A multiset logic for Gamma

Francisco Hernández Quiroz*

Abstract

Gamma is a simple parallel programming language whose only data structure is the multiset or bag. In this paper a partial proof system for Gamma programs is presented. Domain theory in logical form is used as the general framework and to this end a multiset logic is introduced. A small example of its application is also found.

1 The Gamma language

The Gamma language is a very simple notation for parallel algorithms. Its basic data structure is the *multiset*. The idea is simple: a *rewriting rule* takes a multiset, checks if the *reaction condition* (a predicate about elements in the multiset) holds, and if so it performs an *action*: replaces some elements in the multiset by others. Rewriting rules can be composed either in parallel or sequentially. In more formal terms:

Definition 1.1 *Let D be a domain and D the finite multisets of elements in this domain. A reaction condition is a predicate $R : D^n \to \{true, false\}$ about (finite-length) tuples of elements in D. An action is a function $A : D^n \to D$. A Gamma program is defined as:*

$$P ::= (x_1, \ldots, x_n) \to A(x_1, \ldots, x_n) \Leftarrow R(x_1, \ldots, x_n) \mid P \circ P \mid P + P.$$

*Thanks to Steve Vickers and Chris Hankin for their help and useful comments for this paper. Carlos Duarte made also valuable remarks about content and structure. This paper is part of my PhD research, sponsored by the National University of Mexico (UNAM).
E-mail address: f.hernandez@ic.ac.uk.

The following example of a Gamma program is taken from [EHJ 93]:

$$\begin{aligned} P_1 &= x \rightarrow \{\text{x-1, x-2}\} \Leftarrow (x > 1) \\ P_2 &= x \rightarrow \{\text{1}\} \Leftarrow (x = 0) \\ P_3 &= (x, y) \rightarrow \{\text{x+y}\} \Leftarrow \mathit{true} \\ P &= P_3 \circ (P_1 + P_2). \end{aligned}$$

If P is applied to $\{\text{n}\}$, it produces the nth Fibonacci number. In section 5 a proof of its correctness will be presented.

2 Transition trace logic

[GH 96] proposed a logic system for verifying Gamma programs. That logic was built using domain theory in logical form (dtlf from now onwards) [Ab 91]. In dtlf every type τ in a programming language is associated with a domain D_τ. Formation rules and axioms are given in order to produce the set of assertions $L(D_\tau)$ and the logical theory $\mathcal{L}(D_\tau)$, which as a whole has the structure of a frame, though its compact open elements form just a lattice. The set of formulas can be regarded as a topological space and its points are the models of the theory.

The first step in the building of the logical system is to find a suitable (domain-theoretic) denotational semantics. [GH 96] used a semantics based in transition traces (an idea proposed by [Br 92] for parallel languages). Though easier to use than previous approaches ([GH 95], [EHJ 93]), some of its rules were provisional while others were not powerful enough for proving general instances of programs.

The denotation of a Gamma program is a set of (finite or infinite) sequences of multiset pairs $(M_1, N_1)(M_2, N_2)\ldots$ meaning that the program transforms the multiset M_1 into N_1, then the multiset M_2 into N_2 and so on.

Definition 2.1 *Let D be a simple type in Gamma. D is the set of finite sequences of state transitions, also called transition traces. An element of D is of the form* $(M_1, N_1)(M_2, N_2)\ldots(M_n, N_n)$ *with* M_i*,* $N_i \in D$*. D is the* set of finite and infinite transition traces. ϵ *refers to the empty sequence.*

Let $\alpha \in D$, $\beta \in D$ and $T \subseteq D$. We say that

i) *T is closed under* absorption *iff $\alpha(M,N)(N,M')\beta \in T$ implies that $\alpha(M, M')\beta \in T$;*

ii) *T is closed under* left-stuttering *iff $\alpha\beta \in T$ and $\beta \neq \epsilon$ implies that $\alpha(M,M)\beta \in T$.*

If T is an arbitrary set of sequences, $\ddagger T$ denotes its closure under absorption and left-stuttering.

A function $\mathbf{m} : (D - \{\epsilon\}) \to \mathcal{P}(D)$ is called an end-synchronised merger *(*ESM*) iff*

a) *$(M,N) \in \mathbf{m}(\alpha,\beta)$ implies that $\alpha = \beta = (M,N)$; and*

b) *$\alpha \in \mathbf{m}(\beta,\gamma)$ implies that $(M.N)\alpha \in \mathbf{m}((M,N)\beta,\gamma)$ and $(M,N)\alpha \in \mathbf{m}(\gamma,(M.N)\beta)$.*

Let $\alpha\beta$ represent the set $\bigcup\{\mathbf{m}(\alpha,\beta) \mid \mathbf{m}$ is an ESM$\}$.

A domain of transition traces (denoted by $\mathbb{T}$) is built and a domain logic $\mathcal{L}(\mathbb{T})$ is derived from it. Elements in $\mathcal{L}(\mathbb{T})$ are assertions about transition traces. If $\gamma \in \mathcal{L}(\mathbb{T})$ and $T \subseteq \mathbb{T}$ then $T \models \diamond\gamma$ iff $t \models \gamma$ for at least a $t \in T$. Denotations of Gamma programs are subsets of $\mathbb{T}$. If P is a program, its denotation is represented by $[\![P]\!]$ and $P \models \diamond\gamma$ iff $[\![P]\!] \models \diamond\gamma$.

$\phi \circ \psi$ is the sequential composition of the assertions ϕ and ψ. $t \models \phi \circ \psi$ iff $t = t_1t_2$ and $t_1 \models \phi$ and $t_2 \models \psi$. The parallel composition of ϕ and ψ is defined as

$$\phi \parallel \psi = \bigwedge_{\theta \in \phi\psi} \theta.$$

Both $\circ$ and $\parallel$ commute with $\diamond$ and $\bigvee$ and are monotone with respect to $\leq$:

$$(\bigvee_i \diamond\phi_i)\circ(\bigvee_j \diamond\psi_j) = \bigvee_{i,j} \diamond(\phi_i \circ \psi_j) \qquad (\bigvee_i \diamond\phi_i) \parallel (\bigvee_j \diamond\psi_j) = \bigvee_{i,j} \diamond(\phi_i \parallel \psi_j).$$

Now if P and Q are Gamma programs we have the following deduction rules:

$$\text{left-stuttering}\ \frac{P \models \diamond(\theta\psi) \quad \psi \neq \mathsf{nil}}{P \models \diamond(\theta(\phi,\phi)\psi)} \qquad \text{absorption}\ \frac{P \models \diamond(a(\phi,\psi)(\psi,\theta)b)}{P \models \diamond(a(\phi,\theta)b)}$$

$$\text{seq. composition}\ \frac{P \models \phi \quad Q \models \psi}{Q \circ P \models \psi \circ \phi} \qquad \text{par. composition}\ \frac{P \models \phi \quad Q \models \psi}{P + Q \models \phi \parallel \psi}.$$

Left-stuttering and absorption are justified by the fact that sets of transition traces are closed under those two operations.

The proofs in [GH 96] relied on two provisional rules whose validity depended on the existence of a multiset logic:

terminal

$$\frac{\phi \Rightarrow \neg R(x_1, \ldots, x_n)}{(A(x_1, \ldots, x_n) \Leftarrow R(x_1, \ldots, x_n)) \models \Diamond(\phi, \phi)}$$

mediator

$$\frac{\phi \Rightarrow R(x_1, \ldots, x_n)\ A(x_1, \ldots, x_n) \Rightarrow \psi\ (A(x_1, \ldots, x_n) \Leftarrow R(x_1, \ldots, x_n)) \models \theta}{(A(x_1, \ldots, x_n) \Leftarrow R(x_1, \ldots, x_n)) \models \Diamond((\phi, \psi)\theta)}.$$

In section 4 we shall be able to prove a restricted version of these rules. Nevertheless —and conditioned on the existence of a multiset logic— [GH 95] and [GH 96] stated the following:

Theorem 2.2 *If P and Q are two Gamma programs then:*

1. If $\ddagger[\![P]\!] \subseteq \ddagger[\![Q]\!]$ then $P \sqsubseteq_O Q$, where $\sqsubseteq_O$ denotes an observational congruence relation as defined in [GH 95].

2. $P \models \phi$ implies $Q \models \phi$ if and only if $\ddagger T[\![P]\!] \subseteq \ddagger T[\![Q]\!]$.

3. If $P \models \phi$ implies $Q \models \phi$ then $P \sqsubseteq_O Q$.

3 Multiset logic

Let D be a domain associated with the logical theory $\mathcal{L}(D)$. We want to define a logic for D. Let D be a geometric theory [Vi 89] whose formation rules and axioms are the following

Formation rules

The subbasic propositions are built from propositions in the logic of the domain:

$$\frac{\phi_1, \ldots, \phi_n \in L(D)}{\Box\{\phi_1, \ldots, \phi_n\} \in L(D)},$$

where the order of the ϕ_i's is not relevant. More complex propositions can be built by finite conjunctions and arbitrary disjunctions:

$$\frac{}{t \in L(D)} \qquad \frac{\phi, \psi \in L(D)}{\phi \wedge \psi \in L(D)} \qquad \frac{\{\phi_i\} \subseteq L(D),}{\bigvee\{\phi_i\} \in L(D)} \qquad f = \bigvee \emptyset.$$

We will use the following shorthands:

(D_1) if $\phi \in L(D)$ then $\phi^n =_{def} \{\!\!\{\underbrace{\phi, \ldots, \phi}_{n \text{ times}}\}\!\!\}$

(D_2) $\Diamond\{\!\!\{\phi_1, \ldots, \phi_n\}\!\!\} =_{def} \bigvee_m \Box(\{\!\!\{\phi_1, \ldots, \phi_n\}\!\!\} \uplus t^m).$

General axioms

The general axioms give D the structure of a frame:

$(A_1 \leq -\text{ref})$ $\phi \leq \phi,$ $(A_2 \leq -\text{trans})$ $\dfrac{\phi \leq \psi, \psi \leq \chi}{\phi \leq \chi},$

$(A_3 = -I)$ $\dfrac{\phi \leq \psi, \psi \leq \phi}{\phi = \psi},$ $(A_4 = -E)$ $\dfrac{\phi = \psi}{\phi \leq \psi, \psi \leq \phi},$

$(A_5\, t - I)$ $\phi \leq t,$ $(A_6 \wedge -I)$ $\dfrac{\phi \leq \psi_1, \phi \leq \psi_2}{\phi \leq \psi_1 \wedge \psi_2},$

$(A_7 \wedge -E - L)$ $\phi \wedge \psi \leq \phi,$ $(A_8 \wedge -E - R)$ $\phi \wedge \psi \leq \psi,$

$(A_9 \vee -I)$ $\dfrac{\forall \phi \in \Phi\ \phi \leq \psi}{\bigvee \Phi \leq \psi},$ $(A_{10} \vee -E - R)$ $\dfrac{\phi \in \Phi}{\phi \leq \bigvee \Phi},$

$(A_{11} \wedge -\text{dist})$ $\phi \wedge \bigvee\{\psi_i\}_{i \in I} \leq \bigvee\{\phi \wedge \psi_i\}_{i \in I}.$

Specific axioms

The following are specific axioms for our frame of multisets, where S and T are finite multisets of formulas of $L(D)$ and $\Sigma(n)$ is the set of permutations of n elements:

(A_{12}) $\Box S \wedge \Box T \leq f$ if S $\neq$ T

(A_{13}) $\Box\{\!\!\{\phi_1, \ldots, \phi_n\}\!\!\} \wedge \Box\{\!\!\{\psi_1, \ldots, \psi_n\}\!\!\} \leq \bigvee_{\sigma \in \Sigma(n)} \Box\{\!\!\{\phi_1 \wedge \psi_{\sigma(1)}, \ldots, \phi_n \wedge \psi_{\sigma(n)}\}\!\!\}$

$$(A_{14}) \qquad \Box(S \uplus \{\phi\}) \leq \Box(S \uplus \{\psi\}) \qquad \text{if } \phi \leq \psi$$

$$(A_{15}) \qquad \Box(S \uplus \{\bigvee_i \phi_i\}) \leq \bigvee_i \Box(S \uplus \{\phi_i\}).$$

Theorem 3.1 *The following statements are true:*

a) $\Box t^m \wedge \Diamond\{\phi_1, \ldots, \phi_n\} \leq f$ *if* $m < n$.

b) $\Box(S \uplus \{\bigvee_i \phi_i\}) = \bigvee_i \Box(S \uplus \{\phi_i\})$.

c) $\Diamond(S \uplus \{\bigvee_i \phi_i\}) = \bigvee_i \Diamond(S \uplus \{\phi_i\})$.

Proof. For a) we have:

$$\begin{aligned}
\Box t^m \wedge \Diamond\{\phi_1, \ldots, \phi_n\} &= \Box t^m \wedge \bigvee_k \Box(\{\phi_1, \ldots, \phi_n\} \uplus t^k) && \text{definition} \\
&\leq \bigvee_k \Box t^m \wedge \Box(\{\phi_1, \ldots, \phi_n\} \uplus t^k) && A_{11} \\
&\leq f && \text{by } A_{12} \text{ and hypothesis.}
\end{aligned}$$

From A_{14} and the fact that $\phi_i \leq \bigvee_i \phi_i$ for every i we have $\Box(S \uplus \{\phi_i\}) \leq \Box(S \uplus \{\bigvee_i \phi_i\})$, also for every i. Then $\bigvee_i \Box(S \uplus \{\phi_i\}) \leq \Box(S \uplus \{\bigvee_i\})$. The other direction of the inequality is A_{15} and we get b). c) follows from b) and the definition of $\Diamond$. ■

We also want to define a satisfaction relation between D and D. Let us suppose that the relation $x \models \phi$, with $x \in D$ and $\phi \in L(D)$, has been properly defined.

Definition 3.2 *If* $\{x_1, \ldots, x_n\} \in D$ *and* $\phi_1, \ldots, \phi_n \in L(D)$ *then* $\{x_1, \ldots, x_n\} \models \Box\{\phi_1, \ldots, \phi_n\}$ *iff there exist a* $\sigma \in \Sigma(n)$ *such that* $x_{\sigma(1)} \models \phi_1, \ldots, x_{\sigma(n)} \models \phi_n$.

Theorem 3.3 *For every* $M \in D$*: a) if* $\{x_1, \ldots, x_n\} \models \Box\{\phi_1, \ldots, \phi_n\}$ *then* $M \uplus \{x_1, \ldots, x_n\} \models \Diamond\{\phi_1, \ldots, \phi_n\}$*; b)* $M \models \Box t^m$ *iff* $\mathsf{M} = m$*; c)* $M \models \Diamond t^m$ *iff* $\mathsf{M} \geq m$.

Proof. It is enough to observe that $\{x_1, \ldots, x_n\} \uplus M \models \Box\{\phi_1, \ldots, \phi_n\} \uplus t^k$, where $\mathsf{M} = k$. Then $M \models \bigvee_m \Box(\{\phi_1, \ldots, \phi_n\} \uplus t^m = \Diamond\{\phi_1, \ldots, \phi_n\}$. The other properties follow trivially from this and the definition of $\models$. ■

Theorem 3.4 *For every M, if $\phi \leq \psi$ and $M \models \phi$ then $M \models \psi$.*

Proof. If $\phi \leq \psi$ depends on axioms A_1–A_{11} the theorem is clearly because of the general theory and it only remains to be proved for axioms A_{12}–A_{15}.

For axiom A_{12} we have $\phi = \Box S \wedge \Box T$ and $\psi = f$. But no $M \in D$ can satisfy simultaneously $\Box S$ and $\Box T$ if $\mathsf{S} \neq \mathsf{T}$, and the theorem holds by vacuity.

With A_{13}, now $\phi = \Box\{\phi_1, \ldots, \phi_n\} \wedge \Box\{\psi_1, \ldots, \psi_n\}$ and $\psi = \bigvee_{\sigma \in \Sigma(n)} \Box\{\phi_1 \wedge \psi_{\sigma(1)}, \ldots, \phi_n \wedge \psi_{\sigma(n)}\}$. Let us suppose that $\{x_1, \ldots, x_n\} \models \phi$, ie, $x_1 \models \phi_{\sigma_1(1)}, \ldots x_n \models \phi_{\sigma_1(1)}$ and $x_1 \models \psi_{\sigma_2(1)}, \ldots x_n \models \psi_{\sigma_2(n)}$. Then $x_1 \models \phi_{\sigma_1(1)} \wedge \psi_{\sigma_2(1)}, \ldots, x_n \models \phi_{\sigma_1(n)} \wedge \psi_{\sigma_2(n)}$. In other words $\{x_1, \ldots, x_n\} \models \psi$.

Regarding A_{14}, if $M \models \Box(S \uplus \{\phi\})$ then $M = \{x_1, \ldots, x_n\}$ such that $\{x_1, \ldots, x_{n-1}\} \models \Box S$ and $x_n \models \phi$. Hence $x_n \models \psi$. Consequently $M \models \Box(S \uplus \{\psi\})$.

Finally if $M \models \Box(S \uplus \{\bigvee_i \phi_i\})$ then again $M = \{x_1, \ldots, x_n\}$, with $\{x_1, \ldots, x_{n-1}\} \models \Box S$ and $x_n \models \bigvee_i \phi_i$. Therefore $x_n \models \phi_i$ for some i and then $M \models \Box(S \uplus \{\phi_i\})$ for the same i, which leads directly to the desired conclusion. ■

3.1 A locale for the logic

We still do not know if D corresponds to the points of the logic previously defined, ie, the points in D might be something different to finite multisets. Therefore it would be worth to see what the points of the logic look like. Consider the locale Loc_D whose frame of opens is D. A possible way to see true-kernels of elements in $\mathsf{pt}\,D$ is as *completely prime filters* of D (lemma 5.4.6 in [Vi 89]).

D is sound, ie, if $\phi \leq \psi$ then $\phi \in \mathcal{M}$ implies $\psi \in \mathcal{M}$. What about the inverse: is the logic complete?

If we are able to prove coherence of D completeness will come from a general theorem. Consider first what the compact elements in D should look like. If $a \in \mathcal{K}D$ then for every B such that $a \leq \bigvee B$ there exist a finite $B' \subseteq B$ such that $a \leq \bigvee B'$. That is, we are excluding infinite disjunctions and as a consequence the operator $\Diamond$. Every $a \in \mathcal{K}D$ should be a finite conjunction or disjunction of propositions of the form $\Box\{a_1, \ldots, a_n\}$. In the following K_α will denote the set $\{a \mid a \text{ is compact and } a \leq \alpha\}$, where a, α belong either to $L(D)$ or $L(D)$.

Theorem 3.5 *If* $\Box\{a_1, \ldots, a_n\} \in \mathcal{K}D$ *then each of the* a_i*'s is compact in* $\mathcal{L}(D)$*.*

Proof. Suppose $\Box\{a_1, \ldots, a_n\} \in \mathcal{K}D$ but there is a non-compact a_i, that is there exist a directed set $B \subseteq L(D)$ such that $a_i \leq \bigvee^{\uparrow} B$ and $a_i \leq b$ for no $b \in B$ (where $\bigvee^{\uparrow}$ emphasizes the fact that it is a directed join). Consider now the set $B' = \{\Box\{a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n\} \mid b \in B\}$. By A_{14} B' is directed like B. According to A_{15}

$$\begin{aligned}\Box\{a_1, \ldots, a_n\} &\leq \Box\{a_1, \ldots, a_{i-1}, \bigvee\nolimits^{\uparrow} B, a_{i+1}, \ldots, a_n\} \\ &\leq \bigvee_{b \in B}^{\uparrow} \Box\{a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n\} \\ &= \bigvee^{\uparrow} B'.\end{aligned}$$

However, there is no $b' \in B'$ such that $\Box\{a_1, \ldots, a_n\} \leq b'$, which contradicts our assumptions that $\Box\{a_1, \ldots, a_n\}$ was compact. Therefore all a_i's are compact. ■

Theorem 3.6 *D is coherent, that is,* $\mathcal{K}D \simeq D$*.*

Proof. We need to find two frame homomorphisms $h_1 : \mathcal{K}D \to D$ and $h_2 : D \to \mathcal{K}D$ such that $h_1 \circ h_2 = Id_{\mathcal{K}D}$ and $h_2 \circ h_1 = Id_D$. As $\mathcal{K}D \subseteq D$ let h_1 be the inclusion function, and define

$$h_2(\Box\{\alpha_1, \ldots, \alpha_n\}) = \bigvee_{a_i \in K_{\alpha_i}}^{\uparrow} \Box\{a_1, \ldots, a_n\}.$$

h_1 is a frame isomorphism as it preserves relations in A_{12}–A_{15}. Regarding

h_2, let $m \neq n$. Then

$$
\begin{aligned}
h_2(\Box\{\alpha_1,\ldots,\alpha_n\} \wedge \Box\{\beta_1,\ldots,\beta_m\}) &= \bigvee^{\uparrow}_{\substack{a_i \in K_{\alpha_i}\\ b_i \in K_{\beta_i}}} (\Box\{a_1,\ldots,a_n\} \wedge \Box\{b_1,\ldots,b_m\}) \\
&\leq \bigvee^{\uparrow}_{\substack{a_i \in K_{\alpha_i}\\ b_i \in K_{\beta_i}}} f \\
&= f = h_2(f)
\end{aligned}
$$

which proves h_2 respects A_{12}. With respect to A_{13}:

$$
\begin{aligned}
&h_2(\Box\{\alpha_1,\ldots,\alpha_n\} \wedge \Box\{\beta_1,\ldots,\beta_n\}) \\
&\qquad = \bigvee^{\uparrow}_{\substack{a_i \in K_{\alpha_i}\\ b_i \in K_{\beta_i}}} (\Box\{a_1,\ldots,a_n\} \wedge \Box\{b_1,\ldots,b_n\}) \\
&\qquad \leq \bigvee^{\uparrow}_{\substack{a_i \in K_{\alpha_i}\\ b_i \in K_{\beta_i}}} \bigvee_{\sigma \in \Sigma(n)} \Box\{a_1 \wedge b_{\sigma(1)},\ldots,a_n \wedge b_{\sigma(n)}\}
\end{aligned}
$$

On the other hand, $a_i \in K_{\alpha_i}$ and $b_{\sigma(i)} \in K_{\beta_{\sigma(i)}}$ and hence $a_i \wedge b_{\sigma(i)} \in K_{\alpha_i \wedge \beta_{\sigma(i)}}$, which means:

$$
\begin{aligned}
&\leq \bigvee^{\uparrow}_{c_i \in K_{\alpha_i \wedge \beta_{\sigma(i)}}} \bigvee_{\sigma \in \Sigma(n)} \Box\{c_1,\ldots,c_n\} \\
&= h_2(\bigvee_{\sigma \in \Sigma(n)} \Box\{\alpha_1 \wedge \beta_{\sigma(1)},\ldots,\alpha_n \wedge \beta_{\sigma(n)}\}).
\end{aligned}
$$

Axiom A_{14} is easier. If $\alpha_{n+1} \leq \beta$

$$
\begin{aligned}
h_2(\Box(\{\alpha_1,\ldots,\alpha_n\} \uplus \{\alpha_{n+1}\})) &= \bigvee^{\uparrow}_{a_i \in K_{\alpha_i}} \Box(\{a_1,\ldots,a_n\} \uplus \{a_{n+1}\}) \\
&\leq \bigvee^{\uparrow}_{\substack{a_i \in K_{\alpha_i}\\ b \in K_{\beta}}} \Box(\{a_1,\ldots,a_n\} \uplus \{b\}) \\
&= h_2(\{\alpha_1,\ldots,\alpha_n\} \uplus \{\beta\}).
\end{aligned}
$$

Finally we will check A_{15}

$$
\begin{aligned}
h_2(\Box(\{\alpha_1,\dots,\alpha_n\} \uplus \{\textstyle\bigvee_j \beta_j\})) &= \bigvee^{\uparrow}_{\substack{a_i\in K_{\alpha_i}\\ b\in K_{\bigvee_j \beta_j}}} \Box(\{a_1,\dots,a_n\} \uplus \{b\}) \\
&\leq \bigvee^{\uparrow}_{\substack{a_i\in K_{\alpha_i}\\ b_j\in K_{\beta_j}}} \bigvee_j \Box(\{a_1,\dots,a_n\} \uplus \{b_j\}) \\
&= h_2(\bigvee_j \Box(\{\alpha_1,\dots,\alpha_n\} \uplus \{\beta_j\}))
\end{aligned}
$$

Consider now the composition of h_1 and h_2:

$$
\begin{aligned}
h_2 \circ h_1(\Box\{a_1,\dots,a_n\}) &= h_2(\Box\{a_1,\dots,a_n\}) \\
&= \bigvee^{\uparrow}_{\bar{a}_i\in K_{a_i}} \Box\{\bar{a}_1,\dots,\bar{a}_n\} \\
&= \Box\{a_1,\dots,a_n\} \qquad \text{as each } a_i \text{ is compact.} \\
h_1 \circ h_2(\Box\{\alpha_1,\dots,\alpha_n\}) &= h_1(\bigvee^{\uparrow}_{a_i\in K_{\alpha i}} \Box\{a_1,\dots,a_n\}) \\
&= \Box\{\alpha_1,\dots,\alpha_n\} \qquad \text{as } \mathcal{L}(D) \text{ is algebraic.} \qquad \blacksquare
\end{aligned}
$$

Theorem 3.7 *(Completeness of D) If for all* $\mathcal{M} \in \mathsf{pt}\,D$, $\mathcal{M} \models \phi$ *implies* $\mathcal{M} \models \psi$ *then* $\phi \leq \psi$.

Proof. As D is coherent, then Loc_D is spectral. Then, according to [Vi 89] 9.2.4 is also spatial. Then the theorem derives from [Vi 89] 5.3.5. ■

As a nice additional result we have that $\langle \mathsf{pt}\,D, \sqsubseteq \rangle$ is directed cocomplete (7.3.1 and 7.3.2 in [Vi 89]).

The next task is to relate points in $\mathsf{pt}\,D$ to multisets in D. It is not difficult to define a one-to-one function $f : D \to \mathsf{pt}\,D$ in the following way: $f(M) = \mathcal{M}$ such that $M \models \alpha$ iff $\alpha \in \mathcal{M}$ (this function also induces a partial order on D, viz. $M_1 \leq M_2$ iff $f(M_1) \subseteq f(M_2)$). In other words, $\mathsf{pt}\,D$ contains enough points to reflect the structure of D, but it might contain additional objects. The existence of one-to-one function from $\mathsf{pt}\,D$ to D is yet to be proved.

4 Adding to Gamma logic

Once we have an acceptable multiset logic we want to prove properties of Gamma programs. Remember that two important deduction rules were provisional in the proof system proposed in section 2. Now it is possible to prove them, though for a restricted set of reaction conditions.

Definition 4.1 *Let $R(x_1, \ldots, x_n)$ be a reaction condition and $A = \{\!\{f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\}\!\}$ an action.*

1. *R is unary expressible iff it is equivalent to a conjunction of unary predicates $P_1(x_1)$, $\ldots$, $P_n(x_n)$.*
2. *If $P(x)$ is a unary predicate let ψ_P be a formula in $\mathcal{L}(D)$ such that $P(x)$ holds iff $x \models \psi_P$. If $R(x_1, \ldots, x_n) = P_1(x_1) \wedge \cdots \wedge P_n(x_n)$ then $\psi_R = \Diamond\{\!\{\psi_{P_1}, \ldots, \psi_{P_n}\}\!\}$.*
3. *If $f : D^n \to D$ is a function, then $P_{f(x_1,\ldots,x_n)}$ is a unary predicate such that $P_{f(x_1,\ldots,x_n)}(x)$ holds iff $x = f(x_1, \ldots, x_n)$.*
4. *If $p = (k - n) + m$ and $\phi = \Box\{\!\{\phi_1, \ldots, \phi_k\}\!\} \leq \psi_R$ then $M_{A\Leftarrow R}(\phi) = \{\Box\{\!\{\gamma_1, \ldots, \gamma_p\}\!\} \mid \{\!\{\gamma_1, \ldots, \gamma_p\}\!\} = (\{\!\{\phi_1, \ldots, \phi_k\}\!\} - \{\!\{\phi_{i_1} \leq \psi_{P_1}, \ldots, \phi_{i_n} \leq \psi_{P_n}\}\!\}) \uplus \{\!\{\psi_{P_{f_1(x_1,\ldots,x_n)}}, \ldots, \psi_{P_{fm(x_1,\ldots,x_n)}}\}\!\}\}$.*

Using these definitions and what we know about D we can prove a version of the terminal and mediator rules for Gamma.

Theorem 4.2 *Let $A \Leftarrow R$ be a Gamma rewriting rule (where R is unary expressible) and $\phi = \Box\{\!\{\phi_1, \ldots, \phi_n\}\!\}$. Then the following rules are sound:*

$$\textit{mediator}\ \frac{\phi \leq \psi_R,\ \gamma \in M_{A\Leftarrow R}(\phi),\ (A \Leftarrow R) \models \Diamond\theta}{(A \Leftarrow R) \models \Diamond((\phi, \gamma)\theta)}$$
$$\textit{terminal}\ \frac{\phi \wedge \psi_R \leq f}{(A \Leftarrow R) \models \Diamond(\phi, \phi)}.$$

Proof. As the logic is complete, we know that $\mathcal{M} \in \mathsf{pt}D \models \phi$ implies $\mathcal{M} \models \psi_R$ iff $\phi \leq \psi_R$. This and dtlf framework give us the completeness of these rules. Their soundness comes from theorem 2.2. ■

5 The logic at work

[GH 96] proved a particular instance of the Gamma example of section 1. However, in that example it was assumed without proof the correctness of rules mediator and terminal. We restate that proof using our new multiset logic.

In this case $\psi_{P_1} = \Diamond\{x > 1\}$, $\psi_{P_2} = \Diamond\{x = 0\}$ and $\psi_{P_3} = \Diamond\{t,t\}$. From now onwards '$n$' will be a shorthand for the predicate '$x = n$'. Then we want to prove that $P_3 \circ (P_1 + P_2) \models \Diamond(\Box\{4\}, \Box\{5\})$, as 5 is the 4th Fibonacci number. Our proof has a backward-going flavour:

$P_1 \models \Diamond(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\})$ terminal and $\Box\{1,1,1,1,1\} \wedge \Diamond\{x{>}1\} \leq f$

$P_1 \models \Diamond((\Box\{2,1,1,0\}, \Box\{1,1,1,0,0\})(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\}))$
mediator and $\Box\{2,1,1,0\} \leq \Diamond\{x{>}1\}$ and $\Box\{1,1,1,0,0\} \in M_{P_1}(\Box\{2,1,1,0\})$

$P_1 \models \Diamond((\Box\{4\}, \Box\{3,2\})(\Box\{3,2\}, \Box\{2,2,1\})(\Box\{2,2,1\}, \Box\{2,1,1,0\})$
$(\Box\{2,1,1,0\}, \Box\{1,1,1,0,0\})(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\}))$
mediator repeated several times

$P_1 \models \Diamond((\Box\{4\}, \Box\{1,1,1,0,0\})(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\}))$
absorption repeated

$P_2 \models \Diamond(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\})$ terminal and $\Box\{1,1,1,1,1\} \wedge \Diamond\{0\} \leq f$

$P_2 \models \Diamond((\Box\{1,1,1,0,0\}, \Box\{1,1,1,1,0\})(\Box\{1,1,1,1,0\}, \Box\{1,1,1,1,1\})$
$(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\}))$
mediator, twice

$P_2 \models \Diamond((\Box\{1,1,1,0,0\}, \Box\{1,1,1,1,1\})(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\}))$ absorption

$P_1 + P_2 \models \Diamond((\Box\{4\}, \Box\{1,1,1,0,0\})(\Box\{1,1,1,0,0\}, \Box\{1,1,1,1,1\})$
$(\Box\{1,1,1,1,1\}, \Box\{1,1,1,1,1\}))$
parallel

$P_1 + P_2 \models \Diamond(\Box\{4\}, \Box\{1,1,1,1,1\})$ absorption

$P_3 \models \Diamond(\Box\{1,1,1,1,1\}, \Box\{5\})$ terminal, mediator, absorption

$P_3 \circ (P_1 + P_2) \models \diamond((\Box\{\!\!\{4\}\!\!\}, \Box\{\!\!\{1,1,1,1,1\}\!\!\})(\Box\{\!\!\{1,1,1,1,1\}\!\!\}, \Box\{\!\!\{5\}\!\!\}))$ sequential

$P_3 \circ (P_1 + P_2) \models \diamond(\Box\{\!\!\{4\}\!\!\}, \Box\{\!\!\{5\}\!\!\})$ absorption

■

6 Future work

The proof of soundness and completeness of the logic was made using the localic presentation. However, it was not proved that the points of the locale correspond to the kind of finite multisets used in Gamma programs. In other words, our logic might be talking about some other class of objects.

Additionally, the type of predicates expressible by the logic is somewhat restricted. An extension to general predicates would complicate the bags order and our proofs about its properties would also look too complex. A way of avoiding this should be found.

Finally, as the reader might be aware, the logic can only prove particular instances of programs (in the example of the Fibonacci numbers, the proof only holds for the multiset $\{\!\!\{4\}\!\!\}$). A rule for proving that the program produces the n-th Fibonacci number when applied to $\{\!\!\{n\}\!\!\}$ will be most useful. A strategy suggested by S. Vickers uses natural induction, though a more general rule based on arbitrary well-founded orders is being developed at this moment and will be the subject of a future paper.

7 References

[Ab 91] S. Abramsky, Domain Theory in Logical Form, *Annals of Pure and Applied Logic*, 51, 1–77.

[Br 92] S.D. Brookes, An axiomatic treatment of partial correctness and deadlock in a shared variable parallel language, Technical Report CMU-CS-92-154, School of Computer Science, Carnegie Mellon University, June.

[EHJ 93] L. Errington, Chris Hankin and T.P. Jensen, Reasoning about Gamma Programs, in G. Burns, S. Gay and M. Ryan (eds.), *Theory and*

Formal Methods 1993, Workshops in Computing, Springer-Verlag.

[GH 95] S.J. Gay and C.L. Hankin, A Program Logic for Gamma, manuscript, 8th December.

[GH 96] S.J. Gay and C.L. Hankin, Gamma and the Logic of Transition Traces, Theory and Formal Methods Workshop 1996, Department of Computing, Imperial College.

[Vi 89] S. Vickers, *Topology via Logic*, Cambridge Tracts in Theoretical Computer Science 5, Cambridge University Press.