Abstract Interpretations For Free. Introducti

Kevin Backhouse and Roland Backhouse

September 2001

Outline

- Abstract Interpretation
- Theorems For Free
- (Generic) Galois Connections
- Safety is “For Free”
- Discussion

Abstract Interpretation

Abstract interpretation is a technique for approximating the execution behaviour of a computer program.

For example, abstract interpretation aims to answer questions like

is $231 \times 15 \times 44 \times 26 \times 179 \times 182$ even? and

is $231 \times 15 \times 44 \times 26 \times 179 \times 182$ divisible by six?

without performing the multiplications.

NB The examples are *deliberately* simple.

Even

$$231 \times 15 \times 44 \times 26 \times 179 \times 182 \quad \text{is even}$$

$$\equiv$$

$$F \;\vee\; F \;\vee\; T \;\vee\; T \;\vee\; F \;\vee\; T$$

- Interpret each number as true or false depending on whether the number is even or not.
- Interpret multiplication as logical “or”.
- In this case, the result is ***exact***.

Divisible by Six

$231 \times 15 \times 44 \times 26 \times 179 \times 182$ is divisible by six

$\Leftarrow$

$F \vee F \vee F \vee F \vee F \vee F$

- Interpret each number as true or false depending on whether the number is divisible by six or not.
- Interpret multiplication as logical "or".
- In this case, the result is ***safe*** in the sense that a *true* answer can be relied upon.

Abstract interpretations are typically used to give ***safe*** answers to difficult computations.

Theorems-For-Free (Reynolds, Wadler)

Example: the function *fold* has type

$$a \leftarrow List.a \times a \times (a \leftarrow a \times a)$$

for all instances of the type parameter a.

From this type, a "theorem-for-free" is that, for all lists of integers ms and all integers m,

$$even.fold(ms, m, (\times)) \equiv fold(List.even.ms, even.m, (\vee)) \ .$$

Another "theorem-for-free" is that, for all lists of integers ms and all integers m,

$$divbleby6.fold(ms, m, (\times)) \equiv fold(List.divbleby6.ms, divbleby6.m, (\otimes))$$

if there is some "abstract interpretation" $\otimes$ of multiplication such that, for all integers m and n,

$$divbleby6.(m \times n) \equiv divbleby6.m \otimes divbleby6.n \ .$$

But no such function exists.

Relation on Functions

Definition

$$(f,g) \in R \leftarrow S \quad \equiv \quad \langle \forall u,v :: \ (f.u\,,\,g.v) \in R \ \Leftarrow \ (u,v) \in S \rangle$$

In words, f and g map S-related values to R-related values.

$$(fold\,,\,fold) \ \in \ \langle \forall a :: \ a \ \leftarrow \ List.a \times a \times (a \leftarrow a \times a) \rangle \ \ .$$

In particular,

$$(fold\,,\,fold) \quad \in \quad dk \ \leftarrow \ List.dk \times dk \times (dk \leftarrow dk \times dk)$$

where, for all m,

$$dk.m \ \equiv \ k \backslash m \ \ .$$

That is, for all ms, m, $\otimes$, bs, b and $\odot$,

$$dk.fold(ms,m,\otimes) \ = \ fold(bs,b,\odot)$$

$\Leftarrow$

$$bs = List.dk.ms \wedge b = dk.m \wedge \langle \forall m,n :: \ dk.(m \otimes n) \ = \ dk.m \odot dk.n \rangle \ \ .$$

More Examples

Recall

$$(f,g) \in R \leftarrow S \quad \equiv \quad \langle \forall u,v :: \ (f.u\,,\,g.v) \in R \ \Leftarrow \ (u,v) \in S \rangle \ .$$

Example 1:

$$(f,f) \ \in \ \sqsubseteq \leftarrow \preceq \quad \equiv \quad \langle \forall u,v :: \ f.u \sqsubseteq f.v \Leftarrow u \preceq v \rangle \ .$$

Note that, if f and g are monotonic then, after some simplification:

$$(f,g) \ \in \ \sqsubseteq \leftarrow \preceq \quad \equiv \quad \langle \forall u :: \ f.u \sqsubseteq g.u \rangle \ .$$

Thus, $\sqsubseteq \leftarrow \preceq$ is the usual *pointwise-ordering* on monotonic functions.

Example 2: For functions h and k,

$$(f,g) \ \in \ h \leftarrow k^{\cup} \quad \equiv \quad f \ = \ h \bullet g \bullet k \ .$$

Galois Connections And Pair Algebras

We say that the pair of functions $(f\ ,\ f^\sharp)$ is *a Galois connection between the posets $(\mathcal{A}\,,\sqsubseteq)$ and $(\mathcal{B}\,,\preceq)$* if $f \in \mathcal{A} \leftarrow \mathcal{B}$ and $f^\sharp \in \mathcal{B} \leftarrow \mathcal{A}$ and, for all x in $\mathcal{B}$ and all y in $\mathcal{A}$,

$$f.x \sqsubseteq y \quad \equiv \quad x \preceq f^\sharp.y \ .$$

A binary relation R on the posets $(\mathcal{A}\,,\sqsubseteq)$ and $(\mathcal{B}\,,\preceq)$ is called a *pair algebra* if there are functions $f \in \mathcal{A} \leftarrow \mathcal{B}$ and $f^\sharp \in \mathcal{B} \leftarrow \mathcal{A}$ such that, for all x in $\mathcal{B}$ and all y in $\mathcal{A}$,

$$(y,x) \in R \quad \equiv \quad f.x \sqsubseteq y$$

and

$$(y,x) \in R \quad \equiv \quad x \preceq f^\sharp.y \ .$$

Example — Divisible by k

For all (strictly) positive integers k and m and all booleans b,

$$k\backslash m \Leftarrow b \quad \equiv \quad m \;/\; (\textbf{if } b \textbf{ then } k \textbf{ else } 1) \;\; .$$

(Read $k\backslash m$ as "k divides m" and m/k as "m is divisible by k".)

This is a Galois connection between the function $k\backslash$ (denoted by dk earlier) and the function mapping b to **if** b **then** k **else** 1.

The partial orderings are $(Bool\,, \Leftarrow)$ and $(PosInt\,, /)$.

The pair algebra P relates boolean b to positive integer m exactly when $k\backslash m \Leftarrow b$.

$$(b, m) \in P \quad \equiv \quad k\backslash m \Leftarrow b \;\; .$$

Recall

$$(fold\,,\,fold)\ \in\ \langle \forall a{::}\ a\ \leftarrow\ List.a \times a \times (a \leftarrow a \times a)\rangle$$

$$k\backslash m\ \Leftarrow\ b\quad\equiv\quad m\ /\ (\textbf{if}\ b\ \textbf{then}\ k\ \textbf{else}\ 1)\ \ .$$

Define

$$dk.m\ =\ k\backslash m\quad\text{and}\quad kd.b\ =\ \textbf{if}\ b\ \textbf{then}\ k\ \textbf{else}\ 1\ \ .$$

Then

$$dk.m\ \Leftarrow\ b\quad\equiv\quad m\ /\ kd.b\ \ .$$

Extend $(dk\,,\,kd)$ to type of $fold$:

$$DK\quad=\quad dk\ \leftarrow\ List.kd^{\cup}\ \times\ kd^{\cup}\ \times\ (kd^{\cup} \leftarrow dk \times dk)$$

and

$$KD\quad=\quad kd\ \leftarrow\ List.dk^{\cup}\ \times\ dk^{\cup}\ \times\ (dk^{\cup} \leftarrow kd \times kd)\ \ .$$

Extension of Galois adjoints dk and kd

$$DK \;=\; dk \;\leftarrow\; List.kd^{\cup} \times kd^{\cup} \times (kd^{\cup} \leftarrow dk \times dk)$$

$$KD \;=\; kd \;\leftarrow\; List.dk^{\cup} \times dk^{\cup} \times (dk^{\cup} \leftarrow kd \times kd)$$

Theorem The pair $(DK\,,\,KD)$ is a Galois connection between functions of type

$$Bool \;\leftarrow\; List.Bool \times Bool \times (Bool \leftarrow Bool \times Bool)$$

(ordered pointwise by $\Leftarrow$) and functions of type

$$PosInt \;\leftarrow\; List.PosInt \times PosInt \times (PosInt \leftarrow PosInt \times PosInt)$$

(ordered pointwise by $/$).

Recall: pair algebra

$$(b,m) \in P \quad \equiv \quad k\backslash m \Leftarrow b \quad .$$

Equivalently:

$$(b,m) \in P \quad \equiv \quad dk.m \Leftarrow b \quad .$$

Theorem-For-Free obtained by instantiating type parameter a to P

$$(fold\,,\,fold) \quad \in \quad P \;\leftarrow\; List.P \times P \times (P \leftarrow P \times P) \quad .$$

That is, for all ms, m, and monotonic $\otimes$ and $\odot$,

$$dk.fold(ms,m,\otimes) \quad \Leftarrow \quad fold(List.dk.ms\,,\,dk.m\,,\,\odot)$$

$\Leftarrow$

$$\langle \forall m,n{::}\; dk.(m \otimes n) \;\Leftarrow\; dk.m \odot dk.n \rangle \quad .$$

Safety is "For Free"

Given a parametrically polymorphic function f of type $\langle \forall a :: t \rangle$ where $t = u \leftarrow v$ and a collection of Galois connections (abs_a , con_a) between the posets $(\mathcal{A}_a , \sqsubseteq_a)$ and $(\mathcal{B}_a , \preceq_a)$ (one for each type parameter) we

- extend the Galois connection to (abs_t , con_t) between the posets $(\mathcal{A}_t , \sqsubseteq_t)$ and $(\mathcal{B}_t , \preceq_t)$
- extend the corresponding pair algebras P_a to a pair algebra P_t.

Theorem For Free $\quad (f, f) \in P_t$

Our Theorem $\quad \preceq_t \bullet (abs_t)^{\cup} \;\subseteq\; P_t \;\subseteq\; (abs_t)^{\cup} \bullet \sqsubseteq_t$

Safety Corollary $\quad abs_u \bullet f \quad \sqsubseteq_u \leftarrow \preceq_v \quad f \bullet abs_v$

Discussion

- Calculate abstract interpretations.
- Safety “for free”.
- Effectiveness maximised by maximising parametricity.