

Program Construction and Verification Components Based on Kleene Algebra

Victor B. F. Gomes and Georg Struth

December 14, 2021

Abstract

Variants of Kleene algebra support program construction and verification by algebraic reasoning. This entry provides a verification component for Hoare logic based on Kleene algebra with tests, verification components for weakest preconditions and strongest postconditions based on Kleene algebra with domain and a component for step-wise refinement based on refinement Kleene algebra with tests. In addition to these components for the partial correctness of while programs, a verification component for total correctness based on divergence Kleene algebras and one for (partial correctness) of recursive programs based on domain quantales are provided. Finally we have integrated memory models for programs with pointers and a program trace semantics into the weakest precondition component.

Contents

| | | |
|----------|---|----------|
| 1 | Introductory Remarks | 3 |
| 2 | Two Standalone Components | 4 |
| 2.1 | Component Based on Kleene Algebra with Tests | 4 |
| 2.1.1 | KAT: Definition and Basic Properties | 4 |
| 2.1.2 | Propositional Hoare Logic | 6 |
| 2.1.3 | Soundness and Relation KAT | 6 |
| 2.1.4 | Embedding Predicates in Relations | 7 |
| 2.1.5 | Store and Assignment | 8 |
| 2.1.6 | Verification Example | 8 |
| 2.1.7 | Definition of Refinement KAT | 8 |
| 2.1.8 | Propositional Refinement Calculus | 9 |
| 2.1.9 | Soundness and Relation RKAT | 9 |
| 2.1.10 | Assignment Laws | 9 |
| 2.1.11 | Refinement Example | 9 |
| 2.2 | Component Based on Kleene Algebra with Domain | 10 |
| 2.2.1 | KAD: Definitions and Basic Properties | 10 |

| | | |
|----------|--|-----------|
| 2.2.2 | wp Calculus | 13 |
| 2.2.3 | Soundness and Relation KAD | 14 |
| 2.2.4 | Embedding Predicates in Relations | 14 |
| 2.2.5 | Store and Assignment | 15 |
| 2.2.6 | Verification Example | 15 |
| 2.2.7 | Propositional Hoare Logic | 16 |
| 2.2.8 | Definition of Refinement KAD | 16 |
| 2.2.9 | Propositional Refinement Calculus | 16 |
| 2.2.10 | Soundness and Relation RKAD | 17 |
| 2.2.11 | Assignment Laws | 17 |
| 2.2.12 | Refinement Example | 17 |
| 3 | Isomorphisms Between Predicates, Sets and Relations | 18 |
| 3.1 | Isomorphism Between Sets and Relations | 18 |
| 3.2 | Isomorphism Between Predicates and Sets | 19 |
| 3.3 | Isomorphism Between Predicates and Relations | 20 |
| 4 | Components Based on Kleene Algebra with Tests | 22 |
| 4.1 | Verification Component | 22 |
| 4.1.1 | Definitions of Hoare Triple | 22 |
| 4.1.2 | Syntax for Conditionals and Loops | 22 |
| 4.1.3 | Propositional Hoare Logic | 23 |
| 4.1.4 | Store and Assignment | 24 |
| 4.1.5 | Simplified Hoare Rules | 24 |
| 4.1.6 | Verification Examples | 26 |
| 4.1.7 | Verification Examples with Automated VCG | 27 |
| 4.2 | Refinement Component | 28 |
| 4.2.1 | RKAT: Definition and Basic Properties | 28 |
| 4.2.2 | Propositional Refinement Calculus | 28 |
| 4.2.3 | Models of Refinement KAT | 29 |
| 4.2.4 | Assignment Laws | 29 |
| 4.2.5 | Simplified Refinement Laws | 30 |
| 4.2.6 | Refinement Examples | 30 |
| 5 | Components Based on Kleene Algebra with Domain | 31 |
| 5.1 | Verification Component for Backward Reasoning | 31 |
| 5.1.1 | Additional Facts for KAD | 31 |
| 5.1.2 | Syntax for Conditionals and Loops | 31 |
| 5.1.3 | Basic Weakest (Liberal) Precondition Calculus | 31 |
| 5.1.4 | Store and Assignment | 33 |
| 5.1.5 | Simplifications | 33 |
| 5.1.6 | Verification Examples | 34 |
| 5.1.7 | Verification Examples with Automated VCG | 36 |
| 5.2 | Verification Component for Forward Reasoning | 38 |

| | | |
|----------|--|-----------|
| 5.2.1 | Basic Strongest Postcondition Calculus | 38 |
| 5.2.2 | Floyd’s Assignment Rule | 39 |
| 5.2.3 | Verification Examples | 40 |
| 5.3 | Verification Component for Total Correctness | 42 |
| 5.3.1 | Relation Divergence Kleene Algebras | 42 |
| 5.3.2 | Meta-Equational Loop Rule | 43 |
| 5.3.3 | Noethericity and Absence of Divergence | 44 |
| 5.3.4 | Verification Examples | 45 |
| 5.4 | Two Extensions | 45 |
| 5.4.1 | KAD Component with Trace Semantics | 45 |
| 5.4.2 | KAD Component for Pointer Programs | 50 |
| 6 | Bringing KAT Components into Scope of KAD | 50 |
| 7 | Component for Recursive Programs | 52 |
| 7.1 | Lattice-Ordered Monoids with Domain | 52 |
| 7.2 | Boolean Monoids with Domain | 53 |
| 7.3 | Boolean Monoids with Range | 54 |
| 7.4 | Quantales | 55 |
| 7.5 | Domain Quantales | 56 |
| 7.6 | Boolean Domain Quantales | 57 |
| 7.7 | Relational Model of Boolean Domain Quantales | 58 |
| 7.8 | Modal Boolean Quantales | 58 |
| 7.9 | Recursion Rule | 58 |

1 Introductory Remarks

These Isabelle theories provide program construction and verification components for simple while programs based on variants of Kleene algebra with tests and Kleene algebra with domain, as well as a component for parameterless recursive programs based on domain quantales. The general approach consists in using the algebras for deriving verification conditions for the control flow of programs. They are linked by formal soundness proofs with denotational program semantics of the store and data domain—here predominantly with a relational semantics. Assignment laws can then be derived in this semantics. Program construction and verification tasks are performed within the concrete semantics as well; structured syntax for programs could easily be added, but is not provided at the moment.

All components are correct by construction relative to Isabelle’s small trustworthy core, as our soundness proofs make the axiomatic extensions provided by the algebras consistent with respect to it.

The main components are integrated into previous AFP entries for Kleene algebras [3], Kleene algebras with tests [1] and Kleene algebras with do-

main [5]. As an overview and perhaps for educational purposes, we have also added two standalone components based on Hoare logic and weakest (liberal) preconditions that use only Isabelle’s main libraries.

Background information on the general approach and the first main component, which is based on Kleene algebra with tests, can be found in [2]. An introduction to Kleene algebra with domain is given in [4]; a paper describing the corresponding verification component in detail is in preparation.

We are planning to add further components and expand and restructure the existing ones in the future. We would like to invite anyone interested in the algebraic approach to collaborate with us on these and contribute to this project.

2 Two Standalone Components

```
theory VC-KAT-scratch
  imports Main
begin
```

2.1 Component Based on Kleene Algebra with Tests

This component supports the verification and step-wise refinement of simple while programs in a partial correctness setting.

2.1.1 KAT: Definition and Basic Properties

```
notation times (infixl · 70)
```

```
class plus-ord = plus + ord +
  assumes less-eq-def:  $x \leq y \iff x + y = y$ 
  and less-def:  $x < y \iff x \leq y \wedge x \neq y$ 
```

```
class dioid = semiring + one + zero + plus-ord +
  assumes add-idem [simp]:  $x + x = x$ 
  and mult-one1 [simp]:  $1 \cdot x = x$ 
  and mult-one0 [simp]:  $x \cdot 1 = x$ 
  and add-zero1 [simp]:  $0 + x = x$ 
  and annil [simp]:  $0 \cdot x = 0$ 
  and annir [simp]:  $x \cdot 0 = 0$ 
```

```
begin
```

```
subclass monoid-mult
  ⟨proof⟩
```

```
subclass order
  ⟨proof⟩
```

lemma *mult-isol*: $x \leq y \implies z \cdot x \leq z \cdot y$
<proof>

lemma *mult-isor*: $x \leq y \implies x \cdot z \leq y \cdot z$
<proof>

lemma *add-iso*: $x \leq y \implies x + z \leq y + z$
<proof>

lemma *add-lub*: $x + y \leq z \iff x \leq z \wedge y \leq z$
<proof>

end

class *kleene-algebra* = *diod* +
 fixes *star* :: 'a \Rightarrow 'a (*-** [101] 100)
 assumes *star-unfoldl*: $1 + x \cdot x^* \leq x^*$
 and *star-unfoldr*: $1 + x^* \cdot x \leq x^*$
 and *star-inductl*: $z + x \cdot y \leq y \implies x^* \cdot z \leq y$
 and *star-inductr*: $z + y \cdot x \leq y \implies z \cdot x^* \leq y$

begin

lemma *star-sim*: $x \cdot y \leq z \cdot x \implies x \cdot y^* \leq z^* \cdot x$
<proof>

end

class *kat* = *kleene-algebra* +
 fixes *at* :: 'a \Rightarrow 'a
 assumes *test-one* [*simp*]: $at (at 1) = 1$
 and *test-mult* [*simp*]: $at (at (at (at x) \cdot at (at y))) = at (at y) \cdot at (at x)$
 and *test-mult-comp* [*simp*]: $at x \cdot at (at x) = 0$
 and *test-de-morgan*: $at x + at y = at (at (at x) \cdot at (at y))$

begin

definition *t-op* :: 'a \Rightarrow 'a (*t-* [100] 101) **where**
 $t x = at (at x)$

lemma *t-n* [*simp*]: $t (at x) = at x$
<proof>

lemma *t-comm*: $t x \cdot t y = t y \cdot t x$
<proof>

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

lemma *t-mult-closed* [*simp*]: $t (t x \cdot t y) = t x \cdot t y$
 ⟨*proof*⟩

2.1.2 Propositional Hoare Logic

definition *H* :: '*a* ⇒ '*a* ⇒ '*a* ⇒ bool **where**
 $H p x q \longleftrightarrow t p \cdot x \leq x \cdot t q$

definition *if-then-else* :: '*a* ⇒ '*a* ⇒ '*a* ⇒ '*a* (*if - then - else - fi* [64,64,64] 63)
where
 $if\ p\ then\ x\ else\ y\ fi = t p \cdot x + at\ p \cdot y$

definition *while* :: '*a* ⇒ '*a* ⇒ '*a* (*while - do - od* [64,64] 63) **where**
 $while\ p\ do\ x\ od = (t p \cdot x)^* \cdot at\ p$

definition *while-inv* :: '*a* ⇒ '*a* ⇒ '*a* ⇒ '*a* (*while - inv - do - od* [64,64,64] 63)
where
 $while\ p\ inv\ i\ do\ x\ od = while\ p\ do\ x\ od$

lemma *H-skip*: $H p 1 p$
 ⟨*proof*⟩

lemma *H-cons*: $t p \leq t p' \implies t q' \leq t q \implies H p' x q' \implies H p x q$
 ⟨*proof*⟩

lemma *H-seq*: $H r y q \implies H p x r \implies H p (x \cdot y) q$
 ⟨*proof*⟩

lemma *H-cond*: $H (t p \cdot t r) x q \implies H (t p \cdot at\ r) y q \implies H p (if\ r\ then\ x\ else\ y\ fi) q$
 ⟨*proof*⟩

lemma *H-loop*: $H (t p \cdot t r) x p \implies H p (while\ r\ do\ x\ od) (t p \cdot at\ r)$
 ⟨*proof*⟩

lemma *H-while-inv*: $t p \leq t i \implies t i \cdot at\ r \leq t q \implies H (t i \cdot t r) x i \implies H p (while\ r\ inv\ i\ do\ x\ od) q$
 ⟨*proof*⟩

end

2.1.3 Soundness and Relation KAT

notation *relcomp* (*infixl* ; 70)

interpretation *rel-d*: *dioid* *Id* { } (∪) (;) (⊆) (⊂)
 ⟨*proof*⟩

lemma (*in dioid*) *power-inductl*: $z + x \cdot y \leq y \implies x \hat{\ } i \cdot z \leq y$

<proof>

lemma (in *dioid*) *power-inductr*: $z + y \cdot x \leq y \implies z \cdot x^{\wedge} i \leq y$
<proof>

lemma *power-is-relpow*: $\text{rel-d.power } X \ i = X^{\wedge\wedge} i$
<proof>

lemma *rel-star-def*: $X^{\wedge*} = (\bigcup i. \text{rel-d.power } X \ i)$
<proof>

lemma *rel-star-contl*: $X ; Y^{\wedge*} = (\bigcup i. X ; \text{rel-d.power } Y \ i)$
<proof>

lemma *rel-star-contr*: $X^{\wedge*} ; Y = (\bigcup i. (\text{rel-d.power } X \ i) ; Y)$
<proof>

definition *rel-at* :: 'a rel \Rightarrow 'a rel **where**
 $\text{rel-at } X = \text{Id} \cap - X$

interpretation *rel-kat*: $\text{kat } \text{Id } \{ \} (\cup) (;) (\subseteq) (\subset) \text{rtrancl } \text{rel-at}$
<proof>

2.1.4 Embedding Predicates in Relations

type-synonym 'a pred = 'a \Rightarrow bool

abbreviation *p2r* :: 'a pred \Rightarrow 'a rel ($\lceil - \rceil$) **where**
 $\lceil P \rceil \equiv \{ (s, s) \mid s. P \ s \}$

lemma *t-p2r [simp]*: $\text{rel-kat.t-op } \lceil P \rceil = \lceil P \rceil$
<proof>

lemma *p2r-neg-hom [simp]*: $\text{rel-at } \lceil P \rceil = \lceil \lambda s. \neg P \ s \rceil$
<proof>

lemma *p2r-conj-hom [simp]*: $\lceil P \rceil \cap \lceil Q \rceil = \lceil \lambda s. P \ s \wedge Q \ s \rceil$
<proof>

lemma *p2r-conj-hom-var [simp]*: $\lceil P \rceil ; \lceil Q \rceil = \lceil \lambda s. P \ s \wedge Q \ s \rceil$
<proof>

lemma *p2r-disj-hom [simp]*: $\lceil P \rceil \cup \lceil Q \rceil = \lceil \lambda s. P \ s \vee Q \ s \rceil$
<proof>

lemma *impl-prop [simp]*: $\lceil P \rceil \subseteq \lceil Q \rceil \iff (\forall s. P \ s \longrightarrow Q \ s)$
<proof>

2.1.5 Store and Assignment

type-synonym $'a \text{ store} = \text{string} \Rightarrow 'a$

definition $\text{gets} :: \text{string} \Rightarrow ('a \text{ store} \Rightarrow 'a) \Rightarrow 'a \text{ store rel } (- ::= - [70, 65] 61)$
where

$v ::= e = \{(s, s(v := e s)) \mid s. \text{True}\}$

lemma *H-assign*: $\text{rel-kat.H } [\lambda s. P (s (v := e s))] (v ::= e) [P]$
 $\langle \text{proof} \rangle$

lemma *H-assign-var*: $(\forall s. P s \longrightarrow Q (s (v := e s))) \Longrightarrow \text{rel-kat.H } [P] (v ::= e) [Q]$
 $\langle \text{proof} \rangle$

abbreviation *H-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ pred} \Rightarrow \text{bool} (PRE - - POST - [64,64,64] 63)$ **where**
 $PRE P X POST Q \equiv \text{rel-kat.H } [P] X [Q]$

abbreviation *if-then-else-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel} (IF - THEN - ELSE - FI [64,64,64] 63)$ **where**
 $IF P THEN X ELSE Y FI \equiv \text{rel-kat.if-then-else } [P] X Y$

abbreviation *while-inv-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel} (WHILE - INV - DO - OD [64,64,64] 63)$ **where**
 $WHILE P INV I DO X OD \equiv \text{rel-kat.while-inv } [P] [I] X$

2.1.6 Verification Example

lemma *euclid*:

$PRE (\lambda s :: \text{nat store. } s ''x'' = x \wedge s ''y'' = y)$
 $(WHILE (\lambda s. s ''y'' \neq 0) INV (\lambda s. \text{gcd } (s ''x'') (s ''y'') = \text{gcd } x y)$
 DO
 $(''z'' ::= (\lambda s. s ''y''));$
 $(''y'' ::= (\lambda s. s ''x'' \text{ mod } s ''y''));$
 $(''x'' ::= (\lambda s. s ''z''))$
 $OD)$
 $POST (\lambda s. s ''x'' = \text{gcd } x y)$
 $\langle \text{proof} \rangle$

2.1.7 Definition of Refinement KAT

class $\text{rkat} = \text{kat} +$
fixes $R :: 'a \Rightarrow 'a \Rightarrow 'a$
assumes $R1: H p (R p q) q$
and $R2: H p x q \Longrightarrow x \leq R p q$

begin

2.1.8 Propositional Refinement Calculus

lemma *R-skip*: $1 \leq R p p$
 $\langle \text{proof} \rangle$

lemma *R-cons*: $t p \leq t p' \implies t q' \leq t q \implies R p' q' \leq R p q$
 $\langle \text{proof} \rangle$

lemma *R-seq*: $(R p r) \cdot (R r q) \leq R p q$
 $\langle \text{proof} \rangle$

lemma *R-cond*: *if* v *then* $(R (t v \cdot t p) q)$ *else* $(R (at v \cdot t p) q)$ *fi* $\leq R p q$
 $\langle \text{proof} \rangle$

lemma *R-loop*: *while* q *do* $(R (t p \cdot t q) p)$ *od* $\leq R p (t p \cdot at q)$
 $\langle \text{proof} \rangle$

end

2.1.9 Soundness and Relation RKAT

definition *rel-R* :: $'a \text{ rel} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel}$ **where**
 $\text{rel-R } P Q = \bigcup \{X. \text{rel-kat.H } P X Q\}$

interpretation *rel-rkat*: $\text{rkat } Id \ \{\} \ (\cup) \ (\cdot) \ (\subseteq) \ (\subset) \ \text{rtrancl } \text{rel-at } \text{rel-R}$
 $\langle \text{proof} \rangle$

2.1.10 Assignment Laws

lemma *R-assign*: $(\forall s. P s \longrightarrow Q (s (v := e s))) \implies (v ::= e) \subseteq \text{rel-R } [P] [Q]$
 $\langle \text{proof} \rangle$

lemma *R-assignr*: $(\forall s. Q' s \longrightarrow Q (s (v := e s))) \implies (\text{rel-R } [P] [Q']) ; (v ::= e) \subseteq \text{rel-R } [P] [Q]$
 $\langle \text{proof} \rangle$

lemma *R-assignl*: $(\forall s. P s \longrightarrow P' (s (v := e s))) \implies (v ::= e) ; (\text{rel-R } [P'] [Q]) \subseteq \text{rel-R } [P] [Q]$
 $\langle \text{proof} \rangle$

2.1.11 Refinement Example

lemma *var-swap-ref1*:

$\text{rel-R } [\lambda s. s''x'' = a \wedge s''y'' = b] [\lambda s. s''x'' = b \wedge s''y'' = a]$
 $\supseteq (s''z'' ::= (\lambda s. s''x'')); \text{rel-R } [\lambda s. s''z'' = a \wedge s''y'' = b] [\lambda s. s''x'' = b \wedge s''y'' = a]$
 $\langle \text{proof} \rangle$

lemma *var-swap-ref2*:

$\text{rel-R } [\lambda s. s''z'' = a \wedge s''y'' = b] [\lambda s. s''x'' = b \wedge s''y'' = a]$

\supseteq ($\text{"}x'' ::= (\lambda s. s \text{"}y'')$); $\text{rel-R } [\lambda s. s \text{"}z'' = a \wedge s \text{"}x'' = b] [\lambda s. s \text{"}x'' = b \wedge s \text{"}y'' = a]$
 $\langle \text{proof} \rangle$

lemma *var-swap-ref3*:

$\text{rel-R } [\lambda s. s \text{"}z'' = a \wedge s \text{"}x'' = b] [\lambda s. s \text{"}x'' = b \wedge s \text{"}y'' = a]$
 \supseteq ($\text{"}y'' ::= (\lambda s. s \text{"}z'')$); $\text{rel-R } [\lambda s. s \text{"}x'' = b \wedge s \text{"}y'' = a] [\lambda s. s \text{"}x'' = b \wedge s \text{"}y'' = a]$
 $\langle \text{proof} \rangle$

lemma *var-swap-ref-var*:

$\text{rel-R } [\lambda s. s \text{"}x'' = a \wedge s \text{"}y'' = b] [\lambda s. s \text{"}x'' = b \wedge s \text{"}y'' = a]$
 \supseteq ($\text{"}z'' ::= (\lambda s. s \text{"}x'')$); ($\text{"}x'' ::= (\lambda s. s \text{"}y'')$); ($\text{"}y'' ::= (\lambda s. s \text{"}z'')$)
 $\langle \text{proof} \rangle$

end

2.2 Component Based on Kleene Algebra with Domain

This component supports the verification and step-wise refinement of simple while programs in a partial correctness setting.

theory *VC-KAD-scratch*

imports *Main*

begin

2.2.1 KAD: Definitions and Basic Properties

notation *times* (**infixl** \cdot 70)

class *plus-ord* = *plus* + *ord* +
assumes *less-eq-def*: $x \leq y \longleftrightarrow x + y = y$
and *less-def*: $x < y \longleftrightarrow x \leq y \wedge x \neq y$

class *dioid* = *semiring* + *one* + *zero* + *plus-ord* +
assumes *add-idem* [*simp*]: $x + x = x$
and *mult-one1* [*simp*]: $1 \cdot x = x$
and *mult-one0* [*simp*]: $x \cdot 1 = x$
and *add-zero1* [*simp*]: $0 + x = x$
and *annil* [*simp*]: $0 \cdot x = 0$
and *annir* [*simp*]: $x \cdot 0 = 0$

begin

subclass *monoid-mult*

$\langle \text{proof} \rangle$

subclass *order*

$\langle \text{proof} \rangle$

lemma *mult-isor*: $x \leq y \implies x \cdot z \leq y \cdot z$
<proof>

lemma *mult-isol*: $x \leq y \implies z \cdot x \leq z \cdot y$
<proof>

lemma *add-iso*: $x \leq y \implies z + x \leq z + y$
<proof>

lemma *add-ub*: $x \leq x + y$
<proof>

lemma *add-lub*: $x + y \leq z \iff x \leq z \wedge y \leq z$
<proof>

end

class *kleene-algebra* = *diod* +
 fixes *star* :: 'a \Rightarrow 'a (*-** [101] 100)
 assumes *star-unfoldl*: $1 + x \cdot x^* \leq x^*$
 and *star-unfoldr*: $1 + x^* \cdot x \leq x^*$
 and *star-inductl*: $z + x \cdot y \leq y \implies x^* \cdot z \leq y$
 and *star-inductr*: $z + y \cdot x \leq y \implies z \cdot x^* \leq y$

begin

lemma *star-sim*: $x \cdot y \leq z \cdot x \implies x \cdot y^* \leq z^* \cdot x$
<proof>

end

class *antidomain-kleene-algebra* = *kleene-algebra* +
 fixes *ad* :: 'a \Rightarrow 'a (*ad*)
 assumes *as1* [*simp*]: $ad\ x \cdot x = 0$
 and *as2* [*simp*]: $ad\ (x \cdot y) + ad\ (x \cdot ad\ (ad\ y)) = ad\ (x \cdot ad\ (ad\ y))$
 and *as3* [*simp*]: $ad\ (ad\ x) + ad\ x = 1$

begin

definition *dom-op* :: 'a \Rightarrow 'a (*d*) **where**
 d $x = ad\ (ad\ x)$

lemma *a-subid-aux*: $ad\ x \cdot y \leq y$
<proof>

lemma *d1-a* [*simp*]: $d\ x \cdot x = x$
<proof>

lemma *a-mul-d* [*simp*]: $ad\ x \cdot d\ x = 0$

$\langle proof \rangle$

lemma *a-d-closed* [*simp*]: $d (ad x) = ad x$
 $\langle proof \rangle$

lemma *a-idem* [*simp*]: $ad x \cdot ad x = ad x$
 $\langle proof \rangle$

lemma *meet-ord*: $ad x \leq ad y \iff ad x \cdot ad y = ad x$
 $\langle proof \rangle$

lemma *d-wloc*: $x \cdot y = 0 \iff x \cdot d y = 0$
 $\langle proof \rangle$

lemma *gla-1*: $ad x \cdot y = 0 \implies ad x \leq ad y$
 $\langle proof \rangle$

lemma *a2-eq* [*simp*]: $ad (x \cdot d y) = ad (x \cdot y)$
 $\langle proof \rangle$

lemma *a-supdist*: $ad (x + y) \leq ad x$
 $\langle proof \rangle$

lemma *a-antitone*: $x \leq y \implies ad y \leq ad x$
 $\langle proof \rangle$

lemma *a-comm*: $ad x \cdot ad y = ad y \cdot ad x$
 $\langle proof \rangle$

lemma *a-closed* [*simp*]: $d (ad x \cdot ad y) = ad x \cdot ad y$
 $\langle proof \rangle$

lemma *a-exp* [*simp*]: $ad (ad x \cdot y) = d x + ad y$
 $\langle proof \rangle$

lemma *d1-sum-var*: $x + y \leq (d x + d y) \cdot (x + y)$
 $\langle proof \rangle$

lemma *a4*: $ad (x + y) = ad x \cdot ad y$
 $\langle proof \rangle$

lemma *kat-prop*: $d x \cdot y \leq y \cdot d z \iff d x \cdot y \cdot ad z = 0$
 $\langle proof \rangle$

lemma *shunt*: $ad x \leq ad y + ad z \iff ad x \cdot d y \leq ad z$
 $\langle proof \rangle$

2.2.2 wp Calculus

definition *if-then-else* :: 'a ⇒ 'a ⇒ 'a ⇒ 'a (*if - then - else - fi* [64,64,64] 63)

where

$$\text{if } p \text{ then } x \text{ else } y \text{ fi} = d p \cdot x + ad p \cdot y$$

definition *while* :: 'a ⇒ 'a ⇒ 'a (*while - do - od* [64,64] 63) **where**

$$\text{while } p \text{ do } x \text{ od} = (d p \cdot x)^* \cdot ad p$$

definition *while-inv* :: 'a ⇒ 'a ⇒ 'a ⇒ 'a (*while - inv - do - od* [64,64,64] 63)

where

$$\text{while } p \text{ inv } i \text{ do } x \text{ od} = \text{while } p \text{ do } x \text{ od}$$

definition *wp* :: 'a ⇒ 'a ⇒ 'a **where**

$$wp \ x \ p = ad \ (x \cdot ad \ p)$$

lemma *demod*: $d \ p \leq wp \ x \ q \iff d \ p \cdot x \leq x \cdot d \ q$

<proof>

lemma *wp-weaken*: $wp \ x \ p \leq wp \ (x \cdot ad \ q) \ (d \ p \cdot ad \ q)$

<proof>

lemma *wp-seq* [*simp*]: $wp \ (x \cdot y) \ q = wp \ x \ (wp \ y \ q)$

<proof>

lemma *wp-seq-var*: $p \leq wp \ x \ r \implies r \leq wp \ y \ q \implies p \leq wp \ (x \cdot y) \ q$

<proof>

lemma *wp-cond-var* [*simp*]: $wp \ (\text{if } p \text{ then } x \text{ else } y \text{ fi}) \ q = (ad \ p + wp \ x \ q) \cdot (d \ p + wp \ y \ q)$

<proof>

lemma *wp-cond-aux1* [*simp*]: $d \ p \cdot wp \ (\text{if } p \text{ then } x \text{ else } y \text{ fi}) \ q = d \ p \cdot wp \ x \ q$

<proof>

lemma *wp-cond-aux2* [*simp*]: $ad \ p \cdot wp \ (\text{if } p \text{ then } x \text{ else } y \text{ fi}) \ q = ad \ p \cdot wp \ y \ q$

<proof>

lemma *wp-cond* [*simp*]: $wp \ (\text{if } p \text{ then } x \text{ else } y \text{ fi}) \ q = (d \ p \cdot wp \ x \ q) + (ad \ p \cdot wp \ y \ q)$

<proof>

lemma *wp-star-induct-var*: $d \ q \leq wp \ x \ q \implies d \ q \leq wp \ (x^*) \ q$

<proof>

lemma *wp-while*: $d \ p \cdot d \ r \leq wp \ x \ p \implies d \ p \leq wp \ (\text{while } r \text{ do } x \text{ od}) \ (d \ p \cdot ad \ r)$

<proof>

lemma *wp-while-inv*: $d \ p \leq d \ i \implies d \ i \cdot ad \ r \leq d \ q \implies d \ i \cdot d \ r \leq wp \ x \ i \implies d \ p \leq wp \ (\text{while } r \text{ inv } i \text{ do } x \text{ od}) \ q$

<proof>

lemma *wp-while-inv-break*: $d p \leq wp\ y\ i \implies d\ i \cdot ad\ r \leq d\ q \implies d\ i \cdot d\ r \leq wp\ x\ i \implies d\ p \leq wp\ (y \cdot (while\ r\ inv\ i\ do\ x\ od))\ q$
<proof>

end

2.2.3 Soundness and Relation KAD

notation *relcomp* (**infixl** ; 70)

interpretation *rel-d*: *diod* *Id* { } (U) (;) (\subseteq) (\subset)
<proof>

lemma (**in** *diod*) *pow-inductl*: $z + x \cdot y \leq y \implies x \hat{\ } i \cdot z \leq y$
<proof>

lemma (**in** *diod*) *pow-inductr*: $z + y \cdot x \leq y \implies z \cdot x \hat{\ } i \leq y$
<proof>

lemma *power-is-relpow*: $rel\text{-}d.\text{power}\ X\ i = X \hat{\ } i$
<proof>

lemma *rel-star-def*: $X \hat{\ } * = (\bigcup i.\ rel\text{-}d.\text{power}\ X\ i)$
<proof>

lemma *rel-star-contl*: $X ; Y \hat{\ } * = (\bigcup i.\ X ; rel\text{-}d.\text{power}\ Y\ i)$
<proof>

lemma *rel-star-contr*: $X \hat{\ } * ; Y = (\bigcup i.\ (rel\text{-}d.\text{power}\ X\ i) ; Y)$
<proof>

definition *rel-ad* :: 'a *rel* \Rightarrow 'a *rel* **where**
 $rel\text{-}ad\ R = \{(x,x) \mid x. \neg (\exists y. (x,y) \in R)\}$

interpretation *rel-aka*: *antidomain-kleene-algebra* *Id* { } (U) (;) (\subseteq) (\subset) *rtrancl*
rel-ad
<proof>

2.2.4 Embedding Predicates in Relations

type-synonym 'a *pred* = 'a \Rightarrow *bool*

abbreviation *p2r* :: 'a *pred* \Rightarrow 'a *rel* (**[**-**]**) **where**
 $[P] \equiv \{(s,s) \mid s. P\ s\}$

lemma *d-p2r* [*simp*]: *rel-aka.dom-op* $[P] = [P]$
<proof>

lemma *p2r-neg-hom* [*simp*]: *rel-adj* $\lceil P \rceil = \lceil \lambda s. \neg P s \rceil$
 ⟨*proof*⟩

lemma *p2r-conj-hom* [*simp*]: $\lceil P \rceil \cap \lceil Q \rceil = \lceil \lambda s. P s \wedge Q s \rceil$
 ⟨*proof*⟩

lemma *p2r-conj-hom-var* [*simp*]: $\lceil P \rceil ; \lceil Q \rceil = \lceil \lambda s. P s \wedge Q s \rceil$
 ⟨*proof*⟩

lemma *p2r-disj-hom* [*simp*]: $\lceil P \rceil \cup \lceil Q \rceil = \lceil \lambda s. P s \vee Q s \rceil$
 ⟨*proof*⟩

2.2.5 Store and Assignment

type-synonym *'a store* = *string* \Rightarrow *'a*

definition *gets* :: *string* \Rightarrow (*'a store* \Rightarrow *'a*) \Rightarrow *'a store rel* (*- ::= -* [70, 65] 61)
where

v ::= e = $\{(s, s (v := e s)) \mid s. \text{True}\}$

lemma *wp-assign* [*simp*]: *rel-aka.wp* (*v ::= e*) $\lceil Q \rceil = \lceil \lambda s. Q (s (v := e s)) \rceil$
 ⟨*proof*⟩

abbreviation *spec-sugar* :: *'a pred* \Rightarrow *'a rel* \Rightarrow *'a pred* \Rightarrow *bool* (*PRE - - POST -*
 [64, 64, 64] 63) **where**

PRE P X POST Q \equiv *rel-aka.dom-op* $\lceil P \rceil \subseteq$ *rel-aka.wp* *X* $\lceil Q \rceil$

abbreviation *if-then-else-sugar* :: *'a pred* \Rightarrow *'a rel* \Rightarrow *'a rel* \Rightarrow *'a rel* (*IF - THEN -*
ELSE - FI [64, 64, 64] 63) **where**

IF P THEN X ELSE Y FI \equiv *rel-aka.if-then-else* $\lceil P \rceil$ *X Y*

abbreviation *while-inv-sugar* :: *'a pred* \Rightarrow *'a pred* \Rightarrow *'a rel* \Rightarrow *'a rel* (*WHILE -*
INV - DO - OD [64, 64, 64] 63) **where**

WHILE P INV I DO X OD \equiv *rel-aka.while-inv* $\lceil P \rceil$ $\lceil I \rceil$ *X*

2.2.6 Verification Example

lemma *euclid*:

PRE ($\lambda s :: \text{nat store. } s \text{ ''x''} = x \wedge s \text{ ''y''} = y$)
 (*WHILE* ($\lambda s. s \text{ ''y''} \neq 0$) *INV* ($\lambda s. \text{gcd} (s \text{ ''x''}) (s \text{ ''y''}) = \text{gcd } x y$)

DO

$(s \text{ ''z''} ::= (\lambda s. s \text{ ''y''}));$

$(s \text{ ''y''} ::= (\lambda s. s \text{ ''x''} \text{ mod } s \text{ ''y''}));$

$(s \text{ ''x''} ::= (\lambda s. s \text{ ''z''}))$

OD)

POST ($\lambda s. s \text{ ''x''} = \text{gcd } x y$)

⟨*proof*⟩

context *antidomain-kleene-algebra*

begin

2.2.7 Propositional Hoare Logic

definition $H :: 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow \text{bool}$ where
 $H\ p\ x\ q \longleftrightarrow d\ p \leq wp\ x\ q$

lemma *H-skip*: $H\ p\ 1\ p$
<proof>

lemma *H-cons*: $d\ p \leq d\ p' \Longrightarrow d\ q' \leq d\ q \Longrightarrow H\ p'\ x\ q' \Longrightarrow H\ p\ x\ q$
<proof>

lemma *H-seq*: $H\ p\ x\ r \Longrightarrow H\ r\ y\ q \Longrightarrow H\ p\ (x \cdot y)\ q$
<proof>

lemma *H-cond*: $H\ (d\ p \cdot d\ r)\ x\ q \Longrightarrow H\ (d\ p \cdot ad\ r)\ y\ q \Longrightarrow H\ p\ (\text{if } r \text{ then } x \text{ else } y\ fi)\ q$
<proof>

lemma *H-loop*: $H\ (d\ p \cdot d\ r)\ x\ p \Longrightarrow H\ p\ (\text{while } r \text{ do } x\ od)\ (d\ p \cdot ad\ r)$
<proof>

lemma *H-while-inv*: $d\ p \leq d\ i \Longrightarrow d\ i \cdot ad\ r \leq d\ q \Longrightarrow H\ (d\ i \cdot d\ r)\ x\ i \Longrightarrow H\ p\ (\text{while } r \text{ inv } i \text{ do } x\ od)\ q$
<proof>

end

2.2.8 Definition of Refinement KAD

class *rkad* = *antidomain-kleene-algebra* +
fixes $R :: 'a \Rightarrow 'a \Rightarrow 'a$
assumes *R-def*: $x \leq R\ p\ q \longleftrightarrow d\ p \leq wp\ x\ q$

begin

2.2.9 Propositional Refinement Calculus

lemma *HR*: $H\ p\ x\ q \longleftrightarrow x \leq R\ p\ q$
<proof>

lemma *wp-R1*: $d\ p \leq wp\ (R\ p\ q)\ q$
<proof>

lemma *wp-R2*: $x \leq R\ (wp\ x\ q)\ q$
<proof>

lemma *wp-R3*: $d\ p \leq wp\ x\ q \Longrightarrow x \leq R\ p\ q$
<proof>

lemma *H-R1*: $H\ p\ (R\ p\ q)\ q$

<proof>

lemma *H-R2*: $H\ p\ x\ q \implies x \leq R\ p\ q$
<proof>

lemma *R-skip*: $1 \leq R\ p\ p$
<proof>

lemma *R-cons*: $d\ p \leq d\ p' \implies d\ q' \leq d\ q \implies R\ p'\ q' \leq R\ p\ q$
<proof>

lemma *R-seq*: $(R\ p\ r) \cdot (R\ r\ q) \leq R\ p\ q$
<proof>

lemma *R-cond*: *if* v *then* $(R\ (d\ v \cdot d\ p)\ q)$ *else* $(R\ (ad\ v \cdot d\ p)\ q)$ *fi* $\leq R\ p\ q$
<proof>

lemma *R-loop*: *while* q *do* $(R\ (d\ p \cdot d\ q)\ p)$ *od* $\leq R\ p\ (d\ p \cdot ad\ q)$
<proof>

end

2.2.10 Soundness and Relation RKAD

definition *rel-R* :: '*a rel* \Rightarrow '*a rel* \Rightarrow '*a rel* **where**
 $rel-R\ P\ Q = \bigcup \{X. rel-aka.dom-op\ P \subseteq rel-aka.wp\ X\ Q\}$

interpretation *rel-rkad*: $rkad\ Id\ \{\} \ (\cup) \ (\cdot) \ (\subseteq) \ (\subset) \ rtrancl\ rel-ad\ rel-R$
<proof>

2.2.11 Assignment Laws

lemma *R-assign*: $(\forall s. P\ s \longrightarrow Q\ (s\ (v := e\ s))) \implies (v := e) \subseteq rel-R\ [P]\ [Q]$
<proof>

lemma *H-assign-var*: $(\forall s. P\ s \longrightarrow Q\ (s\ (v := e\ s))) \implies rel-aka.H\ [P]\ (v := e)\ [Q]$
<proof>

lemma *R-assignr*: $(\forall s. Q'\ s \longrightarrow Q\ (s\ (v := e\ s))) \implies (rel-R\ [P]\ [Q']) ; (v := e) \subseteq rel-R\ [P]\ [Q]$
<proof>

lemma *R-assignl*: $(\forall s. P\ s \longrightarrow P'\ (s\ (v := e\ s))) \implies (v := e) ; (rel-R\ [P']\ [Q]) \subseteq rel-R\ [P]\ [Q]$
<proof>

2.2.12 Refinement Example

lemma *var-swap-ref1*:

$rel-R \ [\lambda s. s \ 'x'' = a \wedge s \ 'y'' = b] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\supseteq ('z'' ::= (\lambda s. s \ 'x'')); rel-R \ [\lambda s. s \ 'z'' = a \wedge s \ 'y'' = b] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\langle proof \rangle$

lemma *var-swap-ref2*:

$rel-R \ [\lambda s. s \ 'z'' = a \wedge s \ 'y'' = b] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\supseteq ('x'' ::= (\lambda s. s \ 'y'')); rel-R \ [\lambda s. s \ 'z'' = a \wedge s \ 'x'' = b] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\langle proof \rangle$

lemma *var-swap-ref3*:

$rel-R \ [\lambda s. s \ 'z'' = a \wedge s \ 'x'' = b] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\supseteq ('y'' ::= (\lambda s. s \ 'z'')); rel-R \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\langle proof \rangle$

lemma *var-swap-ref-var*:

$rel-R \ [\lambda s. s \ 'x'' = a \wedge s \ 'y'' = b] \ [\lambda s. s \ 'x'' = b \wedge s \ 'y'' = a]$
 $\supseteq ('z'' ::= (\lambda s. s \ 'x'')); ('x'' ::= (\lambda s. s \ 'y'')); ('y'' ::= (\lambda s. s \ 'z''))$
 $\langle proof \rangle$

end

3 Isomorphisms Between Predicates, Sets and Relations

theory *P2S2R*

imports *Main*

begin

notation *relcomp* (**infixl** ; 70)

notation *inf* (**infixl** \sqcap 70)

notation *sup* (**infixl** \sqcup 65)

notation *Id-on* (*s2r*)

notation *Domain* (*r2s*)

notation *Collect* (*p2s*)

definition *rel-n* :: 'a rel \Rightarrow 'a rel **where**

$rel-n \equiv (\lambda X. Id \cap - X)$

lemma *subid-meet*: $R \subseteq Id \Rightarrow S \subseteq Id \Rightarrow R \cap S = R ; S$

$\langle proof \rangle$

3.1 Isomorphism Between Sets and Relations

lemma *srs*: $r2s \circ s2r = id$

<proof>

lemma *rsr*: $R \subseteq Id \implies s2r (r2s R) = R$
<proof>

lemma *s2r-inj*: *inj s2r*
<proof>

lemma *r2s-inj*: $R \subseteq Id \implies S \subseteq Id \implies r2s R = r2s S \implies R = S$
<proof>

lemma *s2r-surj*: $\forall R \subseteq Id. \exists A. R = s2r A$
<proof>

lemma *r2s-surj*: $\forall A. \exists R \subseteq Id. A = r2s R$
<proof>

lemma *s2r-union-hom*: $s2r (A \cup B) = s2r A \cup s2r B$
<proof>

lemma *s2r-inter-hom*: $s2r (A \cap B) = s2r A \cap s2r B$
<proof>

lemma *s2r-inter-hom-var*: $s2r (A \cap B) = s2r A ; s2r B$
<proof>

lemma *s2r-compl-hom*: $s2r (- A) = rel-n (s2r A)$
<proof>

lemma *r2s-union-hom*: $r2s (R \cup S) = r2s R \cup r2s S$
<proof>

lemma *r2s-inter-hom*: $R \subseteq Id \implies S \subseteq Id \implies r2s (R \cap S) = r2s R \cap r2s S$
<proof>

lemma *r2s-inter-hom-var*: $R \subseteq Id \implies S \subseteq Id \implies r2s (R ; S) = r2s R \cap r2s S$
<proof>

lemma *r2s-ad-hom*: $R \subseteq Id \implies r2s (rel-n R) = - r2s R$
<proof>

3.2 Isomorphism Between Predicates and Sets

type-synonym *'a pred* = *'a* \Rightarrow *bool*

definition *s2p* :: *'a set* \Rightarrow *'a pred* **where**
 $s2p S = (\lambda x. x \in S)$

lemma *sps* [*simp*]: $s2p \circ p2s = id$

<proof>

lemma *psp [simp]: p2s ∘ s2p = id*
<proof>

lemma *s2p-bij: bij s2p*
<proof>

lemma *p2s-bij: bij p2s*
<proof>

lemma *s2p-compl-hom: s2p (¬ A) = ¬ (s2p A)*
<proof>

lemma *s2p-inter-hom: s2p (A ∩ B) = (s2p A) ∩ (s2p B)*
<proof>

lemma *s2p-union-hom: s2p (A ∪ B) = (s2p A) ∪ (s2p B)*
<proof>

lemma *p2s-neg-hom: p2s (¬ P) = ¬ (p2s P)*
<proof>

lemma *p2s-conj-hom: p2s (P ∩ Q) = p2s P ∩ p2s Q*
<proof>

lemma *p2s-disj-hom: p2s (P ∪ Q) = p2s P ∪ p2s Q*
<proof>

3.3 Isomorphism Between Predicates and Relations

definition *p2r :: 'a pred ⇒ 'a rel* where
p2r P = {(s,s) | s. P s}

definition *r2p :: 'a rel ⇒ 'a pred* where
r2p R = (λx. x ∈ Domain R)

lemma *p2r-subid: p2r P ⊆ Id*
<proof>

lemma *p2s2r: p2r = s2r ∘ p2s*
<proof>

lemma *r2s2p: r2p = s2p ∘ r2s*
<proof>

lemma *prp [simp]: r2p ∘ p2r = id*
<proof>

lemma *rpr*: $R \subseteq Id \implies p2r (r2p R) = R$
<proof>

lemma *p2r-inj*: $inj\ p2r$
<proof>

lemma *r2p-inj*: $R \subseteq Id \implies S \subseteq Id \implies r2p R = r2p S \implies R = S$
<proof>

lemma *p2r-surj*: $\forall R \subseteq Id. \exists P. R = p2r P$
<proof>

lemma *r2p-surj*: $\forall P. \exists R \subseteq Id. P = r2p R$
<proof>

lemma *p2r-neg-hom*: $p2r (- P) = rel-n (p2r P)$
<proof>

lemma *p2r-conj-hom [simp]*: $p2r P \cap p2r Q = p2r (P \sqcap Q)$
<proof>

lemma *p2r-conj-hom-var [simp]*: $p2r P ; p2r Q = p2r (P \sqcap Q)$
<proof>

lemma *p2r-id-neg [simp]*: $Id \cap -\ p2r\ p = p2r (-p)$
<proof>

lemma *[simp]*: $p2r\ bot = \{\}$
<proof>

lemma *p2r-disj-hom [simp]*: $p2r P \cup p2r Q = p2r (P \sqcup Q)$
<proof>

lemma *r2p-ad-hom*: $R \subseteq Id \implies r2p (rel-n R) = - (r2p R)$
<proof>

lemma *r2p-inter-hom*: $R \subseteq Id \implies S \subseteq Id \implies r2p (R \cap S) = (r2p R) \sqcap (r2p S)$
<proof>

lemma *r2p-inter-hom-var*: $R \subseteq Id \implies S \subseteq Id \implies r2p (R ; S) = (r2p R) \sqcap (r2p S)$
<proof>

lemma *rel-to-pred-union-hom*: $R \subseteq Id \implies S \subseteq Id \implies r2p (R \cup S) = (r2p R) \sqcup (r2p S)$
<proof>

end

4 Components Based on Kleene Algebra with Tests

4.1 Verification Component

This component supports the verification of simple while programs in a partial correctness setting.

```
theory VC-KAT
imports ../P2S2R
          KAT-and-DRA.PHL-KAT
          KAT-and-DRA.KAT-Models
```

begin

This first part changes some of the facts from the AFP KAT theories. It should be added to KAT in the next AFP version. Currently these facts provide an interface between the KAT theories and the verification component.

```
no-notation if-then-else (if - then - else - fi [64,64,64] 63)
no-notation while (while - do - od [64,64] 63)
no-notation Archimedean-Field.ceiling ([-])
```

```
notation relcomp (infixl ; 70)
notation p2r ([-])
```

```
context kat
begin
```

4.1.1 Definitions of Hoare Triple

```
definition H :: 'a  $\Rightarrow$  'a  $\Rightarrow$  'a  $\Rightarrow$  bool where
  H p x q  $\longleftrightarrow$  t p  $\cdot$  x  $\leq$  x  $\cdot$  t q
```

```
lemma H-var1: H p x q  $\longleftrightarrow$  t p  $\cdot$  x  $\cdot$  n q = 0
  <proof>
```

```
lemma H-var2: H p x q  $\longleftrightarrow$  t p  $\cdot$  x = t p  $\cdot$  x  $\cdot$  t q
  <proof>
```

4.1.2 Syntax for Conditionals and Loops

```
definition ifthenelse :: 'a  $\Rightarrow$  'a  $\Rightarrow$  'a  $\Rightarrow$  'a (if - then - else - fi [64,64,64] 63)
where
  if p then x else y fi = (t p  $\cdot$  x + n p  $\cdot$  y)
```

```
definition while :: 'a  $\Rightarrow$  'a  $\Rightarrow$  'a (while - do - od [64,64] 63) where
  while b do x od = (t b  $\cdot$  x)*  $\cdot$  n b
```

```
definition while-inv :: 'a  $\Rightarrow$  'a  $\Rightarrow$  'a  $\Rightarrow$  'a (while - inv - do - od [64,64,64] 63)
where
```

$while\ p\ inv\ i\ do\ x\ od = while\ p\ do\ x\ od$

4.1.3 Propositional Hoare Logic

lemma *H-skip*: $H\ p\ 1\ p$
 $\langle proof \rangle$

lemma *H-cons-1*: $t\ p \leq t\ p' \implies H\ p'\ x\ q \implies H\ p\ x\ q$
 $\langle proof \rangle$

lemma *H-cons-2*: $t\ q' \leq t\ q \implies H\ p\ x\ q' \implies H\ p\ x\ q$
 $\langle proof \rangle$

lemma *H-cons*: $t\ p \leq t\ p' \implies t\ q' \leq t\ q \implies H\ p'\ x\ q' \implies H\ p\ x\ q$
 $\langle proof \rangle$

lemma *H-seq-swap*: $H\ p\ x\ r \implies H\ r\ y\ q \implies H\ p\ (x \cdot y)\ q$
 $\langle proof \rangle$

lemma *H-seq*: $H\ r\ y\ q \implies H\ p\ x\ r \implies H\ p\ (x \cdot y)\ q$
 $\langle proof \rangle$

lemma *H-exp1*: $H\ (t\ p \cdot t\ r)\ x\ q \implies H\ p\ (t\ r \cdot x)\ q$
 $\langle proof \rangle$

lemma *H-exp2*: $H\ p\ x\ q \implies H\ p\ (x \cdot t\ r)\ (t\ q \cdot t\ r)$
 $\langle proof \rangle$

lemma *H-cond-iff*: $H\ p\ (if\ r\ then\ x\ else\ y\ fi)\ q \iff H\ (t\ p \cdot t\ r)\ x\ q \wedge H\ (t\ p \cdot n\ r)\ y\ q$
 $\langle proof \rangle$

lemma *H-cond*: $H\ (t\ p \cdot t\ r)\ x\ q \implies H\ (t\ p \cdot n\ r)\ y\ q \implies H\ p\ (if\ r\ then\ x\ else\ y\ fi)\ q$
 $\langle proof \rangle$

lemma *H-loop*: $H\ (t\ p \cdot t\ r)\ x\ p \implies H\ p\ (while\ r\ do\ x\ od)\ (t\ p \cdot n\ r)$
 $\langle proof \rangle$

lemma *H-while-inv*: $t\ p \leq t\ i \implies t\ i \cdot n\ r \leq t\ q \implies H\ (t\ i \cdot t\ r)\ x\ i \implies H\ p\ (while\ r\ inv\ i\ do\ x\ od)\ q$
 $\langle proof \rangle$

Finally we prove a frame rule.

lemma *H-frame*: $H\ p\ x\ p \implies H\ q\ x\ r \implies H\ (t\ p \cdot t\ q)\ x\ (t\ p \cdot t\ r)$
 $\langle proof \rangle$

end

4.1.4 Store and Assignment

The proper verification component starts here.

type-synonym $'a \text{ store} = \text{string} \Rightarrow 'a$

lemma $t\text{-}p2r$ [simp]: $\text{rel-diod-tests.t } \lceil P \rceil = \lceil P \rceil$
 $\langle \text{proof} \rangle$

lemma impl-prop [simp]: $\lceil P \rceil \subseteq \lceil Q \rceil \iff (\forall s. P \ s \longrightarrow Q \ s)$
 $\langle \text{proof} \rangle$

lemma Id-simp [simp]: $\text{Id} \cap (- \ \text{Id} \cup X) = \text{Id} \cap X$
 $\langle \text{proof} \rangle$

lemma Id-p2r [simp]: $\text{Id} \cap \lceil P \rceil = \lceil P \rceil$
 $\langle \text{proof} \rangle$

lemma Id-p2r-simp [simp]: $\text{Id} \cap (- \ \text{Id} \cup \lceil P \rceil) = \lceil P \rceil$
 $\langle \text{proof} \rangle$

Next we derive the assignment command and assignment rules.

definition $\text{gets} :: \text{string} \Rightarrow ('a \text{ store} \Rightarrow 'a) \Rightarrow 'a \text{ store rel } (- ::= - \ [70, 65] \ 61)$
where

$v ::= e = \{(s, s \ (v := e \ s)) \mid s. \ \text{True}\}$

lemma H-assign-prop : $\lceil \lambda s. P \ (s \ (v := e \ s)) \rceil ; (v ::= e) = (v ::= e) ; \lceil P \rceil$
 $\langle \text{proof} \rangle$

lemma H-assign : $\text{rel-kat.H } \lceil \lambda s. P \ (s \ (v := e \ s)) \rceil (v ::= e) \lceil P \rceil$
 $\langle \text{proof} \rangle$

lemma H-assign-var : $(\forall s. P \ s \longrightarrow Q \ (s \ (v := e \ s))) \implies \text{rel-kat.H } \lceil P \rceil (v ::= e) \lceil Q \rceil$
 $\langle \text{proof} \rangle$

lemma H-assign-iff [simp]: $\text{rel-kat.H } \lceil P \rceil (v ::= e) \lceil Q \rceil \iff (\forall s. P \ s \longrightarrow Q \ (s \ (v := e \ s)))$
 $\langle \text{proof} \rangle$

lemma H-assign-floyd : $\text{rel-kat.H } \lceil P \rceil (v ::= e) \lceil \lambda s. \exists w. s \ v = e \ (s \ (v := w)) \wedge P \ (s \ (v := w)) \rceil$
 $\langle \text{proof} \rangle$

4.1.5 Simplified Hoare Rules

lemma sH-cons-1 : $\forall s. P \ s \longrightarrow P' \ s \implies \text{rel-kat.H } \lceil P' \rceil \ X \ \lceil Q \rceil \implies \text{rel-kat.H } \lceil P \rceil \ X \ \lceil Q \rceil$
 $\langle \text{proof} \rangle$

lemma *sH-cons-2*: $\forall s. Q' s \longrightarrow Q s \implies \text{rel-kat.H } [P] X [Q'] \implies \text{rel-kat.H } [P] X [Q]$

<proof>

lemma *sH-cons*: $\forall s. P s \longrightarrow P' s \implies \forall s. Q' s \longrightarrow Q s \implies \text{rel-kat.H } [P'] X [Q'] \implies \text{rel-kat.H } [P] X [Q]$

<proof>

lemma *sH-cond*: $\text{rel-kat.H } [P \sqcap T] X [Q] \implies \text{rel-kat.H } [P \sqcap \neg T] Y [Q] \implies \text{rel-kat.H } [P] (\text{rel-kat.ifthenelse } [T] X Y) [Q]$

<proof>

lemma *sH-cond-iff*: $\text{rel-kat.H } [P] (\text{rel-kat.ifthenelse } [T] X Y) [Q] \longleftrightarrow (\text{rel-kat.H } [P \sqcap T] X [Q] \wedge \text{rel-kat.H } [P \sqcap \neg T] Y [Q])$

<proof>

lemma *sH-while-inv*: $\forall s. P s \longrightarrow I s \implies \forall s. I s \wedge \neg R s \longrightarrow Q s \implies \text{rel-kat.H } [I \sqcap R] X [I]$

$\implies \text{rel-kat.H } [P] (\text{rel-kat.while-inv } [R] [I] X) [Q]$

<proof>

lemma *sH-H*: $\text{rel-kat.H } [P] X [Q] \longleftrightarrow (\forall s s'. P s \longrightarrow (s, s') \in X \longrightarrow Q s')$

<proof>

Finally we provide additional syntax for specifications and commands.

abbreviation *H-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ pred} \Rightarrow \text{bool}$ (*PRE - - POST* - [64,64,64] 63) **where**

$\text{PRE } P \text{ X } \text{POST } Q \equiv \text{rel-kat.H } [P] X [Q]$

abbreviation *if-then-else-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel}$ (*IF - THEN - ELSE - FI* [64,64,64] 63) **where**

$\text{IF } P \text{ THEN } X \text{ ELSE } Y \text{ FI} \equiv \text{rel-kat.ifthenelse } [P] X Y$

abbreviation *while-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel}$ (*WHILE - DO - OD* [64,64] 63) **where**

$\text{WHILE } P \text{ DO } X \text{ OD} \equiv \text{rel-kat.while } [P] X$

abbreviation *while-inv-sugar* :: $'a \text{ pred} \Rightarrow 'a \text{ pred} \Rightarrow 'a \text{ rel} \Rightarrow 'a \text{ rel}$ (*WHILE - INV - DO - OD* [64,64,64] 63) **where**

$\text{WHILE } P \text{ INV } I \text{ DO } X \text{ OD} \equiv \text{rel-kat.while-inv } [P] [I] X$

lemma *H-cond-iff2[simp]*: $\text{PRE } p \text{ (IF } r \text{ THEN } x \text{ ELSE } y \text{ FI) POST } q \longleftrightarrow (\text{PRE } (p \sqcap r) x \text{ POST } q) \wedge (\text{PRE } (p \sqcap \neg r) y \text{ POST } q)$

<proof>

end

4.1.6 Verification Examples

```
theory VC-KAT-Examples
  imports VC-KAT
begin
```

lemma *euclid*:

```
PRE ( $\lambda s::nat$  store.  $s \text{ ''}x'' = x \wedge s \text{ ''}y'' = y$ )
(WHILE ( $\lambda s. s \text{ ''}y'' \neq 0$ ) INV ( $\lambda s. gcd (s \text{ ''}x'') (s \text{ ''}y'') = gcd x y$ )
DO
  ( $\text{''}z'' ::= (\lambda s. s \text{ ''}y'')$ );
  ( $\text{''}y'' ::= (\lambda s. s \text{ ''}x'' mod s \text{ ''}y'')$ );
  ( $\text{''}x'' ::= (\lambda s. s \text{ ''}z'')$ )
OD)
POST ( $\lambda s. s \text{ ''}x'' = gcd x y$ )
<proof>
```

lemma *maximum*:

```
PRE ( $\lambda s:: nat$  store. True)
(IF ( $\lambda s. s \text{ ''}x'' \geq s \text{ ''}y''$ )
THEN ( $\text{''}z'' ::= (\lambda s. s \text{ ''}x'')$ )
ELSE ( $\text{''}z'' ::= (\lambda s. s \text{ ''}y'')$ )
FI)
POST ( $\lambda s. s \text{ ''}z'' = max (s \text{ ''}x'') (s \text{ ''}y'')$ )
<proof>
```

lemma *integer-division*:

```
PRE ( $\lambda s::nat$  store.  $s \text{ ''}x'' \geq 0$ )
( $\text{''}q'' ::= (\lambda s. 0)$ );
( $\text{''}r'' ::= (\lambda s. s \text{ ''}x'')$ );
(WHILE ( $\lambda s. s \text{ ''}y'' \leq s \text{ ''}r''$ ) INV ( $\lambda s. s \text{ ''}x'' = s \text{ ''}q'' * s \text{ ''}y'' + s \text{ ''}r'' \wedge s$ 
 $\text{''}r'' \geq 0$ )
DO
  ( $\text{''}q'' ::= (\lambda s. s \text{ ''}q'' + 1)$ );
  ( $\text{''}r'' ::= (\lambda s. s \text{ ''}r'' - s \text{ ''}y'')$ )
OD)
POST ( $\lambda s. s \text{ ''}x'' = s \text{ ''}q'' * s \text{ ''}y'' + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0 \wedge s \text{ ''}r'' < s \text{ ''}y''$ )
<proof>
```

lemma *imp-reverse*:

```
PRE ( $\lambda s:: 'a$  list store.  $s \text{ ''}x'' = X$ )
( $\text{''}y'' ::= (\lambda s. [])$ );
(WHILE ( $\lambda s. s \text{ ''}x'' \neq []$ ) INV ( $\lambda s. rev (s \text{ ''}x'') @ s \text{ ''}y'' = rev X$ )
DO
  ( $\text{''}y'' ::= (\lambda s. hd (s \text{ ''}x'') \# s \text{ ''}y'')$ );
  ( $\text{''}x'' ::= (\lambda s. tl (s \text{ ''}x''))$ )
OD)
POST ( $\lambda s. s \text{ ''}y'' = rev X$ )
<proof>
```

end

4.1.7 Verification Examples with Automated VCG

```
theory VC-KAT-Examples2
imports VC-KAT HOL-Eisbach.Eisbach
begin
```

The following simple tactic for verification condition generation has been implemented with the Eisbach proof methods language.

```
named-theorems hl-intro
```

```
declare sH-while-inv [hl-intro]
  rel-kat.H-seq [hl-intro]
  H-assign-var [hl-intro]
  rel-kat.H-cond [hl-intro]
```

```
method hoare = (rule hl-intro; hoare?)
```

lemma euclid:

```
PRE ( $\lambda s::\text{nat store. } s \text{ ''}x'' = x \wedge s \text{ ''}y'' = y$ )
(WHILE ( $\lambda s. s \text{ ''}y'' \neq 0$ ) INV ( $\lambda s. \text{gcd } (s \text{ ''}x'') (s \text{ ''}y'') = \text{gcd } x y$ )
DO
  ( $s \text{ ''}z'' ::= (\lambda s. s \text{ ''}y'')$ );
  ( $s \text{ ''}y'' ::= (\lambda s. s \text{ ''}x'' \bmod s \text{ ''}y'')$ );
  ( $s \text{ ''}x'' ::= (\lambda s. s \text{ ''}z'')$ )
OD)
POST ( $\lambda s. s \text{ ''}x'' = \text{gcd } x y$ )
<proof>
```

lemma integer-division:

```
PRE ( $\lambda s::\text{nat store. } s \text{ ''}x'' \geq 0$ )
  ( $s \text{ ''}q'' ::= (\lambda s. 0)$ );
  ( $s \text{ ''}r'' ::= (\lambda s. s \text{ ''}x'')$ );
(WHILE ( $\lambda s. s \text{ ''}y'' \leq s \text{ ''}r''$ ) INV ( $\lambda s. s \text{ ''}x'' = s \text{ ''}q'' * s \text{ ''}y'' + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0$ )
DO
  ( $s \text{ ''}q'' ::= (\lambda s. s \text{ ''}q'' + 1)$ );
  ( $s \text{ ''}r'' ::= (\lambda s. s \text{ ''}r'' - s \text{ ''}y'')$ )
OD)
POST ( $\lambda s. s \text{ ''}x'' = s \text{ ''}q'' * s \text{ ''}y'' + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0 \wedge s \text{ ''}r'' < s \text{ ''}y''$ )
<proof>
```

lemma imp-reverse:

```
PRE ( $\lambda s::\text{'a list store. } s \text{ ''}x'' = X$ )
  ( $s \text{ ''}y'' ::= (\lambda s. [])$ );
(WHILE ( $\lambda s. s \text{ ''}x'' \neq []$ ) INV ( $\lambda s. \text{rev } (s \text{ ''}x'') @ s \text{ ''}y'' = \text{rev } X$ )
DO
  ( $s \text{ ''}y'' ::= (\lambda s. \text{hd } (s \text{ ''}x'') \# s \text{ ''}y'')$ );
```

```

    ("x'' ::= (λs. tl (s 'x'))))
  OD)
  POST (λs. s 'y'' = rev X )
  ⟨proof⟩

```

end

4.2 Refinement Component

```

theory RKAT
  imports AVC-KAT/VC-KAT

```

begin

4.2.1 RKAT: Definition and Basic Properties

A refinement KAT is a KAT expanded by Morgan's specification statement.

```

class rkat = kat +
  fixes R :: 'a ⇒ 'a ⇒ 'a
  assumes spec-def: x ≤ R p q ⟷ H p x q

```

begin

```

lemma R1: H p (R p q) q
  ⟨proof⟩

```

```

lemma R2: H p x q ⟹ x ≤ R p q
  ⟨proof⟩

```

4.2.2 Propositional Refinement Calculus

```

lemma R-skip: 1 ≤ R p p
  ⟨proof⟩

```

```

lemma R-cons: t p ≤ t p' ⟹ t q' ≤ t q ⟹ R p' q' ≤ R p q
  ⟨proof⟩

```

```

lemma R-seq: (R p r) · (R r q) ≤ R p q
  ⟨proof⟩

```

```

lemma R-cond: if v then (R (t v · t p) q) else (R (n v · t p) q) fi ≤ R p q
  ⟨proof⟩

```

```

lemma R-loop: while q do (R (t p · t q) p) od ≤ R p (t p · n q)
  ⟨proof⟩

```

```

lemma R-zero-one: x ≤ R 0 1
  ⟨proof⟩

```

lemma *R-one-zero*: $R \ 1 \ 0 = 0$
 $\langle proof \rangle$

end

end

4.2.3 Models of Refinement KAT

theory *RKAT-Models*
imports *RKAT*

begin

So far only the relational model is developed.

definition *rel-R* :: $'a \ rel \Rightarrow 'a \ rel \Rightarrow 'a \ rel$ **where**
 $rel-R \ P \ Q = \bigcup \{X. \ rel-kat.H \ P \ X \ Q\}$

interpretation *rel-rkat*: $rkat \ (\cup) \ (;) \ Id \ \{\} \ (\subseteq) \ (\subset) \ rtrancl \ (\lambda X. \ Id \ \cap \ - \ X) \ rel-R$
 $\langle proof \rangle$

end

theory *VC-RKAT*
imports *../RKAT-Models*

begin

This component supports the step-wise refinement of simple while programs in a partial correctness setting.

4.2.4 Assignment Laws

The store model is taken from KAT

lemma *R-assign*: $(\forall s. \ P \ s \longrightarrow Q \ (s \ (v := e \ s))) \Longrightarrow (v ::= e) \subseteq \ rel-R \ [P] \ [Q]$
 $\langle proof \rangle$

lemma *R-assignr*: $(\forall s. \ Q' \ s \longrightarrow Q \ (s \ (v := e \ s))) \Longrightarrow (\rel-R \ [P] \ [Q']) ; (v ::= e) \subseteq \ rel-R \ [P] \ [Q]$
 $\langle proof \rangle$

lemma *R-assignl*: $(\forall s. \ P \ s \longrightarrow P' \ (s \ (v := e \ s))) \Longrightarrow (v ::= e) ; (\rel-R \ [P'] \ [Q]) \subseteq \ rel-R \ [P] \ [Q]$
 $\langle proof \rangle$

4.2.5 Simplified Refinement Laws

lemma *R-cons*: $(\forall s. P\ s \longrightarrow P'\ s) \Longrightarrow (\forall s. Q'\ s \longrightarrow Q\ s) \Longrightarrow \text{rel-R } [P']\ [Q']$
 $\subseteq \text{rel-R } [P]\ [Q]$
 ⟨proof⟩

lemma *if-then-else-ref*: $X \subseteq X' \Longrightarrow Y \subseteq Y' \Longrightarrow \text{IF } P\ \text{THEN } X\ \text{ELSE } Y\ \text{FI} \subseteq$
 $\text{IF } P\ \text{THEN } X'\ \text{ELSE } Y'\ \text{FI}$
 ⟨proof⟩

lemma *while-ref*: $X \subseteq X' \Longrightarrow \text{WHILE } P\ \text{DO } X\ \text{OD} \subseteq \text{WHILE } P\ \text{DO } X'\ \text{OD}$
 ⟨proof⟩

end

4.2.6 Refinement Examples

theory *VC-RKAT-Examples*
imports *VC-RKAT*
begin

Currently there is only one example, and no tactic for automating refinement proofs is provided.

lemma *var-swap-ref1*:

$\text{rel-R } [\lambda s. s\ \text{"x''} = a \wedge s\ \text{"y''} = b]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]$
 $\supseteq (\text{"z''} ::= (\lambda s. s\ \text{"x''})); \text{rel-R } [\lambda s. s\ \text{"z''} = a \wedge s\ \text{"y''} = b]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]$
 ⟨proof⟩

lemma *var-swap-ref2*:

$\text{rel-R } [\lambda s. s\ \text{"z''} = a \wedge s\ \text{"y''} = b]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]$
 $\supseteq (\text{"x''} ::= (\lambda s. s\ \text{"y''})); \text{rel-R } [\lambda s. s\ \text{"z''} = a \wedge s\ \text{"x''} = b]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]$
 ⟨proof⟩

lemma *var-swap-ref3*:

$\text{rel-R } [\lambda s. s\ \text{"z''} = a \wedge s\ \text{"x''} = b]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]$
 $\supseteq (\text{"y''} ::= (\lambda s. s\ \text{"z''})); \text{rel-R } [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"z''} = a]$
 ⟨proof⟩

lemma *var-swap-ref-var*:

$\text{rel-R } [\lambda s. s\ \text{"x''} = a \wedge s\ \text{"y''} = b]\ [\lambda s. s\ \text{"x''} = b \wedge s\ \text{"y''} = a]$
 $\supseteq (\text{"z''} ::= (\lambda s. s\ \text{"x''})); (\text{"x''} ::= (\lambda s. s\ \text{"y''})); (\text{"y''} ::= (\lambda s. s\ \text{"z''}))$
 ⟨proof⟩

end

5 Components Based on Kleene Algebra with Domain

theory *VC-KAD*

imports *KAD.Modal-Kleene-Algebra-Models ../P2S2R*

begin

5.1 Verification Component for Backward Reasoning

This component supports the verification of simple while programs in a partial correctness setting.

no-notation *Archimedean-Field.ceiling* ($\lceil _ \rceil$)

no-notation *Archimedean-Field.floor* ($\lfloor _ \rfloor$)

notation *p2r* ($\lceil _ \rceil$)

notation *r2p* ($\lfloor _ \rfloor$)

context *antidomain-kleene-algebra*

begin

5.1.1 Additional Facts for KAD

lemma *fbox-shunt*: $d p \cdot d q \leq |x| t \iff d p \leq ad q + |x| t$
<proof>

5.1.2 Syntax for Conditionals and Loops

definition *cond* :: $'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$ (*if - then - else - fi* [64,64,64] 63) **where**
if p then x else y fi = $d p \cdot x + ad p \cdot y$

definition *while* :: $'a \Rightarrow 'a \Rightarrow 'a$ (*while - do - od* [64,64] 63) **where**
while p do x od = $(d p \cdot x)^* \cdot ad p$

definition *whilei* :: $'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$ (*while - inv - do - od* [64,64,64] 63) **where**
while p inv i do x od = *while p do x od*

5.1.3 Basic Weakest (Liberal) Precondition Calculus

In the setting of Kleene algebra with domain, the wlp operator is the forward modal box operator of antidomain Kleene algebra.

lemma *fbox-export1*: $ad p + |x| q = |d p \cdot x| q$
<proof>

lemma *fbox-export2*: $|x| p \leq |x \cdot ad q| (d p \cdot ad q)$
<proof>

lemma *fbox-export3*: $|x \cdot ad\ p| \ q = |x| \ (d\ p + d\ q)$
 ⟨proof⟩

lemma *fbox-seq* [*simp*]: $|x \cdot y| \ q = |x| \ |y| \ q$
 ⟨proof⟩

lemma *fbox-seq-var*: $p' \leq |y| \ q \implies p \leq |x| \ p' \implies p \leq |x \cdot y| \ q$
 ⟨proof⟩

lemma *fbox-cond-var* [*simp*]: $|if\ p\ then\ x\ else\ y\ fi| \ q = (ad\ p + |x| \ q) \cdot (d\ p + |y| \ q)$
 ⟨proof⟩

lemma *fbox-cond-aux1* [*simp*]: $d\ p \cdot |if\ p\ then\ x\ else\ y\ fi| \ q = d\ p \cdot |x| \ q$
 ⟨proof⟩

lemma *fbox-cond-aux2* [*simp*]: $ad\ p \cdot |if\ p\ then\ x\ else\ y\ fi| \ q = ad\ p \cdot |y| \ q$
 ⟨proof⟩

lemma *fbox-cond* [*simp*]: $|if\ p\ then\ x\ else\ y\ fi| \ q = (d\ p \cdot |x| \ q) + (ad\ p \cdot |y| \ q)$
 ⟨proof⟩

lemma *fbox-cond-var2* [*simp*]: $|if\ p\ then\ x\ else\ y\ fi| \ q = if\ p\ then\ |x| \ q\ else\ |y| \ q\ fi$
 ⟨proof⟩

lemma *fbox-while-unfold*: $|while\ t\ do\ x\ od| \ p = (d\ t + d\ p) \cdot (ad\ t + |x| \ |while\ t\ do\ x\ od| \ p)$
 ⟨proof⟩

lemma *fbox-while-var1*: $d\ t \cdot |while\ t\ do\ x\ od| \ p = d\ t \cdot |x| \ |while\ t\ do\ x\ od| \ p$
 ⟨proof⟩

lemma *fbox-while-var2*: $ad\ t \cdot |while\ t\ do\ x\ od| \ p \leq d\ p$
 ⟨proof⟩

lemma *fbox-while*: $d\ p \cdot d\ t \leq |x| \ p \implies d\ p \leq |while\ t\ do\ x\ od| \ (d\ p \cdot ad\ t)$
 ⟨proof⟩

lemma *fbox-while-var*: $d\ p = |d\ t \cdot x| \ p \implies d\ p \leq |while\ t\ do\ x\ od| \ (d\ p \cdot ad\ t)$
 ⟨proof⟩

lemma *fbox-whilei*: $d\ p \leq d\ i \implies d\ i \cdot ad\ t \leq d\ q \implies d\ i \cdot d\ t \leq |x| \ i \implies d\ p \leq |while\ t\ inv\ i\ do\ x\ od| \ q$
 ⟨proof⟩

The next rule is used for dealing with while loops after a series of sequential steps.

lemma *fbox-whilei-break*: $d\ p \leq |y| \ i \implies d\ i \cdot ad\ t \leq d\ q \implies d\ i \cdot d\ t \leq |x| \ i \implies d\ p \leq |y \cdot (while\ t\ inv\ i\ do\ x\ od)| \ q$

$\langle proof \rangle$

Finally we derive a frame rule.

lemma *fbox-frame*: $d p \cdot x \leq x \cdot d p \implies d q \leq |x| t \implies d p \cdot d q \leq |x| (d p \cdot d t)$
 $\langle proof \rangle$

lemma *fbox-frame-var*: $d p \leq |x| p \implies d q \leq |x| t \implies d p \cdot d q \leq |x| (d p \cdot d t)$
 $\langle proof \rangle$

end

5.1.4 Store and Assignment

type-synonym *'a store* = *string* \Rightarrow *'a*

notation *rel-antidomain-kleene-algebra.fbox* (*wp*)
and *rel-antidomain-kleene-algebra.fdia* (*relfdia*)

definition *gets* :: *string* \Rightarrow (*'a store* \Rightarrow *'a*) \Rightarrow *'a store* *rel* ($- ::= -$ [70, 65] 61)
where

$$v ::= e = \{(s, s (v := e s)) \mid s. True\}$$

lemma *assign-prop*: $\lceil \lambda s. P (s (v := e s)) \rceil ; (v ::= e) = (v ::= e) ; \lceil P \rceil$
 $\langle proof \rangle$

lemma *wp-assign* [*simp*]: $wp (v ::= e) \lceil Q \rceil = \lceil \lambda s. Q (s (v := e s)) \rceil$
 $\langle proof \rangle$

lemma *wp-assign-var* [*simp*]: $\lfloor wp (v ::= e) \lceil Q \rceil \rfloor = (\lambda s. Q (s (v := e s)))$
 $\langle proof \rangle$

lemma *wp-assign-det*: $wp (v ::= e) \lceil Q \rceil = relfdia (v ::= e) \lceil Q \rceil$
 $\langle proof \rangle$

5.1.5 Simplifications

notation *rel-antidomain-kleene-algebra.ads-d* (*rdom*)

abbreviation *spec-sugar* :: *'a pred* \Rightarrow *'a rel* \Rightarrow *'a pred* \Rightarrow *bool* (*PRE* - - *POST* -
[64,64,64] 63) **where**
 $PRE P X POST Q \equiv rdom \lceil P \rceil \subseteq wp X \lceil Q \rceil$

abbreviation *cond-sugar* :: *'a pred* \Rightarrow *'a rel* \Rightarrow *'a rel* \Rightarrow *'a rel* (*IF* - *THEN* - *ELSE*
- *FI* [64,64,64] 63) **where**
 $IF P THEN X ELSE Y FI \equiv rel-antidomain-kleene-algebra.cond \lceil P \rceil X Y$

abbreviation *whilei-sugar* :: *'a pred* \Rightarrow *'a pred* \Rightarrow *'a rel* \Rightarrow *'a rel* (*WHILE* - *INV*
- *DO* - *OD* [64,64,64] 63) **where**
 $WHILE P INV I DO X OD \equiv rel-antidomain-kleene-algebra.whilei \lceil P \rceil \lceil I \rceil X$

lemma *d-p2r* [simp]: $\text{rdom } \lceil P \rceil = \lceil P \rceil$
 ⟨proof⟩

lemma *p2r-conj-hom-var-symm* [simp]: $\lceil P \rceil ; \lceil Q \rceil = \lceil P \sqcap Q \rceil$
 ⟨proof⟩

lemma *p2r-neg-hom* [simp]: $\text{rel-ad } \lceil P \rceil = \lceil \neg P \rceil$
 ⟨proof⟩

lemma *wp-trafo*: $\lfloor \text{wp } X \lceil Q \rceil \rfloor = (\lambda s. \forall s'. (s, s') \in X \longrightarrow Q s')$
 ⟨proof⟩

lemma *wp-trafo-var*: $\lfloor \text{wp } X \lceil Q \rceil \rfloor s = (\forall s'. (s, s') \in X \longrightarrow Q s')$
 ⟨proof⟩

lemma *wp-simp*: $\text{rdom } \lceil \lfloor \text{wp } X Q \rfloor \rceil = \text{wp } X Q$
 ⟨proof⟩

lemma *wp-simp-var* [simp]: $\text{wp } \lceil P \rceil \lceil Q \rceil = \lceil \neg P \sqcup Q \rceil$
 ⟨proof⟩

lemma *impl-prop* [simp]: $\lceil P \rceil \subseteq \lceil Q \rceil \longleftrightarrow (\forall s. P s \longrightarrow Q s)$
 ⟨proof⟩

lemma *p2r-eq-prop* [simp]: $\lceil P \rceil = \lceil Q \rceil \longleftrightarrow (\forall s. P s \longleftrightarrow Q s)$
 ⟨proof⟩

lemma *impl-prop-var* [simp]: $\text{rdom } \lceil P \rceil \subseteq \text{rdom } \lceil Q \rceil \longleftrightarrow (\forall s. P s \longrightarrow Q s)$
 ⟨proof⟩

lemma *p2r-eq-prop-var* [simp]: $\text{rdom } \lceil P \rceil = \text{rdom } \lceil Q \rceil \longleftrightarrow (\forall s. P s \longleftrightarrow Q s)$
 ⟨proof⟩

lemma *wp-whilei*: $(\forall s. P s \longrightarrow I s) \implies (\forall s. (I \sqcap \neg T) s \longrightarrow Q s) \implies (\forall s. (I \sqcap T) s \longrightarrow \lfloor \text{wp } X \lceil I \rceil \rfloor s)$
 $\implies (\forall s. P s \longrightarrow \lfloor \text{wp } (\text{WHILE } T \text{ INV } I \text{ DO } X \text{ OD}) \lceil Q \rceil \rfloor s)$
 ⟨proof⟩

end

5.1.6 Verification Examples

theory *VC-KAD-Examples*

imports *VC-KAD*

begin

lemma *euclid*:

$PRE (\lambda s::nat \text{ store. } s \text{ ''}x'' = x \wedge s \text{ ''}y'' = y)$
 $(WHILE (\lambda s. s \text{ ''}y'' \neq 0) INV (\lambda s. gcd (s \text{ ''}x'') (s \text{ ''}y'') = gcd x y)$
 DO
 $(s \text{ ''}z'' ::= (\lambda s. s \text{ ''}y''));$
 $(s \text{ ''}y'' ::= (\lambda s. s \text{ ''}x'' \bmod s \text{ ''}y''));$
 $(s \text{ ''}x'' ::= (\lambda s. s \text{ ''}z''))$
 $OD)$
 $POST (\lambda s. s \text{ ''}x'' = gcd x y)$
 $\langle proof \rangle$

lemma euclid-diff:

$PRE (\lambda s::nat \text{ store. } s \text{ ''}x'' = x \wedge s \text{ ''}y'' = y \wedge x > 0 \wedge y > 0)$
 $(WHILE (\lambda s. s \text{ ''}x'' \neq s \text{ ''}y'') INV (\lambda s. gcd (s \text{ ''}x'') (s \text{ ''}y'') = gcd x y)$
 DO
 $(IF (\lambda s. s \text{ ''}x'' > s \text{ ''}y'')$
 $THEN (s \text{ ''}x'' ::= (\lambda s. s \text{ ''}x'' - s \text{ ''}y''))$
 $ELSE (s \text{ ''}y'' ::= (\lambda s. s \text{ ''}y'' - s \text{ ''}x''))$
 $FI)$
 $OD)$
 $POST (\lambda s. s \text{ ''}x'' = gcd x y)$
 $\langle proof \rangle$

lemma variable-swap:

$PRE (\lambda s. s \text{ ''}x'' = a \wedge s \text{ ''}y'' = b)$
 $(s \text{ ''}z'' ::= (\lambda s. s \text{ ''}x''));$
 $(s \text{ ''}x'' ::= (\lambda s. s \text{ ''}y''));$
 $(s \text{ ''}y'' ::= (\lambda s. s \text{ ''}z''))$
 $POST (\lambda s. s \text{ ''}x'' = b \wedge s \text{ ''}y'' = a)$
 $\langle proof \rangle$

lemma maximum:

$PRE (\lambda s:: nat \text{ store. } True)$
 $(IF (\lambda s. s \text{ ''}x'' \geq s \text{ ''}y'')$
 $THEN (s \text{ ''}z'' ::= (\lambda s. s \text{ ''}x''))$
 $ELSE (s \text{ ''}z'' ::= (\lambda s. s \text{ ''}y''))$
 $FI)$
 $POST (\lambda s. s \text{ ''}z'' = max (s \text{ ''}x'') (s \text{ ''}y''))$
 $\langle proof \rangle$

lemma integer-division:

$PRE (\lambda s::nat \text{ store. } x \geq 0)$
 $(s \text{ ''}q'' ::= (\lambda s. 0));$
 $(s \text{ ''}r'' ::= (\lambda s. x));$
 $(WHILE (\lambda s. y \leq s \text{ ''}r'') INV (\lambda s. x = s \text{ ''}q'' * y + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0)$
 DO
 $(s \text{ ''}q'' ::= (\lambda s. s \text{ ''}q'' + 1));$
 $(s \text{ ''}r'' ::= (\lambda s. s \text{ ''}r'' - y))$
 $OD)$
 $POST (\lambda s. x = s \text{ ''}q'' * y + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0 \wedge s \text{ ''}r'' < y)$

<proof>

lemma factorial:

```
PRE ( $\lambda s::\text{nat store. True}$ )
  (" $x'' ::= (\lambda s. 0)$ ");
  (" $y'' ::= (\lambda s. 1)$ ");
  (WHILE ( $\lambda s. s''x'' \neq x0$ ) INV ( $\lambda s. s''y'' = \text{fact } (s''x'')$ )
  DO
    (" $x'' ::= (\lambda s. s''x'' + 1)$ ");
    (" $y'' ::= (\lambda s. s''y'' \cdot s''x'')$ )
  OD)
POST ( $\lambda s. s''y'' = \text{fact } x0$ )
<proof>
```

lemma my-power:

```
PRE ( $\lambda s::\text{nat store. True}$ )
  (" $i'' ::= (\lambda s. 0)$ ");
  (" $y'' ::= (\lambda s. 1)$ ");
  (WHILE ( $\lambda s. s''i'' < n$ ) INV ( $\lambda s. s''y'' = x \wedge (s''i'' \wedge s''i'' \leq n)$ )
  DO
    (" $y'' ::= (\lambda s. (s''y'' * x))$ ");
    (" $i'' ::= (\lambda s. s''i'' + 1)$ )
  OD)
POST ( $\lambda s. s''y'' = x \wedge n$ )
<proof>
```

lemma imp-reverse:

```
PRE ( $\lambda s::\text{'a list store. } s''x'' = X$ )
  (" $y'' ::= (\lambda s. [])$ ");
  (WHILE ( $\lambda s. s''x'' \neq []$ ) INV ( $\lambda s. \text{rev } (s''x'') @ s''y'' = \text{rev } X$ )
  DO
    (" $y'' ::= (\lambda s. \text{hd } (s''x'') \# s''y'')$ ");
    (" $x'' ::= (\lambda s. \text{tl } (s''x''))$ )
  OD)
POST ( $\lambda s. s''y'' = \text{rev } X$ )
<proof>
```

end

5.1.7 Verification Examples with Automated VCG

theory VC-KAD-Examples2

imports VC-KAD HOL-Eisbach.Eisbach

begin

We have provide a simple tactic in the Eisbach proof method language. Additional simplification steps are sometimes needed to bring the resulting verification conditions into shape for first-order automated theorem proving.

named-theorems *ht*

declare *rel-antidomain-kleene-algebra.fbox-whilei* [ht]
rel-antidomain-kleene-algebra.fbox-seq-var [ht]
subset-refl[ht]

method *hoare* = (rule ht; hoare?)

lemma *euclid2*:

PRE ($\lambda s::\text{nat store. } s \text{ ''}x'' = x \wedge s \text{ ''}y'' = y$)
(*WHILE* ($\lambda s. s \text{ ''}y'' \neq 0$) *INV* ($\lambda s. \text{gcd } (s \text{ ''}x'') (s \text{ ''}y'') = \text{gcd } x y$)
DO
($s \text{ ''}z'' ::= (\lambda s. s \text{ ''}y'')$);
($s \text{ ''}y'' ::= (\lambda s. s \text{ ''}x'' \text{ mod } s \text{ ''}y'')$);
($s \text{ ''}x'' ::= (\lambda s. s \text{ ''}z'')$)
OD)
POST ($\lambda s. s \text{ ''}x'' = \text{gcd } x y$)
⟨*proof*⟩

lemma *euclid-diff2*:

PRE ($\lambda s::\text{nat store. } s \text{ ''}x'' = x \wedge s \text{ ''}y'' = y \wedge x > 0 \wedge y > 0$)
(*WHILE* ($\lambda s. s \text{ ''}x'' \neq s \text{ ''}y''$) *INV* ($\lambda s. \text{gcd } (s \text{ ''}x'') (s \text{ ''}y'') = \text{gcd } x y$)
DO
(*IF* ($\lambda s. s \text{ ''}x'' > s \text{ ''}y''$)
THEN ($s \text{ ''}x'' ::= (\lambda s. s \text{ ''}x'' - s \text{ ''}y'')$)
ELSE ($s \text{ ''}y'' ::= (\lambda s. s \text{ ''}y'' - s \text{ ''}x'')$)
FI)
OD)
POST ($\lambda s. s \text{ ''}x'' = \text{gcd } x y$)
⟨*proof*⟩

lemma *integer-division2*:

PRE ($\lambda s::\text{nat store. } x \geq 0$)
($s \text{ ''}q'' ::= (\lambda s. 0)$);
($s \text{ ''}r'' ::= (\lambda s. x)$);
(*WHILE* ($\lambda s. y \leq s \text{ ''}r''$) *INV* ($\lambda s. x = s \text{ ''}q'' * y + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0$)
DO
($s \text{ ''}q'' ::= (\lambda s. s \text{ ''}q'' + 1)$);
($s \text{ ''}r'' ::= (\lambda s. s \text{ ''}r'' - y)$)
OD)
POST ($\lambda s. x = s \text{ ''}q'' * y + s \text{ ''}r'' \wedge s \text{ ''}r'' \geq 0 \wedge s \text{ ''}r'' < y$)
⟨*proof*⟩

lemma *factorial2*:

PRE ($\lambda s::\text{nat store. True}$)
($s \text{ ''}x'' ::= (\lambda s. 0)$);
($s \text{ ''}y'' ::= (\lambda s. 1)$);
(*WHILE* ($\lambda s. s \text{ ''}x'' \neq x0$) *INV* ($\lambda s. s \text{ ''}y'' = \text{fact } (s \text{ ''}x'')$)
DO
($s \text{ ''}x'' ::= (\lambda s. s \text{ ''}x'' + 1)$);

```

  ("y'' ::= (λs. s ''y'' . s ''x''))
  OD
  POST (λs. s ''y'' = fact x0)
  ⟨proof⟩

```

lemma *my-power2*:

```

  PRE (λs::nat store. True)
  ("i'' ::= (λs. 0));
  ("y'' ::= (λs. 1));
  (WHILE (λs. s ''i'' < n) INV (λs. s ''y'' = x ^ (s ''i'' ) ∧ s ''i'' ≤ n)
  DO
    ("y'' ::= (λs. (s ''y'' ) * x));
    ("i'' ::= (λs. s ''i'' + 1))
  OD
  POST (λs. s ''y'' = x ^ n)
  ⟨proof⟩

```

lemma *imp-reverse2*:

```

  PRE (λs::'a list store. s ''x'' = X)
  ("y'' ::= (λs. []));
  (WHILE (λs. s ''x'' ≠ [] ) INV (λs. rev (s ''x'' ) @ s ''y'' = rev X)
  DO
    ("y'' ::= (λs. hd (s ''x'' ) # s ''y'' ));
    ("x'' ::= (λs. tl (s ''x'' )))
  OD
  POST (λs. s ''y'' = rev X )
  ⟨proof⟩

```

end

5.2 Verification Component for Forward Reasoning

```

theory VC-KAD-dual
  imports VC-KAD
begin

```

```

context modal-kleene-algebra
begin

```

This component supports the verification of simple while programs in a partial correctness setting.

5.2.1 Basic Strongest Postcondition Calculus

In modal Kleene algebra, strongest postconditions are backward diamond operators. These are linked with forward boxes aka weakest preconditions by a Galois connection. This duality has been implemented in the AFP entry for Kleene algebra with domain and is picked up automatically in the following proofs.

lemma *r-ad* [*simp*]: $r (ad\ p) = ad\ p$
 ⟨*proof*⟩

lemma *bdia-export1*: $\langle x \mid (r\ p \cdot r\ t) \rangle = \langle r\ t \cdot x \mid p \rangle$
 ⟨*proof*⟩

lemma *bdia-export2*: $r\ p \cdot \langle x \mid q \rangle = \langle x \cdot r\ p \mid q \rangle$
 ⟨*proof*⟩

lemma *bdia-seq* [*simp*]: $\langle x \cdot y \mid q \rangle = \langle y \mid \langle x \mid q \rangle$
 ⟨*proof*⟩

lemma *bdia-seq-var*: $\langle x \mid p \leq p' \implies \langle y \mid p' \leq q \implies \langle x \cdot y \mid p \leq q \rangle$
 ⟨*proof*⟩

lemma *bdia-cond-var* [*simp*]: $\langle if\ p\ then\ x\ else\ y\ fi \mid q \rangle = \langle x \mid (d\ p \cdot r\ q) \rangle + \langle y \mid (ad\ p \cdot r\ q) \rangle$
 ⟨*proof*⟩

lemma *bdia-while*: $\langle x \mid (d\ t \cdot r\ p) \leq r\ p \implies \langle while\ t\ do\ x\ od \mid p \leq r\ p \cdot ad\ t \rangle$
 ⟨*proof*⟩

lemma *bdia-whilei*: $r\ p \leq r\ i \implies r\ i \cdot ad\ t \leq r\ q \implies \langle x \mid (d\ t \cdot r\ i) \leq r\ i \implies \langle while\ t\ inv\ i\ do\ x\ od \mid p \leq r\ q \rangle$
 ⟨*proof*⟩

lemma *bdia-whilei-break*: $\langle y \mid p \leq r\ i \implies r\ i \cdot ad\ t \leq r\ q \implies \langle x \mid (d\ t \cdot r\ i) \leq r\ i \implies \langle y \cdot (while\ t\ inv\ i\ do\ x\ od) \mid p \leq r\ q \rangle$
 ⟨*proof*⟩

end

5.2.2 Floyd's Assignment Rule

lemma *bdia-assign* [*simp*]: *rel-antirange-kleene-algebra.bdia* $(v ::= e) \lceil P \rceil = \lceil \lambda s. \exists w. s\ v = e\ (s(v := w)) \wedge P\ (s(v := w)) \rceil$
 ⟨*proof*⟩

lemma *d-p2r* [*simp*]: *rel-antirange-kleene-algebra.ars-r* $\lceil P \rceil = \lceil P \rceil$
 ⟨*proof*⟩

abbreviation *fspec-sugar* :: 'a *pred* \implies 'a *rel* \implies 'a *pred* \implies *bool* (*FPRE* - - *POST* - $[64, 64, 64]$ 63) **where**

FPRE $P\ X\ POST\ Q \equiv$ *rel-antirange-kleene-algebra.bdia* $X \lceil P \rceil \subseteq$ *rel-antirange-kleene-algebra.ars-r* $\lceil Q \rceil$

end

5.2.3 Verification Examples

theory *VC-KAD-dual-Examples*

imports *VC-KAD-dual*

begin

The proofs are essentially the same as with forward boxes.

lemma *euclid*:

```

FPRE ( $\lambda s::\text{nat}$  store.  $s \text{''}x'' = x \wedge s \text{''}y'' = y$ )
  (WHILE ( $\lambda s. s \text{''}y'' \neq 0$ ) INV ( $\lambda s. \text{gcd } (s \text{''}x'') (s \text{''}y'') = \text{gcd } x y$ )
    DO
      ( $\text{''}z'' ::= (\lambda s. s \text{''}y'')$ );
      ( $\text{''}y'' ::= (\lambda s. s \text{''}x'' \bmod s \text{''}y'')$ );
      ( $\text{''}x'' ::= (\lambda s. s \text{''}z'')$ )
    OD)
POST ( $\lambda s. s \text{''}x'' = \text{gcd } x y$ )
<proof>

```

lemma *euclid-diff*:

```

FPRE ( $\lambda s::\text{nat}$  store.  $s \text{''}x'' = x \wedge s \text{''}y'' = y \wedge x > 0 \wedge y > 0$ )
  (WHILE ( $\lambda s. s \text{''}x'' \neq s \text{''}y''$ ) INV ( $\lambda s. \text{gcd } (s \text{''}x'') (s \text{''}y'') = \text{gcd } x y$ )
    DO
      (IF ( $\lambda s. s \text{''}x'' > s \text{''}y''$ )
        THEN ( $\text{''}x'' ::= (\lambda s. s \text{''}x'' - s \text{''}y'')$ )
        ELSE ( $\text{''}y'' ::= (\lambda s. s \text{''}y'' - s \text{''}x'')$ )
      FI)
    OD)
POST ( $\lambda s. s \text{''}x'' = \text{gcd } x y$ )
<proof>

```

lemma *variable-swap*:

```

FPRE ( $\lambda s. s \text{''}x'' = a \wedge s \text{''}y'' = b$ )
  ( $\text{''}z'' ::= (\lambda s. s \text{''}x'')$ );
  ( $\text{''}x'' ::= (\lambda s. s \text{''}y'')$ );
  ( $\text{''}y'' ::= (\lambda s. s \text{''}z'')$ )
POST ( $\lambda s. s \text{''}x'' = b \wedge s \text{''}y'' = a$ )
<proof>

```

lemma *maximum*:

```

FPRE ( $\lambda s::\text{nat}$  store. True)
  (IF ( $\lambda s. s \text{''}x'' \geq s \text{''}y''$ )
    THEN ( $\text{''}z'' ::= (\lambda s. s \text{''}x'')$ )
    ELSE ( $\text{''}z'' ::= (\lambda s. s \text{''}y'')$ )
  FI)
POST ( $\lambda s. s \text{''}z'' = \max (s \text{''}x'') (s \text{''}y'')$ )
<proof>

```

lemma *integer-division*:

```

FPRE ( $\lambda s::\text{nat}$  store.  $x \geq 0$ )

```


$(\text{"}q'' ::= (\lambda s. 0));$
 $(\text{"}r'' ::= (\lambda s. x));$
 $(\text{WHILE } (\lambda s. y \leq s \text{"}r'') \text{ INV } (\lambda s. x = s \text{"}q'' * y + s \text{"}r'' \wedge s \text{"}r'' \geq 0)$
 DO
 $(\text{"}q'' ::= (\lambda s. s \text{"}q'' + 1));$
 $(\text{"}r'' ::= (\lambda s. s \text{"}r'' - y))$
 OD
 $\text{POST } (\lambda s. x = s \text{"}q'' * y + s \text{"}r'' \wedge s \text{"}r'' \geq 0 \wedge s \text{"}r'' < y)$
 $\langle \text{proof} \rangle$

lemma factorial:

$\text{FPRE } (\lambda s::\text{nat store. True})$
 $(\text{"}x'' ::= (\lambda s. 0));$
 $(\text{"}y'' ::= (\lambda s. 1));$
 $(\text{WHILE } (\lambda s. s \text{"}x'' \neq x0) \text{ INV } (\lambda s. s \text{"}y'' = \text{fact } (s \text{"}x''))$
 DO
 $(\text{"}x'' ::= (\lambda s. s \text{"}x'' + 1));$
 $(\text{"}y'' ::= (\lambda s. s \text{"}y'' \cdot s \text{"}x''))$
 OD
 $\text{POST } (\lambda s. s \text{"}y'' = \text{fact } x0)$
 $\langle \text{proof} \rangle$

lemma my-power:

$\text{FPRE } (\lambda s::\text{nat store. True})$
 $(\text{"}i'' ::= (\lambda s. 0));$
 $(\text{"}y'' ::= (\lambda s. 1));$
 $(\text{WHILE } (\lambda s. s \text{"}i'' < n) \text{ INV } (\lambda s. s \text{"}y'' = x \wedge (s \text{"}i'' \wedge s \text{"}i'' \leq n)$
 DO
 $(\text{"}y'' ::= (\lambda s. (s \text{"}y'' * x));$
 $(\text{"}i'' ::= (\lambda s. s \text{"}i'' + 1))$
 OD
 $\text{POST } (\lambda s. s \text{"}y'' = x \wedge n)$
 $\langle \text{proof} \rangle$

lemma imp-reverse:

$\text{FPRE } (\lambda s::\text{'a list store. } s \text{"}x'' = X)$
 $(\text{"}y'' ::= (\lambda s. []));$
 $(\text{WHILE } (\lambda s. s \text{"}x'' \neq []) \text{ INV } (\lambda s. \text{rev } (s \text{"}x'') @ s \text{"}y'' = \text{rev } X)$
 DO
 $(\text{"}y'' ::= (\lambda s. \text{hd } (s \text{"}x'') \# s \text{"}y''));$
 $(\text{"}x'' ::= (\lambda s. \text{tl } (s \text{"}x'')))$
 OD
 $\text{POST } (\lambda s. s \text{"}y'' = \text{rev } X)$
 $\langle \text{proof} \rangle$

end

5.3 Verification Component for Total Correctness

theory *VC-KAD-wf*

imports *VC-KAD KAD.Modal-Kleene-Algebra-Applications*

begin

This component supports the verification of simple while programs in a total correctness setting.

5.3.1 Relation Divergence Kleene Algebras

Divergence Kleene algebras have been formalised in the AFP entry for Kleene algebra with domain. The nabla or divergence operation models those states of a relation from which infinitely ascending chains may start.

definition *rel-nabla* :: 'a rel \Rightarrow 'a rel **where**
 $rel-nabla X = \bigcup \{P. P \subseteq relfdia X P\}$

definition *rel-nabla-bin* :: 'a rel \Rightarrow 'a rel \Rightarrow 'a rel **where**
 $rel-nabla-bin X Q = \bigcup \{P. P \subseteq relfdia X P \cup rdom Q\}$

lemma *rel-nabla-d-closed* [*simp*]: $rdom (rel-nabla x) = rel-nabla x$
<proof>

lemma *rel-nabla-bin-d-closed* [*simp*]: $rdom (rel-nabla-bin x q) = rel-nabla-bin x q$
<proof>

lemma *rel-nabla-unfold*: $rel-nabla X \subseteq relfdia X (rel-nabla X)$
<proof>

lemma *rel-nabla-bin-unfold*: $rel-nabla-bin X Q \subseteq relfdia X (rel-nabla-bin X Q) \cup rdom Q$
<proof>

lemma *rel-nabla-coinduct-var*: $P \subseteq relfdia X P \Longrightarrow P \subseteq rel-nabla X$
<proof>

lemma *rel-nabla-bin-coinduct*: $P \subseteq relfdia X P \cup rdom Q \Longrightarrow P \subseteq rel-nabla-bin X Q$
<proof>

The two fusion lemmas are, in fact, hard-coded fixpoint fusion proofs. They might be replaced by more generic fusion proofs eventually.

lemma *nabla-fusion1*: $rel-nabla X \cup relfdia (X^*) Q \subseteq rel-nabla-bin X Q$
<proof>

lemma *rel-ad-inter-seq*: $rel-ad X \cap rel-ad Y = rel-ad X ; rel-ad Y$

<proof>

lemma *fusion2-aux2*: $\text{rdom } (\text{rel-nabla-bin } X \ Q) \subseteq \text{rdom } (\text{rel-nabla-bin } X \ Q \cap \text{rel-ad } (\text{relfdia } (X^*) \ Q) \cup \text{relfdia } (X^*) \ Q)$
<proof>

lemma *nabla-fusion2*: $\text{rel-nabla-bin } X \ Q \subseteq \text{rel-nabla } X \cup \text{relfdia } (X^*) \ Q$
<proof>

lemma *rel-nabla-coinduct*: $P \subseteq \text{relfdia } X \ P \cup \text{rdom } Q \implies P \subseteq \text{rel-nabla } X \cup \text{relfdia } (\text{rtrancl } X) \ Q$
<proof>

interpretation *rel-fdivka*: *fdivergences-kleene-algebra rel-ad* (\cup) ($;$) *Id* $\{\}$ (\subseteq) (\subset)
rtrancl rel-nabla
<proof>

5.3.2 Meta-Equational Loop Rule

context *fdivergences-kleene-algebra*

begin

The rule below is inspired by Arden' rule from language theory. It can be used in total correctness proofs.

lemma *fdia-arden*: $\nabla x = 0 \implies d \ p \leq d \ q + |x\rangle \ p \implies d \ p \leq |x^*\rangle \ q$
<proof>

lemma *fdia-arden-eq*: $\nabla x = 0 \implies d \ p = d \ q + |x\rangle \ p \implies d \ p = |x^*\rangle \ q$
<proof>

lemma *fdia-arden-iff*: $\nabla x = 0 \implies (d \ p = d \ q + |x\rangle \ p \longleftrightarrow d \ p = |x^*\rangle \ q)$
<proof>

lemma $|x^*\rangle \ p \leq |x\rangle \ p$
<proof>

lemma *fbox-arden*: $\nabla x = 0 \implies d \ q \cdot |x\rangle \ p \leq d \ p \implies |x^*\rangle \ q \leq d \ p$
<proof>

lemma *fbox-arden-eq*: $\nabla x = 0 \implies d \ q \cdot |x\rangle \ p = d \ p \implies |x^*\rangle \ q = d \ p$
<proof>

lemma *fbox-arden-iff*: $\nabla x = 0 \implies (d \ p = d \ q \cdot |x\rangle \ p \longleftrightarrow d \ p = |x^*\rangle \ q)$
<proof>

lemma *fbox-arden-while-iff*: $\nabla (d \ t \cdot x) = 0 \implies (d \ p = (d \ t + d \ q) \cdot |d \ t \cdot x\rangle \ p \longleftrightarrow d \ p = |\text{while } t \text{ do } x \text{ od}\rangle \ q)$
<proof>

lemma *fbx-arden-whilei*: $\nabla (d t \cdot x) = 0 \implies (d i = (d t + d q) \cdot |d t \cdot x] i \implies d i = |while t inv i do x od] q)$
 ⟨proof⟩

lemma *fbx-arden-whilei-iff*: $\nabla (d t \cdot x) = 0 \implies (d i = (d t + d q) \cdot |d t \cdot x] i \iff d i = |while t inv i do x od] q)$
 ⟨proof⟩

5.3.3 Noethericity and Absence of Divergence

Noetherian elements have been defined in the AFP entry for Kleene algebra with domain. First we show that noethericity and absence of divergence coincide. Then we turn to the relational model and show that noetherian relations model terminating programs.

lemma *noether-nabla*: *Noetherian* $x \implies \nabla x = 0$
 ⟨proof⟩

lemma *nabla-noether-iff*: *Noetherian* $x \iff \nabla x = 0$
 ⟨proof⟩

lemma *nabla-preloeb-iff*: $\nabla x = 0 \iff \text{PreLoebian } x$
 ⟨proof⟩

end

lemma *rel-nabla-prop*: $\text{rel-nabla } R = \{\} \iff (\forall P. P \subseteq \text{relfdia } R P \longrightarrow P = \{\})$
 ⟨proof⟩

lemma *fdia-rel-im1*: $s2r ((\text{converse } R) \text{ `` } P) = \text{relfdia } R (s2r P)$
 ⟨proof⟩

lemma *fdia-rel-im2*: $s2r ((\text{converse } R) \text{ `` } (r2s (rdom P))) = \text{relfdia } R P$
 ⟨proof⟩

lemma *wf-nabla-aux*: $(P \subseteq (\text{converse } R) \text{ `` } P \longrightarrow P = \{\}) \iff (s2r P \subseteq \text{relfdia } R (s2r P) \longrightarrow s2r P = \{\})$
 ⟨proof⟩

A relation is noetherian if its converse is wellfounded. Hence a relation is noetherian if and only if its divergence is empty. In the relational program semantics, noetherian programs terminate.

lemma *wf-nabla*: $\text{wf } (\text{converse } R) \iff \text{rel-nabla } R = \{\}$
 ⟨proof⟩

end

5.3.4 Verification Examples

```

theory VC-KAD-wf-Examples
  imports VC-KAD-wf
begin

```

The example should be taken with a grain of salt. More work is needed to make the while rule cooperate with simplification.

lemma *euclid*:

```

rel-nabla (
  [λs::nat store. 0 < s ''y'' ] ;
  (('z'' ::= (λs. s ''y'')) ;
  (''y'' ::= (λs. s ''x'' mod s ''y'')) ;
  (''x'' ::= (λs. s ''z'')))
= {}
⇒
PRE (λs::nat store. s ''x'' = x ∧ s ''y'' = y)
(WHILE (λs. s ''y'' ≠ 0) INV (λs. gcd (s ''x'') (s ''y'') = gcd x y)
DO
  ('z'' ::= (λs. s ''y''));
  (''y'' ::= (λs. s ''x'' mod s ''y''));
  (''x'' ::= (λs. s ''z''))
OD)
POST (λs. s ''x'' = gcd x y)
⟨proof⟩

```

The termination assumption is now explicit in the verification proof. Here it is left untouched. Means beyond these components are required for discharging it.

end

5.4 Two Extensions

5.4.1 KAD Component with Trace Semantics

```

theory Path-Model-Example
  imports VC-KAD HOL-Eisbach.Eisbach
begin

```

This component supports the verification of simple while programs in a partial correctness setting based on a program trace semantics.

Program traces are modelled as non-empty paths or state sequences. The non-empty path model of Kleene algebra is taken from the AFP entry for Kleene algebra. Here we show that sets of paths form antidomain Kleene Algebras.

definition *pp-a* :: 'a *ppath set* ⇒ 'a *ppath set* **where**
pp-a X = {(Node u) | u. ¬ (∃ v ∈ X. u = pp-first v)}

interpretation *ppath-aka*: antidomain-kleene-algebra *pp-a* (\sqcup) *pp-prod* *pp-one* $\{\}$
 (\subseteq) (\subset) *pp-star*
 \langle *proof* \rangle

A verification component can then be built with little effort, by and large reusing parts of the relational components that are generic with respect to the store.

definition *pp-gets* :: *string* \Rightarrow ('*a store* \Rightarrow '*a*) \Rightarrow '*a store ppath set* (- ::= - [70, 65] 61) **where**
 $v ::= e = \{Cons\ s\ (Node\ (s\ (v ::= e\ s)))\ |\ s.\ True\}$

definition *p2pp* :: '*a pred* \Rightarrow '*a ppath set* **where**
 $p2pp\ P = \{Node\ s\ |\ s.\ P\ s\}$

lemma *pp-a-neg* [*simp*]: *pp-a* (*p2pp* *Q*) = *p2pp* ($-Q$)
 \langle *proof* \rangle

lemma *ppath-assign* [*simp*]: *ppath-aka.fbox* ($v ::= e$) (*p2pp* *Q*) = *p2pp* ($\lambda s.\ Q\ (s(v ::= e\ s))$)
 \langle *proof* \rangle

no-notation *spec-sugar* (*PRE* - - *POST* - [64,64,64] 63)
and *relcomp* (**infixl** ; 70)
and *cond-sugar* (*IF* - *THEN* - *ELSE* - *FI* [64,64,64] 63)
and *whilei-sugar* (*WHILE* - *INV* - *DO* - *OD* [64,64,64] 63)
and *gets* (- ::= - [70, 65] 61)
and *rel-antidomain-kleene-algebra.fbox* (*wp*)
and *rel-antidomain-kleene-algebra.ads-d* (*rdom*)
and *p2r* (\lceil - \rceil)

notation *ppath-aka.fbox* (*wp*)
and *ppath-aka.ads-d* (*rdom*)
and *p2pp* (\lceil - \rceil)
and *pp-prod* (**infixl** ; 70)

abbreviation *spec-sugar* :: '*a pred* \Rightarrow '*a ppath set* \Rightarrow '*a pred* \Rightarrow *bool* (*PRE* - - *POST* - [64,64,64] 63) **where**
 $PRE\ P\ X\ POST\ Q \equiv rdom\ [P] \subseteq wp\ X\ [Q]$

abbreviation *cond-sugar* :: '*a pred* \Rightarrow '*a ppath set* \Rightarrow '*a ppath set* \Rightarrow '*a ppath set* (*IF* - *THEN* - *ELSE* - *FI* [64,64,64] 63) **where**
 $IF\ P\ THEN\ X\ ELSE\ Y\ FI \equiv ppath-aka.cond\ [P]\ X\ Y$

abbreviation *whilei-sugar* :: '*a pred* \Rightarrow '*a pred* \Rightarrow '*a ppath set* \Rightarrow '*a ppath set* (*WHILE* - *INV* - *DO* - *OD* [64,64,64] 63) **where**
 $WHILE\ P\ INV\ I\ DO\ X\ OD \equiv ppath-aka.whilei\ [P]\ [I]\ X$

lemma [*simp*]: *p2pp* *P* \cup *p2pp* *Q* = *p2pp* ($P \sqcup Q$)
 \langle *proof* \rangle

lemma [*simp*]: $p2pp\ P; p2pp\ Q = p2pp\ (P \sqcap Q)$
 ⟨*proof*⟩

lemma [*intro!*]: $P \leq Q \implies \lceil P \rceil \subseteq \lceil Q \rceil$
 ⟨*proof*⟩

lemma [*simp*]: $rdom\ \lceil P \rceil = \lceil P \rceil$
 ⟨*proof*⟩

lemma *euclid*:

PRE $(\lambda s::nat\ store.\ s\ \prime x'' = x \wedge s\ \prime y'' = y)$
(WHILE $(\lambda s.\ s\ \prime y'' \neq 0)$ *INV* $(\lambda s.\ gcd\ (s\ \prime x'')\ (s\ \prime y'') = gcd\ x\ y)$
DO
 $(\prime z'' ::= (\lambda s.\ s\ \prime y''));$
 $(\prime y'' ::= (\lambda s.\ s\ \prime x''\ mod\ s\ \prime y''));$
 $(\prime x'' ::= (\lambda s.\ s\ \prime z''))$
OD)
POST $(\lambda s.\ s\ \prime x'' = gcd\ x\ y)$
 ⟨*proof*⟩

lemma *euclid-diff*:

PRE $(\lambda s::nat\ store.\ s\ \prime x'' = x \wedge s\ \prime y'' = y \wedge x > 0 \wedge y > 0)$
(WHILE $(\lambda s.\ s\ \prime x'' \neq s\ \prime y'')$ *INV* $(\lambda s.\ gcd\ (s\ \prime x'')\ (s\ \prime y'') = gcd\ x\ y)$
DO
 $(IF\ (\lambda s.\ s\ \prime x'' > s\ \prime y'')$
 $\quad THEN\ (\prime x'' ::= (\lambda s.\ s\ \prime x'' - s\ \prime y''))$
 $\quad ELSE\ (\prime y'' ::= (\lambda s.\ s\ \prime y'' - s\ \prime x''))$
 $\quad FI)$
OD)
POST $(\lambda s.\ s\ \prime x'' = gcd\ x\ y)$
 ⟨*proof*⟩

lemma *variable-swap*:

PRE $(\lambda s.\ s\ \prime x'' = a \wedge s\ \prime y'' = b)$
 $(\prime z'' ::= (\lambda s.\ s\ \prime x''));$
 $(\prime x'' ::= (\lambda s.\ s\ \prime y''));$
 $(\prime y'' ::= (\lambda s.\ s\ \prime z''))$
POST $(\lambda s.\ s\ \prime x'' = b \wedge s\ \prime y'' = a)$
 ⟨*proof*⟩

lemma *maximum*:

PRE $(\lambda s::nat\ store.\ True)$
 $(IF\ (\lambda s.\ s\ \prime x'' \geq s\ \prime y'')$
 $\quad THEN\ (\prime z'' ::= (\lambda s.\ s\ \prime x''))$
 $\quad ELSE\ (\prime z'' ::= (\lambda s.\ s\ \prime y''))$
 $\quad FI)$
POST $(\lambda s.\ s\ \prime z'' = max\ (s\ \prime x'')\ (s\ \prime y''))$
 ⟨*proof*⟩

lemma *integer-division*:

```

PRE ( $\lambda s::\text{nat store. } x \geq 0$ )
  ("q'' ::= ( $\lambda s. 0$ ));
  ("r'' ::= ( $\lambda s. x$ ));
  (WHILE ( $\lambda s. y \leq s \text{ ''r''}$ ) INV ( $\lambda s. x = s \text{ ''q''} * y + s \text{ ''r''} \wedge s \text{ ''r''} \geq 0$ ))
  DO
    ("q'' ::= ( $\lambda s. s \text{ ''q''} + 1$ ));
    ("r'' ::= ( $\lambda s. s \text{ ''r''} - y$ ))
  OD
POST ( $\lambda s. x = s \text{ ''q''} * y + s \text{ ''r''} \wedge s \text{ ''r''} \geq 0 \wedge s \text{ ''r''} < y$ )
<proof>

```

We now reconsider these examples with an Eisbach tactic.

named-theorems *ht*

```

declare ppath-aka.fbox-whilei [ht]
  ppath-aka.fbox-seq-var [ht]
  subset-refl[ht]

```

method *hoare* = (*rule ht; hoare?*)

lemma *euclid2*:

```

PRE ( $\lambda s::\text{nat store. } s \text{ ''x''} = x \wedge s \text{ ''y''} = y$ )
  (WHILE ( $\lambda s. s \text{ ''y''} \neq 0$ ) INV ( $\lambda s. \text{gcd } (s \text{ ''x''}) (s \text{ ''y''}) = \text{gcd } x y$ ))
  DO
    ("z'' ::= ( $\lambda s. s \text{ ''y''}$ ));
    ("y'' ::= ( $\lambda s. s \text{ ''x''} \bmod s \text{ ''y''}$ ));
    ("x'' ::= ( $\lambda s. s \text{ ''z''}$ ))
  OD
POST ( $\lambda s. s \text{ ''x''} = \text{gcd } x y$ )
<proof>

```

lemma *euclid-diff2*:

```

PRE ( $\lambda s::\text{nat store. } s \text{ ''x''} = x \wedge s \text{ ''y''} = y \wedge x > 0 \wedge y > 0$ )
  (WHILE ( $\lambda s. s \text{ ''x''} \neq s \text{ ''y''}$ ) INV ( $\lambda s. \text{gcd } (s \text{ ''x''}) (s \text{ ''y''}) = \text{gcd } x y$ ))
  DO
    (IF ( $\lambda s. s \text{ ''x''} > s \text{ ''y''}$ )
      THEN ("x'' ::= ( $\lambda s. s \text{ ''x''} - s \text{ ''y''}$ ))
      ELSE ("y'' ::= ( $\lambda s. s \text{ ''y''} - s \text{ ''x''}$ ))
    FI)
  OD
POST ( $\lambda s. s \text{ ''x''} = \text{gcd } x y$ )
<proof>

```

lemma *variable-swap2*:

```

PRE ( $\lambda s. s \text{ ''x''} = a \wedge s \text{ ''y''} = b$ )
  ("z'' ::= ( $\lambda s. s \text{ ''x''}$ ));
  ("x'' ::= ( $\lambda s. s \text{ ''y''}$ ));

```


$(\text{"y''} ::= (\lambda s. s \text{"z''}))$
 $POST (\lambda s. s \text{"x''} = b \wedge s \text{"y''} = a)$
 $\langle proof \rangle$

lemma maximum2:

$PRE (\lambda s:: nat \text{ store. True})$
 $(IF (\lambda s. s \text{"x''} \geq s \text{"y''})$
 $THEN (\text{"z''} ::= (\lambda s. s \text{"x''}))$
 $ELSE (\text{"z''} ::= (\lambda s. s \text{"y''}))$
 $FI)$
 $POST (\lambda s. s \text{"z''} = \max (s \text{"x''}) (s \text{"y''}))$
 $\langle proof \rangle$

lemma integer-division2:

$PRE (\lambda s:: nat \text{ store. } x \geq 0)$
 $(\text{"q''} ::= (\lambda s. 0));$
 $(\text{"r''} ::= (\lambda s. x));$
 $(WHILE (\lambda s. y \leq s \text{"r''}) INV (\lambda s. x = s \text{"q''} * y + s \text{"r''} \wedge s \text{"r''} \geq 0)$
 DO
 $(\text{"q''} ::= (\lambda s. s \text{"q''} + 1));$
 $(\text{"r''} ::= (\lambda s. s \text{"r''} - y))$
 $OD)$
 $POST (\lambda s. x = s \text{"q''} * y + s \text{"r''} \wedge s \text{"r''} \geq 0 \wedge s \text{"r''} < y)$
 $\langle proof \rangle$

lemma my-power2:

$PRE (\lambda s:: nat \text{ store. True})$
 $(\text{"i''} ::= (\lambda s. 0));$
 $(\text{"y''} ::= (\lambda s. 1));$
 $(WHILE (\lambda s. s \text{"i''} < n) INV (\lambda s. s \text{"y''} = x \wedge (s \text{"i''}) \wedge s \text{"i''} \leq n)$
 DO
 $(\text{"y''} ::= (\lambda s. (s \text{"y''}) * x));$
 $(\text{"i''} ::= (\lambda s. s \text{"i''} + 1))$
 $OD)$
 $POST (\lambda s. s \text{"y''} = x \wedge n)$
 $\langle proof \rangle$

lemma imp-reverse2:

$PRE (\lambda s:: 'a \text{ list store. } s \text{"x''} = X)$
 $(\text{"y''} ::= (\lambda s. []));$
 $(WHILE (\lambda s. s \text{"x''} \neq []) INV (\lambda s. \text{rev} (s \text{"x''}) @ s \text{"y''} = \text{rev } X)$
 DO
 $(\text{"y''} ::= (\lambda s. \text{hd} (s \text{"x''}) \# s \text{"y''}));$
 $(\text{"x''} ::= (\lambda s. \text{tl} (s \text{"x''})))$
 $OD)$
 $POST (\lambda s. s \text{"y''} = \text{rev } X)$
 $\langle proof \rangle$

end

5.4.2 KAD Component for Pointer Programs

theory *Pointer-Examples*

imports *VC-KAD-Examples2 HOL-Hoare.Heap*

begin

This component supports the verification of simple while programs with pointers in a partial correctness setting.

All we do here is integrating Nipkow's implementation of pointers and heaps.

type-synonym *'a state = string* \Rightarrow (*'a ref + ('a \Rightarrow 'a ref)*)

lemma *list-reversal*:

PRE ($\lambda s :: 'a \text{ state. List (projr (s ''h'')) (projl (s ''p'')) Ps$

$\wedge \text{List (projr (s ''h'')) (projl (s ''q'')) Qs$

$\wedge \text{set Ps} \cap \text{set Qs} = \{\}$)

(*WHILE* ($\lambda s. \text{projl (s ''p'')} \neq \text{Null}$)

INV ($\lambda s. \exists ps \ qs. \text{List (projr (s ''h'')) (projl (s ''p'')) ps$

$\wedge \text{List (projr (s ''h'')) (projl (s ''q'')) qs$

$\wedge \text{set ps} \cap \text{set qs} = \{\} \wedge \text{rev ps} @ \text{qs} = \text{rev Ps} @ \text{Qs}$)

DO

'r'' ::= ($\lambda s. s ''p''$);

'p'' ::= ($\lambda s. \text{Inl (projr (s ''h'')) (addr (projl (s ''p'')))$);

'h'' ::= ($\lambda s. \text{Inr ((projr (s ''h''))(addr (projl (s ''r'')) := projl (s ''q'')))$);

'q'' ::= ($\lambda s. s ''r''$)

OD)

POST ($\lambda s. \text{List (projr (s ''h'')) (projl (s ''q'')) (rev Ps} @ \text{Qs)}$)

<proof>

end

6 Bringing KAT Components into Scope of KAD

theory *KAD-is-KAT*

imports *KAD.Antidomain-Semiring*

KAT-and-DRA.KAT

AVC-KAD/VC-KAD

AVC-KAT/VC-KAT

begin

context *antidomain-kleene-algebra*

begin

Every Kleene algebra with domain is a Kleene algebra with tests. This fact should eventually move into the AFP KAD entry.

sublocale *kat* (+) (\cdot) 1 0 (\leq) ($<$) *star antidomain-op*

<proof>

The next statement links the wp operator with the Hoare triple.

lemma *H-kat-to-kad*: $H\ p\ x\ q \longleftrightarrow d\ p \leq |x| (d\ q)$
 ⟨proof⟩

end

lemma *H-eq*: $P \subseteq Id \implies Q \subseteq Id \implies rel\text{-kat}.H\ P\ X\ Q = rel\text{-antidomain-kleene-algebra}.H\ P\ X\ Q$
 ⟨proof⟩

no-notation *VC-KAD.spec-sugar* (*PRE* - - *POST* - [64,64,64] 63)
and *VC-KAD.cond-sugar* (*IF* - *THEN* - *ELSE* - *FI* [64,64,64] 63)
and *VC-KAD.gets* (- ::= - [70, 65] 61)

Next we provide some syntactic sugar.

lemma *H-from-kat*: $PRE\ p\ x\ POST\ q = (\lceil p \rceil \leq (rel\text{-antidomain-kleene-algebra}.fbox\ x)\ \lceil q \rceil)$
 ⟨proof⟩

lemma *cond-iff*: $rel\text{-kat}.ifthenelse\ \lceil P \rceil\ X\ Y = rel\text{-antidomain-kleene-algebra}.cond\ \lceil P \rceil\ X\ Y$
 ⟨proof⟩

lemma *gets-iff*: $v ::= e = VC\text{-KAD}.gets\ v\ e$
 ⟨proof⟩

Finally we present two examples to test the integration.

lemma *maximum*:
 $PRE\ (\lambda s. nat\ store.\ True)$
 $(IF\ (\lambda s. s\ ''x'' \geq s\ ''y'')$
 $\quad THEN\ (''z'' ::= (\lambda s. s\ ''x''))$
 $\quad ELSE\ (''z'' ::= (\lambda s. s\ ''y''))$
 $\quad FI)$
 $POST\ (\lambda s. s\ ''z'' = max\ (s\ ''x'')\ (s\ ''y''))$
 ⟨proof⟩

lemma *maximum2*:
 $PRE\ (\lambda s. nat\ store.\ True)$
 $(IF\ (\lambda s. s\ ''x'' \geq s\ ''y'')$
 $\quad THEN\ (''z'' ::= (\lambda s. s\ ''x''))$
 $\quad ELSE\ (''z'' ::= (\lambda s. s\ ''y''))$
 $\quad FI)$
 $POST\ (\lambda s. s\ ''z'' = max\ (s\ ''x'')\ (s\ ''y''))$
 ⟨proof⟩

end

7 Component for Recursive Programs

```
theory Domain-Quantale
  imports KAD.Modal-Kleene-Algebra
```

```
begin
```

This component supports the verification and step-wise refinement of recursive programs in a partial correctness setting.

```
notation
```

```
  times (infixl · 70) and
  bot ( $\perp$ ) and
  top ( $\top$ ) and
  inf (infixl  $\sqcap$  65) and
  sup (infixl  $\sqcup$  65)
```

7.1 Lattice-Ordered Monoids with Domain

```
class bd-lattice-ordered-monoid = bounded-lattice + distrib-lattice + monoid-mult
+
  assumes left-distrib:  $x \cdot (y \sqcup z) = x \cdot y \sqcup x \cdot z$ 
  and right-distrib:  $(x \sqcup y) \cdot z = x \cdot z \sqcup y \cdot z$ 
  and bot-annil [simp]:  $\perp \cdot x = \perp$ 
  and bot-annir [simp]:  $x \cdot \perp = \perp$ 
```

```
begin
```

```
sublocale semiring-one-zero ( $\sqcup$ ) ( $\cdot$ ) 1 bot
  <proof>
```

```
sublocale dioid-one-zero ( $\sqcup$ ) ( $\cdot$ ) 1 bot ( $\leq$ ) ( $<$ )
  <proof>
```

```
end
```

```
no-notation ads-d ( $d$ )
  and ars-r ( $r$ )
  and antirange-op (ar - [999] 1000)
```

```
class domain-bdlo-monoid = bd-lattice-ordered-monoid +
  assumes rdv:  $(z \sqcap x \cdot top) \cdot y = z \cdot y \sqcap x \cdot top$ 
```

```
begin
```

```
definition d  $x = 1 \sqcap x \cdot \top$ 
```

```
sublocale ds: domain-semiring ( $\sqcup$ ) ( $\cdot$ ) 1  $\perp$  d ( $\leq$ ) ( $<$ )
  <proof>
```

end

7.2 Boolean Monoids with Domain

class *boolean-monoid* = *boolean-algebra* + *monoid-mult* +
 assumes *left-distrib'*: $x \cdot (y \sqcup z) = x \cdot y \sqcup x \cdot z$
 and *right-distrib'*: $(x \sqcup y) \cdot z = x \cdot z \sqcup y \cdot z$
 and *bot-annil'* [*simp*]: $\perp \cdot x = \perp$
 and *bot-annir'* [*simp*]: $x \cdot \perp = \perp$

begin

subclass *bd-lattice-ordered-monoid*
 ⟨*proof*⟩

lemma *inf-bot-iff-le*: $x \sqcap y = \perp \iff x \leq -y$
 ⟨*proof*⟩

end

class *domain-boolean-monoid* = *boolean-monoid* +
 assumes *rdv'*: $(z \sqcap x \cdot \top) \cdot y = z \cdot y \sqcap x \cdot \top$

begin

sublocale *dblo*: *domain-bdlo-monoid* 1 (\cdot) (\sqcap) (\leq) ($<$) (\sqcup) \perp \top
 ⟨*proof*⟩

definition *a* $x = 1 \sqcap -(dblo.d\ x)$

lemma *a-d-iff*: $a\ x = 1 \sqcap -(x \cdot \top)$
 ⟨*proof*⟩

lemma *topr*: $-(x \cdot \top) \cdot \top = -(x \cdot \top)$
 ⟨*proof*⟩

lemma *dd-a*: $dblo.d\ x = a\ (a\ x)$
 ⟨*proof*⟩

lemma *ad-a* [*simp*]: $a\ (dblo.d\ x) = a\ x$
 ⟨*proof*⟩

lemma *da-a* [*simp*]: $dblo.d\ (a\ x) = a\ x$
 ⟨*proof*⟩

lemma *a1* [*simp*]: $a\ x \cdot x = \perp$
 ⟨*proof*⟩

lemma *a2* [*simp*]: $a\ (x \cdot y) \sqcup a\ (x \cdot a\ (a\ y)) = a\ (x \cdot a\ (a\ y))$

<proof>

lemma *a3* [*simp*]: $a (a x) \sqcup a x = 1$
<proof>

subclass *domain-bdlo-monoid* *<proof>*

The next statement shows that every boolean monoid with domain is an antidomain semiring. In this setting the domain operation has been defined explicitly.

sublocale *ad*: *antidomain-semiring* a (\sqcup) (\cdot) 1 \perp (\leq) ($<$)
rewrites *ad-eq*: $ad.ads-d x = d x$
<proof>

end

7.3 Boolean Monoids with Range

class *range-boolean-monoid* = *boolean-monoid* +
assumes *ldv'*: $y \cdot (z \sqcap \top \cdot x) = y \cdot z \sqcap \top \cdot x$

begin

definition $r x = 1 \sqcap \top \cdot x$

definition $ar x = 1 \sqcap -(r x)$

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

lemma *topl*: $\top \cdot -(\top \cdot x) = -(\top \cdot x)$
<proof>

lemma *r-ar*: $r x = ar (ar x)$
<proof>

lemma *ar-ar* [*simp*]: $ar (r x) = ar x$
<proof>

lemma *r-ar-ar* [*simp*]: $r (ar x) = ar x$
<proof>

lemma *ar1* [*simp*]: $x \cdot ar x = \perp$
<proof>

lemma *ars*: $r (r x \cdot y) = r (x \cdot y)$
<proof>

lemma *ar2* [*simp*]: $ar (x \cdot y) \sqcup ar (ar (ar x) \cdot y) = ar (ar (ar x) \cdot y)$

<proof>

lemma *ar3* [*simp*]: $ar (ar x) \sqcup ar x = 1$
<proof>

sublocale *ar*: *antirange-semiring* (\sqcup) (\cdot) $1 \perp ar$ (\leq) ($<$)
rewrites *ar-eq*: $ar.ars-r x = r x$
<proof>

end

7.4 Quantales

This part will eventually move into an AFP quantale entry.

class *quantale* = *complete-lattice* + *monoid-mult* +
assumes *Sup-distr*: $Sup X \cdot y = Sup \{z. \exists x \in X. z = x \cdot y\}$
and *Sup-distl*: $x \cdot Sup Y = Sup \{z. \exists y \in Y. z = x \cdot y\}$

begin

lemma *bot-annil''* [*simp*]: $\perp \cdot x = \perp$
<proof>

lemma *bot-annirr''* [*simp*]: $x \cdot \perp = \perp$
<proof>

lemma *sup-distl*: $x \cdot (y \sqcup z) = x \cdot y \sqcup x \cdot z$
<proof>

lemma *sup-distr*: $(x \sqcup y) \cdot z = x \cdot z \sqcup y \cdot z$
<proof>

sublocale *semiring-one-zero* (\sqcup) (\cdot) $1 \perp$
<proof>

sublocale *dioid-one-zero* (\sqcup) (\cdot) $1 \perp$ (\leq) ($<$)
<proof>

lemma *Sup-sup-pred*: $x \sqcup Sup\{y. P y\} = Sup\{y. y = x \vee P y\}$
<proof>

definition *star* :: $'a \Rightarrow 'a$ **where**
 $star x = (SUP i. x \hat{=} i)$

lemma *star-def-var1*: $star x = Sup\{y. \exists i. y = x \hat{=} i\}$
<proof>

lemma *star-def-var2*: $star x = Sup\{x \hat{=} i \mid i. True\}$
<proof>

lemma *star-unfoldl'* [*simp*]: $1 \sqcup x \cdot (\text{star } x) = \text{star } x$
 ⟨*proof*⟩

lemma *star-unfoldr'* [*simp*]: $1 \sqcup (\text{star } x) \cdot x = \text{star } x$
 ⟨*proof*⟩

lemma (in *dioid-one-zero*) *power-inductl*: $z + x \cdot y \leq y \implies (x \hat{\ } n) \cdot z \leq y$
 ⟨*proof*⟩

lemma (in *dioid-one-zero*) *power-inductr*: $z + y \cdot x \leq y \implies z \cdot (x \hat{\ } n) \leq y$
 ⟨*proof*⟩

lemma *star-inductl'*: $z \sqcup x \cdot y \leq y \implies (\text{star } x) \cdot z \leq y$
 ⟨*proof*⟩

lemma *star-inductr'*: $z \sqcup y \cdot x \leq y \implies z \cdot (\text{star } x) \leq y$
 ⟨*proof*⟩

sublocale *ka*: *kleene-algebra* (\sqcup) (\cdot) $1 \perp (\leq)$ ($<$) *star*
 ⟨*proof*⟩

end

Distributive quantales are often assumed to satisfy infinite distributivity laws between joins and meets, but finite ones suffice for our purposes.

class *distributive-quantale* = *quantale* + *distrib-lattice*

begin

subclass *bd-lattice-ordered-monoid*
 ⟨*proof*⟩

lemma $(1 \sqcap x \cdot \top) \cdot x = x$

⟨*proof*⟩

end

7.5 Domain Quantales

class *domain-quantale* = *distributive-quantale* +
assumes *rdv''*: $(z \sqcap x \cdot \top) \cdot y = z \cdot y \sqcap x \cdot \top$

begin

subclass *domain-bdlo-monoid*
 ⟨*proof*⟩


```

end

class range-quantale = distributive-quantale +
  assumes ldv'':  $y \cdot (z \sqcap \top \cdot x) = y \cdot z \sqcap \top \cdot x$ 

class boolean-quantale = quantale + complete-boolean-algebra

begin

subclass boolean-monoid
   $\langle proof \rangle$ 

lemma  $(1 \sqcap x \cdot \top) \cdot x = x$ 

 $\langle proof \rangle$ 

lemma  $(1 \sqcap \neg(x \cdot \top)) \cdot x = \perp$ 

 $\langle proof \rangle$ 

end

```

7.6 Boolean Domain Quantaes

```

class domain-boolean-quantale = domain-quantale + boolean-quantale

begin

subclass domain-boolean-monoid
   $\langle proof \rangle$ 

lemma fbox-eq:  $ad.fbox\ x\ q = Sup\{d\ p \mid p. d\ p \cdot x \leq x \cdot d\ q\}$ 
   $\langle proof \rangle$ 

lemma fdia-eq:  $ad.fdia\ x\ p = Inf\{d\ q \mid q. x \cdot d\ p \leq d\ q \cdot x\}$ 
   $\langle proof \rangle$ 

The specification statement can be defined explicitly.

definition  $R :: 'a \Rightarrow 'a \Rightarrow 'a$  where
   $R\ p\ q \equiv Sup\{x. (d\ p) \cdot x \leq x \cdot d\ q\}$ 

lemma  $x \leq R\ p\ q \implies d\ p \leq ad.fbox\ x\ (d\ q)$ 
   $\langle proof \rangle$ 

lemma  $d\ p \leq ad.fbox\ x\ (d\ q) \implies x \leq R\ p\ q$ 
   $\langle proof \rangle$ 

end

```

7.7 Relational Model of Boolean Domain Quantales

interpretation *rel-dbq: domain-boolean-quantale*

$\langle (-) \rangle$ *uminus* $\langle (\cap) \rangle$ $\langle (\subseteq) \rangle$ $\langle (\subset) \rangle$ $\langle (\cup) \rangle$ $\langle \{ \} \rangle$ *UNIV* $\langle \cap \rangle$ $\langle \cup \rangle$ *Id* $\langle (O) \rangle$
 $\langle \text{proof} \rangle$

7.8 Modal Boolean Quantales

class *range-boolean-quantale* = *range-quantale* + *boolean-quantale*

begin

subclass *range-boolean-monoid*

$\langle \text{proof} \rangle$

lemma *fbox-eq*: $ar.bbox\ x\ (r\ q) = Sup\{r\ p\ |p.\ x \cdot r\ p \leq (r\ q) \cdot x\}$

$\langle \text{proof} \rangle$

lemma *fdia-eq*: $ar.bdia\ x\ (r\ p) = Inf\{r\ q\ |q.\ (r\ p) \cdot x \leq x \cdot r\ q\}$

$\langle \text{proof} \rangle$

end

class *modal-boolean-quantale* = *domain-boolean-quantale* + *range-boolean-quantale*

+

assumes *domrange'* [*simp*]: $d\ (r\ x) = r\ x$

and *rangedom'* [*simp*]: $r\ (d\ x) = d\ x$

begin

sublocale *mka: modal-kleene-algebra* (\sqcup) (\cdot) $1 \perp$ (\leq) ($<$) *star a ar*

$\langle \text{proof} \rangle$

end

no-notation *fbox* (($|$ - $|$ -) [*61,81*] *82*)

and *antidomain-semiringl-class.fbox* (($|$ - $|$ -) [*61,81*] *82*)

notation *ad.fbox* (($|$ - $|$ -) [*61,81*] *82*)

7.9 Recursion Rule

lemma *recursion: mono* ($f :: 'a \Rightarrow 'a :: \text{domain-boolean-quantale}$) \Longrightarrow

$(\bigwedge x.\ d\ p \leq |x]\ d\ q \Longrightarrow d\ p \leq |f\ x]\ d\ q) \Longrightarrow d\ p \leq |lfp\ f]\ d\ q$

$\langle \text{proof} \rangle$

We have already tested this rule in the context of test quantales [2], which is based on a formalisation of quantales that is currently not in the AFP. The two theories will be merged as soon as the quantale is available in the AFP.

end

References

- [1] A. Armstrong, V. B. F. Gomes, and G. Struth. Kleene algebra with tests and demonic refinement algebras. *Archive of Formal Proofs*, 2014.
- [2] A. Armstrong, V. B. F. Gomes, and G. Struth. Building program construction and verification tools from algebraic principles. *Formal Aspects of Computing*, 28(2):265–293, 2016.
- [3] A. Armstrong, G. Struth, and T. Weber. Kleene algebra. *Archive of Formal Proofs*, 2013.
- [4] J. Desharnais and G. Struth. Internal axioms for domain semirings. *Science of Computer Programming*, 76(3):181–203, 2011.
- [5] V. B. F. Gomes, W. Guttman, P. Höfner, G. Struth, and T. Weber. Kleene algebra with domain. *Archive of Formal Proofs*, 2016.