\text{Function } f \circ g \text{ has every distributivity or continuity property shared by } f \text{ and } g \quad . \tag{102}$$

Theorem

If W is a set of functions from Y to Z then

$$\uparrow W \text{ has each type of } \uparrow\text{-distributivity shared by functions in } W \tag{103}$$

$$\downarrow W \text{ has each type of } \downarrow\text{-distributivity shared by functions in } W \tag{104}$$

Proof

Let all functions in V be $\uparrow$-distributive over V.

$$
\begin{array}{ll}
 & (\uparrow W).\uparrow V \\
= & \quad \{\ (66)\ \} \\
 & \uparrow\{f : f \in W : f.\uparrow V\} \\
= & \quad \{\ \text{all functions in } V \text{ are } \uparrow\text{-distributive over } V\ \} \\
 & \uparrow\{f : f \in W : \uparrow\{v : v \in V : f.v\}\} \\
= & \quad \{\ (47)\ \} \\
 & \uparrow\{v : v \in V : \uparrow\{f : f \in W : f.v\}\} \\
= & \quad \{\ (66)\ \} \\
 & \uparrow\{v : v \in V : (\uparrow W).v\}
\end{array}
$$

□

Theorem

$$\text{If } f.x = g.x \downarrow y \text{ then } f \text{ inherits all } \uparrow\text{-distributivity properties of } g \tag{105}$$

$$\text{If } f.x = g.x \uparrow y \text{ then } f \text{ inherits all } \downarrow\text{-distributivity properties of } g \tag{106}$$

$$x \downarrow (u \uparrow \neg x)$$

$=$ { (93): complement rule }

$$x \downarrow u$$

$\leq$ { (62) }

$$u$$

from which we conclude $x \downarrow \uparrow Y \leq \uparrow\{y :: x \downarrow y\}$.

□

Theorem *generalized De Morgan*

In a complete boolean lattice Z

$$\forall(Y : Y \subseteq Z : \neg \downarrow Y = \uparrow\{y : y \in Y : \neg y\}) \quad (100)$$

$$\forall(Y : Y \subseteq Z : \neg \uparrow Y = \downarrow\{y : y \in Y : \neg y\}) \quad (101)$$

7 Distributivity of functions

Function f is said to be $\uparrow$-distributive over V just when $\uparrow(f.V) = f.\uparrow V$. If f is $\uparrow$-distributive over all V then f is called universally $\uparrow$-distributive. If f is $\uparrow$-distributive over all nonempty V then f is called positively $\uparrow$-distributive. If f is $\uparrow$-distributive over all nonempty, finite V then f is called finitely $\uparrow$-distributive. A chain is a set V with the property that all elements can be arranged in a sequence such that each element is below the next element in the sequence. If f is $\uparrow$-distributive over every chain then f is called universally $\uparrow$-continuous. If f is $\uparrow$-distributive over every nonempty chain then f is called positively $\uparrow$-continuous. If f is $\uparrow$-distributive over every nonempty, finite chain then f is called finitely $\uparrow$-continuous. Note that finitely $\uparrow$-continuous is equivalent to monotonic:

f is finitely $\uparrow$-continuous

$=$

f distributes over all chains of length one or two

$=$

$$\forall(x, y : x \leq y : f.x \uparrow f.y = f.(x \uparrow y))$$

$=$ { $x \leq y \ = \ (x \uparrow y = y)$ }

$$\forall(x, y : x \leq y : f.x \uparrow f.y = f.y)$$

$=$ { $f.x \leq f.y \ = \ (f.x \uparrow f.y = f.y)$ }

$$\forall(x, y : x \leq y : f.x \leq f.y)$$

$=$

f is monotonic

Theorem *A complete boolean lattice is universally distributive*

In a complete boolean lattice

$$x \downarrow \uparrow Y = \uparrow\{y : y \in Y : x \downarrow y\} \tag{98}$$

$$x \uparrow \downarrow Y = \downarrow\{y : y \in Y : x \uparrow y\} \tag{99}$$

Proof

We omit range $y \in Y$.

$$\begin{array}{ll} & \uparrow\{y :: x \downarrow y\} \leq x \downarrow \uparrow Y \\ = & \qquad \{ \ (20) \ \} \\ & \forall(y :: x \downarrow y \leq x \downarrow \uparrow Y) \\ \Leftarrow & \qquad \{ \ \text{monotonicity} \ \} \\ & \forall(y :: y \leq \uparrow Y) \\ = & \qquad \{ \ (20) \ \} \\ & \mathit{true} \end{array}$$

Let u be such that $\uparrow\{y :: x \downarrow y\} = u$. Then

$$\begin{array}{ll} & y \\ = & \\ & y \downarrow (x \uparrow \neg x) \\ = & \qquad \{ \ \text{distribution} \ \} \\ & (y \downarrow x) \uparrow (y \downarrow \neg x) \\ \leq & \qquad \{ \ (22) \ \} \\ & u \uparrow (y \downarrow \neg x) \\ \leq & \qquad \{ \ (62) \ \} \\ & u \uparrow \neg x \end{array}$$

and hence

$$\begin{array}{ll} & x \downarrow \uparrow Y \\ \leq & \qquad \{ \ \ y \leq u \uparrow \neg x \, , \, (42) \ \} \\ & x \downarrow \uparrow\{y :: u \uparrow \neg x\} \\ = & \qquad \{ \ \text{check this step; do I need } \ Y \neq \emptyset \ \ ? \ \} \end{array}$$

Proof

$lhs \Rightarrow rhs$:

$$
\begin{aligned}
& x \\
= \quad & \{\ (59)\ \} \\
& x \downarrow \top \\
= \quad & \{\ (88)\ \} \\
& x \downarrow (\neg y \uparrow z \uparrow \neg(\neg y \uparrow z)) \\
= \quad & \{\ (91)\ \} \\
& x \downarrow (\neg y \uparrow z \uparrow (y \downarrow \neg z)) \\
= \quad & \{\ \text{distribution}\ \} \\
& (x \downarrow (\neg y \uparrow z)) \uparrow (x \downarrow y \downarrow \neg z) \\
= \quad & \{\ x \downarrow y \leq z \ \Rightarrow\ x \downarrow y \neg z = \bot\ \} \\
& (x \downarrow (\neg y \uparrow z)) \uparrow \bot \\
= \quad & \{\ (58)\ \} \\
& x \downarrow (\neg y \uparrow z)
\end{aligned}
$$

$lhs \Leftarrow rhs$:

$$
\begin{aligned}
& x \downarrow y \leq z \\
= \quad & \{\ \text{consistency}\ \} \\
& x \downarrow y \downarrow z = x \downarrow y \\
= \quad & \{\ (x \leq \neg y \uparrow z) \ = \ (x = x \downarrow (\neg y \uparrow z))\ \} \\
& x \downarrow y \downarrow z = x \downarrow (\neg y \uparrow z) \downarrow y \\
= \quad & \{\ (93)\ \} \\
& \mathit{true}
\end{aligned}
$$

$\square$

From (95) and (89) we have

Theorem *contrapositive*

$$\forall(x, y :: x \leq y \ = \ \neg y \leq \neg x) \tag{96}$$

Theorem

$$\forall(x, y :: x \leq y \ = \ (x \downarrow \neg y = \bot) \ = \ (\neg x \uparrow y = \top)) \tag{97}$$

$$
\begin{aligned}
& (x \downarrow y) \downarrow (\neg x \uparrow \neg y) \\
= & \qquad \{ \text{distribution} \} \\
& (x \downarrow y \downarrow \neg x) \uparrow (x \downarrow y \downarrow \neg y) \\
= & \qquad \{ \text{definition } \perp \} \\
& (\perp \downarrow y) \uparrow (x \downarrow \perp) \\
= & \qquad \{ (57), (58) \} \\
& \perp
\end{aligned}
$$

$$
\begin{aligned}
& (x \downarrow y) \uparrow \neg x \uparrow \neg y \\
= & \qquad \{ \text{distribution} \} \\
& (x \uparrow \neg x \uparrow \neg y) \downarrow (y \uparrow \neg x \uparrow \neg y) \\
= & \qquad \{ \text{definition } \top \} \\
& (\top \uparrow \neg y) \downarrow (y \uparrow \top) \\
= & \qquad \{ (56), (59) \} \\
& \top
\end{aligned}
$$

□

Theorem *complement rules*

$$x \uparrow (y \downarrow \neg x) \;=\; x \uparrow y \tag{92}$$

$$x \downarrow (y \uparrow \neg x) \;=\; x \downarrow y \tag{93}$$

Theorem

$$\forall (x, y, z :: (\neg x \uparrow y) \downarrow (x \uparrow z) \;=\; (x \downarrow y) \uparrow (\neg x \downarrow z) \tag{94}$$

Proof

$$
\begin{aligned}
& (\neg x \uparrow y) \downarrow (x \uparrow z) \\
= & \qquad \{ \text{ distribution } \} \\
& (\neg x \downarrow x) \uparrow (\neg x \downarrow z) \uparrow (y \downarrow x) \uparrow (y \downarrow z) \\
= & \qquad \{ \; \neg x \downarrow x = \perp \; \} \\
& (\neg x \downarrow z) \uparrow (y \downarrow x) \uparrow (y \downarrow z) \\
= & \qquad \{ \text{ need to eliminate } y \downarrow z \text{; aim for absorption } \} \\
& (\neg x \downarrow z) \uparrow (y \downarrow x) \uparrow ((x \uparrow \neg x) \downarrow y \downarrow z) \\
= & \qquad \{ \text{ distribution } \} \\
& (\neg x \downarrow z) \uparrow (y \downarrow x) \uparrow (x \downarrow y \downarrow z) \uparrow (\neg x \downarrow y \downarrow z) \\
= & \qquad \{ \text{ absorption, twice } \} \\
& (\neg x \downarrow z) \uparrow (y \downarrow x)
\end{aligned}
$$

□

Theorem *shunting*

$$\forall (x, y :: x \downarrow y \leq z \;=\; x \leq \neg y \uparrow z) \tag{95}$$

$$x \uparrow z = y \uparrow z \quad \wedge \quad x \downarrow z = y \downarrow z$$

$\Leftarrow$

$$x = y$$

□

We say that a lattice is *universally distributive* if

$$\forall(x, Y :: x \downarrow \uparrow Y \;=\; \uparrow\{y : y \in Y : x \downarrow y\}) \tag{85}$$

$$\forall(x, Y :: x \uparrow \downarrow Y \;=\; \downarrow\{y : y \in Y : x \uparrow y\}) \tag{86}$$

Not every distributive lattice is universally distributive.

6 Boolean lattices

For a lattice with $\top$ and $\bot$, a complement of element x is any element y such that

$$x \downarrow y = \bot \;\wedge\; x \uparrow y = \top \qquad . \tag{87}$$

A boolean lattice is a distributive lattice with $\top$ and $\bot$ in which every element has a complement. From theorem (84), it follows that complements are unique. We write $\neg x$ for the complement of x.

Theorem

$$x \downarrow \neg x = \bot, \qquad x \uparrow \neg x = \top \tag{88}$$

$$x = \neg\neg x \tag{89}$$

Proof

(88) is immediate from the definition of $\neg$. From theorem (84) it follows that complements are unique and by the symmetry of the definition of $\neg$ it follows that x is the complement of $\neg x$, hence $x = \neg\neg x$.

□

Theorem *De Morgan*

$$\neg(x \downarrow y) = \neg x \uparrow \neg y \tag{90}$$

$$\neg(x \uparrow y) = \neg x \downarrow \neg y \tag{91}$$

Proof

We verify (90) by checking $(x \downarrow y) \downarrow (\neg x \uparrow \neg y) = \bot$ and $(x \downarrow y) \uparrow \neg x \uparrow \neg y = \top$.

$$
\begin{array}{ll}
= & \{\ x \geq z\ \} \\
& (x \uparrow y) \downarrow (y \uparrow z) \downarrow x = (x \downarrow y) \uparrow (y \downarrow z) \uparrow z \\
= & \{\ (53)\text{: absorption, } (51)\text{: symmetry}\ \} \\
& x \downarrow (y \uparrow z) = (x \downarrow y) \uparrow z \quad .
\end{array}
$$

Next, we derive

$$
\begin{array}{ll}
& \mathit{true} \\
\Rightarrow & \{\ (\mathrm{e})\ \} \\
& x \downarrow (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x) = x \downarrow ((x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x)) \\
\Rightarrow & \{\ x \geq (x \downarrow y) \uparrow (z \downarrow x) \text{ and use previous result}\ \} \\
& x \downarrow (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x) = (x \downarrow y \downarrow z) \uparrow (x \downarrow y) \uparrow (z \downarrow x) \\
= & \{\ (53)\text{: absorption, } (51)\text{: symmetry}\ \} \\
& x \downarrow (y \uparrow z) = (x \downarrow y) \uparrow (z \downarrow x)
\end{array}
$$

□

Conditions (79) and (80) with their inequalities replaced by equalities are strictly weaker than the above four conditions. A lattice in which a distribution property holds (and, hence, also the other four) is called a *distributive lattice.*

Theorem

In a distributive lattice

$$\forall(x, y, z :: (x \uparrow z = y \uparrow z \ \wedge\ x \downarrow z = y \downarrow z) = (x = y)) \tag{84}$$

Proof

$$
\begin{array}{ll}
& x = y \\
= & \{\ (53)\text{: absorption}\ \} \\
& x \uparrow (x \downarrow z) = y \uparrow (y \downarrow z) \\
\Leftarrow & \\
& x \uparrow (y \downarrow z) = y \uparrow (x \downarrow z) \ \wedge\ x \downarrow z = y \downarrow z \\
= & \{\ \text{distribution}\ \} \\
& (x \uparrow y) \downarrow (x \uparrow z) = (y \uparrow x) \downarrow (y \uparrow z) \ \wedge\ x \downarrow z = y \downarrow z \\
\Leftarrow & \\
& x \uparrow y = y \uparrow x \ \wedge\ x \uparrow z = y \uparrow z \ \wedge\ x \downarrow z = y \downarrow z \\
= & \{\ (51)\text{: symmetry}\ \}
\end{array}
$$

(d) $\Rightarrow$ (e):

$$
\begin{array}{ll}
& (x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x) \\
\geq & \quad \{ \text{ (d) } \} \\
& ((x \downarrow y) \uparrow (y \downarrow z) \uparrow z) \downarrow x \\
= & \quad \{ \text{ (53): absorption } \} \\
& ((x \downarrow y) \uparrow z) \downarrow x \\
\geq & \quad \{ \text{ (d) } \} \\
& (x \downarrow (y \uparrow z)) \downarrow x \\
= & \quad \{ \text{ (50): idempotence } \} \\
& x \downarrow (y \uparrow z)
\end{array}
$$

and hence

$$
\begin{array}{ll}
& (x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x) \\
\geq & \quad \{ \text{ above step, (20) } \} \\
& (x \downarrow (y \uparrow z)) \uparrow (y \downarrow (z \uparrow x)) \uparrow (z \downarrow (x \uparrow y)) \\
\geq & \quad \{ \text{ (d) } \} \\
& ((x \downarrow (y \uparrow z)) \uparrow (y \downarrow (z \uparrow x)) \uparrow z) \downarrow (x \uparrow y) \\
= & \quad \{ \text{ (50): idempotence, (51): symmetry } \} \\
& (z \uparrow (x \downarrow (y \uparrow z)) \uparrow z \uparrow (y \downarrow (z \uparrow x))) \downarrow (x \uparrow y) \\
\geq & \quad \{ \text{ (d), monotonicity } \} \\
& ((z \uparrow x) \downarrow (y \uparrow z)) \uparrow ((z \uparrow y) \downarrow (z \uparrow x)) \downarrow (x \uparrow y) \\
= & \quad \{ \text{ (51): symmetry, (50): idempotence } \} \\
& (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x) \\
\geq & \quad \{ \text{ (78) } \} \\
& (x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x)
\end{array}
$$

(e) $\Rightarrow$ (a):
First we show $x \geq z \;\Rightarrow\; (x \downarrow y) \uparrow z = x \downarrow (y \uparrow z)$. Assuming z, we have

$$
\begin{array}{ll}
& \mathit{true} \\
= & \quad \{ \text{ (e) } \} \\
& (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x) = (x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x)
\end{array}
$$

$$
\begin{array}{ll}
& ((x \uparrow y) \downarrow x) \uparrow ((x \uparrow y) \downarrow z) \\
= & \quad \{ \text{ (53): absorption, (51): symmetry } \} \\
& x \uparrow (z \downarrow (x \uparrow y)) \\
= & \quad \{ \text{ (a) } [x, y, z := z, x, y], \text{ associativity } \} \\
& x \uparrow (z \downarrow x) \uparrow (z \downarrow y) \\
= & \quad \{ \text{ (53): absorption, (51): symmetry } \} \\
& x \uparrow (y \downarrow z)
\end{array}
$$

(b) $\Rightarrow$ (c):

$$
\begin{array}{ll}
& x \downarrow y \leq z \quad \wedge \quad x \leq y \uparrow z \\
= & \quad \{ \text{ (54):consistency } \} \\
& (x \downarrow y) \uparrow z = z \quad \wedge \quad x \uparrow y \uparrow z = y \uparrow z \\
= & \quad \{ \text{ (b) } \} \\
& (x \uparrow z) \downarrow (y \uparrow z) = z \quad \wedge \quad x \uparrow y \uparrow z = y \uparrow z \\
= & \\
& (x \uparrow z) \downarrow (x \uparrow y \uparrow z) = z \quad \wedge \quad x \uparrow y \uparrow z = y \uparrow z \\
= & \quad \{ \text{ (53):absorption } \} \\
& x \uparrow z = z \quad \wedge \quad x \uparrow y \uparrow z = y \uparrow z \\
= & \\
& x \uparrow z = z \quad \wedge \quad y \uparrow z = y \uparrow z \\
= & \quad \{ \text{ (54):consistency } \} \\
& x \leq z
\end{array}
$$

(c) $\Rightarrow$ (d):

$$
\begin{array}{ll}
& (x \uparrow y) \downarrow z \leq x \uparrow (y \downarrow z) \\
= & \quad \{ \text{ (c) } [x, z := (x \uparrow y) \downarrow z, (x \downarrow y) \uparrow z] \ \} \\
& (x \uparrow y) \downarrow z \downarrow y \leq x \uparrow (y \downarrow z) \quad \wedge \quad (x \uparrow y) \downarrow z \leq y \uparrow x \uparrow (y \downarrow z) \\
= & \quad \{ \text{ (53):absorption } \} \\
& z \downarrow y \leq x \uparrow (y \downarrow z) \quad \wedge \quad (x \uparrow y) \downarrow z \leq y \uparrow x \\
= & \\
& \mathit{true}
\end{array}
$$

□

Theorem

$$\forall(x, y, z :: x \geq z \ = \ x \downarrow(y \uparrow z) \geq (x \downarrow y) \uparrow z) \tag{81}$$

$$\forall(x, y, z :: x \leq z \ = \ x \uparrow(y \downarrow z) \leq (x \uparrow y) \downarrow z) \tag{82}$$

Proof

$$\begin{array}{ll} & x \uparrow(y \downarrow z) \leq (x \uparrow y) \downarrow z \\ = & \quad \{ \ (61) \ \} \\ & x \uparrow(y \downarrow z) \leq x \uparrow y \quad \wedge \quad x \uparrow(y \downarrow z) \leq z \\ = & \quad \{ \ (60) \ \} \\ & x \leq x \uparrow y \quad \wedge \quad y \downarrow z \leq x \uparrow y \quad \wedge \quad x \leq z \quad \wedge \quad y \downarrow z \leq z \\ = & \quad \{ \ (62) \ \} \\ & x \leq z \end{array}$$

□

We do not necessarily have that $\uparrow$ distributes through $\downarrow$ or the other way round, but the two operators are equally distributive.

Theorem

Properties (83)

(a) $\forall(x, y, z :: x \downarrow(y \uparrow z) = (x \downarrow y) \uparrow(x \downarrow z))$

(b) $\forall(x, y, z :: x \uparrow(y \downarrow z) = (x \uparrow y) \downarrow(x \uparrow z))$

(c) $\forall(x, y, z :: (x \downarrow y \leq z \quad \wedge \quad x \leq y \uparrow z) \ = \ x \leq z)$

(d) $\forall(x, y, z :: (x \uparrow y) \downarrow z \leq x \uparrow(y \downarrow z))$

(e) $\forall(x, y, z :: (x \uparrow y) \downarrow(y \uparrow z) \downarrow(z \uparrow x) = (x \downarrow y) \uparrow(y \downarrow z) \uparrow(z \downarrow x))$

are equivalent.

Proof

(a) $\Rightarrow$ (b):

$$\begin{array}{ll} & (x \uparrow y) \downarrow(x \uparrow z) \\ = & \quad \{ \ (a)\,[x, y, z := x \uparrow y, x, z] \ \} \end{array}$$

$$
\begin{array}{ll}
 & x \downarrow (y \uparrow z) \geq (x \downarrow y) \uparrow (x \downarrow z) \\
= & \quad \{ \ (60) \ \} \\
 & x \downarrow (y \uparrow z) \geq x \downarrow y \quad \wedge \quad x \downarrow (y \uparrow z) \geq x \downarrow z \\
\Leftarrow & \quad \{ \ \downarrow \text{ is monotonic } \} \\
 & y \uparrow z \geq y \quad \wedge \quad y \uparrow z \geq z \\
= & \quad \{ \ (62) \ \} \\
 & \mathit{true}
\end{array}
$$

□

Theorem

$$\forall (x, y, z :: (x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x) \leq (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x)) \tag{78}$$

Proof

We show $x \downarrow y \leq \mathit{rhs}$ and then the result follows by (61) and symmetry.

$$
\begin{array}{ll}
 & x \downarrow y \leq (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x) \\
\Leftarrow & \quad \{ \ (76) \ \} \\
 & x \downarrow y \leq (x \uparrow (y \downarrow z)) \downarrow (y \uparrow z) \\
= & \quad \{ \ (61) \ \} \\
 & x \downarrow y \leq x \uparrow (y \downarrow z) \quad \wedge \quad x \downarrow y \leq y \uparrow z \\
= & \quad \{ \ (62) \ \} \\
 & \mathit{true}
\end{array}
$$

□

Theorem

$$\forall (x, y, z :: (x \downarrow y) \uparrow (x \downarrow z) \leq x \downarrow (y \uparrow (x \downarrow z))) \tag{79}$$

$$\forall (x, y, z :: (x \uparrow y) \downarrow (x \uparrow z) \geq x \uparrow (y \downarrow (x \uparrow z))) \tag{80}$$

Proof

$$
\begin{array}{ll}
 & (x \downarrow y) \uparrow (x \downarrow z) \\
= & \quad \{ \ (50)\text{: idempotence of } \downarrow \ \} \\
 & (x \downarrow y) \uparrow (x \downarrow x \downarrow z) \\
\leq & \quad \{ \ (77)[z := x \downarrow z] \ \} \\
 & x \downarrow (y \uparrow (x \downarrow z))
\end{array}
$$

□

Theorem

$$\uparrow(X \times Y) = (\uparrow X, \uparrow Y) \tag{74}$$

$$\downarrow(X \times Y) = (\downarrow X, \downarrow Y) \tag{75}$$

Proof

$$\begin{array}{ll}
 & \uparrow(X \times Y) \leq (a, b) \\
= & \qquad \{\ (20)\ \} \\
 & \forall(x, y : x \in X \wedge y \in Y : (x, y) \leq (a, b)) \\
= & \qquad \{\ (49)\ \} \\
 & \forall(x, y : x \in X \wedge y \in Y : x \leq a \wedge y \leq b) \\
= & \\
 & \forall(x : x \in X : x \leq a) \quad \wedge \quad \forall(y : y \in Y : y \leq b) \\
= & \qquad \{\ (20)\ \} \\
 & \uparrow X \leq a \quad \wedge \quad \uparrow Y \leq b \\
= & \qquad \{\ (49)\ \} \\
 & (\uparrow X, \uparrow Y) \leq (a, b)
\end{array}$$

□

(*** Lifting is insufficiently explored in what follows and, consequently, we have more dummies than needed ***)

5 Distributivity

In any lattice, we have

Theorem

$$\forall(x, y, z :: x \uparrow (y \downarrow z) \leq (x \uparrow y) \downarrow (x \uparrow z)) \tag{76}$$

$$\forall(x, y, z :: x \downarrow (y \uparrow z) \geq (x \downarrow y) \uparrow (x \downarrow z)) \tag{77}$$

Proof

□

A special case that we will need is the following.

Theorem

For all $y \in Y$, we have

$$(f \uparrow g).y \;=\; f.y \uparrow g.y \tag{68}$$

$$(f \downarrow g).y \;=\; f.y \downarrow g.y \tag{69}$$

Notice that the above properties can also be written in so-called point-free notation.

Theorem

If W is a set of functions from Y to Z and $g : X \to Y$ then

$$(\uparrow W) \circ g = \uparrow\{f : f \in W : f \circ g\} \tag{70}$$

$$(\downarrow W) \circ g = \downarrow\{f : f \in W : f \circ g\} \tag{71}$$

Theorem

If W is a set of functions $Y \to Z$ that are $\uparrow$-distributive over V then

$$\uparrow W \text{ is } \uparrow-\text{distributive over } V \quad . \tag{72}$$

If W is a set of functions $Y \to Z$ that are $\downarrow$-distributive over V then

$$\downarrow W \text{ is } \downarrow-\text{distributive over } V \quad . \tag{73}$$

Proof

$$
\begin{array}{ll}
 & (\downarrow W).\downarrow V \\
= & \quad \{\ (67)\ \} \\
 & \downarrow\{f : f \in W : f.\downarrow V\} \\
= & \quad \{\ f \text{ is } \downarrow\text{-distributive over } V\ \} \\
 & \downarrow\{f : f \in W : \downarrow\{y : y \in V : f.y\}\} \\
= & \quad \{\ (48)\ \} \\
 & \downarrow\{y : y \in V : \downarrow\{f : f \in W : f.y\}\} \\
= & \quad \{\ (67)\ \} \\
 & \downarrow\{y : y \in V : (\downarrow W).y\} \\
= & \quad \{\ (12)\ \} \\
 & \downarrow((\downarrow W).V)
\end{array}
$$

$$
\begin{array}{ll}
 & x \downarrow y \leq x \downarrow z \\
= & \quad \{ \text{ (54): consistency } \} \\
 & x \downarrow y \; = \; x \downarrow y \downarrow x \downarrow z \\
= & \quad \{ \text{ (51): symmetry, (50): idempotence } \} \\
 & x \downarrow y \; = \; x \downarrow y \downarrow z \\
\Leftarrow & \quad \{ \text{ Leibniz } \} \\
 & y \; = \; y \downarrow z \\
= & \quad \{ \text{ (54): consistency } \} \\
 & y \leq z
\end{array}
$$

$\square$

Theorem

If Z is a complete lattice,

the set of functions $Y \rightarrow Z$ forms a complete lattice; (64)

the set of monotonic functions $Y \rightarrow Z$ forms a complete lattice. (65)

The lifting of $\leq$ to functions induces operators $\uparrow$ and $\downarrow$ on functions also.

Theorem

If W is a set of functions from Y to Z then

$$(\uparrow W).y = \uparrow\{f : f \in W : f.y\} \tag{66}$$

$$(\downarrow W).y = \downarrow\{f : f \in W : f.y\} \tag{67}$$

Proof

$$
\begin{array}{ll}
 & \uparrow W \leq g \\
= & \quad \{ \text{ (18) } \} \\
 & \forall(f : f \in W : f \leq g) \\
= & \quad \{ \text{ (15) } \} \\
 & \forall(f, y : f \in W \quad \wedge \quad y \in Y : f.y \leq g.y) \\
= & \quad \{ \text{ (18) } \} \\
 & \forall(y : y \in Y : \uparrow\{f : f \in W : f.y\} \leq g.y) \\
= & \quad \{ \text{ (15) } \} \\
 & \lambda(y : y \in Y : \uparrow\{f : f \in W : f.y\}) \leq g
\end{array}
$$

is equivalent to the conjunction of (51) through (53).

Theorem

$$\forall(x, y, x', y' :: x \leq y \;\;\wedge\;\; x' \leq y' \;\Rightarrow\; x \downarrow x' \leq y \downarrow y' \;\;\wedge\;\; x \uparrow x' \leq y \uparrow y') \tag{55}$$

Proof

$$\begin{array}{ll} & x \leq y \quad \wedge \quad x' \leq y' \\ = & \qquad \{ \text{ consistentcy } \} \\ & x \downarrow y = x \quad \wedge \quad x' \downarrow y' = x' \\ \Rightarrow & \\ & x \downarrow y \downarrow x' \downarrow y' = x \downarrow x' \\ = & \qquad \{ \;\downarrow \text{ is symmetric, associative; consistency } \} \\ & x \downarrow x' \leq y \downarrow y' \end{array}$$

□

Here are a few more properties for a lattice in which $\bot$ and $\top$ are defined.

$$x \uparrow \top = \top \tag{56}$$

$$x \downarrow \bot = \bot \tag{57}$$

$$x \uparrow \bot = x \tag{58}$$

$$x \downarrow \top = x \tag{59}$$

From (20) and (21) we obtain

$$\forall(x, y, z :: x \geq y \uparrow z \;=\; (x \geq y \;\;\wedge\;\; x \geq z)) \tag{60}$$

$$\forall(x, y, z :: x \leq y \downarrow z \;=\; (x \leq y \;\;\wedge\;\; x \leq z)) \tag{61}$$

From (22) and (23) we obtain

$$\forall(x, y :: x \downarrow y \leq x \leq x \uparrow y) \tag{62}$$

Theorem

Both $\uparrow$ and $\downarrow$ are monotonic. (63)

Proof

□

We started our development with $\leq$ and derived $\uparrow$ and $\downarrow$. We could also have proceeded the other way round. If $\uparrow$ and $\downarrow$ are arbitrary infix operators that satisfy (50) through (53), we first show $(x = x \uparrow y) \;=\; (x \downarrow y = y)$

$$
\begin{array}{ll}
 & x = x \uparrow y \\
= & \qquad \{\ (53)\text{: absorption }\ \} \\
 & x \uparrow (x \downarrow y) = x \uparrow y \\
\Leftarrow & \\
 & x \downarrow y = y \\
= & \qquad \{\ (51)\text{: symmetry, } (53)\text{: absorption }\ \} \\
 & y \downarrow x = y \downarrow (x \uparrow y) \\
\Leftarrow & \\
 & x = x \uparrow y \qquad ,
\end{array}
$$

and then define $\leq$ by either half of this equality, show that $\leq$ is a partial order, and finally show that $x \uparrow y$ and $x \downarrow y$ are the lowest upper bound and highest lower bound of $\{x, y\}$.

Theorem

Absorption implies idempotence.

Proof

$$
\begin{array}{ll}
 & x \downarrow x \\
= & \qquad \{\ (53)\text{: } (x = x \uparrow (x \downarrow y))\ \ \} \\
 & x \downarrow (x \uparrow (x \downarrow y)) \\
= & \qquad \{\ (53)\text{: } (x = x \downarrow (x \uparrow y))[y := x \downarrow x]\ \ \} \\
 & x
\end{array}
$$

□

As a result, a lattice is characterized by the three conditions (51) through (53). A characterization of lattices with only two axioms is due to [8]. The existence of a one-axiom system is shown in [10].

Theorem *Kalman*

The conjunction of conditions

$$\forall(a, b :: a \;=\; (b \downarrow a) \uparrow a)$$
$$\forall(a, b, c, d, e, f :: (((a \downarrow b) \downarrow c) \uparrow d) \uparrow e \;=\; (((b \downarrow c) \downarrow a) \uparrow e) \uparrow ((f \uparrow d) \downarrow d))$$

$$
\begin{array}{ll}
 & h = x \uparrow y \\
= & \quad \{ \text{ definition of } \uparrow \ \} \\
 & \forall (z :: h \leq z \ = \ \forall (u : u \in \{x, y\} : u \leq z))
\end{array}
$$

and the result follows from the fact that the latter is symmetric in x and y.
Associativity:
For all h, we have

$$
\begin{array}{ll}
 & (x \uparrow y) \uparrow z \leq h \\
= & \quad \{ \ (18) \ \} \\
 & x \uparrow y \leq h \quad \wedge \quad z \leq h \\
= & \quad \{ \ (18) \ \} \\
 & x \leq h \quad \wedge \quad y \leq h \quad \wedge \quad z \leq h
\end{array}
$$

and the result follows from the fact that the latter is symmetric in x, y, and z.
Absorption:

$$
\begin{array}{ll}
 & x \downarrow (x \uparrow y) = x \\
= & \quad \{ \ (54)\text{: consistency } \} \\
 & x \leq x \uparrow y \\
= & \quad \{ \ (22) \ \} \\
 & \mathit{true}
\end{array}
$$

Consistency:

$$
\begin{array}{ll}
 & x = x \downarrow y \\
= & \quad \{ \text{ definition of } \downarrow \ \} \\
 & \forall (z :: z \leq x \ = \ \forall (u : u \in \{x, y\} : z \leq u)) \\
= & \\
 & \forall (z :: z \leq x \ = \ z \leq x \quad \wedge \quad z \leq y) \\
= & \quad \{ \text{ predicate calculus } \} \\
 & \forall (z :: z \leq x \ \Rightarrow \ z \leq y) \\
= & \quad \{ \ (7) \ \} \\
 & x \leq y
\end{array}
$$

If Y and Z are lattices, then their Cartesian product $Y \times Z$ consisting of pairs (y, z) ordered by

$$(y, z) \leq (y', z') \ = \ y \leq y' \wedge z \leq z' \tag{49}$$

is a lattice. If Y and Z are complete, $Y \times Z$ is complete.

4 Lattice algebra

For sets of two elements, we introduce an infix operator for $\uparrow$, also written as $\uparrow$.

$$x \uparrow y = \uparrow\{x, y\}$$

Similarly for $\downarrow$. Both $\uparrow$ and $\downarrow$ have a binding power higher than $\leq$ and $\geq$ but lower than $.$ and $\circ$. They have the following five properties.

$$\forall(x :: x \uparrow x = x \ \ \wedge \ \ x \downarrow x = x) \tag{50}$$

$$\forall(x, y :: x \uparrow y = y \uparrow x \ \ \wedge \ \ x \downarrow y = y \downarrow x) \tag{51}$$

$$\forall(x, y, z :: (x \uparrow y) \uparrow z = x \uparrow(y \uparrow z) \ \ \wedge \ \ (x \downarrow y) \downarrow z = x \downarrow(y \downarrow z)) \tag{52}$$

$$\forall(x, y :: x \uparrow(x \downarrow y) = x = x \downarrow(x \uparrow y)) \tag{53}$$

$$\forall(x, y :: (x = x \downarrow y) \ = \ (x \leq y) \ = \ (x \uparrow y = y)) \tag{54}$$

known as *idempotence*, *symmetry*, *associativity*, *absorption*, and *consistency* respectively.
Proof
Idempotence:

$$
\begin{array}{ll}
 & x \uparrow x = x \\
= & \quad \{ \text{ definition of } \uparrow \ \} \\
 & \forall(z :: x \leq z \ = \ \forall(y : y \in \{x, x\} : y \leq z)) \\
= & \\
 & \forall(z :: x \leq z \ = \ x \leq z) \\
= & \\
 & \mathit{true}
\end{array}
$$

Symmetry:

$$
\begin{array}{ll}
& f.\downarrow X = \downarrow(f.X) \\
= & \quad \{ \ (23)\,[x := f.\downarrow X, Y := (f.X)] \ \} \\
& \forall(y : y \in f.X : y \geq f.\downarrow X) \ \wedge \ \forall(z : \forall(y : y \in f.X : y \geq z) \ \Rightarrow \ f.\downarrow X \geq z) \\
= & \quad \{ \ \text{predicate calculus} \ \} \\
& \forall(x : x \in X : f.x \geq f.\downarrow X) \ \wedge \ \forall(z : \forall(x : x \in X : f.x \geq z) \ \Rightarrow \ f.\downarrow X \geq z) \\
\Leftarrow & \quad \{ \ f \ \text{is monotonic} \ \} \\
& \forall(x : x \in X : x \geq \downarrow X) \ \wedge \ \forall(z : \forall(x : x \in X : f.x \geq z) \ \Rightarrow \ f.\downarrow X \geq z) \\
= & \quad \{ \ (23)\text{:} \ x \geq \downarrow X \ \} \\
& \forall(z : \forall(x : x \in X : f.x \geq z) \ \Rightarrow \ f.\downarrow X \geq z) \\
= & \quad \{ \ \downarrow X \in X \ \} \\
& \mathit{true}
\end{array}
$$

□

Theorem

If Z is a lattice, then

$$\uparrow\{Y : Y \in V : \uparrow Y\} \ = \ \uparrow\cup(Y : Y \in V : Y) \tag{47}$$

$$\downarrow\{Y : Y \in V : \downarrow Y\} \ = \ \downarrow\cup(Y : Y \in V : Y) \tag{48}$$

for every finite, nonempty set V of subsets of Z. If Z is complete, it holds for all V.

Proof

For all z

$$
\begin{array}{ll}
& \uparrow\{Y : Y \in V : \uparrow Y\} \leq z \\
= & \quad \{ \ (18) \ \} \\
& \forall(Y : Y \in V : \uparrow Y \leq z) \\
= & \quad \{ \ (18) \ \} \\
& \forall(Y : Y \in V : \forall(y : y \in Y : y \leq z)) \\
= & \quad \{ \ (18) \ \} \\
& \uparrow\{y, Y : y \in Y \ \wedge \ Y \in V : y\} \leq z \\
= & \\
& \uparrow\cup(Y : Y \in V : Y) \leq z
\end{array}
$$

□

$$
\begin{array}{ll}
 & \downarrow(f.Y) \le \downarrow(g.Y) \\
= & \quad \{ \ (7) \ \} \\
 & \forall(z :: \downarrow(f.Y) \le z \Leftarrow \downarrow(g.Y) \le z) \\
= & \quad \{ \ (20) \ \} \\
 & \forall(z :: \forall(y : y \in Y : f.y \le z) \Leftarrow \forall(y : y \in Y : g.y \le z)) \\
\Leftarrow & \quad \{ \text{ monotonicity of } \forall \ \} \\
 & \forall(z :: \forall(y : y \in Y : f.y \le z \ \Leftarrow \ g.y \le z)) \\
= & \quad \{ \text{ swap quantifiers } \} \\
 & \forall(y : y \in Y : \forall(z :: f.y \le z \ \Leftarrow \ g.y \le z)) \\
= & \quad \{ \ (7) \ \} \\
 & \forall(y : y \in Y : f.y \le g.y)
\end{array}
$$

□

Theorem

For monotonic f

$$\uparrow(f.X) \le f.\uparrow X \tag{43}$$

$$f.\downarrow X \le \downarrow(f.X) \tag{44}$$

Proof

$$
\begin{array}{ll}
 & f.\downarrow X \le \downarrow(f.X) \\
= & \quad \{ \ (21)\,[x := f.\downarrow X,\, Y := (f.X)]\,;\ \text{predicate calculus } \} \\
 & \forall(x : x \in X : f.\downarrow X \le f.x) \\
\Leftarrow & \quad \{ \ f \text{ is monotonic } \} \\
 & \forall(x : x \in X : \downarrow X \le x) \\
= & \quad \{ \ (23) \ \} \\
 & \mathit{true}
\end{array}
$$

□

Theorem

For monotonic f

$$\uparrow X \in X \ \Rightarrow\ \uparrow(f.X) = f.\uparrow X \tag{45}$$

$$\downarrow X \in X \ \Rightarrow\ f.\downarrow X = \downarrow(f.X) \tag{46}$$

Proof

$$\uparrow\{x\} \le y$$
$=$ { (18) }
$$\forall(z : z \in \{x\} : z \le y)$$
$=$
$$x \le y$$

□

Theorem

$$\forall(X, y : X \neq \emptyset : y \uparrow \uparrow X \;=\; \uparrow\{x : x \in X : y \uparrow x\}) \tag{35}$$

$$\forall(X, y : X \neq \emptyset : y \downarrow \downarrow X \;=\; \downarrow\{x : x \in X : y \downarrow x\}) \tag{36}$$

Theorem

$$\forall(X :: \uparrow\{x : x \in X : \bot\} \;=\; \bot \tag{37}$$

$$\forall(X :: \downarrow\{x : x \in X : \top\} \;=\; \top \tag{38}$$

Theorem *the extreme bounds are monotonic*

$$X \subseteq Y \;\Rightarrow\; \uparrow X \le \uparrow Y \tag{39}$$

$$X \subseteq Y \;\Rightarrow\; \downarrow X \ge \downarrow Y \tag{40}$$

Proof

$$\downarrow X \ge \downarrow Y$$
$=$ { (7) }
$$\forall(z :: z \le \downarrow X \;\Leftarrow\; z \le \downarrow Y)$$
$=$ { (21) }
$$\forall(z :: \forall(x : x \in X : z \le x\} \;\Leftarrow\; \forall(y :: y \in Y : z \le y\})$$
$\Leftarrow$ { predicate calculus }
$$X \subseteq Y$$

□

Theorem *the extreme bounds are monotonic*

$$\forall(y : y \in Y : f.y \le g.y) \;\Rightarrow\; \uparrow(f.Y) \le \uparrow(g.Y) \tag{41}$$

$$\forall(y : y \in Y : f.y \le g.y) \;\Rightarrow\; \downarrow(f.Y) \le \downarrow(g.Y) \tag{42}$$

Proof

□

Theorem

$$\forall(x :: \downarrow\{y : x \le y : y\} \;=\; x \;=\; \uparrow\{y : y \le x : y\}) \tag{28}$$

It is not necessarily the case that $\uparrow Y$ or $\downarrow Y$ is defined for every set Y : it may be that no x satisfies (18) or (19). A poset is called a *lattice* if both $\uparrow Y$ and $\downarrow Y$ are defined for every finite, nonempty set Y. Of course, this is identical to saying that poset Z is a lattice just when $\uparrow\{x, y\}$ and $\downarrow\{x, y\}$ are defined for all $x, y \in Z$. A poset is called a *complete lattice* if both $\uparrow Y$ and $\downarrow Y$ are defined for every set Y.

Two elements of Z have names, provided they exist: top $\top$ and bottom $\perp$. They are defined as

$$\top = \uparrow Z \tag{29}$$

$$\perp = \downarrow Z \tag{30}$$

Theorem

$$\perp = \uparrow \emptyset \tag{31}$$

$$\top = \downarrow \emptyset \tag{32}$$

Proof

$$\downarrow \emptyset = \uparrow Z$$

$$= \qquad \{ \;\; (19)[Y := \emptyset, x := \uparrow Z] \;\; \}$$

$$\forall(z : z \in Z : z \le \uparrow Z \;=\; \forall(y : y \in \emptyset : z \le y))$$

$$= \qquad \{ \;\; \forall(y : \mathit{false} : p) \;\; \}$$

$$\forall(z : z \in Z : z \le \uparrow Z)$$

$$= \qquad \{ \;\; (22)[Y := Z] \;\; \}$$

$$\mathit{true}$$

□

Theorem

$$\uparrow\{x\} \;=\; x \tag{33}$$

$$\uparrow\{x\} \;=\; x \tag{34}$$

Proof

For all y

□

The first conjunct in (22) expresses that x is an upper bound. The second conjunct expresses that it is the lowest upper bound.

Theorem

$$\forall(x :: x \in Y \;\wedge\; \forall(y : y \in Y : y \leq x) \;\Rightarrow\; x = \uparrow Y) \tag{24}$$

$$\forall(x :: x \in Y \;\wedge\; \forall(y : y \in Y : y \geq x) \;\Rightarrow\; x = \downarrow Y) \tag{25}$$

Proof

$$\begin{array}{ll}
 & x = \uparrow Y \\
= & \quad \{\ (18)\ \} \\
 & \forall(z : z \in Z : x \leq z \;=\; \forall(y : y \in Y : y \leq z)) \\
= & \quad \{\ \text{instantiate } z := x\,;\ (1)\text{: reflexivity}\ \} \\
 & \forall(z : z \in Z : x \leq z \;=\; \forall(y : y \in Y : y \leq z)) \wedge \forall(y : y \in Y : y \leq x) \\
\Leftarrow & \quad \{\ x \in Y \wedge \forall(y : y \in Y : y \leq x) \;\Rightarrow\; x \leq z\ \} \\
 & \forall(z : z \in Z : x \leq z \;\Rightarrow\; \forall(y : y \in Y : y \leq z)) \;\;\wedge\;\; \forall(y : y \in Y : y \leq x) \;\;\wedge\;\; x \in Y \\
= & \quad \{\ (3)\text{: transitivity}\ \} \\
 & \forall(y : y \in Y : y \leq x) \;\;\wedge\;\; x \in Y
\end{array}$$

□

Theorem

$$\forall(x :: \exists(y : y \in Y : x \leq y) \;\Rightarrow\; x \leq \uparrow Y) \tag{26}$$

$$\forall(x :: \exists(y : y \in Y : x \geq y) \;\Rightarrow\; x \geq \downarrow Y) \tag{27}$$

Proof

$$\begin{array}{ll}
 & \forall(x :: \exists(y : y \in Y : x \leq y) \;\Rightarrow\; x \leq \uparrow Y) \\
= & \quad \{\ \text{predicate calculus}\ \} \\
 & \forall(x, y : y \in Y : x \leq y \;\Rightarrow\; x \leq \uparrow Y) \\
\Leftarrow & \quad \{\ (3)\text{: transitivity}\ \} \\
 & \forall(x, y : y \in Y : y \leq \uparrow Y) \\
= & \quad \{\ (22)\ \} \\
 & \mathit{true}
\end{array}$$

is called a lowest upper bound. Similarly, the highest lower bound is defined as any x for which

$$\forall(z : z \in Z : z \leq x \;=\; \forall(y : y \in Y : z \leq y)) \tag{19}$$

First, we show that such an equation defines x uniquely. Let both x and x' satisfy (18), then for all z

$$\begin{array}{ll} & x \leq z \\ = & \qquad \{\; x \text{ satisfies } (18) \;\} \\ & \forall(y : y \in Y : y \leq z) \\ = & \qquad \{\; x' \text{ satisfies } (18) \;\} \\ & x' \leq z \end{array}$$

from which, on account of (8), $x = x'$ follows. This allows us to introduce a functional notation. We write $\uparrow Y$ for the lowest upper bound and $\downarrow Y$ for the highest lower bound. These prefix operators are partial functions and have higher binding power than any infix operator. From (18) and (19) we obtain

$$\forall(x :: x \geq \uparrow Y \;=\; \forall(y : y \in Y : x \geq y)) \tag{20}$$

$$\forall(x :: x \leq \downarrow Y \;=\; \forall(y : y \in Y : x \leq y)) \tag{21}$$

Next, we show why $\uparrow Y$ and $\downarrow Y$ are called the lowest upper bound and highest lower bound of Y.

Theorem

$$\forall(x :: (x = \uparrow Y) \;=\; (\forall(y : y \in Y : y \leq x) \;\wedge\; \forall(z :: \forall(y : y \in Y : y \leq z) \Rightarrow x \leq z))) \tag{22}$$

$$\forall(x :: (x = \downarrow Y) \;=\; (\forall(y : y \in Y : y \geq x) \;\wedge\; \forall(z :: \forall(y : y \in Y : y \geq z) \Rightarrow x \geq z))) \tag{23}$$

Proof

$$\begin{array}{ll} & x = \uparrow Y \\ = & \qquad \{\; \text{definition } (18) \;\} \\ & \forall(z :: x \leq z \;=\; \forall(y : y \in Y : y \leq z)) \\ = & \qquad \{\; \text{instantiate with } z := x \;\} \\ & \forall(z :: x \leq z \;=\; \forall(y : y \in Y : y \leq z)) \;\wedge\; x \leq x \;=\; \forall(y : y \in Y : y \leq x) \\ = & \qquad \{\; (1)\text{: reflexivity} \;\} \\ & \forall(z :: x \leq z \;=\; \forall(y : y \in Y : y \leq z)) \;\wedge\; \forall(y : y \in Y : y \leq x) \\ = & \qquad \{\; (3)\text{: } y \leq x \wedge x \leq z \;\Rightarrow\; y \leq z \;\} \\ & \forall(z :: x \leq z \;\Leftarrow\; \forall(y : y \in Y : y \leq z)) \;\wedge\; \forall(y : y \in Y : y \leq x) \end{array}$$

Observe that $\leq$ in the right-hand side is $\leq$ on Z.
Theorem *Function composition is monotonic*

$$f \circ g \text{ is monotonic in } f \tag{16}$$

Proof

$$\begin{array}{ll} & f \circ g \leq f' \circ g \\ = & \quad \{ \ (15) \ \} \\ & \forall(x :: (f \circ g).x \leq (f' \circ g).x) \\ \Leftarrow & \quad \{ \ \text{switch from } g.x \text{ to } y \ \} \\ & \forall(y :: f.y \leq f'.y) \\ = & \quad \{ \ (15) \ \} \\ & f \leq f' \end{array}$$

□

Theorem *Function composition is monotonic*

$$f \circ g \text{ is monotonic in } g \text{ if } f \text{ is monotonic} \tag{17}$$

Proof

$$\begin{array}{ll} & f \circ g \leq f \circ g' \\ = & \quad \{ \ (15) \ \} \\ & \forall(x :: (f \circ g).x \leq (f \circ g').x) \\ \Leftarrow & \quad \{ \ f \text{ is monotonic } \} \\ & \forall(x :: g.x \leq g'.x) \\ = & \quad \{ \ (15) \ \} \\ & g \leq g' \end{array}$$

□

3 Upper and lower bounds

An upper bound of a subset Y of Z is an element $z \in Z$ such that every element in Y is below z. The lowest upper bound is an upper bound below every other upper bound. We give a formal definition. Any x for which

$$\forall(z : z \in Z : x \leq z \ = \ \forall(y : y \in Y : y \leq z)) \tag{18}$$

Function application is written with infix operator $.$ instead of surrounding the argument with parentheses. The ordering relation between x and y is taken from Y whereas the ordering between $f.x$ and $f.y$ is taken from Z. They need not be the same orderings. We use the same symbol nevertheless and resolve potential ambiguities by looking at the types of the quantities involved.

Function composition is written with infix operator $\circ$ and for mapping a function over a set is we use the same infix operator $.$ that we use for function application.

$$\forall(z : z \in Z : (f \circ g).z \ = \ f.(g.z)) \tag{11}$$

$$\forall(Y : Y \subseteq Z : f.Y = \{y : y \in Y : f.y\}) \tag{12}$$

The two operators $.$ and $\circ$ have the highest binding power of all infix operators. Operator $\circ$ is associative, but $.$ is not.

Theorem

Composition of monotonic functions is monotonic. (13)

Proof
For monotonic f and g, we have

$$
\begin{array}{ll}
 & f \circ g \text{ is monotonic} \\
= & \quad \{ \ (10)\text{: definition of monotonicity } \} \\
 & \forall(x, y :: x \le y \ \Rightarrow \ (f \circ g).x \le (f \circ g).y) \\
= & \quad \{ \ (11)\text{: definition of } \circ \ \} \\
 & \forall(x, y :: x \le y \ \Rightarrow \ f.(g.x) \le f.(g.y)) \\
\Leftarrow & \quad \{ \ f \text{ is monotonic } \} \\
 & \forall(x, y :: x \le y \ \Rightarrow \ g.x \le g.y) \\
= & \quad \{ \ g \text{ is monotonic } \} \\
 & \mathit{true}
\end{array}
$$

□

Theorem

$$f.(g.Y) \ = \ (f \circ g).Y \tag{14}$$

Next we lift the partial ordering to functions. Let Y be any set. For functions $f, g : Y \to Z$ we define

$$f \le g \ = \ \forall(y : y \in Y : f.y \le g.y) \tag{15}$$

We also have

$$\forall(x,y :: x \leq y \ = \ \forall(z :: z \leq x \ \Rightarrow \ z \leq y)) \tag{7}$$

Proof

$$\begin{array}{ll} & x \leq y \ = \ \forall(z :: z \leq x \ \Rightarrow \ z \leq y) \\ = & \qquad \{ \text{ switch to dual } \} \\ & y \geq x \ = \ \forall(z :: x \geq z \ \Rightarrow \ y \geq z) \\ = & \qquad \{ \ (6)[x,y,\leq \ := y,x,\geq] \text{ since } \geq \text{ is a partial order } \} \\ & \mathit{true} \end{array}$$

□

We also have

$$\forall(x,z :: \forall(y :: (x \leq y) \ = \ (z \leq y)) \ = \ (x = z)) \tag{8}$$

as shown by

$$\begin{array}{ll} & x = z \\ \Rightarrow & \\ & \forall(y :: (x \leq y) \ = \ (z \leq y)) \\ \Rightarrow & \\ & \forall(y :: (x \leq y) \ \Rightarrow \ (z \leq y)) \ \wedge \ \forall(y :: (z \leq y) \ \Rightarrow \ (x \leq y)) \\ = & \qquad \{ \ (6) \ \} \\ & z \leq x \ \wedge \ x \leq z \\ = & \qquad \{ \ (2)\text{: antisymmetry } \} \\ & x = z \qquad . \end{array}$$

Switching to the dual, we have

$$\forall(x,z :: \forall(y :: (y \leq x) \ = \ (y \leq z)) \ = \ (x = z)) \tag{9}$$

2 Functions

Function f from Y to Z is called *monotonic* if

$$\forall(x,y :: x \leq y \ \Rightarrow \ f.x \leq f.y) \tag{10}$$

Formula (1) is equivalent to

$$\forall(x, y :: x \leq y \;\Leftarrow\; \forall(z :: y \leq z \;\Rightarrow\; x \leq z)) \tag{4}$$

Proof

(1) $\Rightarrow$ (4)

$$\begin{array}{ll}
 & \forall(z :: y \leq z \;\Rightarrow\; x \leq z) \\
\Rightarrow & \qquad \{ \text{ instantiate } z := y \;\} \\
 & y \leq y \;\Rightarrow\; x \leq y \\
= & \qquad \{ \text{ (1) } \} \\
 & x \leq y
\end{array}$$

(4) $\Rightarrow$ (1)

$$\begin{array}{ll}
 & x \leq x \\
\Leftarrow & \qquad \{ \text{ (4)} \, [y := x] \;\} \\
 & \forall(z :: x \leq z \;\Rightarrow\; x \leq z) \\
= & \\
 & \mathit{true}
\end{array}$$

□

Formula (3) is equivalent to

$$\forall(x, y :: x \leq y \;\Rightarrow\; \forall(z :: y \leq z \;\Rightarrow\; x \leq z)) \tag{5}$$

Proof

$$\begin{array}{ll}
 & \forall(x, y, z :: x \leq y \;\;\wedge\;\; y \leq z \;\Rightarrow\; x \leq z) \\
= & \\
 & \forall(x, y, z :: x \leq y \;\Rightarrow\; (y \leq z \;\Rightarrow\; x \leq z)) \\
= & \\
 & \forall(x, y :: x \leq y \;\Rightarrow\; \forall(z :: y \leq z \;\Rightarrow\; x \leq z))
\end{array}$$

□

Combining formulae (4) and (5), we get

$$\forall(x, y :: x \leq y \;=\; \forall(z :: y \leq z \;\Rightarrow\; x \leq z)) \tag{6}$$

On lattice theory and program semantics

Jan L.A. van de Snepscheut
Spring 1993

This note is to record some lattice theory. It is a theory concerned with the properties of an uninterpreted partial order $\leq$, to be read as "at most", "below", "implies", or "is contained in".

In the first half of the last century, Boole's formalization of propositional logic led to the concept of boolean algebra. Pierce and Schröder investigated axiomatic definitions of boolean algebras and introduced the notion of a lattice. Dedekind's work on ideals of algebraic numbers led independently to the same notion.

The general development of lattice theory started in the 1930's with Birkhoff. His *Lattice Theory* (cf. [2]) is still the standard reference work. A more recent book is [7]. Some results are from [5] and some are from [6].

In a later section we study an operational semantics of a program notation. This semantics is based on [9], and so is the link to the subsequent sections. The axiomatic semantics that follows is largely based on [6]. The refinement ordering is from ([1]); ([13]) studies refinement in a lattice-theoretical setting.

1 Partial orders

Let me start with the definition of a partial order. It is a binary relation $\leq$ on a set Z and has three properties:

$$\forall(x :: x \leq x) \tag{1}$$

$$\forall(x, y :: x \leq y \ \wedge \ y \leq x \ \Rightarrow \ x = y) \tag{2}$$

$$\forall(x, y, z :: x \leq y \ \wedge \ y \leq z \ \Rightarrow \ x \leq z) \tag{3}$$

known as *reflexivity*, *antisymmetry*, and *transitivity* respectively. All bound variables are taken from set Z but this restriction has been omitted from the formulae. Pair $(Z, \leq)$ is called a *poset,* for partially ordered set. If $\leq$ is understood, we may refer to Z as a poset.

Formula $x \leq y$ is also written as $y \geq x$. Relation $\geq$ is called the dual of $\leq$. If a relation is a partial order, then so is its dual. Both $\leq$ and $\geq$ have a higher binding power than has $=$.