Contracts for Lazy Functional Languages

Olaf Chitil

University of Kent

From Assertions to Contracts

- specify & dynamically check properties
- more expressive than static types, less effort than verification
- testing with real values

In functional languages assertion application is a partial identity.

```
assert (prop (>= 0)) 42     ⇝  42
assert (prop (>= 0)) (-2)   ⇝  exception
```

Contracts

Systematic use of assertions as contract between a server and a client, separating their responsibilities.

Function contract:

- pre-condition has to be met by caller of the function
- post-condition has to be met by function itself

```
data Formula = Imp Formula Formula | And Formula Formula |
               Or Formula Formula | Not Formula | Atom Char

clausalNF :: Formula -> [[Formula]]

cClausalNF = assert (conjNF & right >-> list (list lit)) clausalNF
```

For Scheme: [Findler & Felleisen: *Contracts for higher-order functions*, ICFP '02]

The Challenge for Lazy Languages

According to
[Deggen, Thiemann, Wehr: *The Interaction of Contracts and Laziness*, PEPM '12]

- meaning preservation and
- completeness

are contradictory:

```
ep = assert (pair (prop (== 0)) true) (loop, 42)
main = print (snd ep)
```

The Challenge for Lazy Languages

According to
[Deggen, Thiemann, Wehr: *The Interaction of Contracts and Laziness*, PEPM '12]

- meaning preservation and
- completeness

are contradictory:

```
ep = assert (pair (prop (== 0)) true) (loop, 42)
main = print (snd ep)
```

My aim: Meaning preservation but weaker completeness.

High Expressiveness Violates Semantics

Old approach

[Chitil & Huch: *Monadic, prompt lazy assertions in Haskell*, APLAS 2007]

is meaning preserving, but

```
let x = assert equal (True,False)
in (fst x, snd x)
```

$\rightsquigarrow$ exception

and

```
(fst (assert equal (True,False)),
 snd (assert equal (True,False)))
```

$\rightsquigarrow$

```
(True,
 False)
```

High Expressiveness Violates Semantics

Old approach

[Chitil & Huch: *Monadic, prompt lazy assertions in Haskell*, APLAS 2007]

is meaning preserving, but

```
let x = assert equal (True,False)   ⇝  (True, error "...")   or
in (fst x, snd x)                       (error "...", False)
```

and

```
(fst (assert equal (True,False)),  ⇝ (True,
 snd (assert equal (True,False)))      False)
```

Hence: First define semantics, then derive an implementation.

Overview

Part I Identify contract axioms, derive an implementation.
[Chitil: *A Semantics for Lazy Assertions*, PEPM '11]

Part II Consider practical problems for a useful contract library.
[Chitil: *Practical Typed Lazy Contracts*, ICFP 2012]

Lazy Contracts ...

... have to work with non-strict functions and infinite data structures.

```
fibs :: [Integer]
fibs = assert nats (0 : 1 : zipWith (+) fibs (tail fibs))
```

Need to consider partial values:

$$
\begin{array}{lcl}
\texttt{assert nats (0:1:}\perp\texttt{)} & \rightsquigarrow & \texttt{0:1:}\perp \\
\texttt{assert nats (0:1:1:}\perp\texttt{)} & \rightsquigarrow & \texttt{0:1:1:}\perp \\
\texttt{assert nats (0:1:1:2:}\perp\texttt{)} & \rightsquigarrow & \texttt{0:1:1:2:}\perp
\end{array}
$$

Any approximation of an acceptable value has to be accepted!

Axioms of Contracts

Write $\langle c \rangle : D \to D$ for semantics of `assert c`.
Domain D is directed complete partial order with $\perp$.

Definition

Acceptance set $[\![c]\!] := \{v \in D \mid \langle c \rangle\ v = v\} \subseteq D$.

Definition

c is lazy contract, if

1. $\langle c \rangle : D \to D$ is a continuous function,
2. c is trustworthy, that is, $\langle c \rangle\ v \in [\![c]\!]$ for any value v, (equivalent: $\langle c \rangle$ is idempotent)
3. $\langle c \rangle$ is a partial identity, that is, $\langle c \rangle\ v \sqsubseteq v$ for any value v, and
4. $[\![c]\!]$ is a lower set.

Contracts and Projections

Definition

A function $p : D \to D$ on a domain D is a projection if it is

- continuous,
- idempotent, and
- a partial identity.

Lemma

c is lazy contract $\Leftrightarrow$ $\langle c \rangle$ is projection and its image is a lower set

cf. [Findler & Blume: *Contracts as pairs of projections*, FLOPS 2006]

Looking for Alternative Axioms

Definition

$$\downarrow\{v\} := \{v' \mid v' \sqsubseteq v\}$$
$$A_v := \downarrow\{v\} \cap A$$

Theorem

$[\![c]\!]_v$ is an ideal (lower & directed)

$$\langle c \rangle\, v = \bigsqcup [\![c]\!]_v$$

Alternative Axioms

Definition

A set $A \subseteq D$ is a lazy domain if

- A is lower,
- A contains the least upper bound of any directed subset, and
- $A_v = \downarrow\{v\} \cap A$ is directed for all values $v \in D$.

Lemma

If c is a lazy assertion, then $[\![c]\!]$ is a lazy domain.

Theorem

If A is a lazy domain, then c with

$$\langle c \rangle\; v := \bigsqcup [\![c]\!]_v$$

is a lazy assertion with $[\![c]\!] = A$.

Basic Contracts: Minimal & Maximal

Definition

$$[\![\texttt{false}]\!] := \{\perp\}$$
$$[\![\texttt{true}]\!] := D$$

Derived contract applications

$$\langle\texttt{false}\rangle\ v = \bigsqcup[\![\texttt{false}]\!]_v = \bigsqcup \downarrow\{v\} \cap \{\perp\} = \bigsqcup\{\perp\} = \perp$$

$$\langle\texttt{true}\rangle\ v = \bigsqcup[\![\texttt{true}]\!]_v = \bigsqcup \downarrow\{v\} \cap D = \bigsqcup \downarrow\{v\} = v$$

Contract Combinators: Conjunction

Definition

$$[\![c \,\&\, d]\!] := [\![c]\!] \cap [\![d]\!]$$

Lemma Conjunction is commutative and associative and has `true` as neutral element.

Lemma (Conjunction equals two contracts)

$$\langle c \,\&\, d \rangle\ v = \langle c \rangle\ (\langle d \rangle\ v)$$

Contract Combinators: Disjunction

Not $[\![c \mid\!> d]\!] := [\![c]\!] \cup [\![d]\!]$
because $[\![c \mid\!> d]\!]_v = (\downarrow\{v\} \cap [\![c]\!]) \cup (\downarrow\{v\} \cap [\![d]\!])$ not directed.

Definition

$$[\![c \mid\!> d]\!] := \bigcap\{Y \mid [\![c]\!] \cup [\![d]\!] \subseteq Y, Y \text{ lazy domain}\}$$

Attention!

$$D = \{\bot, (\bot,\bot), (\texttt{True},\bot), (\texttt{False},\bot), \ldots, (\texttt{False},\texttt{False})\}$$
$$[\![\texttt{fstTrue}]\!] = D \setminus \{(\texttt{False},\bot), (\texttt{False},\texttt{True}), (\texttt{False},\texttt{False})\}$$

$$[\![\texttt{fstTrue |> sndTrue}]\!] = D$$
$$[\![\texttt{(fstTrue \& sndTrue) |> (fstFalse \& sndFalse)}]\!] = D$$

Lemma Disjunction is commutative and associative and has `false` as neutral element.

Bounded Distributive Lattice of Contracts

Lemma (Absorption laws)

$$c \mathbin{\&} (c \mid\!> d) = c$$
$$c \mid\!> (c \mathbin{\&} d) = c$$

Lemma (Distributive laws)

$$c \mid\!> (d \mathbin{\&} e) = (c \mid\!> d) \mathbin{\&} (c \mid\!> e)$$
$$c \mathbin{\&} (d \mid\!> e) = (c \mathbin{\&} d) \mid\!> (c \mathbin{\&} e)$$

Theorem Lazy contracts form a bounded distributive lattice with meet `&`, join `|>`, least element `false` and greatest element `true`. The ordering is the subset-relationship on acceptance sets.

Corollary (Idempotency laws)

$$c \mathbin{\&} c = c$$
$$c \mid\!> c = c$$

No Negation

Let $[\![c]\!] := \{\perp, (\perp, \perp)\}$

$c \,\&\, \neg c = \texttt{false}$ implies $[\![c]\!] \cap [\![\neg c]\!] = \{\perp\}$.

$[\![\neg c]\!]$ must be a lower set.

So $[\![\neg c]\!] = \{\perp\}$.

But then $[\![c \mid\!> \neg c]\!] = [\![c]\!]$.

Contradiction to $c \mid\!> \neg c = \texttt{true}$.

Deriving an Implementation: Primitive Data Types

Flat domain, i.e., $v \sqsubset w$ implies $v = \perp$.

Definition (Acceptance set of Boolean property contract)

$$[\![\texttt{prop}\ \phi]\!] := \{\perp\} \cup \{v \mid \phi\ v = \texttt{True}\}$$

Derive application of contract:

$$\begin{aligned}
\langle \texttt{prop}\ \phi \rangle\ v &= \bigsqcup \downarrow\{v\} \cap [\![\phi]\!] \\
&= \bigsqcup \{\perp, v\} \cap (\{\perp\} \cup \{w \mid \phi\, w = \texttt{True}\}) \\
&= \bigsqcup \{\perp\} \cup (\texttt{if}\ \ \phi\, v\ \ \texttt{then}\ \ \{v\}\ \ \texttt{else}\ \ \{\}) \\
&= \texttt{if}\ \ \phi\ v\ \ \texttt{then}\ \ v\ \ \texttt{else}\ \ \perp
\end{aligned}$$

Note: $\{\perp\} \cup \{v \mid \phi\ v \neq \texttt{False}\}$ as acceptance set is un-implementable.

Primitive Data Types: Conjunction & Disjunction

Expected definitions:

$$\texttt{prop}\ \phi\ \texttt{\&}\ \texttt{prop}\ \psi := \texttt{prop}\ (\lambda x.\phi\, x \wedge \psi\, x)$$

$$\texttt{prop}\ \phi\ \texttt{|>}\ \texttt{prop}\ \psi := \texttt{prop}\ (\lambda x.\phi\, x \vee \psi\, x)$$

Verify they work:

$$[\![\texttt{prop}\ \phi\ \texttt{\&}\ \texttt{prop}\ \psi]\!] = [\![\texttt{prop}\ \phi]\!] \cap [\![\texttt{prop}\ \psi]\!] = \{\bot\} \cup \{v \mid \phi\, v \wedge \psi\, v\}$$

$$\begin{aligned}[\![\texttt{prop}\ \phi\ \texttt{|>}\ \texttt{prop}\ \psi]\!] &= \bigcap\{X \mid [\![\texttt{prop}\ \phi]\!] \cup [\![\texttt{prop}\ \psi]\!] \subseteq X, X \text{ lazy domain}\} \\ &= \bigcap\{X \mid [\![\texttt{prop}\ \phi]\!] \cup [\![\texttt{prop}\ \psi]\!] \subseteq X\} \\ &= [\![\texttt{prop}\ \phi]\!] \cup [\![\texttt{prop}\ \psi]\!] = \{\bot\} \cup \{v \mid \phi\, v \vee \psi\, v\}\end{aligned}$$

Negation is possible:

$$\neg(\texttt{prop}\ \phi) := \texttt{prop}\ (\lambda x.\neg(\phi\ x))$$

Pattern Contracts for Algebraic Data Types

Recall:

```
data Formula = Imp Formula Formula | And Formula Formula |
               Or Formula Formula | Not Formula | Atom Char

clausalNF :: Formula -> [[Formula]]

cClausalNF = assert (conjNF & right >-> list (list lit)) clausalNF
```

So define

```
lit :: Contract Formula
lit = pAtom true |> pNot (pAtom true)

list :: Contract a -> Contract [a]
list c = pNil |> pCons c (list c)
```

Deriving an Implementation: Algebraic Data Types

Definition (Acceptance set for pattern contract)

$$[\![\mathrm{p}C\ c_1 \ldots c_n]\!] := \{\bot\} \cup \{C\ v_1 \ldots v_n \mid v_1 \in [\![c_1]\!] \ldots v_n \in [\![c_n]\!]\}$$

Lemma (Conjunction of constructor assertions)

$$(\mathrm{p}C\ c_1 \ldots c_n)\ \&\ (\mathrm{p}C\ d_1 \ldots d_n) = \mathrm{p}C\ (c_1 \& d_1) \ldots (c_n \& d_n)$$
$$(\mathrm{p}C\ c_1 \ldots c_n)\ \&\ (\mathrm{p}C'\ d_1 \ldots d_n) = \mathtt{false} \qquad \text{if } C \neq C'$$

Lemma (Disjunction of constructor assertions)

$$(\mathrm{p}C\ c_1 \ldots c_n)\ \mathsf{|>}\ (\mathrm{p}C\ d_1 \ldots d_n) = \mathrm{p}C\ (c_1 \mathsf{|>} d_1) \ldots (c_n \mathsf{|>} d_n)$$

Also if $C \neq C'$, then

$$[\![(\mathrm{p}C\ c_1 \ldots c_n)\ \mathsf{|>}\ (\mathrm{p}C'\ d_1 \ldots d_n)]\!] = [\![\mathrm{p}C\ c_1 \ldots c_n]\!] \cup [\![\mathrm{p}C'\ d_1 \ldots d_n]\!]$$

Contract Representation and Application

Representation of constructor contract

$$\mathtt{p}C_1\ \overline{c}_1\ \texttt{|>}\ \mathtt{p}C_2\ \overline{c}_2\ \texttt{|>}\ \ldots\ \texttt{|>}\ \mathtt{p}C_m\ \overline{c}_m$$

where $\{C_1, \ldots, C_m\}$ is subset of all data constructors of the type.

Application of a constructor contract

$$\begin{array}{lcl} \langle \mathtt{p}C_1\,\overline{c}_1\ \texttt{|>}\ \ldots\ \texttt{|>}\,\mathtt{p}C_m\,\overline{c}_m\rangle\ (C\,\overline{v}) & = & \begin{cases} C\ (\langle\overline{c}_j\rangle\,\overline{v}) & \text{if } C = C_j \\ \perp & \text{otherwise} \end{cases} \\ \langle \mathtt{p}C_1\,\overline{c}_1\ \texttt{|>}\ \ldots\ \texttt{|>}\,\mathtt{p}C_m\,\overline{c}_m\rangle\ \ \perp & = & \perp \end{array}$$

Algebraic Data Types

Conjunction

$$
\begin{aligned}
& (\mathtt{p}C_{i_1}\,\overline{c}_{i_1} \mathrel{|\!>} \ldots \mathrel{|\!>} \mathtt{p}C_{i_m}\,\overline{c}_{i_m}) \mathbin{\&} (\mathtt{p}C_{j_1}\,\overline{d}_{j_1} \mathrel{|\!>} \ldots \mathrel{|\!>} \mathtt{p}C_{j_l}\,\overline{d}_{j_l}) \\
= \;& \mathtt{p}C_{k_1}\,(\overline{c}_{k_1} \mathbin{\&} \overline{d}_{k_1}) \mathrel{|\!>} \ldots \mathrel{|\!>} \mathtt{p}C_{k_o}\,(\overline{c}_{k_o} \mathbin{\&} \overline{d}_{k_o})
\end{aligned}
$$

where $\{k_1, \ldots, k_o\} = \{i_1, \ldots, i_m\} \cap \{j_1, \ldots, j_l\}$

Disjunction

$$
\begin{aligned}
& (\mathtt{p}C_{i_1}\,\overline{c}_{i_1} \mathrel{|\!>} \ldots \mathrel{|\!>} \mathtt{p}C_{i_m}\,\overline{c}_{i_m}) \mathrel{|\!>} (\mathtt{p}C_{j_1}\,\overline{d}_{j_1} \mathrel{|\!>} \ldots \mathrel{|\!>} \mathtt{p}C_{j_l}\,\overline{d}_{j_l}) \\
= \;& \mathtt{p}C_{k_1}\,\overline{z}_{k_1} \mathrel{|\!>} \ldots \mathrel{|\!>} \mathtt{p}C_{k_o}\,\overline{z}_{k_o}
\end{aligned}
$$

where $\{k_1, \ldots, k_o\} = \{i_1, \ldots, i_m\} \cup \{j_1, \ldots, j_l\}$

$$
z_{k_s} = \begin{cases} \overline{c}_{k_s} \mathrel{|\!>} \overline{d}_{k_s} & \text{if } k_s \in \{i_1, \ldots, i_m\} \cap \{j_1, \ldots, j_l\} \\ \overline{c}_{k_s} & \text{if } k_s \in \{i_1, \ldots, i_m\} \setminus \{j_1, \ldots, j_l\} \\ \overline{d}_{k_s} & \text{if } k_s \in \{j_1, \ldots, j_l\} \setminus \{i_1, \ldots, i_m\} \end{cases}
$$

What about Function Types?

Function contract $c \texttt{>->} d$

Eager definition of function contract application:

$$\langle c \texttt{>->} d \rangle \, \delta = \lambda x. \langle d \rangle \, (\delta(\langle c \rangle \, x))$$

But

$$[\![c \texttt{>->} d]\!] = \{\delta \mid \langle d \rangle \circ \delta \circ \langle c \rangle = \delta\}$$

is not a lower set!

Maybe need to relax axiom for function types?

From Theory to Practice

Have

- pure Haskell: language semantics unchanged; portable library
- lazy contracts: preserve program meaning

  eager: `assert (list nat) [4,-4] = error "..."`

  lazy: `assert (list nat) [4,-4] = [4, error "..."]`

- a nice algebra of contracts

Still Want

- function type contracts
- simple parametrically polymorphic types

  `(&), (|>) :: Contract a -> Contract a -> Contract a`

- simple data-type dependent code
  - easy to write by hand
  - can be derived automatically
- when violated, a contract provides information beyond blaming

The Contract API

```
type Contract a

assert :: Contract a -> (a -> a)

prop :: Flat a => (a -> Bool) -> Contract a

true  :: Contract a
false :: Contract a

(&)   :: Contract a -> Contract a -> Contract a
(>->) :: Contract a -> Contract b -> Contract (a -> b)

pNil  :: Contract [a]
pCons :: Contract a -> Contract [a] -> Contract [a]
```

Cf. [Hinze, Jeuring & Löh: Typed contracts for functional programming, FLOPS 2006]

A Simple Implementation ...

```
type Contract a = a -> a

assert c = c

prop p x = if p x then x else error "..."

true  = id
false = const (error "...")

c1 & c2       = c2 . c1
pre >-> post = \f -> post . f . pre

pNil []    = []
pNil (_:_) = error "..."

pCons c cs []     = error "..."
pCons c cs (x:xs) = c x : cs xs
```

Cf. [Findler & Felleisen: Contracts for higher-order functions, ICFP 2002]

...with a Problem

We need disjunction of contracts for lazy algebraic data types

```
(|>) :: Contract a -> Contract a -> Contract a
```

for example for

```
nats :: Contract [Int]
nats = pNil |> pCons nat nats
```

Solution

```
type Contract a = a -> Maybe a

assert c x = case c x of
               Just y  -> y
               Nothing -> error "..."

(c1 |> c2) x = case c1 x of
                 Nothing -> c2 x
                 Just y   -> Just y

true x  = Just x
false x = Nothing

...
```

An Algebra of Contracts

Same laws as non-strict `&&` and `||` (not commutative):

$$
\begin{aligned}
\texttt{c}_1 \;\texttt{\&}\; (\texttt{c}_2 \;\texttt{\&}\; \texttt{c}_3) &= (\texttt{c}_1 \;\texttt{\&}\; \texttt{c}_2) \;\texttt{\&}\; \texttt{c}_3 \\
\texttt{true} \;\texttt{\&}\; \texttt{c} &= \texttt{c} \\
\texttt{c} \;\texttt{\&}\; \texttt{true} &= \texttt{c} \\
\texttt{false} \;\texttt{\&}\; \texttt{c} &= \texttt{false} \\
&\ldots
\end{aligned}
$$

For function contracts:

$$
\begin{aligned}
\texttt{true} \;\texttt{>->}\; \texttt{true} &= \texttt{true} \\
\texttt{c}_1 \;\texttt{>->}\; \texttt{false} &= \texttt{c}_2 \;\texttt{>->}\; \texttt{false} \\
(\texttt{c}_1 \texttt{>->} \texttt{c}_2) \;\texttt{\&}\; (\texttt{c}_3 \texttt{>->} \texttt{c}_4) &= (\texttt{c}_3 \;\texttt{\&}\; \texttt{c}_1) \;\texttt{>->}\; (\texttt{c}_2 \;\texttt{\&}\; \texttt{c}_4) \\
(\texttt{c}_1 \texttt{>->} \texttt{c}_2) \;\texttt{|>}\; (\texttt{c}_3 \texttt{>->} \texttt{c}_4) &= \texttt{c}_1 \;\texttt{>->}\; \texttt{c}_2
\end{aligned}
$$

Contracts are Projections

Lemma (Partial identity)

$$\texttt{assert c} \sqsubseteq \texttt{id}$$

Claim (Idempotency)

$$\texttt{assert c . assert c} = \texttt{assert c}$$

Contracts for our Original Example

```
cClausalNF = assert (conjNF & right >-> list (list lit)) clausalNF
```

Contracts:

```
conjNF, disj, lit, atom, right :: Contract Formula

conjNF = pAnd conjNF conjNF |> disj
disj   = pOr disj disj |> lit
lit    = pNot atom |> atom
atom   = pAtom true

right = pImp (right & pNotImp) right |>
        pAnd (right & pNotAnd) right |>
        pOr (right & pNotOr) right |>
        pNot right |> pAtom true
```

No general negation, but negated pattern contracts `pNotImp`, ...

Blaming

Implement like eager contracts: blame server or client.

```
cConst = assert (true >-> false >-> true) const
```

`true`: never blames anybody
`false`: always blames the *client*

Different from [Findler & Blume: *Contracts as pairs of projections*, FLOPS 2006]

Add Witness Tracing

On violation report a *path* of data constructors:

```
*Main> cClausalNF form
[[Atom 'a'],[Atom 'b',Not
*** Exception: Contract at ContractTest.hs:101:3
violated by
((And _ (Or _ (Not {Not _})))->_)
The client is to blame.
```

- Starting point for debugging.
- Blaming can be wrong: The contract may be wrong.

Derive data-type-dependent code

Derive a contract pattern on demand

```
conjNF = $(p 'And) conjNF conjNF |> disj
disj   = $(p 'Or) disj disj |> lit
lit    = $(p 'Not) atom |> atom
atom   = $(p 'Atom) true
```

or declare

```
$(deriveContracts ''Formula)
```

Use Template Haskell; other generic Haskell systems

- introduce a class context (`Data a`)
- cannot handle functions, e.g. inside data structures

Last Slide

Lazy Contracts

- Need lazy pattern combinators (`pCons`) and disjunction (`|>`).
- Pattern assertions similar to algebraic data types; subtypes!
- Laziness restricts expressibility!

Semantics

- Few axioms: continuous, trustworthy, partial identity, lower set.
- Acceptance sets $[\![c]\!]$ are lazy domains, subdomains.
- Algebra of contracts: bounded distributive lattice.

Practice

- `type Contract a = a -> Maybe a`
- Portable library: `hackage.haskell.org/package/Contract`

Future

- Dependent function contracts?
- Contracts to express non-strictness properties?

Example Contracts

A predicate contract:

```
nat :: Contract Int
nat = prop (>= 0)
```

Expressing non-strictness of a function:

```
cLength = assert (list false >-> nat) length

cConst = assert (true >-> false >-> true) const
```

A list is not finite:

```
infinite :: Contract [a]
infinite = pCons true infinite
```