

# Computational Logic

## Abstract Interpretation of Logic Programs

## Introduction

---

[Material partly from Cousot, Nielson, Gallagher, Sondergaard, Bruynooghe, and others]

- Many CS problems related to program analysis / synthesis
- Prove that some property holds for program  $P$   
(program analysis)
- Alternatively: derive properties which do hold for program  $P$   
(program analysis)
- Given a program  $P$ , generate a program  $P'$  which is
  - ◇ in some way equivalent to  $P$
  - ◇ behaves better than  $P$  w.r.t. some criteria(program analysis / synthesis)
- Standard Approach:
  - ◇ *identify* that some *invariant* holds, and
  - ◇ *specialize* the program for the particular case

## Program Analysis

---

- Frequent in compilers although seldom treated in a formal way:
  - ◇ “code optimization”,
  - ◇ “dead code elimination”,
  - ◇ “code motion”,
  - ◇ ...

[Aho, Ullman 77]

- Often referred to as “dataflow analysis”
- Abstract interpretation provides a formal framework for developing program analysis tools
- Analysis phase + synthesis phase  $\equiv$  Abstract Interpretation + Program Transformation

## What is abstract interpretation?

---

- Consider detecting that one branch will not be taken in:

```
int x, y, z;  y := read(file);  x := y * y;  
if x ≥ 0 then z := 1 else z := 0
```

- ◇ Exhaustive analysis in the standard domain: non-termination
  - ◇ Human reasoning about programs – uses abstractions or approximations: signs, order of magnitude, odd/even, ...
  - ◇ Basic Idea: use *approximate* (generally *finite*) representations of computational objects to make the problem of program dataflow analysis *tractable*
- Abstract interpretation is a formalization of this idea:
    - ◇ define a non-standard semantics which can approximate the *meaning* or *behaviour* of the program in a finite way
    - ◇ expressions are computed over an approximate (abstract) domain rather than the concrete domain (i.e., meaning of operators has to be reconsidered w.r.t. this new domain)

## Comparison to other methods

---

- Very general:  
can be applied to any language with well defined (procedural or declarative) semantics
- Automatic – (vs. proof methods)
- Static – not all possible runs actually tried (vs. model checking)
- Sound – no possible run omitted (vs. debugging)

## Example: integer sign arithmetic

---

- Consider the domain  $D = Z$  (integers)
- and the multiplication operator:  $* : Z^2 \rightarrow Z$
- We define an “abstract domain”:  $D_\alpha = \{[-], [+]\}$

- Abstract multiplication:  $*_\alpha : D_\alpha^2 \rightarrow D_\alpha$  defined by

|            |       |       |
|------------|-------|-------|
| $*_\alpha$ | $[-]$ | $[+]$ |
| $[-]$      | $[+]$ | $[-]$ |
| $[+]$      | $[-]$ | $[+]$ |

- This allows us to reason, for example, that  $y = x^2 = x * x$  is never negative
- Some observations:
  - ◇ The basis is that whenever we have  $z = x * y$  then:  
if  $x, y \in Z$  are approximated by  $x_\alpha, y_\alpha \in D_\alpha$   
then  $z \in Z$  is approximated by  $z_\alpha = x_\alpha *_\alpha y_\alpha$
  - ◇ It is important to formalize this notion of approximation,  
in order to be able to prove an analysis correct
  - ◇ Approximate computation is generally less precise but faster (tradeoff)

## Example: integer sign arithmetic (Contd.)

---

- Again,  $D = \mathbb{Z}$  (integers)
- and:  $*$  :  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$
- Let's define a *more refined* “abstract domain”:  $D'_\alpha = \{[-], [0], [+]\}$

- Abstract multiplication:  $*_\alpha : D'^2_\alpha \rightarrow D'_\alpha$  defined by

| $*_\alpha$ | $[-]$ | $[0]$ | $[+]$ |
|------------|-------|-------|-------|
| $[-]$      | $[+]$ | $[0]$ | $[-]$ |
| $[0]$      | $[0]$ | $[0]$ | $[0]$ |
| $[+]$      | $[-]$ | $[0]$ | $[+]$ |

- This now allows us to reason that  $z = y * (0 * x)$  is zero
- Some observations:
  - ◇ There is a degree of freedom in defining different abstract operators and domains
  - ◇ The minimal requirement is that they be “safe” or “correct”
  - ◇ Different “safe” definitions result in different kinds of analyses

## Example: integer sign arithmetic (Contd.)

- Again  $D = Z$  (integers)
- and the *addition* operator:  $+ : Z^2 \rightarrow Z$
- We cannot use  $D'_\alpha = \{[-], [0], [+]\}$  because we wouldn't know how to represent the result of  $[+] +_\alpha [-]$   
(i.e. our abstract addition would not be closed)
- New element “ $\top$ ” (supremum): approximation of any integer
- New “abstract domain”:  $D''_\alpha = \{[-], [0], [+], \top\}$
- Abstract addition:  $+_\alpha : D''_\alpha{}^2 \rightarrow D''_\alpha$  defined by:

| $+_\alpha$ | $[-]$  | $[0]$  | $[+]$  | $\top$ |
|------------|--------|--------|--------|--------|
| $[-]$      | $[-]$  | $[-]$  | $\top$ | $\top$ |
| $[0]$      | $[-]$  | $[0]$  | $[+]$  | $\top$ |
| $[+]$      | $\top$ | $[+]$  | $[+]$  | $\top$ |
| $\top$     | $\top$ | $\top$ | $\top$ | $\top$ |

...

(alt: )

| $+_\alpha$ | $[-]$  | $[0]$  | $[+]$  | $\top$ |
|------------|--------|--------|--------|--------|
| $[-]$      | $\top$ | $\top$ | $\top$ | $\top$ |
| $[0]$      | $\top$ | $\top$ | $\top$ | $\top$ |
| $[+]$      | $\top$ | $\top$ | $\top$ | $\top$ |
| $\top$     | $\top$ | $\top$ | $\top$ | $\top$ |

- We can now reason that  $z = x^2 + y^2$  is never negative



## Important observations

---

- In addition to the imprecision due to the coarseness of  $D_\alpha$ , the abstract versions of the operations (dependent on  $D_\alpha$ ) may introduce further imprecision
- Thus, the choice of *abstract domain* and the definition of the *abstract operators* are crucial

## Issues in Abstract Interpretation

---

- Required:
  - ◇ Correctness – safe approximations: because most “interesting” properties are undecidable the analysis necessarily has to be approximate. We want to ensure that the analysis is “conservative” and errs on the “safe side”
  - ◇ Termination – compilation should definitely terminate

(note: not always the case in every day program analysis tools!)
- Desirable – “practicality”:
  - ◇ Efficiency – in practice finite analysis time is not enough: finite *and* small
  - ◇ Accuracy – of the collected information: depends on the appropriateness of the abstract domain and the level of detail to which the interpretation procedure mimics the semantics of the language
  - ◇ “Usefulness” – determines which information is worth collecting
- The first two received the most attention initially (understandably)
- Last three recently studied empirically (e.g., for logic programs)

## Safe Approximations

---

- Basic idea in approximation: for some property  $p$  we want to show that

$$\forall x, x \in S \Rightarrow p(x)$$

Alternative: construct a set  $S_a \supseteq S$ , and prove

$$\forall x, x \in S_a \Rightarrow p(x)$$

then,  $S_a$  is a *safe approximation* of  $S$

- Approximation on functions: for some property  $p$  we want to show that

$$\forall x, x \in S \Rightarrow p(F(x))$$

- A function

$$G : S \rightarrow S$$

is a *safe approximation* of  $F$  if

$$\forall x, x \in S, p(G(x)) \Rightarrow p(F(x))$$

## Approximation of the meaning of a program

---

- Let the meaning of a program  $P$  be a mapping  $F_P$  from input to output, input and output values  $\in$  “standard” domain  $D$ :

$$F_P : D \rightarrow D$$

- Let's ‘lift’ this meaning to map sets of inputs to sets of outputs

$$F_P^* : \wp(D) \rightarrow \wp(D)$$

where  $\wp(S)$  denotes the powerset of  $S$ , and

$$F_P^*(S) = \{F_P(x) \mid x \in S\}$$

- A function

$$G : \wp(D) \rightarrow \wp(D)$$

is a *safe approximation* of  $F_P^*$  if

$$\forall S, S \in \wp(D), G(S) \supseteq F_P^*(S)$$

- Properties can be proved using  $G$  instead of  $F_P^*$

## Approximation of the meaning of a program (Contd.)

---

- For some property  $p$  we want to show that  
for some inputs  $S$ ,  $p(F_P^*(S))$
- We show that  
for some inputs  $S_a$ ,  $p(G(S_a))$
- Since  $G(S_a) \supseteq F_P^*(S_a)$   
for some inputs  $S_a$ ,  $p(F_P^*(S_a))$   
(Note: abuse of notation –  $F_P^*$  does not work on abstract values  $S_a$ )
- As long as  $F_P^*$  is monotonic:  
$$S_a \supseteq S \Rightarrow F_P^*(S_a) \supseteq F_P^*(S)$$
- And since  $S_a \supseteq S$ , then:  
for some inputs  $S$ ,  $p(F_P^*(S))$

## Abstract Domain and Concretization Function

---

- The domain  $\wp(D)$  can be represented by an “abstract” domain  $D_\alpha$  of finite representations of (possibly) infinite objects in  $\wp(D)$
- The representation of  $\wp(D)$  by  $D_\alpha$  is expressed by a (monotonic) function called a *concretization function*:

$$\gamma : D_\alpha \rightarrow \wp(D)$$

such that  $\gamma(\lambda) = d$  if  $d$  is the largest element (under  $\subseteq$ ) of  $\wp(D)$  that  $\lambda$  describes  
[  $(\wp(D), \subseteq)$  is obviously a complete lattice ]

e.g. in the “signs” example, with  $D_\alpha = \{[-], [0], [+], \top\}$ ,  $\gamma$  is given by

$$\gamma([-]) = \{x \in Z \mid x < 0\}$$

$$\gamma([0]) = \{0\}$$

$$\gamma([+]) = \{x \in Z \mid x > 0\}$$

$$\gamma(\top) = Z$$

- $\gamma(?) = \emptyset \rightarrow$  we define  $\perp \mid \gamma(\perp) = \emptyset$

## Abstraction Function

---

- We can also define (not strictly needed) a (monotonic) *abstraction function*

$$\alpha : \wp(D) \rightarrow D_\alpha$$

$\alpha(d) = \lambda$  if  $\lambda$  is the “least” element of  $D_\alpha$  that describes  $d$   
[ under a suitable ordering defined on the elements of  $D_\alpha$  ]

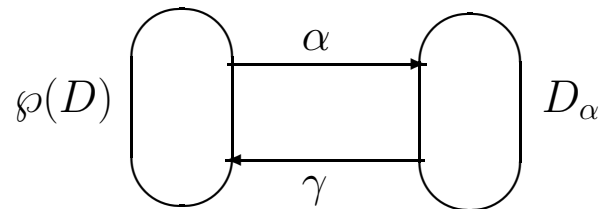
e.g. in the “signs” example,

$$\alpha(\{1, 2, 3\}) = [+ ] \text{ (and not } \top \text{)}$$

$$\alpha(\{-1, -2, -3\}) = [- ] \text{ (and not } \top \text{)}$$

$$\alpha(\{0\}) = [0]$$

$$\alpha(\{-1, 0, 1\}) = \top$$



## Abstract Meaning and Safety

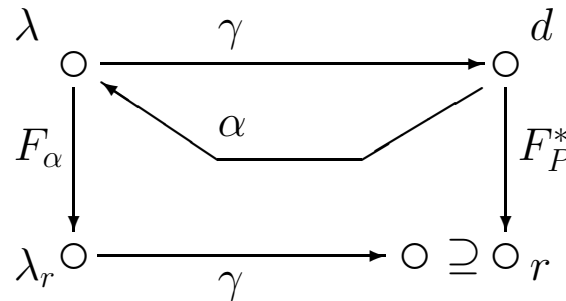
---

- We can now define an abstract meaning function as

$$F_\alpha : D_\alpha \rightarrow D_\alpha$$

which is then safe if

$$\forall \lambda, \lambda \in D_\alpha, \gamma(F_\alpha(\lambda)) \supseteq F_P^*(\gamma(\lambda))$$



- We can then prove a property of the output of a given class of inputs represented by  $\lambda$  by proving that all elements of  $\gamma(F_\alpha(\lambda))$  have such property
- E.g. in our example, a property such as “if this program takes a positive number it will produce a negative number as output” can be proved



## Proving properties in the abstract

---

- Generating  $F_\alpha$ :
  - ◇  $F_P$  obtained from program and predefined semantics of operators  
 $(x + z) * 3, F_P = (x + z) * 3$
  - ◇ Automatic analysis:  
 $F_\alpha$  should be obtainable from program and semantics of abstract operators  
(compositional properties)  
 $\{odd, even, +_\alpha, *_\alpha\} \Rightarrow F_\alpha = (x +_\alpha z) *_\alpha odd$
- “If this program takes a positive number it will produce a negative number as output”
  - ◇  $P = (y := x * -3), x$  input,  $y$  output
  - ◇  $F_P = x * -3$
  - ◇  $F_\alpha = x *_\alpha [-]$
  - ◇  $F_\alpha([+]) = [+ ] *_\alpha [-] = [-]$

## Collecting Semantics

---

- “Input-output” semantics often too coarse for useful analysis: information about “state” at *program points* generally required → “extended semantics”
- Program points can be reached many times, from different points, and in different “states” → “collecting” (“sticky”) semantics

$$\{x > 3\} y := x * -3 \{y < -9\} \text{ or } \{x < -3\} y := x * -3 \{y > 9\}$$

$$\{x = [+]\} y := x * -3 \{y = [-]\} \text{ or } \{x = [-]\} y := x * -3 \{y = [+]\}$$

- Analysis often computes a collection of abstract states for a program point

$$\{x = \{[+], [-]\}\} y := x * -3 \{y = \{[-], [+]\}\}$$

- Often more efficient to “summarize” states into one which gives the best overall description → lattice structure in abstract domain

$$\{x = \sqcup\{[+], [-]\}\} y := x * -3 \{y = \sqcup\{[-], [+]\}\}$$

## Lattice Structure

---

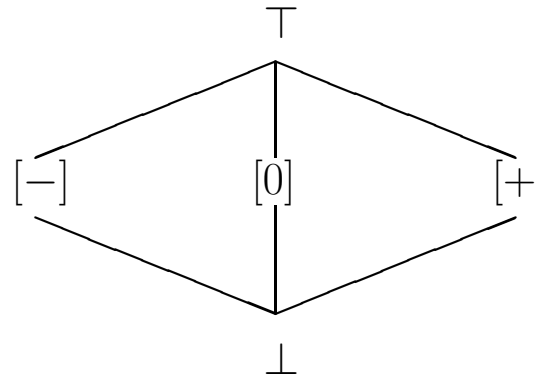
- The ordering on  $\wp(D)$ ,  $\subseteq$ , induces an ordering on  $D_\alpha$ ,  $\leq_\alpha$  (“approximates better”)  
E.g., we can choose either  $\alpha(\{1, 2, 3\}) = [+]$  or  $\alpha(\{1, 2, 3\}) = \top$ ,  
but  $\gamma([+]) = \{x \in Z \mid x > 0\}$  and  $\gamma(\top) = Z$ , and  
since  $\{x \in Z \mid x > 0\} \subseteq Z$  we have  $[+] \leq_\alpha \top$ , i.e.,  $[+]$  approximates better than  $\top$ ,  
it is more precise
- It is generally required that  $(D_\alpha, \leq_\alpha)$  be a complete lattice
- Therefore, for all  $S \subseteq D_\alpha$  there exists a unique least upper bound  $\sqcup S \in D_\alpha$  –i.e.,  
such that
  - ◇  $\forall \lambda_s \in S, \lambda_s \leq_\alpha \sqcup S$
  - ◇  $(\forall \lambda_s \in S, \lambda_s \leq_\alpha \lambda) \Rightarrow \sqcup S \leq_\alpha \lambda$
- Intuition: given a set of approximations of the “current state” at a given point in a  
program, to ensure that it is the best “overall” description for the point:
  - ◇  $\sqcup S$  approximates *everything* the elements of  $S$  approximate
  - ◇  $\sqcup S$  is the best approximation in  $D_\alpha$

## Example: integer sign arithmetic

- We consider  $D_\alpha = \{[-], [0], [+], \top\}$ 
  - ◇ We add  $\perp$  (infimum) so that  $\alpha(\emptyset)$  exists and to have a complete lattice:  
 $D_\alpha = \{\perp, [-], [0], [+], \top\}$
  - ◇ (Intuition:  
it represents a program point that is never reached)
  - ◇ The concretization function has to be extended with

$$\gamma(\perp) = \emptyset$$

- ◇ The lattice is then given by:



- ◇  $\sqcup\{[+], [-]\} = \sqcup\{[-], [+]\} = \top$

## Example: integer sign arithmetic (Contd.)

- To make  $\sqcup$  more meaningful we consider  $D_\alpha = \{\perp, [-], [0^-], [0], [0^+], [+], \top\}$

$$\gamma(\perp) = \emptyset$$

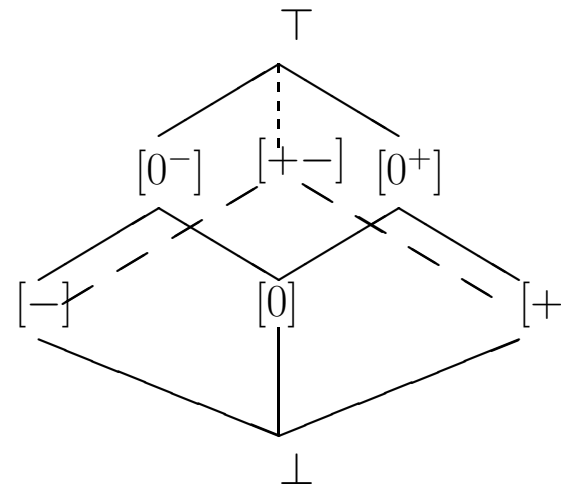
$$\gamma(\top) = Z$$

$$\gamma([-]) = \{x \in Z \mid x < 0\} \quad \gamma([+]) = \{x \in Z \mid x > 0\} \quad \gamma([0]) = \{0\}$$

$$\gamma([0^-]) = \{x \in Z \mid x \leq 0\} \quad \gamma([0^+]) = \{x \in Z \mid x \geq 0\}$$

- The lattice is then given by:

$$\sqcup\{+, [-]\} = \top?$$



- $\sqcup\{[-], [0]\} = [0^-]$

accurately represents a program point where a variable can be negative or zero

## The Galois Insertion Approach

---

- In the following, we will refer to  $\wp(D)$  simply as  $D$
- (Collecting) program semantics is often given as  $lfp(F)$  (the least  $S$  s.t.  $S = F(S)$ ,  $F$  being the program-dependent semantic function on  $D$ )
- Thus, we need to relate this fixpoint to (that of) the approximate semantic function  $F_\alpha$  (which approximates  $F$  and operates on elements of an abstract domain  $D_\alpha$ )
- Assume:  $D$  and  $D_\alpha$  are complete lattices;  $\gamma : D_\alpha \rightarrow D$  and  $\alpha : D \rightarrow D_\alpha$  are monotonic functions. The structure  $(D_\alpha, \gamma, D, \alpha)$  is called a *Galois Insertion* if:
  - ◇  $\forall \lambda \in D_\alpha. \lambda = \alpha(\gamma(\lambda))$
  - ◇  $\forall d \in D. d \subseteq \gamma(\alpha(d))$
- *Safe approximation*, defined now in terms of a Galois insertion:  
Let a Galois insertion  $(D_\alpha, \gamma, D, \alpha)$ ,  $\lambda \in D_\alpha$  *safely approximates*  $d \in D$  iff  $d \subseteq \gamma(\lambda)$
- Fundamental Theorem [Cousot]: Given a Galois insertion  $(D_\alpha, \gamma, D, \alpha)$ , and two (monotonic) functions  $F : D \rightarrow D$  and  $F_\alpha : D_\alpha \rightarrow D_\alpha$  then if  $F_\alpha$  approximates  $F$ ,  $lfp(F_\alpha)$  approximates  $lfp(F)$

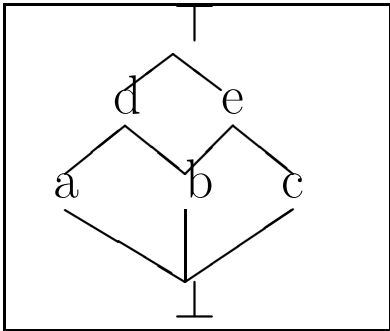
## Termination: conditions on $F_\alpha$ and $D_\alpha$

---

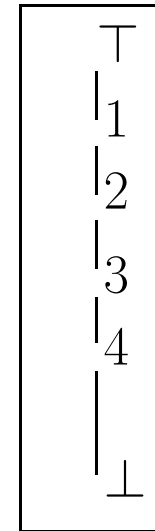
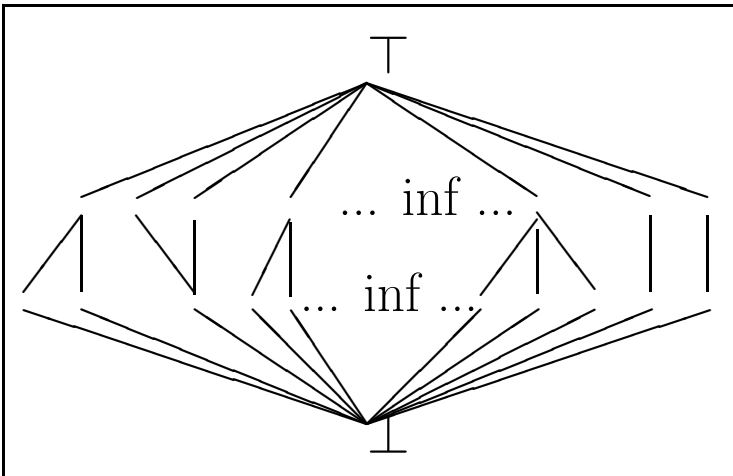
- The question is whether  $lfp (F_\alpha)$  is finitely computable
- The abstract operator  $F_\alpha$  operates on elements of an abstract domain  $D_\alpha$ , which we have required to be a complete lattice, and  $F_\alpha$  is monotonic, therefore
$$lfp F_\alpha = F_\alpha \uparrow n$$
for some  $n$  which we would like to be finite (i.e. we would like the Kleene sequence to be finite)
- Recalling the characteristics of fixpoints on lattices, the Kleene sequence will be finite in cases including:
  - ◇  $D_\alpha$  is finite
  - ◇  $D_\alpha$  is ascending chain finite

# Lattice Structures

finite



finite\_depth



ascending chain finite



## Termination: Discussion

---

- Showing monotonicity of  $F_\alpha$  may be more difficult than showing that  $D_\alpha$  meets the finiteness conditions
- There may be an  $F_\alpha$  which terminates even if the conditions are not met
- Conditions also be relaxed by restricting the class of programs (e.g. non-recursive programs pose few difficulties, although they are hardly interesting)
- In some cases an approximation from above ( $gfp (F_\alpha)$ ) can also be interesting
- There are other alternatives to finiteness: dynamic bounded depth, etc. (See: Widening and Narrowing)

## Origins (General Programming)

---

- The idea itself (i.e. rule of signs) predates computation...
- The idea of computing by approximations was used as early as 1963 by Naur (“pseudo evaluation”, in the Gier Algol compiler),  
“a process which combines the operators and operands of the source text in the manner in which an actual evaluation would have to do it, but which operates on descriptions of the operands, not on their values”
- 1972, Sintzoff (proving well-formedness and termination properties)
- 1975, Wegbreit appears to be the first to develop a lattice-theoretic model
- Mid 70’s: Kam, Kindall, Tarjan, Ullman, ...
- 1976,77, Patrick and Radhia Cousot proposed a formal model for the analysis of imperative (“flowchart”) languages: unifying framework
  - ◇ Define a “static” semantics: associate a set of possible storage states with each program point
  - ◇ Dataflow analysis constructed then as a finitely computable approximation to the static semantics

## Analyzing Logic Programs

---

- Which semantics?
  - ◇ Declarative semantics: concerned with what is a consequence of the program
    - \* Model-theoretic semantics
    - \* Fixpoint ( $T_P$  operator-based) semantics  
can be what the program actually does (cf. database-style bottom-up evaluation)
  - ◇ Operational semantics: close to the behavior of the program
    - \* SLD-resolution based (success sets)
    - \* Denotational
    - \* Can cover possibilities other than SLD: reactive, parallel, ...
- Analyses based on declarative semantics are often called “bottom up” analyses
- Analysis based on the (top-down) operational semantics are often called “top-down” analyses
- Also, intermediate cases (generally achieved through program transformation)

## Case Study: Fixpoint Semantics

---

- Given the first-order language  $L$  associated with a given program  $P$ , the *Herbrand universe* ( $U$ ) is the set of all *ground terms* of  $L$ .
- The *Herbrand Base* ( $B$ ) is the set of all *ground atoms* of  $L$ .
- A *Herbrand Interpretation* is a subset of  $B$ .  
 $I$  is the set of all Herbrand interpretations ( $\wp(B)$ ).
- A *Herbrand Model* is a Herbrand interpretation which contains all logical consequences of the program.
- The *Immediate Consequence Operator* ( $T_P$ ) is a mapping  $T_P : I \rightarrow I$  defined by:  
$$T_P(M) = \{h \in B \mid \exists C \in \text{ground}(P), C = h \leftarrow b_1, \dots, b_n \text{ and } b_1, \dots, b_n \in M\}$$
  
(in particular, if  $(a \leftarrow) \in P$ , then  $\text{ground}(a) \subseteq T_P(M)$ , for every  $M$ ).
- $T_P$  is monotonic, so it has a least fixpoint  $lfp(T_P)$  which can be obtained as  $T_P \uparrow \omega$  starting from the bottom element of the lattice (the empty interpretation,  $\emptyset$ ).
- (Characterization Theorem) [Van Emden and Kowalski]:  
The Least Herbrand Model of  $P$ ,  $H$  is  $lfp(T_P)$

## Fixpoint Semantics: Example

---

- Example:

$$P = \{ p(f(X)) \leftarrow p(X), \\ p(a), \\ q(a), \\ q(b). \}$$

$$U = \{ a, b, f(a), f(b), f(f(a)), f(f(b)), \dots \}$$

$$B = \{ p(a), p(b), q(a), q(b), p(f(a)), p(f(b)), q(f(a)), \dots \}$$

$I =$  *all subsets of*  $B$

$$H = \{ q(a), q(b), p(a), p(f(a)), p(f(f(a))), \dots \}$$

$$T_P \uparrow 0 = \{ p(a), q(a), q(b) \}$$

$$T_P \uparrow 1 = \{ p(a), q(a), q(b), p(f(a)) \}$$

$$T_P \uparrow 2 = \{ p(a), q(a), q(b), p(f(a)), p(f(f(a))) \}$$

...

$$T_P \uparrow \omega = H$$

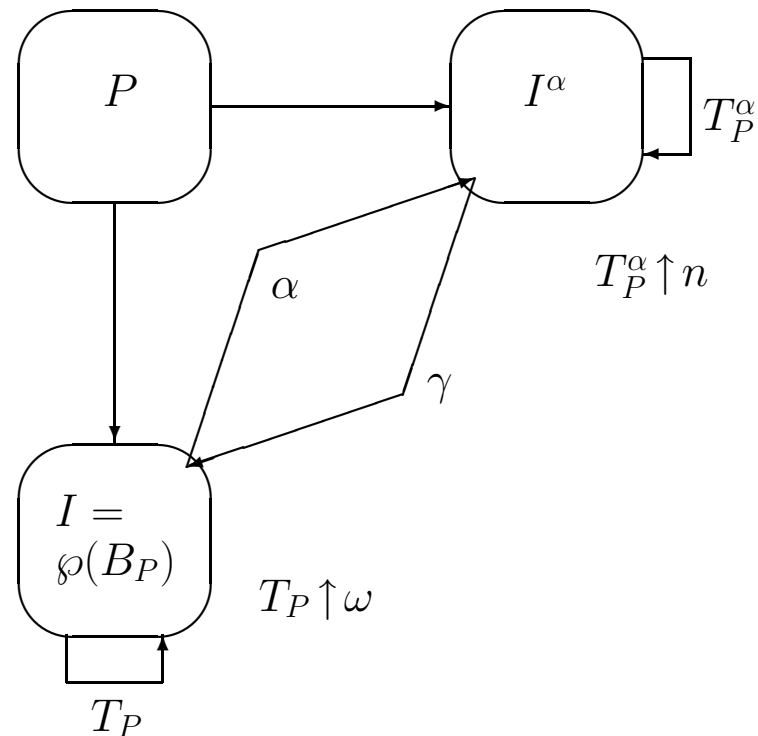
## “Bottom-up” Abstract Interpretation

---

- Finds an approximation of  $H$  by approximating  $lfp(T_P)$
- We apply abstract interpretation:
  - ◇ Domain:  $I^\alpha$ , s.t. elements of  $I^\alpha$  approximate elements of  $I = \wp(B)$ .
  - ◇ Concretization function:  $\gamma : I^\alpha \rightarrow I$
  - ◇ Abstraction function:  $\alpha : I \rightarrow I^\alpha$
  - ◇ Operator abstraction: abstract version of the  $T_P$  operator  $T_P^\alpha : I^\alpha \rightarrow I^\alpha$
  - ◇ Correctness:
    - \*  $(I^\alpha, \gamma, I, \alpha)$  should be a Galois insertion, i.e. ,  $I^\alpha$  complete lattice and it should approximate  $I$ :  $\forall M \in I, \gamma(\alpha(M)) \supseteq M$
    - \*  $T_P^\alpha$  safe approximation of  $T_P$ , i.e.  $\forall d, d \in I^\alpha, \gamma(T_P^\alpha(d)) \supseteq T_P(\gamma(d))$
  - ◇ Termination:
    - \*  $T_P^\alpha$  monotonic.
    - \*  $I^\alpha$  (at least) ascending chain finite.
- Then,  $H^\alpha = lfp(T_P^\alpha) = T_P^\alpha \uparrow n$  will be obtained in a finite number of steps  $n$  and  $H^\alpha$  will approximate  $H$ .

## “Bottom-up” Abstract Interpretation (Contd.)

---



Such “bottom-up” analyses have been proposed for example by Marriott and Sondergaard, and, more recently, by Codish, Dams, and Yardeni, Debray and Ramakrishnan, Barbuti, Giacobazzi, and Levi, and others.

## Example: simple “type” inference

---

- Minimal “type inferencing” problem [Sondergaard]:  
Approximating which predicates are in  $H$
- $pred(a)$ : denotes the predicate symbol for an atom  $a$
- $B^\alpha = S$  (set of predicate symbols in a program  $P$ )  
Then  $I^\alpha = \wp(S)$ , we call it  $S^*$
- Concretization function:  
 $\gamma : S^* \rightarrow I$   
 $\gamma(D) = \{a \in B \mid pred(a) \in D\}$
- Abstraction function:  
 $\alpha : I \rightarrow S^*$   
 $\alpha(M) = \{p \in S \mid \exists a \in M, pred(a) = p\}$
- $(S^*, \gamma, I, \alpha)$  is a Galois insertion



## Example: simple “type” inference (Contd.)

---

- Abstract version of  $T_P$  (after some simplification):

$$T_P^\alpha : S^* \rightarrow S^*$$

$$T_P^\alpha(D) = \{ p \in S \mid \exists C \in P, \\ C = h \leftarrow b_1, \dots, b_n, \\ \text{pred}(h) \leftarrow \text{pred}(b_1), \dots, \text{pred}(b_n) \equiv p \leftarrow p_1, \dots, p_n, \\ \text{and } p_1, \dots, p_n \in D \}$$

- $S^*$  finite (finite number of predicate symbols in program) and  $T_P^\alpha$  monotonic  
→  
analysis will terminate in a finite number of steps  $n$  and  
 $H^\alpha = T_P^\alpha \uparrow n$  approximates  $H$ .

## Example: simple “type” inference (Contd.)

---

- Example:

$$\begin{array}{ll} P = \{ p(f(X)) \leftarrow p(X). & P_\alpha = \{ p \leftarrow p. \\ \quad p(a). & \quad p. \\ \quad r(X) \leftarrow t(X, Y). & \quad r \leftarrow t. \\ \quad q(a). & \quad q. \\ \quad q(b). \} & \quad \} \end{array}$$

- ◇  $S = \{p/1, q/1, r/1, t/2\}$

- ◇ Abstraction:

$$\alpha(\{p(a), p(b), q(a)\}) = \{p/1, q/1\}$$

- ◇ Concretization:

$$\begin{aligned} \gamma(\{p/1, q/1\}) &= \{A \in B \mid \text{pred}(A) = p/1 \vee \text{pred}(A) = q/1\} \\ &= \{p(a), p(b), p(f(a)), p(f(b)), \dots, q(a), q(b), q(f(a)), \dots\} \end{aligned}$$

- ◇ Analysis:

$$T_P^\alpha \uparrow 0 = T_P^\alpha(\emptyset) = \{p/1, q/1\}$$

$$T_P^\alpha \uparrow 1 = T_P^\alpha(\{p/1, q/1\}) = \{p/1, q/1\} = T_P^\alpha \uparrow 0 = H^\alpha$$

## $T_P$ -based Bottom-up Analysis: Discussion

---

- Advantages:

- ◇ Simple and elegant. Based on the declarative, fixpoint semantics
- ◇ General: results independent of the query form

- Disadvantages:

- ◇ Information only about “procedure exit.” Normally information needed at various program points in compilation, e.g., “call patterns” (closures)
- ◇ The “logical variable” not observed (uses ground data). Information on instantiation state, substitutions, etc. often needed in compilation
- ◇ Not query-directed: analyzes whole program, not the part (and modes) that correspond to “normal” use (expressed through a query form)

## $T_P$ -based Bottom-up Analysis: Discussion (II)

---

- Solutions:
  - ◇ Call patterns obtainable via “magic sets” transformation [Marriott and Sondergaard]  
Used also for query-directed analysis by [Barbuti et al.], [Codish et al.], [Gallagher et al.], [Ramakrishnan et al.], and others
  - ◇ Enhanced fixpoint semantics (e.g, S-semantics [Falaschi et al.], [Gaifman and Shapiro])

## “Top-down” analysis (summarized)

---

- Define an extended (collecting) concrete semantics, derived from SLD resolution, making relevant information *observable*.
- Abstract domain: generally “abstract substitutions”.
- Abstract operations: unification, composition, projection, extension, ...
- Abstract semantic function: takes a query form (abstraction of initial goal or set of initial goals) and the program and returns abstract descriptions of the substitutions at relevant program points.
- Variables complicate things:
  - ◇ correctness (due to aliasing),
  - ◇ termination (merging information related to different renamings of a variable)
- Logic variables are in fact (well behaved) pointers:  
`X = tree(N,L,R), L = nil, Y = N, Y = 3, ...`  
this makes analysis of logic programs very interesting  
(and quite relevant to other paradigms).

## Domains

---

- Simple domains [Mellish,Debray], e.g.:  
{ closed (ground), don't know, empty, free, non-var }  
(e.g.  $f(a)$ ,  $?$ ,  $\perp$ ,  $X$ ,  $f(X)$ )
- May need to be very imprecise to be correct:  

```
:- entry p(X,Y) : ( free(X), free(Y) ).  
p(X,Y) :-  
    q(X,Y),  
    X = a.  
q(Z,Z).
```
- Correct/more accurate treatment of aliasing [Debray]:  
associate with a program variable a pair  
< *abstraction of the set of terms the variable may be bound to* ,  
*set of program variables it may "share" with* >.

## Domains: Pair Sharing

---

- More accurate sharing – pair sharing [Sondergaard] [Codish]: pairs of variables denoting possible sharing.

```
:- entry p(X,Y) : ( free(X), free(Y) ).
```

```
p(X,Y) :-
```

```
    q(X,Y), % { X=f, Y=f } and { (X,Y) }
```

```
    X = a. % { X=g, Y=g } and { (X,Y) }
```

```
q(Z,Z).
```

- Note: we have used a “combined” domain: simple modes plus pair sharing
- Pair sharing can encode linearity:  $(x, x)$

```
:- entry p(X,Y) : ( free(X), free(Y) ).
```

```
p(X,Y) :-
```

```
    q(X,Y), % { X=f, Y=f } and { (X,Y) }
```

```
    W = f(X,Y). % { W=nv, X=f, Y=f } and { (W,W), (X,Y) }
```

```
q(Z,Z).
```

## Domains: Set Sharing

---

- Even more accurate sharing – set sharing [Jacobs et al.] [Muthukumar et al.]: sets of sets of variables.

$$\theta = \{W/a, X/f(A_1, A_2, A_3), Y/g(A_2), Z/A_3\}$$

$$\theta^\alpha = \{\emptyset, \{X\}, \{X, Y\}, \{X, Z\}\}$$

- A bit tricky to understand. Try:

$$\{X\} \quad \{X, Y\} \quad \{X, Z\}$$

$$A_1 \quad A_2 \quad A_3$$

$$\theta = \{W/a, X/f(A_1, A_2, A_3, B_1), Y/g(h(A_2, B_1)), Z/A_3\}$$

$$\theta^\alpha = \{\emptyset, \{X\}, \{X, Y\}, \{X, Z\}\}$$

$$\{X\} \quad \{X, Y\} \quad \{X, Z\}$$

$$A_1 \quad A_2 + B_1 \quad A_3$$

- Encodes grounding and independence
  - ◇  $W$  has no occurrence in any set: it is ground
  - ◇  $\{Y, Z\}$  has no occurrence in any set: they are independent



## Other domains

---

- Sharing+Freeness [Muthukumar et al.] (and + depth-K)
- Type graphs [Janssens et al.]
- Depth-K [Sato and Tamaki]
- Pattern structure [Van Hentenryck et al.]
- Variable dereferencing [VanRoy] [Taylor]
- ...
- Much work by [Codish et al.] [File et al.] [Giacobazzi et al.] ... on combining and comparing these domains

## Frameworks

---

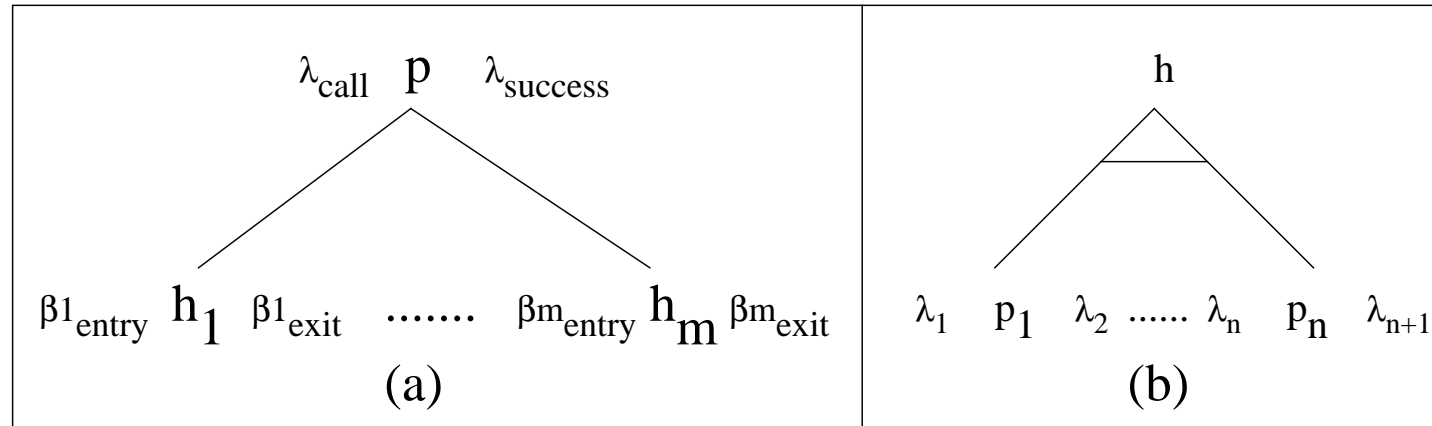
- Debray: predicate level mode inference (call and success patterns for predicates). Unification reformulated as entry + exit unification. Termination by tabling.
- Jones, Marriott, and Sondergaard: using denotational semantics.
- Bruynooghe:
  - ◇ Concrete semantics constructs “generalized” AND trees: nodes contain instance of goal before and after execution: *call substitution* and *success substitution*.
  - ◇ Analysis constructs “abstract AND-OR trees”. Each represents a (possibly infinite) set of (possibly infinite) concrete trees. Widening to regular trees for termination.
  - ◇ Framework is generic: parametric on some basic domain related functions + conditions for correctness and termination.
- Muthukumar and Hermenegildo: “PLAI” framework.  
Improvement over previous frameworks: Efficient fixpoint algorithms (dependency tracking) and memory savings (no explicit representation of trees).

## Abstract AND-OR Tree

- Tree exploration:

$?- p.$

$h:- p_1, \dots, p_n.$



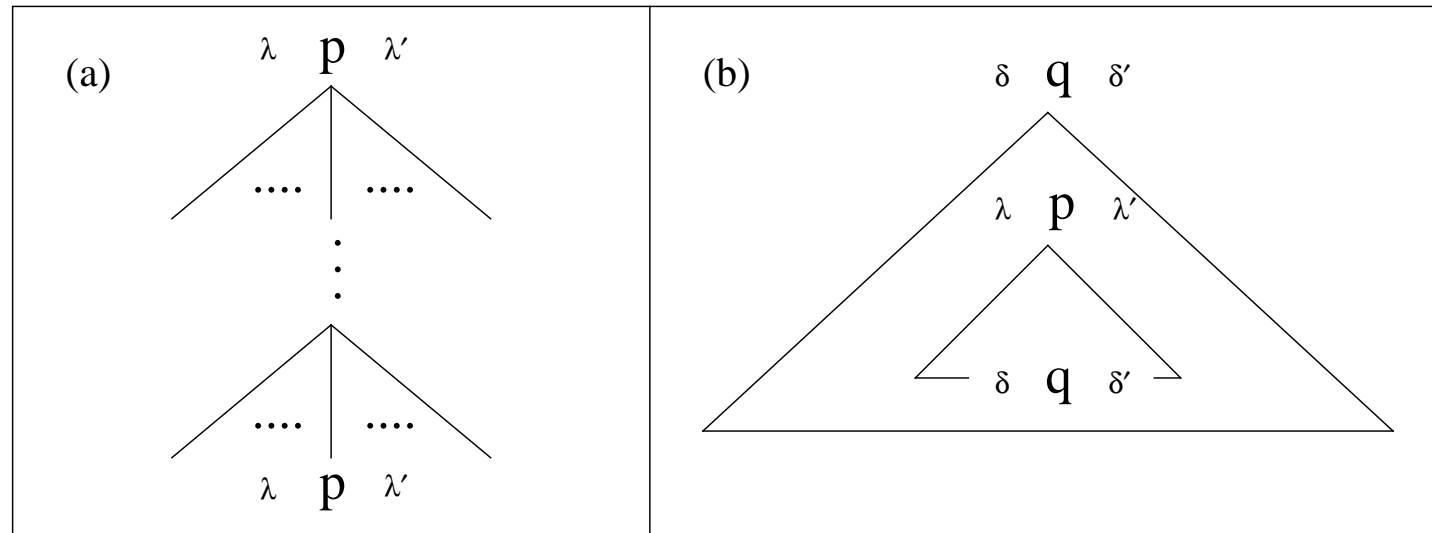
- Basic operations:

- ◇ Procedure entry: from  $\lambda_{call}$  obtain  $\beta_{1_{entry}}$
- ◇ Entry-to-exit (b): from  $\beta_{1_{entry}}$  obtain  $\beta_{1_{exit}}$
- ◇ Clause entry: from  $\beta_{1_{entry}}$  obtain  $\lambda_1$  (and clause exit)
- ◇ Body traversal: from  $\lambda_1$  obtain  $\lambda_{n+1}$  (iteratively applying (a))
- ◇ Procedure exit: from (each or all of the)  $\beta_{i_{exit}}$  obtain  $\lambda_{success}$

## Fixpoint Optimization

---

- Fixpoint required on recursive predicates only:



- Simply recursive (a)
- Mutually recursive (b)

“Use current success substitution and iterate until a fixpoint is reached”

## Other Improvements

---

- Abstract tree contains several occurrences of the same atom in a clause (for precision): useful for program specialization ( Multivariance )  
However, too many versions if not controlled  
(solutions proposed [Gianotti et al.], [Jacobs et al.], [Puebla et al.] )
- Much recent work in domains, improvement of fixpoints, application, etc. [Taylor],[VanRoy], GAIA [LeCharlier et al.]
- Abstract compilation:  
Compute over and “abstract version” of the program
- Reexecution [Bruynooghe, LeCharlier et. al.]  
(alternative to keeping track of accurate sharing)
- Caching of operations [LeCharlier et al.]

## Analysis of Constraint Logic Programs

---

- CLP: (relation-based) programs over symbolic and non symbolic domains: constraint satisfaction instead unification (e.g. CLP(R), PrologIII, CHIP, etc.)
- Jorgensen, Marriott, and Michaylov [ISLP'91] and later Marriott and Stuckey [POPL'93] identified numerous opportunities for improvement via static analysis
- A number of proposals for analysis frameworks:
  - ◇ Marriott and Sondergaard [NACLP90]: denotational approach
  - ◇ Codognet and Filé [ICPL92]: uses constraint solving for the analysis itself and “abstract compilation”
  - ◇ G. de la Banda and Hermenegildo [WICLP'91,ILPS'93]: adaptation of LP frameworks (PLAI).

## Analysis of Constraint Logic Programs (Contd.)

---

- Example: Definiteness analysis (Def) [G. de la Banda et al.]

Domain:  $Def = \{d, \wp(\wp(Pvar)), \top\}$

$X = Y + Z \quad \Rightarrow [(X, [[Y, Z]]), (Y, [[X, Z]]), (Z, [[X, Y]])]$

$X = f(Y, Z) \quad \Rightarrow [(X, [[Y, Z]]), (Y, [[X]]), (Z, [[X]])]$

$X :: N \quad \Rightarrow [(X, \top), (N, [[X]])]$

$X > Y \quad \Rightarrow [(X, \top), (Y, \top)]$

$X = 3 \quad \Rightarrow [(X, d)]$

- Other analyses:

- ◇ Freeness analysis [Dumortier et al.] and combinations.

- ◇ LSign [Marriott, Sondergaard and Stuckey, ILPS'94]

- Applications:

- ◇ optimization [Keely et al., CP'96]

- ◇ parallelization [Bueno et al., PLILP'96]

- ◇ ...

## Origins (Declarative Paradigms, to CLP)

---

- A few milestones (on the road to CLP analysis):
  - ◇ 1981, Mycroft: strictness analysis of applicative languages
  - ◇ 1981, Mellish: proposes application to logic programs
  - ◇ 1986, Debray: framework with safe treatment of logic variables, discussion of efficiency
  - ◇ 1987, Bruynooghe: framework for LP based on and-or trees
  - ◇ 1987, Jones and Sondergaard: framework based on a denotational definition of SLD
  - ◇ 1988, Warren, Debray and Hermenegildo:  $M_s$  and  $MA^3$  practicality of Abs. Int. for Logic Programs shown (for program parallelization)
  - ◇ 1989, Muthukumar and Hermenegildo: PLAI generic system
  - ◇ 1990, Van Roy / Taylor: application to sequential optimization of Prolog
  - ◇ 1991, Marriott et al.: first extension to CLP
  - ◇ 1992, Garcia de la Banda and Hermenegildo: generalization of Bruynooghe's algorithm to CLP, extension of PLAI



## Conclusions

---

- Abstract Interpretation is a very elegant program analysis technique
- It has in addition been proved useful and efficient. E.g., for LP and CLP:
  - ◇ Static parallelization of logic (and CLP) programs [Hermenegildo et al]
  - ◇ (Sequential) program optimization [Taylor, VanRoy, ...]
  - ◇ Optimization of CLP programs [Marriott et al, ...]
  - ◇ Abstract debugging, etc.

## Conclusions (and Coda!)

---

- Interesting issues studied for handling large real programs:
  - ◇ Modularity
  - ◇ Handling extra-logical features, higher order
  - ◇ Handling dynamic code
  - ◇ Support of test-debug cycle

Solutions include [See, e.g., papers in ESOP'96, SAS'96]:

- ◇ Module interface definition: modular analysis
  - ◇ Analysis of “Full Prolog”
  - ◇ Incremental analysis
- Demo!