pGCL for Isabelle

David Cock

September 19, 2015
Chapter 1

Overview

pGCL is both a programming language and a specification language that incorporates both probabilistic and nondeterministic choice, in a unified manner. Program verification is by refinement or annotation (or both), using either Hoare triples, or weakest-precondition entailment, in the style of GCL [Dijkstra, 1975].

This document is divided into three parts: Chapter 2 gives a tutorial-style introduction to pGCL, and demonstrates the tools provided by the package; Chapter 3 covers the development of the semantic interpretation: expectation transformers; and Chapter 4 covers the formalisation of the language primitives, the associated healthiness results, and the tools for structured and automated reasoning. This second part follows the technical development of the pGCL theory package, in detail. It is not a great place to start learning pGCL. For that, see either the tutorial or McIver and Morgan [2004].

This formalisation was first presented (as an overview) in Cock [2012]. The language has previously been formalised in HOL4 by Hurd et al. [2005]. Two substantial results using this package were presented in Cock [2013], Cock [2014a] and Cock [2014b].
CHAPTER 1. OVERVIEW
Chapter 2

Introduction to pGCL

2.1 Language Primitives

theory Primitives imports ..:/pGCL begin

Programs in pGCL are probabilistic automata. They can do anything a
traditional program can, plus, they may make truly probabilistic choices.

2.1.1 The Basics

Imagine flipping a pair of fair coins: $a$ and $b$. Using a record type for the
state allows a number of syntactic niceties, which we describe shortly:

datatype coin = Heads | Tails

record coins =
  $a$ :: coin
  $b$ :: coin

The primitive state operation is $Apply$, which takes a state transformer as
an argument, constructs the pGCL equivalent. Thus $Apply (a\text{-update } (\lambda$. $Heads))$ sets the value of coin $a$ to $Heads$. As records are so common as state
types, we introduce syntax to make these update neater: The same program
may be defined more simply as $Apply (a\text{-update } (\lambda$. $Heads))$ (note that the
syntax translation involved does not apply to Latex output, and thus this
lemma appears trivial):

lemma
  $Apply (\lambda s. s \{(a := Heads)\}) = (a := (\lambda s. Heads))$
  ⟨proof⟩

We can treat the record’s fields as the names of variables. Note that the
right-hand side of an assignment is always a function of the current state.
Thus we may use a record accessor directly, for example $Apply (\lambda s. s[(a :=
$b s)]), which updates $a$ with the current value of $b$. If we wish to formally
establish that the previous statement is correct i.e. that in the final state, 
a really will have whatever value b had in the initial state, we must first 
introduce the assertion language.

2.1.2 Assertion and Annotation

Assertions in pGCL are real-valued functions of the state, which are often 
interpreted as a probability distribution over possible outcomes. These func-
tions are termed expectations, for reasons which shortly be clear. Initially, 
however, we need only consider standard expectations: those derived from 
a binary predicate. A predicate \( P : s \rightarrow \text{bool} \) is embedded as \( \langle P \rangle : s \rightarrow \text{real} \), such that \( P s \rightarrow \langle P \rangle s = 1 \wedge \neg P s \rightarrow \langle P \rangle s = 0 \).

An annotation consists of an assertion on the initial state and one on the 
final state, which for standard expectations may be interpreted as ‘if \( P \) 
holds in the initial state, then \( Q \) will hold in the final state’. These are 
in weakest-precondition form: we assert that the precondition implies the 
weakest precondition: the weakest assertion on the initial state, which implies 
that the postcondition must hold on the final state. So far, this is identical 
to the standard approach. Remember, however, that we are working with 
real-valued assertions. For standard expectations, the logic is nevertheless 
identical, if the implication \( \forall s. P s \rightarrow Q s \) is substituted with the equivalent 
expectation entailment \( \langle P \rangle \vdash \langle Q \rangle, \langle ?P \rangle \vdash \langle ?Q \rangle; \ ?P \ ?s \implies ?Q \ ?s \). 

Thus a valid specification of \( \text{Apply} (\lambda s. s(a := b s)) \) is:

\[
\text{lemma} \\
\forall x. \langle \lambda s. b s = x \rangle \vdash \text{wp} (a := b) \langle \lambda s. a s = x \rangle
\]

\[
\langle \text{proof} \rangle
\]

Any ordinary computation and its associated annotation can be expressed 
in this form.

2.1.3 Probability

Next, we introduce the syntax \( x ; y \) for the sequential composition of \( x \) and 
\( y \), and also demonstrate that one can operate directly on a real-valued (and 
thus infinite) state space:

\[
\text{lemma} \\
\langle \lambda s::\text{real}. s \neq 0 \rangle \vdash \text{wp} (\text{Apply} (op * 2) ; \text{Apply} (\lambda s. s / s)) \langle \lambda s. s = 1 \rangle
\]

\[
\langle \text{proof} \rangle
\]

So far, we haven’t done anything that required probabilities, or expectations 
other than 0 and 1. As an example of both, we show that a single coin toss is 
fair. We introduce the syntax \( x p \oplus y \) for a probabilistic choice between \( x \) and 
\( y \). This program behaves as \( x \) with probability \( p \), and as \( y \) with probability 
\( (1::'a) \sim p \). The probability may depend on the state, and is therefore of
type 's ⇒ real. The following annotation states that the probability of heads is exactly 1/2:

**definition**

flip-a :: real ⇒ coins prog

**where**

flip-a p = a := (λ-. Heads) (λs. p) ⊕ a := (λ-. Tails)

**lemma**

(λs. 1/2) = wp (flip-a (1/2)) «λs. a s = Heads»

(proof)

2.1.4 Nondeterminism

We can also under-specify a program, using the nondeterministic choice operator, x ∩ y. This is interpreted demonically, giving the pointwise minimum of the pre-expectations for x and y: the chance of seeing heads, if your opponent is allowed choose between a pair of coins, one biased 2/3 heads and one 2/3 tails, and then flips it, is at least 1/3, but we can make no stronger statement:

**lemma**

λs. 1/3 ⊢ wp (flip-a (2/3) ∩ flip-a (1/3)) «λs. a s = Heads»

(proof)

2.1.5 Properties of Expectations

The probabilities of independent events combine as usual, by multiplying: The chance of getting heads on two separate coins is \((1::'a) / (4::'a)\).

**definition**

flip-b :: real ⇒ coins prog

**where**

flip-b p = b := (λ-. Heads) (λs. p) ⊕ b := (λ-. Tails)

**lemma**

(λs. 1/4) = wp (flip-a (1/2) ;; flip-b (1/2)) «λs. a s = Heads ∧ b s = Heads»

(proof)

If, rather than two coins, we use two dice, we can make some slightly more involved calculations. We see that the weakest pre-expectation of the value on the face of the die after rolling is its expected value in the initial state, which justifies the use of the term expectation.

**record** dice =

red :: nat
blue :: nat

definition Puniform :: 'a set ⇒ ('a ⇒ real)
where \( P\text{uniform } S = (\lambda x. \text{ if } x \in S \text{ then } 1 / \text{card } S \text{ else } 0) \)

**Lemma** \( P\text{uniform-in}: \)
\[ x \in S \implies P\text{uniform } S x = 1 / \text{card } S \]
\(\langle\text{proof}\rangle\)

**Lemma** \( P\text{uniform-out}: \)
\[ x \notin S \implies P\text{uniform } S x = 0 \]
\(\langle\text{proof}\rangle\)

**Lemma** \( \text{supp-Puniform}: \)
\[ \text{finite } S \implies \text{supp } (P\text{uniform } S) = S \]
\(\langle\text{proof}\rangle\)

The expected value of a roll of a six-sided die is \((7::'a) / (2::'a)\):

**Lemma**
\[ (\lambda s. 7/2) = \text{wp } ((\text{bind } v \text{ at } (\lambda s. \text{Puniform } \{1..6\} v) \text{ in red := } (\lambda s. v)) \text{ red} \]
\(\langle\text{proof}\rangle\)

The expectations of independent variables add:

**Lemma**
\[ (\lambda s. 7) = \text{wp } ((\text{bind } v \text{ at } (\lambda s. \text{Puniform } \{1..6\} v) \text{ in red := } (\lambda s. v)) \text{ in blue := } (\lambda s. v)) \]
\[ (\lambda s. \text{red } s + \text{blue } s) \]
\(\langle\text{proof}\rangle\)

end

2.2 Loops

**Theory** LoopExamples imports ../pGCL begin

Reasoning about loops in pGCL is mostly familiar, in particular in the use of invariants. Proving termination for truly probabilistic loops is slightly different: We appeal to a 0–1 law to show that the loop terminates with probability 1. In our semantic model, terminating with certainty and with probability 1 are exactly equivalent.

2.2.1 Guaranteed Termination

We start with a completely classical loop, to show that standard techniques apply. Here, we have a program that simply decrements a counter until it hits zero:

**Definition** countdown :: int prog

where
\[ \text{countdown} = \text{do } (\lambda x. 0 < x) \rightarrow \text{Apply } (\lambda s. s - 1) \text{ od} \]
Clearly, this loop will only terminate from a state where \((0::\cdot a) \leq x\). This is, in fact, also a loop invariant.

**Definition** \(inv\text{-}count :: \text{int} \Rightarrow \text{bool}\)

where

\[ \text{inv\text{-}count} = (\lambda x. \ 0 \leq x) \]

Read \(wp\text{-}inv \ G \ \text{body} \ I\) as: \(I\) is an invariant of the loop \(\mu x. \ \text{body} ;; \ x \ « \ G » \oplus \text{Skip}\), or \(« \ G » \&\& \ I \vdash wp \ \text{body} \ I\).

**Lemma** \(wp\text{-}inv\text{-}count\):

\[ wp\text{-}inv \ (\lambda x. \ 0 < x) \ (\text{Apply} \ (\lambda s. \ s - 1)) \ « \text{inv\text{-}count} » \]

(proof)

This example is contrived to give us an obvious variant, or measure function: the counter itself.

**Lemma** \(term\text{-}countdown\):

\[ « \text{inv\text{-}count} » \vdash wp \ \text{countdown} \ (\lambda s. \ 1) \]

(proof)

### 2.2.2 Probabilistic Termination

Loops need not terminate deterministically: it is sufficient to terminate with probability 1. Here we show the intuitively obvious result that by flipping a coin repeatedly, you will eventually see heads.

**Type-synonym** \(\text{coin} = \text{bool}\)

**Definition** \(\text{Heads} = \text{True}\)

**Definition** \(\text{Tails} = \text{False}\)

**Definition** \(\text{flip} :: \text{coin prog}\)

where

\[ \text{flip} = \text{Apply} \ (\lambda -. \ \text{Heads}) \ (\lambda s. \ 1/2) \oplus \text{Apply} \ (\lambda -. \ \text{Tails}) \]

We can’t define a measure here, as we did previously, as neither of the two possible states guarantee termination.

**Definition** \(\text{wait\text{-}for\text{-}heads} :: \text{coin prog}\)

where

\[ \text{wait\text{-}for\text{-}heads} = \text{do} \ (\text{op} \neq \text{Heads}) \rightarrow \text{flip} \ \text{od} \]

Nonetheless, we can show termination.

**Lemma** \(\text{wait\text{-}for\text{-}heads\text{-}term}\):

\[ \lambda s. \ 1 \vdash wp \ \text{wait\text{-}for\text{-}heads} \ (\lambda s. \ 1) \]

(proof)
2.3 The Monty Hall Problem

We now tackle a more substantial example, allowing us to demonstrate the tools for compositional reasoning and the use of invariants in non-recursive programs. Our example is the well-known Monty Hall puzzle in statistical inference [Selvin, 1975].

The setting is a game show: There is a prize hidden behind one of three doors, and the contestant is invited to choose one. Once the guess is made, the host than opens one of the remaining two doors, revealing a goat and showing that the prize is elsewhere. The contestant is then given the choice of switching their guess to the other unopened door, or sticking to their first guess.

The puzzle is whether the contestant is better off switching or staying put; or indeed whether it makes a difference at all. Most people’s intuition suggests that it make no difference, whereas in fact, switching raises the chance of success from $1/3$ to $2/3$.

2.3.1 The State Space

The game state consists of the prize location, the guess, and the clue (the door the host opens). These are not constrained a priori to the range $\{1, 2, 3\}$, but are simply natural numbers: We instead show that this is in fact an invariant.

```plaintext
record game =
  prize :: nat
  guess :: nat
  clue :: nat
```

The victory condition: The player wins if they have guessed the correct door, when the game ends.

```plaintext
definition player-wins :: game \rightarrow bool
where player-wins g \equiv guess g = prize g
```

Invariants

We prove explicitly that only valid doors are ever chosen.

```plaintext
definition inv-prize :: game \rightarrow bool
where inv-prize g \equiv prize g \in \{1,2,3\}

definition inv-clue :: game \rightarrow bool
where inv-clue g \equiv clue g \in \{1,2,3\}

definition inv-guess :: game \rightarrow bool
where inv-guess g \equiv guess g \in \{1,2,3\}
```
2.3.2 The Game

Hide the prize behind door $D$.

definition hide-behind :: nat $\Rightarrow$ game prog
where hide-behind $D \equiv$ Apply (prize-update ($\lambda x. D$))

Choose door $D$.

definition guess-behind :: nat $\Rightarrow$ game prog
where guess-behind $D \equiv$ Apply (guess-update ($\lambda x. D$))

Open door $D$ and reveal what’s behind.

definition open-door :: nat $\Rightarrow$ game prog
where open-door $D \equiv$ Apply (clue-update ($\lambda x. D$))

Hide the prize behind door 1, 2 or 3, demonically i.e. according to any probability distribution (or none).

definition hide-prize :: game prog
where hide-prize $\equiv$ hide-behind 1 $\sqcap$ hide-behind 2 $\sqcap$ hide-behind 3

Guess uniformly at random.

definition make-guess :: game prog
where make-guess $\equiv$ guess-behind 1 ($\lambda s. 1/3$) $\oplus$ guess-behind 2 ($\lambda s. 1/2$) $\oplus$ guess-behind 3

Open one of the two doors that doesn’t hide the prize.

definition reveal :: game prog
where reveal $\equiv$ $\sqcap$ $\exists d \in (\lambda s. \{1,2,3\} - \{prize s, guess s\}).$ open-door $d$

Switch your guess to the other unopened door.

definition switch-guess :: game prog
where switch-guess $\equiv$ $\sqcap$ $\exists d \in (\lambda s. \{1,2,3\} - \{clue s, guess s\}).$ guess-behind $d$

The complete game, either with or without switching guesses.

definition monty :: bool $\Rightarrow$ game prog
where
  monty switch $\equiv$ hide-prize $; ;$
  make-guess $; ;$
  reveal $; ;$
  (if switch then switch-guess else Skip)

2.3.3 A Brute Force Solution

For sufficiently simple programs, we can calculate the exact weakest pre-expectation by unfolding.

lemma eval-win[simp];
  $p = g \Rightarrow \langle \text{player-wins} \rangle (s[p, \text{prize} := p, \text{guess} := g, \text{clue} := c]) = 1$
CHAPTER 2. INTRODUCTION TO PGCL

\langle \text{proof} \rangle

\textbf{lemma} \text{eval-loss[simp]}: \\
\ p \neq g \implies \text{«player-wins»}(s\|\,\text{prize} := p, \text{guess} := g, \text{clue} := c \|) = 0 \\
\langle \text{proof} \rangle

If they stick to their guns, the player wins with \( p = \frac{1}{3} \).

\textbf{lemma} \text{wp-monty-noswitch}: \\
\ (\lambda s. \frac{1}{3}) = \text{wp} (\text{monty False}) \text{«player-wins»} \\
\langle \text{proof} \rangle

\textbf{lemma} \text{swap-upd}: \\
\ s\| \text{prize} := p, \text{clue} := c, \text{guess} := g \| = \\
\ s\| \text{prize} := p, \text{guess} := g, \text{clue} := c \| \\
\langle \text{proof} \rangle

If they switch, they win with \( p = \frac{2}{3} \). Brute force here takes longer, but is still feasible. On larger programs, this will rapidly become impossible, as the size of the terms (generally) grows exponentially with the length of the program.

\textbf{lemma} \text{wp-monty-switch-bruteforce}: \\
\ (\lambda s. \frac{2}{3}) = \text{wp} (\text{monty True}) \text{«player-wins»} \\
\langle \text{proof} \rangle

2.3.4 A Modular Approach

We can solve the problem more efficiently, at the cost of a little more user effort, by breaking up the problem and annotating each step of the game separately. While this is not strictly necessary for this program, it will scale to larger examples, as the work in annotation only increases linearly with the length of the program.

\textbf{Healthiness}

We first establish healthiness for each step. This follows straightforwardly by applying the supplied rulesets.

\textbf{lemma} \text{wd-hide-prize}: \\
\ well-def hide-prize \\
\langle \text{proof} \rangle

\textbf{lemma} \text{wd-make-guess}: \\
\ well-def make-guess \\
\langle \text{proof} \rangle

\textbf{lemma} \text{wd-reveal}: \\
\ well-def reveal \\
\langle \text{proof} \rangle
2.3. THE MONTY HALL PROBLEM

lemma wd-switch-guess:
  well-def switch-guess
 ⟨proof⟩

lemmas monty-healthy =
  wd-switch-guess wd-reveal wd-make-guess wd-hide-prize

Annotations

We now annotate each step individually, and then combine them to produce
an annotation for the entire program.

hide-prize chooses a valid door.

lemma wp-hide-prize:
  (λs. 1) ⊢ wp hide-prize «inv-prize»
 ⟨proof⟩

Given the prize invariant, make-guess chooses a valid door, and guesses
incorrectly with probability at least 2/3.

lemma wp-make-guess:
  (λs. 2/3 * «λg. inv-prize g» s) ⊢
  wp make-guess «λg. guess g ≠ prize g ∧ inv-prize g ∧ inv-guess g»
 ⟨proof⟩

lemma last-one:
  assumes a ≠ b and a ∈ {1::nat,2,3} and b ∈ {1,2,3}
  shows ∃!c. {1,2,3} − {b,a} = {c}
 ⟨proof⟩

Given the composed invariants, and an incorrect guess, reveal will give a
cue that is neither the prize, nor the guess.

lemma wp-reveal:
  «λg. guess g ≠ prize g ∧ inv-prize g ∧ inv-guess g» ⊢
  wp reveal «λg. guess g ≠ prize g ∧
  clue g ≠ prize g ∧
  clue g ≠ guess g ∧
  inv-prize g ∧ inv-guess g ∧ inv-clue g»
 (is ?X ⊬ wp reveal ?Y)
 ⟨proof⟩

Showing that the three doors are all district is a largeish first-order problem,
for which sledgehammer gives us a reasonable script.

lemma distinct-game:
  [ guess g ≠ prize g; clue g ≠ prize g; clue g ≠ guess g;
    inv-prize g; inv-guess g; inv-clue g ] →
  {1, 2, 3} = {guess g, prize g, clue g}
 ⟨proof⟩
Given the invariants, switching from the wrong guess gives the right one.

**lemma** wp-switch-guess:
\[
\lambda g. \text{guess } g \neq \text{prize } g \land \text{clue } g \neq \text{prize } g \land \text{clue } g \neq \text{guess } g \land \\
\text{inv-prize } g \land \text{inv-guess } g \land \text{inv-clue } g \vdash \\
\text{wp switch-guess } \llbracket \text{player-wins} \rrbracket
\]
 ⟨proof⟩

Given componentwise specifications, we can glue them together with calculational reasoning to get our result.

**lemma** wp-monty-switch-modular:
\[
(\lambda s. \frac{2}{3}) \vdash wp (\text{monty True}) \llbracket \text{player-wins} \rrbracket
\]
 ⟨proof⟩

**Using the VCG**

**lemmas** scaled-hide = wp-scale[\text{OF wp-hide-prize, simplified}]
**declare** scaled-hide[\text{pwp}] wp-make-guess[pwp] wp-reveal[pwp] wp-switch-guess[pwp]
**declare** wd-hide-prize[\text{wd}] wd-make-guess[\text{wd}] wd-reveal[\text{wd}] wd-switch-guess[\text{wd}]

Alternatively, the VCG will get this using the same annotations.

**lemma** wp-monty-switch-vcg:
\[
(\lambda s. \frac{2}{3}) \vdash wp (\text{monty True}) \llbracket \text{player-wins} \rrbracket
\]
 ⟨proof⟩

end
Chapter 3

Semantic Structures

3.1 Expectations

declaration Expectations imports Misc begin type-synonym ‘s expect = ‘s ⇒ real

Expectations are a real-valued generalisation of boolean predicates: An expectation on state ‘s is a function ‘s ⇒ real. A predicate P on ‘s is embedded as an expectation by mapping True to 1 and False to 0. Under this embedding, implication becomes comparison, as the truth tables demonstrate:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>a → b</th>
<th>x</th>
<th>y</th>
<th>x ≤ y</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>0</td>
<td>0</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>1</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>1</td>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>1</td>
<td>1</td>
<td>T</td>
</tr>
</tbody>
</table>

For probabilistic automata, an expectation gives the current expected value of some expression, if it were to be evaluated in the final state. For example, consider the automaton of Figure 3.1, with transition probabilities affixed to edges. Let \( P_b = 2.0 \) and \( P_c = 3.0 \). Both states b and c are final (accepting) states, and thus the ‘final expected value’ of \( P \) in state b is 2.0 and in state c.

Figure 3.1: A probabilistic automaton

13
The expected value from state $a$ is the weighted sum of these, or $0.7 \times 2.0 + 0.3 \times 3.0 = 2.3$.

All expectations must be non-negative and bounded i.e. $\forall s. 0 \leq P \; s$ and $\exists b. \forall s. P \; s \leq b$. Note that although every expectation must have a bound, there is no bound on all expectations; In particular, the following series has no global bound, although each element is clearly bounded:

$$P_1 = \lambda s. i \text{ where } i \in \mathbb{N}$$

### 3.1.1 Bounded Functions

**definition** `bounded-by` :: $\mathbb{R} \Rightarrow (\forall a \Rightarrow \mathbb{R}) \Rightarrow \mathbb{B}$

**where**

`bounded-by b P ≡ ∀ x. P x ≤ b`

By instantiating the classical reasoner, both establishing and appealing to boundedness is largely automatic.

**lemma** `bounded-byI`[

`intro`]:

$$[ \forall x. P x \leq b ] \implies \text{bounded-by } b \; P$$

```proof
```

**lemma** `bounded-byI2`[

`intro`]:

$$P \leq (\lambda s. b) \implies \text{bounded-by } b \; P$$

```proof
```

**lemma** `bounded-byD`[

`dest`]:

`bounded-by b P` $\implies$ $P x \leq b$

```proof
```

**lemma** `bounded-byD2`[

`dest`]:

`bounded-by b P` $\implies$ $P \leq (\lambda s. b)$

```proof
```

A function is bounded if there exists at least one upper bound on it.

**definition** `bounded` :: $(\forall a \Rightarrow \mathbb{R}) \Rightarrow \mathbb{B}$

**where**

`bounded P ≡ (\exists b. \text{bounded-by } b \; P)`

In the reals, if there exists any upper bound, then there must exist a least upper bound.

**definition** `bound-of` :: $(\forall a \Rightarrow \mathbb{R}) \Rightarrow \mathbb{R}$

**where**

`bound-of P ≡ \text{Sup} \; (P \cdot \text{UNIV})`

**lemma** `bounded-bdd-above`[

`intro`]:

`assumes bP: bounded P`

`shows bdd-above (range P)`

```proof
```

The least upper bound has the usual properties:
3.1. EXPECTATIONS

lemma bound-of-least[intro]:
  assumes bP: bounded-by b P
  shows bound-of P ≤ b
  ⟨proof⟩

lemma bounded-by-bound-of[intro]:
  fixes P::'a ⇒ real
  assumes bP: bounded P
  shows bounded-by (bound-of P) P
  ⟨proof⟩

lemma bound-of-greater[intro]:
  bounded P =⇒ P x ≤ bound-of P
  ⟨proof⟩

lemma bounded-by-mono:
  [ bounded-by a P; a ≤ b ] =⇒ bounded-by b P
  ⟨proof⟩

lemma bounded-by-imp-bounded[intro]:
  bounded-by b P =⇒ bounded P
  ⟨proof⟩

This is occasionally easier to apply:

lemma bounded-by-bound-of-alt:
  [ bounded P; bound-of P = a ] =⇒ bounded-by a P
  ⟨proof⟩

lemma bounded-const[simp]:
  bounded (λx. c)
  ⟨proof⟩

lemma bounded-by-const[intro]:
  c ≤ b =⇒ bounded-by b (λx. c)
  ⟨proof⟩

lemma bounded-by-mono-alt[intro]:
  [ bounded-by b Q; P ≤ Q ] =⇒ bounded-by b P
  ⟨proof⟩

lemma bound-of-const[simp, intro]:
  bound-of (λx. c) = (c::real)
  ⟨proof⟩

lemma bound-of-leI:
  assumes \( \forall x. P x ≤ (c::real) \)
  shows bound-of P ≤ c
  ⟨proof⟩
**CHAPTER 3. SEMANTIC STRUCTURES**

**Lemma** bound-of-mono[intro]:

\[ P \leq Q; \text{bounded } P; \text{bounded } Q \implies \text{bound-of } P \leq \text{bound-of } Q \]

\( \langle \text{proof} \rangle \)

**Lemma** bounded-by-o[intro, simp]:

\( \forall b. \text{bounded-by } b P \implies \text{bounded-by } b (P \circ f) \)

\( \langle \text{proof} \rangle \)

**Lemma** le-bound-of[intro]:

\( \forall x. \text{bounded } f \implies f x \leq \text{bound-of } f \)

\( \langle \text{proof} \rangle \)

### 3.1.2 Non-Negative Functions.

The definitions for non-negative functions are analogous to those for bounded functions.

**Definition**

\( \text{nneq} :: (\forall a \Rightarrow b : (\text{zero, order})) \Rightarrow \text{bool} \)

**Where**

\( \text{nneq } P \leftarrow \left( \forall x. 0 \leq P x \right) \)

**Lemma** nneqI[intro]:

\[ \forall x. 0 \leq P x \implies \text{nneq } P \]

\( \langle \text{proof} \rangle \)

**Lemma** nneqI2[intro]:

\( (\lambda s. 0) \leq P \implies \text{nneq } P \)

\( \langle \text{proof} \rangle \)

**Lemma** nneqD[dest]:

\( \text{nneq } P \implies 0 \leq P x \)

\( \langle \text{proof} \rangle \)

**Lemma** nneqD2[dest]:

\( \text{nneq } P \implies (\lambda s. 0) \leq P \)

\( \langle \text{proof} \rangle \)

**Lemma** nneq-bdd-below[intro]:

\( \text{nneq } P \implies \text{bdd-below } (\text{range } P) \)

\( \langle \text{proof} \rangle \)

**Lemma** nneq-const[iff]:

\( \text{nneq } (\lambda x. c) \leftarrow \ 0 \leq c \)

\( \langle \text{proof} \rangle \)

**Lemma** nneq-o[intro, simp]:

\( \text{nneq } P \implies \text{nneq } (P \circ f) \)

\( \langle \text{proof} \rangle \)
3.1. EXPECTATIONS

**lemma** nneg-bound-nneg[intro]:

\[ \text{bounded } P; \ nneg \ P \implies 0 \leq \text{bound-of } P \]

(proof)

**lemma** nneg-bounded-by-nneg[dest]:

\[ \text{bounded-by } b \ P; \ nneg \ P \implies 0 \leq (b::real) \]

(proof)

**lemma** bounded-by-nneg[dest]:

fixes \( P :: \text{'s} \Rightarrow \text{real} \)

shows \[ \text{bounded-by } b \ P; \ nneg \ P \implies 0 \leq b \]

(proof)

3.1.3 Sound Expectations

**definition** sound :: (\text{'s} \Rightarrow \text{real}) \Rightarrow \text{bool}

where sound \( P \equiv \text{bounded } P \land \text{nneg } P \)

Combining nneg and Expectations.bounded, we have sound expectations. We
set up the classical reasoner and the simplifier, such that showing soundess,
or deriving a simple consequence (e.g. \( \text{sound } P \implies 0 \leq P \text{ s} \)) will usually
follow by blast, force or simp.

**lemma** soundI:

\[ \text{bounded } P; \ nneg \ P \implies \text{sound } P \]

(proof)

**lemma** soundI2[intro]:

\[ \text{bounded-by } b \ P; \ nneg \ P \implies \text{sound } P \]

(proof)

**lemma** sound-bounded[dest]:

\( \text{sound } P \implies \text{bounded } P \)

(proof)

**lemma** sound-nneg[dest]:

\( \text{sound } P \implies \text{nneg } P \)

(proof)

**lemma** bound-of-sound[intro]:

assumes \( sP: \text{sound } P \)

shows \( 0 \leq \text{bound-of } P \)

(proof)

This proof demonstrates the use of the classical reasoner (specifically blast),
to both introduce and eliminate soundness terms.

**lemma** sound-sum[simp,intro]:

assumes \( sP: \text{sound } P \ \text{and} \ sQ: \text{sound } Q \)

shows \( \text{sound } (\lambda s. \ P \ s + Q \ s) \)

(proof)
\textbf{lemma} mult-sound:
\begin{enumerate}
\item \textbf{assumes} \(sP\): sound \(P\) \textbf{and} \(sQ\): sound \(Q\)
\item \textbf{shows} sound \((\lambda s. P s \ast Q s)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} div-sound:
\begin{enumerate}
\item \textbf{assumes} \(sP\): sound \(P\) \textbf{and} \(cpos: 0 < c\)
\item \textbf{shows} sound \((\lambda s. P s / c)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} tminus-sound:
\begin{enumerate}
\item \textbf{assumes} \(sP\): sound \(P\) \textbf{and} \(nnc: 0 \leq c\)
\item \textbf{shows} sound \((\lambda s. P s \ominus c)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} const-sound:
\begin{enumerate}
\item \(0 \leq c \implies\) sound \((\lambda s. c)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} sound-o\{intro,simp\}:
\begin{enumerate}
\item sound \(P\) \implies sound \((P o f)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} sc-bounded-by\{intro,simp\}:
\begin{enumerate}
\item \([\text{sound } P; 0 \leq c]\) \implies bounded-by \((c \cdot \text{bound-of } P) (\lambda x. c \cdot P x)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} sc-bounded\{intro,simp\}:
\begin{enumerate}
\item \textbf{assumes} \(sP\): sound \(P\) \textbf{and} \(pos: 0 \leq c\)
\item \textbf{shows} bounded \((\lambda x. c \cdot P x)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} sc-bound\{simp\}:
\begin{enumerate}
\item \textbf{assumes} \(sP\): sound \(P\)
\item \textbf{and} \(cnn: 0 \leq c\)
\item \textbf{shows} \(c \cdot \text{bound-of } P = \text{bound-of } (\lambda x. c \cdot P x)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} sc-sound:
\begin{enumerate}
\item \([\text{sound } P; 0 \leq c]\) \implies sound \((\lambda s. c \cdot P s)\)
\end{enumerate}
\textbf{⟨proof⟩}

\textbf{lemma} bounded-by-mult:
\begin{enumerate}
\item \textbf{assumes} \(sP\): sound \(P\) \textbf{and} \(bP\): bounded-by \(a P\)
\item \textbf{and} \(sQ\): sound \(Q\) \textbf{and} \(bQ\): bounded-by \(b Q\)
\item \textbf{shows} bounded-by \((a \cdot b) (\lambda s. P s \ast Q s)\)
\end{enumerate}
\textbf{⟨proof⟩}
3.1. EXPECTATIONS

lemma bounded-by-add:
  fixes P::'s ⇒ real and Q
  assumes bP: bounded-by a P
         and bQ: bounded-by b Q
  shows bounded-by (a + b) (λs. P s + Q s)
⟨proof⟩

lemma sound-unit[intro!,simp]:
  sound (λs. 1)
⟨proof⟩

lemma unit-mult[intro]:
  assumes sP: sound P and bP: bounded-by 1 P
         and sQ: sound Q and bQ: bounded-by 1 Q
  shows bounded-by 1 (λs. P s * Q s)
⟨proof⟩

lemma setsum-sound:
  assumes sP: ∀x∈S. sound (P x)
  shows sound (λs. ∑x∈S. P x s)
⟨proof⟩

3.1.4 Unitary expectations

A unitary expectation is a sound expectation that is additionally bounded by one. This is the domain on which the liberal (partial correctness) semantics operates.

definition unitary :: 's expect ⇒ bool
where unitary P ←→ sound P ∧ bounded-by 1 P

lemma unitaryI[intro]:
  [ sound P; bounded-by 1 P ] ⇒ unitary P
⟨proof⟩

lemma unitaryI2:
  [ nneg P; bounded-by 1 P ] ⇒ unitary P
⟨proof⟩

lemma unitary-sound[dest]:
  unitary P ⇒ sound P
⟨proof⟩

lemma unitary-bound[dest]:
  unitary P ⇒ bounded-by 1 P
⟨proof⟩

3.1.5 Standard Expectations

definition
embed-bool :: (‘s ⇒ bool) ⇒ ‘s ⇒ real (« - » 1000)

where

« P » ≡ (λs. if P s then 1 else 0)

Standard expectations are the embeddings of boolean predicates, mapping False to 0 and True to 1. We write « P » rather than [P] (the syntax employed by McIver and Morgan [2004]) for boolean embedding to avoid clashing with the HOL syntax for lists.

lemma embed-bool-nneg[simp,intro]:
    nneg « P »
    ⟨proof⟩

lemma embed-bool-bounded-by-1[simp,intro]:
    bounded-by 1 « P »
    ⟨proof⟩

lemma embed-bool-bounded[simp,intro]:
    bounded « P »
    ⟨proof⟩

Standard expectations have a number of convenient properties, which mostly follow from boolean algebra.

lemma embed-bool-idem:
    « P » s * « P » s = « P » s
    ⟨proof⟩

lemma eval-embed-true[simp]:
    P s ⇒ « P » s = 1
    ⟨proof⟩

lemma eval-embed-false[simp]:
    ¬P s ⇒ « P » s = 0
    ⟨proof⟩

lemma embed-le-0[simp,intro]:
    0 ≤ « G » s
    ⟨proof⟩

lemma embed-le-1[simp,intro]:
    « G » s ≤ 1
    ⟨proof⟩

lemma embed-le-1-alt[simp,intro]:
    0 ≤ 1 - « G » s
    ⟨proof⟩

lemma expect-1-I:
    P x ⇒ 1 ≤ « P » x
    ⟨proof⟩
3.1. EXPECTATIONS

**lemma** standard-sound[intro,simp]:

\[ \text{sound } \langle P \rangle \]

(proof)

**lemma** embed-o[simp]:

\[ \langle P \rangle \circ f = \langle P \circ f \rangle \]

(proof)

Negating a predicate has the expected effect in its embedding as an expectation:

**definition** negate :: (′s ⇒ bool) ⇒ ′s ⇒ bool (N)

where

\[ \text{negate } P = (\lambda s. \neg P s) \]

**lemma** negateI:

\[ \neg P s \implies N P s \]

(proof)

**lemma** embed-split:

\[ f s = \langle P \rangle s \ast f s + \langle N P \rangle s \ast f s \]

(proof)

**lemma** negate-embed:

\[ \langle N P \rangle s = 1 - \langle P \rangle s \]

(proof)

**lemma** eval-nembed-true[simp]:

\[ P s \implies \langle N P \rangle s = 0 \]

(proof)

**lemma** eval-nembed-false[simp]:

\[ \neg P s \implies \langle N P \rangle s = 1 \]

(proof)

**lemma** negate-Not[simp]:

\[ \text{N Not} = (\lambda x. x) \]

(proof)

**lemma** negate-negate[simp]:

\[ N (N P) = P \]

(proof)

**lemma** embed-bool-cancel:

\[ \langle G \rangle s \ast \langle N G \rangle s = 0 \]

(proof)
3.1.6 Entailment

Entailment on expectations is a generalisation of that on predicates, and is defined by pointwise comparison:

**abbreviation** \( \text{entails} :: (s \Rightarrow \text{real}) \Rightarrow (s \Rightarrow \text{real}) \Rightarrow \text{bool} (\cdot \vdash \cdot 50) \)

**where** \( P \vdash Q \equiv P \leq Q \)

**lemma** \( \text{entailsI}[\text{intro}]: \)

\[
[\forall s. \ P s \leq Q s] \implies P \vdash Q
\]

(\text{proof})

**lemma** \( \text{entailsD}[\text{dest}]: \)

\[\vdash P \vdash Q \implies P s \leq Q s\]

(\text{proof})

**lemma** \( \text{eq-entails}[\text{intro}]: \)

\[P = Q \implies P \vdash Q\]

(\text{proof})

**lemma** \( \text{entails-trans}[\text{trans}]: \)

\[
[ \vdash P; Q \vdash R ] \implies P \vdash R
\]

(\text{proof})

For standard expectations, both notions of entailment coincide. This result justifies the above claim that our definition generalises predicate entailment:

**lemma** \( \text{implies-entails}: \)

\[
[ \forall s. \ P s \Rightarrow Q s ] \implies \{P\} \vdash \{Q\}
\]

(\text{proof})

**lemma** \( \text{entails-implies}: \)

\[
\forall s. \ \{P\} \vdash \{Q\}; \ P s \implies Q s
\]

(\text{proof})

3.1.7 Expectation Conjunction

**definition** \( \text{pconj} :: \text{real} \Rightarrow \text{real} \Rightarrow \text{real} (\text{infixl} \ & 71) \)

**where** \( p \ . q \equiv p + q \ominus 1 \)

**definition** \( \text{exp-conj} :: (s \Rightarrow \text{real}) \Rightarrow (s \Rightarrow \text{real}) \Rightarrow (s \Rightarrow \text{real}) (\text{infixl} \& \& 71) \)

**where** \( a \ & \& b \equiv \lambda s. \ (a \ s \ & \& b \ s) \)

Expectation conjunction likewise generalises (boolean) predicate conjunction. We show that the expected properties are preserved, and instantiate both the classical reasoner, and the simplifier (in the case of associativity and commutativity).
3.1. EXPECTATIONS

\textbf{Lemma} \texttt{pconj-lzero[\texttt{intro,simp}]}:
\[
b \leq 1 \implies 0 \land b = 0
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-rzero[\texttt{intro,simp}]}:
\[
b \leq 1 \implies b \land 0 = 0
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-lone[\texttt{intro,simp}]}:
\[
0 \leq b \implies 1 \land b = b
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-rone[\texttt{intro,simp}]}:
\[
0 \leq b \implies b \land 1 = b
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-bconj}:
\[
\langle a \rangle s \land \langle b \rangle s = \langle \lambda s. a s \land b s \rangle s
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-comm[\texttt{ac-simps}]}:
\[
a \land b = b \land a
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-assoc}:
\[
\{ \theta \leq a; a \leq 1; \theta \leq b; b \leq 1; \theta \leq c; c \leq 1 \} \implies
a \land (b \land c) = (a \land b) \land c
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-mono}:
\[
\{ a \leq b; c \leq d \} \implies a \land c \leq b \land d
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-nneg[\texttt{intro,simp}]}:
\[
0 \leq a \land b
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{min-pconj}:
\[
\langle \min a b \rangle \land \langle \min c d \rangle \leq \min (a \land c) (b \land d)
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-less-one[\texttt{simp}]}:
\[
a + b < 1 \implies a \land b = 0
\]
⟨\texttt{proof}⟩

\textbf{Lemma} \texttt{pconj-ge-one[\texttt{simp}]}:
\[
1 \leq a + b \implies a \land b = a + b - 1
\]
⟨\texttt{proof}⟩
3.1.8 Rules Involving Conjunction.

**lemma** exp-conj-mono-left:
\[ P \vdash Q \Rightarrow P \& R \vdash Q \& R \]
\langle proof \rangle

**lemma** exp-conj-mono-right:
\[ Q \vdash R \Rightarrow P \& Q \vdash P \& R \]
\langle proof \rangle

**lemma** exp-conj-comm[ac-simps]:
\[ a \& b = b \& a \]
\langle proof \rangle

**lemma** exp-conj-bounded-by[intro,simp]:
assumes \[ bP: \text{bounded-by } 1 P \]
and \[ bQ: \text{bounded-by } 1 Q \]
shows \[ \text{bounded-by } 1 (P \& Q) \]
\langle proof \rangle

**lemma** exp-conj-o-distrib[simp]:
\[ (P \& Q) \circ f = (P \circ f) \& (Q \circ f) \]
\langle proof \rangle

**lemma** exp-conj-assoc:
assumes unitary P and unitary Q and unitary R
shows \[ P \& (Q \& R) = (P \& Q) \& R \]
\langle proof \rangle

**lemma** exp-conj-top-left[simp]:
\[ \text{sound } P \Rightarrow \lambda s. \text{True} \& P = P \]
\langle proof \rangle

**lemma** exp-conj-top-right[simp]:
\[ \text{sound } P \Rightarrow P \& \lambda s. \text{True} = P \]
\langle proof \rangle

**lemma** exp-conj-idem[simp]:
\[ P \& P = P \]
\langle proof \rangle

**lemma** exp-conj-nneg[intro,simp]:
\[ (\lambda s. 0) \leq P \& Q \]
\langle proof \rangle
3.1. EXPECTATIONS

**lemma** \texttt{exp-conj-sound}[\texttt{intro,simp}]:
\begin{itemize}
\item \texttt{assumes} \texttt{s-P}: \text{sound} \; P
\item \text{and} \; \texttt{s-Q}: \text{sound} \; Q
\item \texttt{shows} \text{sound} \; (P \&\& Q)
\end{itemize}
\begin{proof}
\end{proof}

**lemma** \texttt{exp-conj-rzero}[\texttt{simp}]:
\begin{itemize}
\item \text{bounded-by} 1 \; P \implies P \&\& (\lambda s, 0) = (\lambda s, 0)
\end{itemize}
\begin{proof}
\end{proof}

**lemma** \texttt{exp-conj-1-right}[\texttt{simp}]:
\begin{itemize}
\item \texttt{assumes} \texttt{nn}: \text{nneg} \; A
\item \texttt{shows} \; A \&\& (\lambda s, 1) = A
\end{itemize}
\begin{proof}
\end{proof}

**lemma** \texttt{exp-conj-std-split}:
\begin{itemize}
\item «\lambda s. P s \land Q s» = «P» \&\& «Q»
\end{itemize}
\begin{proof}
\end{proof}

3.1.9 Rules Involving Entailment and Conjunction Together

Meta-conjunction distributes over expectation entailment, becoming expectation conjunction:

**lemma** \texttt{entails-frame}:
\begin{itemize}
\item \texttt{assumes} \texttt{ePR}: \; P \vdash \vdash R
\item \text{and} \; \texttt{eQS}: \; Q \vdash \vdash S
\item \texttt{shows} \; P \&\& Q \vdash \vdash R \&\& S
\end{itemize}
\begin{proof}
\end{proof}

This rule allows something very much akin to a case distinction on the pre-expectation.

**lemma** \texttt{pentails-cases}:
\begin{itemize}
\item \texttt{assumes} \texttt{PQe}: \bigwedge x. P x \vdash Q x
\item \text{and} \; \texttt{exhaust}: \bigwedge s. \exists x. P (x s) s = 1
\item \text{and} \; \texttt{framed}: \bigwedge x. P x \&\& R \vdash Q x \&\& S
\item \text{and} \; \texttt{sR}: \; \text{sound} \; R \text{ and} \; \texttt{sS}: \; \text{sound} \; S
\item \text{and} \; \texttt{bQ}: \; \bigwedge x. \; \text{bounded-by} \; 1 \; (Q x)
\item \texttt{shows} \; R \vdash \vdash S
\end{itemize}
\begin{proof}
\end{proof}

**lemma** \texttt{unitary-bot}[\texttt{iff}]:
\begin{itemize}
\item \texttt{unitary} \; (\lambda s, 0::\text{real})
\end{itemize}
\begin{proof}
\end{proof}

**lemma** \texttt{unitary-top}[\texttt{iff}]:
\begin{itemize}
\item \texttt{unitary} \; (\lambda s, 1::\text{real})
\end{itemize}
\begin{proof}
\end{proof}
lemma unitary-embed[iff]:
  \( \text{unitary \ « P »} \)
  \( \langle \text{proof} \rangle \)

lemma unitary-const[iff]:
\[ 0 \leq c; c \leq 1 \] \( \implies \) \( \text{unitary (\lambda s. c)} \)
\( \langle \text{proof} \rangle \)

lemma unitary-mult:
  \( \text{assumes uA: unitary A and uB: unitary B} \)
  \( \text{shows unitary (\lambda s. A \times B s)} \)
\( \langle \text{proof} \rangle \)

lemma exp-conj-unitary:
\[ \text{[ unitary P; unitary Q ]} \implies \text{unitary (P \&\& Q)} \]
\( \langle \text{proof} \rangle \)

lemma unitary-comp[simp]:
  \( \text{unitary P} \implies \text{unitary (P o f)} \)
\( \langle \text{proof} \rangle \)

lemmas unitary-intros =
  \( \text{unitary-bot} \) \( \text{unitary-top} \) \( \text{unitary-embed} \) \( \text{unitary-mult} \) \( \text{exp-conj-unitary} \)
  \( \text{unitary-comp} \) \( \text{unitary-const} \)

lemmas sound-intros =
  \( \text{mult-sound} \) \( \text{div-sound} \) \( \text{const-sound} \) \( \text{sound-o} \) \( \text{sound-sum} \)
  \( \text{tminus-sound} \) \( \text{sc-sound} \) \( \text{exp-conj-sound} \) \( \text{setsam-sound} \)

end

3.2 Expectation Transformers

theory Transformers imports Expectations begin
  \text{type-synonym} \ 's trans = \ 's expect \Rightarrow \ 's expect

Transformers are functions from expectations to expectations i.e. \( (\ 's \Rightarrow \text{real}) \Rightarrow \ 's \Rightarrow \text{real} \).
The set of \textit{healthy} transformers is the universe into which we place our semantic interpretation of pGCL programs. In its standard presentation, the healthiness condition for pGCL programs is \textit{sublinearity}, for demonic programs, and \textit{superlinearity} for angelic programs. We extract a minimal core property, consisting of monotonicity, feasibility and scaling to form our healthiness property, which holds across all programs. The additional components of sublinearity are broken out separately, and shown later. The two reasons for this are firstly to avoid the effort of establishing sub-(super-)linearity globally, and to allow us to define primitives whose sublinearity,
and indeed healthiness, depend on context.

Consider again the automaton of Figure 3.1. Here, the effect of executing the automaton from its initial state (a) until it reaches some final state (b or c) is to transform the expectation on final states ($P$), into one on initial states, giving the expected value of the function on termination. Here, the transformation is linear: $P_{\text{prior}}(a) = 0.7 \cdot P_{\text{post}}(b) + 0.3 \cdot P_{\text{post}}(c)$, but this need not be the case.

Consider the automaton of Figure 3.2. Here, we have extended that of Figure 3.1 with two additional states, d and e, and a pair of silent (unlabelled) transitions. From the initial state, e, this automaton is free to transition either to the original starting state (a), and thence behave exactly as the previous automaton did, or to d, which has the same set of available transitions, now with different probabilities. Where previously we could state that the automaton would terminate in state b with probability 0.7 (and in c with probability 0.3), this now depends on the outcome of the nondeterministic transition from e to either a or d. The most we can now say is that we must reach b with probability at least 0.5 (the minimum from either a or d) and c with at least probability 0.3. Note that these probabilities do not sum to one (although the sum will still always be less than one). The associated expectation transformer is now sub-linear: $P_{\text{prior}}(e) = 0.5 \cdot P_{\text{post}}(b) + 0.3 \cdot P_{\text{post}}(c)$.

Finally, Figure 3.3 shows the other way in which strict sublinearity arises: divergence. This automaton transitions with probability 0.5 to state d, from which it never escapes. Once there, the probability of reaching any terminating state is zero, and thus the probability of terminating from the initial state (c) is no higher than 0.5. If it instead takes the edge to state a, we again see a self loop, and thus in theory an infinite trace. In this case, however, every time the automaton reaches state a, with probability $0.5 + 0.3 = 0.8$, it transitions to a terminating state. An infinite trace of transitions $a \rightarrow a \rightarrow \ldots$ thus has probability 0, and the automaton

![Figure 3.2: A nondeterministic-probabilistic automaton.](image-url)
terminates with probability 1. We formalise such probabilistic termination arguments in Section 4.11.

Having reached a, the automaton will proceed to b with probability $0.5 \times \frac{1}{0.5 + 0.3} = 0.625$, and to c with probability 0.375. As a is in turn reached half the time, the final probability of ending in b is 0.3125, and in c, 0.1875, which sum to only 0.5. The remaining probability is that the automaton diverges via d. We view nondeterminism and divergence demonically: we take the least probability of reaching a given final state, and use it to calculate the expectation. Thus for this automaton, $P_{\text{ prior}}(c) = 0.3125 \times P_{\text{ post}}(b) + 0.1875 \times P_{\text{ post}}(c)$. The end result is the same as for nondeterminism: a sublinear transformation (the weights sum to less than one).

The two outcomes are thus unified in the semantic interpretation, although as we will establish in Section 4.6, the two have slightly different algebraic properties.

This pattern holds for all pGCL programs: probabilistic choices are always linear, while struct sublinearity is introduced both nondeterminism and divergence.

Healthiness, again, is the combination of three properties: feasibility, monotonicity and scaling. Feasibility requires that a transformer take non-negative expectations to non-negative expectations, and preserve bounds. Thus, starting with an expectation bounded between 0 and some bound, b, after applying any number of feasible transformers, the result will still be bounded between 0 and b. This closure property allows us to treat expectations almost as a complete lattice. Specifically, for any b, the set of expectations bounded by b is a complete lattice $\{ \lambda s.0, \top = (\lambda s.b) \}$, and is closed under the action of feasible transformers, including $\sqcap$ and $\sqcup$, which are themselves feasible. We are thus able to define both least and greatest fixed points on this set, and thus give semantics to recursive programs built from feasible components.
3.2. EXPECTATION TRANSFORMERS

3.2.1 Comparing Transformers

Transformers are compared pointwise, but only on sound expectations. From the preorder so generated, we define equivalence by antisymmetry, giving a partial order.

definition le-trans :: 's trans ⇒ 's trans ⇒ bool
where
le-trans t u ≡ ∀ P. sound P → t P ≤ u P

We also need to define relations restricted to unitary transformers, for the liberal (wlp) semantics.

definition le-utrans :: 's trans ⇒ 's trans ⇒ bool
where
le-utrans t u ←→ (∀ P. unitary P → t P ≤ u P)

lemma le-transI[intro]:
[ [ \forall P. sound P \implies t P \leq u P ] ] \implies le-trans t u
⟨proof⟩

lemma le-utransI[intro]:
[ [ \forall P. unitary P \implies t P \leq u P ] ] \implies le-utrans t u
⟨proof⟩

lemma le-transD[dest]:
[ le-trans t u; sound P ] \implies t P \leq u P
⟨proof⟩

lemma le-utransD[dest]:
[ le-utrans t u; unitary P ] \implies t P \leq u P
⟨proof⟩

lemma le-trans-trans[trans]:
[ le-trans x y; le-trans y z ] \implies le-trans x z
⟨proof⟩

lemma le-utrans-trans[trans]:
[ le-utrans x y; le-utrans y z ] \implies le-utrans x z
⟨proof⟩

lemma le-trans-refl[iff]:
le-trans x x
⟨proof⟩

lemma le-utrans-refl[iff]:
le-utrans x x
⟨proof⟩
**Lemma**: `le-trans-le-utrans[dest]`:

\[ \text{le-trans } t \; u \implies \text{le-utrans } t \; u \]

(proof)

**Definition**

\[ \text{l-trans } :: \; \text{'} s \; \text{trans} \implies \; \text{'} s \; \text{trans} \implies \; \text{bool} \]

**Where**

\[ \text{l-trans } t \; u \iff \text{le-trans } t \; u \land \neg \text{le-trans } u \; t \]

Transformer equivalence is induced by comparison:

**Definition**

\[ \text{equiv-trans } :: \; \text{'} s \; \text{trans} \implies \; \text{'} s \; \text{trans} \implies \; \text{bool} \]

**Where**

\[ \text{equiv-trans } t \; u \iff \text{le-trans } t \; u \land \text{le-trans } u \; t \]

**Definition**

\[ \text{equiv-utrans } :: \; \text{'} s \; \text{trans} \implies \; \text{'} s \; \text{trans} \implies \; \text{bool} \]

**Where**

\[ \text{equiv-utrans } t \; u \iff \text{le-utrans } t \; u \land \text{le-utrans } u \; t \]

**Lemma**: `equiv-transI[intro]`:

\[ \left[ \forall P, \; \text{sound } P \implies t \; P = u \; P \right] \implies \text{equiv-trans } t \; u \]

(proof)

**Lemma**: `equiv-utransI[intro]`:

\[ \left[ \forall P, \; \text{sound } P \implies t \; P = u \; P \right] \implies \text{equiv-utrans } t \; u \]

(proof)

**Lemma**: `equiv-transD[dest]`:

\[ \left[ \text{equiv-trans } t \; u; \; \text{sound } P \right] \implies t \; P = u \; P \]

(proof)

**Lemma**: `equiv-utransD[dest]`:

\[ \left[ \text{equiv-utrans } t \; u; \; \text{unitary } P \right] \implies t \; P = u \; P \]

(proof)

**Lemma**: `equiv-trans-refl[iff]`:

\[ \text{equiv-trans } t \; t \]

(proof)

**Lemma**: `equiv-utrans-refl[iff]`:

\[ \text{equiv-utrans } t \; t \]

(proof)

**Lemma**: `le-trans-antisym`:

\[ \left[ \text{le-trans } x \; y; \; \text{le-trans } y \; x \right] \implies \text{equiv-trans } x \; y \]

(proof)

**Lemma**: `le-utrans-antisym`:
3.2. EXPECTATION TRANSFORMERS

\[ [\text{le-utrans } x \ y; \text{le-utrans } y \ x] \implies \text{equiv-utrans } x \ y \]
⟨proof⟩

**Lemma equiv-trans-comm**[ac-simps]:
\[ \text{equiv-trans } t \ u \longleftrightarrow \text{equiv-trans } u \ t \]
⟨proof⟩

**Lemma equiv-utrans-comm**[ac-simps]:
\[ \text{equiv-utrans } t \ u \leftrightarrow \text{equiv-utrans } u \ t \]
⟨proof⟩

**Lemma equiv-imp-le**[intro]:
\[ \text{equiv-trans } t \ u \implies \text{le-trans } t \ u \]
⟨proof⟩

**Lemma equiv-imp-le-alt**:
\[ \text{equiv-utrans } t \ u \implies \text{le-utrans } t \ u \]
⟨proof⟩

**Lemma equiv-imp-le-alt**:  
\[ \text{equiv-utrans } t \ u \implies \text{le-utrans } t \ u \]
⟨proof⟩

**Lemma le-trans-equiv-rsp**[simp]:
\[ \text{equiv-trans } t \ u \implies \text{le-trans } t \ v \longleftrightarrow \text{le-trans } u \ v \]
⟨proof⟩

**Lemma le-utrans-equiv-rsp**[simp]:
\[ \text{equiv-utrans } t \ u \implies \text{le-utrans } t \ v \longleftrightarrow \text{le-utrans } u \ v \]
⟨proof⟩

**Lemma equiv-trans-le-trans**[trans]:
\[ [\text{equiv-trans } t \ u; \text{le-trans } u \ v] \implies \text{le-trans } t \ v \]
⟨proof⟩

**Lemma equiv-utrans-le-utrans**[trans]:
\[ [\text{equiv-utrans } t \ u; \text{le-utrans } u \ v] \implies \text{le-utrans } t \ v \]
⟨proof⟩

**Lemma le-trans-equiv-rsp-right**[simp]:
\[ \text{equiv-trans } t \ u \implies \text{le-trans } v \ t \longleftrightarrow \text{le-trans } v \ u \]
⟨proof⟩

**Lemma le-utrans-equiv-rsp-right**[simp]:
\[ \text{equiv-utrans } t \ u \implies \text{le-utrans } v \ t \longleftrightarrow \text{le-utrans } v \ u \]
CHAPTER 3. SEMANTIC STRUCTURES

⟨proof⟩

lemma le-trans-equiv-trans [trans]:
\[ \text{le-trans } t \ u; \ \text{equiv-trans } u \ v \] \implies \text{le-trans } t \ v
⟨proof⟩

lemma le-utrans-equiv-utrans [trans]:
\[ \text{le-utrans } t \ u; \ \text{equiv-utrans } u \ v \] \implies \text{le-utrans } t \ v
⟨proof⟩

lemma equiv-trans-trans [trans]:
assumes \( xy \): \text{equiv-trans } x \ y
and \( yz \): \text{equiv-trans } y \ z
shows \text{equiv-trans } x \ z
⟨proof⟩

lemma equiv-utrans-trans [trans]:
assumes \( xy \): \text{equiv-utrans } x \ y
and \( yz \): \text{equiv-utrans } y \ z
shows \text{equiv-utrans } x \ z
⟨proof⟩

lemma equiv-trans-equiv-utrans [dest]:
\text{equiv-trans } t \ u \implies \text{equiv-utrans } t \ u
⟨proof⟩

3.2.2 Healthy Transformers

Feasibility

definition feasible :: \((a \Rightarrow \text{real}) \Rightarrow (a \Rightarrow \text{real}) \Rightarrow \text{bool}\)
where feasible \( t \) \iff \( (\forall b \ P. \ \text{bounded-by } b \ P \ \land \ \text{nneg } P \ \Rightarrow \ \text{bounded-by } b \ (t \ P) \ \land \ \text{nneg } (t \ P) ) \)

A feasible transformer preserves non-negativity, and bounds. A feasible transformer always takes its argument ‘closer to 0’ (or leaves it where it is). Note that any particular value of the expectation may increase, but no element of the new expectation may exceed any bound on the old. This is thus a relatively weak condition.

lemma feasibleI [intro]:
\[ (\forall b \ P. \ \text{bounded-by } b \ P \ \land \ \text{nneg } P \ \Rightarrow \ \text{bounded-by } b \ (t \ P) ); \ \text{nneg } P \] \implies \text{feasible } t
⟨proof⟩

lemma feasible-boundedD [dest]:
\[ \text{feasible } t \; \text{bounded-by } b \ P; \ \text{nneg } P \ \Rightarrow \ \text{bounded-by } b \ (t \ P) \]
⟨proof⟩

lemma feasible-nnegD [dest]:

3.2. EXPECTATION TRANSFORMERS

\[ \text{feasible } t; \text{ bounded-by } b \ P; \text{nneq } P \implies \text{nneq} \ (t \ P) \]

(\text{proof})

\textbf{lemma feasible-sound[dest]}:
\[ \text{feasible } t; \text{ sound } P \implies \text{ sound} \ (t \ P) \]
(\text{proof})

\textbf{lemma feasible-pr-0[simp]}:
- \textbf{fixes} \( t::(s \Rightarrow \text{real}) \Rightarrow s \Rightarrow \text{real} \)
- \textbf{assumes} \( ft: \text{ feasible } t \)
- \textbf{shows} \( t \ (\lambda x. \ 0) = (\lambda x. \ 0) \)
(\text{proof})

\textbf{lemma feasible-id}:
- \text{feasible} \ (\lambda x. \ x) 
(\text{proof})

\textbf{lemma feasible-bounded-by[dest]}:
\[ \text{feasible } t; \text{ sound } P; \text{ bounded-by } b \ P \implies \text{ bounded-by } b \ (t \ P) \]
(\text{proof})

\textbf{lemma feasible-fixes-top}:
- \text{feasible } t \implies t \ (\lambda s. \ 1) \leq (\lambda s. \ (1::\text{real}))
(\text{proof})

\textbf{lemma feasible-fixes-bot}:
- \textbf{assumes} \( ft: \text{ feasible } t \)
- \textbf{shows} \( t \ (\lambda s. \ 0) = (\lambda s. \ 0) \)
(\text{proof})

\textbf{lemma feasible-unitaryD[dest]}:
- \textbf{assumes} \( ft: \text{ feasible } t \) \textbf{and} \( uP: \text{unitary } P \)
- \textbf{shows} \( \text{unitary} \ (t \ P) \)
(\text{proof})

\textbf{Monotonicity}

\textbf{definition}
- \textit{mono-trans} :: \((s \Rightarrow \text{real}) \Rightarrow (s \Rightarrow \text{real}) \Rightarrow \text{bool} \)
\textbf{where}
- \textit{mono-trans} \( t \equiv \forall P Q. \ (\text{sound } P \land \text{sound } Q \land P \leq Q) \implies t \ P \leq t \ Q \)

Monotonicity allows us to compose transformers, and thus model sequential computation. Recall the definition of predicate entailment (Section 3.1.6) as less-than-or-equal. The statement \( Q \vdash t R \) means that \( Q \) is everywhere below \( t R \). For standard expectations (Section 3.1.5), this simply means that \( Q \) implies \( t R \), the weakest precondition of \( R \) under \( t \).
Given another, monotonic, transformer \( u \), we have that \( u \ Q \vdash u \ (t \ R) \), or that the weakest precondition of \( Q \) under \( u \) entails that of \( R \) under the
composition $u \circ t$. If we additionally know that $P \vdash u Q$, then by transitivity we have $P \vdash t R$. We thus derive a probabilistic form of the standard rule for sequential composition: $\left[ \text{mono-trans } t; P \vdash u Q; Q \vdash t R \right] \implies P \vdash u (t R)$.

**Lemma** **mono-transI [intro]:**

$\left[ \wedge P Q; \text{ sound } P; \text{ sound } Q; P \leq Q \right] \implies t P \leq t Q \implies \text{mono-trans } t$

**Lemma** **mono-transD [dest]:**

$\left[ \text{mono-trans } t; \text{ sound } P; \text{ sound } Q; P \leq Q \right] \implies t P \leq t Q$

**Scaling**

A healthy transformer commutes with scaling by a non-negative constant.

**Definition** **scaling :: (\(\text{real} \Rightarrow \text{real}\)) \Rightarrow \text{bool}**

where

scaling $t \equiv \forall P c x. \text{sound } P \land 0 \leq c \rightarrow c \cdot t P x = t (\lambda x. c \cdot P x) x$

The `scaling` and feasibility properties together allow us to treat transformers as a complete lattice, when operating on bounded expectations. The action of a transformer on such a bounded expectation is completely determined by its action on unitary expectations (those bounded by 1): $t P s = \text{bound-of } P * t (\lambda s. P s / \text{bound-of } P) s$. Feasibility in turn ensures that the lattice of unitary expectations is closed under the action of a healthy transformer. We take advantage of this fact in Section 3.3, in order to define the fixed points of healthy transformers.

**Lemma** **scalingI [intro]:**

$\left[ \wedge P c x. \text{sound } P; 0 \leq c \right] \implies c \cdot t P x = t (\lambda x. c \cdot P x) x \implies \text{scaling } t$

**Lemma** **scalingD [dest]:**

$\left[ \text{scaling } t; \text{ sound } P; 0 \leq c \right] \implies c \cdot t P x = t (\lambda x. c \cdot P x) x$

**Lemma** **right-scalingD:**

assumes $st$: scaling $t$

and $sP$: sound $P$

and $nnc$: $0 \leq c$

shows $t P s * c = t (\lambda s. P s * c) s$

**Healthiness**

Healthy transformers are feasible and monotonic, and respect scaling
definition
\textit{healthy} :: \((\text{'s} \Rightarrow \text{real}) \Rightarrow (\text{'s} \Rightarrow \text{real}) \Rightarrow \text{bool}

where
\begin{align*}
\text{healthy } t & \iff \text{feasible } t \land \text{mono-trans } t \land \text{scaling } t
\end{align*}

\texttt{lemma} \texttt{healthyI[intro]}:
\begin{align*}
\left[ \text{feasible } t; \text{mono-trans } t; \text{scaling } t \right] & \implies \text{healthy } t
\end{align*}

\texttt{lemmas} \texttt{healthy-parts = healthyI[OF feasibleI mono-transI scalingI]}

\texttt{lemma} \texttt{healthy-monoD[dest]}:
\begin{align*}
\text{healthy } t & \implies \text{mono-trans } t
\end{align*}

\texttt{lemmas} \texttt{healthy-monoD2 = mono-transD[OF healthy-monoD]}

\texttt{lemma} \texttt{healthy-feasibleD[dest]}:
\begin{align*}
\text{healthy } t & \implies \text{feasible } t
\end{align*}

\texttt{lemma} \texttt{healthy-scalingD[dest]}:
\begin{align*}
\text{healthy } t & \implies \text{scaling } t
\end{align*}

\texttt{lemma} \texttt{healthy-bounded-byD[intro]}:
\begin{align*}
\left[ \text{healthy } t; \text{bounded-by } b \ P; \text{nneg } P \right] & \implies \text{bounded-by } b \ (t \ P)
\end{align*}

\texttt{lemma} \texttt{healthy-bounded-byD2}:
\begin{align*}
\left[ \text{healthy } t; \text{bounded-by } b \ P; \text{sound } P \right] & \implies \text{bounded-by } b \ (t \ P)
\end{align*}

\texttt{lemma} \texttt{healthy-boundedD[dest,simp]}:
\begin{align*}
\left[ \text{healthy } t; \text{sound } P \right] & \implies \text{bounded } (t \ P)
\end{align*}

\texttt{lemma} \texttt{healthy-nnegD[dest,simp]}:
\begin{align*}
\left[ \text{healthy } t; \text{sound } P \right] & \implies \text{nneg } (t \ P)
\end{align*}

\texttt{lemma} \texttt{healthy-nnegD2[dest,simp]}:
\begin{align*}
\left[ \text{healthy } t; \text{bounded-by } b \ P; \text{nneg } P \right] & \implies \text{nneg } (t \ P)
\end{align*}

\texttt{lemma} \texttt{healthy-sound[intro]}:
\begin{align*}
\left[ \text{healthy } t; \text{sound } P \right] & \implies \text{sound } (t \ P)
\end{align*}
lemma healthy-unitary[intro]:
\[
\begin{array}{l}
\text{[ healthy } t; \text{ unitary } P \text{ ] } \implies \text{ unitary } (t \ P)
\end{array}
\]
⟨proof⟩

lemma healthy-id[simp,intro!]:
\[
\begin{array}{l}
\text{healthy id}
\end{array}
\]
⟨proof⟩

lemmas healthy-fixes-bot = feasible-fixes-bot[OF healthy-feasibleD]

Some additional results on le-trans, specific to healthy transformers.

lemma le-trans-bot[intro,simp]:
\[
\begin{array}{l}
\text{healthy } t \implies \text{ le-trans } (\lambda \ P \ s. 0) \ t
\end{array}
\]
⟨proof⟩

lemma le-trans-top[intro,simp]:
\[
\begin{array}{l}
\text{healthy } t \implies \text{ le-trans } t \ (\lambda \ P \ s. \ \text{bound-of } P)
\end{array}
\]
⟨proof⟩

lemma healthy-pr-bot[simp]:
\[
\begin{array}{l}
\text{healthy } t \implies t \ (\lambda \ s. 0) = (\lambda \ s. 0)
\end{array}
\]
⟨proof⟩

The first significant result is that healthiness is preserved by equivalence:

lemma healthy-equiv1:
\[
\begin{array}{l}
\text{fixes } t.:('s \Rightarrow \text{real}) \Rightarrow 's \Rightarrow \text{real and } u
\end{array}
\]
\[
\begin{array}{l}
\text{assumes equiv}: \text{equiv-trans } t \ u
\end{array}
\]
\[
\begin{array}{l}
\text{and healthy}: \text{healthy } t
\end{array}
\]
\[
\begin{array}{l}
\text{shows healthy } u
\end{array}
\]
⟨proof⟩

lemma healthy-equiv:
\[
\begin{array}{l}
\text{equiv-trans } t \ u \implies \text{healthy } t \iff \text{healthy } u
\end{array}
\]
⟨proof⟩

lemma healthy-scale:
\[
\begin{array}{l}
\text{fixes } t.:('s \Rightarrow \text{real}) \Rightarrow 's \Rightarrow \text{real}
\end{array}
\]
\[
\begin{array}{l}
\text{assumes ht}: \text{healthy } t \ \text{and } nc: 0 \leq c \ \text{and } bc: c \leq 1
\end{array}
\]
\[
\begin{array}{l}
\text{shows healthy } (\lambda P \ s. c \ast t \ P \ s)
\end{array}
\]
⟨proof⟩

lemma healthy-top[iff]:
\[
\begin{array}{l}
\text{healthy } (\lambda P \ s. \ \text{bound-of } P)
\end{array}
\]
⟨proof⟩

lemma healthy-bot[iff]:
\[
\begin{array}{l}
\text{healthy } (\lambda P \ s. 0)
\end{array}
\]
⟨proof⟩

This weaker healthiness condition is for the liberal (wlp) semantics. We
only insist that the transformer preserves unitarity (bounded by 1), and drop scaling (it is unnecessary in establishing the lattice structure here, unlike for the strict semantics).

**Definition**

\[ \text{nearly-healthy} :: ((\forall s^{\prime} \Rightarrow \text{real}) \Rightarrow (\forall s^{\prime} \Rightarrow \text{real})) \Rightarrow \text{bool} \]

**Where**

\[ \text{nearly-healthy} \; t \leftarrow (\forall P. \text{unitary} \; P \implies \text{unitary} \; (t \; P)) \wedge \]

\[ (\forall P \; Q. \text{unitary} \; P \implies \text{unitary} \; Q \implies P \vdash Q \implies t \; P \vdash t \; Q) \]

**Lemma** nearly-healthy\[\text{intro}\]:

\[ \ell P. \text{unitary} \; P \implies \text{unitary} \; (t \; P); \]

\[ \ell P \; Q. \ell \text{unitary} \; P; \ell \text{unitary} \; Q; P \vdash Q \]

\[ \implies t \; P \vdash t \; Q \implies \text{nearly-healthy} \; t \]

**Proof**

**Lemma** nearly-healthy\[\text{monoD}\[\text{dest}\]:

\[ \ell \text{nearly-healthy} \; t; P \vdash Q; \text{unitary} \; P; \text{unitary} \; Q \]

\[ \implies t \; P \vdash t \; Q \]

**Lemma** nearly-healthy\[\text{unitaryD}\[\text{dest}\]:

\[ \ell \text{nearly-healthy} \; t; \text{unitary} \; P \]

\[ \implies \text{unitary} \; (t \; P) \]

**Lemma** healthy-nearly-healthy\[\text{dest}\]:

**Assumes** \( \text{ht} \): healthy \( t \)

**Shows** nearly-healthy \( t \)

**Proof**

**Lemmas** nearly-healthy\[\text{id}\[\text{iff}\] =

healthy-nearly-healthy\[\text{OF healthy-id, unfolded id-def}\]

### 3.2.3 Sublinearity

As already mentioned, the core healthiness property (aside from feasibility and continuity) for transformers is **sublinearity**: The transformation of a quasi-linear combination of sound expectations is greater than the same combination applied to the transformation of the expectations themselves. The term \( x \ominus y \) represents truncated subtraction i.e. \( \max (x - y) (0::\text{\prime}a) \) (see Section 4.13.1).

**Definition** sublinear ::

\[ ((\forall s^{\prime} \Rightarrow \text{real}) \Rightarrow (\forall s^{\prime} \Rightarrow \text{real})) \Rightarrow \text{bool} \]

**Where**

\[ \ell \text{sublinear} \; t \leftarrow (\forall a \; b \; c \; P \; Q \; s. \; (\text{sound} \; P \wedge \text{sound} \; Q \wedge 0 \leq a \wedge 0 \leq b \wedge 0 \leq c) \]

\[ \leftarrow \]

\[ a * t \; P \; s + b * t \; Q \; s \ominus c \]

\[ \leq t \; (\lambda s^{\prime}. \; a * P \; s^{\prime} + b * Q \; s^{\prime} \ominus c) \; s) \]

**Lemma** sublinear\[\text{I}\[\text{intro}\]:
CHAPTER 3. SEMANTIC STRUCTURES

Figure 3.4: A graphical depiction of sub-additivity as convexity.

\[
\begin{pmatrix}
\text{P} \\
\text{tP} \\
\text{Q} = \text{tP} \cap \text{uP} \\
\text{Q}(x) + \text{Q}(y) \\
\end{pmatrix}
\]

\[x \quad y\]

\[\frac{x + y}{2}\]

\[Q(x)\]

\[Q(y)\]

Sub-additivity, together with scaling (Section 3.2.2) gives the linear portion of sublinearity. Together, these two properties are equivalent to convexity, as Figure 3.4 illustrates by analogy.

Here \(P\) is an affine function (expectation) real \(\Rightarrow\) real, restricted to some finite interval. In practice the state space (the left-hand type) is typically
discrete and multi-dimensional, but on the reals we have a convenient geometrical intuition. The lines $tP$ and $uP$ represent the effect of two healthy transformers (again affine). Neither monotonicity nor scaling are represented, but both are feasible: Both lines are bounded above by the greatest value of $P$.

The curve $Q$ is the pointwise minimum of $tP$ and $tQ$, written $tP \sqcap tQ$. This is, not coincidentally, the syntax for a binary nondeterministic choice in pGCL: The probability that some property is established by the choice between programs $a$ and $b$ cannot be guaranteed to be any higher than either the probability under $a$, or that under $b$.

The original curve, $P$, is trivially convex—it is linear. Also, both $t$ and $u$, and the operator $\sqcap$ preserve convexity. A probabilistic choice will also preserve it. The preservation of convexity is a property of sub-additive transformers that respect scaling. Note the form of the definition of convexity:

$$\forall x, y, \frac{Q(x) + Q(y)}{2} \leq Q\left(\frac{x + y}{2}\right)$$

Were we to replace $Q$ by some sub-additive transformer $v$, and $x$ and $y$ by expectations $R$ and $S$, the equivalent expression:

$$\frac{vR + vS}{2} \leq v\left(\frac{R + S}{2}\right)$$

Can be rewritten, using scaling, to:

$$\frac{1}{2}(vR + vS) \leq \frac{1}{2}v(R + S)$$

Which holds everywhere exactly when $v$ is sub-additive i.e.:

$$vR + vS \leq v(R + S)$$

**lemma** sub-addI[intro]:

\[
\begin{array}{l}
\forall x, y, \frac{Q(x) + Q(y)}{2} \leq Q\left(\frac{x + y}{2}\right) \\
\alpha \quad \text{sound } P; \text{ sound } Q \quad \Rightarrow \\

tP \ s + tQ \ s \leq t \ (\lambda s'. P \ s' + Q \ s') \ s \\
\Rightarrow \quad \text{sub-add } t
\end{array}
\]

(proof)

**lemma** sub-addI2:

\[
\begin{array}{l}
\forall x, y, \frac{Q(x) + Q(y)}{2} \leq Q\left(\frac{x + y}{2}\right) \\
\alpha \quad \text{sound } P; \text{ sound } Q \quad \Rightarrow \\
\lambda s. tP \ s + tQ \ s \vdash t \ (\lambda s'. P \ s' + Q \ s') \\
\Rightarrow \quad \text{sub-add } t
\end{array}
\]

(proof)

**lemma** sub-addD[dest]:

\[
\begin{array}{l}
\forall x, y, \frac{Q(x) + Q(y)}{2} \leq Q\left(\frac{x + y}{2}\right) \\
\alpha \quad \text{sound } P; \text{ sound } Q \quad \Rightarrow \\
\alpha \quad \text{sound } P; \text{ sound } Q \quad \Rightarrow \\
tP \ s + tQ \ s \leq t \ (\lambda s'. P \ s' + Q \ s') \ s
\end{array}
\]

(proof)
lemma equiv-sub-add:
  fixes $t :: ('s ⇒ real) ⇒ 's ⇒ real$
  assumes $eq :: equiv-trans t u$
  and $sa :: sub-add t$
  shows $sub-add u$
⟨proof⟩

Sublinearity and feasibility imply sub-additivity.

lemma sublinear-subadd:
  fixes $t :: ('s ⇒ real) ⇒ 's ⇒ real$
  assumes $slt :: sublinear t$
  and $ft :: feasible t$
  shows $sub-add t$
⟨proof⟩

A few properties following from sub-additivity:

lemma standard-negate:
  assumes $ht :: healthy t$
  and $sat :: sub-add t$
  shows $t « P » s + t « N P » s ≤ 1$
⟨proof⟩

lemma sub-add-setsum:
  fixes $t :: 's trans$ and $S :: 'a set$
  assumes $sat :: sub-add t$
  and $ht :: healthy t$
  and $sP :: ∀ x. sound (P x)$
  shows $(λ x. ∑ y ∈ S. t (P y) x) ≤ t (λ x. ∑ y ∈ S. P y x)$
⟨proof⟩

lemma sub-add-guard-split:
  fixes $t :: 's :: finite trans$ and $P :: 's expect$ and $s :: 's$
  assumes $sat :: sub-add t$
  and $ht :: healthy t$
  and $sP :: sound P$
  shows $(∑ y ∈ {s. G s}. P y * t « λ z. z = y » s) +$
  $(∑ y ∈ {s. ¬ G s}. P y * t « λ z. z = y » s) ≤ t P s$
⟨proof⟩

Sub-distributivity

definition sub-distrib ::
  (('s ⇒ real) ⇒ ('s ⇒ real)) ⇒ bool
where
  sub-distrib $t$ $←→$ $∀ P s. sound P → t P s ⊕ 1 ≤ t (λs'. P s' ⊕ 1) s$

lemma sub-distribI[intro]:
  [$ ∀ P s. sound P → t P s ⊕ 1 ≤ t (λs'. P s' ⊕ 1) s$] $→$ sub-distrib $t$
⟨proof⟩
3.2. EXPECTATION TRANSFORMERS

**lemma** `sub-distrib2`:

\[
\forall P. \text{sound } P \implies \lambda s. t \ s \uplus I \vdash t (\lambda s. \ P \ s \uplus I) \implies \text{sub-distrib } t
\]

(proof)

**lemma** `sub-distribD[dest]`:

\[
\text{sub-distrib } t ; \text{sound } P \implies t \ P \ s \uplus I \leq t (\lambda s'. \ P \ s' \uplus I) \ s
\]

(proof)

**lemma** `equiv-sub-distrib`:

fixes \( t:: ('s \Rightarrow \text{real}) \Rightarrow ('s \Rightarrow \text{real}) \)

assumes \( \text{eq: equiv-trans } t \ u \)

and \( \text{sd: sub-distrib } t \)

shows \( \text{sub-distrib } u \)

(proof)

Sublinearity implies sub-distributivity:

**lemma** `sublinear-sub-distrib`:

fixes \( t:: ('s \Rightarrow \text{real}) \Rightarrow ('s \Rightarrow \text{real}) \)

assumes \( \text{slt: sublinear } t \)

shows \( \text{sub-distrib } t \)

(proof)

Healthiness, sub-additivity and sub-distributivity imply sublinearity. This is how we usually show sublinearity.

**lemma** `sd-sa-sublinear`:

fixes \( t:: ('s \Rightarrow \text{real}) \Rightarrow ('s \Rightarrow \text{real}) \)

assumes \( \text{sdt: sub-distrib } t \) and \( \text{sat: sub-add } t \) and \( \text{ht: healthy } t \)

shows \( \text{sublinear } t \)

(proof)

Sub-conjunctivity

definition

\( \text{sub-conj} :: (('s \Rightarrow \text{real}) \Rightarrow ('s \Rightarrow \text{real}) \Rightarrow \text{bool} \)

where

\( \text{sub-conj } t \equiv \forall P \ Q. (\text{sound } P \land \text{sound } Q) \implies \ P \land Q \vdash t (P \land Q) \)

**lemma** `sub-conjI[intro]`:

\[
\forall P \ Q. \ [ \text{sound } P ; \text{sound } Q ] \implies t \ P \land Q \vdash t (P \land Q) \implies \text{sub-conj } t
\]

(proof)

**lemma** `sub-conjD[dest]`:

\[
[ \text{sub-conj } t ; \text{sound } P ; \text{sound } Q ] \implies t \ P \land Q \vdash t (P \land Q)
\]

(proof)

**lemma** `sub-conj-wp-twice`:
\texttt{fixes} f::\texttt{'}s \Rightarrow ((\texttt{'}s \Rightarrow \texttt{real}) \Rightarrow \texttt{'}s \Rightarrow \texttt{real}) \\
\texttt{assumes} \ all: \forall s. \texttt{sub-conj} (f \ s) \\
\texttt{shows} \ \texttt{sub-conj} (\lambda P \ s. f \ s \ P \ s)  \\
\langle \texttt{proof} \rangle  \\
\text{Sublinearity implies sub-conjunctivity:}  \\
\texttt{lemma sublinear-sub-conj:}  \\
\texttt{fixes} \ t::(\texttt{'}s \Rightarrow \texttt{real}) \Rightarrow \texttt{'}s \Rightarrow \texttt{real} \\
\texttt{assumes} \ \texttt{slt}: \texttt{sublinear} \ t \\
\texttt{shows} \ \texttt{sub-conj} \ t  \\
\langle \texttt{proof} \rangle  \\
\text{Sublinearity under equivalence}  \\
\text{Sublinearity is preserved by equivalence.} \\
\texttt{lemma equiv-sublinear:}  \\
\big\{ \texttt{equiv-trans} \ t \ u; \texttt{sublinear} \ t; \texttt{healthy} \ t \big\} = \Rightarrow \texttt{sublinear} \ u  \\
\langle \texttt{proof} \rangle  \\
\textbf{3.2.4 Determinism}  \\
\text{Transformers which are both additive, and maximal among those that satisfy feasibility are \textit{deterministic}, and will turn out to be maximal in the refinement order.}  \\
\textbf{Additivity}  \\
\text{Full additivity is not generally satisfied. It holds for (sub-)probabilistic transformers however.} \\
\texttt{definition} \\
\texttt{additive} :: (\texttt{'}a \Rightarrow \texttt{real}) \Rightarrow \texttt{'}a \Rightarrow \texttt{real} \Rightarrow \texttt{bool} \\
\texttt{where} \\
\texttt{additive} \ t \equiv \forall \ P \ Q. \ (\texttt{sound} \ P \land \texttt{sound} \ Q) \Rightarrow \ t (\lambda s. \ P \ s + Q \ s) = (\lambda s. \ t \ P \ s + t \ Q \ s)  \\
\texttt{lemma additiveD:}  \\
\big\{ \texttt{additive} \ t; \texttt{sound} \ P; \texttt{sound} \ Q \big\} = \Rightarrow (\lambda s. \ P \ s + Q \ s) = (\lambda s. \ t \ P \ s + t \ Q \ s)  \\
\langle \texttt{proof} \rangle \\
\texttt{lemma additiveI[intro]:}  \\
\big\{ \ [ \lambda P \ Q \ s. \ [ \texttt{sound} \ P; \texttt{sound} \ Q ] \Rightarrow t (\lambda s. \ P \ s + Q \ s) \ s = t \ P \ s + t \ Q \ s ] \Rightarrow \texttt{additive} \ t \big\} = \Rightarrow \  \\
\langle \texttt{proof} \rangle \\
\text{Additivity is strictly stronger than sub-additivity.} \\
\texttt{lemma additive-sub-add:} \\
\ \texttt{additive} \ t =\Rightarrow \ \texttt{sub-add} \ t
3.2. EXPECTATION TRANSFORMERS

The additivity property extends to finite summation.

**Lemma** additive-setsum:

```plaintext
fixes S::'s set
assumes additive: additive t
    and healthy: healthy t
    and finite: finite S
    and sPz: \( \bigwedge z. \text{sound } (P z) \)
shows \( t (\lambda x. \sum y \in S. P y x) = (\lambda x. \sum y \in S. t (P y) x) \)
```

An additive transformer (over a finite state space) is linear: it is simply the weighted sum of final expectation values, the weights being the probability of reaching a given final state. This is useful for reasoning using the forward, or “gambling game” interpretation.

**Lemma** additive-delta-split:

```plaintext
fixes t::('s::finite \Rightarrow \text{real}) \Rightarrow 's \Rightarrow \text{real}
assumes additive: additive t
    and ht: healthy t
    and sP: sound P
shows \( t P x = (\sum y \in \text{UNIV}. P y * t \{z. z = y\} x) \)
```

We can group the states in the linear form, to split on the value of a predicate (guard).

**Lemma** additive-guard-split:

```plaintext
fixes t::('s::finite \Rightarrow \text{real}) \Rightarrow 's \Rightarrow \text{real}
assumes additive: additive t
    and ht: healthy t
    and sP: sound P
shows \( t P x = (\sum y \in \{s. G s\}. P y * t \{z. z = y\} x) + (\sum y \in \{s. \neg G s\}. P y * t \{z. z = y\} x) \)
```

**Maximality**

**Definition**

```plaintext
maximal :: (('a \Rightarrow \text{real}) \Rightarrow 'a \Rightarrow \text{real}) \Rightarrow \text{bool}
where
maximal t \equiv \forall c. 0 \leq c \rightarrow t (\lambda -. c) = (\lambda -. c)
```

**Lemma** maximalI[intro]:

```plaintext
\[ \forall c. 0 \leq c \implies t (\lambda -. c) = (\lambda -. c) \implies \text{maximal } t \]
```

**Lemma** maximalD[dest]:

```plaintext
\[ \text{maximal } t; 0 \leq c \implies t (\lambda -. c) = (\lambda -. c) \]
A transformer that is both additive and maximal is deterministic:

**definition** `determ` :: \((\langle a \Rightarrow \text{real} \rangle \Rightarrow \langle a \Rightarrow \text{real} \rangle) \Rightarrow \text{bool}\)

**where**
\[\text{determ } t \equiv \text{additive } t \land \text{maximal } t\]

**lemma** `determI`[intro]:
\[
\left[ \text{additive } t; \text{maximal } t \right] \Rightarrow \text{determ } t
\]

**lemma** `determ-additiveD`[intro]:
\[\text{determ } t \Rightarrow \text{additive } t\]

**lemma** `determ-maximalD`[intro]:
\[\text{determ } t \Rightarrow \text{maximal } t\]

For a fully-deterministic transformer, a transformed standard expectation, and its transformed negation are complementary.

**lemma** `determ-negate`:
\[\text{assumes determ: } \text{determ } t \text{ shows } t \langle \text{P} \rangle s + t \langle \text{N} \rangle P s = 1\]

### 3.2.5 Modular Reasoning

The emphasis of a mechanised logic is on automation, and letting the computer tackle the large, uninteresting problems. However, as terms generally grow exponentially in the size of a program, it is still essential to break up a proof and reason in a modular fashion.

The following rules allow proof decomposition, and later will be incorporated into a verification condition generator.

**lemma** `entails-combine`:
\[\text{assumes wp1: } P \vdash t R \text{ and wp2: } Q \vdash t S \text{ and sc: } \text{sub-conj } t \text{ and sR: } \text{sound } R \text{ and sS: } \text{sound } S \text{ shows } P \&\& Q \vdash t (R \&\& S)\]

These allow mismatched results to be composed

**lemma** `entails-strengthen-post`:
\[
\left[ P \vdash t Q; \text{healthy } t; \text{sound } R; Q \vdash R; \text{sound } Q \right] \Rightarrow P \vdash t R
\]
3.2. EXPECTATION TRANSFORMERS

**Lemma entail-weak-pre:**

\[
\begin{array}{c}
Q \vdash t R; P \vdash Q \\
\implies P \vdash t R
\end{array}
\]

(proof)

This rule is unique to pGCL. Use it to scale the post-expectation of a rule to 'fit under' the precondition you need to satisfy.

**Lemma entail-scale:**

assumes wp: \(P \vdash t Q\) and \(h: \text{healthy } t\)

and \(sQ: \text{sound } Q\) and pos: \(0 \leq c\)

shows \((\lambda s. c * P s) \vdash t (\lambda s. c * Q s)\)

(proof)

3.2.6 Transforming Standard Expectations

Reasoning with standard expectations, those obtained by embedding a predicate, is often easier, as the analogues of many familiar boolean rules hold in modified form.

One may use a standard pre-expectation as an assumption:

**Lemma use-premise:**

assumes \(h: \text{healthy } t\) and \(wP: \bigwedge s. P s \implies 1 \leq t \langle Q \rangle s\)

shows \(\langle P \rangle \vdash t \langle Q \rangle\)

(proof)

The other direction works too.

**Lemma fold-premise:**

assumes \(ht: \text{healthy } t\)

and \(wp: \langle P \rangle \vdash t \langle Q \rangle\)

shows \(\forall s. P s \implies 1 \leq t \langle Q \rangle s\)

(proof)

Predicate conjunction behaves as expected:

**Lemma conj-post:**

\[
\begin{array}{c}
\big[ P \vdash t \langle \lambda s. Q s \land R s \rangle; \text{healthy } t \big] \implies P \vdash t \langle Q \rangle
\end{array}
\]

(proof)

Similar to \(\text{[healthy } ?t; \bigwedge s. ?P s \implies 1 \leq ?t \langle ?Q \rangle s]\implies \langle ?P \rangle \vdash ?t \langle ?Q \rangle\), but more general.

**Lemma entail-pconj-assumption:**

assumes \(f: \text{feasible } t\) and \(wP: \bigwedge s. P s \implies Q s \leq t R s\)

and \(uQ: \text{unitary } Q\) and \(uR: \text{unitary } R\)

shows \(\langle P \rangle \land Q \vdash t R\)

(proof)

end
CHAPTER 3. SEMANTIC STRUCTURES

3.3 Induction

theory Induction
  imports Expectations Transformers Conditionally-Complete-Lattices
begin

3.3.1 The Lattice of Expectations

Defining recursive (or iterative) programs requires us to reason about fixed points on the semantic objects, in this case expectations. The complication here, compared to the standard Knaster-Tarski theorem (for example, as shown in /src/HOL/Inductive.thy), is that we do not have a complete lattice.

Finding a lower bound is easy (it’s $\lambda$. 0::'b), but as we do not insist on any global bound on expectations (and work directly in HOL’s real type, rather than extending it with a point at infinity), there is no top element. We solve the problem by defining the least (greatest) fixed point, restricted to an internally-bounded set, allowing us to substitute this bound for the top element. This works as long as the set contains at least one fixed point, which appears as an extra assumption in all the theorems.

This also works semantically, thanks to the definition of healthiness. Given a healthy transformer parameterised by some sound expectation: t. Imagine that we wish to find the least fixed point of $t \ P$. In practice, t is generally doubly healthy, that is $\forall \ P. \ sound \ P \rightarrow healthy \ (t \ P)$ and $\forall \ Q. \ sound \ Q \rightarrow healthy \ (\lambda P. \ t \ P \ Q)$. Thus by feasibility, $t \ P \ Q$ must be bounded by $bound-of \ P$. Thus, as by definition $x \leq t \ P \ x$ for any fixed point, all must lie in the set of sound expectations bounded above by $\lambda$. $bound-of \ P$.

definition Inf-exp :: 's expect set ⇒ 's expect
where Inf-exp S = ($\lambda s. \ Inf \ \{ f s | f \in S \}$)

lemma Inf-exp-lower:
[ $P \in S; \ \forall P\in S. \ nneg \ P \ \\implies \ Inf-exp \ S \leq P$
(proof]

lemma Inf-exp-greatest:
[ $S \neq \{}; \ \forall P\in S. \ Q \leq P \ \\implies \ Q \leq \ Inf-exp \ S$
(proof]

definition Sup-exp :: 's expect set ⇒ 's expect
where Sup-exp S = (if $S = \{}$ then $\lambda s. \ 0$ else ($\lambda s. \ Sup \ \{ f s | f \in S \}$))

lemma Sup-exp-upper:
[ $P \in S; \ \forall P\in S. \ bounded-by \ b \ P \ \\implies \ P \leq \ Sup-exp \ S$
(proof]

lemma Sup-exp-least:
3.3. INDUCTION

\[
\forall P \in S. \ P \leq Q; \ \text{neg} \ Q \implies \ \text{Sup-exp} \ S \leq Q
\]
(proof)

lemma Sup-exp-sound:
  assumes sS: \( \forall P. \ P \in S \implies \text{sound} \ P \)
  and bS: \( \forall P. \ P \in S \implies \text{bounded-by} \ b \ P \)
  shows sound (Sup-exp S)
(proof)

definition lfp-exp :: 's \ trans \Rightarrow 's \ expect
where lfp-exp t = Inf-exp \{ P. \ \text{sound} \ P \land \ t \ P \leq P \}

lemma lfp-exp-lowerbound:
  \( \forall P. \ P \leq t; \ \text{sound} \ P \implies lfp-exp \ t \leq P \)
(proof)

lemma lfp-exp-greatest:
  \( \forall P. \ \text{sound} \ P \implies Q \leq P; \ \text{sound} \ Q; \ t \ R \vdash \ R; \ \text{sound} \ R \implies Q \leq lfp-exp \ t \)
(proof)

lemma feasible-lfp-exp-sound:
  feasible \ t \implies \text{sound} (lfp-exp \ t)
(proof)

lemma lfp-exp-sound:
  assumes fR: \( t \ R \vdash \ R \) and sR: \( \text{sound} \ R \)
  shows \( \text{sound} (lfp-exp \ t) \)
(proof)

lemma lfp-exp-bound:
  \( \forall P. \ \text{unitary} \ P \implies \text{unitary} (t \ P) \implies \text{bounded-by} \ t \ (lfp-exp \ t) \)
(proof)

lemma lfp-exp-unitary:
  \( \forall P. \ \text{unitary} \ P \implies \text{unitary} (t \ P) \implies \text{unitary} (lfp-exp \ t) \)
(proof)

lemma lfp-exp-lemma2:
  fixes t::'s \ trans
  assumes st: \( \forall P. \ \text{sound} \ P \implies \text{sound} (t \ P) \)
  and mt: \( \text{mono-trans} \ t \)
  and fR: \( t \ R \vdash \ R \) and sR: \( \text{sound} \ R \)
  shows \( t (lfp-exp \ t) \leq lfp-exp \ t \)
(proof)

lemma lfp-exp-lemma3:
  assumes st: \( \forall P. \ \text{sound} \ P \implies \text{sound} (t \ P) \)
  and mt: \( \text{mono-trans} \ t \)
...and \( \text{ff} : t \vdash R \) and \( \text{sR} : \text{sound } R \)
shows \( \text{lfp-exp } t \leq t (\text{lfp-exp } t) \)
\(\langle \text{proof} \rangle\)

**lemma** \( \text{lfp-exp-unfold} : \)
 embarrasses \( \text{nt} : \forall P. \text{sound } P \implies \text{sound } (t P) \)
and \( \text{mt} : \text{mono-trans } t \)
and \( \text{ff} : t \vdash R \) and \( \text{sR} : \text{sound } R \)
shows \( \text{lfp-exp } t = t (\text{lfp-exp } t) \)
\(\langle \text{proof} \rangle\)

**definition** \( \text{gfp-exp} : \text{'}s \text{ trans } \Rightarrow \text{'s expect} \)
where \( \text{gfp-exp } t = \text{Sup-exp } \{ P. \text{unitary } P \land P \leq t P \} \)

**lemma** \( \text{gfp-exp-upperbound} : \)
\( \begin{align*}
[ & P \leq t P; \text{unitary } P ] \implies P \leq \text{gfp-exp } t \\
\langle \text{proof} \rangle
\end{align*} \)

**lemma** \( \text{gfp-exp-least} : \)
\( \begin{align*}
[ & \forall P. [ P \leq t P; \text{unitary } P ] \implies P \leq Q; \text{unitary } Q ] \implies \text{gfp-exp } t \leq Q \\
\langle \text{proof} \rangle
\end{align*} \)

**lemma** \( \text{gfp-exp-bound} : \)
\( \langle \forall P. \text{unitary } P \implies \text{unitary } (t P) \rangle \implies \text{bounded-by } 1 (\text{gfp-exp } t) \)
\(\langle \text{proof} \rangle\)

**lemma** \( \text{gfp-exp-nneg[iff]} : \)
\( \text{nneg } (\text{gfp-exp } t) \)
\(\langle \text{proof} \rangle\)

**lemma** \( \text{gfp-exp-unitary} : \)
\( \begin{align*}
( & \forall P. \text{unitary } P \implies \text{unitary } (t P)) \implies \text{unitary } (\text{gfp-exp } t) \\
\langle \text{proof} \rangle
\end{align*} \)

**lemma** \( \text{gfp-exp-lemma2} : \)
 embarrasses \( \text{ft} : \forall P. \text{unitary } P \implies \text{unitary } (t P) \)
and \( \text{mt} : \forall P Q. [ \text{unitary } P; \text{unitary } Q; P \vdash Q ] \implies t P \vdash t Q \)
shows \( \text{gfp-exp } t \leq t (\text{gfp-exp } t) \)
\(\langle \text{proof} \rangle\)

**lemma** \( \text{gfp-exp-lemma3} : \)
 embarrasses \( \text{ft} : \forall P. \text{unitary } P \implies \text{unitary } (t P) \)
and \( \text{mt} : \forall P Q. [ \text{unitary } P; \text{unitary } Q; P \vdash Q ] \implies t P \vdash t Q \)
solves \( t (\text{gfp-exp } t) \leq \text{gfp-exp } t \)
\(\langle \text{proof} \rangle\)

**lemma** \( \text{gfp-exp-unfold} : \)
\( \langle \forall P. \text{unitary } P \implies \text{unitary } (t P) \rangle \implies \langle \forall P Q. [ \text{unitary } P; \text{unitary } Q; P \vdash Q ] \implies t P \vdash t Q \rangle \implies \)
3.3. INDUCTION

\[ \text{gfp-exp } t = t (\text{gfp-exp } t) \]

(proof)

3.3.2 The Lattice of Transformers

In addition to fixed points on expectations, we also need to reason about fixed points on expectation transformers. The interpretation of a recursive program in pGCL is as a fixed point of a function from transformers to transformers. In contrast to the case of expectations, healthy transformers do form a complete lattice, where the bottom element is \( \lambda \cdot - \cdot 0 \cdot \cdot \), and the top element is the greatest allowed by feasibility: \( \lambda P \cdot \cdot \cdot \text{bound-of } P \).

**definition** Inf-trans :: 's trans set \( \Rightarrow \) 's trans

**where** Inf-trans \( S = (\lambda P. \text{Inf-exp} \{ t P \mid t \in S \}) \)

**lemma** Inf-trans-lower:

\[ [ t \in S; \forall u \in S. \forall P. \text{sound } P \longrightarrow \text{sound } (u P) ] \implies \text{le-trans } (\text{Inf-trans } S) t \]

(proof)

**lemma** Inf-trans-greatest:

\[ [ S \neq \{\}; \forall t \in S. \forall P. \text{le-trans } u t ] \implies \text{le-trans } u (\text{Inf-trans } S) \]

(proof)

**definition** Sup-trans :: 's trans set \( \Rightarrow \) 's trans

**where** Sup-trans \( S = (\lambda P. \text{Sup-exp} \{ t P \mid t \in S \}) \)

**lemma** Sup-trans-upper:

\[ [ t \in S; \forall u \in S. \forall P. \text{unitary } P \longrightarrow \text{unitary } (u P) ] \implies \text{le-utrans } t (\text{Sup-trans } S) \]

(proof)

**lemma** Sup-trans-upper2:

\[ [ t \in S; \forall u \in S. \forall P. (\text{nneg } P \wedge \text{bounded-by } b P) \longrightarrow (\text{nneg } (u P) \wedge \text{bounded-by } b (u P)); \text{nneg } P; \text{bounded-by } b P ] \implies t P \vdash \text{Sup-trans } S P \]

(proof)

**lemma** Sup-trans-least:

\[ [ \forall t \in S. \text{le-utrans } t u; \forall P. \text{unitary } P \longrightarrow \text{unitary } (u P) ] \implies \text{le-utrans } (\text{Sup-trans } S) u \]

(proof)

**lemma** Sup-trans-least2:

\[ [ \forall t \in S. \forall P. \text{nneg } P \longrightarrow \text{bounded-by } b P \longrightarrow t P \vdash u P; \forall u \in S. \forall P. (\text{nneg } P \wedge \text{bounded-by } b P) \longrightarrow (\text{nneg } (u P) \wedge \text{bounded-by } b (u P)); \text{nneg } P; \text{bounded-by } b P; \forall P. [ \text{nneg } P; \text{bounded-by } b P ] \implies \text{nneg } (u P) ] \implies \text{Sup-trans } S P \vdash u P \]

(proof)
lemma feasible-Sup-trans:
fixes $S$::’s trans set
assumes $fS$: $\forall t \in S$. feasible $t$
shows feasible $(\operatorname{Sup-trans} S)$
⟨proof⟩

definition lfp-trans :: (’s trans ⇒ ’s trans) ⇒ ’s trans
where lfp-trans $T = \operatorname{Inf-trans} \{ t. (\forall P. \operatorname{sound} P \implies \operatorname{sound} (t P)) \wedge \operatorname{le-trans} (T t) t \} $

lemma lfp-trans-lowerbound:
\[
\begin{array}{l}
\forall t P. \begin{array}{l}
\begin{array}{l}
\operatorname{le-trans} (T t) t;
\forall P. \operatorname{sound} P \implies \operatorname{sound} (t P)
\end{array}
\rightarrow
\operatorname{le-trans} (\text{lfp-trans} T) t
\end{array}
\rightarrow
\begin{array}{l}
\forall P. \operatorname{sound} P \implies \operatorname{sound} (v P)
\end{array}
\operatorname{le-trans} (T v) v
\end{array}
\] 
⟨proof⟩

lemma lfp-trans-greatest:
\[
\begin{array}{l}
\forall t P. \begin{array}{l}
\begin{array}{l}
\forall P. \operatorname{sound} P \implies \operatorname{sound} (t P)
\end{array}
\rightarrow
\forall P. \operatorname{sound} P \implies \operatorname{sound} (v P)
\end{array}
\end{array}
\] 
⟨proof⟩

lemma lfp-trans-sound:
fixes $P Q$::’s expect
assumes $sP$: \operatorname{sound} $P$
and $fv$: \operatorname{le-trans} (T v) v
and $sv$: $\forall P. \operatorname{sound} P \implies \operatorname{sound} (v P)$
shows \operatorname{sound} (lfp-trans $T P$
⟨proof⟩

lemma lfp-trans-unitary:
fixes $P Q$::’s expect
assumes $uP$: \operatorname{unitary} $P$
and $fv$: \operatorname{le-trans} (T v) v
and $sv$: $\forall P. \operatorname{sound} P \implies \operatorname{sound} (v P)$
and $fT$: \operatorname{le-trans} (T ($\lambda P s. \operatorname{bound-of} P )) ($\lambda P s. \operatorname{bound-of} P$
shows \operatorname{unitary} (lfp-trans $T P$
⟨proof⟩

lemma lfp-trans-lemma2:
fixes $v$::’s trans
assumes $\text{mono}$: $\forall t u. [\begin{array}{l}
\begin{array}{l}
\operatorname{le-trans} t u;
\forall P. \operatorname{sound} P \implies \operatorname{sound} (t P);
\forall P. \operatorname{sound} P \implies \operatorname{sound} (u P)
\end{array}
\rightarrow
\operatorname{le-trans} (T t) (T u)
\end{array}
\] 
and $nT$: $\forall t P. [\begin{array}{l}
\begin{array}{l}
\forall Q. \operatorname{sound} Q \implies \operatorname{sound} (Q P); \operatorname{sound} P
\end{array}
\rightarrow
\begin{array}{l}
\forall P. \operatorname{sound} P \implies \operatorname{sound} (T t P)
\end{array}
\] 
\rightarrow
\begin{array}{l}
\forall P. \operatorname{sound} P \implies \operatorname{sound} (v P)
\end{array}
\rightarrow
\begin{array}{l}
\operatorname{le-trans} (T (lfp-trans T)) (lfp-trans T)
\end{array}
\] 
⟨proof⟩

lemma lfp-trans-lemma3:
3.3. INDUCTION

\textbf{fixes} v::'s trans
\textbf{assumes} mono: \forall t u. \ [ \text{le-trans} \ t \ u; \ \forall P. \ \text{sound} \ P \Rightarrow \ \text{sound} \ (t \ P); \\
\forall P. \ \text{sound} \ P \Rightarrow \ \text{sound} \ (u \ P) \ ] \Rightarrow \ \text{le-trans} \ (T \ t) \ (T \ u) \\
\text{and} sT: \ \forall t. \ [ \ \forall Q. \ \text{sound} \ Q \Rightarrow \ \text{sound} \ (t \ Q); \ \text{sound} \ P \ ] \Rightarrow \ \text{sound} \ (T \ t \ P) \\
\text{and} fv: \ \text{le-trans} \ (T \ v) \ v \\
\text{and} sv: \ \forall P. \ \text{sound} \ P \Rightarrow \ \text{sound} \ (v \ P) \\
\textbf{shows} \ \text{le-trans} \ ((\text{lfp-trans} \ T) \ (T \ (\text{lfp-trans} \ T)))
\langle \text{proof} \rangle

\textbf{lemma} \ \text{lfp-trans-unfold:} \\
\textbf{fixes} P::'s expect \\
\textbf{assumes} mono: \forall t u. \ [ \ \text{le-trans} \ t \ u; \ \forall P. \ \text{sound} \ P \Rightarrow \ \text{sound} \ (t \ P); \\
\forall P. \ \text{sound} \ P \Rightarrow \ \text{sound} \ (u \ P) \ ] \Rightarrow \ \text{le-trans} \ (T \ t) \ (T \ u) \\
\text{and} sT: \ \forall t. \ [ \ \forall Q. \ \text{sound} \ Q \Rightarrow \ \text{sound} \ (t \ Q); \ \text{sound} \ P \ ] \Rightarrow \ \text{sound} \ (T \ t \ P) \\
\text{and} fv: \ \text{le-trans} \ (T \ v) \ v \\
\text{and} sv: \ \forall P. \ \text{sound} \ P \Rightarrow \ \text{sound} \ (v \ P) \\
\textbf{shows} \ \text{equiv-trans} \ ((\text{lfp-trans} \ T) \ (T \ (\text{lfp-trans} \ T)))
\langle \text{proof} \rangle

\textbf{definition} \ \text{gfp-trans ::} (\forall \ P. \ \text{trans} \ P \Rightarrow \forall \ P. \ \text{trans} \ P) \Rightarrow \forall \ P. \ \text{trans} \ P \\
\textbf{where} \ \text{gfp-trans} \ T = \text{Sup-trans} \ \{t. \ \forall P. \ \text{unitary} \ P \Rightarrow \ \text{unitary} \ (t \ P) \ \land \ \text{le-utrans} \ t \ (T \ t)\}

\textbf{lemma} \ \text{gfp-trans-upperbound:} \\
[ \ \text{le-utrans} \ t \ (T \ t); \ \forall P. \ \text{unitary} \ P \Rightarrow \ \text{unitary} \ (t \ P) \ ] \Rightarrow \ \text{le-utrans} \ t \ (\text{gfp-trans} \ T)
\langle \text{proof} \rangle

\textbf{lemma} \ \text{gfp-trans-least:} \\
[ \ \forall t. \ [ \ \text{le-utrans} \ t \ (T \ t); \ \forall P. \ \text{unitary} \ P \Rightarrow \ \text{unitary} \ (t \ P) \ ] \Rightarrow \ \text{le-utrans} \ t \ u; \\
\forall P. \ \text{unitary} \ P \Rightarrow \ \text{unitary} \ (u \ P) \ ] \Rightarrow \ \\
\text{le-utrans} \ (\text{gfp-trans} \ T) \ u
\langle \text{proof} \rangle

\textbf{lemma} \ \text{gfp-trans-unitary:} \\
\textbf{fixes} P::'s expect \\
\textbf{assumes} uP: \text{unitary} \ P \\
\textbf{shows} \ \text{unitary} \ (\text{gfp-trans} \ T \ P)
\langle \text{proof} \rangle

\textbf{lemma} \ \text{gfp-trans-lemma2:} \\
\textbf{assumes} mono: \forall t u. \ [ \ \text{le-utrans} \ t \ u; \ \forall P. \ \text{unitary} \ P \Rightarrow \ \text{unitary} \ (t \ P); \\
\forall P. \ \text{unitary} \ P \Rightarrow \ \text{unitary} \ (u \ P) \ ] \Rightarrow \ \text{le-utrans} \ (T \ t) \ (T \ u) \\
\text{and} hT: \ \forall t. \ [ \ \forall Q. \ \text{unitary} \ Q \Rightarrow \ \text{unitary} \ (t \ Q); \ \text{unitary} \ P \ ] \Rightarrow \ \text{unitary} \\
(T \ t \ P) \\
\textbf{shows} \ \text{le-utrans} \ ((\text{gfp-trans} \ T) \ (T \ (\text{gfp-trans} \ T)))
\langle \text{proof} \rangle
CHAPTER 3. SEMANTIC STRUCTURES

lemma gfp-trans-lemma3:
  assumes mono: \( \forall t. u. \langle \text{le-utrans } t \ u; \ \land P. \ \text{unitary } P \Rightarrow \text{unitary } (t P) \rangle \)
  and hT: \( \forall t. P. \ [\ \land Q. \ \text{unitary } Q \Rightarrow \text{unitary } (t Q); \ \text{unitary } P \ ] \Rightarrow \text{unitary } (T t P) \)
  shows le-utrans (T (gfp-trans T)) (gfp-trans T)
 ⟨proof⟩

lemma gfp-trans-unfold:
  assumes mono: \( \forall t. u. \langle \text{le-utrans } t \ u; \ \land P. \ \text{unitary } P \Rightarrow \text{unitary } (t P) \rangle \)
  and hT: \( \forall t. P. \ [\ \land Q. \ \text{unitary } Q \Rightarrow \text{unitary } (t Q); \ \text{unitary } P \ ] \Rightarrow \text{unitary } (T t P) \)
  shows equiv-utrans (gfp-trans T) (T (gfp-trans T))
 ⟨proof⟩

3.3.3 Tail Recursion

The least (greatest) fixed point of a tail-recursive expression on transformers is equivalent (given appropriate side conditions) to the least (greatest) fixed point on expectations.

lemma gfp-pulldown:
  fixes P::'s expect and t::'s expect ⇒ 's trans
  assumes tailcall: \( \forall u. P. \ \text{unitary } P \Rightarrow T u P = t P (u P) \)
  and ft: \( \forall t. P. \ [\ \land Q. \ \text{unitary } Q \Rightarrow \text{unitary } (t Q); \ \text{unitary } P \ ] \Rightarrow \text{unitary } (T t P) \)
  and ft: \( \forall P. Q. \ \text{unitary } P \Rightarrow \text{unitary } Q \Rightarrow \text{unitary } (t P Q) \)
  and mt: \( \forall P. Q R. \ [\ \text{unitary } P; \ \text{unitary } Q; \ \text{unitary } R; Q \vdash R \ ] \Rightarrow t P Q \)
  and uP: \( \forall u. P. \ \text{unitary } P \)
  and monoT: \( \forall t. u. \langle \text{le-utrans } t \ u; \ \land P. \ \text{unitary } P \Rightarrow \text{unitary } (t P) \rangle \)
  \( \forall P. \ \text{unitary } P \Rightarrow \text{unitary } (u P) \] \Rightarrow \text{le-utrans } (T t P) (T u)
  shows gfp-trans T P = gfp-exp (t P) (is ?X P = ?Y P)
 ⟨proof⟩

lemma lfp-pulldown:
  fixes P::'s expect and t::'s expect ⇒ 's trans
  and T::'s trans ⇒ 's trans
  assumes tailcall: \( \forall u. P. \ \text{sound } P \Rightarrow T u P = t P (u P) \)
  and st: \( \forall P. Q. \ \text{sound } P \Rightarrow \text{sound } Q \Rightarrow \text{sound } (t P Q) \)
  and mt: \( \forall P. \ \text{sound } P \Rightarrow \text{mono-trans } (t P) \)
  and monoT: \( \forall t. u. \langle \text{le-trans } t \ u; \ \land P. \ \text{sound } P \Rightarrow \text{sound } (t P) \rangle \)
  \( \forall P. \ \text{sound } P \Rightarrow \text{sound } (u P) \] \Rightarrow \text{le-trans } (T t P) (T u)
  and nT: \( \forall t. P. \ [\ \land Q. \ \text{sound } Q \Rightarrow \text{sound } (t Q); \ \text{sound } P \ ] \Rightarrow \text{sound } (T t P) \)
  and fv: \( \text{le-trans } (T v) v \)
  and sv: \( \forall P. \ \text{sound } P \Rightarrow \text{sound } (v P) \)
3.3. INDUCTION

and sP: sound P
shows \( \text{lfp-trans } T P = \text{lfp-exp } (t P) \) (is \( ?X P = ?Y P \))
⟨proof⟩

**definition** Inf-utrans \::\ 's trans set \( \Rightarrow \) 's trans
**where** Inf-utrans \( S = \) (if \( S = \{ \} \) then \( \lambda P \ s. \ I \) else Inf-trans \( S \))

**lemma** Inf-utrans-lower:
\[ [ t \in S; \forall t \in S. \forall P. \text{unitary } P \rightarrow \text{unitary } (t P) ] \rightarrow \text{le-utrans } (\text{Inf-utrans } S) t \]
⟨proof⟩

**lemma** Inf-utrans-greatest:
\[ [ \bigwedge P. \text{unitary } P \rightarrow \text{unitary } (t P); \forall u \in S. \text{le-utrans } t u ] \rightarrow \text{le-utrans } t \]
(Inf-utrans \( S \))
⟨proof⟩

end
Chapter 4

The pGCL Language

4.1 A Shallow Embedding of pGCL in HOL

theory Embedding imports Misc Induction begin

4.1.1 Core Primitives and Syntax

A pGCL program is embedded directly as its strict or liberal transformer. This is achieved with an additional parameter, specifying which semantics should be obeyed.

type-synonym 's prog = bool ⇒ ('s ⇒ real) ⇒ ('s ⇒ real)

Abort either always fails, λP s. 0::'c, or always succeeds, λP s. 1::'c.

definition Abort :: 's prog
where Abort ≡ λab P s. if ab then 0 else 1

Skip does nothing at all.

definition Skip :: 's prog
where Skip ≡ λab P. P

Apply lifts a state transformer into the space of programs.

definition Apply :: ('s ⇒ 's ⇒ real) ⇒ 's prog
where Apply f ≡ λab P s. P (f s)

Seq is sequential composition.

definition Seq :: 's prog ⇒ 's prog ⇒ 's prog
(infixl ;; 59)
where Seq a b ≡ (λab. a ab o b ab)

PC is probabilistic choice between programs.

definition PC :: 's prog ⇒ ('s ⇒ real) ⇒ 's prog ⇒ 's prog
(· ⊕ · [58,57,57] 57)
where PC a P b ≡ λab Q s. P s * a ab Q s + (1 − P s) * b ab Q s
**DC** is demonic choice between programs.

**definition** **DC** :: 's prog ⇒ 's prog ⇒ 's prog (- ∏ - [58,57] 57)

**where**  
\[ DC \ a \ b \equiv \lambda \ ab \ Q \ s. \ \min (a \ ab \ Q \ s) \ (b \ ab \ Q \ s) \]

**AC** is angelic choice between programs.

**definition** **AC** :: 's prog ⇒ 's prog ⇒ 's prog (- ∪ - [58,57] 57)

**where**  
\[ AC \ a \ b \equiv \lambda \ ab \ Q \ s. \ \max (a \ ab \ Q \ s) \ (b \ ab \ Q \ s) \]

**Embed** allows any expectation transformer to be treated syntactically as a program, by ignoring the failure flag.

**definition** **Embed** :: 's trans ⇒ 's prog

**where**  
\[ Embed \ t \equiv (\lambda \ ab. \ t) \]

**Mu** is the recursive primitive, and is either then least or greatest fixed point.

**definition** **Mu** :: ('s prog ⇒ 's prog) ⇒ 's prog

**where**  
\[ Mu \ (T) \equiv (\lambda \ ab. \ if \ ab \ then \ \ \ \ \ \ lfp-trans \ (\lambda \ t. \ T (Embed \ t) \ ab)) \ else \ gfp-trans \ (\lambda \ t. \ T (Embed \ t) \ ab)) \]

**repeat** expresses finite repetition

**primrec**

\[ repeat :: nat ⇒ 'a prog ⇒ 'a prog \]

**where**

\[ repeat \ 0 \ p = \text{Skip} | \]

\[ repeat \ (\text{Suc} \ n) \ p = p ;; \text{repeat} \ n \ p \]

**SetDC** is demonic choice between a set of alternatives, which may depend on the state.

**definition** **SetDC** :: ('a ⇒ 's prog) ⇒ ('s ⇒ 'a set) ⇒ 's prog

**where**  
\[ SetDC \ f \ S \equiv \lambda \ ab \ P \ s. \ \text{Inf} ((\lambda a. \ f \ a \ ab \ P \ s) \ S \ s) \]

**syntax** **-SetDC** :: pttrn =⇒ ('s ⇒ 'a set) =⇒ 's prog =⇒ 's prog

\[ \prod x \in S. \ p \Rightarrow \text{CONST} \ SetDC \ (\%x. \ p) \ S \]

The above syntax allows us to write \( \prod x \in S. \ \text{Apply} \ f \)

**SetPC** is probabilistic choice from a set. Note that this is only meaningful for distributions of finite support.

**definition** **SetPC** :: ('a ⇒ 's prog) ⇒ ('s ⇒ 'a ⇒ real) ⇒ 's prog

**where**  
\[ SetPC \ f \ p \equiv \lambda \ ab \ P \ s. \ \sum a \in \text{supp} (p \ s). \ p \ s \ a \ * \ f \ a \ ab \ P \ s \]

**Bind** allows us to name an expression in the current state, and re-use it later.

**definition**

\[ Bind :: ('a ⇒ 'a) ⇒ ('a ⇒ 's prog) ⇒ 's prog \]
4.1. A SHALLOW EMBEDDING OF PGCL IN HOL

where

\[ \text{Bind } g f ab \equiv \lambda P s. \text{let } a = g s \text{ in } f a ab P s \]

This gives us something like let syntax

**syntax** -Bind :: pttrn => ('s => 'a) => 's prog => 's prog

**translations** x is f in a => CONST Bind f (%x. a)

**definition** flip :: ('a => 'b => 'c) => 'b => 'a => 'c

where [simp]: flip f = (\lambda b a. f a b)

The following pair of translations introduce let-style syntax for SetPC and SetDC, respectively.

**syntax** -PBind :: pttrn => ('s => real) => 's prog => 's prog

**translations** bind x at p in a => CONST SetPC (%x. a) (CONST flip (%x. p))

**syntax** -DBind :: pttrn => ('s => 'a set) => 's prog => 's prog

**translations** bind x from S in a => CONST SetDC (%x. a) S

The following syntax translations are for convenience when using a record as the state type.

**syntax** -assign :: ident => 'a => 's prog (- := - [1000,900]900)

⟨ML⟩

**syntax** -SetPC :: ident => ('s => 'a => real) => 's prog

(choose - at - [66,66]66)

⟨ML⟩

**syntax** -set-dc :: ident => ('s => 'a set) => 's prog (- :∈ - [66,66]66)

⟨ML⟩

These definitions instantiate the embedding as either weakest precondition (True) or weakest liberal precondition (False).

**syntax** -set-dc-UNIV :: ident => 's prog (any - [66,66])

**translations** -set-dc-UNIV x => -set-dc x (%-. CONST UNIV)

**definition** wp :: 's prog => 's trans

**where** wp pr \equiv pr True
**CHAPTER 4. THE PGCL LANGUAGE**

**definition**

\[ \text{wlp} :: \text{'s prog} \Rightarrow \text{'s trans} \]

**where**

\[ \text{wlp pr} \equiv \text{pr False} \]

If-Then-Else as a degenerate probabilistic choice.

**abbreviation**

\[
\text{if-then-else} :: \text{[bool, s prog] \Rightarrow s prog}
\]

**where**

\[ \text{If } P \text{ Then } a \text{ Else } b \equiv a \cdot P \oplus b \]

Syntax for loops

**abbreviation**

\[
\text{do-while} :: \text{[bool, s prog] \Rightarrow s prog}
\]

**where**

\[ \text{do-while } P \ a \equiv \mu x. \text{If } P \text{ Then } a \;;; x \text{ Else Skip} \]

### 4.1.2 Unfolding rules for non-recursive primitives

**lemma** \text{eval-wp-Abort}:

\[ \text{wp Abort } P = (\lambda s. 0) \]

**lemma** \text{eval-wlp-Abort}:

\[ \text{wlp Abort } P = (\lambda s. 1) \]

**lemma** \text{eval-wp-Skip}:

\[ \text{wp Skip } P = P \]

**lemma** \text{eval-wlp-Skip}:

\[ \text{wlp Skip } P = P \]

**lemma** \text{eval-wp-Apply}:

\[ \text{wp } (\text{Apply } f) P = P \circ f \]

**lemma** \text{eval-wlp-Apply}:

\[ \text{wlp } (\text{Apply } f) P = P \circ f \]

**lemma** \text{eval-wp-Seq}:

\[ \text{wp } (a ;; b) P = (\text{wp } a \circ \text{wp } b) P \]
4.1. A SHALLOW EMBEDDING OF PGCL IN HOL

**lemma** eval-wlp-Seq:

\[ \text{wlp} \ (a \ ;; \ b) \ P = (\text{wlp} \ a \ o \ \text{wlp} \ b) \ P \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wp-PC:

\[ \text{wp} \ (a \ Q \oplus \ b) \ P = (\lambda s. \ Q \ s \ast \ \text{wp} \ a \ P \ s + (1 - Q \ s) \ast \ \text{wp} \ b \ P \ s) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wlp-PC:

\[ \text{wlp} \ (a \ Q \oplus \ b) \ P = (\lambda s. \ Q \ s \ast \ \text{wlp} \ a \ P \ s + (1 - Q \ s) \ast \ \text{wlp} \ b \ P \ s) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wp-DC:

\[ \text{wp} \ (a \ \cap \ b) \ P = (\lambda s. \ \min \ (\text{wp} \ a \ P \ s) \ (\text{wp} \ b \ P \ s)) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wlp-DC:

\[ \text{wlp} \ (a \ \cap \ b) \ P = (\lambda s. \ \min \ (\text{wlp} \ a \ P \ s) \ (\text{wlp} \ b \ P \ s)) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wp-AC:

\[ \text{wp} \ (a \ \cup \ b) \ P = (\lambda s. \ \max \ (\text{wp} \ a \ P \ s) \ (\text{wp} \ b \ P \ s)) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wlp-AC:

\[ \text{wlp} \ (a \ \cup \ b) \ P = (\lambda s. \ \max \ (\text{wlp} \ a \ P \ s) \ (\text{wlp} \ b \ P \ s)) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wp-Embed:

\[ \text{wp} \ (\text{Embed} \ t) = t \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wlp-Embed:

\[ \text{wlp} \ (\text{Embed} \ t) = t \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wp-SetDC:

\[ \text{wp} \ (\text{SetDC} \ p \ S) \ R \ s = \text{Inf} \ ((\lambda a. \ \text{wp} \ (p \ a) \ R \ s) \ ; \ S \ s) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wlp-SetDC:

\[ \text{wlp} \ (\text{SetDC} \ p \ S) \ R \ s = \text{Inf} \ ((\lambda a. \ \text{wlp} \ (p \ a) \ R \ s) \ ; \ S \ s) \]

\( \langle \text{proof} \rangle \)

**lemma** eval-wp-SetPC:

\[ \text{wp} \ (\text{SetPC} \ f \ p) \ P = (\lambda s. \ \sum a \in \text{supp} \ (p \ s). \ p \ s \ a \ast \ \text{wp} \ (f \ a) \ P \ s) \]

\( \langle \text{proof} \rangle \)
lemma eval-wlp-SetPC:
\[ \text{wlp} \ (\text{SetPC} \ f \ p) \ P = (\lambda s. \sum a \in \text{supp} \ (p \ s) \cdot p \ s \ a \ast \text{wlp} \ (f \ a) \ P \ s) \]
\<proof\>

lemma eval-wp-Mu:
\[ \text{wp} \ (\mu \ t. \ T \ t) = \text{lfp-trans} \ (\lambda t. \text{wp} \ (T \ (\text{Embed} \ t))) \]
\<proof\>

lemma eval-wlp-Mu:
\[ \text{wlp} \ (\mu \ t. \ T \ t) = \text{gfp-trans} \ (\lambda t. \text{wlp} \ (T \ (\text{Embed} \ t))) \]
\<proof\>

lemma eval-wp-Bind:
\[ \text{wp} \ (\text{Bind} \ g \ f) = (\lambda P \ s. \text{wp} \ (f \ (g \ s)) \ P \ s) \]
\<proof\>

lemma eval-wlp-Bind:
\[ \text{wlp} \ (\text{Bind} \ g \ f) = (\lambda P \ s. \text{wlp} \ (f \ (g \ s)) \ P \ s) \]
\<proof\>

Use simp add:wp_eval to fully unfold a program fragment


lemma Skip-Seq:
\[ \text{Skip} :: A = A \]
\<proof\>

lemma Seq-Skip:
\[ A :: \text{Skip} = A \]
\<proof\>

Use these as simp rules to clear out Skips

lemmas skip-simps = Skip-Seq Seq-Skip

end

4.2 Healthiness

theory Healthiness imports Embedding begin
4.2. HEALTHINESS

4.2.1 The Healthiness of the Embedding

Healthiness is mostly derived by structural induction using the simplifier. *Abort, Skip* and *Apply* form base cases.

**Lemma healthy-wp-Abort:**

```plaintext
healthy (wp Abort)
```

**Lemma nearly-healthy-wlp-Abort:**

```plaintext
nearly-healthy (wlp Abort)
```

**Lemma healthy-wp-Skip:**

```plaintext
healthy (wp Skip)
```

**Lemma nearly-healthy-wlp-Skip:**

```plaintext
nearly-healthy (wlp Skip)
```

**Lemma healthy-wp-Seq:**

```plaintext
fixes t::'s prog and u
assumes ht: healthy (wp t) and hu: healthy (wp u)
shows healthy (wp (t ;; u))
```

**Lemma nearly-healthy-wlp-Seq:**

```plaintext
fixes t::'s prog and u
assumes ht: nearly-healthy (wlp t) and hu: nearly-healthy (wlp u)
shows nearly-healthy (wlp (t ;; u))
```

**Lemma healthy-wp-PC:**

```plaintext
fixes f::'s prog
assumes kf: healthy (wp f) and kg: healthy (wp g)
and uP: unitary P
shows healthy (wp (f ⊕ g))
```

**Lemma nearly-healthy-wlp-PC:**

```plaintext
fixes f::'s prog
assumes kf: nearly-healthy (wlp f) and kg: nearly-healthy (wlp g)
and uP: unitary P
shows nearly-healthy (wlp (f ⊕ g))
```

**Lemma healthy-wp-DC:**

```plaintext
fixes f::'s prog
```
assumes hf: healthy (wp f) and hg: healthy (wp g)
shows healthy (wp (f ∩ g))
⟨proof⟩

lemma nearly-healthy-wlp-DC:
fixes f::'s prog
assumes hf: nearly-healthy (wlp f)
and hg: nearly-healthy (wlp g)
shows nearly-healthy (wlp (f ∩ g))
⟨proof⟩

lemma healthy-wp-AC:
fixes f::'s prog
assumes hf: healthy (wp f) and hg: healthy (wp g)
shows healthy (wp (f ∪ g))
⟨proof⟩

lemma nearly-healthy-wlp-AC:
fixes f::'s prog
assumes hf: nearly-healthy (wlp f)
and hg: nearly-healthy (wlp g)
shows nearly-healthy (wlp (f ∪ g))
⟨proof⟩

lemma healthy-wp-Embed:
healthy t =⇒ healthy (wp (Embed t))
⟨proof⟩

lemma nearly-healthy-wlp-Embed:
nearly-healthy t =⇒ nearly-healthy (wlp (Embed t))
⟨proof⟩

lemma healthy-wp-repeat:
assumes h-a: healthy (wp a)
shows healthy (wp (repeat n a)) (is ?X n)
⟨proof⟩

lemma nearly-healthy-wlp-repeat:
assumes h-a: nearly-healthy (wlp a)
shows nearly-healthy (wlp (repeat n a)) (is ?X n)
⟨proof⟩

lemma healthy-wp-SetDC:
fixes prog::'b ⇒ 'a prog and S::'a ⇒ 'b set
assumes healthy: \(\forall s. \; x \in S \; \Rightarrow \; \text{healthy} \; (\text{wp} \; (\text{prog} \; x))\)
and nonempty: \(\forall s. \; \exists x. \; x \in S \; s\)
shows healthy (wp (SetDC prog S)) (is healthy ?T)
⟨proof⟩
4.2. HEALTHINESS

lemma nearly-healthy-wlp-SetDC:
  fixes prog::'b ⇒ 'a prog and S::'a ⇒ 'b set
  assumes healthy: ℓ ∧ s. x ∈ S s ⇒ nearly-healthy (wlp (prog x))
  and nonempty: ℓ ∧ s. ∃x. x ∈ S s
  shows nearly-healthy (wlp (SetDC prog S)) (is nearly-healthy ?T)
 ⟨proof⟩

lemma healthy-wp-SetPC:
  fixes p::'s ⇒ 'a ⇒ real
  and f::'a ⇒ 's prog
  assumes healthy: ℓ ∧ s. a ∈ supp (p s) ⇒ healthy (wp (f a))
  and sound: ℓ ∧ s. sound (p s)
  and sub-dist: ℓ ∧ s. (∑a∈supp (p s). p s a) ≤ 1
  shows healthy (wp (SetPC f p)) (is healthy ?X)
 ⟨proof⟩

lemma nearly-healthy-wlp-SetPC:
  fixes p::'s ⇒ 'a ⇒ real
  and f::'a ⇒ 's prog
  assumes healthy: ℓ ∧ s. a ∈ supp (p s) ⇒ nearly-healthy (wlp (f a))
  and sound: ℓ ∧ s. sound (p s)
  and sub-dist: ℓ ∧ s. (∑a∈supp (p s). p s a) ≤ 1
  shows nearly-healthy (wlp (SetPC f p)) (is nearly-healthy ?X)
 ⟨proof⟩

lemma healthy-wp-Apply:
  healthy (wp (Apply f))
 ⟨proof⟩

lemma nearly-healthy-wlp-Apply:
  nearly-healthy (wlp (Apply f))
 ⟨proof⟩

lemma healthy-wp-Bind:
  fixes f::'s ⇒ 'a
  assumes hsub: ℓ ∧ s. healthy (wp (p (f s)))
  shows healthy (wp (Bind f p))
 ⟨proof⟩

lemma nearly-healthy-wlp-Bind:
  fixes f::'s ⇒ 'a
  assumes hsub: ℓ ∧ s. nearly-healthy (wlp (p (f s)))
  shows nearly-healthy (wlp (Bind f p))
 ⟨proof⟩

4.2.2 Healthiness for Loops

lemma wp-loop-step-mono:
  fixes t u::'s trans
assumes \( hb: \text{healthy (wp body)} \)
and \( le: \text{le-trans } t \ u \)
and \( ht: \bigwedge P. \text{sound } P \Rightarrow \text{sound } (t \ P) \)
and \( hu: \bigwedge P. \text{sound } P \Rightarrow \text{sound } (u \ P) \)
sows \( le-trans \ (\text{wp } (\text{body };; \text{Embed } t \ « G » \oplus \text{Skip}))) \)
\( (\text{wp } (\text{body };; \text{Embed } u \ « G » \oplus \text{Skip}))) \)

\[ \langle \text{proof} \rangle \]

\begin{align*}
\text{lemma } &\text{wlp-loop-step-mono:} \\
\text{fixes } &t \ u::\text{trans} \\
\text{assumes } &mb: \text{nearly-healthy (wlp body)} \\
\text{and } &le: \text{le-utrans } t \ u \\
\text{and } &ht: \bigwedge P. \text{unitary } P \Rightarrow \text{unitary } (t \ P) \\
\text{and } &hu: \bigwedge P. \text{unitary } P \Rightarrow \text{unitary } (u \ P) \\
sows \ &le-utrans \ (\text{wlp } (\text{body };; \text{Embed } t \ « G » \oplus \text{Skip}))) \\
\text{(wlp } &\text{body };; \text{Embed } u \ « G » \oplus \text{Skip}))) \\
\langle \text{proof} \rangle \\
\end{align*}

For each sound expectation, we have a pre fixed point of the loop body. This lets us use the relevant fixed-point lemmas.

\begin{align*}
\text{lemma } &\text{lfp-loop-fp:} \\
\text{assumes } &hb: \text{healthy (wp body)} \\
\text{and } &sP: \text{sound } P \\
sows \ &\lambda s. «G» \ s * \text{wp body } (\lambda s. \text{bound-of } P) \ s + «N G» \ s * P \ s \vdash \lambda s. \text{bound-of } P \\
\langle \text{proof} \rangle \\
\end{align*}

\begin{align*}
\text{lemma } &\text{lfp-loop-greatest:} \\
\text{fixes } &P::\text{expect} \\
\text{assumes } &hb: \bigwedge R. \lambda s. «G» \ s * \text{wp body } R \ s + «N G» \ s * P \ s \vdash R \Rightarrow \text{sound } R \\
\text{and } &bb: \text{healthy (wp body)} \\
\text{and } &sP: \text{sound } P \\
\text{and } &sQ: \text{sound } Q \\
sows \ &Q \vdash \text{lfp-exp } (\lambda Q s. «G» \ s * \text{wp body } Q \ s + «N G» \ s * P \ s) \\
\langle \text{proof} \rangle \\
\end{align*}

\begin{align*}
\text{lemma } &\text{lfp-loop-sound:} \\
\text{fixes } &P::\text{expect} \\
\text{assumes } &hb: \text{healthy (wp body)} \\
\text{and } &sP: \text{sound } P \\
sows \ &\text{sound } (\text{lfp-exp } (\lambda Q s. «G» \ s * \text{wp body } Q \ s + «N G» \ s * P \ s)) \\
\langle \text{proof} \rangle \\
\end{align*}

\begin{align*}
\text{lemma } &\text{wlp-loop-step-unitary:} \\
\text{fixes } &t \ u::\text{trans} \\
\text{assumes } &hb: \text{nearly-healthy (wlp body)} \\
\text{and } &ht: \bigwedge P. \text{unitary } P \Rightarrow \text{unitary } (t \ P) \\
\text{and } &uP: \text{unitary } P
\end{align*}
4.2. HEALTHINESS

shows unitary (wp \((\text{body} :: \text{Embed } t \leftarrow G \oplus \text{Skip}) \) P)
\langle proof \rangle

lemma wp-loop-step-sound:
fixes \(t u::\)'s trans
assumes \(hb:: \text{healthy (wp body)}\)
and \(ht:: \text{sound } P \implies \text{sound } (t P)\)
and \(sP:: \text{sound } P\)
shows \(\text{sound (wp } (\text{body} :: \text{Embed } t \leftarrow G \oplus \text{Skip}) \) P)\)
\langle proof \rangle

This gives the equivalence with the alternative definition for loops[McIver and Morgan, 2004, §7, p. 198, footnote 23].

lemma wlp-Loop1:
fixes body :: '#s prog
assumes \(sP:: \text{sound } P\)
and \(hb:: \text{healthy (wp body)}\)
shows \(\text{wp } (\text{do } G \rightarrow \text{body od } P) = gfp-exp (\lambda Q s. \langle G \rangle s \ast \text{wp body } Q s + \langle N G \rangle s \ast P s)\)
\(\langle is ?X = gfp-exp (?Y P) \rangle\)
\langle proof \rangle

lemma wp-loop-sound:
assumes \(sP:: \text{sound } P\)
and \(hb:: \text{healthy (wp body)}\)
shows \(\text{sound (wp } (\text{do } G \rightarrow \text{body od } P)\)\)
\langle proof \rangle

Likewise, we can rewrite strict loops.

lemma wp-Loop1:
fixes body :: '#s prog
assumes \(sP:: \text{sound } P\)
and \(hb:: \text{healthy (wp body)}\)
shows \(\text{wp } (\text{do } G \rightarrow \text{body od } P) = \text{lfp-exp } (\lambda Q s. \langle G \rangle s \ast \text{wp body } Q s + \langle N G \rangle s \ast P s)\)
\(\langle is ?X = \text{lfp-exp } (?Y P) \rangle\)
\langle proof \rangle

lemma nearly-healthy-wlp-loop:
fixes body::'#s prog
assumes \(hb:: \text{nearly-healthy (wlp body)}\)
shows \(\text{nearly-healthy } (\text{wlp } (\text{do } G \rightarrow \text{body od}))\)
\langle proof \rangle

We show healthiness by appealing to the properties of expectation fixed points, applied to the alternative loop definition.

lemma healthy-wp-loop:
fixes body::'#s prog
assumes \( h:\text{healthy} (\text{wp} \ \text{body}) \)
shows \( \text{healthy} (\text{wp} \ (\text{do} \ G \rightarrow \text{body} \ \text{od})) \)
⟨proof⟩

Use 'simp add:healthy_intros' or 'blast intro:healthy_intros' as appropriate to discharge healthiness side-conditions for primitive programs automatically.

lemmas healthy-intros =
  healthy-wp-Abort nearly-healthy-wlp-Abort healthy-wp-Skip nearly-healthy-wlp-Skip
  healthy-wp-Seq nearly-healthy-wlp-Seq healthy-wp-PC nearly-healthy-wlp-PC
  healthy-wp-DC nearly-healthy-wlp-DC healthy-wp-AC nearly-healthy-wlp-AC
  healthy-wp-Embed nearly-healthy-wlp-Embed healthy-wp-Apply nearly-healthy-wlp-Apply
  healthy-wp-SetDC nearly-healthy-wlp-SetDC healthy-wp-SetPC nearly-healthy-wlp-SetPC
  healthy-wp-Bind nearly-healthy-wlp-Bind healthy-wp-repeat nearly-healthy-wlp-repeat
  healthy-wp-loop nearly-healthy-wlp-loop
end

4.3 Continuity

theory Continuity imports Healthiness begin

We rely on one additional healthiness property, continuity, which is shown here separately, as its proof relies, in general, on healthiness. It is only relevant when a program appears in an inductive context i.e. inside a loop.

A continuous transformer preserves limits (or the suprema of ascending chains).

definition bd-cts :: ′s trans ⇒ bool
where bd-cts t = (∀ M. (∀ i. (M i ⊢ M (Suc i)) ∧ sound (M i)) →
  (∃ b. ∀ i. bounded-by b (M i)) →
  t (Sup-exp (range M)) = Sup-exp (range (t o M)))

lemma bd-ctsD:

\[ \text{bd-cts t; } (\forall i. M i \vdash M (Suc i); \forall i. \text{sound} (M i); \forall i. \text{bounded-by} b (M i) \rightarrow
  t (\text{Sup-exp} (\text{range} M)) = \text{Sup-exp} (\text{range} (t \circ M))) \]
⟨proof⟩

lemma bd-ctsI:

\[(\forall b. M i \vdash M (Suc i)) \Rightarrow (\forall i. \text{sound} (M i)) \Rightarrow (\forall i. \text{bounded-by} b (M i)) \Rightarrow
  t (\text{Sup-exp} (\text{range} M)) = \text{Sup-exp} (\text{range} (t \circ M))) \Rightarrow \text{bd-cts} t \]
⟨proof⟩

A generalised property for transformers of transformers.

definition bd-cts-tr :: ′s trans ⇒ ′s trans ⇒ bool
where bd-cts-tr T = (∀ M. (∀ i. le-trans (M i) (M (Suc i)) \land \text{feasible} (M i)) →
4.3. CONTINUITY

equiv-trans \left( T \left( \Sup-trans \left( M \cdot \UNIV \right) \right) \left( \Sup-trans \left( \left( T \circ M \right) \cdot \UNIV \right) \right) \right)

lemma bd-cts-trD:
\[ \begin{array}{l}
\begin{array}{l}
\vdash \text{bd-cts tr } T; \ \wedge i. \ le\text{-trans } (M \ i) \ (M \ (\text{Suc } i)) ; \ \wedge i. \ feasible \ (M \ i)
\end{array}
\end{array} \implies
\begin{array}{l}
equiv-trans \left( T \left( \Sup-trans \left( M \cdot \UNIV \right) \right) \left( \Sup-trans \left( \left( T \circ M \right) \cdot \UNIV \right) \right) \right)
\end{array}
\]
\[ \langle \text{proof} \rangle \]

lemma bd-cts-trI:
\[ \begin{array}{l}
\begin{array}{l}
\vdash \wedge i. \ le\text{-trans } (M \ i) \ (M \ (\text{Suc } i)) \implies \wedge i. \ feasible \ (M \ i)
\end{array}
\end{array} \implies
\begin{array}{l}
equiv-trans \left( T \left( \Sup-trans \left( M \cdot \UNIV \right) \right) \left( \Sup-trans \left( \left( T \circ M \right) \cdot \UNIV \right) \right) \right)
\end{array}
\]
\[ \langle \text{proof} \rangle \]

4.3.1 Continuity of Primitives

lemma cts-wp-Abort:
\[ \begin{array}{l}
\text{bd-cts } \left( \wp \left( \text{Abort::'s prog} \right) \right)
\end{array} \]
\[ \langle \text{proof} \rangle \]

lemma cts-wp-Skip:
\[ \begin{array}{l}
\text{bd-cts } \left( \wp \text{ Skip} \right)
\end{array} \]
\[ \langle \text{proof} \rangle \]

lemma cts-wp-Apply:
\[ \begin{array}{l}
\text{bd-cts } \left( \wp \left( \text{Apply } f \right) \right)
\end{array} \]
\[ \langle \text{proof} \rangle \]

lemma cts-wp-Bind:
\[ \begin{array}{l}
\text{fixes } a::'a \Rightarrow 's prog
\end{array} \]
\[ \begin{array}{l}
\text{assumes } ca: \wedge s. \text{ bd-cts } \left( \wp \left( a \ (f \ s) \right) \right)
\end{array} \]
\[ \begin{array}{l}
\text{shows } \text{bd-cts } \left( \wp \left( \text{Bind } f \ a \right) \right)
\end{array} \]
\[ \langle \text{proof} \rangle \]

The first nontrivial proof. We transform the suprema into limits, and appeal to the continuity of the underlying operation (here infimum). This is typical of the remainder of the nonrecursive elements.

lemma cts-wp-DC:
\[ \begin{array}{l}
\text{fixes } a \ b::'s \ prog
\end{array} \]
\[ \begin{array}{l}
\text{assumes } ca: \text{ bd-cts } \left( \wp \ a \right)
\end{array} \]
\[ \begin{array}{l}
\text{and } cb: \text{ bd-cts } \left( \wp \ b \right)
\end{array} \]
\[ \begin{array}{l}
\text{and } ha: \text{ healthy } \left( \wp \ a \right)
\end{array} \]
\[ \begin{array}{l}
\text{and } hb: \text{ healthy } \left( \wp \ b \right)
\end{array} \]
\[ \begin{array}{l}
\text{shows } \text{bd-cts } \left( \wp \left( a \ \bigcap \ b \right) \right)
\end{array} \]
\[ \langle \text{proof} \rangle \]

lemma cts-wp-Seq:
\[ \text{fixes } a \ b::'s \ prog \]
\[ \text{assumes } ca: \text{ bd-cts } \left( \wp \ a \right) \]
and cb: bd-cts (wp b)
and hb: healthy (wp b)
shows bd-cts (wp (a ;; b))

⟨proof⟩

lemma cts-wp-PC:
fixes a b::′s prog
assumes ca: bd-cts (wp a)
and cb: bd-cts (wp b)
and ha: healthy (wp a)
and hb: healthy (wp b)
and up: unitary p
shows bd-cts (wp (PC a p b))
⟨proof⟩

Both set-based choice operators are only continuous for finite sets (probabilistic choice can be extended infinitely, but we have not done so). The proofs for both are inductive, and rely on the above results on binary operators.

lemma SetPC-Bind:
SetPC a p = Bind p (λp. SetPC a (λ-. p))
⟨proof⟩

lemma SetPC-remove:
assumes nz: p x ≠ 0 and n1: p x ≠ 1
and fsupp: finite (supp p)
shows SetPC a (λ-. p) = PC (a x) (λ-. p x) (SetPC a (λ-. dist-remove p x))
⟨proof⟩

lemma cts-bot:
bd-cts (λ(P::′s expect) (s::′s). 0::real)
⟨proof⟩

lemma wp-SetPC-nil:
wp (SetPC a (λs a 0)) = (λP s. 0)
⟨proof⟩

lemma SetPC-sgl:
supp p = {x} ⇒ SetPC a (λ-. p) = (λab P s. p x * a x ab P s)
⟨proof⟩

lemma bd-cts-scale:
fixes a::′s trans
assumes ca: bd-cts a
and ha: healthy a
and nnc: 0 ≤ c
shows bd-cts (λP s. c * a P s)
⟨proof⟩
4.3. CONTINUITY

lemma cts-wp-SetPC-const:
fixes $a ::'a \Rightarrow 's \text{ prog}$
assumes $ca: \forall x. x \in (\text{supp } p) \Rightarrow \text{bd-cts} (wp (a x))$
and $ha: \forall x. x \in (\text{supp } p) \Rightarrow \text{healthy} (wp (a x))$
and $up: \text{unitary } p$
and $sump: \text{setsum } p (\text{supp } p) \leq 1$
and $fsupp: \forall s. \text{finite} (\text{supp } p)$
shows $\text{bd-cts} (wp (\text{SetPC} a (\lambda\cdot p)))$
⟨proof⟩

lemma cts-wp-SetPC:
fixes $a ::'a \Rightarrow 's \text{ prog}$
assumes $ca: \forall s. x \in (\text{supp } p s) \Rightarrow \text{bd-cts} (wp (a x))$
and $ha: \forall s. x \in (\text{supp } p s) \Rightarrow \text{healthy} (wp (a x))$
and $up: \forall s. \text{unitary} (p s)$
and $sump: \forall s. \text{setsum } p s (\text{supp } p s) \leq 1$
and $fsupp: \forall s. \text{finite} (\text{supp } p s)$
shows $\text{bd-cts} (wp (\text{SetPC} a p))$
⟨proof⟩

lemma wp-SetDC-Bind:
$\text{SetDC} a S = \text{Bind } S (\lambda s. \text{SetDC} a (\lambda\cdot S))$
⟨proof⟩

lemma SetDC-finite-insert:
assumes $fS: \forall S. \text{finite } S$
and $neS: S \neq \{\}$
shows $\text{SetDC} a (\lambda\cdot \text{insert } x S) = a x \bigcup \text{SetDC} a (\lambda\cdot S)$
⟨proof⟩

lemma SetDC-singleton:
$\text{SetDC} a (\lambda\cdot \{x\}) = a x$
⟨proof⟩

lemma cts-wp-SetDC-const:
fixes $a ::'a \Rightarrow 's \text{ prog}$
assumes $ca: \exists s. x \in S \Rightarrow \text{bd-cts} (wp (a x))$
and $ha: \exists s. x \in S \Rightarrow \text{healthy} (wp (a x))$
and $fS: \forall s. \text{finite } S$
and $neS: S \neq \{\}$
shows $\text{bd-cts} (wp (\text{SetDC} a (\lambda\cdot S)))$
⟨proof⟩

lemma cts-wp-SetDC:
fixes $a ::'a \Rightarrow 's \text{ prog}$
assumes $ca: \exists s. x \in S s \Rightarrow \text{bd-cts} (wp (a x))$
and $ha: \exists s. x \in S s \Rightarrow \text{healthy} (wp (a x))$
and $fS: \forall s. \text{finite } (S s)$
and $neS: \forall s. S s \neq \{\}$
shows \( bd-cts \ (wp \ (SetDC \ a \ S)) \)
\langle \text{proof} \rangle

\textbf{lemma} \cts-wp-repeat:
\[ bd-cts \ (wp \ a) \Rightarrow \text{healthy} \ (wp \ a) \Rightarrow bd-cts \ (wp \ \text{repeat} \ n \ a) \]
\langle \text{proof} \rangle

\textbf{lemma} \cts-wp-\Embed:
\[ bd-cts \ t \Rightarrow bd-cts \ (wp \ \Embed \ t) \]
\langle \text{proof} \rangle

\subsection{Continuity of a Single Loop Step}

A single loop iteration is continuous, in the more general sense defined above for transformer transformers.

\textbf{lemma} \cts-wp-loopstep:
\begin{align*}
\text{fixes} & \quad \text{body} :: \mathcal{S} \ \text{prog} \\
\text{assumes} & \quad \text{hb} : \text{healthy} \ (wp \ \text{body}) \\
\text{and} & \quad \text{cb} : bd-cts \ (wp \ \text{body}) \\
\text{shows} & \quad bd-cts-tr \ (\lambda x. \ wp \ (\text{body} \ ; \ \Embed \ x \ « \ G \ » \Skip) \) \ (\text{is} \ bd-cts-tr \ ?F)
\end{align*}
\langle \text{proof} \rangle

\end

\subsection{Continuity and Induction for Loops}

\textbf{theory} \ LoopInduction \ \textbf{imports} \ Healthiness \ Continuity \ \textbf{begin}

Showing continuity for loops requires a stronger induction principle than we have used so far, which in turn relies on the continuity of loops (inductively). Thus, the proofs are intertwined, and broken off from the main set of continuity proofs. This result is also essential in showing the sublinearity of loops.

A loop step is monotonic.

\textbf{lemma} \wp-loop-step-mono-trans:
\begin{align*}
\text{fixes} & \quad \text{body} :: \mathcal{S} \ \text{prog} \\
\text{assumes} & \quad \text{sP} : \text{sound} \ P \\
\text{and} & \quad \text{hb} : \text{healthy} \ (wp \ \text{body}) \\
\text{shows} & \quad \text{mono-trans} \ (\lambda Q \ s. \ wp \ \text{body} \ Q \ s \ + \ « \ N \ G \ » \ s \ * \ P \ s)
\end{align*}
\langle \text{proof} \rangle

We can therefore apply the standard fixed-point lemmas to unfold it:

\textbf{lemma} \lfp-wp-loop-unfold:
\begin{align*}
\text{fixes} & \quad \text{body} :: \mathcal{S} \ \text{prog} \\
\text{assumes} & \quad \text{hb} : \text{healthy} \ (wp \ \text{body}) \\
\text{and} & \quad \text{sP} : \text{sound} \ P
\end{align*}
shows \( \text{lfp-exp} (\lambda Q \ s. \ G \ s \ast \text{wp body} Q \ s + \ N \ G \ s \ast P \ s) = \)
\( (\lambda s. \ G \ s \ast \text{wp body} (\text{lfp-exp} (\lambda Q \ s. \ G \ s \ast \text{wp body} Q \ s + \ N \ G \ s \ast P \ s)) \ s + \ N \ G \ s \ast P \ s) \)

\( \langle \text{proof} \rangle \)

**Lemma wp-loop-step-unitary:**
fixes body::'s prog
assumes hb: healthy (wp body)
\( \text{and} \ uP: \text{unitary P} \) \( \text{and} \ uQ: \text{unitary Q} \)
shows unitary \( (\lambda s. \ G \ s \ast \text{wp body} Q \ s + \ N \ G \ s \ast P \ s) \)

\( \langle \text{proof} \rangle \)

**Lemma lfp-loop-unitary:**
fixes body::'s prog
assumes hb: healthy (wp body)
\( \text{and} \ uP: \text{unitary P} \)
shows unitary \( (\text{lfp-exp} (\lambda Q \ s. \ G \ s \ast \text{wp body} Q \ s + \ N \ G \ s \ast P \ s)) \)

\( \langle \text{proof} \rangle \)

From the lattice structure on transformers, we establish a transfinite induction principle for loops. We use this to show a number of properties, particularly subdistributivity, for loops. This proof follows the pattern of lemma lfp_ordinal_induct in HOL/Inductive.

**Lemma loop-induct:**
fixes body::'s prog
assumes hwp: healthy (wp body)
\( \text{and} \ hwlp: \text{nearly-healthy (wlp body)} \)
\( \text{and} \ Limit: \ W S. [ \forall x \in S. \ P (\text{fst x}); \forall x \in S. \ \text{feasible (fst x)}; \forall x \in S. \forall Q. \ \text{unitary Q} =\rightarrow \text{unitary (snd x Q)} ] \implies \ P (\text{Sup-trans (fst ' S)}) (\text{Inf-utrans (snd ' S)}) \)
\( \text{and} \ IH: \ W t u. [ \forall Q. \ \text{unitary Q} =\rightarrow \text{unitary (u Q)} ] \implies \ P (\text{wp (body :: Embed t ' G} \oplus \text{Skip)} (\text{wlp (body :: Embed u ' G} \oplus \text{Skip))}) \)
\( \text{and} \ P\text{-equiv: \ W t u'. } [ \forall t u; \text{equiv-trans t t'; equiv-utrans a u'} ] \implies P t' \)
\( \text{and} \ P\text{-equiv: \ W t u'. } [ \forall t u; \text{equiv-trans t t'; equiv-utrans a u'} ] \implies P t' \)
we can appeal to various properties of the finite iterates (which will follow by finite induction), which we can then transfer to the limit.

**definition** iterates :: `'s prog ⇒ (nat ⇒ bool) ⇒ nat ⇒ 's trans

where iterates body G i = ((λx. wp (body ;; Embed x « G ⊕ Skip)) ⊕ Skip) ▼ i) (λP s. 0)

**lemma** iterates-0[simp]:

iterates body G 0 = (λP s. 0)

⟨proof⟩

**lemma** iterates-Suc[simp]:

iterates body G (Suc i) = wp (body ;; Embed (iterates body G i) « G ⊕ Skip)

⟨proof⟩

All iterates are healthy.

**lemma** iterates-healthy:

healthy (wp body) ⇒ healthy (iterates body G i)

⟨proof⟩

The iterates are an ascending chain.

**lemma** iterates-increasing:

fixes body :: `'s prog

assumes hb: healthy (wp body)

shows le-trans (iterates body G i) (iterates body G (Suc i))

⟨proof⟩

**lemma** wp-loop-step-bounded:

fixes t::'s trans and Q::'s expect

assumes nQ: nneg Q

and bQ: bounded-by b Q

and ht: healthy t

and hb: healthy (wp body)

shows bounded-by b (wp (body ;; Embed t « G ⊕ Skip) Q)

⟨proof⟩

This is the key result: The loop is equivalent to the supremum of its iterates.

This proof follows the pattern of lemma continuous_lfp in HOL/Library/Continuity.

**lemma** lfp-iterates:

fixes body::'s prog

assumes hb: healthy (wp body)

and cb: bd-cts (wp body)

shows equiv-trans (wp (do G → body od)) (Sup-trans (range (iterates body G)))

(is equiv-trans ?X ?Y)

⟨proof⟩

Therefore, evaluated at a given point (state), the sequence of iterates gives a sequence of real values that converges on that of the loop itself.

**corollary** loop-iterates:
4.5. **SUBLINEARITY**

```
fixes body::'s prog
assumes hb: healthy (wp body)
   and cb: bd-cts (wp body)
   and sP: sound P
shows (λi. iterates body G i P s) -----> wp (do G ----> body od) P s
⟨proof⟩
```

The iterates themselves are all continuous.

**Lemma cts-iterates:**
```
fixes body::'s prog
assumes hb: healthy (wp body)
   and cb: bd-cts (wp body)
shows bd-cts (iterates body G i)
⟨proof⟩
```

Therefore so is the loop itself.

**Lemma cts-wp-loop:**
```
fixes body::'s prog
assumes hb: healthy (wp body)
   and cb: bd-cts (wp body)
shows bd-cts (wp do G ----> body od)
⟨proof⟩
```

**Lemmas cts-intros =**
```
cts-wp-Abort  cts-wp-Skip
cts-wp-Seq    cts-wp-PC
cts-wp-DC     cts-wp-Embed
cts-wp-Apply  cts-wp-SetDC
cts-wp-SetPC   cts-wp-Bind
cts-wp-repeat
```

**4.5 Sublinearity**

**Theory Sublinearity imports** Embedding Healthiness LoopInduction begin

**4.5.1 Nonrecursive Primitives**

Sublinearity of non-recursive programs is generally straightforward, and follows from the algebraic properties of the underlying operations, together with healthiness.

**Lemma sublinear-wp-Skip:**
```
sublinear (wp Skip)
⟨proof⟩
```

**Lemma sublinear-wp-Abort:**
lemma sublinear-wp-Apply:
sublinear (wp (Apply f))
⟨proof⟩

lemma sublinear-wp-Seq:
fixes x::s prog
assumes slx: sublinear (wp x) and sly: sublinear (wp y)
and hx: healthy (wp x) and hy: healthy (wp y)
shows sublinear (wp (x ;; y))
⟨proof⟩

lemma sublinear-wp-PC:
fixes x::s prog
assumes slx: sublinear (wp x) and sly: sublinear (wp y)
and uP: unitary P
shows sublinear (wp (x ⊕ y))
⟨proof⟩

lemma sublinear-wp-DC:
fixes x::s prog
assumes slx: sublinear (wp x) and sly: sublinear (wp y)
shows sublinear (wp (x ∩ y))
⟨proof⟩

As for continuity, we insist on a finite support.

lemma sublinear-wp-SetPC:
fixes p::a ⇒ 's prog
assumes slp: ∃s a. a ∈ supp (P s) ⇒ sublinear (wp (p a))
and sum: ∀s. (∑ a∈supp (P s). P s a) ≤ 1
and nnP: ∀s a. 0 ≤ P s a
and fin: ∃s. finite (supp (P s))
shows sublinear (wp (SetPC p P))
⟨proof⟩

lemma sublinear-wp-SetDC:
fixes p::a ⇒ 's prog
assumes slp: ∃s a. a ∈ S s ⇒ sublinear (wp (p a))
and hp: ∀s a. a ∈ S s ⇒ healthy (wp (p a))
and ne: ∀s. S s ≠ {}
shows sublinear (wp (SetDC p S))
⟨proof⟩

lemma sublinear-wp-Embed:
sublinear t ⇒ sublinear (wp (Embed t))
⟨proof⟩
4.5. **Sublinearity**

**Lemma** sublinear-wp-repeat:

\[
\left[ \text{sublinear } (\text{wp } p); \text{healthy } (\text{wp } p) \right] \implies \text{sublinear } (\text{wp } (\text{repeat } n \ p))
\]

(proof)

**Lemma** sublinear-wp-Bind:

\[
\left[ \bigwedge s. \text{sublinear } (\text{wp } (a (f \ s))) \right] \implies \text{sublinear } (\text{wp } (\text{Bind } a))
\]

(proof)

### 4.5.2 Sublinearity for Loops

We break the proof of sublinearity loops into separate proofs of sub-distributivity and sub-additivity. The first follows by transfinite induction.

**Lemma** sub-distrib-wp-loop:

- **Fixes** body :: ′s prog
- **Assumes** sdb: sub-distrib (wp body)
  - and hb: healthy (wp body)
  - and nhb: nearly-healthy (wlp body)
- **Shows** sub-distrib (wp (do G → body od))

(proof)

For sub-additivity, we again use the limit-of-iterates characterisation. Firstly, all iterates are sublinear:

**Lemma** sublinear-iterates:

- **Assumes** hb: healthy (wp body)
  - and sb: sublinear (wp body)
- **Shows** sublinear (iterates body G i)

(proof)

From this, sub-additivity follows for the limit (i.e. the loop), by appealing to the property at all steps.

**Lemma** sub-add-wp-loop:

- **Fixes** body :: ′s prog
- **Assumes** sb: sublinear (wp body)
  - and cb: bd-cts (wp body)
  - and hwp: healthy (wp body)
- **Shows** sub-add (wp (do G → body od))

(proof)

**Lemma** sublinear-wp-loop:

- **Fixes** body :: ′s prog
- **Assumes** hb: healthy (wp body)
  - and nhb: nearly-healthy (wlp body)
  - and sb: sublinear (wp body)
  - and cb: bd-cts (wp body)
- **Shows** sublinear (wp (do G → body od))

(proof)

**Lemmas** sublinear-intros =
4.6 Determinism

theory Determinism imports WellDefined begin

We provide a set of lemmas for establishing that appropriately restricted programs are fully additive, and maximal in the refinement order. This is particularly useful with data refinement, as it implies correspondence.

4.6.1 Additivity

lemma additive-wp-Abort: additive (wp (Abort))
⟨proof⟩

wlp Abort is not additive.

lemma additive-wp-Skip: additive (wp (Skip))
⟨proof⟩

lemma additive-wp-Apply: additive (wp (Apply f))
⟨proof⟩

lemma additive-wp-Seq: fixes a::s prog
assumes adda: additive (wp a) and addb: additive (wp b) and wb: well-def b
shows additive (wp (a ;; b))
⟨proof⟩

lemma additive-wp-PC: [ additive (wp a); additive (wp b) ] ⇒ additive (wp (a \uparrow b))
4.6. DETERMINISM

DC is not additive.

**Lemma** additive-wp-SetPC:
\[
[ \forall x \ s \ . \ x \in \text{supp} (p \ s) \implies \text{additive } (wp (a \ x)) ; \ \text{finite } (\text{supp} (p \ s))] \implies \\
\text{additive } (wp (\text{SetPC } a \ p))
\]

**Lemma** additive-wp-Bind:
\[
[ \forall x . \text{additive } (wp (a (f \ x))) ] \implies \text{additive } (wp (\text{Bind } f \ a))
\]

**Lemma** additive-wp-Embed:
\[
[ \text{additive } t ] \implies \text{additive } (wp (\text{Embed } t))
\]

**Lemma** additive-wp-repeat:
\[
\text{additive } (wp a) \implies \text{well-def } a \implies \text{additive } (wp (\text{repeat } n \ a))
\]

**Lemmas** fa-intros =
additive-wp-Abort additive-wp-Skip
additive-wp-Apply additive-wp-Seq
additive-wp-PC additive-wp-SetPC
additive-wp-Bind additive-wp-Embed
additive-wp-repeat

4.6.2 Maximality

**Lemma** max-wp-Skip:
\[
\text{maximal } (wp \ Skip)
\]

**Lemma** max-wp-Apply:
\[
\text{maximal } (wp (\text{Apply } f))
\]

**Lemma** max-wp-Seq:
\[
[ \text{maximal } (wp a) ; \text{maximal } (wp b) ] \implies \text{maximal } (wp (a ; ; b))
\]

**Lemma** max-wp-PC:
\[
[ \text{maximal } (wp a) ; \text{maximal } (wp b) ] \implies \text{maximal } (wp (a \ P \oplus b))
\]

**Lemma** max-wp-DC:
\[
[ \text{maximal } (wp a) ; \text{maximal } (wp b) ] \implies \text{maximal } (wp (a \ P \cap b))
\]
**Lemma** max-wp-SetPC:

\[ \forall s. a \in \text{supp} (P s) \implies \text{maximal} (wp (p a)); \forall s. (\sum_{a \in \text{supp} (P s)} P s a) = 1 \] \implies \text{maximal} (wp (\text{SetPC} p P))

⟨proof⟩

**Lemma** max-wp-SetDC:

fixes p::'a ⇒ 's prog

assumes wp: \( \forall s. a \in S s \implies \text{maximal} (wp (p a)) \)

and ne: \( \forall s. S s \neq \{\} \)

shows \( \text{maximal} (wp (\text{SetDC} p S)) \)

⟨proof⟩

**Lemma** max-wp-Embed:

\( \text{maximal} t \implies \text{maximal} (wp (\text{Embed} t)) \)

⟨proof⟩

**Lemma** max-wp-repeat:

\( \text{maximal} (wp a) \implies \text{maximal} (wp (\text{repeat} n a)) \)

⟨proof⟩

**Lemma** max-wp-Bind:

assumes ma: \( \forall s. \text{maximal} (wp (a (f s))) \)

shows \( \text{maximal} (wp (\text{Bind} f a)) \)

⟨proof⟩

**Lemmas** max-intros =

max-wp-Skip max-wp-Apply
max-wp-Seq max-wp-PC
max-wp-DC max-wp-SetPC
max-wp-SetDC max-wp-Embed
max-wp-Bind max-wp-repeat

A healthy transformer that terminates is maximal.

**Lemma** healthy-term-max:

assumes ht: healthy t

and trm: \( \lambda s. 1 \vdash t \ (\lambda s. 1) \)

shows \( \text{maximal} t \)

⟨proof⟩

### 4.6.3 Determinism

**Lemma** det-wp-Skip:

determ (wp Skip)

⟨proof⟩

**Lemma** det-wp-Apply:

determ (wp (Apply f))

⟨proof⟩
4.7. WELL-DEFINED PROGRAMS.

lemma det-wp-Seq:
\[ \text{determ} (wp \ a) \implies \text{determ} (wp \ b) \implies \text{well-def} \ b \implies \text{determ} (wp (a ;; b)) \]
(proof)

lemma det-wp-PC:
\[ \text{determ} (wp \ a) \implies \text{determ} (wp \ b) \implies \text{determ} (wp (a \oplus b)) \]
(proof)

lemma det-wp-SetPC:
\[ (\forall x \ s. \ x \in \supp(p \ s) \implies \text{determ} (wp (a \ x))) \implies \\
(\forall s. \ \text{finite} (\supp(p \ s)) \implies \\
(\forall s. \ \text{setsum} (p \ s) (\supp(p \ s)) = 1) \implies \\
\text{determ} (wp \ (\text{SetPC} \ a \ p)) \]
(proof)

lemma det-wp-Bind:
\[ (\forall x. \ \text{determ} (wp (a \ (f \ x)))) \implies \text{determ} (wp \ (\text{Bind} f a)) \]
(proof)

lemma det-wp-Embed:
\[ \text{determ} \ t \implies \text{determ} (wp \ (\text{Embed} \ t)) \]
(proof)

lemma det-wp-repeat:
\[ \text{determ} (wp \ a) \implies \text{well-def} \ a \implies \text{determ} (wp \ (\text{repeat} \ n \ a)) \]
(proof)

lemmas determ-intros =
det-wp-Skip det-wp-Apply
det-wp-Seq det-wp-PC
det-wp-SetPC det-wp-Bind
det-wp-Embed det-wp-repeat

end

4.7 Well-Defined Programs.

theory WellDefined imports
    Healthiness
    Sublinearity
    LoopInduction
begin

The definition of a well-defined program collects the various notions of healthiness and well-behavedness that we have so far established: healthiness of the strict and liberal transformers, continuity and sublinearity of the strict transformers, and two new properties. These are that the strict transformer always lies below the liberal one (i.e. that it is at least as \textit{strict},
recalling the standard embedding of a predicate), and that expectation conjunction is distributed between then in a particular manner, which will be crucial in establishing the loop rules.

### 4.7.1 Strict Implies Liberal

This establishes the first connection between the strict and liberal interpretations ($wp$ and $wlp$).

**definition**

\[
wp-under-wlp :: 's prog ⇒ bool
\]

**where**

\[wp-under-wlp prog ≜ ∀ P. unitary P → wp prog P ⊢ wlp prog P\]

**lemma** $wp-under-wlpI[\text{intro}]$:

\[\{ P. unitary P ⇒ wp prog P ⊢ wlp prog P \} ⇒ wp-under-wlp prog\]

**lemma** $wp-under-wlpD[\text{dest}]$:

\[wp-under-wlp prog; unitary P \} ⇒ wp prog P ⊢ wlp prog P\]

**lemma** $wp-under-le-trans$:

\[wp-under-wlp a ⇒ le-utrans (wp a) (wlp a)\]

**lemma** $wp-under-wlp-Abort$:

\[wp-under-wlp Abort\]

**lemma** $wp-under-wlp-Skip$:

\[wp-under-wlp Skip\]

**lemma** $wp-under-wlp-Apply$:

\[wp-under-wlp (Apply f)\]

**lemma** $wp-under-wlp-Seq$:

assumes $h-wlp-a$: nearly-healthy $(wp a)$

and $h-wp-b$: healthy $(wp b)$

and $h-wlp-b$: nearly-healthy $(wlp b)$

and $wp-u-a$: $wp-under-wlp a$

and $wp-u-b$: $wp-under-wlp b$

shows $wp-under-wlp (a ;; b)$

**lemma** $wp-under-wlp-PC$:

assumes $h-wp-a$: healthy $(wp a)$
4.7. WELL-DEFINED PROGRAMS.

and h-wlp-a: nearly-healthy (wlp a)
and h-wp-b: healthy (wp b)
and h-wlp-b: nearly-healthy (wlp b)
and wp-a: wp-under-wlp a
and wp-b: wp-under-wlp b
and uP: unitary P
shows wp-under-wlp (a ⊕ b)

⟨proof⟩

lemma wp-under-wlp-DC:
assumes wp-u-a: wp-under-wlp a
and wp-u-b: wp-under-wlp b
shows wp-under-wlp (a ⊓ b)

⟨proof⟩

lemma wp-under-wlp-SetPC:
assumes wp-u-f: \( \forall s. \ a \in \text{supp}(P \ s) \implies wp-under-wlp(f \ a) \)
and nP: \( \forall s. \ a \in \text{supp}(P \ s) \implies 0 \leq P \ s \ a \)
shows wp-under-wlp (SetPC f P)

⟨proof⟩

lemma wp-under-wlp-SetDC:
assumes wp-u-f: \( \forall s. \ a \in S \ s \implies wp-under-wlp(f \ a) \)
and hf: \( \forall s. \ a \in S \ s \implies \text{healthy}(wp(f \ a)) \)
and nS: \( \forall s. \ S \ s \neq \{\} \)
shows wp-under-wlp (SetDC f S)

⟨proof⟩

lemma wp-under-wlp-Embed:
wp-under-wlp (Embed t)

⟨proof⟩

lemma wp-under-wlp-loop:
fixes body::′s prog
assumes hwp: healthy (wp body)
and hwlp: nearly-healthy (wlp body)
and wp-under: wp-under-wlp body
shows wp-under-wlp (do G → body od)

⟨proof⟩

lemma wp-under-wlp-repeat:
\[ \text{healthy}(wp \ a); \text{nearly-healthy}(wlp \ a); \text{wp-under-wlp} \ a \ \] →
\[ \text{wp-under-wlp} \ (\text{repeat} \ n \ a) \]

⟨proof⟩

lemma wp-under-wlp-Bind:
\[ \forall s. \text{wp-under-wlp} \ (a \ (f \ s)) \] → \[ \text{wp-under-wlp} \ (\text{Bind} \ f \ a) \]

⟨proof⟩
lemmas wp-under-wlp-intros =
  wp-under-wlp-Abort wp-under-wlp-Skip
  wp-under-wlp-Apply wp-under-wlp-Seq
  wp-under-wlp-PC wp-under-wlp-DC
  wp-under-wlp-SetPC wp-under-wlp-SetDC
  wp-under-wlp-Embed wp-under-wlp-loop
  wp-under-wlp-repeat wp-under-wlp-Bind

4.7.2 Sub-Distributivity of Conjunction

definition
  sub-distrib-pconj :: 's prog ⇒ bool
where
  sub-distrib-pconj prog ≡
  ∀ P Q. unitary P → unitary Q →
  wlp prog P &-& wp prog Q ⊢ wp prog (P &-& Q)

lemma sub-distrib-pconjI[intro]:
  \[ \begin{array}{c}
  \forall P Q. \text{unitary } P; \text{unitary } Q \Rightarrow wlp \text{ prog } P \& \& wp \text{ prog } Q \vdash wp \text{ prog } (P \& \& Q)
  \end{array} \]
  sub-distrib-pconj prog
  ⟨proof⟩

lemma sub-distrib-pconjD[dest]:
  P Q. \[ sub-distrib-pconj \text{ prog}; \text{unitary } P; \text{unitary } Q \] \Rightarrow
  wlp \text{ prog } P \& \& wp \text{ prog } Q \vdash wp \text{ prog } (P \& \& Q)
  ⟨proof⟩

lemma sdp-Abort:
  sub-distrib-pconj Abort
  ⟨proof⟩

lemma sdp-Skip:
  sub-distrib-pconj Skip
  ⟨proof⟩

lemma sdp-Seq:
  fixes a and b
  assumes sdp-a: sub-distrib-pconj a
  and sdp-b: sub-distrib-pconj b
  and h-wp-a: healthy (wp a)
  and h-wp-b: healthy (wp b)
  and h-wlp-b: nearly-healthy (wlp b)
  shows sub-distrib-pconj (a ;; b)
  ⟨proof⟩

lemma sdp-Apply:
  sub-distrib-pconj (Apply f)
  ⟨proof⟩
4.7. WELL-DEFINED PROGRAMS.

**Lemma sdp-DC:**

- **Fixes** $a::s$ prog and $b$
- **Assumes** sdp-a: sub-distrib-pconj $a$
  and sdp-b: sub-distrib-pconj $b$
  and h-wp-a: healthy (wp $a$)
  and h-wp-b: healthy (wp $b$)
  and h-wlp-b: nearly-healthy (wlp $b$)
- **Shows** sub-distrib-pconj ($a \land b$)

⟨proof⟩

**Lemma sdp-PC:**

- **Fixes** $a::s$ prog and $b$
- **Assumes** sdp-a: sub-distrib-pconj $a$
  and sdp-b: sub-distrib-pconj $b$
  and h-wp-a: healthy (wp $a$)
  and h-wp-b: healthy (wp $b$)
  and h-wlp-b: nearly-healthy (wlp $b$)
  and $uP$: unitary $P$
- **Shows** sub-distrib-pconj ($aP \oplus b$)

⟨proof⟩

**Lemma sdp-Embed:**

$[\forall P. Q. [\forall unitary P; unitary Q ] \implies tP \land tQ \vdash (P \land Q)] \implies$

sub-distrib-pconj (Embed $t$)

⟨proof⟩

**Lemma sdp-repeat:**

- **Fixes** $a::s$ prog
- **Assumes** sdp: sub-distrib-pconj $a$
  and hw: healthy (wp $a$) and hwlp: nearly-healthy (wlp $a$)
- **Shows** sub-distrib-pconj (repeat $n$ $a$) (is ?X $n$)

⟨proof⟩

**Lemma sdp-SetPC:**

- **Fixes** $p::a \Rightarrow s$ prog
- **Assumes** sdp: $\forall s. a \in supp (P s) \implies$ sub-distrib-pconj ($p a$)
  and fin: $\forall s. finite (supp (P s))$
  and nnp: $\forall s. 0 \leq P s a$
  and sub: $\forall s. setsum (P s) (supp (P s)) \leq 1$
- **Shows** sub-distrib-pconj (SetPC $p P$)

⟨proof⟩

**Lemma sdp-SetDC:**

- **Fixes** $p::a \Rightarrow s$ prog
- **Assumes** sdp: $\forall s. a \in S s \implies$ sub-distrib-pconj ($p a$)
  and hw: $\forall s. a \in S s \implies$ healthy (wp ($p a$))
  and hwlp: $\forall s. a \in S s \implies$ nearly-healthy (wlp ($p a$))
  and nc: $\forall s. S s \neq \{\}$
shows sub-distrib-pconj \(\text{SetDC} p S\)
(\text{proof})

**Lemma** sdp-Bind:
\[
[\forall s. \text{sub-distrib-pconj} (p (f s))] \implies \text{sub-distrib-pconj} (\text{Bind} f p)
\]
(\text{proof})

For loops, we again appeal to our transfinite induction principle, this time taking advantage of the simultaneous treatment of both strict and liberal transformers.

**Lemma** sdp-loop:
fixes body::'s prog
assumes sdp-body: sub-distrib-pconj body and hwlp: nearly-healthy \((\text{wlp body})\) and hwp: healthy \((\text{wp body})\)
shows sub-distrib-pconj \((\text{do G \rightarrow body \ ad})\)
(\text{proof})

**Lemmas** sdp-intros =
sdp-Abort sdp-Skip sdp-Apply
sdp-Seq sdp-DC sdp-PC
sdp-SetPC sdp-SetDC sdp-Embed
sdp-repeat sdp-Bind sdp-loop

### 4.7.3 The Well-Defined Predicate.

**Definition**
well-def :: 's prog \Rightarrow \text{bool}
where
well-def prog \equiv \text{healthy} \((\text{wp prog})\) \land \text{nearly-healthy} \((\text{wlp prog})\)
\land \text{wp-under-wlp prog} \land \text{sub-distrib-pconj prog}
\land \text{sublinear} \((\text{wp prog})\) \land \text{bd-cts} \((\text{wp prog})\)

**Lemma** well-defI[\text{intro}]:
\[
[\text{healthy} \((\text{wp prog})\); \text{nearly-healthy} \((\text{wlp prog})\);
\text{wp-under-wlp prog}; \text{sub-distrib-pconj prog}; \text{sublinear} \((\text{wp prog})\);
\text{bd-cts} \((\text{wp prog})\)] \implies \text{well-def prog}
\]
(\text{proof})

**Lemma** well-def-wp-healthy[\text{dest}]:
well-def prog \implies \text{healthy} \((\text{wp prog})\)
(\text{proof})

**Lemma** well-def-wlp-nearly-healthy[\text{dest}]:
well-def prog \implies \text{nearly-healthy} \((\text{wlp prog})\)
(\text{proof})

**Lemma** well-def-wp-under[\text{dest}]:
4.7. WELL-DEFINED PROGRAMS.

\[ \text{well-def prog} \Rightarrow \text{wp-under-wlp prog} \]
\[ \langle \text{proof} \rangle \]

**Lemma** well-def-sdp\[dest\]:
\[ \text{well-def prog} \Rightarrow \text{sub-distrib-pconj prog} \]
\[ \langle \text{proof} \rangle \]

**Lemma** well-def-wp-sublinear\[dest\]:
\[ \text{well-def prog} \Rightarrow \text{sublinear (wp prog)} \]
\[ \langle \text{proof} \rangle \]

**Lemma** well-def-wp-cts\[dest\]:
\[ \text{well-def prog} \Rightarrow \text{bd-cts (wp prog)} \]
\[ \langle \text{proof} \rangle \]

**Lemmas** wd-dests =
\[ \text{well-def-wp-healthy} \text{ well-def-wlp-nearly-healthy} \]
\[ \text{well-def-wp-under well-def-sdp} \]
\[ \text{well-def-wp-sublinear well-def-wp-cts} \]

**Lemma** wd-Abort:
\[ \text{well-def Abort} \]
\[ \langle \text{proof} \rangle \]

**Lemma** wd-Skip:
\[ \text{well-def Skip} \]
\[ \langle \text{proof} \rangle \]

**Lemma** wd-Apply:
\[ \text{well-def (Apply f)} \]
\[ \langle \text{proof} \rangle \]

**Lemma** wd-Seq:
\[ [ \text{well-def a; well-def b} ] \Rightarrow \text{well-def (a ;; b)} \]
\[ \langle \text{proof} \rangle \]

**Lemma** wd-PC:
\[ [ \text{well-def a; well-def b; unitary P} ] \Rightarrow \text{well-def (a P;; b)} \]
\[ \langle \text{proof} \rangle \]

**Lemma** wd-DC:
\[ [ \text{well-def a; well-def b} ] \Rightarrow \text{well-def (a \phi b)} \]
\[ \langle \text{proof} \rangle \]

**Lemma** wd-SetDC:
\[ [ \forall x s. x \in S s \Rightarrow \text{well-def (a x)); } \forall s. S s \neq {}; \]
\[ \forall s. \text{finite (S s)} ] \Rightarrow \text{well-def (SetDC a S)} \]
\[ \langle \text{proof} \rangle \]
lemma \( \text{wd-SetPC} \):
\[
\left[ \forall x. x \in (\text{supp} (p \ s)) \implies \text{well-def} (a \ x); \ \forall s. \text{unitary} (p \ s); \ \forall s. \text{finite} (\text{supp} (p \ s)); \ \forall s. \text{setsum} (p \ s) (\text{supp} (p \ s)) \leq 1 \right] \implies \text{well-def} (\text{SetPC} a \ p)
\]
\langle \text{proof} \rangle

lemma \( \text{wd-Embed} \):
\[
\text{fixes } t :: \mathcal{S} \ \text{trans}
\]
\[
\text{assumes } ht: \text{healthy} t \text{ and } st: \text{sublinear} t \text{ and } ct: \text{bd-cts} t
\]
\[
\text{shows } \text{well-def} (\text{Embed} t)
\]
\langle \text{proof} \rangle

lemma \( \text{wd-repeat} \):
\[
\text{well-def} a \implies \text{well-def} (\text{repeat} n a)
\]
\langle \text{proof} \rangle

lemma \( \text{wd-Bind} \):
\[
\left[ \forall s. \text{well-def} (a (f \ s)) \right] \implies \text{well-def} (\text{Bind} f a)
\]
\langle \text{proof} \rangle

lemma \( \text{wd-loop} \):
\[
\text{well-def body} \implies \text{well-def} (\text{do} G \rightarrow \text{body} \ od)
\]
\langle \text{proof} \rangle

lemmas \( \text{wd-intros} = \)
\[
\text{wd-Abort} \quad \text{wd-Skip} \quad \text{wd-Apply} \\
\text{wd-Embed} \quad \text{wd-Seq} \quad \text{wd-PC} \\
\text{wd-DC} \quad \text{wd-SetPC} \quad \text{wd-SetDC} \\
\text{wd-Bind} \quad \text{wd-repeat} \quad \text{wd-loop}
\]
end

4.8 The Loop Rules

theory Loops imports WellDefined begin

Given a well-defined body, we can annotate a loop using an invariant, just as in the classical setting.

4.8.1 Liberal and Strict Invariants.

A probabilistic invariant generalises a boolean one: it entails itself, given the loop guard.

definition \( \text{wp-inv} :: ('s \Rightarrow \text{bool}) \Rightarrow 's \text{ prog} \Rightarrow ('s \Rightarrow \text{real}) \Rightarrow \text{bool} \)

where
\[
\text{wp-inv} G \text{ body } I \longleftrightarrow (\forall s. \text{«} G \text{» s } s I \leq \text{wp body } I s)
\]
4.8. THE LOOP RULES

Lemma \( \text{wp-invI} \):
\[ \forall I. (\forall s. \langle \text{G} \rangle s \ast I s \leq \text{wp body I s}) \implies \text{wp-inv G body I} \]
(\text{proof})

definition \( \text{wlp-inv} \):
\[ \text{wlp-inv} :: (\forall s. \langle \text{G} \rangle s \ast I s \leq \text{wp body I s}) \]
where

Lemma \( \text{wlp-invI} \):
\[ \forall I. (\forall s. \langle \text{G} \rangle s \ast I s \leq \text{wp body I s}) \implies \text{wlp-inv G body I} \]
(\text{proof})

Lemma \( \text{wlp-invD} \):
\[ \text{wlp-inv G body I} \implies \langle \text{G} \rangle s \ast I s \leq \text{wp body I s} \]
(\text{proof})

For standard invariants, the multiplication reduces to conjunction.

Lemma \( \text{wp-inv-stdD} \):
\[ \text{assumes inv: wp-inv G body } \langle \text{I} \rangle \]
and \( \text{hb: healthy (wp body)} \)
shows \( \langle \text{G} \rangle \& \& \langle \text{I} \rangle \vdash \text{wp body } \langle \text{I} \rangle \]
(\text{proof})

4.8.2 Partial Correctness


Lemma \( \text{wlp-Loop} \):
\[ \text{assumes wd: well-def body} \]
and \( \text{uI: unitary I} \)
and \( \text{inv: wlp-inv G body I} \)
shows \( I \leq \text{wlp do G } \rightarrow \text{body od } (\lambda s. \langle \text{N} \rangle \text{G} s \ast I s) \)
(is \( I \leq \text{wlp do G } \rightarrow \text{body od } ?P \))
(\text{proof})

4.8.3 Total Correctness

The first total correctness lemma for loops which terminate with probability 1[McIver and Morgan, 2004, Lemma 7.3.1, §7, p. 186].

Lemma \( \text{wp-Loop} \):
\[ \text{assumes wd: well-def body} \]
and \( \text{inv: wlp-inv G body I} \)
and \( \text{unit: unitary I} \)
shows \( I \& \& \text{wp (do G } \rightarrow \text{body od)} (\lambda s. 1) \vdash \text{wp (do G } \rightarrow \text{body od)} (\lambda s. \langle \text{N} \rangle \text{G} s \ast I s) \)
(is \( I \& \& ?T \vdash \text{wp ?loop } ?X \))
(\text{proof})
4.8.4 Unfolding

**Lemma wp-loop-unfold:**

**Fixes** body :: 's prog

**Assumes** sP: sound P

and h: healthy (wp body)

**Shows** wp (do G → body od) P =

\( \lambda s. \langle \text{N} \rangle G' s P s + \langle \text{G} \rangle s w P (wp (do G → body od) P) s \)  

⟨proof⟩

**Lemma wp-loop-nguard:**

[ [ healthy (wp body); sound P; ¬G s ] ] = \[ wp do G → body od P s = P s \]  

⟨proof⟩

**Lemma wp-loop-guard:**

[ [ healthy (wp body); sound P; G s ] ] = \[ wp do G → body od P s = wp (body ;; do G → body od) P s \]  

⟨proof⟩

end

4.9 The Algebra of pGCL

**Theory Algebra imports WellDefined begin**

Programs in pGCL have a rich algebraic structure, largely mirroring that for GCL. We show that programs form a lattice under refinement, with \( a \sqcap b \) and \( a \sqcup b \) as the meet and join operators, respectively. We also take advantage of the algebraic structure to establish a framework for the modular decomposition of proofs.

4.9.1 Program Refinement

Refinement in pGCL relates to refinement in GCL exactly as probabilistic entailment relates to implication. It turns out to have a very similar algebra, the rules of which we establish shortly.

**Definition**

refines :: 's prog ⇒ 's prog ⇒ bool (infix \( \sqsubseteq \))

**Where**

\( \text{prog} \sqsubseteq \text{prog}' \) \( \equiv \forall P. \text{sound } P \rightarrow \text{wp prog } P \vdash \text{wp prog}' \ P \)

**Lemma refinesL[intro]:**

[ \[ \land P. \text{sound } P \rightarrow \text{wp prog } P \vdash \text{wp prog}' \ P \] ] \( \Rightarrow \text{prog} \sqsubseteq \text{prog}' \)  

⟨proof⟩

**Lemma refinesD[dest]:**

[ \[ \text{prog} \sqsubseteq \text{prog}'; \text{sound } P \] ] \( \Rightarrow \text{wp prog } P \vdash \text{wp prog}' \ P \)  

⟨proof⟩
4.9. THE ALGEBRA OF PGCL

The equivalence relation below will turn out to be that induced by refinement. It is also the application of equiv-trans to the weakest precondition.

**Definition**

\[
\text{pequiv} :: \text{‘s prog} \Rightarrow \text{‘s prog} \Rightarrow \text{bool} \quad (\text{infix } \equiv)
\]

**Where**

\[
\text{prog} \equiv \text{prog’} \equiv \forall P. \text{ sound } P \rightarrow \text{ wp prog } P = \text{ wp prog’ } P
\]

**Lemma** pequiv\[\text{intro}]:

\[
[ \Lambda P. \text{ sound } P \rightarrow \text{ wp prog } P = \text{ wp prog’ } P ] \implies \text{ prog } \equiv \text{ prog’}
\]

**Lemma** pequiv\[\text{D}][\text{dest,simp}]:

\[
[ \text{ prog } \equiv \text{ prog’ }; \text{ sound } P ] \implies \text{ wp prog } P = \text{ wp prog’ } P
\]

**Lemma** pequiv-equiv-trans:

\[
a \equiv b \iff \text{ equiv-trans } (\text{ wp } a) (\text{ wp } b)
\]

4.9.2 Simple Identities

The following identities involve only the primitive operations as defined in Section 4.1.1, and refinement as defined above.

**Laws following from the basic arithmetic of the operators separately**

**Lemma** DC-comm[ac-simps]:

\[
a \sqcap b = b \sqcap a
\]

**Lemma** DC-assoc[ac-simps]:

\[
a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c
\]

**Lemma** DC-idem:

\[
a \sqcap a = a
\]

**Lemma** AC-comm[ac-simps]:

\[
a \sqcup b = b \sqcup a
\]

**Lemma** AC-assoc[ac-simps]:

\[
a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c
\]

**Lemma** AC-idem:
a \bigcup a = a
⟨proof⟩

**lemma** PC-quasi-comm:
\[
a p \plug b = b \langle \lambda s. 1 - p \rangle \plug a
\]
⟨proof⟩

**lemma** PC-idem:
\[
a p \plug a = a
\]
⟨proof⟩

**lemma** Seq-assoc[ae-simps]:
\[
A ;; (B ;; C) = A ;; B ;; C
\]
⟨proof⟩

**lemma** Abort-refines[intro]:
well-def a \implies Abort \subseteq a
⟨proof⟩

**Laws relating demonic choice and refinement**

**lemma** left-refines-DC:
\[
(a \cap b) \subseteq a
\]
⟨proof⟩

**lemma** right-refines-DC:
\[
(a \cap b) \subseteq b
\]
⟨proof⟩

**lemma** DC-refines:
fixes a::s prog and b and c
assumes rab: a \subseteq b and rac: a \subseteq c
shows a \subseteq (b \cap c)
⟨proof⟩

**lemma** DC-mono:
fixes a::s prog
assumes rab: a \subseteq b and rcd: c \subseteq d
shows (a \cap c) \subseteq (b \cap d)
⟨proof⟩

**Laws relating angelic choice and refinement**

**lemma** left-refines-AC:
\[
a \subseteq (a \bigcup b)
\]
⟨proof⟩

**lemma** right-refines-AC:
\[
b \subseteq (a \bigcup b)
\]
⟨proof⟩
4.9. THE ALGEBRA OF PGCL

lemma AC-refines:
  fixes a::'s prog and b and c
  assumes rac: a ⊑ c and rbc: b ⊑ c
  shows (a ⨆ b) ⊑ c
⟨proof⟩

lemma AC-mono:
  fixes a::'s prog
  assumes rab: a ⊑ b and rcd: c ⊑ d
  shows (a ⨆ c) ⊑ (b ⨆ d)
⟨proof⟩

Laws depending on the arithmetic of \( a \oplus b \) and \( a \cap b \) together

lemma DC-refines-PC:
  assumes unit: unitary p
  shows (a ⨆ b) ⊑ (a \( \oplus \) b)
⟨proof⟩

Laws depending on the arithmetic of \( a \oplus b \) and \( a \cup b \) together

lemma PC-refines-AC:
  assumes unit: unitary p
  shows (a \( \oplus \) b) ⊑ (a \( \cup \) b)
⟨proof⟩

Laws depending on the arithmetic of \( a \cup b \) and \( a \cap b \) together

lemma DC-refines-AC:
  (a ⨆ b) ⊑ (a \( \cup \) b)
⟨proof⟩

Laws Involving Refinement and Equivalence

lemma pr-trans[trans]:
  fixes A::'a prog
  assumes prAB: A ⊑ B
  and prBC: B ⊑ C
  shows A ⊑ C
⟨proof⟩

lemma pequiv-refl[intro!,simp]:
  a ≃ a
⟨proof⟩

lemma pequiv-comm[ac-simps]:
  a ≃ b \iff b ≃ a
⟨proof⟩
Lemma \texttt{pequiv-pr[dest]}:
\[
a \simeq b \implies a \sqsubseteq b
\]
\langle proof \rangle

Lemma \texttt{pequiv-trans[intro,trans]}:
\[
[ a \simeq b; b \simeq c ] \implies a \simeq c
\]
\langle proof \rangle

Lemma \texttt{pequiv-pr-trans[intro,trans]}:
\[
[ a \simeq b; b \sqsubseteq c ] \implies a \sqsubseteq c
\]
\langle proof \rangle

Lemma \texttt{pr-pequiv-trans[intro,trans]}:
\[
[ a \sqsubseteq b; b \simeq c ] \implies a \sqsubseteq c
\]
\langle proof \rangle

Refinement induces equivalence by antisymmetry:

Lemma \texttt{pequiv-antisym}:
\[
[ a \sqsubseteq b; b \sqsubseteq a ] \implies a \simeq b
\]
\langle proof \rangle

Lemma \texttt{pequiv-DC}:
\[
[ a \simeq c; b \simeq d ] \implies (a \sqcap b) \simeq (c \sqcap d)
\]
\langle proof \rangle

Lemma \texttt{pequiv-AC}:
\[
[ a \simeq c; b \simeq d ] \implies (a \sqcup b) \simeq (c \sqcup d)
\]
\langle proof \rangle

4.9.3 Deterministic Programs are Maximal

Any sub-additive refinement of a deterministic program is in fact an equivalence. Deterministic programs are thus maximal (under the refinement order) among sub-additive programs.

Lemma \texttt{refines-determ}:
\[
\text{fixes } a::'s \text{ prog}
\text{ assumes } da: \text{ determ (wp a)}
\quad \text{and } wa: \text{ well-def a}
\quad \text{and } wb: \text{ well-def b}
\quad \text{and } dr: a \sqsubseteq b
\text{ shows } a \simeq b
\]

Proof by contradiction.

\langle proof \rangle
4.9. **The Algebra of PGCL**

4.9.4 **The Algebraic Structure of Refinement**

Well-defined programs form a half-bounded semilattice under refinement, where \textit{Abort} is bottom, and \( a \sqcup b \) is \textit{inf}. There is no unique top element, but all fully-deterministic programs are maximal.

The type that we construct here is not especially useful, but serves as a convenient way to express this result.

\[
\text{quotient-type } \text{'s program} = \\
\text{'s prog / partial : } \lambda a \; b . \; a \simeq b \land \text{well-def } a \land \text{well-def } b
\]

\[
\text{instantiation } program :: (type) \text{ semilattice-inf begin}\\
\text{lift-definition} \\
\text{less-eq-program} :: \text{'a program } \Rightarrow \text{'a program } \Rightarrow \text{bool is refines}\\
\langle \text{proof} \rangle
\]

\[
\text{lift-definition} \\
\text{less-program} :: \text{'a program } \Rightarrow \text{'a program } \Rightarrow \text{bool} \\
\text{is } \lambda a \; b . \; a \sqsubseteq b \land \neg b \sqsubseteq a\\
\langle \text{proof} \rangle
\]

\[
\text{lift-definition} \\
\text{inf-program} :: \text{'a program } \Rightarrow \text{'a program } \Rightarrow \text{'a program } \text{is DC} \\
\langle \text{proof} \rangle
\]

\[
\text{instance} \\
\langle \text{proof} \rangle \\
\text{end}
\]

\[
\text{instantiation } program :: (type) \text{ bot begin}\\
\text{lift-definition} \\
\text{bot-program} :: \text{'a program is Abort}\\
\langle \text{proof} \rangle
\]

\[
\text{instance} \langle \text{proof} \rangle \\
\text{end}
\]

\[
\text{lemma eq-det}: \forall a \; b . \text{'s prog. } [ \; a \simeq b ; \text{determ (wp a) } ] \implies \text{determ (wp b)}\\
\langle \text{proof} \rangle
\]

\[
\text{lift-definition} \\
\text{pdeterm} :: \text{'s program } \Rightarrow \text{bool} \\
\text{is } \lambda a . \text{determ (wp a)}\\
\langle \text{proof} \rangle
\]

\[
\text{lemma determ-maximal}: \\
[ \; \text{pdeterm } a ; \; a \leq x \; ] \implies a = x\\
\langle \text{proof} \rangle
\]
4.9.5 Data Refinement

A projective data refinement construction for pGCL. By projective, we mean that the abstract state is always a function ($\varphi$) of the concrete state. Refinement may be predicated ($G$) on the state.

**definition**

drefines :: ('b ⇒ 'a) ⇒ ('b ⇒ bool) ⇒ 'a prog ⇒ 'b prog ⇒ bool

**where**

drefines $\varphi$ G A B ≡ ∀ P Q. (unitary P ∧ unitary Q ∧ (P ⊢ wp A Q)) →→

\[
(G) \&\& (P \circ \varphi) \vdash wp B (Q \circ \varphi)
\]

**lemma** drefinesD[dest]:

\[
\begin{aligned}
& \text{assumes } dr: \text{drefines } \varphi \ G A B, \ \text{unitary } P, \ \text{unitary } Q, \ P \vdash wp A Q \ \\
& \text{and } G: \text{G s} \\
& \text{shows } (P \circ \varphi) s \leq wp B (Q \circ \varphi) s
\end{aligned}
\]

⟨proof⟩

We can alternatively use G as an assumption:

**lemma** drefinesD2:

\[
\begin{aligned}
& \text{assumes } dr: \text{drefines } \varphi \ G A B, \ \text{unitary } P, \ \text{unitary } Q, \ P \vdash wp A Q \\
& \text{and } G: \text{G s} \\
& \text{shows } (P \circ \varphi) s \leq wp B (Q \circ \varphi) s
\end{aligned}
\]

⟨proof⟩

This additional form is sometimes useful:

**lemma** drefinesD3:

\[
\begin{aligned}
& \text{assumes } dr: \text{drefines } \varphi \ G a b, \ \text{unitary } P, \ G s \\
& \text{and } uQ: \text{unitary } Q \\
& \text{and } wa: \text{well-def } a \\
& \text{shows } wp a Q (\varphi s) \leq wp b (Q \circ \varphi) s
\end{aligned}
\]

⟨proof⟩

**lemma** drefinesI[intro]:

\[
\begin{aligned}
& \text{assumes } dr: \text{drefines } \varphi \ G A B \\
& \text{and } G: \text{G s} \\
& \text{shows } drefines \varphi \ G A B
\end{aligned}
\]

⟨proof⟩

Use G as an assumption, when showing refinement:

**lemma** drefinesI2:

\[
\begin{aligned}
& \text{fixes } A: \text{'a prog} \\
& \text{and } B: \text{'b prog} \\
& \text{and } \varphi: \text{b ⇒ 'a} \\
& \text{and } G: \text{'b ⇒ bool} \\
& \text{assumes } wB: \text{well-def } B
\end{aligned}
\]
and withAs:
\[ P Q s \mid \text{unitary } P, \text{unitary } Q; \]
\[ G s; P \vdash \text{wp } A Q \] \implies (P o \varphi) s \leq \text{wp } B (Q o \varphi) s
shows drefines \varphi G A B

\text{lemma dr-strengthen-guard:}
\text{fixes } a::'s \text{ prog and } b::'t \text{ prog}
\text{assumes ff: } G s \implies \text{wp } A Q o \varphi = \text{wp } B (Q o \varphi)
\text{and drab: drefines } \varphi G a b
shows drefines \varphi F a b

Probabilistic correspondence, pcorres, is equality on distribution transformers, modulo a guard. It is the analogue, for data refinement, of program equivalence for program refinement.

\text{definition}
pcorres :: ('b => 'a) => ('b => bool) => 'a prog => 'b prog => bool
where
\[ \forall Q. \text{unitary } Q \implies \langle G \rangle \&\& (\text{wp } A Q o \varphi) = \langle G \rangle \&\& \text{wp } B (Q o \varphi) \]

\text{lemma pcorresI:}
\[ \forall Q. \text{unitary } Q \implies \langle G \rangle \&\& (\text{wp } A Q o \varphi) = \langle G \rangle \&\& \text{wp } B (Q o \varphi) \] \implies pcorres \varphi G A B

Often easier to use, as it allows one to assume the precondition.

\text{lemma pcorresI2[intro]:}
\text{fixes } A::'a \text{ prog and } B::'b \text{ prog}
\text{assumes withG: } G s \mid \text{unitary } Q; G s \implies \text{wp } A Q (\varphi s) = \text{wp } B (Q o \varphi) s
\text{and wA: well-def } A
\text{and wB: well-def } B
shows pcorres \varphi G A B

\text{lemma pcorresD:}
\[ \forall Q. \text{unitary } Q \implies \langle G \rangle \&\& (\text{wp } A Q o \varphi) = \langle G \rangle \&\& \text{wp } B (Q o \varphi) \]

Again, easier to use if the precondition is known to hold.

\text{lemma pcorresD2:}
\text{assumes pc: pcorres } \varphi G A B
\text{and uQ: unitary } Q
\text{and wA: well-def } A \text{ and wB: well-def } B
\text{and G: } G s
shows \text{wp } A Q (\varphi s) = \text{wp } B (Q o \varphi) s
4.9.6 The Algebra of Data Refinement

Program refinement implies a trivial data refinement:

**lemma** refines-drefines:
- fixes $a::s$ prog
- assumes $rab: a \subseteq b$ and $wb: well-def b$
- shows $drefines (\lambda s. s) G a b$

**proof**

Data refinement is transitive:

**lemma** dr-trans[trans]:
- fixes $A::a$ prog and $B::b$ prog and $C::c$ prog
- assumes $drAB: drefines \varphi G A B$
- and $drBC: drefines \varphi' G' B C$
- and $Gimp: \forall s. G' s \implies G (\varphi' s)$
- shows $drefines (\varphi \circ \varphi') G' A C$

**proof**

Data refinement composes with program refinement:

**lemma** pr-dr-trans[trans]:
- assumes $prAB: A \sqsubseteq B$
- and $drBC: drefines \varphi G B C$
- shows $drefines \varphi G A C$

**proof**

**lemma** dr-pr-trans:
- assumes $drAB: drefines \varphi G A B$
- assumes $prBC: B \sqsubseteq C$
- shows $drefines \varphi G A C$

**proof**

If the projection $\varphi$ commutes with the transformer, then data refinement is reflexive:

**lemma** dr-refl:
- assumes $wa: well-def a$
- and comm: $\forall Q. unitary Q \implies wp a Q o \varphi \vdash wp a (Q o \varphi)$
- shows $drefines \varphi G a a$

**proof**

Correspondence implies data refinement

**lemma** pcorres-drefine:
- assumes $corres: pcorres \varphi G A C$
- and $wC: well-def C$
- shows $drefines \varphi G A C$

**proof**

Any data refinement of a deterministic program is correspondence. This is the analogous result to that relating program refinement and equivalence.
4.9. THE ALGEBRA OF PGCL

**Lemma** drefines-determ:

- **Fixes**: \( a :: \text{prog} \) and \( b :: \text{\textquotesingle b prog} \)
- **Assumes**: \( da :: \text{determ} (wp \ a) \)
  - and \( wa :: \text{well-def} \ a \)
  - and \( wb :: \text{well-def} \ b \)
  - and \( dr :: \text{drefines} \ \varphi \ G \ a \ b \)
- **Shows**: \( \text{pccores} \ \varphi \ G \ a \ b \)

The proof follows exactly the same form as that for program refinement: Assuming that correspondence doesn't hold, we show that \( wp \ b \) is not feasible, and thus not healthy, contradicting the assumption.

**Proof**

4.9.7 Structural Rules for Correspondence

**Lemma** pccores-Skip:

- \( \text{pccores} \ \varphi \ G \ \text{Skip} \ \text{Skip} \)

Correspondence composes over sequential composition.

**Lemma** pccores-Seq:

- **Fixes**: \( A :: \text{\textquotesingle b prog} \) and \( B :: \text{\textquotesingle c prog} \)
  - and \( C :: \text{\textquotesingle b prog} \) and \( D :: \text{\textquotesingle c prog} \)
  - and \( \varphi :: \text{\textquotesingle c} \Rightarrow \text{\textquotesingle b} \)
- **Assumes**: \( \text{pccores} \ \varphi \ G \ A \ B \)
  - and \( \text{pccores} \ \varphi \ H \ C \ D \)
  - and \( wA :: \text{well-def} \ A \) and \( wB :: \text{well-def} \ B \)
  - and \( wC :: \text{well-def} \ C \) and \( wD :: \text{well-def} \ D \)
  - and \( p3p2 :: \bigwedge Q \rightarrow \text{unitary} \ Q \Rightarrow \text{\textquotesingle I} \) \&\& \( wp \ B \ Q = wp \ B \ (\text{\textquotesingle H} \) \&\& \( Q) \)
  - and \( p1p3 :: \bigwedge s \rightarrow \text{I} \ s \)
- **Shows**: \( \text{pccores} \ \varphi \ G \ (A ; ; C) \ (B ; ; D) \)

**Proof**

4.9.8 Structural Rules for Data Refinement

**Lemma** dr-Skip:

- **Fixes**: \( \varphi :: \text{\textquotesingle c} \Rightarrow \text{\textquotesingle b} \)
- **Shows**: \( \text{drefines} \ \varphi \ G \ \text{Skip} \ \text{Skip} \)

**Lemma** dr-Abort:

- **Fixes**: \( \varphi :: \text{\textquotesingle c} \Rightarrow \text{\textquotesingle b} \)
- **Shows**: \( \text{drefines} \ \varphi \ G \ \text{Abort} \ \text{Abort} \)

**Lemma** dr-Apply:

- **Fixes**: \( \varphi :: \text{\textquotesingle c} \Rightarrow \text{\textquotesingle b} \)
- **Assumes**: \( \text{commutes: f o } \varphi = \varphi \ o g \)
- **Shows**: \( \text{drefines} \ \varphi \ G \ \{ \text{Apply f} \} \ \{ \text{Apply g} \} \)
chapter 4. the pgcl language

\langle proof \rangle

lemma \textit{dr-Seq}:\
\textit{assumes \text{drAB}: \text{drefines } \varphi \text{ P A B}}\
\text{and \text{drBC}: \text{drefines } \varphi \text{ Q C D}}\
\text{and \text{wpB}: «P» \vdash \text{wp B «Q»}}\
\text{and \text{wB: well-def B}}\
\text{and \text{wC: well-def C}}\
\text{and \text{wD: well-def D}}\
\text{shows \text{drefines } \varphi \text{ P (A;; C) (B;; D)}}

\langle proof \rangle

end

4.10 Structured Reasoning

theory StructuredReasoning imports Algebra begin

By linking the algebraic, the syntactic, and the semantic views of computation, we derive a set of rules for decomposing expectation entailment proofs, firstly over the syntactic structure of a program, and secondly over the refinement relation. These rules also form the basis for automated reasoning.

4.10.1 Syntactic Decomposition

lemma \textit{wp-Abort}:\
\text{(\lambda s. 0) \vdash \text{wp Abort Q}}

\langle proof \rangle

lemma \textit{wlp-Abort}:\
\text{(\lambda s. 1) \vdash \text{wlp Abort Q}}

\langle proof \rangle

lemma \textit{wp-Skip}:\
\text{P \vdash \text{wp Skip P}}

\langle proof \rangle

lemma \textit{wlp-Skip}:\
\text{P \vdash \text{wlp Skip P}}
4.10. STRUCTURED REASONING

lemma \textit{wp-Apply}:
\[ Q \circ f \vdash wp (\text{Apply } f) \ Q \]

lemma \textit{wlp-Apply}:
\[ Q \circ f \vdash wlp (\text{Apply } f) \ Q \]

lemma \textit{wp-Seq}:
\begin{align*}
\text{assumes } & \text{ent-a: } P \vdash wp a \ Q \\
& \text{ent-b: } Q \vdash wp b \ R \\
& \text{wa: } \text{well-def } a \\
& \text{wb: } \text{well-def } b \\
& \text{s-Q: } \text{sound } Q \\
& \text{s-R: } \text{sound } R \\
\text{shows } & P \vdash wp (a \ ; ; b) \ R
\end{align*}

lemma \textit{wlp-Seq}:
\begin{align*}
\text{assumes } & \text{ent-a: } P \vdash wlp a \ Q \\
& \text{ent-b: } Q \vdash wlp b \ R \\
& \text{wa: } \text{well-def } a \\
& \text{wb: } \text{well-def } b \\
& \text{u-Q: } \text{unitary } Q \\
& \text{u-R: } \text{unitary } R \\
\text{shows } & P \vdash wlp (a \ ; ; b) \ R
\end{align*}

lemma \textit{wp-PC}:
\[ (\lambda s. \ P \ s \cdot wp a \ Q \ s + (1 - P \ s) \cdot wp b \ Q \ s) \vdash wp (a \ p \oplus b) \ Q \]

lemma \textit{wlp-PC}:
\[ (\lambda s. \ P \ s \cdot wlp a \ Q \ s + (1 - P \ s) \cdot wlp b \ Q \ s) \vdash wlp (a \ p \oplus b) \ Q \]

A simpler rule for when the probability does not depend on the state.

lemma \textit{PC-fixed}:
\begin{align*}
\text{assumes } & \text{wpa: } P \vdash a \ ab \ R \\
& \text{wpb: } Q \vdash b \ ab \ R \\
& \text{np: } 0 \leq p \ \text{and} \ bp: p \leq 1 \\
\text{shows } & (\lambda s. \ p \ s + (1 - p) \ s) \vdash (a \ (\lambda s. \ p) \oplus b) \ ab \ R
\end{align*}

lemma \textit{wp-PC-fixed}:
\[ [ \ P \vdash wp a \ R; \ Q \vdash wp b \ R; \ 0 \leq p; \ p \leq 1 ] \implies \]
\[ (\lambda s. \ p \ s + (1 - p) \ s) \vdash wp (a \ (\lambda s. \ p) \oplus b) \ R \]
CHAPTER 4. THE PGCL LANGUAGE

(\text{proof})

\textbf{lemma} \ wlp-PC-fixed:  
\[(\lambda s. p \cdot P s + (1 - p) \cdot Q s) \vdash wlp (a (\lambda s. p) \oplus b) R \]
(\text{proof})

\textbf{lemma} \ wp-DC:  
\[(\lambda s. \min (wp a Q s) (wp b Q s)) \vdash wp (a \sqcap b) Q \]
(\text{proof})

\textbf{lemma} \ wlp-DC:  
\[(\lambda s. \min (wlp a Q s) (wlp b Q s)) \vdash wlp (a \sqcap b) Q \]
(\text{proof})

Combining annotations for both branches:

\textbf{lemma} \ DC-split:  
\texttt{fixes} \ a :: 's prog \texttt{and} \ b  
\texttt{assumes} \ wp_a: P \vdash a \ ab R  
\texttt{and} \ wp_b: Q \vdash b \ ab R  
\texttt{shows} \ (\lambda s. \min (P s) (Q s)) \vdash (a \sqcap b) \ ab R  
(\text{proof})

\textbf{lemma} \ wp-DC-split:  
\[(P \vdash wp \ prog \ R; Q \vdash wp \ prog' \ R) \implies 
(\lambda s. \min (P s) (Q s)) \vdash wp (prog \sqcap prog') R \]
(\text{proof})

\textbf{lemma} \ wlp-DC-split:  
\[(P \vdash wlp \ prog \ R; Q \vdash wlp \ prog' \ R) \implies 
(\lambda s. \min (P s) (Q s)) \vdash wlp (prog \sqcap prog') R \]
(\text{proof})

\textbf{lemma} \ wp-DC-split-same:  
\[(P \vdash wp \ prog \ Q; P \vdash wp \ prog' \ Q) \implies P \vdash wp (prog \sqcap prog') Q \]
(\text{proof})

\textbf{lemma} \ wlp-DC-split-same:  
\[(P \vdash wlp \ prog \ Q; P \vdash wlp \ prog' \ Q) \implies P \vdash wlp (prog \sqcap prog') Q \]
(\text{proof})

\textbf{lemma} \ \text{SetPC-split}:  
\texttt{fixes} \ f :: 'x \Rightarrow 'y prog  
\texttt{and} \ p :: 'y \Rightarrow 'x \Rightarrow \text{real}  
\texttt{assumes} \ rec: \forall x s. x \in \text{supp} (p s) \implies P x \vdash f x \ ab Q  
\texttt{and} \ nnp: \forall s. \text{nneg} (p s)  
\texttt{shows} \ (\lambda s. \sum x \in \text{supp} (p s). p s x \ast P x s) \vdash \text{SetPC} f p \ ab Q  
(\text{proof})
4.10. STRUCTURED REASONING

\textbf{lemma} \textit{wp-SetPC-split}:

\[ \[ \forall x s. x \in \text{supp} (p s) \implies P x \vdash \text{wp} (f x) Q; \forall s. \text{nneg} (p s) \] \implies \\
(\lambda s. \sum x \in \text{supp} (p s). p s x \ast P x s) \vdash \text{wp} (\text{SetPC} f p) Q \]

(\textit{proof})

\textbf{lemma} \textit{wlp-SetPC-split}:

\[ \[ \forall x s. x \in \text{supp} (p s) \implies P x \vdash \text{wlp} (f x) Q; \forall s. \text{nneg} (p s) \] \implies \\
(\lambda s. \sum x \in \text{supp} (p s). p s x \ast P x s) \vdash \text{wlp} (\text{SetPC} f p) Q \]

(\textit{proof})

\textbf{lemma} \textit{wp-SetDC-split}:

\[ \[ \forall s x. x \in S s \implies P x \vdash \text{wp} (f x) Q; \forall s. S s \neq \{} \] \implies \\
P \vdash \text{wp} (\text{SetDC} f S) Q \]

(\textit{proof})

\textbf{lemma} \textit{wlp-SetDC-split}:

\[ \[ \forall s x. x \in S s \implies P x \vdash \text{wlp} (f x) Q; \forall s. S s \neq \{} \] \implies \\
P \vdash \text{wlp} (\text{SetDC} f S) Q \]

(\textit{proof})

\textbf{lemma} \textit{wp-SetDC}:

\textbf{assumes} wp: \[ \forall s x. x \in S s \implies P x \vdash \text{wp} (f x) Q \]

\textbf{and} \textbf{nc}: \[ \forall s. S s \neq \{} \]

\textbf{and} \textbf{sP}: \[ \forall x. \text{sound} (P x) \]

\textbf{shows} (\lambda s. \text{Inf} ((\lambda x. P x s) \ast S s)) \vdash \text{wp} (\text{SetDC} f S) Q

(\textit{proof})

\textbf{lemma} \textit{wlp-SetDC}:

\textbf{assumes} wp: \[ \forall s x. x \in S s \implies P x \vdash \text{wlp} (f x) Q \]

\textbf{and} \textbf{nc}: \[ \forall s. S s \neq \{} \]

\textbf{and} \textbf{sP}: \[ \forall x. \text{sound} (P x) \]

\textbf{shows} (\lambda s. \text{Inf} ((\lambda x. P x s) \ast S s)) \vdash \text{wlp} (\text{SetDC} f S) Q

(\textit{proof})

\textbf{lemma} \textit{wp-Embed}:

\[ P \vdash t Q \implies P \vdash \text{wp} (\text{Embed} t) Q \]

(\textit{proof})

\textbf{lemma} \textit{wlp-Embed}:

\[ P \vdash t Q \implies P \vdash \text{wlp} (\text{Embed} t) Q \]

(\textit{proof})

\textbf{lemma} \textit{wp-Bind}:

\[ \[ \forall s. P s \leq \text{wp} (a (f s)) Q s \] \implies P \vdash \text{wp} (\text{Bind} f a) Q \]

(\textit{proof})

\textbf{lemma} \textit{wlp-Bind}:

\[ \[ \forall s. P s \leq \text{wlp} (a (f s)) Q s \] \implies P \vdash \text{wlp} (\text{Bind} f a) Q \]

(\textit{proof})
lemma wp-repeat:
\[
[ P \vdash \wp a Q; Q \vdash \wp (\text{repeat } n \ a) \ R; \\
\text{well-def } a; \text{sound } Q; \text{sound } R ] \implies P \vdash \wp (\text{repeat } (\text{Suc } n) \ a) \ R \\
\langle \text{proof} \rangle
\]

lemma wlp-repeat:
\[
[ P \vdash \wlp a Q; Q \vdash \wlp (\text{repeat } n \ a) \ R; \\
\text{well-def } a; \text{unitary } Q; \text{unitary } R ] \implies P \vdash \wlp (\text{repeat } (\text{Suc } n) \ a) \ R \\
\langle \text{proof} \rangle
\]

Note that the loop rules presented in section Section 4.8 are of the same form, and would belong here, had they not already been stated.

The following rules are specialisations of those for general transformers, and are easier for the unifier to match.

lemmas wp-strengthen-post=
entails-strengthen-post[\text{where } t=\wp a \text{ for } a]

lemma wlp-strengthen-post:
P \vdash \wlp a Q \implies \text{nearly-healthy } (\wlp a) \implies \text{unitary } R \implies Q \vdash R \implies \text{unitary } Q \\
\langle \text{proof} \rangle

lemmas wp-weaken-pre=
entails-weaken-pre[\text{where } t=\wp a \text{ for } a]
lemmas wlp-weaken-pre=
entails-weaken-pre[\text{where } t=\wlp a \text{ for } a]

lemmas wp-scale=
entails-scale[\text{where } t=\wp a \text{ for } a, \text{OF - well-def-}wp-\text{healthy}]

4.10.2 Algebraic Decomposition

Refinement is a powerful tool for decomposition, belied by the simplicity of the rule. This is an axiomatic formulation of refinement (all annotations of the \( a \) are annotations of \( b \)), rather than an operational version (all traces of \( b \) are traces of \( a \)).

lemma wp-refines:
\[
[ a \sqsubseteq b; P \vdash \wp a Q; \text{sound } Q ] \implies P \vdash \wp b Q \\
\langle \text{proof} \rangle
\]

lemmas wp-drefines = drefinesD
4.10.3 Hoare triples

The Hoare triple, or validity predicate, is logically equivalent to the weakest-precondition entailment form. The benefit is that it allows us to define transitivity rules for computational (also/finally) reasoning.

**definition**

\[ \text{wp-valid} :: (\forall a \Rightarrow \text{real}) \Rightarrow (\forall a \Rightarrow \text{real}) \Rightarrow \text{bool} \]

**where**

\[ \text{wp-valid} P \text{ prog } Q \equiv P \vdash \text{ wp prog } Q \]

**lemma wp-validI**:

\[ P \vdash \text{ wp prog } Q \Rightarrow \{ P \} \text{ prog } \{ Q \} p \]

**lemma wp-validD**:

\[ \{ P \} \text{ prog } \{ Q \} p \Rightarrow P \vdash \text{ wp prog } Q \]

**lemma valid-Seq**:

\[ \begin{array}{l}
\{ P \} a \{ Q \} p; \{ Q \} b \{ R \} p; \text{ well-def } a; \text{ well-def } b; \text{ sound } Q; \text{ sound } R \\
\{ P \} a ;; b \{ R \} p
\end{array} \]

We make it available to the computational reasoner:

**declare** valid-Seq[trans]

4.11 Loop Termination

**theory** Termination **imports** Embedding StructuredReasoning Loops **begin**

Termination for loops can be shown by classical means (using a variant, or a measure function), or by probabilistic means: We only need that the loop terminates with probability one.

4.11.1 Trivial Termination

A maximal transformer (program) doesn’t affect termination. This is essentially saying that such a program doesn’t abort (or diverge).

**lemma maximal-Seq-term**:

**fixes** r::'s prog and s::'s prog

**assumes** mr: maximal (wp r)

and ws: well-def s

and ts: (\lambda s. 1) \vdash wp s (\lambda s. 1)

**shows** (\lambda s. 1) \vdash wp (r ;; s) (\lambda s. 1)

**(proof)**
From any state where the guard does not hold, a loop terminates in a single step.

**Lemma** `term-onestep`:
- **Assumes** `wb : well-def body`
- **Shows** `\langle \lambda s. 1 \rangle \vdash \vdash \text{wp } G \rightarrow \text{do } G \rightarrow \text{body od } (\lambda s. 1)`

### 4.11.2 Classical Termination

The first non-trivial termination result is quite standard: If we can provide a natural-number-valued measure, that decreases on every iteration, and implies termination on reaching zero, the loop terminates.

**Lemma** `loop-term-nat-measure-noinv`:
- **Fixes** `m :: 's \Rightarrow \text{nat} and body :: 's \text{ prog}`
- **Assumes** `wb : well-def body`
- **Guard** `\forall s. m s = 0 \rightarrow \neg G s`
- **Variant** `\\forall n. \langle \lambda s. m s = \text{Suc } n \rangle \vdash \text{wp body } (\lambda s. m s = n)`
- **Shows** `\langle \lambda s. 1 \rangle \vdash \vdash \text{wp } G \rightarrow \text{do } G \rightarrow \text{body od } (\lambda s. 1)`

This version allows progress to depend on an invariant. Termination is then determined by the invariant’s value in the initial state.

**Lemma** `loop-term-nat-measure`:
- **Fixes** `m :: 's \Rightarrow \text{nat} and body :: 's \text{ prog}`
- **Assumes** `wb : well-def body`
- **Guard** `\forall s. m s = 0 \rightarrow \neg G s`
- **Variant** `\\forall n. \langle \lambda s. m s = \text{Suc } n \rangle \& \langle I \rangle \vdash \vdash \text{wp body } (\lambda s. m s = n) & \langle I \rangle`
- **Inv** `wp-inv G body \langle I \rangle`
- **Shows** `\langle I \rangle \vdash \vdash \text{wp } G \rightarrow \text{do } G \rightarrow \text{body od } (\lambda s. 1)`

### 4.11.3 Probabilistic Termination

Any loop that has a non-zero chance of terminating after each step terminates with probability 1.

**Lemma** `termination-0-1`:
- **Fixes** `body :: 's \text{ prog}`
- **Assumes** `wb : well-def body`
  - The loop terminates in one step with nonzero probability
  - **OneStep** `\langle \lambda s. p \vdash \text{wp body } (\text{N } G) \rangle`
  - **NZP** `0 < p`
- The body is maximal i.e. it terminates absolutely.
  - **MB** `maximal (wp body)`
- **Shows** `\langle \lambda s. 1 \rangle \vdash \vdash \text{wp } G \rightarrow \text{do } G \rightarrow \text{body od } (\lambda s. 1)`

end
4.12 Automated Reasoning

theory Automation imports StructuredReasoning
begin
This theory serves as a container for automated reasoning tactics for pGCL, implemented in ML. At present, there is a basic verification condition generator (VCG).

named-theorems wd
  theorems to automatically establish well-definedness
named-theorems pwp-core
  core probabilistic wp rules, for evaluating primitive terms
named-theorems pwp
  user-supplied probabilistic wp rules
named-theorems pwp
  user-supplied probabilistic wlp rules

end
Additional Material

4.13 Miscellaneous Mathematics

theory Misc imports Real Multivariate-Analysis begin

lemma setsum-UNIV:
  fixes S :: finite set
  assumes complete: \( \forall x. x \notin S \Rightarrow f \ x = 0 \)
  shows \( \text{setsum} \ f \ S = \text{setsum} \ f \ \text{UNIV} \)
{proof}

lemma cInf-mono:
  fixes A :: \text{conditionally-complete-lattice set}
  assumes lower: \( \forall b. b \in B \Rightarrow \exists a \in A. a \leq b \)
  and bounded: \( \forall a. a \in A \Rightarrow c \leq a \)
  and ne: \( B \neq \{\} \)
  shows \( \text{Inf} \ A \leq \text{Inf} \ B \)
{proof}

lemma max-distrib:
  fixes c :: real
  assumes nn: 0 \leq c
  shows \( c \times \max a \ b = \max (c \times a) \ (c \times b) \)
{proof}

lemma mult-div-mono-left:
  fixes c :: real
  assumes nnc: 0 \leq c and nzc: c \neq 0
  and inv: a \leq inverse c \times b
  shows \( c \times a \leq b \)
{proof}

lemma mult-div-mono-right:
  fixes c :: real
  assumes nnc: 0 \leq c and nzc: c \neq 0
  and inv: inverse c \times a \leq b
  shows \( a \leq c \times b \)
{proof}

lemma min-distrib:
  fixes c :: real

{proof}

107
assumes nnc: 0 ≤ c
shows c * min a b = min (c * a) (c * b)
⟨proof⟩

lemma nonempty-witness:
S ≠ { } ⟹ ∃ x. x ∈ S
⟨proof⟩

lemma finite-set-least:
fixes S :: 'a::linorder set
assumes finite: finite S
and ne: S ≠ { }
shows ∃ x∈S. ∀ y ∈ S. x ≤ y
⟨proof⟩

lemma cSup-add:
fixes c :: real
assumes ne: S ≠ { }
and bS: ∀ x. x ∈ S ⟹ x ≤ b
shows Sup S + c = Sup { x + c | x ∈ S }
⟨proof⟩

lemma cSup-mult:
fixes c :: real
assumes ne: S ≠ { }
and bS: ∀ x. x ∈ S ⟹ x ≤ b
and nnc: 0 ≤ c
shows c * Sup S = Sup { c * x | x ∈ S }
⟨proof⟩

lemma closure-contains-Sup:
fixes S :: real set
assumes neS: S ≠ { } and bS: ∀ x∈S. x ≤ B
shows Sup S ∈ closure S
⟨proof⟩

lemma tendsto-min:
fixes x y :: real
assumes ta: a ----> x
and tb: b ----> y
shows (λ i. min (a i) (b i)) ----> min x y
⟨proof⟩

definition supp :: ('s ⇒ real) ⇒ 's set
where supp f = { x. f x ≠ 0 }

definition dist-remove :: ('s ⇒ real) ⇒ 's ⇒ 's ⇒ real
where dist-remove p x = (λ y. if y=x then 0 else p y / (1 - p x))
4.13. MISCELLANEOUS MATHEMATICS

lemma supp-dist-remove:
\[ p \neq 0 \implies p \neq 1 \implies \text{supp} \ (\text{dist}-\text{remove} \ p \ x) = \text{supp} \ p - \{x\} \]
(proof)

lemma supp-empty:
\[ \text{supp} \ f = \{\} \implies f \ x = 0 \]
(proof)

lemma nsupp-zero:
\[ x \notin \text{supp} \ f \implies f \ x = 0 \]
(proof)

lemma setsum-supp:
\[ \text{fixes} \ f :: \ 'a :: \text{finite} \Rightarrow \text{real} \]
\[ \text{shows} \ \text{setsum} \ f \ (\text{supp} \ f) = \text{setsum} \ f \ \text{UNIV} \]
(proof)

4.13.1 Truncated Subtraction

definition tminus :: \text{real} \Rightarrow \text{real} \Rightarrow \text{real} \ (\text{infix} \ominus 60)
where
\[ x \ominus y = \max (x - y) \ 0 \]

lemma minus-le-tminus[intro!,simp]:
\[ a - b \leq a \ominus b \]
(proof)

lemma tminus-cancel-1:
\[ 0 \leq a \implies a + 1 \ominus 1 = a \]
(proof)

lemma tminus-zero-imp-le:
\[ x \ominus y \leq 0 \implies x \leq y \]
(proof)

lemma tminus-zero[simp]:
\[ 0 \leq x \implies x \ominus 0 = x \]
(proof)

lemma tminus-left-mono:
\[ a \leq b \implies a \ominus c \leq b \ominus c \]
(proof)

lemma tminus-less:
\[ [0 \leq a; 0 \leq b] \implies a \ominus b \leq a \]
(proof)

lemma tminus-left-distrib:
assumes nna: 0 ≤ a
shows a * (b ⊙ c) = a * b ⊙ a * c
⟨proof⟩

lemma tminus-le[simp]:
  b ≤ a → a ⊙ b = a − b
⟨proof⟩

lemma tminus-le-alt[simp]:
  a ≤ b → a ⊙ b = 0
⟨proof⟩

lemma tminus-nle[simp]:
  ¬b ≤ a → a ⊙ b = 0
⟨proof⟩

lemma tminus-add-mono:
  (a + b) ⊙ (c + d) ≤ (a ⊙ c) + (b ⊙ d)
⟨proof⟩

lemma tminus-setsum-mono:
  assumes fS: finite S
  shows setsum f S ⊙ setsum g S ≤ setsum (λx. f x ⊙ g x) S
  ⟨is ?X S⟩
  ⟨proof⟩

lemma tminus-nneg[simp,intro]:
  0 ≤ a ⊙ b
⟨proof⟩

lemma tminus-right-antimono:
  assumes clb: c ≤ b
  shows a ⊙ b ≤ a ⊙ c
⟨proof⟩

lemma min-tminus-distrib:
  min a b ⊙ c = min (a ⊙ c) (b ⊙ c)
⟨proof⟩

end
Bibliography


