

# Modal quantales, involutive Quantales, Dedekind Quantales

Cameron Calk and Georg Struth

May 26, 2024

## Abstract

This AFP entry provides mathematical components for modal quantales, involutive quantales and Dedekind quantales. Modal quantales are simple extensions of modal Kleene algebras useful for the verification of recursive programs. Involutive quantales appear in the study of  $C^*$ -algebras. Dedekind quantales are relatives of Tarski's relation algebras, hence relevant to program verification and beyond that to higher rewriting. We also provide components for weaker variants such as Kleene algebras with converse and modal Kleene algebras with converse.

## Contents

<b>1</b>	<b>Introductory Remarks</b>	<b>2</b>
<b>2</b>	<b>Modal Kleene algebra based on domain and range semirings</b>	<b>3</b>
2.1	Modal semirings . . . . .	3
2.2	Modal Kleene algebra . . . . .	3
<b>3</b>	<b>Kleene algebra with converse</b>	<b>4</b>
3.1	Involutive Kleene algebra . . . . .	4
3.2	Kleene algebra with converse . . . . .	5
<b>4</b>	<b>Modal Kleene algebra with converse</b>	<b>5</b>
4.1	Involutive modal Kleene algebras . . . . .	5
4.2	Modal semirings algebras with converse . . . . .	6
4.3	Modal Kleene algebras with converse . . . . .	6
<b>5</b>	<b>Modal quantales</b>	<b>7</b>
5.1	Simplified modal semirings and Kleene algebras . . . . .	7
5.2	Domain quantales . . . . .	7
5.3	Codomain quantales . . . . .	10
5.4	Modal quantales . . . . .	10
5.5	Antidomain and anticodomain quantales . . . . .	11

<b>6</b>	<b>Quantales with converse</b>	<b>12</b>
6.1	Properties of unital quantales . . . . .	12
6.2	Involutive quantales . . . . .	13
6.3	Dedekind quantales . . . . .	16
6.4	Boolean Dedekind quantales . . . . .	29

## 1 Introductory Remarks

In this AFP entry we provide mathematical components for modal quantales, involutive quantales and Dedekind quantales. Modal quantales are simple extensions of modal Kleene algebras that can be used in the verification of recursive programs [6]. Involutive quantales appear in the study of  $C^*$ -algebras [8]. Dedekind quantales, categorifications of which are known as *modular quantaloids* [9], are relatives of Tarski’s relation algebras [11], and hence relevant to program verification as well. We also provide components for weaker variants such as Kleene algebras and modal Kleene algebras with converse.

Our main interest in these structures comes from recent applications in higher-dimensional rewriting [2, 3], where they are used in coherence proofs for rewriting systems based on computads or polygraphs. This includes proofs of coherent Church-Rosser theorems and coherent Newman’s lemmas. A more long-term programme considers the formalisation of algebraic aspects of higher rewriting with proof assistants.

Modal quantales have previously been studied in [4], where it is shown, for instance, that any category can be lifted to a modal quantale at powerset level. Such lifting results will be formalised in a companion AFP entry.

Dedekind quantales give also rise to intuitionistic modal algebras, as the results in this AFP entry show. In particular, the set of all subidentities or coreflexives of a Dedekind quantale forms a complete Heyting algebra (aka frame or locale), on which modal box and diamond operators can be defined. A paper explaining these results is in preparation [7]. A further application of Dedekind quantales lies once again in higher-dimensional rewriting [2, 3]. Any groupoid, in particular, can be lifted to a Dedekind quantale at powerset level, a result which will once again be formalised in a companion AFP entry. Our components build on extant AFP components for Kleene algebras [1], modal Kleene algebras [5] and quantales [10].

Georg Struth is grateful for an invited professorship at École polytechnique and a fellowship at the Collegium de Lyon, Institute of Advanced Study, during which most of this formalisation work has been done.

## 2 Modal Kleene algebra based on domain and range semirings

```
theory Modal-Kleene-Algebra-Var
  imports KAD.Domain-Semiring KAD.Range-Semiring
```

```
begin
```

```
notation domain-op (dom)
```

```
notation range-op (cod)
```

```
subclass (in domain-semiring) dioid-one-zero⟨proof⟩
```

```
subclass (in range-semiring) dioid-one-zero
  ⟨proof⟩
```

### 2.1 Modal semirings

The following modal semirings are based on domain and range semirings instead of antidomain and antirange semirings, as in the AFP entry for Kleene algebra with domain.

```
class dr-modal-semiring = domain-semiring + range-semiring +
  assumes dc-compat [simp]: dom (cod x) = cod x
  and cd-compat [simp]: cod (dom x) = dom x
```

```
begin
```

```
sublocale msrdual: dr-modal-semiring (+)  $\lambda x y. y \cdot x$  1 0 cod ( $\leq$ ) ( $<$ ) dom
  ⟨proof⟩
```

```
lemma d-cod-fix: (dom x = x) = (x = cod x)
  ⟨proof⟩
```

```
lemma local-var: (x · y = 0) = (cod x · dom y = 0)
  ⟨proof⟩
```

```
lemma fbdia-conjugation: (fd x (dom p) · dom q = 0) = (dom p · bd x (dom q) =
  0)
  ⟨proof⟩
```

```
end
```

### 2.2 Modal Kleene algebra

```
class dr-modal-kleene-algebra = dr-modal-semiring + kleene-algebra
```

```
end
```

### 3 Kleene algebra with converse

```
theory Kleene-Algebra-Converse
  imports Kleene-Algebra.Kleene-Algebra
```

```
begin
```

We start from involutive dioids and Kleene algebra and then add a so-called strong Gelfand property to obtain an operation of converse that is closer to algebras of paths and relations.

#### 3.1 Involutive Kleene algebra

```
class invol-op =
  fixes invol :: 'a ⇒ 'a (-° [101] 100)

class involutive-doid = doid-one-zero + invol-op +
  assumes inv-invol [simp]: (x°)° = x
  and inv-contrav [simp]: (x · y)° = y° · x°
  and inv-sup [simp]: (x + y)° = x° + y°
```

```
begin
```

```
lemma inv-zero [simp]: 0° = 0
⟨proof⟩
```

```
lemma inv-one [simp]: 1° = 1
⟨proof⟩
```

```
lemma inv-iso: x ≤ y ⇒ x° ≤ y°
⟨proof⟩
```

```
lemma inv-adj: (x° ≤ y) = (x ≤ y°)
⟨proof⟩
```

```
end
```

Here is an equivalent axiomatisation from Doornbos, Backhouse and van der Woude's paper on a calculational approach to mathematical induction.

```
class involutive-doid-alt = doid-one-zero +
  fixes inv-alt :: 'a ⇒ 'a
  assumes inv-alt: (inv-alt x ≤ y) = (x ≤ inv-alt y)
  and inv-alt-contrav [simp]: inv-alt (x · y) = inv-alt y · inv-alt x
```

```
begin
```

```
lemma inv-alt-invol [simp]: inv-alt (inv-alt x) = x
⟨proof⟩
```

**lemma** *inv-alt-add*:  $\text{inv-alt } (x + y) = \text{inv-alt } x + \text{inv-alt } y$   
 ⟨*proof*⟩

**sublocale** *altinv*: *involutive-diod* - - - - - *inv-alt*  
 ⟨*proof*⟩

**end**

**sublocale** *involutive-diod*  $\subseteq$  *altinv*: *involutive-diod-alt* - - - - - *invol*  
 ⟨*proof*⟩

**class** *involutive-kleene-algebra* = *involutive-diod* + *kleene-algebra*

**begin**

**lemma** *inv-star*:  $(x^*)^\circ = (x^\circ)^*$   
 ⟨*proof*⟩

**end**

### 3.2 Kleene algebra with converse

The name "strong Gelfand property" has been borrowed from Palmigiano and Re.

**class** *diod-converse* = *involutive-diod* +  
**assumes** *strong-gelfand*:  $x \leq x \cdot x^\circ \cdot x$

**lemma** (in *diod-converse*) *subid-conv*:  $x \leq 1 \implies x^\circ = x$   
 ⟨*proof*⟩

**class** *kleene-algebra-converse* = *involutive-kleene-algebra* + *diod-converse*

**end**

## 4 Modal Kleene algebra with converse

**theory** *Modal-Kleene-Algebra-Converse*  
**imports** *Modal-Kleene-Algebra-Var* *Kleene-Algebra-Converse*

**begin**

Here we mainly study the interaction of converse with domain and codomain.

### 4.1 Involutive modal Kleene algebras

**class** *involutive-domain-semiring* = *domain-semiring* + *involutive-diod*

**begin**

**notation** *domain-op* (*dom*)

**lemma** *strong-conv-conv*:  $\text{dom } x \leq x \cdot x^\circ \implies x \leq x \cdot x^\circ \cdot x$   
*<proof>*

**end**

**class** *involutive-dr-modal-semiring* = *dr-modal-semiring* + *involutive-dioid*

**class** *involutive-dr-modal-kleene-algebra* = *involutive-dr-modal-semiring* + *kleene-algebra*

## 4.2 Modal semirings algebras with converse

**class** *dr-modal-semiring-converse* = *dr-modal-semiring* + *dioid-converse*

**begin**

**lemma** *d-conv* [*simp*]:  $(\text{dom } x)^\circ = \text{dom } x$   
*<proof>*

**lemma** *cod-conv*:  $(\text{cod } x)^\circ = \text{cod } x$   
*<proof>*

**lemma** *d-conv-cod* [*simp*]:  $\text{dom } (x^\circ) = \text{cod } x$   
*<proof>*

**lemma** *cod-conv-d*:  $\text{cod } (x^\circ) = \text{dom } x$   
*<proof>*

**lemma** *dom y = y*  $\implies \text{fd } (x^\circ) y = \text{bd } x y$   
*<proof>*

**lemma** *dom y = y*  $\implies \text{bd } (x^\circ) y = \text{fd } x y$   
*<proof>*

**end**

## 4.3 Modal Kleene algebras with converse

**class** *dr-modal-kleene-algebra-converse* = *dr-modal-semiring-converse* + *kleene-algebra*

**class** *dr-modal-semiring-strong-converse* = *involutive-dr-modal-semiring* +  
**assumes** *weak-dom-def*:  $\text{dom } x \leq x \cdot x^\circ$   
**and** *weak-cod-def*:  $\text{cod } x \leq x^\circ \cdot x$

**subclass** (**in** *dr-modal-semiring-strong-converse*) *dr-modal-semiring-converse*  
*<proof>*

```
class dr-modal-kleene-algebra-strong-converse = dr-modal-semiring-strong-converse
+ kleene-algebra
```

```
end
```

## 5 Modal quantales

```
theory Modal-Quantale
```

```
imports Quantales.Quantale-Star Modal-Kleene-Algebra-Var KAD.Modal-Kleene-Algebra
```

```
begin
```

### 5.1 Simplified modal semirings and Kleene algebras

The previous formalisation of modal Kleene algebra in the AFP adds two compatibility axioms between domain and codomain when combining an antidomain semiring with an antirange semiring. But these are unnecessary. They are derivable from the other axioms. Thus I provide a simpler axiomatisation that should eventually replace the one in the AFP.

```
class modal-semiring-simp = antidomain-semiring + antirange-semiring
```

```
lemma (in modal-semiring-simp) dr-compat [simp]: d (r x) = r x
⟨proof⟩
```

```
lemma (in modal-semiring-simp) rd-compat [simp]: r (d x) = d x
⟨proof⟩
```

```
subclass (in modal-semiring-simp) modal-semiring
⟨proof⟩
```

```
class modal-kleene-algebra-simp = modal-semiring-simp + kleene-algebra
```

```
subclass (in modal-kleene-algebra-simp) modal-kleene-algebra⟨proof⟩
```

### 5.2 Domain quantales

```
class domain-quantale = unital-quantale + domain-op +
  assumes dom-absorb:  $x \leq \text{dom } x \cdot x$ 
  and dom-local:  $\text{dom } (x \cdot \text{dom } y) = \text{dom } (x \cdot y)$ 
  and dom-add:  $\text{dom } (x \sqcup y) = \text{dom } x \sqcup \text{dom } y$ 
  and dom-subid:  $\text{dom } x \leq 1$ 
  and dom-zero [simp]:  $\text{dom } \perp = \perp$ 
```

The definition is that of a domain semiring. I cannot extend the quantale class with respect to domain semirings because of different operations are used for addition/sup. The following sublocale statement brings all those properties into scope.

**sublocale** *domain-quantale*  $\subseteq$  *dqmsr*: *domain-semiring* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp$  *dom* ( $\leq$ ) ( $\langle$ )  
 $\langle$ *proof* $\rangle$

**sublocale** *domain-quantale*  $\subseteq$  *dqmka*: *domain-kleene-algebra* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp$  *dom* ( $\leq$ )  
 $\langle$  $\langle$ ) *qstar* $\langle$ *proof* $\rangle$

**typedef** (**overloaded**) 'a *d-element* = {x :: 'a :: *domain-quantale*. *dom* x = x}  
 $\langle$ *proof* $\rangle$

**setup-lifting** *type-definition-d-element*

**instantiation** *d-element* :: (*domain-quantale*) *bounded-lattice*

**begin**

**lift-definition** *less-eq-d-element* :: 'a *d-element*  $\Rightarrow$  'a *d-element*  $\Rightarrow$  bool **is** ( $\leq$ )  
 $\langle$ *proof* $\rangle$

**lift-definition** *less-d-element* :: 'a *d-element*  $\Rightarrow$  'a *d-element*  $\Rightarrow$  bool **is** ( $\langle$ )  $\langle$ *proof* $\rangle$

**lift-definition** *bot-d-element* :: 'a *d-element* **is**  $\perp$   
 $\langle$ *proof* $\rangle$

**lift-definition** *top-d-element* :: 'a *d-element* **is** 1  
 $\langle$ *proof* $\rangle$

**lift-definition** *inf-d-element* :: 'a *d-element*  $\Rightarrow$  'a *d-element*  $\Rightarrow$  'a *d-element* **is** ( $\cdot$ )  
 $\langle$ *proof* $\rangle$

**lift-definition** *sup-d-element* :: 'a *d-element*  $\Rightarrow$  'a *d-element*  $\Rightarrow$  'a *d-element* **is**  
 $\langle$  $\sqcup$  $\rangle$   
 $\langle$ *proof* $\rangle$

**instance**  
 $\langle$ *proof* $\rangle$

**end**

**instance** *d-element* :: (*domain-quantale*) *distrib-lattice*  
 $\langle$ *proof* $\rangle$

**context** *domain-quantale*

**begin**

**lemma** *dom-top* [*simp*]: *dom*  $\top$  = 1  
 $\langle$ *proof* $\rangle$

**lemma** *dom-top2*: x  $\cdot$   $\top$   $\leq$  *dom* x  $\cdot$   $\top$   
 $\langle$ *proof* $\rangle$



**lemma** *weak-twisted*:  $x \cdot \text{dom } y \leq \text{dom } (x \cdot y) \cdot x$   
 ⟨proof⟩

**lemma** *dom-meet*:  $\text{dom } x \cdot \text{dom } y = \text{dom } x \sqcap \text{dom } y$   
 ⟨proof⟩

**lemma** *dom-meet-pres*:  $\text{dom } (\text{dom } x \sqcap \text{dom } y) = \text{dom } x \sqcap \text{dom } y$   
 ⟨proof⟩

**lemma** *dom-meet-distl*:  $\text{dom } x \cdot (y \sqcap z) = (\text{dom } x \cdot y) \sqcap (\text{dom } x \cdot z)$   
 ⟨proof⟩

**lemma** *dom-meet-approx*:  $\text{dom } ((\text{dom } x \cdot y) \sqcap (\text{dom } x \cdot z)) \leq \text{dom } x$   
 ⟨proof⟩

**lemma** *dom-inf-pres-aux*:  $Y \neq \{\}$   $\implies \text{dom } (\prod y \in Y. \text{dom } x \cdot y) \leq \text{dom } x$   
 ⟨proof⟩

**lemma** *dom-inf-pres-aux2*:  $(\prod y \in Y. \text{dom } x \cdot y) \leq \prod Y$   
 ⟨proof⟩

**lemma** *dom-inf-pres*:  $Y \neq \{\}$   $\implies \text{dom } x \cdot (\prod Y) = (\prod y \in Y. \text{dom } x \cdot y)$   
 ⟨proof⟩

**lemma** *dom*:  $\text{dom } (\prod X) \leq \prod (\text{dom } \cdot X)$   
 ⟨proof⟩

The domain operation need not preserve arbitrary sups, though this property holds, for instance, in quantales of binary relations. I do not aim at a stronger axiomatisation in this theory.

**lemma** *dom-top-pres*:  $(x \leq \text{dom } y \cdot x) = (x \leq \text{dom } y \cdot \top)$   
 ⟨proof⟩

**lemma** *dom-lla-var*:  $(\text{dom } x \leq \text{dom } y) = (x \leq \text{dom } y \cdot \top)$   
 ⟨proof⟩

**lemma** *dom*:  $(1 \sqcap x) = 1 \sqcap x \implies x \leq 1 \implies \text{dom } x = x$   
 ⟨proof⟩

**lemma** *dom-meet-sub*:  $\text{dom } (x \sqcap y) \leq \text{dom } x \sqcap \text{dom } y$   
 ⟨proof⟩

**lemma** *dom-dist1*:  $\text{dom } x \sqcup (\text{dom } y \sqcap \text{dom } z) = (\text{dom } x \sqcup \text{dom } y) \sqcap (\text{dom } x \sqcup \text{dom } z)$   
 ⟨proof⟩

**lemma** *dom-dist2*:  $\text{dom } x \sqcap (\text{dom } y \sqcup \text{dom } z) = (\text{dom } x \sqcap \text{dom } y) \sqcup (\text{dom } x \sqcap \text{dom } z)$

*<proof>*

**abbreviation**  $fd' \equiv dqmsr.fd$

**definition**  $bb\ x\ y = \sqcup \{ dom\ z \mid z. fd'\ x\ z \leq dom\ y \}$

**lemma**  $fd'-bb-galois-aux: fd'\ x\ (dom\ p) \leq dom\ q \implies dom\ p \leq bb\ x\ (dom\ q)$   
*<proof>*

**lemma**  $dom-iso-var: (\sqcup x \in X. dom\ x) \leq dom\ (\sqcup x \in X. dom\ x)$   
*<proof>*

**lemma**  $dom-iso-var2: (\sqcup x \in X. dom\ x) \leq dom\ (\sqcup x \in X. x)$   
*<proof>*

**end**

### 5.3 Codomain quantales

**class**  $codomain-quantale = unital-quantale + range-op +$   
**assumes**  $cod-absorb: x \leq x \cdot cod\ x$   
**and**  $cod-local: cod\ (cod\ x \cdot y) = cod\ (x \cdot y)$   
**and**  $cod-add: cod\ (x \sqcup y) = cod\ x \sqcup cod\ y$   
**and**  $cod-subid: cod\ x \leq 1$   
**and**  $cod-zero: cod\ \perp = \perp$

**sublocale**  $codomain-quantale \subseteq coddual: domain-quantale\ range-op - \lambda x\ y. y \cdot x -$   
-----  
*<proof>*

**abbreviation** (in  $codomain-quantale$ )  $bd' \equiv coddual.fd'$

**definition** (in  $codomain-quantale$ )  $fb\ x\ y = \sqcup \{ cod\ z \mid z. bd'\ x\ z \leq cod\ y \}$

**lemma** (in  $codomain-quantale$ )  $bd'-fb-galois-aux: bd'\ x\ (cod\ p) \leq cod\ q \implies cod\ p \leq fb\ x\ (cod\ q)$   
*<proof>*

### 5.4 Modal quantales

**class**  $dc-modal-quantale = domain-quantale + codomain-quantale +$   
**assumes**  $dc-compat\ [simp]: dom\ (cod\ x) = cod\ x$   
**and**  $cd-compat\ [simp]: cod\ (dom\ x) = dom\ x$

**sublocale**  $dc-modal-quantale \subseteq mqs: dr-modal-kleene-algebra\ (\sqcup)\ (\cdot)\ 1\ \perp\ (\leq)\ (<)$   
 $qstar\ dom\ cod$   
*<proof>*

**sublocale**  $dc-modal-quantale \subseteq mqdual: dc-modal-quantale - \lambda x\ y. y \cdot x - - - - -$   
- -  $dom\ cod$

*<proof>*

**lemma** (in *dc-modal-quantale*)  $x \cdot \top = \text{dom } x \cdot \top$

*<proof>*

**lemma** (in *dc-modal-quantale*)  $\top \cdot x = \top \cdot \text{cod } x$

*<proof>*

## 5.5 Antidomain and anticodomain quantales

**notation** *antidomain-op* (*adom*)

**class** *antidomain-quantale* = *unital-quantale* + *antidomain-op* +

**assumes** *as1* [*simp*]:  $\text{adom } x \cdot x = \perp$

**and** *as2* [*simp*]:  $\text{adom } (x \cdot y) \leq \text{adom } (x \cdot \text{adom } (\text{adom } y))$

**and** *as3* [*simp*]:  $\text{adom } (\text{adom } x) \sqcup \text{adom } x = 1$

**definition** (in *antidomain-quantale*)  $\text{ddom} = \text{adom} \circ \text{adom}$

**sublocale** *antidomain-quantale*  $\subseteq$  *adqmsr*: *antidomain-semiring*  $\text{adom } (\sqcup) (\cdot) 1 \perp$

$(\leq) (<)$

*<proof>*

**sublocale** *antidomain-quantale*  $\subseteq$  *adqmka*: *antidomain-kleene-algebra*  $\text{adom } (\sqcup) (\cdot)$

$1 \perp (\leq) (<) \text{qstar}$ *<proof>*

**sublocale** *antidomain-quantale*  $\subseteq$  *addq*: *domain-quantale*  $\text{ddom}$

*<proof>*

**notation** *antirange-op* (*acod*)

**class** *anticodomain-quantale* = *unital-quantale* + *antirange-op* +

**assumes** *ars1* [*simp*]:  $x \cdot \text{acod } x = \perp$

**and** *ars2* [*simp*]:  $\text{acod } (x \cdot y) \leq \text{acod } (\text{acod } (\text{acod } x) \cdot y)$

**and** *ars3* [*simp*]:  $\text{acod } (\text{acod } x) \sqcup \text{acod } x = 1$

**sublocale** *anticodomain-quantale*  $\subseteq$  *acoddual*: *antidomain-quantale*  $\text{acod} - \lambda x y. y$

$\cdot x$  -----

*<proof>*

**definition** (in *anticodomain-quantale*)  $\text{ccod} = \text{acod} \circ \text{acod}$

**sublocale** *anticodomain-quantale*  $\subseteq$  *acdmsr*: *antirange-semiring*  $(\sqcup) (\cdot) 1 \perp \text{acod}$

$(\leq) (<)$ *<proof>*

**sublocale** *anticodomain-quantale*  $\subseteq$  *acdqmka*: *antirange-kleene-algebra*  $(\sqcup) (\cdot) 1 \perp$

$(\leq) (<) \text{qstar } \text{acod}$ *<proof>*

```

sublocale anticodomain-quantale  $\subseteq$  acddq: codomain-quantale - - - - -  $\lambda$ 
x. acod (acod x)
  <proof>

class modal-quantale = antidomain-quantale + anticodomain-quantale

sublocale modal-quantale  $\subseteq$  mmqs: modal-kleene-algebra-simp ( $\sqcup$ ) ( $\cdot$ )  $1$   $\perp$  ( $\leq$ ) ( $<$ )
qstar adom acod<proof>

sublocale modal-quantale  $\subseteq$  mmqdual: modal-quantale -  $\lambda x y. y \cdot x$  - - - - -
adom acod
  <proof>

end

```

## 6 Quantales with converse

```

theory Quantale-Converse
  imports Modal-Quantale Modal-Kleene-Algebra-Converse

```

```

begin

```

### 6.1 Properties of unital quantales

These properties should eventually added to the quantales AFP entry.

```

lemma (in quantale) bres-bot-top [simp]:  $\perp \rightarrow \top = \top$ 
  <proof>

```

```

lemma (in quantale) fres-top-bot [simp]:  $\top \leftarrow \perp = \top$ 
  <proof>

```

```

lemma (in unital-quantale) bres-top-top2 [simp]:  $(x \rightarrow y \cdot \top) \cdot \top = x \rightarrow y \cdot \top$ 
  <proof>

```

```

lemma (in unital-quantale) fres-top-top2 [simp]:  $\top \cdot (\top \cdot y \leftarrow x) = \top \cdot y \leftarrow x$ 
  <proof>

```

```

lemma (in unital-quantale) bres-top-bot [simp]:  $\top \rightarrow \perp = \perp$ 
  <proof>

```

```

lemma (in unital-quantale) fres-bot-top [simp]:  $\perp \leftarrow \top = \perp$ 
  <proof>

```

```

lemma (in unital-quantale) top-bot-iff:  $(x \cdot \top = \perp) = (x = \perp)$ 
  <proof>

```

## 6.2 Involutive quantales

The following axioms for involutive quantales are standard.

**class** *involutive-quantale* = *unital-quantale* + *invol-op* +  
**assumes** *inv-invol* [*simp*]:  $(x^\circ)^\circ = x$   
**and** *inv-contrav*:  $(x \cdot y)^\circ = y^\circ \cdot x^\circ$   
**and** *inv-sup* [*simp*]:  $(\bigsqcup X)^\circ = (\bigsqcup x \in X. x^\circ)$

**context** *involutive-quantale*  
**begin**

**lemma** *inv-binsup* [*simp*]:  $(x \sqcup y)^\circ = x^\circ \sqcup y^\circ$   
 $\langle$ *proof* $\rangle$

**lemma** *inv-iso*:  $x \leq y \implies x^\circ \leq y^\circ$   
 $\langle$ *proof* $\rangle$

**lemma** *inv-galois*:  $(x^\circ \leq y) = (x \leq y^\circ)$   
 $\langle$ *proof* $\rangle$

**lemma** *bres-fres-conv*:  $(y^\circ \leftarrow x^\circ)^\circ = x \rightarrow y$   
 $\langle$ *proof* $\rangle$

**lemma** *fres-bres-conv*:  $(y^\circ \rightarrow x^\circ)^\circ = x \leftarrow y$   
 $\langle$ *proof* $\rangle$

**sublocale** *invqka*: *involutive-kleene-algebra* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp (\leq) (<)$  *qstar invol*  
 $\langle$ *proof* $\rangle$

**lemma** *inv-binf* [*simp*]:  $(x \sqcap y)^\circ = x^\circ \sqcap y^\circ$   
 $\langle$ *proof* $\rangle$

**lemma** *inv-inf* [*simp*]:  $(\prod X)^\circ = (\prod x \in X. x^\circ)$   
 $\langle$ *proof* $\rangle$

**lemma** *inv-top* [*simp*]:  $\top^\circ = \top$   
 $\langle$ *proof* $\rangle$

**lemma** *inv-qstar-aux* [*simp*]:  $(x \hat{\ } i)^\circ = (x^\circ) \hat{\ } i$   
 $\langle$ *proof* $\rangle$

**lemma** *inv-conjugate*:  $(x^\circ \sqcap y = \perp) = (x \sqcap y^\circ = \perp)$   
 $\langle$ *proof* $\rangle$

We define domain and codomain as in relation algebra and compare with the domain and codomain axioms above.

**definition** *do* :: '*a*  $\Rightarrow$  '*a* **where**  
 $do\ x = 1 \sqcap (x \cdot x^\circ)$

**definition**  $cd :: 'a \Rightarrow 'a$  **where**  
 $cd\ x = 1 \sqcap (x^\circ \cdot x)$

**lemma** *do-inv*:  $do\ (x^\circ) = cd\ x$   
*<proof>*

**lemma** *cd-inv*:  $cd\ (x^\circ) = do\ x$   
*<proof>*

**lemma** *do-le-top*:  $do\ x \leq 1 \sqcap (x \cdot \top)$   
*<proof>*

**lemma** *do-subid*:  $do\ x \leq 1$   
*<proof>*

**lemma** *cd-subid*:  $cd\ x \leq 1$   
*<proof>*

**lemma** *do-bot [simp]*:  $do\ \perp = \perp$   
*<proof>*

**lemma** *cd-bot [simp]*:  $cd\ \perp = \perp$   
*<proof>*

**lemma** *do-iso*:  $x \leq y \implies do\ x \leq do\ y$   
*<proof>*

**lemma** *cd-iso*:  $x \leq y \implies cd\ x \leq cd\ y$   
*<proof>*

**lemma** *do-subdist*:  $do\ x \sqcup do\ y \leq do\ (x \sqcup y)$   
*<proof>*

**lemma** *cd-subdist*:  $cd\ x \sqcup cd\ y \leq cd\ (x \sqcup y)$   
*<proof>*

**lemma** *inv-do [simp]*:  $(do\ x)^\circ = do\ x$   
*<proof>*

**lemma** *inv-cd [simp]*:  $(cd\ x)^\circ = cd\ x$   
*<proof>*

**lemma** *dedekind-modular*:  
**assumes**  $(x \cdot y) \sqcap z \leq (x \sqcap (z \cdot y^\circ)) \cdot (y \sqcap (x^\circ \cdot z))$   
**shows**  $(x \cdot y) \sqcap z \leq (x \sqcap (z \cdot y^\circ)) \cdot y$   
*<proof>*

**lemma** *modular-eq1*:  
**assumes**  $\forall x\ y\ z\ w. (y \sqcap (z \cdot x^\circ) \leq w \implies (y \cdot x) \sqcap z \leq w \cdot x)$

```

shows  $\forall x y z. (x \cdot y) \sqcap z \leq (x \sqcap (z \cdot y^\circ)) \cdot y$ 
<proof>

lemma  $do\ x \cdot do\ y = do\ x \sqcap do\ y$ 
<proof>

lemma  $p \leq 1 \implies q \leq 1 \implies p \cdot q = p \sqcap q$ 
<proof>

end

sublocale ab-unital-quantale  $\subseteq$  cig: involutive-quantale id - - - - -
<proof>

class distributive-involutive-quantale = involutive-quantale + distrib-unital-quantale

class boolean-involutive-quantale = involutive-quantale + bool-unital-quantale

begin

lemma res-peirce:
  assumes  $\forall x y. x^\circ \cdot -(x \cdot y) \leq -y$ 
  shows  $((x \cdot y) \sqcap z^\circ = \perp) = ((y \cdot z) \sqcap x^\circ = \perp)$ 
<proof>

lemma res-schroeder1:
  assumes  $\forall x y. x^\circ \cdot -(x \cdot y) \leq -y$ 
  shows  $((x \cdot y) \sqcap z = \perp) = (y \sqcap (x^\circ \cdot z) = \perp)$ 
<proof>

lemma res-schroeder2:
  assumes  $\forall x y. x^\circ \cdot -(x \cdot y) \leq -y$ 
  shows  $((x \cdot y) \sqcap z = \perp) = (x \sqcap (z \cdot y^\circ) = \perp)$ 
<proof>

lemma res-mod:
  assumes  $\forall x y. x^\circ \cdot -(x \cdot y) \leq -y$ 
  shows  $(x \cdot y) \sqcap z \leq (x \sqcap (z \cdot y^\circ)) \cdot y$ 
<proof>

end

The strong Gelfand property (name by Palmigiano and Re) is important
for dioids and Kleene algebras. The modular law is a convenient axiom for
relational quantales, in a setting where the underlying lattice is not boolean.

class quantale-converse = involutive-quantale +
  assumes strong-gelfand:  $x \leq x \cdot x^\circ \cdot x$ 

begin

```

**lemma** *do-gelfand* [*simp*]:  $do\ x \cdot do\ x \cdot do\ x = do\ x$   
*<proof>*

**lemma** *cd-gelfand* [*simp*]:  $cd\ x \cdot cd\ x \cdot cd\ x = cd\ x$   
*<proof>*

**lemma** *do-idem* [*simp*]:  $do\ x \cdot do\ x = do\ x$   
*<proof>*

**lemma** *cd-idem* [*simp*]:  $cd\ x \cdot cd\ x = cd\ x$   
*<proof>*

**lemma** *dodo* [*simp*]:  $do\ (do\ x) = do\ x$   
*<proof>*

**lemma** *cdcd* [*simp*]:  $cd\ (cd\ x) = cd\ x$   
*<proof>*

**lemma** *docd-compat* [*simp*]:  $do\ (cd\ x) = cd\ x$   
*<proof>*

**lemma** *cddo-compat* [*simp*]:  $cd\ (do\ x) = do\ x$   
*<proof>*

**end**

**sublocale** *quantale-converse*  $\subseteq$  *convqka*: *kleene-algebra-converse* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp (\leq)$   
( $<$ ) *invol qstar*  
*<proof>*

### 6.3 Dedekind quantales

**class** *dedekind-quantale* = *involutive-quantale* +  
**assumes** *modular-law*:  $(x \cdot y) \sqcap z \leq (x \sqcap (z \cdot y^\circ)) \cdot y$

**begin**

**sublocale** *convdqka*: *kleene-algebra-converse* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp (\leq)$  ( $<$ ) *invol qstar*  
*<proof>*

**subclass** *quantale-converse*  
*<proof>*

**lemma** *modular-2* [*simp*]:  $((x \sqcap (z \cdot y^\circ)) \cdot y) \sqcap z = (x \cdot y) \sqcap z$   
*<proof>*

**lemma** *modular-1* [*simp*]:  $(x \cdot (y \sqcap (x^\circ \cdot z))) \sqcap z = (x \cdot y) \sqcap z$   
*<proof>*



**lemma modular3:**  $(x \cdot y) \sqcap z \leq x \cdot (y \sqcap (x^\circ \cdot z))$   
 ⟨proof⟩

The name Dedekind quantale owes to the following formula, which is equivalent to the modular law. Dedekind quantales are called modular quantales in Rosenthal's book on quantaloids (to be precise: he discusses modular quantaloids, but the notion of modular quantale is then obvious).

**lemma dedekind:**  $(x \cdot y) \sqcap z \leq (x \sqcap (z \cdot y^\circ)) \cdot (y \sqcap (x^\circ \cdot z))$   
 ⟨proof⟩

**lemma peirce:**  $((x \cdot y) \sqcap z^\circ = \perp) = ((y \cdot z) \sqcap x^\circ = \perp)$   
 ⟨proof⟩

**lemma schroeder-1:**  $((x \cdot y) \sqcap z = \perp) = (y \sqcap (x^\circ \cdot z) = \perp)$   
 ⟨proof⟩

**lemma schroeder-2:**  $((x \cdot y) \sqcap z = \perp) = (x \sqcap (z \cdot y^\circ) = \perp)$   
 ⟨proof⟩

**lemma modular-eg2:**  $y \sqcap (z \cdot x^\circ) \leq w \implies (y \cdot x) \sqcap z \leq w \cdot x$   
 ⟨proof⟩

**lemma lla-top-aux:**  $p \leq 1 \implies ((x \leq p \cdot x) = (x \leq p \cdot \top))$   
 ⟨proof⟩

Next we turn to properties of domain and codomain in Dedekind quantales.

**lemma lra-top-aux:**  $p \leq 1 \implies ((x \leq x \cdot p) = (x \leq \top \cdot p))$   
 ⟨proof⟩

**lemma lla:**  $p \leq 1 \implies ((do\ x \leq p) = (x \leq p \cdot \top))$   
 ⟨proof⟩

**lemma lla-Inf:**  $do\ x = \sqcap \{p. x \leq p \cdot \top \wedge p \leq 1\}$   
 ⟨proof⟩

**lemma lra:**  $p \leq 1 \implies ((cd\ x \leq p) = (x \leq \top \cdot p))$   
 ⟨proof⟩

**lemma lra-Inf:**  $cd\ x = \sqcap \{p. x \leq \top \cdot p \wedge p \leq 1\}$   
 ⟨proof⟩

**lemma lla-var:**  $p \leq 1 \implies ((do\ x \leq p) = (x \leq p \cdot x))$   
 ⟨proof⟩

**lemma lla-Inf-var:**  $do\ x = \sqcap \{p. x \leq p \cdot x \wedge p \leq 1\}$   
 ⟨proof⟩

**lemma lra-var:**  $p \leq 1 \implies ((cd\ x \leq p) = (x \leq x \cdot p))$

*<proof>*

**lemma** *lra-Inf-var*:  $cd\ x = \sqcap \{p. x \leq x \cdot p \wedge p \leq 1\}$   
*<proof>*

**lemma** *do-top*:  $do\ x = 1 \sqcap (x \cdot \top)$   
*<proof>*

**lemma** *cd-top*:  $cd\ x = 1 \sqcap (\top \cdot x)$   
*<proof>*

We start deriving the axioms of modal semirings and modal quantales.

**lemma** *do-absorp*:  $x \leq do\ x \cdot x$   
*<proof>*

**lemma** *cd-absorp*:  $x \leq x \cdot cd\ x$   
*<proof>*

**lemma** *do-absorp-eq [simp]*:  $do\ x \cdot x = x$   
*<proof>*

**lemma** *cd-absorp-eq [simp]*:  $x \cdot cd\ x = x$   
*<proof>*

**lemma** *do-top2*:  $x \cdot \top = do\ x \cdot \top$   
*<proof>*

**lemma** *cd-top2*:  $\top \cdot x = \top \cdot cd\ x$   
*<proof>*

**lemma** *do-local [simp]*:  $do\ (x \cdot do\ y) = do\ (x \cdot y)$   
*<proof>*

**lemma** *cd-local [simp]*:  $cd\ (cd\ x \cdot y) = cd\ (x \cdot y)$   
*<proof>*

**lemma** *do-fix-subid*:  $(do\ x = x) = (x \leq 1)$   
*<proof>*

**lemma** *cd-fix-subid*:  $(cd\ x = x) = (x \leq 1)$   
*<proof>*

**lemma** *do-inf2*:  $do\ (do\ x \sqcap do\ y) = do\ x \sqcap do\ y$   
*<proof>*

**lemma** *do-inf-comp*:  $do\ x \cdot do\ y = do\ x \sqcap do\ y$   
*<proof>*

**lemma** *cd-inf-comp*:  $cd\ x \cdot cd\ y = cd\ x \sqcap cd\ y$

*<proof>*

**lemma** *subid-mult-meet*:  $p \leq 1 \implies q \leq 1 \implies p \cdot q = p \sqcap q$   
*<proof>*

**lemma** *dodo-sup*:  $do (do x \sqcup do y) = do x \sqcup do y$   
*<proof>*

**lemma** *do-sup [simp]*:  $do (x \sqcup y) = do x \sqcup do y$   
*<proof>*

**lemma** *cdcd-sup*:  $cd (cd x \sqcup cd y) = cd x \sqcup cd y$   
*<proof>*

**lemma** *cd-sup [simp]*:  $cd (x \sqcup y) = cd x \sqcup cd y$   
*<proof>*

Next we show that Dedekind quantales are modal quantales, hence also modal semirings.

**sublocale** *dmq*: *dc-modal-quantale 1* ( $\cdot$ ) *Inf Sup* ( $\sqcap$ ) ( $\leq$ ) ( $<$ ) ( $\sqcup$ )  $\perp$   $\top$  *cd do*  
*<proof>*

**lemma** *do-top3 [simp]*:  $do (x \cdot \top) = do x$   
*<proof>*

**lemma** *cd-top3 [simp]*:  $cd (\top \cdot x) = cd x$   
*<proof>*

**lemma** *dodo-Sup-pres*:  $do (\bigsqcup x \in X. do x) = (\bigsqcup x \in X. do x)$   
*<proof>*

The domain elements form a complete Heyting algebra.

**lemma** *do-complete-heyting*:  $do x \sqcap (\bigsqcup y \in Y. do y) = (\bigsqcup y \in Y. do x \sqcap do y)$   
*<proof>*

**lemma** *cdcd-Sup-pres*:  $cd (\bigsqcup x \in X. cd x) = (\bigsqcup x \in X. cd x)$   
*<proof>*

**lemma** *cd-complete-heyting*:  $cd x \sqcap (\bigsqcup y \in Y. cd y) = (\bigsqcup y \in Y. cd x \sqcap cd y)$   
*<proof>*

**lemma** *subid-complete-heyting*:

**assumes**  $p \leq 1$

**and**  $\forall q \in Q. q \leq 1$

**shows**  $p \sqcap (\bigsqcup Q) = (\bigsqcup q \in Q. p \sqcap q)$

*<proof>*

Next we show that domain and codomain preserve arbitrary Sups.

**lemma** *do-Sup-pres-aux*:  $(\bigsqcup x \in X. do x \cdot \top) = (\bigsqcup x \in do \text{ ' } X. x \cdot \top)$

*<proof>*

**lemma** *do-Sup-pres*:  $do (\bigsqcup x \in X. x) = (\bigsqcup x \in X. do x)$   
*<proof>*

**lemma** *cd-Sup-pres*:  $cd (\bigsqcup x \in X. x) = (\bigsqcup x \in X. cd x)$   
*<proof>*

**lemma** *do-inf*:  $do (x \sqcap y) = 1 \sqcap (y \cdot x^\circ)$   
*<proof>*

**lemma** *cd-inf*:  $cd (x \sqcap y) = 1 \sqcap (y^\circ \cdot x)$   
*<proof>*

**lemma** *do-bres-prop*:  $p \leq 1 \implies do (x \rightarrow p \cdot \top) = 1 \sqcap (x \rightarrow p \cdot \top)$   
*<proof>*

**lemma** *cd-fres-prop*:  $p \leq 1 \implies cd (\top \cdot p \leftarrow x) = 1 \sqcap (\top \cdot p \leftarrow x)$   
*<proof>*

**lemma** *do-meet-prop*:  $(do p \cdot x) \sqcap (x \cdot do q) = do p \cdot x \cdot do q$   
*<proof>*

**lemma** *subid-meet-prop*:  $p \leq 1 \implies q \leq 1 \implies (p \cdot x) \sqcap (x \cdot q) = p \cdot x \cdot q$   
*<proof>*

Next we consider box and diamond operators like in modal semirings and modal quantales. These are inherited from domain quantales. Diamonds are defined with respect to domain and codomain. The box operators are defined as Sups and hence right adjoints of diamonds.

**abbreviation** *do-dia*  $\equiv dmq.fd'$

**abbreviation** *cd-dia*  $\equiv dmq.bd'$

**abbreviation** *do-box*  $\equiv dmq.bb$

**abbreviation** *cd-box*  $\equiv dmq.fb$

In the sense of modal logic, the domain-based diamond is a backward operator, the codomain-based one a forward operator. These are related by opposition/converse.

**lemma** *do-dia-cd-dia-conv*:  $p \leq 1 \implies do-dia (x^\circ) p = cd-dia x p$   
*<proof>*

**lemma** *cd-dia-do-dia-conv*:  $p \leq 1 \implies cd-dia (x^\circ) p = do-dia x p$   
*<proof>*

Diamonds preserve sups in both arguments.

**lemma** *do-dia-Sup*:  $do-dia (\bigsqcup X) p = (\bigsqcup x \in X. do-dia x p)$   
 ⟨proof⟩

**lemma** *do-dia-Sup2*:  $do-dia x (\bigsqcup P) = (\bigsqcup p \in P. do-dia x p)$   
 ⟨proof⟩

**lemma** *cd-dia-Sup*:  $cd-dia (\bigsqcup X) p = (\bigsqcup x \in X. cd-dia x p)$   
 ⟨proof⟩

**lemma** *cd-dia-Sup2*:  $cd-dia x (\bigsqcup P) = (\bigsqcup p \in P. cd-dia x p)$   
 ⟨proof⟩

The domain-based box is a forward operator, the codomain-based on a backward one. These interact again with respect to converse.

**lemma** *do-box-var*:  $p \leq 1 \implies do-box x p = \bigsqcup \{q. do-dia x q \leq p \wedge q \leq 1\}$   
 ⟨proof⟩

**lemma** *cd-box-var*:  $p \leq 1 \implies cd-box x p = \bigsqcup \{q. cd-dia x q \leq p \wedge q \leq 1\}$   
 ⟨proof⟩

**lemma** *do-box-cd-box-conv*:  $p \leq 1 \implies do-box (x^\circ) p = cd-box x p$   
 ⟨proof⟩

**lemma** *cd-box-do-box-conv*:  $p \leq 1 \implies cd-box (x^\circ) p = do-box x p$   
 ⟨proof⟩

**lemma** *do-box-subid*:  $do-box x p \leq 1$   
 ⟨proof⟩

**lemma** *cd-box-subid*:  $cd-box x p \leq 1$   
 ⟨proof⟩

Next we prove that boxes and diamonds are adjoints, and then demodalisation laws known from modal semirings.

**lemma** *do-dia-do-box-galois*:  
 assumes  $p \leq 1$   
 and  $q \leq 1$   
 shows  $(do-dia x p \leq q) = (p \leq do-box x q)$   
 ⟨proof⟩

**lemma** *cd-dia-cd-box-galois*:  
 assumes  $p \leq 1$   
 and  $q \leq 1$   
 shows  $(cd-dia x p \leq q) = (p \leq cd-box x q)$   
 ⟨proof⟩

**lemma** *do-dia-demod-subid*:  
 assumes  $p \leq 1$   
 and  $q \leq 1$

**shows**  $(do\text{-}dia\ x\ p \leq q) = (x \cdot p \leq q \cdot x)$   
 $\langle proof \rangle$

The demodalisation laws have variants based on residuals.

**lemma** *do-dia-demod-subid-fres*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(do\text{-}dia\ x\ p \leq q) = (p \leq x \rightarrow q \cdot x)$   
 $\langle proof \rangle$

**lemma** *do-dia-demod-subid-var*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(do\text{-}dia\ x\ p \leq q) = (x \cdot p \leq q \cdot \top)$   
 $\langle proof \rangle$

**lemma** *do-dia-demod-subid-var-fres*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(do\text{-}dia\ x\ p \leq q) = (p \leq x \rightarrow q \cdot \top)$   
 $\langle proof \rangle$

**lemma** *cd-dia-demod-subid*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(cd\text{-}dia\ x\ p \leq q) = (p \cdot x \leq x \cdot q)$   
 $\langle proof \rangle$

**lemma** *cd-dia-demod-subid-fres*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(cd\text{-}dia\ x\ p \leq q) = (p \leq x \cdot q \leftarrow x)$   
 $\langle proof \rangle$

**lemma** *cd-dia-demod-subid-var*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(cd\text{-}dia\ x\ p \leq q) = (p \cdot x \leq \top \cdot q)$   
 $\langle proof \rangle$

**lemma** *cd-dia-demod-subid-var-fres*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(cd\text{-}dia\ x\ p \leq q) = (p \leq \top \cdot q \leftarrow x)$   
 $\langle proof \rangle$

**lemma** *do-box-iso*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$

**and**  $p \leq q$   
**shows**  $do\text{-}box\ x\ p \leq do\text{-}box\ x\ q$   
 $\langle proof \rangle$

**lemma** *cd-box-iso*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**and**  $p \leq q$   
**shows**  $cd\text{-}box\ x\ p \leq cd\text{-}box\ x\ q$   
 $\langle proof \rangle$

**lemma** *do-box-demod-subid*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq do\text{-}box\ x\ q) = (x \cdot p \leq q \cdot x)$   
 $\langle proof \rangle$

**lemma** *do-box-demod-subid-bres*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq do\text{-}box\ x\ q) = (p \leq x \rightarrow q \cdot x)$   
 $\langle proof \rangle$

**lemma** *do-box-demod-subid-var*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq do\text{-}box\ x\ q) = (x \cdot p \leq q \cdot \top)$   
 $\langle proof \rangle$

**lemma** *do-box-demod-subid-var-bres*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq do\text{-}box\ x\ q) = (p \leq x \rightarrow q \cdot \top)$   
 $\langle proof \rangle$

**lemma** *do-box-demod-subid-var-bres-do*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq do\text{-}box\ x\ q) = (p \leq do\ (x \rightarrow q \cdot \top))$   
 $\langle proof \rangle$

**lemma** *cd-box-demod-subid*:  
**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq cd\text{-}box\ x\ q) = (p \cdot x \leq x \cdot q)$   
 $\langle proof \rangle$

**lemma** *cd-box-demod-subid-fres*:  
**assumes**  $p \leq 1$

**and**  $q \leq 1$   
**shows**  $(p \leq \text{cd-box } x \ q) = (p \leq x \cdot q \leftarrow x)$   
 $\langle \text{proof} \rangle$

**lemma** *cd-box-demod-subid-var*:

**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq \text{cd-box } x \ q) = (p \cdot x \leq \top \cdot q)$   
 $\langle \text{proof} \rangle$

**lemma** *cd-box-demod-subid-var-fres*:

**assumes**  $p \leq 1$   
**and**  $q \leq 1$   
**shows**  $(p \leq \text{cd-box } x \ q) = (p \leq \top \cdot q \leftarrow x)$   
 $\langle \text{proof} \rangle$

We substitute demodalisation inequalities for diamonds in the definitions of boxes.

**lemma** *do-box-var2*:  $p \leq 1 \implies \text{do-box } x \ p = \bigsqcup \{q. x \cdot q \leq p \cdot x \wedge q \leq 1\}$   
 $\langle \text{proof} \rangle$

**lemma** *do-box-bres1*:  $p \leq 1 \implies \text{do-box } x \ p = \bigsqcup \{q. q \leq x \rightarrow p \cdot x \wedge q \leq 1\}$   
 $\langle \text{proof} \rangle$

**lemma** *do-box-bres2*:  $p \leq 1 \implies \text{do-box } x \ p = \bigsqcup \{q. q \leq x \rightarrow p \cdot \top \wedge q \leq 1\}$   
 $\langle \text{proof} \rangle$

**lemma** *do-box-var3*:  $p \leq 1 \implies \text{do-box } x \ p = \bigsqcup \{q. x \cdot q \leq p \cdot \top \wedge q \leq 1\}$   
 $\langle \text{proof} \rangle$

**lemma** *cd-box-var2*:  $p \leq 1 \implies \text{cd-box } x \ p = \bigsqcup \{q. q \cdot x \leq x \cdot p \wedge q \leq 1\}$   
 $\langle \text{proof} \rangle$

**lemma** *cd-box-var3*:  $p \leq 1 \implies \text{cd-box } x \ p = \bigsqcup \{q. q \cdot x \leq \top \cdot p \wedge q \leq 1\}$   
 $\langle \text{proof} \rangle$

Using these results we get a simple characterisation of boxes via domain and codomain. Similar laws can be found implicitly in Doornbos, Backhouse and van der Woude's paper on a calculational approach to mathematical induction, which speaks about wlp operators instead modal operators.

**lemma** *bres-do-box*:  $p \leq 1 \implies \text{do-box } x \ p = \text{do } (x \rightarrow p \cdot \top)$   
 $\langle \text{proof} \rangle$

**lemma** *bres-do-box-var*:  $p \leq 1 \implies \text{do-box } x \ p = 1 \sqcap (x \rightarrow p \cdot \top)$   
 $\langle \text{proof} \rangle$

**lemma** *bres-do-box-top*:  $p \leq 1 \implies (\text{do-box } x \ p) \cdot \top = x \rightarrow p \cdot \top$   
 $\langle \text{proof} \rangle$



**lemma** *fres-cd-box*:  $p \leq 1 \implies \text{cd-box } x \ p = \text{cd } (\top \cdot p \leftarrow x)$   
 ⟨proof⟩

**lemma** *fres-cd-box-var*:  $p \leq 1 \implies \text{cd-box } x \ p = 1 \sqcap (\top \cdot p \leftarrow x)$   
 ⟨proof⟩

**lemma** *fres-cd-box-top*:  $p \leq 1 \implies \top \cdot \text{cd-box } x \ p = \top \cdot p \leftarrow x$   
 ⟨proof⟩

Next we show that the box operators act on the complete Heyting algebra of subidentities.

**lemma** *cd-box-act*:  
**assumes**  $p \leq 1$   
**shows**  $\text{cd-box } (x \cdot y) \ p = \text{cd-box } x \ (\text{cd-box } y \ p)$   
 ⟨proof⟩

**lemma** *do-box-act*:  
**assumes**  $p \leq 1$   
**shows**  $\text{do-box } (x \cdot y) \ p = \text{do-box } y \ (\text{do-box } x \ p)$   
 ⟨proof⟩

Next we show that the box operators are Sup reversing in the first and Inf preserving in the second argument.

**lemma** *do-box-sup-inf*:  $p \leq 1 \implies \text{do-box } (x \sqcup y) \ p = \text{do-box } x \ p \cdot \text{do-box } y \ p$   
 ⟨proof⟩

**lemma** *do-box-sup-inf-var*:  $p \leq 1 \implies \text{do-box } (x \sqcup y) \ p = \text{do-box } x \ p \sqcap \text{do-box } y \ p$   
 ⟨proof⟩

**lemma** *do-box-Sup-Inf*:  
**assumes**  $X \neq \{\}$   
**and**  $p \leq 1$   
**shows**  $\text{do-box } (\sqcup X) \ p = (\sqcap x \in X. \text{do-box } x \ p)$   
 ⟨proof⟩

**lemma** *do-box-Sup-Inf2*:  
**assumes**  $P \neq \{\}$   
**and**  $\forall p \in P. p \leq 1$   
**shows**  $\text{do-box } x \ (\sqcap P) = (\sqcap p \in P. \text{do-box } x \ p)$   
 ⟨proof⟩

**lemma** *cd-box-sup-inf*:  $p \leq 1 \implies \text{cd-box } (x \sqcup y) \ p = \text{cd-box } x \ p \cdot \text{cd-box } y \ p$   
 ⟨proof⟩

**lemma** *cd-box-sup-inf-var*:  $p \leq 1 \implies \text{cd-box } (x \sqcup y) \ p = \text{cd-box } x \ p \sqcap \text{cd-box } y \ p$   
 ⟨proof⟩

**lemma** *cd-box-Sup-Inf*:  
**assumes**  $X \neq \{\}$

**and**  $p \leq 1$   
**shows**  $cd\text{-box } (\bigsqcup X) p = (\prod x \in X. cd\text{-box } x p)$   
 $\langle proof \rangle$

**lemma**  $cd\text{-box-Sup-Inf2}$ :  
**assumes**  $P \neq \{\}$   
**and**  $\forall p \in P. p \leq 1$   
**shows**  $cd\text{-box } x (\prod P) = (\prod p \in P. cd\text{-box } x p)$   
 $\langle proof \rangle$

Next we define an antidomain operation in the style of modal semirings. A natural condition is that the antidomain of an element is the greatest test that cannot be left-composed with that elements, and hence a greatest left annihilator. The definition of anticodomain is similar. As we are not in a boolean domain algebra, we cannot expect that the antidomain of the antidomain yields the domain or that the union of a domain element with the corresponding antidomain element equals one.

**definition**  $ado\ x = \bigsqcup \{p. p \cdot x = \perp \wedge p \leq 1\}$

**definition**  $acd\ x = \bigsqcup \{p. x \cdot p = \perp \wedge p \leq 1\}$

**lemma**  $ado\text{-}acd$ :  $ado\ (x^\circ) = acd\ x$   
 $\langle proof \rangle$

**lemma**  $acd\text{-}ado$ :  $acd\ (x^\circ) = ado\ x$   
 $\langle proof \rangle$

**lemma**  $ado\text{-}left\text{-}zero$  [*simp*]:  $ado\ x \cdot x = \perp$   
 $\langle proof \rangle$

**lemma**  $acd\text{-}right\text{-}zero$  [*simp*]:  $x \cdot acd\ x = \perp$   
 $\langle proof \rangle$

**lemma**  $ado\text{-}greatest$ :  $p \leq 1 \implies p \cdot x = \perp \implies p \leq ado\ x$   
 $\langle proof \rangle$

**lemma**  $acd\text{-}greatest$ :  $p \leq 1 \implies x \cdot p = \perp \implies p \leq acd\ x$   
 $\langle proof \rangle$

**lemma**  $ado\text{-}subid$ :  $ado\ x \leq 1$   
 $\langle proof \rangle$

**lemma**  $acd\text{-}subid$ :  $acd\ x \leq 1$   
 $\langle proof \rangle$

**lemma**  $ado\text{-}left\text{-}zero\text{-}iff$ :  $p \leq 1 \implies (p \leq ado\ x) = (p \cdot x = \perp)$   
 $\langle proof \rangle$

**lemma** *acd-right-zero-iff*:  $p \leq 1 \implies (p \leq \text{acd } x) = (x \cdot p = \perp)$   
 ⟨proof⟩

This gives an equational characterisation of antidomain and anticodomain.

**lemma** *ado-cd-bot*:  $\text{ado } x = \text{cd } (\perp \leftarrow x)$   
 ⟨proof⟩

**lemma** *acd-do-bot*:  $\text{acd } x = \text{do } (x \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *ado-cd-bot-id*:  $\text{ado } x = 1 \sqcap (\perp \leftarrow x)$   
 ⟨proof⟩

**lemma** *acd-do-bot-id*:  $\text{acd } x = 1 \sqcap (x \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *ado-cd-bot-var*:  $\text{ado } x = \text{cd } (\perp \leftarrow \text{do } x)$   
 ⟨proof⟩

**lemma** *acd-do-bot-var*:  $\text{acd } x = \text{do } (\text{cd } x \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *ado-do-bot*:  $\text{ado } x = \text{do } (\text{do } x \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *do x = ado (ado x)*  
 ⟨proof⟩

**lemma** *acd-cd-bot*:  $\text{acd } x = \text{cd } (\perp \leftarrow \text{cd } x)$   
 ⟨proof⟩

**lemma** *ado-do-bot-var*:  $\text{ado } x = 1 \sqcap (\text{do } x \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *acd-cd-bot-var*:  $\text{acd } x = 1 \sqcap (\perp \leftarrow \text{cd } x)$   
 ⟨proof⟩

Domain and codomain are compatible with the boxes.

**lemma** *cd-box-ado*:  $\text{cd-box } x \perp = \text{ado } x$   
 ⟨proof⟩

**lemma** *do-box-acd*:  $\text{do-box } x \perp = \text{acd } x$   
 ⟨proof⟩

**lemma** *ado-subid-prop*:  $p \leq 1 \implies \text{ado } p = 1 \sqcap (p \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *ado-do*:  $p \leq 1 \implies \text{ado } p = \text{do } (p \rightarrow \perp)$   
 ⟨proof⟩

**lemma** *ado-do-compl*:  $ado\ x \cdot do\ x = \perp$

*<proof>*

**lemma**  $ado\ x \sqcup do\ x = \top$

*<proof>*

**lemma**  $\forall x\ p.\ \exists f.\ 1 \sqcap (\top \cdot p \leftarrow x) = 1 \sqcap (\perp \leftarrow (x \rightarrow p \cdot \top))$

*<proof>*

**lemma**  $cd\text{-}box\ x\ p = ado\ (x \cdot ado\ p)$

*<proof>*

**lemma** *ad-do-bot* [*simp*]:  $(1 \sqcap (do\ x \rightarrow \perp)) \cdot do\ x = \perp$

*<proof>*

**lemma** *do-heyting-galois*:  $(do\ x \cdot do\ y \leq do\ z) = (do\ x \leq 1 \sqcap (do\ y \rightarrow do\ z))$

*<proof>*

**lemma** *do-heyting-galois-var*:  $(do\ x \cdot do\ y \leq do\ z) = (do\ x \leq cd\text{-}box\ (do\ y)\ (do\ z))$

*<proof>*

Antidomain is therefore Heyting negation.

**lemma** *ado-heyting-negation*:  $ado\ (do\ x) = cd\text{-}box\ (do\ x)\ \perp$

*<proof>*

**lemma** *ad-ax1* [*simp*]:  $(1 \sqcap (do\ x \rightarrow \perp)) \cdot x = \perp$

*<proof>*

**lemma**  $1 \sqcap (do\ (1 \sqcap (do\ x \rightarrow \perp)) \rightarrow \perp) = do\ x$

*<proof>*

**lemma**  $p \leq 1 \implies do\text{-}dia\ x\ p = 1 \sqcap (cd\text{-}box\ x\ (1 \sqcap (p \rightarrow \perp)) \rightarrow \perp)$

*<proof>*

**lemma**  $p \leq 1 \implies cd\text{-}box\ x\ p = 1 \sqcap (do\text{-}dia\ x\ (1 \sqcap (p \rightarrow \perp)) \rightarrow \perp)$

*<proof>*

**lemma**  $p \leq 1 \implies cd\text{-}dia\ x\ p = 1 \sqcap (do\text{-}box\ x\ (1 \sqcap (p \rightarrow \perp)) \rightarrow \perp)$

*<proof>*

**lemma**  $p \leq 1 \implies do\text{-}box\ x\ p = 1 \sqcap (cd\text{-}dia\ x\ (1 \sqcap (p \rightarrow \perp)) \rightarrow \perp)$

*<proof>*

**end**

## 6.4 Boolean Dedekind quantales

**class** *distributive-dedekind-quantale* = *distrib-unital-quantale* + *dedekind-quantale*

**class** *boolean-dedekind-quantale* = *bool-unital-quantale* + *distributive-dedekind-quantale*

**begin**

**lemma** *ad-do-bot* [*simp*]:  $(1 - do\ x) \cdot do\ x = \perp$   
 $\langle proof \rangle$

**lemma** *ad-ax1* [*simp*]:  $(1 - do\ x) \cdot x = \perp$   
 $\langle proof \rangle$

**lemma** *ad-do* [*simp*]:  $1 - do\ (1 - do\ x) = do\ x$   
 $\langle proof \rangle$

**lemma** *ad-ax2*:  $1 - do\ (x \cdot y) \sqcup (1 - do\ (x \cdot (1 - do\ (1 - do\ y)))) = 1 - do\ (x \cdot (1 - do\ (1 - do\ y)))$   
 $\langle proof \rangle$

**lemma** *ad-ax3* [*simp*]:  $do\ x \sqcup (1 - do\ x) = 1$   
 $\langle proof \rangle$

**sublocale** *bdad*: *antidomain-semiring*  $\lambda x. 1 - do\ x \ (\sqcup) \ (\cdot) \ 1 \ \perp \ - \ -$   
 $\langle proof \rangle$

**sublocale** *bdadka*: *antidomain-kleene-algebra*  $\lambda x. 1 - do\ x \ (\sqcup) \ (\cdot) \ 1 \ \perp \ - \ - \ qstar$   
 $\langle proof \rangle$

**sublocale** *bdar*: *antirange-semiring*  $(\sqcup) \ (\cdot) \ 1 \ \perp \ \lambda x. 1 - cd\ x \ - \ -$   
 $\langle proof \rangle$

**sublocale** *bdaka*: *antirange-kleene-algebra*  $(\sqcup) \ (\cdot) \ 1 \ \perp \ - \ - \ qstar \ \lambda x. 1 - cd\ x \ \langle proof \rangle$

**sublocale** *bmod*: *modal-semiring-simp*  $\lambda x. 1 - do\ x \ (\sqcup) \ (\cdot) \ 1 \ \perp \ - \ - \ \lambda x. 1 - cd\ x \ \langle proof \rangle$

**sublocale** *bmod*: *modal-kleene-algebra-simp*  $(\sqcup) \ (\cdot) \ 1 \ \perp \ - \ - \ qstar \ \lambda x. 1 - do\ x \ \lambda x. 1 - cd\ x \ \langle proof \rangle$

**lemma** *inv-neg*:  $(-x)^\circ = -(x^\circ)$   
 $\langle proof \rangle$

**lemma** *residuation*:  $x^\circ \cdot -(x \cdot y) \leq -y$   
 $\langle proof \rangle$

**lemma** *bres-prop*:  $x \rightarrow y = -(x^\circ \cdot -y)$   
 $\langle proof \rangle$

**lemma** *fres-prop*:  $x \leftarrow y = -(-x \cdot y^\circ)$   
 ⟨*proof*⟩

**lemma** *do-dia-fdia*:  $do\text{-}dia\ x\ p = bdad.fdia\ x\ p$   
 ⟨*proof*⟩

**lemma** *cd-dia-bdia*:  $cd\text{-}dia\ x\ p = bdar.bdia\ x\ p$   
 ⟨*proof*⟩

**lemma** *do-dia-fbox-de-morgan*:  $p \leq 1 \implies do\text{-}dia\ x\ p = 1 - bdad.fbox\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *fbox-do-dia-de-morgan*:  $p \leq 1 \implies bdad.fbox\ x\ p = 1 - do\text{-}dia\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *cd-dia-bbox-de-morgan*:  $p \leq 1 \implies cd\text{-}dia\ x\ p = 1 - bdar.bbox\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *bbox-cd-dia-de-morgan*:  $p \leq 1 \implies bdar.bbox\ x\ p = 1 - cd\text{-}dia\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *do-box-bbox*:  $p \leq 1 \implies do\text{-}box\ x\ p = bdar.bbox\ x\ p$   
 ⟨*proof*⟩

**lemma** *cd-box-fbox*:  $p \leq 1 \implies cd\text{-}box\ x\ p = bdad.fbox\ x\ p$   
 ⟨*proof*⟩

**lemma** *do-dia-cd-box-de-morgan*:  $p \leq 1 \implies do\text{-}dia\ x\ p = 1 - cd\text{-}box\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *cd-box-do-dia-de-morgan*:  $p \leq 1 \implies cd\text{-}box\ x\ p = 1 - do\text{-}dia\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *cd-dia-do-box-de-morgan*:  $p \leq 1 \implies cd\text{-}dia\ x\ p = 1 - do\text{-}box\ x\ (1 - p)$   
 ⟨*proof*⟩

**lemma** *do-box-cd-dia-de-morgan*:  $p \leq 1 \implies do\text{-}box\ x\ p = 1 - cd\text{-}dia\ x\ (1 - p)$   
 ⟨*proof*⟩

**end**

**class** *dc-involutive-modal-quantale* = *dc-modal-quantale* + *involutive-quantale*

**begin**

**sublocale** *invmqmka*: *involutive-dr-modal-kleene-algebra* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp$  ( $\leq$ ) ( $<$ ) *qstar*  
*invol dom cod*⟨*proof*⟩

**lemma** *do-approx-dom*:  $do\ x \leq dom\ x$

*<proof>*

**end**

**class** *dc-modal-quantale-converse* = *dc-involutive-modal-quantale* + *quantale-converse*

**sublocale** *dc-modal-quantale-converse*  $\subseteq$  *invmqmka*: *dr-modal-kleene-algebra-converse*  
( $\sqcup$ ) ( $\cdot$ )  $1 \perp (\leq) (<)$  *qstar invol dom cod**<proof>*

**class** *dc-modal-quantale-strong-converse* = *dc-involutive-modal-quantale* +  
**assumes** *weak-dom-def*:  $\text{dom } x \leq x \cdot x^\circ$   
**and** *weak-cod-def*:  $\text{cod } x \leq x^\circ \cdot x$

**begin**

**sublocale** *invmqmka*: *dr-modal-kleene-algebra-strong-converse* ( $\sqcup$ ) ( $\cdot$ )  $1 \perp (\leq) (<)$   
*qstar invol dom cod*  
*<proof>*

**lemma** *dom-def*:  $\text{dom } x = 1 \sqcap (x \cdot x^\circ)$   
*<proof>*

**lemma** *cod-def*:  $\text{cod } x = 1 \sqcap (x^\circ \cdot x)$   
*<proof>*

**lemma** *do-dom*:  $\text{do } x = \text{dom } x$   
*<proof>*

**lemma** *cd-cod*:  $\text{cd } x = \text{cod } x$   
*<proof>*

**end**

**class** *dc-modal-dedekind-quantale* = *dc-involutive-modal-quantale* + *dedekind-quantale*

**class** *cd-distributive-modal-dedekind-quantale* = *dc-modal-dedekind-quantale* + *distrib-unital-quantale*

**class** *dc-boolean-modal-dedekind-quantale* = *dc-modal-dedekind-quantale* + *bool-unital-quantale*

**begin**

**lemma** *subid-idem*:  $p \leq 1 \implies p \cdot p = p$   
*<proof>*

**lemma** *subid-comm*:  $p \leq 1 \implies q \leq 1 \implies p \cdot q = q \cdot p$   
*<proof>*

**lemma** *subid-meet-comp*:  $p \leq 1 \implies q \leq 1 \implies p \sqcap q = p \cdot q$

$\langle proof \rangle$

**lemma** *subid-dom*:  $p \leq 1 \implies dom\ p = p$   
 $\langle proof \rangle$

**lemma** *do-prop*:  $(do\ x \leq do\ y) = (x \leq do\ y \cdot \top)$   
 $\langle proof \rangle$

**lemma** *do-lla*:  $(do\ x \leq do\ y) = (x \leq do\ y \cdot x)$   
 $\langle proof \rangle$

**lemma** *lla-subid*:  $p \leq 1 \implies ((dom\ x \leq p) = (x \leq p \cdot x))$   
 $\langle proof \rangle$

**lemma** *dom-do*:  $dom\ x = do\ x$   
 $\langle proof \rangle$

**end**

**end**

## References

- [1] A. Armstrong, G. Struth, and T. Weber. Kleene algebra. *Archive of Formal Proofs*, 2013.
- [2] C. Calk, E. Goubault, P. Malbos, and G. Struth. Algebraic coherent confluence and higher globular Kleene algebras. *Logical Methods in Computer Science*, 18(4), 2022.
- [3] C. Calk, P. Malbos, D. Pous, and G. Struth. Higher catoids, higher quantales and their correspondences. *arXiv*, 2307.09253, 2023.
- [4] U. Fahrenberg, C. Johansen, G. Struth, and K. Ziemiański. Catoids and modal convolution algebras. *Algebra Universalis*, 84:10, 2023.
- [5] V. B. F. Gomes, W. Guttmann, P. Höfner, G. Struth, and T. Weber. Kleene algebras with domain. *Archive of Formal Proofs*, 2016.
- [6] V. B. F. Gomes and G. Struth. Modal Kleene algebra applied to program correctness. In *FM 2016*, volume 9995 of *LNCS*, pages 310–325, 2016.
- [7] D. Pous and G. Struth. Dedekind quantaloids as intuitionistic modal algebras. In preparation, 2023.
- [8] P. Resende. Open maps of involutive quantales. *Applied Categorical Structures*, 26:631–644, 2018.



- [9] K. I. Rosenthal. *The Theory of Quantaloids*. Addison Wesley Longman Limited, 1996.
- [10] G. Struth. Quantales. *Archive of Formal Proofs*, 2018.
- [11] A. Tarski. On the calculus of relations. *Journal of Symbolic Logic*, 6(3):73–89, 1941.