Ribbon Proofs for Separation Logic (Isabelle Formalisation)

John Wickerson

May 26, 2024

Abstract

This document concerns the theory of *ribbon proofs*: a diagrammatic proof system, based on separation logic, for verifying program correctness. We include the syntax, proof rules, and soundness results for two alternative formalisations of ribbon proofs.

Compared to traditional 'proof outlines', ribbon proofs emphasise the structure of a proof, so are intelligible and pedagogical. Because they contain less redundancy than proof outlines, and allow each proof step to be checked locally, they may be more scalable. Where proof outlines are cumbersome to modify, ribbon proofs can be visually manoeuvred to yield proofs of variant programs.

Contents

1 Introduction

Ribbon proofs are a diagrammatic approach for proving program correctness, based on separation logic. They are due to Wickerson, Dodds and Parkinson [4], and are also described in Wickerson's PhD dissertation [3]. An early version of the proof system, for proving entailments between quantifier-free separation logic assertions, was introduced by Bean [1].

Compared to traditional 'proof outlines', ribbon proofs emphasise the structure of a proof, so are intelligible and pedagogical. Because they contain less redundancy than proof outlines, and allow each proof step to be checked locally, they may be more scalable. Where proof outlines are cumbersome to modify, ribbon proofs can be visually manoeuvred to yield proofs of variant programs.

In this document, we formalise a two-dimensional graphical syntax for ribbon proofs, provide proof rules, and show that any provable ribbon proof can be recreated using the ordinary rules of separation logic.

In fact, we provide two different formalisations. Our "stratified" formalisation sees a ribbon proof as a sequence of rows, with each row containing one step of the proof. This formalisation is very simple, but it does not reflect the visual intuition of ribbon proofs, which suggests that some proof steps can be slid up or down without affecting the validity of the overall proof. Our "graphical" formalisation sees a ribbon proof as a graph; specifically, as a directed acyclic nested graph. Ribbon proofs formalised in this way are more manoeuvrable, but proving soundness is trickier, and requires the assumption that separation logic's Frame rule has no side-condition (an assumption that can be validated by using, for instance, variables-as-resource [2]).

2 Finite partial functions

theory *More-Finite-Map* **imports**
  HOL−Library.Finite-Map
begin

lemma *fdisjoint-iff*: $A\ |\cap|\ B = \{||\} \longleftrightarrow (\forall x.\ x\ |\in|\ A \longrightarrow x\ |\notin|\ B)$
  ⟨*proof*⟩

unbundle *lifting-syntax*
unbundle *fmap.lifting*

type-notation *fmap* (**infix** $\rightharpoonup_f$ *9*)

2.1 Difference

definition
  $map\text{-}diff :: ('k \rightharpoonup 'v) \Rightarrow 'k\ fset \Rightarrow ('k \rightharpoonup 'v)$
where
  $map\text{-}diff\ f\ ks = restrict\text{-}map\ f\ (-\ fset\ ks)$

lift-definition
  $fmap\text{-}diff :: ('k \rightharpoonup_f 'v) \Rightarrow 'k\ fset \Rightarrow ('k \rightharpoonup_f 'v)$ (**infix** $\ominus$ *110*)
is *map-diff*
⟨*proof*⟩

2.2 Comprehension

definition
  $make\text{-}map :: 'k\ fset \Rightarrow 'v \Rightarrow ('k \rightharpoonup 'v)$
where
  $make\text{-}map\ ks\ v \equiv \lambda k.\ if\ k \in fset\ ks\ then\ Some\ v\ else\ None$

lemma *make-map-transfer*[*transfer-rule*]: (*rel-fset* (=) ===> A ===> *rel-map* A) *make-map make-map*
⟨*proof*⟩

lemma *dom-make-map*:
dom (*make-map ks v*) = *fset ks*
⟨*proof*⟩

lift-definition
make-fmap :: $'k$ *fset* ⇒ $'v$ ⇒ ($'k \rightharpoonup_f$ $'v$) ([- |=> -])
is *make-map* **parametric** *make-map-transfer*
⟨*proof*⟩

lemma *make-fmap-empty*[*simp*]: [{||} |=> *f*] = *fmempty*
⟨*proof*⟩

2.3 Domain

lemma *fmap-add-commute*:
assumes *fmdom A* |∩| *fmdom B* = {||}
shows A $++_f$ B = B $++_f$ A
⟨*proof*⟩ **including** *fset.lifting*
⟨*proof*⟩

lemma *make-fmap-union*:
[*xs* |=> *v*] $++_f$ [*ys* |=> *v*] = [*xs* |∪| *ys* |=> *v*]
⟨*proof*⟩

lemma *fdom-make-fmap*: *fmdom* [*ks* |=> *v*] = *ks*

⟨*proof*⟩

2.4 Lookup

lift-definition
lookup :: ($'k \rightharpoonup_f$ $'v$) ⇒ $'k$ ⇒ $'v$
is (∘) *the* ⟨*proof*⟩

lemma *lookup-make-fmap*:
assumes *k* ∈ *fset ks*
shows *lookup* [*ks* |=> *v*] *k* = *v*
⟨*proof*⟩

lemma *lookup-make-fmap1*:
lookup [{|*k*|} |=> *v*] *k* = *v*
⟨*proof*⟩

lemma *lookup-union1*:
assumes *k* |∈| *fmdom ys*
shows *lookup* (*xs* $++_f$ *ys*) *k* = *lookup ys k*

$\langle proof \rangle$ **including** *fset.lifting*
$\langle proof \rangle$

lemma *lookup-union2*:
  assumes $k \; |\notin| \; fmdom \; ys$
  shows $lookup \; (xs \; {+}{+}_f \; ys) \; k = lookup \; xs \; k$
$\langle proof \rangle$ **including** *fset.lifting*
$\langle proof \rangle$

lemma *lookup-union3*:
  assumes $k \; |\notin| \; fmdom \; xs$
  shows $lookup \; (xs \; {+}{+}_f \; ys) \; k = lookup \; ys \; k$
$\langle proof \rangle$ **including** *fset.lifting*
$\langle proof \rangle$

end

3 General purpose definitions and lemmas

theory *JHelper* **imports**
  Main
begin

lemma *Collect-iff*:
  $a \in \{x \; . \; P \; x\} \equiv P \; a$
$\langle proof \rangle$

lemma *diff-diff-eq*:
  assumes $C \subseteq B$
  shows $(A - C) - (B - C) = A - B$
$\langle proof \rangle$

lemma *nth-in-set*:
  $[\![\; i < length \; xs \; ; \; xs \; ! \; i = x \;]\!] \Longrightarrow x \in set \; xs$ $\langle proof \rangle$

lemma *disjI* [*intro*]:
  assumes $\neg \; P \Longrightarrow Q$
  shows $P \vee Q$
$\langle proof \rangle$

lemma *empty-eq-Plus-conv*:
  $(\{\} = A <\!+\!> B) = (A = \{\} \wedge B = \{\})$
$\langle proof \rangle$

3.1 Projection functions on triples

definition $fst3 :: {'a} \times {'b} \times {'c} \Rightarrow {'a}$
where $fst3 \equiv fst$

definition *snd3* :: $'a \times 'b \times 'c \Rightarrow 'b$
where *snd3* $\equiv$ *fst* $\circ$ *snd*

definition *thd3* :: $'a \times 'b \times 'c \Rightarrow 'c$
where *thd3* $\equiv$ *snd* $\circ$ *snd*

lemma *fst3-simp*:
$\bigwedge a\ b\ c.\ fst3\ (a,b,c) = a$
⟨*proof*⟩

lemma *snd3-simp*:
$\bigwedge a\ b\ c.\ snd3\ (a,b,c) = b$
⟨*proof*⟩

lemma *thd3-simp*:
$\bigwedge a\ b\ c.\ thd3\ (a,b,c) = c$
⟨*proof*⟩

lemma *tripleI*:
fixes *T U*
assumes $fst3\ T = fst3\ U$
and $snd3\ T = snd3\ U$
and $thd3\ T = thd3\ U$
shows $T = U$
⟨*proof*⟩

end

4 Proof chains

theory *Proofchain* **imports**
JHelper
begin

An $('a,\ 'c)$ chain is a sequence of alternating $'a$'s and $'c$'s, beginning and ending with an $'a$. Usually $'a$ represents some sort of assertion, and $'c$ represents some sort of command. Proof chains are useful for stating the SMain proof rule, and for conducting the proof of soundness.

datatype $('a,'c)$ *chain* =
cNil $'a$ $(\{\!|\ \text{-}\ |\!\})$
| *cCons* $'a\ 'c\ ('a,'c)$ *chain* $(\{\!|\ \text{-}\ |\!\} \cdot \text{-} \cdot \text{-}\ [0,0,0]\ 60)$

For example, $\{\!|\ a\ |\!\} \cdot proof \cdot \{\!|\ chain\ |\!\} \cdot might \cdot \{\!|\ look\ |\!\} \cdot like \cdot \{\!|\ this\ |\!\}$.

4.1 Projections

Project first assertion.

fun
  pre :: $('a,'c)$ $chain \Rightarrow 'a$
where
  pre $\{\!|$ P $|\!\}$ $= P$
| pre $(\{\!|$ P $|\!\}$ $\cdot$ - $\cdot$ -$)$ $= P$

Project final assertion.

fun
  $post$ :: $('a,'c)$ $chain \Rightarrow 'a$
where
  $post$ $\{\!|$ P $|\!\}$ $= P$
| $post$ $(\{\!|$ - $|\!\}$ $\cdot$ - $\cdot$ $\Pi)$ $= post$ Π

Project list of commands.

fun
  $comlist$ :: $('a,'c)$ $chain \Rightarrow 'c$ $list$
where
  $comlist$ $\{\!|$ - $|\!\}$ $= []$
| $comlist$ $(\{\!|$ - $|\!\}$ $\cdot$ x $\cdot$ $\Pi)$ $= x$ # $(comlist$ $\Pi)$

4.2 Chain length

fun
  $chainlen$ :: $('a,'c)$ $chain \Rightarrow nat$
where
  $chainlen$ $\{\!|$ - $|\!\}$ $= 0$
| $chainlen$ $(\{\!|$ - $|\!\}$ $\cdot$ - $\cdot$ $\Pi)$ $= 1 + (chainlen$ $\Pi)$

lemma *len-comlist-chainlen*:
  $length$ $(comlist$ $\Pi) = chainlen$ Π
$\langle proof \rangle$

4.3 Extracting triples from chains

nthtriple Π n extracts the nth triple of Π, counting from 0. The function is well-defined when $n < chainlen$ Π.

fun
  $nthtriple$ :: $('a,'c)$ $chain \Rightarrow nat \Rightarrow ('a * 'c * 'a)$
where
  $nthtriple$ $(\{\!|$ P $|\!\}$ $\cdot$ x $\cdot$ $\Pi)$ 0 $= (P, x, pre$ $\Pi)$
| $nthtriple$ $(\{\!|$ P $|\!\}$ $\cdot$ x $\cdot$ $\Pi)$ $(Suc$ $n)$ $= nthtriple$ Π n

The list of middle components of Π's triples is the list of Π's commands.

lemma *snds-of-triples-form-comlist*:
  fixes Π i
  shows $i < chainlen$ $\Pi \Longrightarrow snd3$ $(nthtriple$ Π $i) = (comlist$ $\Pi)!i$
$\langle proof \rangle$

4.4 Evaluating a predicate on each triple of a chain

chain-all φ holds of Π iff φ holds for each of Π's individual triples.

fun
  $\textit{chain-all} :: (('a \times 'c \times 'a) \Rightarrow \textit{bool}) \Rightarrow ('a,'c)\ \textit{chain} \Rightarrow \textit{bool}$
where
  $\textit{chain-all}\ \varphi\ \{\!|\ \sigma\ |\!\} = \textit{True}$
$|\ \textit{chain-all}\ \varphi\ (\{\!|\ \sigma\ |\!\} \cdot x \cdot \Pi) = (\varphi\ (\sigma,x,\textit{pre}\ \Pi) \wedge \textit{chain-all}\ \varphi\ \Pi)$

lemma *chain-all-mono* [*mono*]:
  $x \leq y \Longrightarrow \textit{chain-all}\ x \leq \textit{chain-all}\ y$
$\langle \textit{proof} \rangle$

lemma *chain-all-nthtriple*:
  $(\textit{chain-all}\ \varphi\ \Pi) = (\forall\, i < \textit{chainlen}\ \Pi.\ \varphi\ (\textit{nthtriple}\ \Pi\ i))$
$\langle \textit{proof} \rangle$

4.5 A map function for proof chains

chainmap $f\ g\ \Pi$ maps f over each of Π's assertions, and g over each of Π's commands.

fun
  $\textit{chainmap} :: ('a \Rightarrow 'b) \Rightarrow ('c \Rightarrow 'd) \Rightarrow ('a,'c)\ \textit{chain} \Rightarrow ('b,'d)\ \textit{chain}$
where
  $\textit{chainmap}\ f\ g\ \{\!|\ P\ |\!\} = \{\!|\ f\ P\ |\!\}$
$|\ \textit{chainmap}\ f\ g\ (\{\!|\ P\ |\!\} \cdot x \cdot \Pi) = \{\!|\ f\ P\ |\!\} \cdot g\ x \cdot \textit{chainmap}\ f\ g\ \Pi$

Mapping over a chain preserves its length.

lemma *chainmap-preserves-length*:
  $\textit{chainlen}\ (\textit{chainmap}\ f\ g\ \Pi) = \textit{chainlen}\ \Pi$
$\langle \textit{proof} \rangle$

lemma *pre-chainmap*:
  $\textit{pre}\ (\textit{chainmap}\ f\ g\ \Pi) = f\ (\textit{pre}\ \Pi)$
$\langle \textit{proof} \rangle$

lemma *post-chainmap*:
  $\textit{post}\ (\textit{chainmap}\ f\ g\ \Pi) = f\ (\textit{post}\ \Pi)$
$\langle \textit{proof} \rangle$

lemma *nthtriple-chainmap*:
  assumes $i < \textit{chainlen}\ \Pi$
  shows $\textit{nthtriple}\ (\textit{chainmap}\ f\ g\ \Pi)\ i$
    $= (\lambda t.\ (f\ (\textit{fst3}\ t),\ g\ (\textit{snd3}\ t),\ f\ (\textit{thd3}\ t)))\ (\textit{nthtriple}\ \Pi\ i)$
$\langle \textit{proof} \rangle$

4.6 Extending a chain on its right-hand side

fun

$cSnoc$ :: $('a,'c)$ $chain \Rightarrow 'c \Rightarrow 'a \Rightarrow ('a,'c)$ $chain$
where
$cSnoc$ $\{\!\!\{ \sigma \}\!\!\}$ y $\tau = \{\!\!\{ \sigma \}\!\!\} \cdot y \cdot \{\!\!\{ \tau \}\!\!\}$
| $cSnoc$ $(\{\!\!\{ \sigma \}\!\!\} \cdot x \cdot \Pi)$ y $\tau = \{\!\!\{ \sigma \}\!\!\} \cdot x \cdot (cSnoc\ \Pi\ y\ \tau)$

lemma *len-snoc*:
fixes Π x P
shows $chainlen\ (cSnoc\ \Pi\ x\ P) = 1 + (chainlen\ \Pi)$
⟨*proof*⟩

lemma *pre-snoc*:
$pre\ (cSnoc\ \Pi\ x\ P) = pre\ \Pi$
⟨*proof*⟩

lemma *post-snoc*:
$post\ (cSnoc\ \Pi\ x\ P) = P$
⟨*proof*⟩

lemma *comlist-snoc*:
$comlist\ (cSnoc\ \Pi\ x\ p) = comlist\ \Pi\ @\ [x]$
⟨*proof*⟩

end

5 Assertions, commands, and separation logic proof rules

theory *Ribbons-Basic* **imports**
Main
begin

We define a command language, assertions, and the rules of separation logic, plus some derived rules that are used by our tool. This is the only theory file that is loaded by the tool. We keep it as small as possible.

5.1 Assertions

The language of assertions includes (at least) an emp constant, a star-operator, and existentially-quantified logical variables.

typedecl *assertion*

axiomatization
Emp :: *assertion*

axiomatization

Star :: *assertion* ⇒ *assertion* ⇒ *assertion* (**infixr** $\star$ *55*)
where
star-comm: $p \star q = q \star p$ **and**
star-assoc: $(p \star q) \star r = p \star (q \star r)$ **and**
star-emp: $p \star Emp = p$ **and**
emp-star: $Emp \star p = p$

lemma *star-rot*:
$q \star p \star r = p \star q \star r$
⟨*proof*⟩

axiomatization
Exists :: *string* ⇒ *assertion* ⇒ *assertion*

Extracting the set of program variables mentioned in an assertion.

axiomatization
rd-ass :: *assertion* ⇒ *string set*
where *rd-emp*: *rd-ass Emp* = {}
and *rd-star*: *rd-ass* $(p \star q)$ = *rd-ass p* ∪ *rd-ass q*
and *rd-exists*: *rd-ass* (*Exists x p*) = *rd-ass p*

5.2 Commands

The language of commands comprises (at least) non-deterministic choice, non-deterministic looping, skip and sequencing.

typedecl *command*

axiomatization
Choose :: *command* ⇒ *command* ⇒ *command*

axiomatization
Loop :: *command* ⇒ *command*

axiomatization
Skip :: *command*

axiomatization
Seq :: *command* ⇒ *command* ⇒ *command* (**infixr** ;; *55*)
where *seq-assoc*: *c1* ;; (*c2* ;; *c3*) = (*c1* ;; *c2*) ;; *c3*
and *seq-skip*: *c* ;; *Skip* = *c*
and *skip-seq*: *Skip* ;; *c* = *c*

Extracting the set of program variables read by a command.

axiomatization
rd-com :: *command* ⇒ *string set*
where *rd-com-choose*: *rd-com* (*Choose c1 c2*) = *rd-com c1* ∪ *rd-com c2*
and *rd-com-loop*: *rd-com* (*Loop c*) = *rd-com c*
and *rd-com-skip*: *rd-com* (*Skip*) = {}

and *rd-com-seq*: $rd\text{-}com\ (c1\ ;;\ c2) = rd\text{-}com\ c1 \cup rd\text{-}com\ c2$

Extracting the set of program variables written by a command.

axiomatization
  $wr\text{-}com :: command \Rightarrow string\ set$
where *wr-com-choose*: $wr\text{-}com\ (Choose\ c1\ c2) = wr\text{-}com\ c1 \cup wr\text{-}com\ c2$
  and *wr-com-loop*: $wr\text{-}com\ (Loop\ c) = wr\text{-}com\ c$
  and *wr-com-skip*: $wr\text{-}com\ (Skip) = \{\}$
  and *wr-com-seq*: $wr\text{-}com\ (c1\ ;;\ c2) = wr\text{-}com\ c1 \cup wr\text{-}com\ c2$

5.3 Separation logic proof rules

Note that the frame rule has a side-condition concerning program variables. When proving the soundness of our graphical formalisation of ribbon proofs, we shall omit this side-condition.

inductive
  $prov\text{-}triple :: assertion \times command \times assertion \Rightarrow bool$
where
  exists: $prov\text{-}triple\ (p,\ c,\ q) \Longrightarrow prov\text{-}triple\ (Exists\ x\ p,\ c,\ Exists\ x\ q)$
| *choose*: $[\![\ prov\text{-}triple\ (p,\ c1,\ q);\ prov\text{-}triple\ (p,\ c2,\ q)\ ]\!]$
  $\Longrightarrow prov\text{-}triple\ (p,\ Choose\ c1\ c2,\ q)$
| *loop*: $prov\text{-}triple\ (p,\ c,\ p) \Longrightarrow prov\text{-}triple\ (p,\ Loop\ c,\ p)$
| *frame*: $[\![\ prov\text{-}triple\ (p,\ c,\ q);\ wr\text{-}com(c) \cap rd\text{-}ass(r) = \{\}\ ]\!]$
  $\Longrightarrow prov\text{-}triple\ (p \star r,\ c,\ q \star r)$
| *skip*: $prov\text{-}triple\ (p,\ Skip,\ p)$
| *seq*: $[\![\ prov\text{-}triple\ (p,\ c1,\ q);\ prov\text{-}triple\ (q,\ c2,\ r)\ ]\!]$
  $\Longrightarrow prov\text{-}triple\ (p,\ c1\ ;;\ c2,\ r)$

Here are some derived proof rules, which are used in our ribbon-checking tool.

lemma *choice-lemma*:
  assumes $prov\text{-}triple\ (p1,\ c1,\ q1)$ **and** $prov\text{-}triple\ (p2,\ c2,\ q2)$
    and $p = p1$ **and** $p1 = p2$ **and** $q = q1$ **and** $q1 = q2$
  shows $prov\text{-}triple\ (p,\ Choose\ c1\ c2,\ q)$
$\langle proof \rangle$

lemma *loop-lemma*:
  assumes $prov\text{-}triple\ (p1,\ c,\ q1)$ **and** $p = p1$ **and** $p1 = q1$ **and** $q1 = q$
  shows $prov\text{-}triple\ (p,\ Loop\ c,\ q)$
$\langle proof \rangle$

lemma *seq-lemma*:
  assumes $prov\text{-}triple\ (p1,\ c1,\ q1)$ **and** $prov\text{-}triple\ (p2,\ c2,\ q2)$
    and $q1 = p2$
  shows $prov\text{-}triple\ (p1,\ c1\ ;;\ c2,\ q2)$
$\langle proof \rangle$

end

6 Ribbon proof interfaces

theory *Ribbons-Interfaces* **imports**
Ribbons-Basic
Proofchain
HOL−Library.FSet
begin

Interfaces are the top and bottom boundaries through which diagrams can be connected into a surrounding context. For instance, when composing two diagrams vertically, the bottom interface of the upper diagram must match the top interface of the lower diagram.

We define a datatype of concrete interfaces. We then quotient by the associativity, commutativity and unity properties of our horizontal-composition operator.

6.1 Syntax of interfaces

datatype *conc-interface* =
Ribbon-conc assertion
| *HComp-int-conc conc-interface conc-interface* (**infix** $\otimes_c$ *50*)
| *Emp-int-conc* (ε_c)
| *Exists-int-conc string conc-interface*

We define an equivalence on interfaces. The first three rules make this an equivalence relation. The next three make it a congruence. The next two identify interfaces up to associativity and commutativity of ($\otimes_c$) The final two make ε_c the left and right unit of ($\otimes_c$).

inductive
equiv-int :: *conc-interface* ⇒ *conc-interface* ⇒ *bool* (**infix** $\simeq$ *45*)
where
refl: $P \simeq P$
| *sym*: $P \simeq Q \Longrightarrow Q \simeq P$
| *trans*: $[\![P \simeq Q;\ Q \simeq R]\!] \Longrightarrow P \simeq R$
| *cong-hcomp1*: $P \simeq Q \Longrightarrow P' \otimes_c P \simeq P' \otimes_c Q$
| *cong-hcomp2*: $P \simeq Q \Longrightarrow P \otimes_c P' \simeq Q \otimes_c P'$
| *cong-exists*: $P \simeq Q \Longrightarrow$ *Exists-int-conc* $x\ P \simeq$ *Exists-int-conc* $x\ Q$
| *hcomp-conc-assoc*: $P \otimes_c (Q \otimes_c R) \simeq (P \otimes_c Q) \otimes_c R$
| *hcomp-conc-comm*: $P \otimes_c Q \simeq Q \otimes_c P$
| *hcomp-conc-unit1*: $\varepsilon_c \otimes_c P \simeq P$
| *hcomp-conc-unit2*: $P \otimes_c \varepsilon_c \simeq P$

lemma *equiv-int-cong-hcomp*:
$[\![\ P \simeq Q\ ;\ P' \simeq Q'\ ]\!] \Longrightarrow P \otimes_c P' \simeq Q \otimes_c Q'$
⟨*proof*⟩

quotient-type *interface* = *conc-interface* / *equiv-int*
⟨*proof*⟩

lift-definition
  Ribbon :: *assertion* ⇒ *interface*
is *Ribbon-conc* ⟨*proof*⟩

lift-definition
  Emp-int :: *interface* (ε)
is ε_c ⟨*proof*⟩

lift-definition
  Exists-int :: *string* ⇒ *interface* ⇒ *interface*
is *Exists-int-conc*
⟨*proof*⟩

lift-definition
  HComp-int :: *interface* ⇒ *interface* ⇒ *interface* (**infix** ⊗ *50*)
is *HComp-int-conc* ⟨*proof*⟩

lemma *hcomp-comm*:
  $(P \otimes Q) = (Q \otimes P)$
⟨*proof*⟩

lemma *hcomp-assoc*:
  $(P \otimes (Q \otimes R)) = ((P \otimes Q) \otimes R)$
⟨*proof*⟩

lemma *emp-hcomp*:
  $\varepsilon \otimes P = P$
⟨*proof*⟩

lemma *hcomp-emp*:
  $P \otimes \varepsilon = P$
⟨*proof*⟩

lemma *comp-fun-commute-hcomp*:
  comp-fun-commute (⊗)
⟨*proof*⟩

6.2 An iterated horizontal-composition operator

definition *iter-hcomp* :: (*'a fset*) ⇒ (*'a* ⇒ *interface*) ⇒ *interface*
where
  iter-hcomp X f ≡ *ffold* ((⊗) ∘ *f*) ε *X*

syntax *iter-hcomp-syntax* ::
  'a ⇒ (*'a fset*) ⇒ (*'a* ⇒ *interface*) ⇒ *interface*
    ((⨂ -|∈|-. -) [*0*,*0*,*10*] *10*)
translations ⨂ *x*|∈|*M*. *e* == *CONST iter-hcomp M* (λ*x*. *e*)

term $\bigotimes P|\in|Ps.\ f\ P$ — this is eta-expanded, so prints in expanded form
term $\bigotimes P|\in|Ps.\ f$ — this isn't eta-expanded, so prints as written

lemma *iter-hcomp-cong*:
  assumes $\forall\, v \in \mathit{fset}\ vs.\ \varphi\ v = \varphi'\ v$
  shows $(\bigotimes v|\in|vs.\ \varphi\ v) = (\bigotimes v|\in|vs.\ \varphi'\ v)$
$\langle proof \rangle$

lemma *iter-hcomp-empty*:
  shows $(\bigotimes x\ |\in|\ \{||\}.\ p\ x) = \varepsilon$
  $\langle proof \rangle$

lemma *iter-hcomp-insert*:
  assumes $v\ |\notin|\ ws$
  shows $(\bigotimes x\ |\in|\ \mathit{finsert}\ v\ ws.\ p\ x) = (p\ v \otimes (\bigotimes x\ |\in|\ ws.\ p\ x))$
$\langle proof \rangle$

lemma *iter-hcomp-union*:
  assumes $vs\ |\cap|\ ws = \{||\}$
  shows $(\bigotimes x\ |\in|\ vs\ |\cup|\ ws.\ p\ x) = ((\bigotimes x\ |\in|\ vs.\ p\ x) \otimes (\bigotimes x\ |\in|\ ws.\ p\ x))$
$\langle proof \rangle$

6.3 Semantics of interfaces

The semantics of an interface is an assertion.

fun
  $\mathit{conc\text{-}asn} :: \mathit{conc\text{-}interface} \Rightarrow \mathit{assertion}$
where
  $\mathit{conc\text{-}asn}\ (\mathit{Ribbon\text{-}conc}\ p) = p$
$|\ \mathit{conc\text{-}asn}\ (P \otimes_c Q) = (\mathit{conc\text{-}asn}\ P) \star (\mathit{conc\text{-}asn}\ Q)$
$|\ \mathit{conc\text{-}asn}\ (\varepsilon_c) = \mathit{Emp}$
$|\ \mathit{conc\text{-}asn}\ (\mathit{Exists\text{-}int\text{-}conc}\ x\ P) = \mathit{Exists}\ x\ (\mathit{conc\text{-}asn}\ P)$

lift-definition
  $\mathit{asn} :: \mathit{interface} \Rightarrow \mathit{assertion}$
is *conc-asn*
$\langle proof \rangle$

lemma *asn-simps* [*simp*]:
  $\mathit{asn}\ (\mathit{Ribbon}\ p) = p$
  $\mathit{asn}\ (P \otimes Q) = (\mathit{asn}\ P) \star (\mathit{asn}\ Q)$
  $\mathit{asn}\ \varepsilon = \mathit{Emp}$
  $\mathit{asn}\ (\mathit{Exists\text{-}int}\ x\ P) = \mathit{Exists}\ x\ (\mathit{asn}\ P)$
$\langle proof \rangle$

6.4 Program variables mentioned in an interface.

fun

rd-conc-int :: *conc-interface* ⇒ *string set*
where
rd-conc-int (*Ribbon-conc p*) = *rd-ass p*
| *rd-conc-int* ($P \otimes_c Q$) = *rd-conc-int P* ∪ *rd-conc-int Q*
| *rd-conc-int* (ε_c) = {}
| *rd-conc-int* (*Exists-int-conc x P*) = *rd-conc-int P*

lift-definition
rd-int :: *interface* ⇒ *string set*
is *rd-conc-int*
⟨*proof*⟩

The program variables read by an interface are the same as those read by its corresponding assertion.

lemma *rd-int-is-rd-ass*:
rd-ass (*asn P*) = *rd-int P*
⟨*proof*⟩

Here is an iterated version of the Hoare logic sequencing rule.

lemma *seq-fold*:
$\bigwedge\Pi$. ⟦ *length cs* = *chainlen* Π ; *p1* = *asn* (*pre* Π) ; *p2* = *asn* (*post* Π) ;
$\bigwedge i$. *i* < *chainlen* Π ⟹ *prov-triple*
(*asn* (*fst3* (*nthtriple* Π *i*)), *cs* ! *i*, *asn* (*thd3* (*nthtriple* Π *i*))) ⟧
⟹ *prov-triple* (*p1*, *foldr* (;;) *cs Skip*, *p2*)
⟨*proof*⟩

end

7 Syntax and proof rules for stratified diagrams

theory *Ribbons-Stratified* **imports**
Ribbons-Interfaces
Proofchain
begin

We define the syntax of stratified diagrams. We give proof rules for stratified diagrams, and prove them sound with respect to the ordinary rules of separation logic.

7.1 Syntax of stratified diagrams

datatype *sdiagram* = *SDiagram* (*cell* × *interface*) *list*
and *cell* =
Filler interface
| *Basic interface command interface*
| *Exists-sdia string sdiagram*
| *Choose-sdia interface sdiagram sdiagram interface*
| *Loop-sdia interface sdiagram interface*

datatype-compat *sdiagram cell*

type-synonym $row = cell \times interface$

Extracting the command from a stratified diagram.

fun
  $com\text{-}sdia :: sdiagram \Rightarrow command$ **and**
  $com\text{-}cell :: cell \Rightarrow command$
where
  $com\text{-}sdia\ (SDiagram\ \varrho s) = foldr\ (;;)\ (map\ (com\text{-}cell \circ fst)\ \varrho s)\ Skip$
$|\ com\text{-}cell\ (Filler\ P) = Skip$
$|\ com\text{-}cell\ (Basic\ P\ c\ Q) = c$
$|\ com\text{-}cell\ (Exists\text{-}sdia\ x\ D) = com\text{-}sdia\ D$
$|\ com\text{-}cell\ (Choose\text{-}sdia\ P\ D\ E\ Q) = Choose\ (com\text{-}sdia\ D)\ (com\text{-}sdia\ E)$
$|\ com\text{-}cell\ (Loop\text{-}sdia\ P\ D\ Q) = Loop\ (com\text{-}sdia\ D)$

Extracting the program variables written by a stratified diagram.

fun
  $wr\text{-}sdia :: sdiagram \Rightarrow string\ set$ **and**
  $wr\text{-}cell :: cell \Rightarrow string\ set$
where
  $wr\text{-}sdia\ (SDiagram\ \varrho s) = (\bigcup r \in set\ \varrho s.\ wr\text{-}cell\ (fst\ r))$
$|\ wr\text{-}cell\ (Filler\ P) = \{\}$
$|\ wr\text{-}cell\ (Basic\ P\ c\ Q) = wr\text{-}com\ c$
$|\ wr\text{-}cell\ (Exists\text{-}sdia\ x\ D) = wr\text{-}sdia\ D$
$|\ wr\text{-}cell\ (Choose\text{-}sdia\ P\ D\ E\ Q) = wr\text{-}sdia\ D \cup wr\text{-}sdia\ E$
$|\ wr\text{-}cell\ (Loop\text{-}sdia\ P\ D\ Q) = wr\text{-}sdia\ D$

The program variables written by a stratified diagram correspond to those written by the commands therein.

lemma *wr-sdia-is-wr-com*:
  fixes $\varrho s :: row\ list$
  and $\varrho :: row$
  shows $(wr\text{-}sdia\ D = wr\text{-}com\ (com\text{-}sdia\ D))$
  and $(wr\text{-}cell\ \gamma = wr\text{-}com\ (com\text{-}cell\ \gamma))$
  and $(\bigcup \varrho \in set\ \varrho s.\ wr\text{-}cell\ (fst\ \varrho))$
    $= wr\text{-}com\ (foldr\ (;;)\ (map\ (\lambda(\gamma,F).\ com\text{-}cell\ \gamma)\ \varrho s)\ Skip)$
  and $wr\text{-}cell\ (fst\ \varrho) = wr\text{-}com\ (com\text{-}cell\ (fst\ \varrho))$
⟨*proof*⟩

7.2 Proof rules for stratified diagrams

inductive
  $prov\text{-}sdia :: [sdiagram, interface, interface] \Rightarrow bool$ **and**
  $prov\text{-}row :: [row, interface, interface] \Rightarrow bool$ **and**
  $prov\text{-}cell :: [cell, interface, interface] \Rightarrow bool$
where
  SRibbon: $prov\text{-}cell\ (Filler\ P)\ P\ P$

| *SBasic*: *prov-triple* (*asn* P, c, *asn* Q) $\Longrightarrow$ *prov-cell* (*Basic* P c Q) P Q
| *SExists*: *prov-sdia* D P Q
$\Longrightarrow$ *prov-cell* (*Exists-sdia* x D) (*Exists-int* x P) (*Exists-int* x Q)
| *SChoice*: $[\![$ *prov-sdia* D P Q ; *prov-sdia* E P Q $]\!]$
$\Longrightarrow$ *prov-cell* (*Choose-sdia* P D E Q) P Q
| *SLoop*: *prov-sdia* D P P $\Longrightarrow$ *prov-cell* (*Loop-sdia* P D P) P P
| *SRow*: $[\![$ *prov-cell* γ P Q ; *wr-cell* $\gamma \cap$ *rd-int* $F = \{\}$ $]\!]$
$\Longrightarrow$ *prov-row* (γ, F) ($P \otimes F$) ($Q \otimes F$)
| *SMain*: $[\![$ *chain-all* ($\lambda(P,\varrho,Q)$. *prov-row* ϱ P Q) Π ; $0 <$ *chainlen* Π $]\!]$
$\Longrightarrow$ *prov-sdia* (*SDiagram* (*comlist* Π)) (*pre* Π) (*post* Π)

7.3 Soundness

lemma *soundness-strat-helper*:
(*prov-sdia* D P Q $\longrightarrow$ *prov-triple* (*asn* P, *com-sdia* D, *asn* Q)) $\wedge$
(*prov-row* ϱ P Q $\longrightarrow$ *prov-triple* (*asn* P, *com-cell* (*fst* ϱ), *asn* Q)) $\wedge$
(*prov-cell* γ P Q $\longrightarrow$ *prov-triple* (*asn* P, *com-cell* γ, *asn* Q))
$\langle$*proof*$\rangle$

corollary *soundness-strat*:
assumes *prov-sdia* D P Q
shows *prov-triple* (*asn* P, *com-sdia* D, *asn* Q)
$\langle$*proof*$\rangle$

end

8 Syntax and proof rules for graphical diagrams

theory *Ribbons-Graphical* **imports**
Ribbons-Interfaces
begin

We introduce a graphical syntax for diagrams, describe how to extract commands and interfaces, and give proof rules for graphical diagrams.

8.1 Syntax of graphical diagrams

Fix a type for node identifiers

typedecl *node*

Note that this datatype is necessarily an overapproximation of syntactically-wellformed diagrams, for the reason that we can't impose the well-formedness constraints while maintaining admissibility of the datatype declarations. So, we shall impose well-formedness in a separate definition.

datatype *assertion-gadget* =
Rib assertion
| *Exists-dia string diagram*

and *command-gadget* =
  Com command
| *Choose-dia diagram diagram*
| *Loop-dia diagram*
and *diagram* = *Graph*
  node fset
  node ⇒ *assertion-gadget*
  (*node fset* × *command-gadget* × *node fset*) *list*
type-synonym *labelling* = *node* ⇒ *assertion-gadget*
type-synonym *edge* = *node fset* × *command-gadget* × *node fset*

Projecting components from a graph

fun *vertices* :: *diagram* ⇒ *node fset* (-^*V* [*1000*] *1000*)
where (*Graph V* Λ *E*)^*V* = *V*

term *this* (*is*^*V*) = (*a test*)^*V*

fun *labelling* :: *diagram* ⇒ *labelling* (-^Λ [*1000*] *1000*)
where (*Graph V* Λ *E*)^Λ = Λ

fun *edges* :: *diagram* ⇒ *edge list* (-^*E* [*1000*] *1000*)
where (*Graph V* Λ *E*)^*E* = *E*

8.2 Well formedness of graphical diagrams

definition *acyclicity* :: *edge list* ⇒ *bool*
where
  acyclicity E ≡ *acyclic* (⋃ *e* ∈ *set E*. *fset* (*fst3 e*) × *fset* (*thd3 e*))

definition *linearity* :: *edge list* ⇒ *bool*
where
  linearity E ≡
    distinct E ∧ (∀ *e* ∈ *set E*. ∀ *f* ∈ *set E*. *e* ≠ *f* ⟶
    fst3 e |∩| *fst3 f* = {||} ∧
    thd3 e |∩| *thd3 f* = {||})

lemma *linearityD*:
  assumes *linearity E*
  shows *distinct E*
  and ⋀*e f*. ⟦ *e* ∈ *set E* ; *f* ∈ *set E* ; *e* ≠ *f* ⟧ ⟹
    fst3 e |∩| *fst3 f* = {||} ∧
    thd3 e |∩| *thd3 f* = {||}
⟨*proof*⟩

lemma *linearityD2*:
  linearity E ⟹ (∀ *e f*. *e* ∈ *set E* ∧ *f* ∈ *set E* ∧ *e* ≠ *f* ⟶
    fst3 e |∩| *fst3 f* = {||} ∧
    thd3 e |∩| *thd3 f* = {||})
⟨*proof*⟩

inductive
wf-ass :: *assertion-gadget* ⇒ *bool* **and**
wf-com :: *command-gadget* ⇒ *bool* **and**
wf-dia :: *diagram* ⇒ *bool*
where
wf-rib: *wf-ass* (*Rib p*)
| *wf-exists*: *wf-dia G* ⟹ *wf-ass* (*Exists-dia x G*)
| *wf-com*: *wf-com* (*Com c*)
| *wf-choice*: ⟦ *wf-dia G* ; *wf-dia H* ⟧ ⟹ *wf-com* (*Choose-dia G H*)
| *wf-loop*: *wf-dia G* ⟹ *wf-com* (*Loop-dia G*)
| *wf-dia*: ⟦ ∀ *e* ∈ *set E*. *wf-com* (*snd3 e*) ; ∀ *v* ∈ *fset V*. *wf-ass* (Λ *v*) ;
acyclicity E ; *linearity E* ; ∀ *e* ∈ *set E*. *fst3 e* |∪| *thd3 e* |⊆| *V* ⟧ ⟹
wf-dia (*Graph V* Λ *E*)

inductive-cases *wf-dia-inv′*: *wf-dia* (*Graph V* Λ *E*)

lemma *wf-dia-inv*:
assumes *wf-dia* (*Graph V* Λ *E*)
shows ∀ *v* ∈ *fset V*. *wf-ass* (Λ *v*)
and ∀ *e* ∈ *set E*. *wf-com* (*snd3 e*)
and *acyclicity E*
and *linearity E*
and ∀ *e* ∈ *set E*. *fst3 e* |∪| *thd3 e* |⊆| *V*
⟨*proof*⟩

8.3 Initial and terminal nodes

definition
initials :: *diagram* ⇒ *node fset*
where
initials G = *ffilter* (λ*v*. (∀ *e* ∈ *set G^E*. *v* |∉| *thd3 e*)) *G^V*

definition
terminals :: *diagram* ⇒ *node fset*
where
terminals G = *ffilter* (λ*v*. (∀ *e* ∈ *set G^E*. *v* |∉| *fst3 e*)) *G^V*

lemma *no-edges-imp-all-nodes-initial*:
initials (*Graph V* Λ []) = *V*
⟨*proof*⟩

lemma *no-edges-imp-all-nodes-terminal*:
terminals (*Graph V* Λ []) = *V*
⟨*proof*⟩

lemma *initials-in-vertices*:
initials G |⊆| *G^V*
⟨*proof*⟩

lemma *terminals-in-vertices*:
  terminals G $|\subseteq|$ $G\hat{\ }V$
$\langle$*proof*$\rangle$

8.4 Top and bottom interfaces

primrec
  top-ass :: *assertion-gadget* $\Rightarrow$ *interface* **and**
  top-dia :: *diagram* $\Rightarrow$ *interface*
where
  top-dia (*Graph* V Λ E) = ($\bigotimes v$ $|\in|$ *initials* (*Graph* V Λ E). *top-ass* (Λ v))
| *top-ass* (*Rib* p) = *Ribbon* p
| *top-ass* (*Exists-dia* x G) = *Exists-int* x (*top-dia* G)

primrec
  bot-ass :: *assertion-gadget* $\Rightarrow$ *interface* **and**
  bot-dia :: *diagram* $\Rightarrow$ *interface*
where
  bot-dia (*Graph* V Λ E) = ($\bigotimes v$ $|\in|$ *terminals* (*Graph* V Λ E). *bot-ass* (Λ v))
| *bot-ass* (*Rib* p) = *Ribbon* p
| *bot-ass* (*Exists-dia* x G) = *Exists-int* x (*bot-dia* G)

8.5 Proof rules for graphical diagrams

inductive
  prov-dia :: [*diagram*, *interface*, *interface*] $\Rightarrow$ *bool* **and**
  prov-com :: [*command-gadget*, *interface*, *interface*] $\Rightarrow$ *bool* **and**
  prov-ass :: *assertion-gadget* $\Rightarrow$ *bool*
where
  Skip: *prov-ass* (*Rib* p)
| *Exists*: *prov-dia* G - - $\Longrightarrow$ *prov-ass* (*Exists-dia* x G)
| *Basic*: *prov-triple* (*asn* P, c, *asn* Q) $\Longrightarrow$ *prov-com* (*Com* c) P Q
| *Choice*: $[\![$ *prov-dia* G P Q ; *prov-dia* H P Q $]\!]$
    $\Longrightarrow$ *prov-com* (*Choose-dia* G H) P Q
| *Loop*: *prov-dia* G P P $\Longrightarrow$ *prov-com* (*Loop-dia* G) P P
| *Main*: $[\![$ *wf-dia* G ; $\bigwedge v.$ $v \in$ *fset* $G\hat{\ }V$ $\Longrightarrow$ *prov-ass* ($G\hat{\ }\Lambda$ v);
    $\bigwedge e.$ $e \in$ *set* $G\hat{\ }E$ $\Longrightarrow$ *prov-com* (*snd3* e)
      ($\bigotimes v$ $|\in|$ *fst3* e. *bot-ass* ($G\hat{\ }\Lambda$ v))
      ($\bigotimes v$ $|\in|$ *thd3* e. *top-ass* ($G\hat{\ }\Lambda$ v))$]\!]$
    $\Longrightarrow$ *prov-dia* G (*top-dia* G) (*bot-dia* G)

inductive-cases *main-inv*: *prov-dia* (*Graph* V Λ E) P Q
inductive-cases *loop-inv*: *prov-com* (*Loop-dia* G) P Q
inductive-cases *choice-inv*: *prov-com* (*Choose-dia* G H) P Q
inductive-cases *basic-inv*: *prov-com* (*Com* c) P Q
inductive-cases *exists-inv*: *prov-ass* (*Exists-dia* x G)
inductive-cases *skip-inv*: *prov-ass* (*Rib* p)

8.6 Extracting commands from diagrams

type-synonym *lin* = (*node* + *edge*) *list*

A linear extension (lin) of a diagram is a list of its nodes and edges which respects the order of those nodes and edges. That is, if an edge e goes from node v to node w, then v and e and w must have strictly increasing positions in the list.

definition $lins :: diagram \Rightarrow lin\ set$
where
$lins\ G \equiv \{\pi :: lin.$
$\quad (distinct\ \pi)$
$\quad \wedge\ (set\ \pi = (fset\ G\hat{\ }V)\ \text{<+>}\ (set\ G\hat{\ }E))$
$\quad \wedge\ (\forall\, i\ j\ v\ e.\ i < length\ \pi \wedge j < length\ \pi \wedge \pi!i = Inl\ v \wedge \pi!j = Inr\ e$
$\quad\quad \wedge\ v\ |{\in}|\ fst3\ e \longrightarrow i{<}j)$
$\quad \wedge\ (\forall\, j\ k\ w\ e.\ j < length\ \pi \wedge k < length\ \pi \wedge \pi!j = Inr\ e \wedge \pi!k = Inl\ w$
$\quad\quad \wedge\ w\ |{\in}|\ thd3\ e \longrightarrow j{<}k)\ \}$

lemma *linsD*:
assumes $\pi \in lins\ G$
shows $(distinct\ \pi)$
and $(set\ \pi = (fset\ G\hat{\ }V)\ \text{<+>}\ (set\ G\hat{\ }E))$
and $(\forall\, i\ j\ v\ e.\ i < length\ \pi \wedge j < length\ \pi$
$\quad \wedge\ \pi!i = Inl\ v \wedge \pi!j = Inr\ e \wedge v\ |{\in}|\ fst3\ e \longrightarrow i{<}j)$
and $(\forall\, j\ k\ w\ e.\ j < length\ \pi \wedge k < length\ \pi$
$\quad \wedge\ \pi!j = Inr\ e \wedge \pi!k = Inl\ w \wedge w\ |{\in}|\ thd3\ e \longrightarrow j{<}k)$
$\langle proof \rangle$

The following lemma enables the inductive definition below to be proved monotonic. It does this by showing how one of the premises of the *coms-main* rule can be rewritten in a form that is more verbose but easier to prove monotonic.

lemma *coms-mono-helper*:
$(\forall\, i{<}length\ \pi.\ case\text{-}sum\ (coms\text{-}ass \circ \Lambda)\ (coms\text{-}com \circ snd3)\ (\pi!i)\ (cs!i))$
$=$
$((\forall\, i.\ i{<}length\ \pi \wedge (\exists\, v.\ (\pi!i) = Inl\ v) \longrightarrow$
$\quad coms\text{-}ass\ (\Lambda\ (projl\ (\pi!i)))\ (cs!i)) \wedge$
$(\forall\, i.\ i{<}length\ \pi \wedge (\exists\, e.\ (\pi!i) = Inr\ e) \longrightarrow$
$\quad coms\text{-}com\ (snd3\ (projr\ (\pi!i)))\ (cs!i)))$
$\langle proof \rangle$

The *coms-dia* function extracts a set of commands from a diagram. Each command in *coms-dia* G is obtained by extracting a command from each of G's nodes and edges (using *coms-ass* or *coms-com* respectively), then picking a linear extension π of these nodes and edges (using *lins*), and composing the extracted commands in accordance with π.

inductive
$coms\text{-}dia :: [diagram,\ command] \Rightarrow bool$ **and**

coms-ass :: [*assertion-gadget*, *command*] $\Rightarrow$ *bool* **and**
coms-com :: [*command-gadget*, *command*] $\Rightarrow$ *bool*
where
coms-skip: *coms-ass* (*Rib p*) *Skip*
| *coms-exists*: *coms-dia G c* $\Longrightarrow$ *coms-ass* (*Exists-dia x G*) *c*
| *coms-basic*: *coms-com* (*Com c*) *c*
| *coms-choice*: $[\![$ *coms-dia G c*; *coms-dia H d* $]\!]$ $\Longrightarrow$
coms-com (*Choose-dia G H*) (*Choose c d*)
| *coms-loop*: *coms-dia G c* $\Longrightarrow$ *coms-com* (*Loop-dia G*) (*Loop c*)
| *coms-main*: $[\![$ $\pi \in$ *lins* (*Graph V* Λ *E*); *length cs* = *length* π;
$\forall\, i<$*length* π. *case-sum* (*coms-ass* $\circ$ Λ) (*coms-com* $\circ$ *snd3*) ($\pi!i$) ($cs!i$) $]\!]$
$\Longrightarrow$ *coms-dia* (*Graph V* Λ *E*) (*foldr* (;;) *cs Skip*)
monos
coms-mono-helper

inductive-cases *coms-skip-inv*: *coms-ass* (*Rib p*) *c*
inductive-cases *coms-exists-inv*: *coms-ass* (*Exists-dia x G*) *c*
inductive-cases *coms-basic-inv*: *coms-com* (*Com* c') *c*
inductive-cases *coms-choice-inv*: *coms-com* (*Choose-dia G H*) *c*
inductive-cases *coms-loop-inv*: *coms-com* (*Loop-dia G*) *c*
inductive-cases *coms-main-inv*: *coms-dia G c*

end

9 Soundness for graphical diagrams

theory *Ribbons-Graphical-Soundness* **imports**
Ribbons-Graphical
More-Finite-Map
begin

We prove that the proof rules for graphical ribbon proofs are sound with respect to the rules of separation logic.

We impose an additional assumption to achieve soundness: that the Frame rule has no side-condition. This assumption is reasonable because there are several separation logics that lack such a side-condition, such as "variables-as-resource".

We first describe how to extract proofchains from a diagram. This process is similar to the process of extracting commands from a diagram, which was described in *Ribbon-Proofs.Ribbons-Graphical*. When we extract a proofchain, we don't just include the commands, but the assertions in between them. Our main lemma for proving soundness says that each of these proofchains corresponds to a valid separation logic proof.

9.1 Proofstate chains

When extracting a proofchain from a diagram, we need to keep track of which nodes we have processed and which ones we haven't. A proofstate, defined below, maps a node to "Top" if it hasn't been processed and "Bot" if it has.

datatype *topbot* = *Top* | *Bot*

type-synonym *proofstate* = *node* $\rightharpoonup_f$ *topbot*

A proofstate chain contains all the nodes and edges of a graphical diagram, interspersed with proofstates that track which nodes have been processed at each point.

type-synonym *ps-chain* = (*proofstate*, *node* + *edge*) *chain*

The *next-ps* σ function processes one node or one edge in a diagram, given the current proofstate σ. It processes a node v by replacing the mapping from v to *Top* with a mapping from v to *Bot*. It processes an edge e (whose source and target nodes are *vs* and *ws* respectively) by removing all the mappings from *vs* to *Bot*, and adding mappings from *ws* to *Top*.

fun *next-ps* :: *proofstate* ⇒ *node* + *edge* ⇒ *proofstate*
where
  next-ps σ (*Inl* v) = $\sigma \ominus \{|v|\} ++_f [\{|v|\} \mid\!=\!> Bot]$
| *next-ps* σ (*Inr* e) = $\sigma \ominus fst3\ e ++_f [thd3\ e \mid\!=\!> Top]$

The function *mk-ps-chain* Π π generates from π, which is a list of nodes and edges, a proofstate chain, by interspersing the elements of π with the appropriate proofstates. The first argument Π is the part of the chain that has already been converted.

definition
  mk-ps-chain :: [*ps-chain*, (*node* + *edge*) *list*] ⇒ *ps-chain*
where
  mk-ps-chain ≡ *foldl* (λΠ *x*. *cSnoc* Π *x* (*next-ps* (*post* Π) *x*))

lemma *mk-ps-chain-preserves-length*:
  fixes π Π
  shows *chainlen* (*mk-ps-chain* Π π) = *chainlen* Π + *length* π
⟨*proof*⟩

Distributing *mk-ps-chain* over (#).

lemma *mk-ps-chain-cons*:
  mk-ps-chain Π (*x* # π) = *mk-ps-chain* (*cSnoc* Π *x* (*next-ps* (*post* Π) *x*)) π
⟨*proof*⟩

Distributing *mk-ps-chain* over *snoc*.

lemma *mk-ps-chain-snoc*:

mk-ps-chain Π (π @ [x])
  = *cSnoc* (*mk-ps-chain* Π π) x (*next-ps* (*post* (*mk-ps-chain* Π π)) x)
$\langle$*proof*$\rangle$

Distributing *mk-ps-chain* over *cCons*.

lemma *mk-ps-chain-ccons*:
  fixes π Π
  shows *mk-ps-chain* ($\{\!|\ \sigma\ |\!\}$ $\cdot$ x $\cdot$ Π) π = $\{\!|\ \sigma\ |\!\}$ $\cdot$ x $\cdot$ *mk-ps-chain* Π π
$\langle$*proof*$\rangle$

lemma *pre-mk-ps-chain*:
  fixes Π π
  shows *pre* (*mk-ps-chain* Π π) = *pre* Π
$\langle$*proof*$\rangle$

A chain which is obtained from the list π, has π as its list of commands. The following lemma states this in a slightly more general form, that allows for part of the chain to have already been processed.

lemma *comlist-mk-ps-chain*:
  comlist (*mk-ps-chain* Π π) = *comlist* Π @ π
$\langle$*proof*$\rangle$

In order to perform induction over our diagrams, we shall wish to obtain "smaller" diagrams, by removing nodes or edges. However, the syntax and well-formedness constraints for diagrams are such that although we can always remove an edge from a diagram, we cannot (in general) remove a node – the resultant diagram would not be a well-formed if an edge connected to that node.

Hence, we consider "partially-processed diagrams" (G, S), which comprise a diagram G and a set S of nodes. S denotes the subset of G's initial nodes that have already been processed, and can be thought of as having been removed from G.

We now give an updated version of the *lins* G function. This was originally defined in *Ribbon-Proofs.Ribbons-Graphical*. We provide an extra parameter, S, which denotes the subset of G's initial nodes that shouldn't be included in the linear extensions.

definition *lins2* :: [*node fset*, *diagram*] $\Rightarrow$ *lin set*
where
  lins2 S G $\equiv$ {π :: *lin* .
    (*distinct* π)
  $\wedge$ (*set* π = (*fset* G^V − *fset* S) <+> *set* G^E)
  $\wedge$ ($\forall$ i j v e. i < *length* π $\wedge$ j < *length* π
    $\wedge$ $\pi!i$ = *Inl* v $\wedge$ $\pi!j$ = *Inr* e $\wedge$ v $|\!\in\!|$ *fst3* e $\longrightarrow$ i<j)
  $\wedge$ ($\forall$ j k w e. j < *length* π $\wedge$ k < *length* π
    $\wedge$ $\pi!j$ = *Inr* e $\wedge$ $\pi!k$ = *Inl* w $\wedge$ w $|\!\in\!|$ *thd3* e $\longrightarrow$ j<k) }

lemma *lins2D*:
  assumes $\pi \in$ *lins2 S G*
  shows *distinct* π
    and *set* $\pi = (fset\ G\hat{\ }V\ -\ fset\ S)$ <+> *set* $G\hat{\ }E$
    and $\bigwedge i\ j\ v\ e.\ [\![\ i < length\ \pi\ ;\ j < length\ \pi\ ;$
      $\pi!i = Inl\ v\ ;\ \pi!j = Inr\ e\ ;\ v\ |\!\in\!|\ fst3\ e\ ]\!] \Longrightarrow i{<}j$
    and $\bigwedge i\ k\ w\ e.\ [\![\ j < length\ \pi\ ;\ k < length\ \pi\ ;$
      $\pi!j = Inr\ e\ ;\ \pi!k = Inl\ w\ ;\ w\ |\!\in\!|\ thd3\ e\ ]\!] \Longrightarrow j{<}k$
⟨*proof*⟩

lemma *lins2I*:
  assumes *distinct* π
    and *set* $\pi = (fset\ G\hat{\ }V\ -\ fset\ S)$ <+> *set* $G\hat{\ }E$
    and $\bigwedge i\ j\ v\ e.\ [\![\ i < length\ \pi\ ;\ j < length\ \pi\ ;$
      $\pi!i = Inl\ v\ ;\ \pi!j = Inr\ e\ ;\ v\ |\!\in\!|\ fst3\ e\ ]\!] \Longrightarrow i{<}j$
    and $\bigwedge j\ k\ w\ e.\ [\![\ j < length\ \pi\ ;\ k < length\ \pi\ ;$
      $\pi!j = Inr\ e\ ;\ \pi!k = Inl\ w\ ;\ w\ |\!\in\!|\ thd3\ e\ ]\!] \Longrightarrow j{<}k$
  shows $\pi \in$ *lins2 S G*
⟨*proof*⟩

When S is empty, the two definitions coincide.

lemma *lins-is-lins2-with-empty-S*:
  lins G = *lins2* {||} *G*
⟨*proof*⟩

The first proofstate for a diagram G is obtained by mapping each of its initial nodes to *Top*.

definition
  initial-ps :: *diagram* ⇒ *proofstate*
where
  initial-ps G ≡ [*initials G* |=> *Top*]

The first proofstate for the partially-processed diagram G is obtained by mapping each of its initial nodes to *Top*, except those in S, which are mapped to *Bot*.

definition
  initial-ps2 :: [*node fset*, *diagram*] ⇒ *proofstate*
where
  initial-ps2 S G ≡ [*initials G* − *S* |=> *Top*] $++_f$ [*S* |=> *Bot*]

When S is empty, the above two definitions coincide.

lemma *initial-ps-is-initial-ps2-with-empty-S*:
  initial-ps = *initial-ps2* {||}
⟨*proof*⟩

The following function extracts the set of proofstate chains from a diagram.

definition
  ps-chains :: *diagram* ⇒ *ps-chain set*

where
  $\mathit{ps\text{-}chains}\ G \equiv \mathit{mk\text{-}ps\text{-}chain}\ (\mathit{cNil}\ (\mathit{initial\text{-}ps}\ G))$ ‘ $\mathit{lins}\ G$

The following function extracts the set of proofstate chains from a partially-processed diagram. Nodes in S are excluded from the resulting chains.

definition
  $\mathit{ps\text{-}chains2} :: [\mathit{node\ fset},\ \mathit{diagram}] \Rightarrow \mathit{ps\text{-}chain\ set}$
where
  $\mathit{ps\text{-}chains2}\ S\ G \equiv \mathit{mk\text{-}ps\text{-}chain}\ (\mathit{cNil}\ (\mathit{initial\text{-}ps2}\ S\ G))$ ‘ $\mathit{lins2}\ S\ G$

When S is empty, the above two definitions coincide.

lemma *ps-chains-is-ps-chains2-with-empty-S*:
  $\mathit{ps\text{-}chains} = \mathit{ps\text{-}chains2}\ \{||\}$
$\langle \mathit{proof} \rangle$

We now wish to describe proofstates chain that are well-formed. First, let us say that $f\ {++}_f\ \mathit{disjoint}\ g$ is defined, when f and g have disjoint domains, as $f\ {++}_f\ g$. Then, a well-formed proofstate chain consists of triples of the form $(\sigma\ {++}_f\ \mathit{disjoint}\ [\ \{|v|\}\ |{=}{>}\ \mathit{Top}\ ],\ \mathit{Inl}\ v,\ \sigma\ {++}_f\ \mathit{disjoint}\ [\ \{|v|\}\ |{=}{>}\ \mathit{Bot}\ ])$, where v is a node, or of the form $(\sigma\ {++}_f\ \mathit{disjoint}\ [\ \{|vs|\}\ |{=}{>}\ \mathit{Bot}\ ],\ \mathit{Inr}\ e,\ \sigma\ {++}_f\ \mathit{disjoint}\ [\ \{|ws|\}\ |{=}{>}\ \mathit{Top}\ ])$, where e is an edge with source and target nodes vs and ws respectively.

The definition below describes a well-formed triple; we then lift this to complete chains shortly.

definition
  $\mathit{wf\text{-}ps\text{-}triple} :: \mathit{proofstate} \times (\mathit{node} + \mathit{edge}) \times \mathit{proofstate} \Rightarrow \mathit{bool}$
where
  $\mathit{wf\text{-}ps\text{-}triple}\ T = (\mathit{case}\ \mathit{snd3}\ T\ \mathit{of}$
    $\mathit{Inl}\ v \Rightarrow (\exists \sigma.\ v\ |{\notin}|\ \mathit{fmdom}\ \sigma$
      $\wedge\ \mathit{fst3}\ T = [\ \{|v|\}\ |{=}{>}\ \mathit{Top}\ ]\ {++}_f\ \sigma$
      $\wedge\ \mathit{thd3}\ T = [\ \{|v|\}\ |{=}{>}\ \mathit{Bot}\ ]\ {++}_f\ \sigma)$
  $|\ \mathit{Inr}\ e \Rightarrow (\exists \sigma.\ (\mathit{fst3}\ e\ |{\cup}|\ \mathit{thd3}\ e)\ |{\cap}|\ \mathit{fmdom}\ \sigma = \{||\}$
      $\wedge\ \mathit{fst3}\ T = [\ \mathit{fst3}\ e\ |{=}{>}\ \mathit{Bot}\ ]\ {++}_f\ \sigma$
      $\wedge\ \mathit{thd3}\ T = [\ \mathit{thd3}\ e\ |{=}{>}\ \mathit{Top}\ ]\ {++}_f\ \sigma))$

lemma *wf-ps-triple-nodeI*:
  assumes $\exists \sigma.\ v\ |{\notin}|\ \mathit{fmdom}\ \sigma\ \wedge$
    $\sigma 1 = [\ \{|v|\}\ |{=}{>}\ \mathit{Top}\ ]\ {++}_f\ \sigma\ \wedge$
    $\sigma 2 = [\ \{|v|\}\ |{=}{>}\ \mathit{Bot}\ ]\ {++}_f\ \sigma$
  shows $\mathit{wf\text{-}ps\text{-}triple}\ (\sigma 1,\ \mathit{Inl}\ v,\ \sigma 2)$
$\langle \mathit{proof} \rangle$

lemma *wf-ps-triple-edgeI*:
  assumes $\exists \sigma.\ (\mathit{fst3}\ e\ |{\cup}|\ \mathit{thd3}\ e)\ |{\cap}|\ \mathit{fmdom}\ \sigma = \{||\}$
      $\wedge\ \sigma 1 = [\ \mathit{fst3}\ e\ |{=}{>}\ \mathit{Bot}\ ]\ {++}_f\ \sigma$
      $\wedge\ \sigma 2 = [\ \mathit{thd3}\ e\ |{=}{>}\ \mathit{Top}\ ]\ {++}_f\ \sigma$
  shows $\mathit{wf\text{-}ps\text{-}triple}\ (\sigma 1,\ \mathit{Inr}\ e,\ \sigma 2)$

⟨*proof*⟩

definition
wf-ps-chain :: *ps-chain* ⇒ *bool*
where
wf-ps-chain ≡ *chain-all wf-ps-triple*

lemma *next-initial-ps2-vertex*:
initial-ps2 ({|*v*|} |∪| *S*) *G*
= *initial-ps2 S G* ⊖ {|*v*|} $++_f$ [{|*v*|} |=> *Bot*]
⟨*proof*⟩

lemma *next-initial-ps2-edge*:
assumes *G* = *Graph V* Λ *E* **and** *G′* = *Graph V′* Λ *E′* **and**
V′ = *V* − *fst3 e* **and** *E′* = *removeAll e E* **and** *e* ∈ *set E* **and**
fst3 e |⊆| *S* **and** *S* |⊆| *initials G* **and** *wf-dia G*
shows *initial-ps2* (*S* − *fst3 e*) *G′* =
initial-ps2 S G ⊖ *fst3 e* $++_f$ [*thd3 e* |=> *Top*]
⟨*proof*⟩

lemma *next-lins2-vertex*:
assumes *Inl v* # π ∈ *lins2 S G*
assumes *v* |∉| *S*
shows π ∈ *lins2* ({|*v*|} |∪| *S*) *G*
⟨*proof*⟩

lemma *next-lins2-edge*:
assumes *Inr e* # π ∈ *lins2 S* (*Graph V* Λ *E*)
and *vs* |⊆| *S*
and *e* = (*vs*,*c*,*ws*)
shows π ∈ *lins2* (*S* − *vs*) (*Graph* (*V* − *vs*) Λ (*removeAll e E*))
⟨*proof*⟩

We wish to prove that every proofstate chain that can be obtained from a linear extension of *G* is well-formed and has as its final proofstate that state in which every terminal node in *G* is mapped to *Bot*.

We first prove this for partially-processed diagrams, for then the result for ordinary diagrams follows as an easy corollary.

We use induction on the size of the partially-processed diagram. The size of a partially-processed diagram (*G*, *S*) is defined as the number of nodes in *G*, plus the number of edges, minus the number of nodes in *S*.

lemma *wf-chains2*:
fixes *k*
assumes *S* |⊆| *initials G*
and *wf-dia G*
and Π ∈ *ps-chains2 S G*
and *fcard G*^*V* + *length G*^*E* = *k* + *fcard S*
shows *wf-ps-chain* Π ∧ (*post* Π = [*terminals G* |=> *Bot*])

$\langle proof \rangle$

corollary *wf-chains*:
  assumes *wf-dia G*
  assumes $\Pi \in$ *ps-chains G*
  shows *wf-ps-chain* $\Pi \wedge$ *post* $\Pi =$ [*terminals G* |=> *Bot*]
$\langle proof \rangle$

9.2 Interface chains

type-synonym *int-chain* = (*interface*, *assertion-gadget* + *command-gadget*) *chain*

An interface chain is similar to a proofstate chain. However, where a proofstate chain talks about nodes and edges, an interface chain talks about the assertion-gadgets and command-gadgets that label those nodes and edges in a diagram. And where a proofstate chain talks about proofstates, an interface chain talks about the interfaces obtained from those proofstates.

The following functions convert a proofstate chain into an interface chain.

definition
  ps-to-int :: [*diagram*, *proofstate*] $\Rightarrow$ *interface*
where
  ps-to-int $G\ \sigma \equiv$
    $\bigotimes v$ |$\in$| *fmdom* σ. *case-topbot top-ass bot-ass* (*lookup* σ v) (G^Λ v)

definition
  ps-chain-to-int-chain :: [*diagram*, *ps-chain*] $\Rightarrow$ *int-chain*
where
  ps-chain-to-int-chain $G\ \Pi \equiv$
    chainmap (*ps-to-int G*) ((*case-sum* (*Inl* $\circ$ G^Λ) (*Inr* $\circ$ *snd3*))) Π

lemma *ps-chain-to-int-chain-simp*:
  ps-chain-to-int-chain (*Graph* $V\ \Lambda\ E$) Π =
    chainmap (*ps-to-int* (*Graph* $V\ \Lambda\ E$)) ((*case-sum* (*Inl* $\circ$ Λ) (*Inr* $\circ$ *snd3*))) Π
$\langle proof \rangle$

9.3 Soundness proof

We assume that *wr-com* always returns {}. This is equivalent to changing our axiomatization of separation logic such that the frame rule has no side-condition. One way to obtain a separation logic lacking a side-condition on its frame rule is to use variables-as- resource.

We proceed by induction on the proof rules for graphical diagrams. We show that: (1) if a diagram G is provable w.r.t. interfaces P and Q, then P and Q are the top and bottom interfaces of G, and that the Hoare triple (*asn* P, c, *asn* Q) is provable for each command c that can be extracted from G; (2) if a command-gadget C is provable w.r.t. interfaces P and Q, then the Hoare triple (*asn* P, c, *asn* Q) is provable for each command c that can be extracted from C; and (3) if an assertion-gadget A is provable, and if the top and bottom interfaces of A are P and Q respectively, then the Hoare triple ($asn\ P$, c, $asn\ Q$) is provable for each command c that can be extracted from A.

lemma *soundness-graphical-helper*:
  assumes *no-var-interference*: $\bigwedge c.\ wr\text{-}com\ c = \{\}$
  shows
    $(prov\text{-}dia\ G\ P\ Q \longrightarrow$
      $(P = top\text{-}dia\ G \wedge Q = bot\text{-}dia\ G \wedge$
      $(\forall c.\ coms\text{-}dia\ G\ c \longrightarrow prov\text{-}triple\ (asn\ P,\ c,\ asn\ Q))))$
    $\wedge\ (prov\text{-}com\ C\ P\ Q \longrightarrow$
      $(\forall c.\ coms\text{-}com\ C\ c \longrightarrow prov\text{-}triple\ (asn\ P,\ c,\ asn\ Q)))$
    $\wedge\ (prov\text{-}ass\ A \longrightarrow$
      $(\forall c.\ coms\text{-}ass\ A\ c \longrightarrow prov\text{-}triple\ (asn\ (top\text{-}ass\ A),\ c,\ asn\ (bot\text{-}ass\ A))))$
$\langle proof \rangle$

The soundness theorem states that any diagram provable using the proof rules for ribbons can be recreated as a valid proof in separation logic.

corollary *soundness-graphical*:
  assumes $\bigwedge c.\ wr\text{-}com\ c = \{\}$
  assumes $prov\text{-}dia\ G\ P\ Q$
  shows $\forall c.\ coms\text{-}dia\ G\ c \longrightarrow prov\text{-}triple\ (asn\ P,\ c,\ asn\ Q)$
$\langle proof \rangle$

end

References

[1] J. Bean. *Ribbon Proofs - A Proof System for the Logic of Bunched Implications*. PhD thesis, Queen Mary University of London, 2006.

[2] R. Bornat, C. Calcagno, and H. Yang. Variables as resource in separation logic. In *Proceedings of the 21st Annual Conference on Mathematical Foundations of Programming Semantics (MFPS XXI)*, volume 155 of *Electronic Notes in Theoretical Computer Science*, pages 247–276. Elsevier, 2006.

[3] J. Wickerson. *Concurrent Verification for Sequential Programs*. PhD thesis, University of Cambridge, 2013.

[4] J. Wickerson, M. Dodds, and M. J. Parkinson. Ribbon proofs for separation logic. In M. Felleisen and P. Gardner, editors, *Proceedings of the 22nd European Symposium on Programming (ESOP '13)*, 2013. To appear.