Guards, Failure, and Partiality: Dijkstra's Guarded-Command Language Formulated Topologically

David A. Schmidt*

Kansas State University, Manhattan, Kansas, USA

Abstract. Existing treatments of Dijkstra's guarded-command language treat divergence and failure as equivalent, even though Dijkstra clearly states they are not. We reexamine Dijkstra's language, redefining its denotational semantics with powerdomains formulated in topological terms. The results refine existing work, give a sound semantics of guards, failure, and divergence for non-flat storage domains, and reveal the important role that general topology plays in program correctness.

1 Introduction: the Guarded-Command Language

Dijkstra's Guarded-Command Language (GCL) [4] introduced nondeterministic conditional choice — and the resultant semantical complications — to the programming world. Dijkstra masterfully hid GCL's complications behind his weakest-precondition calculus and the tacit assumption that primary storage was "flat" — unstructured.[1]

GCL's weakest-precondition calculus is a proof theory that deserves a model, and Plotkin's and Smyth's research on powerdomains [16, 18, 25] led Plotkin to define a denotational semantics for GCL based on Smyth's upper powerdomain applied to a flat domain of storage [17]. Subsequently [26], Smyth explained why the storage domain need not be flat, and in his thesis [2], Bonsangue defined denotational semantics of a GCL variant for all of the lower, upper, and convex powerdomains (but his semantics definitions again used flat storage).

These developments were insightful and important but unfinished in that

1. the semantics of failure of the conditional and divergence of its guards were never completely developed; and
2. the semantics of GCL for non-flat domains was never completely specified.

These points are important because Dijkstra's description of failure is central to the semantics of the nondeterministic conditional (see Harel's thoughtful explanation in [9], Chapters 5-7), and the natural definition of storage might well be a non-flat domain that contains partial values — see Figure 1.

* das@ksu.edu. Supported by NSF CNS-1219746.

[1] Not all difficulties were hidden, however, as witnessed by Chapter 9 of Dijkstra's text [4], which presented a Scott-continuity law for commands.

Mappings from location numbers to possibly uninitialized cells, modelling dynamic cell allocation/deallocation:

$MStore = \mathbb{N} \to \mathbb{N}_\perp$

Sample elements of $MStore$: $\lambda n.n$, $\lambda n.\ \perp$, $\lambda n.n = 0 \to 1; n = 1 \to 2; \perp$

Linear sequences of numbers, modelling storage stacks:

$LStore = (\{nil\} + (\mathbb{N} \times LStore))_\perp$

Sample elements of $LStore$: $(2, (3, nil))$, $(2, \perp)$, $(1, (2, (3, \cdots (i, \cdots) \cdots)))$

Fig. 1. Two non-flat storage domains and sample elements

This paper aims to fill these gaps and summarize existing results in a systematic manner. The unifying methodology is general topology [30], whose concepts of open set and continuous function not only provided Scott with notions he needed to solve the $D = D \to D$ problem but also gave Smyth and others the tools needed to understand computation theory [1, 2, 5, 10, 16, 18, 19, 22, 23, 20, 21, 24–26, 29]. This paper accomplishes the following:

- It reveals the role topology plays in the construction of powerdomains and in the definition of the box and diamond modalities that define predicate transformers for GCL.
- It gives a sound denotational semantics of GCL and its *wp*-calculus for non-flat domains that is faithful to Dijkstra's description of guards, failure, and divergence [4].

2 Technical background

2.1 Domains

For our purposes, a *domain* $(D, \sqsubseteq_D)$ is an algebraic, directed-complete, partially ordered set [5, 18]. When discussing $(D, \sqsubseteq_D)$, we normally state just D and leave $\sqsubseteq_D$ implicit. Standard domain constructions (product, sum, function-space, lift) and their associated functions can be found in any text on denotational semantics [3, 7, 13, 18, 14, 15, 20, 27, 31].

A function f from domain D to domain E is *Scott continuous* iff for all directed $S \subseteq D$, $f(\sqcup S) = \sqcup\{f(d) \mid d \in S\}$. (Recall that nonempty set S is *directed*, if for all $d, d' \in S$, there is some $e \in S$ such that $d \sqsubseteq e$ and $d' \sqsubseteq e$.)

These subsets are useful: for domain D and $S \subseteq D$,

up closure: $\uparrow S = \{d \in D \mid \exists e \in S, e \sqsubseteq d\}$
down closure: $\downarrow S = \{d \in D \mid \exists e \in S, d \sqsubseteq e\}$
Scott closure: $cl(S) = \downarrow\{\sqcup T \mid T \text{ is directed and } T \subseteq S\}$
convex closure: $conv(S) = cl(S) \cap \uparrow S$

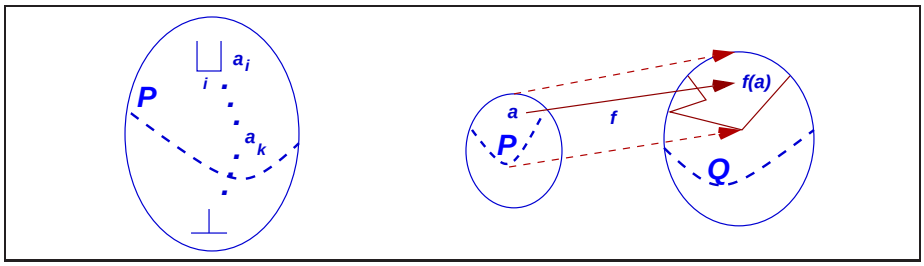

Fig. 2. Scott-open set (P is up-closed and closed under tails of directed sets) and continuous function (when $f(a)$ maps in open set, Q, then $f[P] \subseteq Q$ for some open P)

2.2 Scott topology

Topology is the study of properties (*open sets*) and functions that behave well (are *continuous*) regarding the properties. For example, the real line, $\mathbb{R}$, has as open sets the open intervals, (a, b). A number $r \in \mathbb{R}$ has property (a, b) when $r \in (a, b)$, e.g., $\pi \in (3, 4)$. A function $f : \mathbb{R} \to \mathbb{R}$ is topologically continuous when it maps arguments "close together" (sharing many open sets) to answers "close together" (sharing equally many open sets), e.g., $area(r) = \pi r^2$ is continuous with respect to intervals. The continuous functions on the real line are exactly the topologically continuous functions.

Topology applies to Scott-domain theory [5, 19, 22]: For domain D, Scott defined D's open sets to be those subsets of D that are *(i)* upwards closed and *(ii)* closed under tails of directed sets.[2] See Figure 2. Scott proved that the functions that are topologically continuous for his *Scott topology* of D are exactly the Scott-continuous functions on D. Further, to solve the domain equation, $D = D \to D$, Scott restricted $D \to D$ to the continuous functions, limiting the domain's cardinality to the continuum.

Here are some open sets ("properties") from the domains in Figure 1:

- $O_1 = \{\sigma \in MStore \mid \sigma(1) = 3\}$ ("σ's cell 1 holds 3")
- $O_2 = \{\sigma \in MStore \mid \exists k > 0, \forall 0 \leq i < k, \sigma(i) \in \mathbb{N}\}$ ("σ has a defined finite prefix")
- $O_3 = \{(a, b) \in LStore \mid a \in \mathbb{N}\}$, ("the store has length ≥ 1")
- $O_4 = \{(a, (3, b)) \in LStore\}$ ("the store's second element is 3")
- $O_5 = \{(a_0, (a_1, \cdots (a_k, nil) \cdots)) \in LStore \mid k \geq 0\}$ ("the store has finite length")

Note that $(\lambda n.3)$ belongs to O_1 and O_2, as does $(\lambda n.n \leq 1 \to 3; \bot)$ — a "partial" store can belong to a "property set." Similarly, $(2, (3, \bot))$ belongs to O_3 and O_4, as does the infinite sequence, $(3, (3, \cdots (3, \cdots) \cdots))$. But neither belongs to O_5.

[2] That is, for every directed set, S, when $\sqcup S \in O$, for open set $O \subseteq D$, then there exists some $d \in S$ such that $d \in O$ also. This means S's "tail," from d upwards, is in O. A Scott-open set is like a half-open interval, $(q, \infty]$, $q \in \mathbb{R}$.

This variation of O_5 is not Scott-open: $\{(a_0,(a_1,\cdots(a_i,\cdots)\cdots)) \in LStore \mid a_i \in \mathbb{N}, \forall i \geq 0\}$ ("the store has infinite length"), nor is this variant of O_2: $\{\sigma \in MStore \mid \sigma(i) \in \mathbb{N}, \forall i \in \mathbb{N}\}$ ("σ is total") — Scott-open sets must be closed under tails of directed sets, that is, the property defined by an open set must be decided "finitely."

For domain $\mathbb{N}_\perp$, *any* subset of $\mathbb{N}$ is Scott-open — open sets are not necessarily recursively enumerable. For this reason among others,[3] Plotkin required finitely-generable sets to define the elements of his powerdomain [16].

2.3 General topology

Here are some basic concepts; Willard [30] is a good reference. For a set, X, a *topology* $\Omega X \subseteq \mathcal{P}(X)$, is a family of sets, called the *open sets*, that are closed under arbitrary union (for all $S \subseteq \Omega X$, $\bigcup S \in \Omega X$) and finite intersection (for all finite $S \subseteq \Omega X$, $\bigcap S \in \Omega X$). The complement, $\sim O = X - O$, of an open set $O \in \Omega X$ is a *closed set*; define $\mho X = \{\sim O \mid O \in \Omega X\}$. Note that $\mho X$ is closed under arbitrary intersection and finite union.

For topology ΩX, a *base* is a subset, $\mathcal{B}_X \subseteq \Omega X$, such that every $O \in \Omega X$ is the union of some members of $\mathcal{B}_X$; the members of $\mathcal{B}_X$ are called *basic-open sets*. The topology on the real line uses open intervals, (a,b), for $a,b \in \mathbb{R}$, as its base. A *subbase* is some $\mathcal{SB}_X \subseteq \Omega X$, such that all finite intersections of sets in $\mathcal{SB}_X$ form a base.

Given topologies for sets X and Y, there are standard definitions for the coarsest topologies for $X \times Y$, $X \to Y$, etc. [30].

A function, $f : X \to Y$, is *(topologically) continuous* iff for all $x \in X$ and $V \in \Omega Y$, if $f(x) \in O'$, then there exists some $O \in \Omega X$ such that $x \in O$ and $f[O] \subseteq O'$ (where $f[O] = \{f(x) \mid x \in O\}$). See Figure 2. A crucial result is that f is continuous iff its inverse-image function maps open sets to open sets: for all $O' \in \Omega Y$, $f^{-1}(O') \in \Omega X$, where $f^{-1}(O') = \{x \in X \mid f(x) \in O'\}$. When f is continuous, then f^{-1} maps closed sets to closed sets as well.

A nonempty family of open sets, $F \subseteq \Omega X$, is *directed* if for all $O_1, O_2 \in F$ there is some $O_3 \in F$ such that $O_1 \subseteq O_3$ and $O_2 \subseteq O_3$. A set, $S \subseteq X$, is *compact* if for every directed family of open sets, F, $S \subseteq \bigcup F$ implies $S \subseteq O$ for some $O \in F$.[4] The intuition is that a compact set is "small enough" to be covered by some "finite sized" open set. Plotkin's finitely generable sets are compact [16, 18].

Open sets can be understood as logical properties, and there is a natural intuitionistic propositional logic, defined in Figure 3 [28]. The disjunction can be infinitary. As usual, define $\neg\psi$ as $\psi \supset \mathit{false}$ so that $[\![\neg\psi]\!] = \bigcup\{O \in \Omega X \mid O \cap [\![\psi]\!] \subseteq \emptyset\}$. That is, $\neg\psi$ denotes the largest open set disjoint from ψ. In the Scott topology, $[\![\neg O]\!] = \sim(\downarrow O)$ for $O \in \Omega D$. Thus, for every open $O \neq D$, $\perp_D \notin O$, that is, $\perp_D$ satisfies no nontrivial property.

[3] Also, finitely generable sets ensure that Plotkin's powerdomain, $\mathcal{P}_C(D)$, is algebraic when D is algebraic.

[4] Equivalently, S is compact iff whenever it is covered by the union of any collection of open sets, it is covered by a finite subset of that collection.

$O \in \Omega D \qquad \psi \in Proposition$

$\psi ::= O \mid false \mid \psi \wedge \psi \mid \bigvee_{i \in I} \psi_i \mid \psi \supset \psi$

$[\![O]\!] = O$
$[\![false]\!] = \emptyset$
$[\![\psi_1 \wedge \psi_2]\!] = [\![\psi_1]\!] \cap [\![\psi_2]\!]$

$[\![\bigvee_{i \in I} \psi_i]\!] = \bigcup_{i \in I} [\![\psi_i]\!]$
$[\![\psi_1 \supset \psi_2]\!] = \bigcup \{O \in \Omega X \mid O \cap [\![\psi_1]\!] \subseteq [\![\psi_2]\!]\}$

Fig. 3. Propositional logic: $[\![\cdot]\!] : Proposition \to \Omega D$

2.4 Powerdomains

Because domain D is partially ordered, the naive set-of-all subsets construction, $\mathcal{P}(D)$, does not possess standard functions that are Scott-continuous. In this paper, we generate powerdomains as equivalence classes of sets [16, 20, 25].

For domain D and $PD \subseteq \mathcal{P}(D)$, let $(\sqsubseteq_M) \subseteq PD \times PD$ be a preorder and $\equiv_M$ its derived equivalence relation. Define equivalence classes, $[S]_M \in PD/M$, $S \in PD$, as usual, and define $[S]_M \sqsubseteq_M [T]_M$ iff $S \sqsubseteq_M T$.

Definition 1. $\mathcal{P}_M(D) = (PD/M, \sqsubseteq_M)$ *is a* powerdomain *if the following operations are well-defined (congruences with respect to* $\equiv_M$*) and are Scott-continuous:*

$\{\!|\cdot|\!\} : D \to PD/M$ *is defined*
$\{\!|d|\!\} = [\{d\}]_M$
$\uplus : PD/M \times PD/M \to PD/M$ *is defined*
$[S]_M \uplus [T]_M = [S \cup T]_M$
For any Scott-continuous $f : D \to PD/M$, $f^\dagger : PD/M \to PD/M$ *is defined*
$f^\dagger[S]_M = [\bigcup_{d \in S} F_d]_M$, *where* $f(d) = [F_d]_M$

Plotkin and Smyth [16, 18, 25] showed that there are initial solutions to the above constraints where

1. $[S]_M \sqsubseteq_M [S]_M \uplus [T]_M$ and $[T]_M \sqsubseteq_M [S]_M \uplus [T]_M$: The solution, called the *lower powerdomain*, is $\mathcal{P}_L(D) = (PD/L, \sqsubseteq_L)$, where PD are all nonempty subsets of D and $S \sqsubseteq_L T$ iff for all $O \in \Omega D$, $S \cap O \neq \emptyset$ implies $T \cap O \neq \emptyset$.
2. $[S]_M \uplus [T]_M \sqsubseteq_M [S]_M$ and $[S]_M \uplus [T]_M \sqsubseteq_M [T]_M$: The solution, called the *upper powerdomain*, is $\mathcal{P}_U(D) = (PD/U, \sqsubseteq_U)$, where PD are all nonempty compact subsets of D and $S \sqsubseteq_U T$ iff for all $O \in \Omega D, S \subseteq O$ implies $T \subseteq O$.
3. No orderings are required between $[S]_M$, $[T]_M$, and $[S]_M \uplus [T]_M$: The solution, called the *convex powerdomain*, is $\mathcal{P}_C(D) = (PD/U, \sqsubseteq_U)$, where PD are all nonempty compact subsets of D and $\sqsubseteq_C = \sqsubseteq_L \cap \sqsubseteq_U$.

D's topology identifies which sets possess equal information content. The initial solutions have well-known canonical representations [10, 11, 18, 26]:

lower powerdomain: $(CL(D), \sqsubseteq_{CL})$, where $CL(D) = \{S \subseteq D \mid S = cl(S) \neq \emptyset\}$ and $S \sqsubseteq_{CL} T$ iff for every $d \in S$ there is some $e \in T$ such that $d \sqsubseteq_D e$. (Indeed, $\sqsubseteq_{CL}$ is $\subseteq$.) Define $\{\!|d|\!\} = {\downarrow}\{d\}$, $S \uplus T = S \cup T$, and $f^\dagger(S) = cl(\cup\{f(d) \mid d \in S\})$.

upper powerdomain: $(UC(D), \sqsubseteq_{UC})$, where $UC(D) = \{S \subseteq D \mid S \textit{ is compact}, S = {\uparrow}S \neq \emptyset\}$ and $S \sqsubseteq_{UC} T$ iff for every $e \in T$ there is some $d \in S$ such that $d \sqsubseteq_D e$. (Indeed, $\sqsubseteq_{UC}$ is $\supseteq$.) Define $\{\!|d|\!\} = {\uparrow}\{d\}$, $S \uplus T = S \cup T$, and $f^\dagger(S) = \cup\{f(d) \mid d \in S\}$.

convex powerdomain: $(CONV(D), \sqsubseteq_{CL} \cap \sqsubseteq_{UC})$, where $CONV(D) = \{S \subseteq D \mid S \textit{ is compact}, S = conv(S) \neq \emptyset\}$. Define $\{\!|d|\!\} = \{d\}$, $S \uplus T = conv(S \cup T)$, and $f^\dagger(S) = conv(\cup\{f(d) \mid d \in S\})$.

Note that $f^\dagger$ is well defined for $\mathcal{P}_U(D)$ and $\mathcal{P}_C(D)$ because $f^\dagger$ is binary additive and the domains' elements are compact sets [12].

When working with these representations, care should be taken when performing set-theoretic reasoning. For example, in $\mathcal{P}_L(\mathbb{N}_\perp)$, $\{\!|2|\!\}$ is the equivalence class, $[\{2\}]_L$, whose canonical representation is the Scott-closed set, $\downarrow\{2\} = \{2, \perp\}$. It is tempting to conclude that $\perp \in \{\!|2|\!\}$, but this is not the case for all sets in the equivalence class, $[\{2\}]_L$.[5]

An operation, $f : \mathcal{P}(D) \to E$, is an *M-congruence* with respect to $(\sqsubseteq_M) \subseteq PD \times PD$, $PD \subseteq \mathcal{P}(D)$, if for all $S, T \in PD$, $S \equiv_M T$ implies $f(S) = f(T)$; we define $f : PD/M \to E$ as $f[S]_M = f(S)$.

For domain D, $PD \subseteq \mathcal{P}(D)$, $(\sqsubseteq_M) \subseteq PD \times PD$,

- If $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$, then the property, "$\_ \cap O \neq \emptyset$," for $O \in \Omega D$, is an M-congruence. For $[S]_M \in PD/M$, we write "$[S]_M$ *meets* O" to denote $S \cap O \neq \emptyset$.
- If $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$, then the property, "$\_ \subseteq O$," for $O \in \Omega D$, is an M-congruence. For $[S]_M \in PD/M$, we write "O *covers* $[S]_M$" to denote $S \subseteq U$.

2.5 Powerspace topologies and multifunctions

Smyth [26] developed useful characterizations of topologies on powersets, and they apply to powerdomains, too. For set X, let ΩX be its topology. Then, for $PX \subseteq \mathcal{P}(X)$,

1. PX's *upper powerspace*, $\Omega_U PX$, is the topology generated from a base consisting of sets of form *(i)* $\{S \in PX \mid S \subseteq O\}$ for each $O \in \Omega X$.
2. PX's *lower powerspace*, $\Omega_L PX$, is the topology generated from a subbase consisting of sets of form *(ii)* $\{S \in PX \mid S \cap O \neq \emptyset\}$ for each $O \in \Omega X$.
3. PX's *convex powerspace*, $\Omega_C PX$, is the topology generated from a subbase consisting of sets of form *(i)* and *(ii)* above.

A (pre)ordering underlying a powerspace's elements is defined as follows: for $s, t \in PX$, $s \sqsubseteq t$ iff for all $O \in \Omega PX$, $s \in O$ implies $t \in O$.

Smyth proved that the Scott topologies for the three canonical powerdomains coincide with the powerspaces on domain D:

[5] For this reason, among others, Smyth claimed that the elements of a (power)domain are "bundles of properties" — completely prime filters in a Sober space [26]. Or, one can construct the elements of a (power)domain as ideal completions of directed sets of finite elements [7, 8, 18].

1. $\Omega\mathcal{P}_U(D)$ is topologically isomorphic (*homeomorphic*) to $\Omega_U UC(D)$
2. $\Omega\mathcal{P}_L(D)$ is homeomorphic to $\Omega_L CL(D)$
3. $\Omega\mathcal{P}_C(D)$ is homeomorphic to $\Omega_C CONV(D)$

Further, the underlying orderings for each of the three powerspaces are order-isomorphic to the orderings on the powerdomains. For this reason, *from here on we always understand ΩD to mean the Scott-topology on domain D.*

Smyth also studied set-valued functions. Again, for set Y, let $PY \subseteq \mathcal{P}(Y)$. Call function $f : X \to PY$ a "multifunction" [26]. There are two inverses of f:

upper: $[f] : PY \to \mathcal{P}(X)$, defined $[f]S = \{x \in X \mid f(x) \subseteq S\}$
lower: $\langle f\rangle : PY \to \mathcal{P}(X)$, defined $\langle f\rangle S = \{x \in X \mid f(x) \cap S \neq \emptyset\}$

Say that sets X and Y have topologies ΩX and ΩY. Smyth proved these crucial results for multifunctions, $f : X \to PY$:

1. $[f]$ has arity $\Omega Y \to \Omega X$ (that is, it maps open sets to open sets) iff f is a topologically continuous function of arity $f : X \to \Omega_U PY$ iff $\langle f\rangle$ has arity $\mho Y \to \mho X$ (that is, it maps closed sets to closed sets).
2. $\langle f\rangle$ has arity $\Omega Y \to \Omega X$ iff f is a topologically continuous function of arity $f : X \to \Omega_L PY$ iff $[f]$ has arity $\mho Y \to \mho X$.
3. Both $[f]$ and $\langle f\rangle$ have arity $\Omega Y \to \Omega X$ iff f is a topologically continuous function of arity $f : X \to \Omega_C PY$ iff $\langle f\rangle$ and $[f]$ have arity $\mho Y \to \mho X$.

3 Properties of $[\,\cdot\,]$ and $\langle\,\cdot\,\rangle$

In this section, let D be a domain, $PD \subseteq \mathcal{P}(D)$, and preordering $M \subseteq PD \times PD$ generate the powerdomain, $\mathcal{P}_M(D) = (PD/M, \sqsubseteq_M)$.

Proposition 2. *For $f : D \to \mathcal{P}_M(D)$ and $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$,*

1. $\bigcap_{i\in I} [f]O_i = [f]\bigcap_{i\in I} O_i$, *for* $(O_i)_{i\in I} \subseteq \Omega D$
2. $[f]O \cup [f]O' \subseteq [f](O \cup O')$, *for* O, O" $\in \Omega D$

Proof. (1): $\bigcap_{i\in I} [f]O_i = \bigcap_{i\in I}\{d \in D \mid O_i \textit{ covers } f(d)\} = \{d \in D \mid \textit{for all } i \in I, O_i \textit{ covers } f(d)\} = \{d \in D \mid \bigcap_{i\in I} O_i \textit{ covers } f(d)\}$.

(2): The proof for $\subseteq$ looks like (1)'s. But $\supseteq$ fails: Let $D = \mathbb{N}_\perp$, $O = \{0\}, O' = \{1\}$, $f_0(n) = [\{0,1\}]_M$, for all $n \in D$. Then, $[f_0]\{0,1\} = D$, but $[f_0]\{0\} = [f_0]\{1\} = \emptyset$.

These useful facts are proved in the Appendix:

- If $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$, then $\{E \in \mathcal{P}_M(D) \mid O \textit{ covers } E\}$ is Scott-open in $\Omega\mathcal{P}_M(D)$, for every $O \in \Omega D$.
- If $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$, then $\{E \in \mathcal{P}_M(D) \mid E \textit{ meets } O\}$, is Scott-open in $\Omega\mathcal{P}_M(D)$, for every $O \in \Omega D$.

Proposition 3. *If all sets in $\mathcal{P}_M(D)$ are compact with respect to ΩD, and $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$, then $[f]O$ is continuous in both its arguments, $f : D \to \mathcal{P}_M(D)$ and $O \in \Omega D$.*

Proof. For the first argument, f, we show monotonicity as follows: say that $f \sqsubseteq_{D\to\mathcal{P}_M(D)} g$. So, $f(d) \sqsubseteq_M g(d)$) implying $f(d) \sqsubseteq_L g(d)$), implying O *covers* $f(d)$ implies O *covers* $g(d)$.

To show continuity, let $(f_i)_{i\in I}$ be a directed family of functions. We show that $[\sqcup_{i\in I} f_i]O \subseteq \bigcup_{i\in I} [f_i]O$. First, $[\sqcup_{i\in I} f_i]O = \{d \mid O \text{ covers } (\sqcup_{i\in I} f_i)(d)\} = \{d \mid O \text{ covers } \sqcup_{i\in I}(f_i(d))\}$.

When O *covers* $\sqcup_{i\in I}(f_i(d))$ holds true, then $\sqcup_{i\in I}(f_i(d))$ belongs to the open set, $\{E \in \mathcal{P}_M(D) \mid O \text{ covers } E\}$. The family, $f_i(d)$, $i \in I$, is directed in $\mathcal{P}_M(D)$, so there is some $f_k(d)$ in that same open set, that is, O *covers* $f_k(d)$ holds.

For the second argument, O, monotonicity is immediate. To prove continuity, first $[f](\bigcup_{i\in I} O_i) = \{d \mid \bigcup_{i\in I} O_i \text{ covers } f(d)\}$. When $\bigcup_{i\in I} O_i$ *covers* $f(d)$ holds, it means $F \subseteq \bigcup_{i\in I} O_i$ holds, for $f(d) = [F]_M$, $F \in PD$. Since set F is compact and is covered by the union of the directed family of open sets, $(O_i)_{i\in I}$, it is covered by some O_k, that is, $F \subseteq O_k$, implying O_k *covers* $[F]_M$. Hence, $d \in \bigcup_{i\in I}\{d \mid O_i \text{ covers } f(d)\}$.

We have a parallel set of results (and proofs) for $\langle \cdot \rangle$:

Proposition 4. *For $f : D \to \mathcal{P}_M(D)$ and $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$,*

1. $\bigcup_{i\in I} \langle f\rangle O_i = \langle f\rangle \bigcup_{i\in I} O_i$, *for* $(O_i)_{i\in I} \subseteq \Omega D$
2. $\langle f\rangle(O \cap O') \subseteq \langle f\rangle O \cap \langle f\rangle O'$, *for* $O, O' \in \Omega D$.

Proposition 5. *If $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$, then $\langle f\rangle O$ is continuous in both its arguments, $f : D \to \mathcal{P}_M(D)$ and $O \in \Omega D$.*

In his thesis [2], Bonsangue uses $[\cdot]$ and $\langle \cdot \rangle$ as isomorphism maps between programs and predicate transformers: For domains X and Y,

1. $X \to \mathcal{P}_L(Y)$ is order isomorphic to the domain of completely additive functions, $\Omega Y \to \Omega X$, where the isomorphism takes program f to $[f]$.
2. $X \to \mathcal{P}_U(Y)$ is order isomorphic to the domain of binary-multiplicative functions, $\Omega Y \to \Omega X$, where the isomorphism takes program f to $\langle f\rangle$.
3. A pair of Scott-continuous functions, (bx, di), both of arity $\Omega Y \to \Omega X$, is *jointly multiplicative* if *(i)* bx is multiplicative, *(ii)* di is completely additive, and for all open sets $O, O' \in \Omega Y$, *(iii)* $bx(O \cup O') \subseteq bx(O) \cup di(O')$ and *(iv)* $bx(O) \subseteq di(O)$. The collection of jointly multiplicative pairs forms a domain that is order isomorphic to $X \to \mathcal{P}_C(Y)$, where the isomorphism takes program f to $([f], \langle f\rangle)$.[6]

Bonsangue's results generalize Plotkin's characterization of $Store \to \mathcal{P}_U(Store_\perp)$ for set *Store* [17] and Smyth's characterization of $X \to \mathcal{P}_U(X_\perp)$ for domains (more precisely, for Sober spaces [26]), X.

[6] The definition of "jointly multiplicative pair" given here applies when Y's topology is a *coherent space* [2, 5].

4 Predicate transformers

The preceding results almost demand that we treat correctness properties/predicates as open sets and use $[\,\cdot\,]$ and $\langle\,\cdot\,\rangle$ as predicate transformers.

But we approach the situation from first principles: *Program/function f's weakest-precondition map is its inverse-image map.* This is readily apparent for a deterministic program/function $f : \mathit{Store} \to \mathit{Store}_\perp$, where a correctness property is a set, $\psi \subseteq \mathit{Store}$, and $wp(f)\psi = f^{-1}[\psi] = \{s \in \mathit{Store} \mid f(s) \in \psi\}$.

This maxim should also apply when D is a non-flat domain and $f : D \to \mathcal{P}(D)$ denotes a nondeterministic program. But D's ordering complicates matters — correctness properties can no longer be mere sets, and f's range is a set-of-sets so that $f^{-1}\psi$, for $\psi \subseteq D$, is no longer well defined. Smyth [26] made these two assertions:

1. A correctness property/predicate is an open set, $U \in \Omega D$, in the Scott topology for non-flat domain D.
2. A nondeterministic program is a multifunction, more precisely, a Scott-continuous function of arity $f : D \to \mathcal{P}_U(D)$,[7] and its inverse image is defined $wp(f) = [f] : \Omega D \to \Omega D$.

Smyth's choices are eminently sensible for $D \to \mathcal{P}_U(D)$. Do Bonsangue's results, stated above, suggest that that $\langle f \rangle$ is "wp" for $f : D \to \mathcal{P}_L(D)$? And what about $D \to \mathcal{P}_C(D)$?

4.1 Predicate transformers are inverse-image maps

For non-flat domain D, $PD \subseteq \mathcal{P}(D)$, and nondeterministic program $f : D \to PD$, we can define $wp(f) = f^{-1} : \Omega\mathcal{P}_M(D) \to \Omega\mathcal{P}_M(D)$ for each of the three canonical powerdomains (that is, when $M \in \{U, L, C\}$). The topologies show us how:

Theorem 6. *For (non-flat) domain D, $O' \in \Omega\mathcal{P}_U(D)$, $f : D \to \mathcal{P}_U(D)$, $f^{-1}[O'] = \bigvee_{i\in I} [f]O_i$, for some family, $(O_i)_{i\in I}$, of open sets in ΩD.*

Proof. Recall that the base of the Scott topology on $\mathcal{P}_U(D)$ are those sets of form $B_O = \{S \in \mathcal{P}_U(D) \mid S \subseteq O\}, O \in \Omega D$. Thus, each open $O' = \bigcup_{i\in I} B_{O_i}$, for some family of open sets, $(O_i)_{i\in I}$. So, $f^{-1}[O'] = f^{-1}(\bigcup_{i\in I} B_{O_i}) = \{d \in D \mid f(d) \in \bigcup_{i\in I} B_{O_i}\} = \{d \mid f(d) \in B_{O_k}, \textit{for some } k \in I\} = \{d \mid O_k \textit{ covers } f(d), \textit{for some } k \in I\} = \bigcup_{i\in I}\{d \mid O_i \textit{ covers } f(d)\} = \bigvee_{i\in I} [f]O_i$, using the definitions of $\bigvee$ and $[f]$.

Theorem 7. *For (non-flat) domain D, $O' \in \Omega\mathcal{P}_L(D)$, $f : D \to \mathcal{P}_L(D)$, $f^{-1}[O'] = \bigvee_{i\in I} \bigwedge_{j\in J} \langle f\rangle O_{ij}$, for some family, $(O_{ij})_{i\in I, j\in J}$, of open sets in ΩD, where J must have finite range.*

Proof. Recall that the subbase of the Scott topology on $\mathcal{P}_L(D)$ are those sets of form $S_O = \{S \in \mathcal{P}_L(D) \mid S \cap O \neq \emptyset\}, O \in \Omega D$. Thus, open set $O' = \bigcup_{i\in I} \bigcap_{j\in J} S_{O_{ij}}$, for some family of open sets, $(O_{ij})_{i\in I, j\in J}$, where J must have finite range. The proof proceeds like the one above.

[7] or $f : D \to \mathcal{P}_U(D_\perp)$

Theorem 8. *For (non-flat) domain D, $O' \in \Omega\mathcal{P}_C(D)$, $f : D \to \mathcal{P}_C(D)$, $f^{-1}[O'] = \bigvee_{i\in I}\bigwedge_{j\in J}(\!(f)\!)O_{ij}$, where $(\!(f)\!)$ may be either of $[\![f]\!]$ or $\langle f\rangle$, and $(O_{ij})_{i\in I, j\in J}$ is a family of open sets in ΩD, where J must have finite range.*

Proof. The subbase of the Scott topology on $\mathcal{P}_C(D)$ are those sets of form $B_O = \{S \in \mathcal{P}_C(D) \mid S \cap O \neq \emptyset\}$ and $S_O = \{S \in \mathcal{P}_C(D) \mid S \cap O \neq \emptyset\}, O \in \Omega D$. The proof proceeds like the ones above.

These results assert that the propositional logic of open sets along with $[\![\cdot]\!]$ and $\langle\cdot\rangle$ express all preconditions (inverse images) on open sets.

When program/function f has codomain $\mathcal{P}_M(D_\perp)$, and $O \in \Omega\mathcal{P}_M(D)$, then $f^{-1}[O]$ remains defined as above for $f : D \to \mathcal{P}_M(D_\perp)$ — the Scott topology on $\mathcal{P}_M(D)$ is exactly the relative topology [30] taken from $\mathcal{P}_M(D_\perp)$.

4.2 Predicate transformers for the powerdomains

The previous theorems justify why [17, 26] can take $[\![f]\!] : \Omega D \to \Omega D$ as the weakest-precondition transformer for $f : D \to \mathcal{P}_U(D)$.

It is less evident that $\langle f\rangle : \Omega D \to \Omega D$ defines a total or partial-correctness transformer for $f : D \to \mathcal{P}_L(D)$. Indeed, $\langle f\rangle\phi \wedge \langle f\rangle\neg\phi$ is satisfiable for program f and predicate (open set), ϕ. But $\langle f\rangle$'s *dual* defines partial correctness: For $f : D \to \mathcal{P}_L(D)$, $O \in \Omega D$, $[\![f]\!] \sim O = \sim\langle f\rangle O$. Thus, the partial correctness of f with respect to ϕ, $wlp(f)\phi$, is defined as $[\![f]\!] \sim(\neg\phi)$, which is the well-defined *closed set*, $\sim\langle f\rangle\neg\phi$.

That is, f is partially correct with respect to ϕ if there is no execution whose output satisfies property $\neg\phi$, where $\neg$ is intuitionistic negation. Since $\perp \notin [\![\neg\phi]\!]$ for all $[\![\phi]\!] \in \Omega D$, a diverging answer is partially correct.

Recall that $\langle f\rangle : \Omega D \to \Omega D$ implies $[\![f]\!] : \mho D \to \mho D$, so we can define a closed-set logic that uses $[\![f]\!]$ with finite disjunction and arbitrary conjunction to form partial-correctness propositions. And since the convex powerdomain, $\mathcal{P}_C(D)$, possesses both $[\![f]\!]$ and $\langle f\rangle$, for $f : D \to \mathcal{P}_C(D)$, we can perform both total and partial correctness reasoning. Dijkstra's claim [4], Page 21, that $wp(f)\phi \equiv wlp(f)\phi \wedge wp(f)\,True$ is expressed as follows:

Proposition 9. $[\![f]\!]\phi = \sim\langle f\rangle\neg\phi \wedge [\![f]\!](\phi \vee \neg\phi)$.

Proof. First, $\sim\langle f\rangle\neg\phi = \sim\{\sigma \mid f(\sigma)\, meets \neg\phi\} = \{\sigma \mid not(f(\sigma)\, meets \neg\phi)\} = \{\sigma \mid \downarrow\phi\, covers\, f(\sigma)\}$. This means that $\{\sigma \mid \downarrow\phi\, covers\, f(\sigma)\} \cap [\![f]\!](\phi \vee \neg\phi) = \{\sigma \mid (\downarrow\phi \cap (\phi \cup \neg\phi))\, covers\, f(\sigma)\} = \{\sigma \mid \phi\, covers\, f(\sigma)\}$.

This result is lifted to nonflat domains — the second conjunct asserts that the (partially defined) answer is sufficient for deciding ϕ.

5 Execution semantics of GCL

Dijkstra's Guarded-Command Language (GCL) is distinguished by its conditional statement, which admits nondeterministic choice. The syntax of GCL goes as follows:

$$[\![\cdot]\!] : Command \to Store \to \mathcal{P}_M(Store_{fail,\perp})$$

$$[\![\texttt{skip}]\!]\sigma = \{\!|\sigma|\!\}$$

$$[\![\texttt{abort}]\!]\sigma = \{\!|fail|\!\}$$

$$[\![C_1; C_2]\!] = [\![C_2]\!]^{\dagger}_{fail,\perp} \circ [\![C_1]\!], \quad \text{where } \begin{matrix} f_{fail,\perp}(\perp) = \{\!|\perp|\!\} \\ f_{fail,\perp}(fail) = \{\!|fail|\!\} \end{matrix}$$

$$[\![\texttt{if}\ (G_i?C_i)_{i\in I}\ \texttt{fi}]\!]\sigma = \begin{cases} \{\!|fail|\!\}, \ \textit{if } \bigwedge_{i\in I}(\sigma \in [\![\neg G_i]\!]). \\ \textit{Otherwise:} \\ \quad \biguplus_{i\in I} \begin{cases} [\![C_i]\!]\sigma, \ \textit{if } \sigma \in [\![G_i]\!] \\ \{\!|\perp|\!\}, \ \textit{if } \sigma \notin [\![G_i]\!] \textit{ and } \sigma \notin [\![\neg G_i]\!] \end{cases} \end{cases}$$

$$[\![\cdot]\!] : Guard \to \Omega Store \qquad \textit{See Figure 3}$$

Fig. 4. Semantics of Guarded-Command Language

$$C : Command \qquad P : PrimitiveCommand \qquad G : Guard$$

$$C ::= P \mid \texttt{skip} \mid \texttt{abort} \mid C_1; C_2 \mid \texttt{if}\ (G_i?C_i)_{i\in I}\ \texttt{fi}$$

Primitive comands, P, include assignment. Guards, G, name open sets and represent boolean-valued test expressions. We add the looping construction, $\texttt{do}\cdot\texttt{od}$, momentarily.

In Chapter 4 [4], Dijkstra explains that a program's execution is nondeterministic and can terminate (with a store) or fail or diverge. Here is a semantics that matches Dijkstra's narrative: As before, we use $\mathcal{P}_M(D)$ to denote the powerdomain generated from preordering $M \subseteq PD \times PD$, for $PD \subseteq \mathcal{P}(D)$.

A program has arity, $Store \to \mathcal{P}_M(Store_{fail,\perp})$, where set-or-domain $Store$ represents "proper" outcomes, and $fail$ and $\perp$ denote failure and divergence, respectively. The ordering within $Store_{fail,\perp}$ is $\perp \sqsubseteq fail \sqsubseteq \sigma$, for all $\sigma \in Store$ (in addition to the ordering internal to $Store$).

Figure 4 gives the semantics of GCL. The semantics of the guarded-if construction, $\texttt{if}\,(G_i?C_i)_{i\in I}\,\texttt{fi}$, expresses that the outcome may be any C_k such that G_k is decided true. If all guards, G_i, are decided false, then the construction fails. If any guard can diverge, so can the if-construction.

We treat the iteration construction, $\texttt{do}\cdot\texttt{od}$, as this recursively defined $\texttt{if}\cdot\texttt{fi}$ construction, interpreting it with the usual least-fixed-point semantics [6]:

$$\texttt{do}\,(G_i?C_i)_{i\in I}\,\texttt{od} \equiv w, \quad \textit{where } w \equiv \texttt{if}\,(G_i?C_i; w)_{i\in I}\ (\textstyle\bigwedge_{i\in I} \neg G_i?\texttt{skip})\,\texttt{fi}$$

The Scott-continuity of the above denotational semantics is immediate, except for the $\texttt{if}\cdot\texttt{fi}$ construction:

Proposition 10. *$[\![\texttt{if}\,(G_i?C_i)_{i\in I}\,\texttt{fi}]\!]$ is well defined, that is, it has arity $Store \to \mathcal{P}_M(Store_{fail,\perp})$, and it is Scott-continuous.*

Proof. First, a cases analysis on the possible outcomes of $[\![G_i]\!]\sigma$, for all $i \in I$, shows that the empty set is never an outcome, so the construction is well defined.

Next, monotonicity is verified by checking the possible outcomes of $[\![G_i]\!]\sigma_j$, for $j \in \{0,1\}$, $\sigma_0 \sqsubseteq_{Store} \sigma_1$. (Note that $\{\!|\ \bot\ |\!\}$ is the least element.)

For continuity, consider the outcomes of $[\![\texttt{if}\ (G_i?C_i)_{i\in I}\ \texttt{fi}]\!](\sqcup S)$, for directed set, $S \subseteq Store$: *(i)* If the outcome is $\{\!|fail|\!\}$, then it is the same for $\sqcup_{\sigma\in S}[\![\texttt{if}\ (G_i?C_i)_{i\in I}\ \texttt{fi}]\!]\sigma$, because $\bigcap_{i\in I}[\![\neg G_i]\!]$ is a Scott-open set (and $\{\!|\ \bot\ |\!\}$ is least). *(ii)* If the outcome includes $\{\!|\ \bot\ |\!\}$, then so must $\sqcup_{\sigma\in S}[\![\texttt{if}\ (G_i?C_i)_{i\in I}\ \texttt{fi}]\!]\sigma$, because $\{\!|\ \bot\ |\!\}$ is least. *(iii)* Finally, when $[\![C_i]\!](\sqcup S)$ is included in the outcome, so must be $\sqcup_{\sigma\in S'}[\![C_i]\!]\sigma$, for some "tail", S', of S. By the continuity of $[\![C_i]\!]$, $[\![C_i]\!](\sqcup S) = \sqcup_{\sigma\in S'}[\![C_i]\!]\sigma$.

The semantics in Figure 4 can be used with each of the three canonical powerdomains. Consider these example programs, where $[\![\texttt{True}]\!] = Store$:

1. $[\![\texttt{if}\ (\texttt{True?skip})\ (\texttt{True?abort})\ \texttt{fi}]\!]\sigma = \{\!|\sigma|\!\} \uplus \{\!|fail|\!\}$
2. $[\![\texttt{if True?skip fi}]\!]\sigma = \{\!|\sigma|\!\}$
3. $[\![\texttt{if True?abort fi}]\!]\sigma = \{\!|fail|\!\}$

For the powerdomains,

- $\mathcal{P}_L(Store_{fail,\bot})$'s elements denote "what may be achievable." Examples 1 and 2 above have the same denotation, that is, $[\{\sigma, fail\}]_L = [\{\sigma\}]_L$. Any ordering $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$ uses $\langle\,\cdot\,\rangle$ to define partial-correctness behavior.
- $\mathcal{P}_U(Store_{fail,\bot})$'s elements denote "what must be achievable." Examples 1 and 3 above have the same denotation, that is, $[\{\sigma, fail\}]_U = [\{fail\}]_U$. Any ordering $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$ uses $[\,\cdot\,]$ to define total-correctness behavior.
- $\mathcal{P}_C(Store_{fail,\bot})$'s elements denote both "may" and "must" achievability. All three Examples have distinct denotations, and an ordering $(\sqsubseteq_M) \subseteq (\sqsubseteq_C)$ uese both $\langle\,\cdot\,\rangle$ and $[\,\cdot\,]$.

It is tempting to define $\texttt{if}\,(G_0?C_0)\ (G_1?C_1)\cdots\texttt{fi}$ as $(G_0?C_0)\,|\,(G_1?C_1)\,|\cdots$ using these nondeterministic-choice and guard-as-command constructions:

$$[\![C_1 \mid C_2]\!]\sigma = [\![C_1]\!]\sigma \uplus [\![C_2]\!]\sigma \qquad\qquad [\![G]\!]\sigma = \begin{cases} \{\!|\sigma|\!\}, \textit{if } \sigma \in [\![G]\!] \\ \{\!|fail|\!\}, \textit{if } \sigma \in [\![\neg G]\!] \\ \{\!|\ \bot\ |\!\}, \textit{otherwise} \end{cases}$$

An alternative semantics of $[\![G]\!]\sigma$ is that it equals $\{\!|\ \bot\ |\!\}$ (or even $\emptyset$, if allowed) when $\sigma \in [\![\neg G]\!]$. In any case, $[\![\texttt{if}\ (G_i?C_i)_{i\in I}\ \texttt{fi}]\!]$ does *not* equal $[\![|_{i\in I}(G_i;C_i)]\!]$, because of Dijkstra's description of failure.[8] The next section develops the consequences.

5.1 Failure and divergence

In Chapter 4 [4], Dijkstra states that failure is the outcome of an `if·fi` construction when all guards are decided false. What's more, an empty `if·fi` has failure as its outcome and is semantically identical to the `abort` command. Further,

[8] Indeed, on Page 33 of [4], Dijkstra states that a guard is *not* a command.

evaluation of a guard can diverge and in doing so forces the `if · fi` construction to diverge. Dijkstra does *not* state that guards themselves can fail — only commands are indicated to have failure as a behavior.

There are multiple treatments of failure in the literature: For set, *Store*, Plotkin [17] gives a structured-operational semantics of GCL, where failure is a blocked ("stuck") configuration that cannot be written futher. Plotkin ignores failure in his denotational semantics of GCL, equating it with divergence.

Harel [9] maps a program to a computation tree whose paths represent executions. Failure can appear as a leaf in the computation tree, and divergence appears as an infinite path. Individual guards can fail, and `if · fi` fails when all its guards fail. Like Plotkin, Harel assumes that a guard never diverges. Harel's modelling of failure prevents him from characterizing $wlp(f)\phi$ as $[f]\phi \cap \langle f \rangle \mathit{True}$, as he had hoped [9], Chapter 5.

Bonsangue's denotational semantics [2] also uses a set *Store* and total guards. A guard's failure is "no output," denoted by the empty set. (His powerdomains include $\emptyset$.) In principle, this should make the semantics of $\texttt{if}\,(G_i ? C_i)_{i \in I}\,\texttt{fi}$ into a union of the semantics of the $G_i; C_i$ pairs, but Bonsangue makes the conditional construction *diverge* when all of its guards fail [2], Section 3.3. This is done because $\emptyset$ is the least value in the lower powerdomain (denoting both failure and divergence); the topmost value in the upper powerdomain (meaning it belongs to all open sets of the powerdomain — possessing all possible properties — which is unacceptable for failure); and an isolated element in the convex powerdomain (meaning that logical negation in the powerdomain is neither set complement nor intuitionistic negation).

If failure, *fail*, is a "stuck configuration" that "aborts" [4], Page 34, then we have the ordering, $\bot \sqsubseteq \mathit{fail} \sqsubseteq \sigma$, for all $\sigma \in \mathit{Store}$, which we use for the domain $\mathit{Store}_{\mathit{fail},\bot}$. Thus, *fail* never interferes with any Scott-open set (predicate) in $\Omega\mathit{Store}$ and never interferes with the characterizations of inverse image in Theorems 6-8. This also explains why Plotkin conveniently "merged" *fail* with $\bot$ in his denotational semantics of GCL.

6 Correctness of Dijkstra's laws

Here are Dijkstra's five properties for *wp* [4], Chapters 4,5,9, stated and proved in terms of $[\cdot]$ and $\langle \cdot \rangle$. For domain *Store*, predicates $\phi, \psi \in \Omega\mathit{Store}$, and program $f : \mathit{Store} \to \mathcal{P}_M(\mathit{Store}_{\mathit{fail},\bot})$:

Proposition 11. *When* $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$*:*

1. $[f]\emptyset = \emptyset$.
2. $(\phi \supset \psi) = \mathit{Store}$ *implies* $([f]\phi \supset [f]\psi) = \mathit{Store}$
3. $[f](\phi \wedge \psi) = [f]\phi \wedge [f]\psi$
4. $[f]\phi \vee [f]\psi \subseteq [f](\phi \vee \psi)$*;*
5. *For all directed families* $S \subseteq \Omega\mathit{Store}$, $[f](\bigvee S) = \bigvee_{O \in S}([f]O)$

When $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$*:*

1. $\langle f\rangle\emptyset = \emptyset$
2. $(\phi \supset \psi) = \mathit{Store}$ *implies* $(\langle f\rangle\phi \supset \langle f\rangle\psi) = \mathit{Store}$.
3. $\langle f\rangle(\phi \vee \psi) = \langle f\rangle\phi \vee \langle f\rangle\psi$
4. $\langle f\rangle(\phi \wedge \psi) \subseteq \langle f\rangle\phi \wedge \langle f\rangle\psi$
5. *For all directed families* $S \subseteq \Omega\mathit{Store}$, $\langle f\rangle(\bigvee S) = \bigvee_{O\in S}(\langle f\rangle O)$

Proof. We state the proofs for $[\,\cdot\,]$; the ones for $\langle\,\cdot\,\rangle$ are similar.
(1) is immediate, since $f(\sigma)$ is a nonempty set.
(2) When $\phi \supset \psi = \mathit{Store}$, this implies $\phi \subseteq \psi$, because $\phi \supset \psi = \bigcup\{O \in \Omega\mathit{Store} \mid O \cap \phi \subseteq \psi\}$. This equals *Store*, which is an open set, so $\mathit{Store} \cap \phi \subseteq \psi$, implying $\phi \subseteq \psi$. By monotonicity of $[f]$, $[f]\phi \subseteq [f]\psi$. Next, we must prove for all $\sigma \in \mathit{Store}$, $\sigma \in \bigcup\{O \in \Omega\mathit{Store} \mid O \cap [f]\phi \subseteq [f]\psi\}$, that is, we must find some $O_\sigma \in \Omega\mathit{Store}$ so that $O_\sigma \cap [f]\phi \subseteq [f]\psi$. Choose $O_\sigma = \mathit{Store}$, and this yields the result.
(3)-(5) have been proved earlier, as Propositions 2 and 3.

Dijkstra's laws for GCL are expressed and proved as follows:

Theorem 12. *For domain Store, property* $\phi \in \Omega\mathit{Store}$*, and program* $f : \mathit{Store} \to \mathcal{P}_M(\mathit{Store}_{\mathit{fail},\perp})$*: When* $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$*:*

1. $[\mathtt{skip}]\phi = \phi$
2. $[\mathtt{abort}]\phi = \emptyset$
3. $[C_1; C_2]\phi = [C_1]([C_2]\phi)$
4. $[\mathtt{if}\ (G_i?C_i)_{i\in I}\ \mathtt{fi}]\phi = (\bigwedge_{i\in I}(G_i \vee \neg G_i)) \wedge (\bigvee_{i\in I} G_i) \wedge (\bigwedge_{i\in I}(G_i \supset [C_i]\phi))$

When $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$*:*

1. $\langle\mathtt{skip}\rangle\phi = \phi$
2. $\langle\mathtt{abort}\rangle\phi = \emptyset$
3. $\langle C_1; C_2\rangle\phi = \langle C_1\rangle(\langle C_2\rangle\phi)$
4. $\langle\mathtt{if}\ (G_i?C_i)_{i\in I}\ \mathtt{fi}\rangle\phi = \bigvee_{i\in I}(G_i \wedge \langle C_i\rangle\phi)$

Proof. Proofs are given for $[\,\cdot\,]$; the ones for $\langle\,\cdot\,\rangle$ are similar.
(1) $[\mathtt{skip}]\phi = \{\sigma \mid \phi \mathit{\ covers\ } [\![\mathtt{skip}]\!]\sigma\} = \{\sigma \mid \phi \mathit{\ covers\ } \{\!|\sigma|\!\}\} \supseteq \phi$. If $\sigma' \notin \phi$, then it is not the case that ϕ *covers* $\{\!|\sigma'|\!\}$.
(2) $[\mathtt{abort}]\phi = \{\sigma \mid \phi \mathit{\ covers\ } [\![\mathtt{abort}]\!]\sigma\} = \{\sigma \mid \phi \mathit{\ covers\ } \{\!|\mathit{fail}|\!\}\} = \emptyset$.
(3) The cases when $\perp$ and *fail* arise are straightforward. Now consider $[C_1; C_2]\phi = \{\sigma \mid \phi \mathit{\ covers\ } [\![C_2]\!]^\dagger([\![C_1]\!]\sigma)\} = \{\sigma \mid \phi \mathit{\ covers\ } [\bigcup_{\sigma'\in[\![C_1]\!]\sigma}([\![C_2]\!]\sigma')]_M\} = \{\sigma \mid \forall\sigma' \in [\![C_1]\!]\sigma, \phi \mathit{\ covers\ } [\![C_2]\!]\sigma'\}$. But then, $[C_1]([C_2]\phi) = [C_1]\{\sigma' \mid \phi \mathit{\ covers\ } [\![C_2]\!]\sigma'\} = \{\sigma \mid \{\sigma' \mid \phi \mathit{\ covers\ } [\![C_2]\!]\sigma'\} \mathit{\ covers\ } [\![C_1]\!]\sigma\} = \{\sigma \mid \forall\sigma' \in [\![C_1]\!]\sigma, \phi \mathit{\ covers\ } [\![C_2]\!]\sigma'\}$.
(4) (outline): $\bigwedge_{i\in I}(G_i \vee \neg G_i)$ ensures that all guards are decidable so that $\perp$ is not an outcome. $(\bigvee_{i\in I} G_i)$ ensures that *fail* is not an outcome. For all $\sigma \in \mathit{Store}$, when $\sigma \in [\![G_i]\!]$, then $\sigma \in [C_i]\phi$ must hold, which is $(G_i \supset [C_i]\phi)$.

The weakest-liberal-precondition transformer for the conditional is

Corollary 13. $\sim\langle\mathtt{if}\ (G_i?C_i)_{i\in I}\ \mathtt{fi}\rangle\neg\phi = \bigwedge_{i\in I}(\sim G_i \vee \sim\langle C_i\rangle\neg\phi) = \bigwedge_{i\in I}(\sim G_i \vee [C_i] \sim(\neg\phi))$.

Here is the semantics of $\texttt{do} \cdot \texttt{od}$, simplified to use one clause in its body:

$$\texttt{do}\ G?C\ \texttt{od} \equiv w,\ \textit{where}\ w \equiv \texttt{if}\ (G?C; w)(\neg G?\texttt{skip})\ \texttt{fi}$$

$$[\![w]\!] = \bigsqcup_{j\geq 0} f_j,\ \textit{where}\ \begin{array}{l} f_0\sigma = \bot \\ f_{j+1}\sigma = \begin{cases} f_j^\dagger([\![C]\!]\sigma),\ \textit{if}\ \sigma \in [\![G]\!] \\ \{\!|\sigma|\!\},\ \textit{if}\ \sigma \in [\![\neg G]\!] \\ \{\!|\ \bot\ |\!\},\ \textit{otherwise} \end{cases} \end{array}$$

Therefore, when $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$:

$$[w]\phi = \bigcup_{j\geq 0} [f_j]\phi,\ \textit{where}\ \begin{array}{l} [f_0]\phi = \emptyset \\ [f_{j+1}]\phi = (G \vee \neg G) \wedge (G \supset [C; f_j]\phi) \wedge (\neg G \supset \phi) \end{array}$$

When $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$:

$$\langle w\rangle\phi = \bigcup_{j\geq 0} \langle f_j\rangle\phi,\ \textit{where}\ \begin{array}{l} \langle f_0\rangle\phi = \emptyset \\ \langle f_{j+1}\rangle\phi = (G \wedge \langle C; f_j\rangle\phi) \vee (\neg G \wedge \phi) \end{array}$$

The weakest-liberal-precondition transformer for the loop is

$$\sim\langle w\rangle\neg\phi = \bigcap_{j\geq 0} \sim\langle f_j\rangle\neg\phi = \bigcap_{j\geq 0} [f_j] \sim(\neg\phi)$$

7 Conclusion

Acknowledgements: Hanne Riis Nielson and Flemming Nielson have been friends and inspirational colleagues for many decades, and this paper, based on material that I first learned in Edinburgh in 1982-83 when all three of us were resident there, is dedicated to them. I also thank Mike Smyth for his clear, intuitive papers and explanations.

References

1. S. Abramsky. Domain theory in logical form. *Ann.Pure Appl.Logic*, 51:1–77, 1991.
2. M. Bonsangue. Topological duality in semantics. *Electr. Notes Theor. Comput. Sci.*, 8:1–274, 1998.
3. J. de Bakker. *Mathematical Theory of Program Correctness*. Prentice Hall, 1980.
4. E.W. Dijkstra. *A Discipline of Programming*. Prentice Hall, 1976.
5. G. Gierz, K. Hoffmann, K. Keimel, J. Lawson, M. Mislove, and D. Scott. *Continuous Lattices and Domains*. Cambridge Univ. Press, 2003.
6. I. Guessarian. *Algebraic Semantics*. Springer LNCS 99, 1981.
7. C. Gunter. *Semantics of Programming Languages*. MIT Press, 1992.
8. C. Gunter and D.S. Scott. Semantic domains. In *Handbook of Theoretical Computer Science, Vol. B*, pages 633–674. MIT Press, 1991.
9. D. Harel. *First-Order Dynamic Logic*. Springer LNCS 68, 1979.
10. R. Heckmann. *Power domain constructions*. PhD thesis, Univ. Saarbrücken, 1990.
11. R. Heckmann. Set domains. In *Proc. European Symp. Programming*, LNCS, pages 177–196. Springer Verlag, 1990.

12. M. Main. A powedomain primer. Technical report, Univ. Colorado CU-CS-375-87 and Bull. EATCS, 1987.
13. R. Milne and C. Strachey. *A Theory of Programming Language Semantics*. Chapman and Hall, 1976.
14. H.R. Nielson and F. Nielson. *Principles of Program Analysis*. Springer, 1999.
15. H.R. Nielson, F. Nielson, and C. Hankin. *Semantics with Applications*. Wiley, 1992.
16. G. Plotkin. A powerdomain construction. *SIAM J. Computing*, 5(3):452–487, 1976.
17. G. Plotkin. Dijkstra's predicate transformers and Smyth's powerdomains. In *Abstract Software Specifications*, LNCS. Springer Verlag, 1980.
18. G. Plotkin. Domains. Lecture notes, Univ. Pisa/Edinburgh, 1983.
19. J.C. Reynolds. Notes on a lattice-theoretic approach to the theory of computation. Technical report, Computer Science, Syracuse University, 1972.
20. D.A. Schmidt. *Denotational Semantics*. Allyn and Bacon, 1986.
21. D.A. Schmidt. Abstract interpretation from a topological perspective. In *Static Analysis Symposium*, LNCS 5673, pages 293–308. Springer, 2009.
22. D.S. Scott. Continuous lattices. In *Proc. Dalhousie Conf.*, LNM 274, pages 97–136. Springer Lecture Notes in Mathematics, 1972.
23. D.S. Scott. Lectures on a mathematical theory of computation. Technical report prg-19, Programming Research Group, Oxford University, 1980.
24. M.B. Smyth. Effectively given domains. *Theoretical Comp. Sci.*, 5:257–274, 1977.
25. M.B. Smyth. Power domains. *J. Comput. Syst. Sci.*, 16(1):23–36, 1978.
26. M.B. Smyth. Powerdomains and predicate transformers: a topological view. In *Proc. ICALP'83*, LNCS 154, pages 662–675. Springer, 1983.
27. J. Stoy. *Denotational Semantics*. MIT Press, 1977.
28. D. van Dalen. Intuitionistic logic. In *Handbook of Philosophical Logic, Vol. III*, pages 225–340. Kluwer, 1986.
29. S. Vickers. *Topology via Logic*. Cambridge Univ. Press, 1989.
30. S. Willard. *General Topology*. Dover Publications, 2004.
31. G. Winskel. *Formal Semantics of Programming Languages*. MIT Press, 1993.

Appendix

Assume D is a domain, ΩD its Scott topology, and $PD \subseteq \mathcal{P}(D)$. Recall that $[S]_U \sqsubseteq_U [T]_U$ iff for all $O \in \Omega D, S \subseteq O$ *implies* $T \subseteq O$. The following is an unproved exercise in [18] that is useful here:

Lemma 14. $[S]_U \sqsubseteq_U [T]_U$ *iff for every* $t \in T$*, there exists* $s \in S$ *such that* $s \sqsubseteq_D t$*.*

Proof. Only if: assume $S \subseteq O$ implies $T \subseteq O$ but also that there is some $t_0 \in T$ for which no $s \in S$ satisfies $s \sqsubseteq_D t_0$. Since $\downarrow\{t_0\}$ is a closed set, then $\sim(\downarrow\{t_0\})$ is open and covers S. But T is not covered by this open set, which is a contradiction. If: Assume $S \subseteq O$. Since O is up-closed, it is immediate that $T \subseteq O$ as well.

Let $(\sqsubseteq_M) \subseteq PD \times PD$ generate the powerdomain, $\mathcal{P}_M(D) = (PD/M, \subseteq_M)$, where PD consists of compact sets.

Lemma 15. *If* $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$*, then* $\{E \in \mathcal{P}_M(D) \mid O \,\mathit{covers}\, E\}$*, for* $O \in \Omega D$*, is an open set in the Scott topology,* $\Omega\mathcal{P}_M(D)$*.*

Proof. The set is up-closed because, when $[S]_M \sqsubseteq_M [T]_M$ and $S \subseteq O$, then for every $t \in T$ there is some $s \in S \cap O$ such that $s \sqsubseteq_D t$. Since O is up-closed, $T \subseteq U$.

The set is closed under "directed tails": Assume O *covers* $\bigsqcup_{i\in I}[S_i]_M$. Assume that no O *covers* $[S_i]_M$ holds, for all $i \in I$. This causes a contradiction: First, for every S_i, there is an element, $s_i \in S_i$, such that $s_i \notin O$. Since $(\sqsubseteq_M) \subseteq (\sqsubseteq_U)$, for every $[S_j]_M \sqsubseteq_M [S_i]_M$, there is some $s_j \in S_j$ such that $s_j \sqsubseteq_D s_i$, where $s_j \notin O$. By the Axiom of Choice, one can construct a directed set, $NO = \{s_i \in S_i \mid s_i \notin O\}$, and we have $\sqcup NO \notin O$.

We now show that $(\bigsqcup_{i\in I}[S_i]_M) \uplus \{\!|NO|\!\}$ is an upper bound of the $([S_i]_M)_{i\in I}$: First, the underlying set is compact, because adding NO preserves compactness. Next, for each $[S_k]_M$, $[S_k]_M = [S_k \cup \{s_k\}]_M = [S_k]_M \uplus [\{s_k\}]_M$. This implies $[S_k]_M \sqsubseteq_M (\bigsqcup_{i\in I}[S_i]_M) \uplus \{\!|NO|\!\}$ by the monotonicity of $\uplus$ and $\{\!|\cdot|\!\}$.

But $\bigsqcup_{i\in I}[S_i]_M \not\sqsubseteq_M (\bigsqcup_{i\in I}[S_i]_M) \uplus \{\!|NO|\!\}$, because there is no $t \in D$ in any set represented by equivalence class $\bigsqcup_{i\in I}[S_i]_M$ such that $t \sqsubseteq_D NO$. This contradicts the existence of the least upper bound.

Let $(\sqsubseteq_M) \subseteq PD \times PD$ generate the powerdomain, $\mathcal{P}_M(D) = (PD/M, \subseteq_M)$.

Lemma 16. *If* $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$*, then* $\{E \in \mathcal{P}_M(D) \mid E \mathit{\ meets\ } O\}$*, for* $O \in \Omega D$*, is an open set in the Scott topology,* $\Omega\mathcal{P}_M(D)$*.*

Proof. The set is up-closed because $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$. The set is proved closed under "directed tails" as follows: Let $(E_i)_{i\in I}$ be a directed subset of $\mathcal{P}_M(D)$. Assume $\bigsqcup_{i\in I} E_i$ *meets* O and assume that no E_i *meets* O holds, for all $i \in I$. We generate a contradiction by constructing a discontinuous function using the powerdomain operations (which are all continuous). First, we observe that for any nontrivial domain D, any nontrivial $\mathcal{P}_M(D)$ must possess at least two distinct elements, A_0 and A_1, such that $A_0 \sqsubset_M A_1$ implying that $A_0 \sqsubset_M A_1 \sqsubseteq_M A_0 \uplus A_1$ (because $(\sqsubseteq_M) \subseteq (\sqsubseteq_L)$). We use these two elements to define this continuous function, $f : D \to \mathcal{P}_M(D)$: $f(d) = \begin{cases} A_1, \textit{ if } d \in O \\ A_0, \textit{ if } d \notin O \end{cases}$. By the definition of powerdomain, there is a continuous function, $f^\dagger : \mathcal{P}_M(D) \to \mathcal{P}_M(D)$, defined as $f^\dagger[S]_M = [\bigcup_{d\in S} F_d]_M$, where $f(d) = [F_d]_M$.

Because $\bigsqcup_{i\in I} E_i$ *meets* O holds, it must be that $f^\dagger(\bigsqcup_{i\in I} E_i) \sqsupseteq_M A_1$. But we assumed that no E_i *meets* O holds, for all $i \in I$, so it must be that $\bigsqcup_{i\in I} f^\dagger(E_i) = \bigsqcup_{i\in I}\{A_0\} = A_0$. Since $A_0 \neq A_1$, this contradicts the continuity of $f^\dagger$.