This is a repository copy of Kleene Algebra in Unifying Theories of Programming.

White Rose Research Online URL for this paper:
http://eprints.whiterose.ac.uk/129359/

Monograph:

Reuse
Unless indicated otherwise, fulltext items are protected by copyright with all rights reserved. The copyright exception in section 29 of the Copyright, Designs and Patents Act 1988 allows the making of a single copy solely for the purpose of non-commercial research or private study within the limits of fair dealing. The publisher or other rights-holder may allow further reproduction and re-use of this version - refer to the White Rose Research Online record for this item. Where records identify the publisher as the copyright holder, users can verify any specific terms of use on the publisher's website.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.
Kleene Algebra in Unifying Theories of Programming

Simon Foster

April 5, 2018

Abstract

This development links Isabelle/UTP to the mechanised Kleene Algebra (KA) hierarchy for Isabelle/HOL. We substantiate the required KA laws, and provides a large body of additional theorems for alphabetised relations which are provided by the KA library. Additionally, we show how such theorems can be lifted to a subclass of UTP theories, provided certain conditions hold.

Contents

1 Kleene Algebra and UTP ............................. 1
  1.1 Syntax setup ........................................... 1
  1.2 Kleene Algebra Instantiations ......................... 2
  1.3 Derived Laws ............................................ 3
  1.4 UTP Theories with Kleene Algebra ...................... 3

1 Kleene Algebra and UTP

theory utp-kleene
  imports
    KAT-and-DRA.KAT
    UTP.utp
begin

This theory instantiates the Kleene Algebra [6] (KA) hierarchy, mechanised in Isabelle/HOL by Armstrong, Gomes, Struth et al [1, 4, 2], for Isabelle/UTP alphabetised relations [3, 5]. Specifically, we substantiate the required dioid and KA laws in the type class hierarchy, which allows us to make use of all theorems proved in the former work. Moreover, we also prove an important result that a subclass of UTP theories, which we call “Kleene UTP theories”, always form Kleene algebras. The proof of the latter is obtained by lifting laws from the KA hierarchy.

1.1 Syntax setup

It is necessary to replace parts of the KA syntax to ensure compatibility with UTP. We therefore delete various bits of notation, and hide some constants.

purge-notation star (⋆ [101] 100)

recall-syntax

purge-notation n-op (n - [90] 91)
purge-notation ts-ord (infix ⊑ 50)
notation \( n \)-op \( (n[-]) \)
notation \( t \) \( (n^2[-]) \)
notation \( ts\)-ord \( (\text{infix} \subseteq, 50) \)

hide-const \( t \)

### 1.2 Kleene Algebra Instantiations

Next, import the laws of Kleene Algebra into the UTP relational calculus. We show that relations form a dioid and a Kleene algebra via two locales, the interpretation of which exports a large library of algebraic laws.

**interpretation** urel-dioid: dioid
  where plus = \( \text{op} \cap \) and times = \( \text{op} \);\( _h \) and less-eq = less-eq and less = less

**proof**
  fix \( P \ Q \ R :: 'a \ hrel \)
  show \( (P \cap Q) :: R = P :: R \cap Q :: R \)
    by (simp add: upred-semiring.distrib-right)
  show \( (Q \subseteq P) = (P \cap Q = Q) \)
    by (simp add: semilattice-sup-class.le-iff-sup)
  show \( (P < Q) = (Q \subseteq P \land \neg P = Q) \)
    by (simp add: less-le)
  show \( P \cap P = P \)
    by simp
  qed

**interpretation** urel-ka: kleene-algebra
  where plus = \( \text{op} \cap \) and times = \( \text{op} \);\( _h \) and one = skip-r and zero = false \( _h \) and less-eq = less-eq
  and less = less and star = ustar

**proof**
  fix \( P \ Q \ R :: 'a \ hrel \)
  show \( II :: P = P \) by simp
  show \( P :: II = P \) by simp
  show \( false \cap P = P \) by simp
  show \( false :: P = false \) by simp
  show \( P :: false = false \) by simp
  show \( P^* \subseteq II \cap P :: P^* \)
    using ustar-sub-unfold \( _l \) by blast
  show \( Q \subseteq R \cap P :: Q \Rightarrow Q \subseteq P^* :: R \)
    by (simp add: ustar-induct \( _l \))
  show \( Q \subseteq R \cap Q :: P \Rightarrow Q \subseteq R :: P^* \)
    by (simp add: ustar-induct \( _r \))
  qed

We also show that UTP relations form a Kleene Algebra with Tests \([7, 4]\) (KAT).

**interpretation** urel-kat: kat
  where plus = \( \text{op} \cap \) and times = \( \text{op} \);\( _h \) and one = skip-r and zero = false \( _h \) and less-eq = less-eq
  and less = less and star = ustar and \( n\)-op = \( \lambda x \cdot II \land (\neg x) \)

**proof**
  by (unfold-locales, rel-auto+)

We can now access the laws of KA and KAT for UTP relations as below.

**thm** urel-ka.star-inductr-var
**thm** urel-ka.star-trans
**thm** urel-ka.star-square
**thm** urel-ka.independence1
1.3 Derived Laws

We prove that UTP assumptions are tests.

**lemma test-rassume [simp]**: urel-kat.test $[b]^T$

  ```
  by (simp add: urel-kat.test-def, rel-auto)
  ```

The KAT laws can be used to prove results like the one below.

**lemma while-kat-form**: while $b$ do $P$ od = $([b]^T ;; P)^* ;; [\neg b]^T$ (is $?lhs = ?rhs$)

  ```
  proof -
  have 1:$(II::'a hrel) \sqcap (II::'a hrel) ;; [\neg b]^T = II$
    by (metis assume-true test-rassume urel-kat.test-absorb1)
  have $?lhs = ([b]^T ;; P \sqcap [\neg b]^T ;; II)^* ;; [\neg b]^T$
    by (simp add: while-star-form rcond-rassume-expand)
  also have ...
    by (metis urel-kat.star-denest-var-2)
  also have ...
    by (metis urel-kat.star-invol)
  finally show $?thesis$.
  qed
  ```

**lemma uplus-invol [simp]**: $(P^+)^+ = P^+$

  ```
  by (metis RA1 uplus-def urel-ka.dagger-trans-eq urel-ka.star-denest-var-2 urel-ka.star-invol)
  ```

**lemma uplus-alt-def**: $P^+ = P^* ;; P$

  ```
  by (simp add: uplus-def urel-ka.star-slide-var)
  ```

1.4 UTP Theories with Kleene Algebra

A Kleene UTP theory is continuous UTP theory with left and right units, and the top element as a left zero. The star in such a context has already been defined by lifting the relational Kleene star. Here, we use the KA theorems obtained above to provide corresponding theorems for a Kleene UTP theory.

**locale utp-theory-kleene**

```
begin

**lemma Star-def**: $P^* = P^* ;; \mathcal{I}$

  ```
  by (simp add: utp-star-def)
  ```

**lemma Star-alt-def**:

  ```
  assumes $P$ is $\mathcal{H}$
  shows $P^* = \mathcal{I} \sqcap P^+$
  proof -
  from assms have $P^+ = P^* ;; P ;; \mathcal{I}$
    by (simp add: Unit-Right uplus-alt-def)
  then show $?thesis$
    by (simp add: RA1 utp-star-def)
  qed
  ```

```
lemma Star-Healthy [closure]:
  assumes $P$ is $\mathcal{H}$
  shows $P^*$ is $\mathcal{H}$
  by (simp add: assms closure Star-alt-def)

lemma Star-unfoldl:
  $P^* \subseteq \mathcal{I} \cap P ;; P^*$
  by (simp add: RA1 utp-star-def)

lemma Star-inductl:
  assumes $R$ is $\mathcal{H}$ $Q \subseteq P ;; Q \cap R$
  shows $Q \subseteq P^* ;; R$
  proof –
  from assms(2) have $Q \subseteq R Q \subseteq P ;; Q$
  by auto
  thus $?thesis$
  by (simp add: Unit-Left assms(1) upred-semiring.mult-assoc urel-ka.star-inductl utp-star-def)
  qed

lemma Star-invol:
  assumes $P$ is $\mathcal{H}$
  shows $P^{**} = P^*$
  by (metis (no-types) RA1 Unit-Left Unit-self assms urel-ka.star-invol urel-ka.star-sim3 utp-star-def)

lemma Star-test:
  assumes $P$ is $\mathcal{H}$ utest $T$
  shows $P^* = \mathcal{I}$
  by (metis utp-star-def Star-alt-def Unit-Right Unit-self assms semilattice-sup-class.sup.absorb1 semilattice-sup-class.sup.urel-ka.star-inductr-var-eq2 urel-ka.star-sim1 utest-def)

lemma Star-lemma-1:
  $P$ is $\mathcal{H} \Rightarrow \mathcal{I} ;; P^* ;; \mathcal{I} = P^* ;; \mathcal{I}$
  by (metis utp-star-def Star-Healthy Unit-Left)

lemma Star-lemma-2:
  assumes $P$ is $\mathcal{H}$ $Q$ is $\mathcal{H}$
  shows $(P^* ;; Q^* ;; \mathcal{I})^* ;; \mathcal{I} = (P^* ;; Q^*)^* ;; \mathcal{I}$
  by (metis (no-types) assms RA1 Star-lemma-1 Unit-self urel-ka.star-sim3)

lemma Star-denest:
  assumes $P$ is $\mathcal{H}$ $Q$ is $\mathcal{H}$
  shows $(P \cap Q)^* = (P^* ;; Q^*)^*$
  by (metis (no-types, lifting) RA1 utp-star-def Star-lemma-1 Star-lemma-2 assms urel-ka.star-denest)

lemma Star-denest-disj:
  assumes $P$ is $\mathcal{H}$ $Q$ is $\mathcal{H}$
  shows $(P \lor Q)^* = (P^* ;; Q^*)^*$
  by (simp add: disj-upred-def Star-denest assms)

lemma Star-unfoldl-eq:
  assumes $P$ is $\mathcal{H}$
  shows $\mathcal{I} \cap P ;; P^* = P^*$
  by (simp add: RA1 utp-star-def)
lemma uplus-Star-def:
assumes P is H
shows P* = (P ;; P*)
by (metis (full-types) RA1 utp-star-def Unit-Left Unit-Right assms uplus-def urel-ka.conway.dagger-slide)

lemma Star-trade-skip:
P is H \implies II ;; P* = P* ;; II
by (simp add: Unit-Left Unit-Right urel-ka.star-sim3)

lemma Star-slide:
assumes P is H
shows (P ;; P*) = (P* ;; P)
proof -
  have \?lhs = P ;; P* ;; II
    by (simp add: utp-star-def)
  also have ... = P ;; II ;; P*
    by (simp add: Star-trade-skip assms)
  also have ... = P* ;; P
    by (simp add: RA1 Unit-Right assms)
  also have ... = \?rhs
    by (metis RA1 utp-star-def Unit-Left assms)
  finally show \?thesis.
qed

lemma Star-unfoldr-eq:
assumes P is H
shows II \sqcap P* ;; P = P*
using Star-slide Star-unfoldl-eq assms by auto

lemma Star-inductr:
assumes P is H R is H Q \sqsubseteq P \sqcap Q ;; R
shows Q \sqsubseteq P ;; R*
by (metis (full-types) RA1 Star-def Star-trade-skip Unit-Right assms urel-ka.star-inductr)

lemma Star-Top: \top* = II
  by (simp add: Star-test top-healthy utest-Top)

end

end

References


