# Effect Algebras, Girard Quantales and Complementation in Separation Logic

Callum Bannister[1], Peter Höfner[2], and Georg Struth[2]

[1] University of Queensland, Australia
[2] Australian National University, Australia
[3] University of Sheffield, UK

**Abstract.** We study convolution and residual operations within convolution quantales of maps from partial abelian semigroups and effect algebras into value quantales, thus generalising separating conjunction and implication of separation logic to quantitative settings. We show that effect algebras lift to Girard convolution quantales, but not the standard partial abelian monoids used in separation logic. It follows that the standard assertion quantales of separation logic do not admit a linear negation relating convolution and its right adjoint. We consider alternative dualities for these operations on convolution quantales using boolean negations, some old, some new, relate them with properties of the underlying partial abelian semigroups and outline potential uses.

## 1 Introduction

Separation logic and linear logic reason about resources, and both have powerset quantale semantics that lift certain monoids. The phase quantale semantics of linear logic is even a Girard quantale [21]: it admits a dualising element that relates the quantalic composition with its residuals in the way negation relates conjunction and implication in classical logic. In separation logic, previous work [2,3] suggests that such a linear negation between separating conjunction and implication is impossible, but an algebraic account is missing.

We investigate the relationship between the classical heaplet and statelet models of separation logic and Girard quantales in the more general setting of convolution quantales formed by spaces of functions from partial monoids to quantales [9,11,5]. These yield quantale-valued semantics for linear and separation logic with applications in probabilistic program verification [13].

The classical heaplet models of separation logic are generalised effect algebras [14], but lack the greatest element present in effect algebras [12]. Effect algebras, in turn, are equipped with an orthosupplementation that seems suitable for extending previous lifting results from generalised effect algebras to convolution quantales to effect algebras and Girard quantales.

We prove that this extension works: effect algebras lift to commutative Girard quantales and in particular phase semantics for linear logic.[4] Yet we also prove

[4] To our surprise we could not find such a result in the literature.

that it is impossible to lift generalised effect algebras *without* a greatest element that way. This rules out a linear negation between separating conjunction and implication over the classical heaplet models. Further we present a read-only heaplet model that forms an effect algebra and makes linear negation available to separation logic in some situations, and outline its use.

We generalise these lifting and impossibility results to cover partial abelian monoids with several units, as in the statelet models of separation logic, and from powersets to convolution quantales, for quantitative applications.

Beyond these results, we show how separating conjunction and implication in convolution quantales relate to operations in value quantales and partial abelian monoids. In the absence of linear negation, we follow [4] in studying the effect of boolean negation on separating conjunction and implication. This leads to operations of septraction and coimplication [4,1] as well as some new ones. We also expose the symmetries and dualities between these operations in boolean convolution quantales. Boolean negation may not be the most natural duality for quantales, but the resulting operations are at least useful for program verification [1]. Finally, we constrast these results with a non-boolean assertion quantale for separation logic based on Alexandrov topologies for posets that captures the sub-heaplet and sub-statelet orderings more faithfully than the standard one.

Our main results have been checked with the Isabelle/HOL proof assistant.[5] Our Isabelle theories already contain more general lifting results for non-commutative partial monoids and Girard quantales appropriate for the non-commutative linear logics originally studied by Yetter [21]. These, however, are beyond the scope of this paper.

## 2 Partial Abelian Monoids and Effect Algebras

We recall the basics of partial abelian monoids. Most of the development has been formalised with Isabelle [8]. Most results are known in the special case of generalised effect algebras [14].

A *partial abelian semigroup* (PAS) is a structure $(S, \oplus, D)$ with *domain of definition* $D \subseteq S \times S$ for the partial *composition* $\oplus : S \times S \to S$ (or $\oplus : D \to S$) such that, for all $x, y, z \in S$, $D\,x\,y$ and $D\,(x \oplus y)\,z$ imply that $D\,y\,z$, $D\,x\,(y \oplus z)$ and $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, and $D\,x\,y$ implies that $D\,y\,x$ and $x \oplus y = y \oplus x$.

We identify sets and predicates. The above associativity and commutativity axioms state that if one side of the equation is defined, then so is the other, and both are equal. This notion of equality is known as *Kleene equality* and we write $x \simeq y$ for it. Hence, more briefly, $(x \oplus y) \oplus z \simeq x \oplus (y \oplus z)$ and $x \oplus y \simeq y \oplus x$.

Units of a PAS $S$ can be defined like for (object-free) categories: $e \in S$ is a *unit* in $S$ if there exists an $x \in S$ such that $x \simeq e \oplus x$ and for all $x, y \in S$ if $y \simeq e \oplus x$ then $y = x$. A *partial abelian monoid* (PAM) is a PAS $S$ in which every element has a unit: $\forall x \in S. \exists e \in E.\ D\,e\,x$, writing $E$ for the set of units of $S$.

[5] Most results on partial abelian monoids and (convolution) quantales can be found in the Archive of Formal Proofs [8,19]. The complete formalisation can be found online `http://hoefner-online.de/ramics21`.

Every element of a PAM has precisely one unit, different units cannot be composed and total PAMs have precisely one unit [6].

PAMs and related partial algebras appear across mathematics, they are instances of relational semigroups and monoids or multisemigroups and multimonoids, see [10,5] for details. Relational monoids, in particular, are noting but monoids in the category **Rel** equipped with the canonical monoidal structure.

In any PAM $S$, the *divisibility preorder* is defined, for all $x, y \in S$, by $x \preceq y$ iff $D\,x \oplus z \simeq y$ for some $z \in S$. Hence $x \preceq y$ iff $x \oplus z \simeq y$ has a solution in $z$. This preorder is a precongruence: $x \preceq y$ and $D\,z\,x$ imply $z \oplus x \preceq z \oplus y$ (and $D\,y\,z$). A subtraction can now be defined.

A PAM $S$ is *cancellative* if $x \oplus z \simeq y \oplus z$ imply $x = y$ for all $x, y, z \in S$.

**Lemma 2.1.** *In a cancellative* PAM*, $x \preceq y$ implies $x \oplus z \simeq y$ for exactly one $z$.*

One can thus write $y \ominus x$ for this solution.

**Lemma 2.2.** *In a cancellative* PAM*,*
1. $x \oplus z \simeq y \Leftrightarrow x \preceq y \wedge z = y \ominus x$*,*
2. $D\,x\,y \Rightarrow (x \oplus y) \ominus x = y$ *and* $x \preceq y \Rightarrow x \oplus (y \ominus x) = y$*,*
3. $D\,x\,y \Rightarrow x \preceq x \oplus y$ *and* $x \preceq y \Rightarrow y \ominus x \preceq y$*.*

By Lemma 2.2(1) and (2), $x \oplus (\_)$ and $(\_) \ominus x$ are inverses up-to definedness.

Finally, a PAM is *positive* if $D\,x\,y$ and $x \oplus y \in E$ imply $x \in E$.

**Lemma 2.3.** *In any positive cancellative* PAM*, $\preceq$ is a partial order in which all units are $\preceq$-minimal.*

Cancellative positive PAMs with a single unit $E = \{0\}$ are known as *generalised effect algebras* (GEAs) [14] in the foundations of quantum mechanics.

*Example 2.4 (Heaplets).* Partial maps $X \rightharpoonup Y$ form a GEA $H$ with $D\,\eta_1\,\eta_2$ iff $dom\,\eta_1 \cap dom\,\eta_2 = \emptyset$, $\eta_1 \oplus \eta_2 = \eta_1 \cup \eta_2$ and $E = \{\varepsilon\}$, where $\varepsilon : X \rightharpoonup Y$ is the empty partial function. By definition, $dom\,\varepsilon = \emptyset$. These are the heaplets of separation logic. Alternatively, heaplets have been modelled as a GEA of *finite* partial maps $X \rightharpoonup_{\text{fin}} Y$. The latter capture the fact that programs use finitely many variables and heaps can always be extended. The former admits full heaps where no additional memory can be allocated. □

*Example 2.5 (Generalised Heaplets).* Heaplet models readily generalise to additions defined as union whenever heaplets coincide where they overlap: $D\,\eta_1\,\eta_2$ iff $\eta_1\,x = \eta_2\,x$ for all $x \in \eta_1 \cap dom\,\eta_2$. The resulting PAM is not cancellative. □

An *effect algebra* (EA) [12] is a PAM $S$ with single unit 0 and orthosupplement $(\_)^{\perp} : S \to S$ such that for each $x \in S$, $x^{\perp}$ is the unique element satisfying $x \oplus x^{\perp} = 0^{\perp}$ and if $D\,x\,0^{\perp}$, then $x = 0$. It is standard to write 1 for $0^{\perp}$. It follows that $x^{\perp\perp} = x$. The following fact is well known.

**Proposition 2.6.** *A* PAM *with a single unit is an* EA *iff it is a* GEA *with greatest element* 1 *satisfying* $1 = 0^{\perp}$*. In particular,* $x^{\perp} = 1 \ominus x$ *holds in this setting.*

*Example 2.7.* PAM $H$ from Example 2.4 is not an EA: it is cancellative positive, but has no greatest element when $|Y| > 1$. Replacing any $m \mapsto n \in \eta$ by $m \mapsto n'$ with $n \neq n'$ in heaplet $\eta$ yields an incomparable heaplet. □

Statelet models of separation logic are based on the following coproduct.

**Lemma 2.8.** *Let $X$ be a set and $(S, \oplus, D, E)$ a* PAM*.*

1. $(X \times S, \hat{\oplus}, \hat{D}, \hat{E})$ *forms a* PAM *with* $\hat{D}\,(x_1, y_1)\,(x_2, y_2)$ *iff* $x_1 = x_2$ *and* $D\, y_1\, y_2$*,* $(x_1, y_1) \mathbin{\hat{\oplus}} (x_2, y_2) = (x_1, y_1 \oplus y_2)$ *and* $\hat{E}\,(x, e)$ *iff* $x \in X$ *and* $e \in E$*.*
2. *If $S$ is cancellative or positive, then so is $X \times S$.*

*Example 2.9.* (*Statelets*) The PAM $H$ from Example 2.4 is formed by (finite) partial functions $X \rightharpoonup Y$. Program stores can be modelled as a set $Z$ (e.g. a function from variables to values). Lemma 2.8 then shows that $Z \times (X \rightharpoonup Y)$ forms a cancellative positive PAM with many units $E = \{(z, \varepsilon) \mid z \in Z\}$. □

## 3 Convolution Quantales over PAMs

We apply a lifting construction for functions from partial monoids, and even ternary relations with suitable algebraic properties, to quantales, so that a generalised quantale-weighted separating conjunction arises as a convolution and a quantale-weighted separating implication as its right adjoint [11,10]. A simple instance yields the assertion algebra of separation logic [9]—a convolution quantale of functions from the PAM of statelets into the quantale of booleans.

A *quantale* [18] is a structure $(Q, \leq, \cdot, 1)$ such that $(Q, \leq)$ is a complete lattice, $(Q, \cdot, 1)$ a monoid, and $\cdot$ preserves arbitrary sups in both arguments. We write $\bigvee X$ for the sup of $X \subseteq Q$, $\bigwedge X$ for its inf, $\vee$ for the binary sup and $\wedge$ for the binary inf. We write $\bot = \bigvee \emptyset$ for the least element of the lattice and $\top = \bigwedge \emptyset$ for its greatest element. It follows that $\bot$ is a zero of composition.

A quantale is *commutative* if its monoid is abelian, and *boolean* if its complete lattice is a boolean algebra. We write $\overline{x}$ for the boolean complement of $x$ in $Q$.

As quantalic composition preserves sups in both arguments, it has two right adjoints, $x\backslash(\_)$ of $x \cdot (\_)$ and $(\_)/x$ of $(\_) \cdot x$, for all $x \in Q$, given, as usual, by $x\backslash z = \bigvee\{y \mid x \cdot y \leq z\}$ and $z/x = \bigvee\{y \mid y \cdot x \leq z\}$, and related by $y \leq x\backslash z \Leftrightarrow x \cdot y \leq z \Leftrightarrow x \leq z/y$. The residuals coincide in commutative quantales: $y/x = x\backslash y$. As right adjoints, $x\backslash(\_)$ and $(\_)/x$ preserve infs and therefore $x \cdot y = \bigwedge\{z \mid y \leq x\backslash z\} = \bigwedge\{z \mid x \leq z/y\}$.

*Example 3.1.*

1. Every frame is a commutative quantale and hence every complete boolean algebra. In the latter, finite sups and infs are related by De Morgan duality; the residual is definable as $x \to y = \overline{x} \vee y$.
2. The booleans $\mathbb{B} = \{\mathsf{f}, \mathsf{t}\}$ thus form a two-element commutative quantale with $\cdot$ as $\wedge$/min, $\bigvee$ as max and $\backslash$ as boolean implication $\to$. Predicates over a PAM $S$ are functions $S \to \mathbb{B}$; $\mathbb{B}^S$ is isomorphic to $\mathcal{P}S$. □

We now fix a $\mathsf{PAM}$ $(S, \oplus, D, E)$ and a commutative quantale $(Q, \leq, \cdot, 1)$. We equip the function space $Q^S$ with quantalic operations following [11]. Sups, infs and the order extend pointwise from $Q$ to $Q^S$. Thus $\bot = \lambda x.\ \bot$ and $\top = \lambda x.\ \top$ in $Q^S$. We define the *convolution* of $f, g : S \to Q$ and the unit $id_E : S \to Q$ as

$$(f * g)\ x = \bigvee_{x \simeq y \oplus z} f\ y \cdot g\ z \qquad \text{and} \qquad id_E\, x = \begin{cases} 1 & \text{if } x \in E, \\ \bot & \text{otherwise.} \end{cases}$$

The following lifting result characterises the *convolution algebra* on $Q^S$.

**Theorem 3.2 ([11]).** *If $S$ is a $\mathsf{PAM}$ and $Q$ a commutative quantale, then the convolution algebra $(Q^S, \leq, *, id_E)$ is a commutative quantale.*

In addition, properties, such as being boolean lift from $Q$ to the convolution quantale $Q^S$. As an instance of Theorem 3.2, $Q = \mathbb{B}$ yields the commutative powerset quantale $(\mathcal{P}S, \subseteq, *, E)$ over the $\mathsf{PAM}$ $S$.

Cancellative $\mathsf{PAM}$s give us an arguably more elegant variant of convolution.

**Lemma 3.3.** *If $S$ is cancellative, then $(f * g)\, x = \bigvee_{y \preceq x} f\, y \cdot g\, (x \ominus y)$.*

*Remark 3.4.* Lemma 2.8 yields the following instance of Theorem 3.2: if $X$ is a set, then $Q^{X \times S}$ is a quantale with $id_E\, (x, y) = id_E\, y$ and $(f * g)\, (x, y) = \bigvee_{y \simeq y_1 \oplus y_2} f\, (x, y_1) \cdot g\, (x, y_2)$, where, in the first identity, the left $E$ is on $X \times S$ and the right one on $S$.

The right adjoint $f \twoheadrightarrow (\_)$ of $f * (\_)$ in $Q^S$ is $f \twoheadrightarrow h = \bigvee\{g \mid f * g \leq h\}$. In quantalic notation, $f \twoheadrightarrow g = f \backslash g$.

**Theorem 3.5.** *In every $\mathsf{PAM}$ $S$,*

1. $(f \twoheadrightarrow g)\, x = \bigwedge_{z = x \oplus y} f\, y \backslash g\, z = \bigwedge_{D\, x\, y} f\, y \backslash g\, (x \oplus y)$,
2. $(f \twoheadrightarrow g)\, x = \bigwedge_{x = z \ominus y} f\, y \backslash g\, z$, *if $S$ is cancellative.*

*Proof.*

1. Suppose $D\, x\, y$. Then $f\, y \cdot (f \twoheadrightarrow g)\, x \leq (f * (f \twoheadrightarrow g))\, (x \oplus y) \leq g\, (x \oplus y)$ and therefore $(f \twoheadrightarrow g)\, x \leq f\, y \backslash g\, (x \oplus y) \leq \bigwedge\{f\, y \backslash g\, (x \oplus y) \mid D\, x\, y\}$ by the adjunction and properties of inf.
   Conversely, suppose $D\, x\, z$ and let $\varphi\, x = \bigwedge\{f\, y \backslash g\, (x \oplus y) \mid D\, x\, y\}$. Then $\varphi\, x \leq f\, z \backslash g\, (x \oplus z)$, $f\, z \cdot \varphi\, x \leq g\, (x \oplus z)$ by the adjunction and $f * \varphi \leq g$ by definition of convolution. Finally, $\varphi\, x \leq (\bigvee\{h \mid f * h \leq g\})\ x = (f \twoheadrightarrow g)\, x$.
2. Immediate from (1) using Lemma 2.2(1). □

*Example 3.6.* (*Powerset Lifting*) Theorem 3.2 shows that the convolution algebra $(\mathcal{P}S, \subseteq, *, E)$, for $Q = \mathbb{B}$, is a commutative quantale of predicates over any $\mathsf{PAM}$ $(S, \oplus, E)$, in fact a boolean atomic one. For the $\mathsf{PAM}$ on $X \times S$ and in particular for statelets, convolution is separating conjunction and its residual separating implication (a.k.a. magic wand)

$$\begin{aligned} f * g &= \{(x, y_1) \oplus (x, y_2) \mid (x, y_1) \in f \wedge (x, y_2) \in g \wedge D\, y_1\, y_2\} \\ f \mathrel{-\!\!*} g &= \{(x, y) \mid \forall y'.\ (x, y') \in f \wedge D\, y\, y' \rightarrow (x, y \oplus y') \in g\} \\ &= \{(x, y_1 \ominus y_2) \mid (x, y_2) \in f \wedge y_2 \preceq y_1 \rightarrow (x, y_1) \in g\}, \end{aligned}$$

where the second step requires cancellation. This powerset quantale is the assertion algebra of separation logic. These set-based operations are also described in [7]. □

## 4 PAMs and Girard Quantales

Additional operations have been defined on quantales. A linear negation is inspired by linear logic—a classical multiplicative negation that coincides with boolean negation if $\cdot$ is $\wedge$.

Formally, an element $d$ of a quantale $Q$ is *dualising* if $(d/x)\backslash d = x = d/(x\backslash d)$ for all $x \in Q$. An element $c \in Q$ is *cyclic* if $c/x = x\backslash c$ for all $x \in Q$. A *Girard quantale* [21,18] is a quantale with a cyclic dualising element $d$.

This definition is meant for non-commutative quantales; in the commutative case all elements are cyclic. A *linear negation* can be defined as $x^d = x\backslash d$ (which is then the same as $d/x$). It has many features of classical negation: it is involutive, reverses the order and all sups and infs, hence in particular 0 and $\top$; and it allows expressing residuation in terms of multiplication and vice versa:

$$x\backslash y = \left(y^d \cdot x\right)^d \qquad \text{and} \qquad x \cdot y = \left(y\backslash x^d\right)^d .$$

Moreover, $d^d = 1$ and therefore $1^d = d$, $(x \vee y)^d = x^d \wedge y^d$, $(x \wedge y)^d = x^d \vee y^d$ [18]. Also $d = \top$ implies $\top = \bot$. In a boolean Girard quantale, where the underlying complete lattice is a boolean algebra, both negations commute: $\overline{x^d} = \overline{x}^d$.

First we show that any EA gives rise to a commutative Girard quantale. In any EA $S$ we define $X^\perp = \{x^\perp \mid x \in X\}$ for $X \subseteq S$. Then $X^\perp = \{x \mid x^\perp \in X\}$, $X^{\perp\perp} = X$ and $\overline{X}^\perp = \overline{X^\perp}$ because $x^{\perp\perp} = x$. Also recall that $0^\perp = 1$.

**Proposition 4.1.** *Let* $(S, \oplus, 0, {}^\perp)$ *be an* EA*. Then* $(\mathcal{P}S, \subseteq, *, \{0\})$ *is a commutative Girard quantale with dualising element* $\Delta = S - \{1\}$*.*

*Proof.* Theorem 3.2 implies that every PAM lifts to a powerset quantale. It thus remains to check that $\Delta$ is a dualising element, that is, $X^{\Delta\Delta} = X$ for any $X \subseteq S$. First we compute $X^\Delta$:

$$\begin{aligned} X^\Delta &= \{y \mid \forall x \in X.\ D\, x\, y \rightarrow x \oplus y \in \Delta\} \\ &= \{y \mid \neg\exists x \in X.\ x \oplus y \simeq 1\} \\ &= \{y \mid \neg\exists x \in X.\ x = y^\perp\} \\ &= \{y \mid y^\perp \in \overline{X}\} \\ &= \overline{X}^\perp, \end{aligned}$$

using the definition of $(\_)^{\perp}$ in the second step. Then $X^{\Delta\Delta} = X$ follows immediately from the equations preceding this theorem. $\square$

As a sanity check, $\Delta^{\Delta} = \overline{\Delta}^{\perp} = \{1\}^{\perp} = \{1^{\perp}\} = \{0\}$. Next we show that commutative Girard quantales contain $\mathsf{EA}$s.

**Lemma 4.2.** *Let $x \notin \Delta$ in a commutative powerset Girard quantale over set $S$ with unit $\{0\}$. Then $\{x\}^{\Delta} = \overline{\{0\}}$ and $\{x\} = \overline{\Delta}$.*

*Proof.* We have $x \notin \Delta \Leftrightarrow \{x\} \subseteq \overline{\Delta} \Leftrightarrow \overline{\Delta^{\Delta}} \subseteq \{x\}^{\Delta} \Leftrightarrow \overline{\{0\}} \subseteq \{x\}^{\Delta}$. It then follows that $\{x\}^{\Delta} = \overline{\{0\}}$ because if $S - \{0\} = \overline{\{0\}} \subset \{x\}^{\Delta}$, then $\{x\}^{\Delta} = S$ and therefore $\{x\}^{\Delta\Delta} = S^{\Delta} = \emptyset \neq \{x\}$, a contradiction. Finally, therefore, $\{x\} = \{x\}^{\Delta\Delta} = \overline{\{0\}}^{\Delta} = \overline{\{0\}^{\Delta}} = \overline{\Delta}$. $\square$

It follows that $\overline{\Delta}$ is a singleton set. We call its element 1.

**Proposition 4.3.** *Let $S$ be a $\mathsf{PAM}$ and $\mathcal{P}S$ a commutative Girard quantale with unit $\{0\}$ and dualising element $\Delta$. Then $S$ is an $\mathsf{EA}$.*

*Proof.* For every convolution quantale $Q^S$, $S$ forms a $\mathsf{PAM}$ [5]. It remains to check the two $\mathsf{EA}$ axioms. We abbreviate $\{x\}^{\perp} = \overline{\{x\}}^{\Delta}$. By Lemma 4.2, $\overline{\Delta} = \{1\}$. Then $\{x\}^{\perp} = \overline{\{x\}^{\Delta}} = \{y \mid D\,x\,y \wedge x \oplus y \in \overline{\Delta}\} = \{y \mid x \oplus y \simeq 1\}$, for all $x \in S$. Also, $\{x\}^{\perp} \neq \emptyset$ because otherwise $\overline{\{x\}}^{\Delta\Delta} = S \neq \overline{\{x\}}$. For each $x \in S$ there thus is a $y \in S$ such that $x \oplus y \simeq 1$, that is, 1 is the greatest element of $S$. It also follows that $\{x\} * \{x\}^{\perp} = \{1\}$ and $\{0\}^{\perp} = \{1\}$ using Lemma 4.2.

Next we show that $S$ is cancellative. Suppose $\{x\} * \{y\} = \{x\} * \{z\}$. Then, using $\{x\} * \{y\} = \{x \oplus y\}$, we have $\{x \oplus y\} * \{x \oplus y\}^{\perp} = \{x \oplus z\} * \{x \oplus y\}^{\perp} = \{1\}$ and therefore $\{y\} = (\{x\} * \{x \oplus y\}^{\perp})^{\perp} = \{z\}$.

Cancellativity implies that $x \oplus y \simeq 1$ for at most one $y$ by Lemma 2.1. Thus $\{x\}^{\perp}$ is a singleton set, and we call its element $x^{\perp}$. It satisfies $\{x^{\perp}\} = \{x\}^{\perp}$ and therefore $\{x\} * \{x^{\perp}\} = \{1\}$, which verifies the first $\mathsf{EA}$ axiom.

Moreover, $\preceq$ is a preorder that extends to singleton sets. For the second $\mathsf{EA}$ axiom, now suppose $D\,x\,1$. Then $\{1\} \preceq \{x\} * \{1\}$ by Lemma 2.2(3) and therefore $\{1\} = \{x\} * \{1\}$. Yet $\{1\} = \{0\} * \{0^{\perp}\} = \{0\} * \{1\}$ and $x = 0$, once again by cancellativity. $\square$

**Corollary 4.4.** *Let $S$ be a $\mathsf{GEA}$ without greatest element. Then the commutative quantale $\mathcal{P}S$ is not Girard.*

In particular, therefore, the heaplet model of separation logic, which is not an $\mathsf{EA}$ by Example 2.7, does not give rise to Girard quantales. Consequently, separating conjunction and implication over the heaplet models in Example 2.4 cannot be related by a quantalic linear negation. Next we give an alternative no-Girard proof for heaplets that extends to statelets.

**Theorem 4.5.** *The unital commutative quantale $(\mathcal{P}\,H, \subseteq, *, \mathbf{emp})$ over the $\mathsf{PAM}$ $H$ of heaplets is not Girard.*

*Proof.* Let $\Delta$ be a dualising element in $\mathcal{P}H$. By a remark above, we know $\Delta \neq H$. In fact, we can show that there are two (different) heaplets outside of $\Delta$. Then, by Lemma 4.2, this yields a contradiction.

**Claim:** $\exists \upsilon_1,\, \upsilon_2$ with $\upsilon_1, \upsilon_2 \notin \Delta$ and $\upsilon_1 \neq \upsilon_2$.

*Proof of Claim.* There are exotic cases where this is not the case, e.g., when either $X$ or $Y$ of type $X \rightharpoonup Y$ have cardinality 1.

Example 2.4 shows two standard models for heaplets: arbitrary partial functions and finite mappings.

In the former we can characterise a full heap using heaplets $\eta$ with $dom(\eta) = X$. When $|Y| > 1$—in most standard models it is $\mathbb{Z}$—there are at least two different full heaplets (Example 2.7). It suffices to show that any heaplet $\zeta$ with $dom(\zeta) = X$ is not part of $\Delta$. We use the equality $\overline{x^d} = \overline{x}^d$ and utilise the equivalence $\exists \eta'.\, D\,\eta\,\eta' \wedge \eta' \in X \wedge \eta \oplus \eta' \notin \Delta \;\Leftrightarrow\; \forall \eta'.\, D\,\eta\,\eta' \wedge \eta' \notin X \rightarrow \eta \oplus \eta' \in \Delta$, as in Proposition 4.1. Using $\zeta$ for $\eta$, $X = \mathbf{emp} = \{\varepsilon\}$ and the fact that the only heaplet that can be added to $\zeta$ is the empty heaplet $\varepsilon$ ($D\,\zeta\,\eta \Leftrightarrow \eta = \varepsilon$) yields

$$\begin{aligned} \zeta \notin \Delta \;&\Leftrightarrow\; \forall \eta'.\, D\,\zeta\,\eta' \wedge \eta' \neq \varepsilon \rightarrow \zeta \oplus \eta' \in \Delta \\ &\Leftrightarrow\; \forall \eta'.\, \mathsf{f} \rightarrow \zeta \oplus \eta' \in \Delta \;\Leftrightarrow\; \mathsf{t} \end{aligned}$$

Now consider the model of finite mappings. We follow [17] and assume that the partial functions are of type $\mathbb{Z} \rightharpoonup_{\text{fin}} Y$. We know there exists one heaplet $\upsilon$ with $\upsilon \notin \Delta$, for otherwise the algebra collapses. Next we assume that $\overline{\{\upsilon\}}$ is a dualising element and derive a contradiction. In the heaplet model we have

$$(\overline{\{\upsilon\}}/\{\upsilon\})\backslash\overline{\{\upsilon\}} = (\{\upsilon\} \mathrel{-\!\!*} \overline{\{\upsilon\}}) \mathrel{-\!\!*} \overline{\{\upsilon\}} = \{\eta \mid \forall \eta'.\; D\,\eta\,\eta' \wedge \eta \oplus \eta' = \upsilon \rightarrow \eta' = \varepsilon\}$$

If $\overline{\{\upsilon\}}$ is a dualising element, this set equates to $\{\upsilon\}$. However, every heaplet $\upsilon'$ that is strictly larger than $\upsilon$, i.e. $\upsilon \prec \upsilon'$ is an element of this set as well, since $\upsilon' \oplus \eta' \neq \upsilon$, for all $\eta'$, and therefore the antecedent inside the set evaluates to false. Since $\upsilon$ is a finite mapping and the set of locations is $\mathbb{Z}$, we can always find a larger heaplet $\upsilon'$. □

Theorem 4.5 holds in the standard heaplet models (Examples 2.4 and 2.5) of separation logic and generalises easily to statelets. It shows in particular that separating conjunction and separating implications over PAMs of statelets cannot be related by a linear negation.

## 5 Binative PAMs and Girard Convolution Quantales

We now generalise Proposition 4.1 to PAMs with multiple units and general convolution quantales, the main lifting theorem in this paper.

EAs generalise to several units. Element $x$ of PAS $S$ is *maximal* if $x \oplus y \simeq x$ for all $y$. A PAS $S$ is *orthosupplemented* if $x \oplus x^{\perp}$ is defined and maximal for all $x \in S$, and if $z$ is maximal, then $x \oplus y \simeq z$ iff $y = x^{\perp}$. Orthosupplemented PAMs are automatically PASs, and $e^{\perp}$ is maximal for each $e \in E$.

*Example 5.1 (Read-only-heaplets).* Heaplets become orthosupplemented PAMs with many units when switching to total functions $X \to Y \times \mathbb{B}$. For $b \in \{\mathsf{f}, \mathsf{t}\}$ and projections $\pi_1$, $\pi_2$ of cartesian products, we define

$$\begin{aligned} dom_b\, \eta &= \{x \in X \mid \pi_2(\eta\, x) = b\}, \\ cod_b\, \eta &= \{y \in Y \mid \exists x \in X.\ y = \pi_1(\eta\, x) \wedge \pi_2(\eta\, x) = b\}. \end{aligned}$$

We can now define the PAM $H^{ro}$ in which $D\,\eta_1\,\eta_2$ iff $dom_{\mathsf{t}}\,\eta_1 \cap dom_{\mathsf{t}}\,\eta_1 = \emptyset$, $cod_{\mathsf{t}}\,\eta_1 \subseteq cod_{\mathsf{f}}\,\eta_2$ and $cod_{\mathsf{t}}\,\eta_2 \subseteq cod_{\mathsf{f}}\,\eta_1$ models the domain of definition, $\eta_1 \oplus \eta_2 = \eta_1 \cup \eta_2$ is composition and $E = \{\eta \in H^{ro} \mid dom_{\mathsf{t}}\,\eta = \emptyset\}$ the set of units. Finally, $(\_)^\perp$ defined by $\eta^\perp\, x = (y, b) \Leftrightarrow \eta\, x = (y, \neg b)$ is an orthosupplement.

Such heaplets are "read-only" in the sense that if the composition of heaplets $\eta_1$ and $\eta_2$ is defined, they must agree on the values at each location in memory, and updating one requires updating the other. Hence, for any $f : H^{ro} \to H^{ro}$, we have $D\,\eta_1\,\eta_2 \Rightarrow D\,(f\,\eta_1)\,\eta_2 \Rightarrow f = id$. □

We generalise orthosupplementation further to cover more models. A PAS $S$ is *binative* if it is equipped with a function $(\_)^\perp : S \to S$ such that $D\,x\,x^\perp$, for all $x \in S$, and, for all $x, y, z \in S$, $x \oplus x^\perp \simeq y \oplus z$ implies $y = z^\perp$. Thus $x \oplus x^\perp \simeq x \oplus x^\perp$ implies $x = x^{\perp\perp}$. We call $(x, x^\perp)$ the *binates* of $S$.

Intuitively, binativity generalises positivity for PAMs from units to binates.

**Lemma 5.2.** *Every binative* PAS $S$ *is a cancellative* PAM *with*

$$E = \{(x \oplus x^\perp)^\perp \mid x \in S\}.$$

*Proof.* For cancellation, suppose $x \oplus y \simeq x \oplus z$. Then $(x \oplus y) \oplus (x \oplus y)^\perp \simeq x \oplus y \oplus (x \oplus z)^\perp$, hence $(x \oplus y) \oplus (x \oplus y)^\perp \simeq y \oplus (x \oplus (x \oplus z)^\perp)$ and therefore $z = y = (x \oplus (x \oplus z)^\perp)^\perp$ by binativity.

For the units, $x \oplus x^\perp \oplus (x \oplus x^\perp)^\perp \simeq x^\perp \oplus x \oplus (x \oplus x^\perp)^\perp$ by binativity. By binativity again, $x = x^{\perp\perp} = x \oplus (x \oplus x^\perp)^\perp$. □

*Example 5.3 (Binative* PAM*s).*

1. Orthosupplemented PASs are binative PASs where compositions of binates are maximal. Equivalently, a PAS is orthosupplemented if it is positive and binative.
2. EAs are binative PASs with single unit 0 and greatest element 1.
3. Abelian Groupoids are binative semigroups with $(\_)^\perp$ a inverse and binates composing to units.
4. Partial deterministic CBI models [16] are precisely binative PASs with single unit 0 and the composition of any binate equals $0^\perp$ .[6]

We can now generalise Theorem 4.1.

[6] CBI models are relational monoids, deterministic means that results of compositions are singletons, *partial* deterministic that they are singletons or empty.

**Theorem 5.4.** *Let $S$ be a binative* PAM *and $(Q, \cdot, \leq, d)$ a commutative Girard quantale. Then $(Q^S, \leq, *, \Delta)$ is a commutative Girard quantale with*

$$\Delta\, x = \begin{cases} d & \text{if } x = y \oplus y^\perp \text{ for some } y \in S, \\ \top & \text{otherwise.} \end{cases}$$

*Proof.* Relative to Theorem 3.2 we need to check $f^{\Delta\Delta} = f$ for all $f : S \to Q$. Define $f^\perp\, x = f\,(x^\perp)$ and $f^d\, x = (f\, x)^d$. Then $f^{\perp\perp} = f = f^{dd}$ and $f^{\perp d} = f^{d\perp}$. First we compute

$$f^\Delta\, x = \bigwedge_{D\,x\,y} f\, y \backslash \Delta\,(x \oplus y) = f^d\, x^\perp \wedge \bigwedge_{\substack{D\,x\,y \\ y \neq x^\perp}} f\, y \backslash \top = f^{\perp d}\, x \wedge \top = f^{\perp d}\, x.$$

Binativity is used in the second step. Hence $f^{\Delta\Delta} = f^{\perp d \perp d} = f^{\perp\perp dd} = f$. □

A natural question is whether we could obtain a more general result by restricting $D\,x\,x^\perp$ and avoiding the collapse into a monoid. However, this will not work: if $Q^S$ and $Q$ are both unital and $1 \neq \bot$ in $Q$, then the underlying PAS must be unital, too, and thus a PAM [5, Proposition 4.1]. Girard quantales, in particular, are unital.

Theorem 5.4 generalises further to non-abelian binative semigroups and non-commutative Girard quantales, yet this is beyond the scope of this paper. A proof can be found in our Isabelle theories.

***hier weiter

## 6 Using Linear Negation in Separation Logic

As statelets do not lift to a Girard quantale, it is natural to ask how the lifting results in the previous section might be applied. We show that lifting assertions on ordinary heaps to those on read-only heaps makes it possible to use linear negation to reason about resources that lack binativity.

Separation logic allows enriching a Hoare triple with a *frame*

$$\forall\, R.\ \{P * R\}\, C\, \{Q * R\},$$

which states that the execution of $C$ only modifies the resources whose ownership is asserted by $P$. If these are assertions on a standard heap, then the validity of adding a frame means the only variables that $C$ touches are claimed by $P$. However, if they are assertions on a read-only heap, a triple can only be enriched with a frame if $C$ does *not* mutate the heap. This restriction is somewhat artificial: if a frame $R$ only specifies the values of the heap portion it owns, then $C$ would be free to mutate.

Hence we lift $R$ to $\langle R \rangle$, where $\langle \_ \rangle : \mathcal{P}\, H \to \mathcal{P}\, H^{ro}$ asserts $R$ over the heap where $(v, t)$ is kept and $(v, f)$ is discarded. Note that $\langle \_ \rangle$ is injective, $\langle P * Q \rangle = \langle P \rangle * \langle Q \rangle$, $\langle \{0\} \rangle = \{0\}$, $\langle \top \rangle = \top$, and $\langle \bigvee S \rangle = (\bigvee x \in S. \langle x \rangle)$ so $\langle \_ \rangle$ is a quantale embedding. Then, we can obtain triples

$$\forall\, R. \{P * \langle R \rangle\}\, C\, \{Q * \langle R \rangle\}\,,$$

where $C$ is free to mutate the resource described by $P$. What does linear negation mean in this setting? If we take $(p \to -)$ to be the assertion that *only* the address $p$ is allocated, $(p \hookrightarrow -)$ says that at *least* p is allocated, then for boolean negation we have that $\overline{(p \to -)}$ says that if $p$ is allocated, then some other address is, and $\overline{(p \hookrightarrow -)}$ says that $p$ is not allocated. For *linear* negation we have $(p \hookrightarrow -)^d = \overline{(p \hookrightarrow -)}^{\perp} = (p \hookrightarrow -)$, and $(p \to -)^d = \overline{(p \to -)}^{\perp}$, which says that if p is *not* allocated, then some other address is not.

With a PAM that cannot be lifted into a Girard quantale, and a binative PAM seemingly unsuitable for standard applications of separation logic, we have obtained an enriched assertion language taking the best parts of both. This suggests that it would be fruitful to find binative semigroups that can serve as targets for embedding, rather than taken as resource models directly.

## 7 Other Residuals

A linear negation is not available in separation logic, yet $-\!*$ has been dualised with respect to boolean negation on the boolean assertion quantale. The resulting operation is known as septraction [4,20]. We study it in convolution quantales over a PAM where boolean complementation need not be available.

We define the *septraction* operation more generally as the convolution of $f, g : S \to Q$, where $S$ is a PAM and $Q$ a commutative quantale, as

$$(f \mathbin{-\!\circledast} g)\ x = \bigvee_{x \oplus y = z} f\ y \cdot g\ z$$

The only difference to separating conjunction is that the supremum in $y$ and $z$ is now taken over $x \oplus y = z$ rather than $x = y \oplus z$. In the ternary relation $(\_) \oplus (\_) = (\_)$, septraction is thus separating conjunction up-to an exchange of variables. In such a general relational setting it has been shown that a convolution $\mathbin{-\!\circledast}$ is associative if and only if the dual ternary relation satisfies a relational associativity law [5]. In our setting, this clearly cannot be expected. Similarly, a unit exists in the convolution algebra if and only if the underlying PAM or relational structure has identities [5]. Yet it has also been shown that associativity of the ternary relation is not needed to make the convolution operation sup-preserving in both arguments [10]. These results specialise as follows.

**Lemma 7.1.**

1. *If $S$ is a* PAM *and $Q$ a complete lattice equipped with sup-preserving operation $\cdot$, then $\mathbin{-\!\circledast}$ preserves all sups on $Q^S$.*
2. *The operation $\mathbin{-\!\circledast}$ need not be associative, commutative or have a unit, even for the* PAM*s of heaplets and statelets and for $Q = \mathbb{B}$.*

It follows that $\mathbin{-\!\circledast}$ has two residuals: the right adjoints of $f \mathbin{-\!\circledast} (\_)$ and $(\_) \mathbin{-\!\circledast} f$. The first one has already been studied for the PAM $H$ and $Q = \mathbb{B}$ as *(separating) coimplication* [1]. We define it abstractly on $Q^S$ as

$$f \rightsquigarrow\!\!* \ h = \bigvee \{ g \mid f \mathbin{-\!\circledast} g \le h \}.$$

As a right adjoint, coimplication preserves infs, but is neither associative nor commutative. It does not have a unit either.

In Section 3 we have related separating conjunction and implication in $Q^S$ to corresponding operations in $S$ and $Q$. For $-\circledast$, a simple substitution yields

$$(f -\circledast g)\ x = \bigvee_{D\,x\,y} f\ y \cdot g\ (x \oplus y).$$

The name "septraction" is motivated by the following fact.

**Lemma 7.2.** *If $S$ is a cancellative* PAM *and $Q$ a quantale, then*

$$(f -\circledast g)\ x = \bigvee_{x \preceq z} f\,(z \ominus x) \cdot g\,z.$$

We obtain similar results for $\rightsquigarrow\!\!*$.

**Theorem 7.3.** *If $S$ is a* PAM *and $Q$ a quantale, then*

1. $(f \rightsquigarrow\!\!* g)\,x = \bigwedge_{x = y \oplus z} f\,y \backslash g\,z$,
2. $(f \rightsquigarrow\!\!* g)\,x = \bigwedge_{y \preceq x} f\,y \backslash g\,(x \ominus y)$ *if $S$ is cancellative.*

So far, we have considered septraction and coimplication in isolation. Even when they occur together with separating conjunction and magic wand in one and the same PAM, the target algebra $Q$ could still be a double quantale with different monoidal compositions for separating conjunction and septraction and different residuals for magic wand and coimplication—yet these two operations could also coincide, like in the following example.

*Example 7.4.* (*Powerset Lifting*) For the PAM on $X \times S$ and in particular for statelets,

$$\begin{aligned} f -\circledast g &= \{(x,y) \mid \exists y'.\ D\,y\,y' \wedge (x,y') \in f \wedge (x, y \oplus y') \in g\} \\ f \rightsquigarrow\!\!* g &= \{(x,y) \mid \forall y', y''.\ y \simeq y' \oplus y'' \wedge (x,y') \in f \rightarrow (x,y'') \in g\} \\ &= \{(x,y) \mid \forall y'.\ y' \preceq y \wedge (x,y') \in f \rightarrow (x, y \ominus y') \in g\}, \end{aligned}$$

where the second step for $\rightsquigarrow\!\!*$ requires cancellation. □

In boolean quantales, boolean complementation relates separating conjunction and coimplication on the one hand, and septraction and magic wand on the other hand. In fact, this is how septraction and coimplication were originally defined in the special case of powerset algebras [4,1].

**Theorem 7.5.** *Let $S$ be a* PAM *and $Q$ a boolean quantale, Then, in $Q^S$,*

$$f \rightsquigarrow\!\!* g = \overline{f * \overline{g}} \qquad \textit{and} \qquad f -\circledast g = \overline{f -\!\!* \overline{g}}.$$

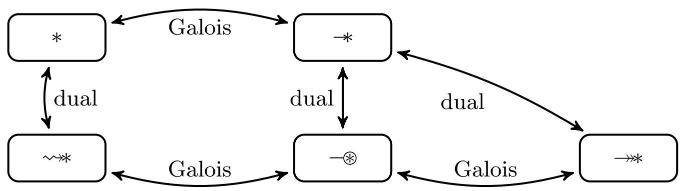


**Fig. 1.** Relationship between operators of separation logic

The relation between separating conjunction, implication, septraction and coimplication is also shown in Figure 1.

Using the Galois connection between $-\!\!\circledast$ and $\leadsto\!\!*$, a complete method for generating strongest postconditions in separation logic is available [1]. It enables the transformation of any giving Hoare triple—enriched with a frame—into a rule for forward reasoning. Symmetrically, the Galois connection between $*$ and $-\!\!*$ yield a method for backward reasoning, generating weakest preconditions. Ideas for this go back to the origins of separation logic [17].

To the best of our knowledge, the second right adjoint of septraction mentioned above has not been studied within the setting of separation logic. We define it abstractly on $Q^S$ as

$$g \twoheadrightarrow\!\!* \; h = \bigvee \{f \mid f -\!\!\circledast \; g \leq h\}.$$

The adjunction implies that this operation preserves infs, but is neither associative nor commutative. It does not have a unit either.

**Theorem 7.6.** *If $S$ is a* PAM *and $Q$ a quantale, then*

$$(f \twoheadrightarrow\!\!* \; g)\, x = \bigwedge_{D\,x\,y} f\,(x \oplus y) \backslash g\, y\,.$$

*Example 7.7.* (*Powerset Lifting*) For the PAM on $X \times S$,

$$f \twoheadrightarrow\!\!* \; g = \{(x, y) \mid \forall y'.\; D\, y\, y' \wedge (x, y \oplus y') \in f \rightarrow (x, y') \in g\}. \qquad \square$$

Boolean complementation relates this right adjoint back to magic wand.

**Theorem 7.8.** *Let $S$ be a* PAM *and $Q$ a boolean quantale, Then, in $Q^S$,*

$$f \twoheadrightarrow\!\!* \; g = \overline{f} -\!\!* \; \overline{g}.$$

This theorem completes Figure 1 and reveals an interesting asymmety. This asymmetry emerges from the fact that coimplication has a contrapositive $f \leadsto\!\!* \; g = -g \leadsto\!\!* -f$, whereas $-\!\!*$ does not.

Theorems 7.5 and 7.8 suggest looking at the boolean dual $\overline{\overline{f} -\!\!* \; g}$ as well. In the PAM on $X \times S$ this equates to $\{(x, y) \mid \exists y'. D\, y\, y' \wedge (x, y') \in \overline{f} \wedge y \oplus y' \in \overline{g}\}$. However, this is the same as $\overline{f} -\!\!\circledast \; \overline{g}$ and and therefore the residual will be $g \leadsto\!\!* \; f$. Hence we stay in the setting of the well-known operators of separation logic.

Finally, we look at these residuals in the setting of boolean Girard quantales.

**Theorem 7.9.** *If $S$ is a binative* PAS *and $Q$ a boolean Girard quantale, then in the convolution quantale $Q^S$ we have*

1. $f \rightsquigarrow\!\!\ast\, g = \overline{f \ast \overline{g}}$ *and* $f \multimap\!\!\circledast\, g = \overline{f \twoheadrightarrow\!\!\ast\, \overline{g}}$
2. $f \ast g = (f \twoheadrightarrow\!\!\ast\, g^d)^d$ *and* $f \multimap\!\!\circledast\, g = (f \rightsquigarrow\!\!\ast\, g^d)^d$
3. $f \rightsquigarrow\!\!\ast\, g = (f \twoheadrightarrow\!\!\ast\, g^{\perp})^{\perp}$ *and* $f \ast g = (f \multimap\!\!\circledast\, g^{\perp})^{\perp}$

Item (1) was already presented in Theorem 7.5, the first part of Item (2) follows directly from linear negation of Girard quantales (see Section 4) The remaining equations follow from results proved in Theorem 5.4. This shows that with a boolean Girard quantale e.g. assertions over an effect algebra, we obtain three dualities—boolean, linear, and binative.

## 8 Another Assertion Quantale for Separation Logic

The standard assertion quantale of separation logic is also somewhat unnatural mathematically in that it does not reflect the order $\preceq$ on heaplets and statelets: it is not the case that $\{x\} \subseteq \{y\}$ iff $x \preceq y$. We present an alternative that supports such more fine-grained comparisons.

We fix a cancellative positive PAM $S$. Then $\preceq$ is a partial order for which the units are minimal by Lemma 2.3. For each $x \in S$, $x{\downarrow} = \{y \mid y \preceq x\}$; for each $X \subseteq S$, $X{\downarrow}$ is the image of $X$ under $\downarrow$. We write $\mathcal{P}_{\downarrow} S$ for the set of downsets in $S$, the closed sets of the Alexandrov topology over $\preceq$.

We also need the following *Riesz decomposition property* [15] of $S$: for all $x, y_1, y_2 \in S$, $x \preceq y_1 \oplus y_2$ implies that there exist $x_1, x_2 \in S$ such that $x_1 \preceq y_1$, $x_2 \preceq y_2$ and $x_1 \oplus x_2 \preceq y_1 \oplus y_2$. It obviously holds in the heaplet and statelet models of separation logic.

**Proposition 8.1.** *Let $S$ be a cancellative positive* PAM *that satisfies the Riesz decomposition property. Then $\mathcal{P}_{\downarrow} S$ forms a commutative quantale.*

*Proof.* Relative to Theorem 3.2 we need to check that $\{e\}$ is closed for each $e \in E$, which is the case due to positivity (Lemma 2.3), and that the quantalic compositions and sups preserve downsets. First, using Riesz decomposition,

$$\begin{aligned}(X \ast Y){\downarrow} &= \{z \mid \exists x \in X, y \in Y.\ z \preceq x \oplus y \wedge D\, x\, y\}\\ &\subseteq \{x' \oplus y' \mid \exists x \in X, y \in Y.\ x' \preceq x \wedge y' \preceq y \wedge D\, x'\, y'\}\\ &= X{\downarrow} \ast Y{\downarrow}.\end{aligned}$$

Hence $(X{\downarrow} \ast Y{\downarrow}){\downarrow} = X{\downarrow} \ast Y{\downarrow}$, by extensivity and transitivity of $\downarrow$ . Second, it is routine to check that $(\bigcup_{i \in I} X_i){\downarrow} = \bigcup_{i \in I}(X_i{\downarrow})$, for all $I$, and therefore $(\bigcup_i X_i{\downarrow}){\downarrow} = \bigcup_i (X_i{\downarrow})$ by transitivity of $\downarrow$. (Similarly, $(\bigcap_i X_i{\downarrow}){\downarrow} = \bigcap_i (X_i{\downarrow})$, which is not strictly needed in the proof). □

Yet obviously, $(\overline{X{\downarrow}}){\downarrow}$ need not be equal to $\overline{X{\downarrow}}$: in the poset defined by $p < q$, for instance, the set $\{q\} = \overline{\{p\}{\downarrow}}$ is not closed. Hence the quantale $\mathcal{P}_{\downarrow} S$ is generally not boolean, and many of the theorems in Section 7 fail. Whether this quantale is Girard is open as well. On one hand, the $\Delta$ used in Proposition 4.1 is closed. On the other hand, residuals are sups taken on the whole of $\mathcal{P} S$, so we should not expect that they preserve downsets.

## 9 Conclusion

In the context of convolution algebras of functions from partial abelian semigroups into commutative quantales, we have explored the standard operations of separation logic—separating conjunction and implication—and some less known ones (septraction, coimplication and a second right adjoint of septraction). Due to the generality of the approach, it can be used with weighted assertions. The Lawvere quantale makes them available in fuzzy settings, the well known isomorphic quantale on the unit interval to probabilistic reasoning.

As the combination of boolean complementation with the quantalic composition seems a rather unnatural duality, we have also investigated the link with the linear negation provided by Girard quantales. We have established a correspondence between effect algebras and commutative powerset Girard quantales, but shown that generalised effect algebras, where a maximal element is missing, cannot be lifted to such quantales. Our results imply that the classical heaplet and statelet models of separation logic do not admit a linear negation; separating conjunction and implication are therefore independent. Yet we have also shown how these models can be embedded into effect algebras and thus made linear negation available for separation logic in some cases.

We have generalised the lifting of effect algebras to more general binative partial semigroups and extended it from powerset quantales to arbitrary convolution Girard quantales. In this paper we only consider commutative algebras, but liftings for non-commutative algebras can be found in our Isabelle theories. We believe that these results are only stepping stones towards more general ones for binative relational monoids or multimonoids. In this setting one may consider the binary operations of separation logic as binary modalities and the underlying monoidal structures as ternary Kripke frames, as in the Jónsson-Tarski duality for boolean algebras with operators. The correspondence between effect algebras and commutative powerset Girard quantales is then a modal correspondence based on this duality. For convolution algebras we expect modal correspondence triangles between properties of relational monoids, value quantales and convolution quantales [5]. All this remains to be explored with a view on linear negation.

Other research questions relate to the generalisation of the adjunctions and dualities between the operations in Section 7 to non-commutative algebras, to their counterparts in convolution Girard quantales over effect algebras, where linear negation is present, and to their status in the setting of non-boolean quantales, as the one introduced in Section 8.

**Acknowledgments** This research was supported in part by Australian Research Council (ARC) Grant DP190102142.

## References

1. C. Bannister, P. Höfner, and G. Klein. Backwards and forwards with separation logic. In *ITP 2018*, volume 10895 of *LNCS*, pages 68–87. Springer, 2018.

2. J. Brotherston and C. Calcagno. Classical BI: its semantics and proof theory. *Logical Methods in Computer Science*, 6(3), 2010.
3. J. Brotherston and J. Villard. Sub-classical boolean bunched logics and the meaning of par. In *CSL 2015*, volume 41 of *LIPIcs*, pages 325–342. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015.
4. C. Calcagno, P. Gardner, and U. Zarfaty. Context logic as modal logic: completeness and parametric inexpressivity. In *POPL 2007*, pages 123–134. ACM, 2007.
5. J. Cranch, S. Doherty, and G. Struth. Convolution and concurrency. *arXiv*, 2002.02321, 2020.
6. J. Cranch, S. Doherty, and G. Struth. Relational semigroups and object-free categories. *arXiv*, 2001.11895, 2020.
7. H.-H. Dang, P. Höfner, and B. Möller. Algebraic separation logic. *J. Logic and Algebraic Programming*, 80(6):221–247, 2011.
8. B. Dongol, V. B. F. Gomes, I. J. Hayes, and G. Struth. Partial semigroups and convolution algebras. *Archive of Formal Proofs*, 2017.
9. B. Dongol, V. B. F. Gomes, and G. Struth. A program construction and verification tool for separation logic. In *MPC 2015*, volume 9129 of *LNCS*, pages 137–158. Springer, 2015.
10. B. Dongol, I. Hayes, and G. Struth. Convolution algebras: Relational convolution, generalised modalities and incidence algebras. *Logical Methods in Computer Science*, 17(1), 2021.
11. B. Dongol, I. J. Hayes, and G. Struth. Convolution as a unifying concept: Applications in separation logic, interval calculi, and concurrency. *ACM Transactions of Computational Logic*, 17(3):15:1–15:25, 2016.
12. D. J. Foulis and M. K. Bennett. Effect algebras and unsharp quantum logics. *Foundations of Physics*, 24:1331–1352, 1994.
13. M. P. L. Haslbeck. *Verified Quantiative Analysis of Imperative Algorithms*. PhD thesis, Fakuktät für Informatik, Technische Universität München, 2021.
14. H. J. and S. Pulmannová. Generalized difference posets and orthoalgebras. *Acta Mathematica Universitatis Comenianae*, LXV:247–279, 1996.
15. G. Jenča and S. Pulmannová. Quotients of partial abelian monoids and the riesz decomposition property. *Algebra Universalis*, 2002.
16. D. Larchey-Wendling. An alternative direct simulation of Minsky machines into classical bunched logics via group semantics. In *MFPS 2010*, volume 265 of *ENTCS*, pages 369–387. Elsevier, 2010.
17. P. W. O'Hearn, J. C. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *CSL 2001*, volume 2142 of *LNCS*, pages 1–19. Springer, 2001.
18. K. L. Rosenthal. *Quantales and Their Applications*. Longman Scientific & Technical, 1990.
19. G. Struth. Quantales. *Archive of Formal Proofs*, 2018.
20. V. Vafeiadis and M. J. Parkinson. A marriage of rely/guarantee and separation logic. In *CONCUR'07*, volume 4703 of *LNCS*, pages 256–271. Springer, 2007.
21. D. N. Yetter. Quantales and (noncommutative) linear logic. *The Journal of Symbolic Logic*, 55(1):41–64, 1990.