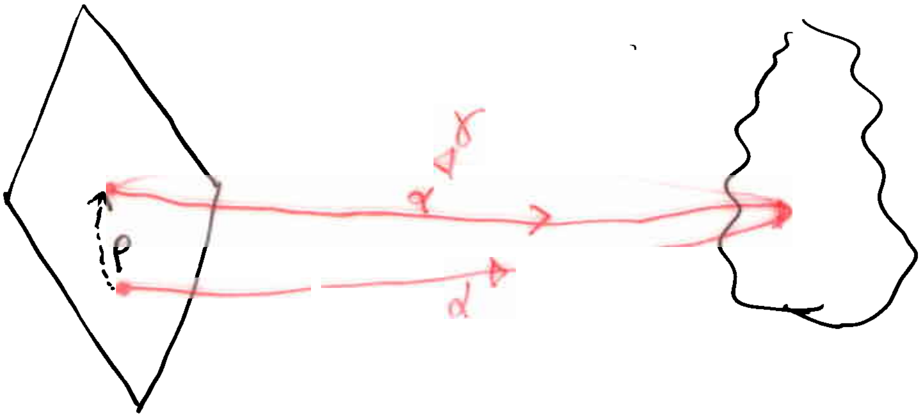
REFINEMENT OPERATORS

- from Galois connections to upper closure operators
- the lattice of abstract interpretations
- refinement operators
    - reduced product
    - disjunctive completion
    - completion by complements
    - reduced cardinal power
- logical interpretation of refinements
- Heyting's completion

FROM GALOIS CONNECTIONS TO UPPER CLOSURE OPERATORS



concrete domain $C, \sqsubseteq$ abstract domain $A, \leq$

- the composition of α with γ is an operator on C

$$\rho \quad C \to C$$

having the following properties

- $\rho(x)$ is a safe approximation of x

$$x \sqsubseteq \rho(x)$$

- ρ is monotonic

composition of monotonic functions

ρ is idempotent

$$\rho(\rho(x)) = \rho(x)$$

- because of properties of Galois insertions

the approximation is obtained in one step

- ρ is an upper closure operator on C

UCO'S AND MOORE FAMILIES

Each closure operators $\rho : C \to C$ is uniquely determined by the set of its fixpoints which is its image $\rho(C)$

- $\rho(C)$ is a complete lattice wrt $\leq_C$, however in general not

- $X \subseteq C$ is the set of fixpoints $\rho(C)$ of a closure operator ρ on C iff it is a Moore family
  - $\top_C \in X$
  - X is closed under glb

- $\mathcal{M}(X)$ is the Moore-closure of X,
  - the least subset of C which contains X and is a Moore family

UPPER CLOSURE OPERATORS ARE ABSTRACT INTERPRETATIONS

- any Galois insertion uniquely determines an upper closure operator

- given any upper closure operator ρ on C
  - there exist many abstract domains A, such that $\rho = \lambda x.\ \gamma(\alpha(x))$
  - these abstract domains are "isomorphic" to ρ
  - each an abstract domain together with its abstraction and concretization functions, defines an abstract interpretation
    - any upper closure operator ρ on C defines an abstract interpretation
      - without an abstract domain, which is just a representation / implementation of the property modeled by ρ
      - it makes easier reasoning on the relation among different abstract interpretations

        because they are all defined on the same domain
    - in [illegible] a representation (abstract domain and Galois insertion) is needed when designing (possibly optimal) abstract operations.

THE LATTICE OF ABSTRACT INTERPRETATIONS

$C \sqsubseteq$ concrete domain

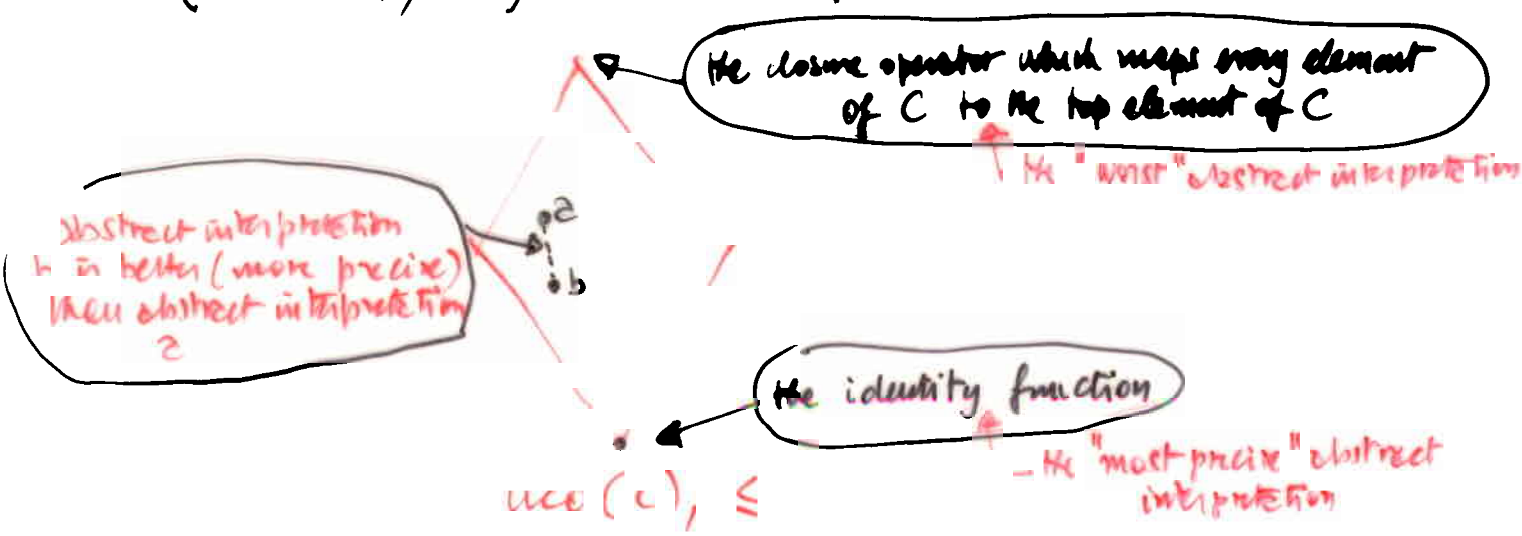
- any uco on C is an abstract interpretation

- the set of upper closure operators on C has a natural partial order relation $\leq$
  - functional pointwise order based on $\sqsubseteq$

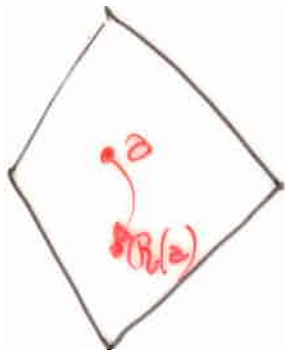
$$\rho_1 : C \to C$$
$$\rho_2 : C \to C$$

$$\rho_1 \leq \rho_2 \quad \text{iff} \quad \forall x \in C \quad \rho_1(x) \sqsubseteq \rho_2(x)$$

- $(uco(C), \leq)$ is a complete lattice



REFINEMENT OPERATORS



$uco(C), \leq$

- refinement of abstract domains (upper closure operators)

  $\mathcal{R} \quad uco(C) \to uco(C)$

  - delivers a more precise abstract domain

    $\forall a \in uco(C) \quad \mathcal{R}(a) \leq a$

  - is monotonic
  - is idempotent
    - the improvement in precision ("refinement") is obtained all in one step

- refinements are lower closure operators on $uco(C)$

SOME REFINEMENT OPERATORS

- reduced product

  $A \sqcap B$

  cartesian product of the two domains where pairs having equivalent meaning (representing the same property) are identified (reduced)

  - given a domain $A \in uco(C)$

    $\lambda x.\, x \sqcap A$ is clearly a lower closure operator on $uco(C)$

    $\Downarrow$

    it is a refinement operator

  - the most abstract (simplest) domain which is more precise of the given domains

    which allows us to derive at least the same properties

  - it is exactly the glb in the lattice of uco's

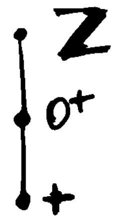
  - it is closed under intersection

    which plays the role of conjunction of properties

AN EXAMPLE OF REDUCED PRODUCT

concrete domain : $\wp(\mathbb{Z}), \subseteq$ as in the Sign example!

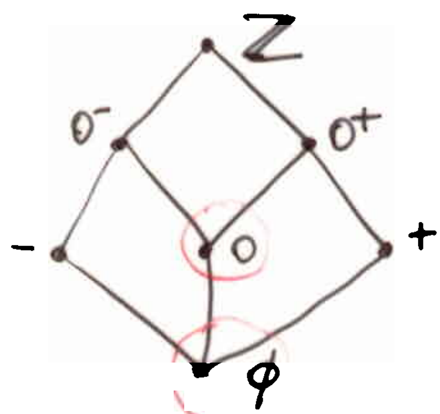
uco 1 A^+



to be read as uco's on $\wp(\mathbb{Z})$

uco 2 A^-

$A^+ \sqcap A^-$



(our friend Sign!)

- the two "new" points are the "intersections"
    - 0 is the intersection between 0^- and 0^+
    - ϕ is the intersection between $-$ and $+$

MORE REFINEMENT OPERATORS

- disjunctive completion $\mathcal{R}_\vee$

$$\mathcal{R}_\vee : uco(C) \to uco(C)$$

$\mathcal{R}_\vee(a)$, $a \in uco(C)$ (abstract domain)

adds to a denotations for concrete disjunctions of its values

- the most abstract domain which can represent concrete disjunctions

- to improve the precision of the domain in abstract computations with multiple branchings

  - conditionals
  - nondeterminism

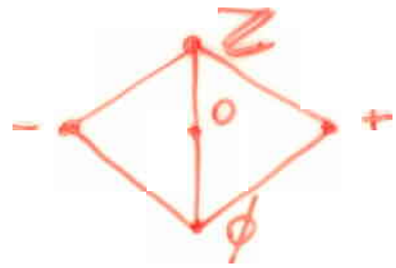
- disjunction of properties, rather than taking lub's on the original abstract domain

AN EXAMPLE OF DISJUNCTIVE COMPLETION

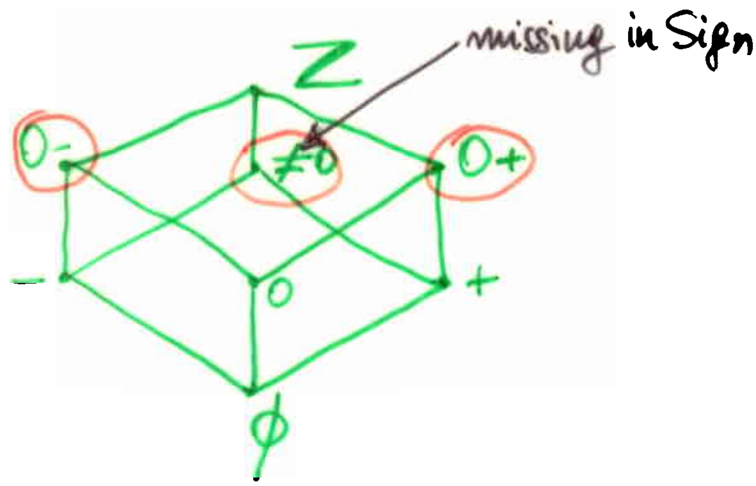
- concrete domain $\wp(\mathbb{Z}), \subseteq$

- abstract domain

$A =$



$\mathcal{R}_\vee(A) =$



- the "new" points

0^-	disjunction of $-$ and 0
$\neq 0$	disjunction of $-$ and $+$
0^+	disjunction of $+$ and 0

- $\mathcal{R}_\vee(A)$ is also the disjunctive completion of Sign

MORE REFINEMENT OPERATORS

- completion by complements

$$\mathcal{R}_{\neg} : uco(C) \to uco(C)$$

- $\mathcal{R}_{\neg}(a)$, $a \in uco(C)$ (abstract domain)

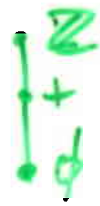
  (when possible) upgrades $\underline{a}$ by adding (lattice-theoretic) complements of its elements

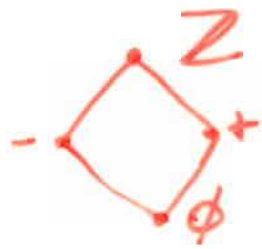
AN EXAMPLE OF COMPLETION BY COMPLEMENTS

- concrete domain $\wp(\mathbb{Z}), \subseteq$

- abstract domains

$A_1 =$ 

$A_2 =$ 

- $\mathcal{R}_\neg(A_1) = \mathcal{R}_\neg(A_2) =$ 

MORE REFINEMENT OPERATORS

- reduced cardinal power

B^A, B (base), A (exponent) $\in uco(C)$

the set of all monotonic functions

$A \xrightarrow{m} B$ (cardinal power in lattice theory)

reduced with respect to concretization

(we identify functions which represent the same properties)

in the original definition (based on Galois insertions)

$C = \wp(X)$

$\alpha_A : A \to C$ $\qquad$ $\alpha_B : B \to C$

$\gamma_A : C \to A$ $\qquad$ $\gamma_B : C \to b$

the abstraction function of B^A

$\alpha = \lambda P.\, \lambda x.\ \underbrace{\alpha_B(P \cap \gamma_A(x))}$ $\qquad$ $P \subseteq X$

for any P

~~count~~ how P changes when put in conjunction with elements of the exponent abstract domain

- with closure operators

$A = \rho_A(C)$, $B = \rho_B(C)$

the function $\lambda x \in A.\, \rho_B(d \wedge x) : A \mapsto B$, $d \in C$

represents a dependency

- the reduced cardinal power is the set of all such dependencies

$B^A = \{\lambda x \in A.\, \rho_B(d \wedge x) \mid d \in C\}$

REDUCED CARDINAL POWER

- the idea is to model dependencies among properties defined by the two domains

  → relational analysis to improve the precision

  - remember properties such as

    "X is ground if Y is ground"

    "X and Y ~~share~~ do not share if Z is free"

- difficult to see on Sign-related abstractions in the present form

  we will show an "almost" equivalent formulation, easier to handle

TOWARDS A LOGICAL INTERPRETATION OF REFINEMENTS

- if the concrete domain C is structured as $\wp(X)$
  - a property is modeled by
    - an abstract domain or
    - an upper closure operator
- some refinement operators can be viewed as completions, which allow to model
  - property ~~[illegible]~~ conjunction (reduced product)
  - property disjunction (disjunctive completion)
  - negation of properties (completion by complements) (under suitable conditions)
- what is the logical interpretation of reduced cardinal power?

  which, in principle, allows us to handle dependencies among properties and should, therefore, be the basic component of (more accurate) relational analyses?

THE LOGICAL RECONSTRUCTION OF A DOMAIN FOR SIGN ANALYSIS BY MEANS OF REFINEMENTS

1. Basic properties

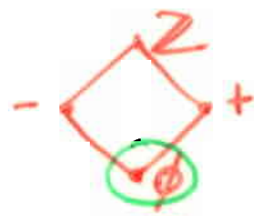
A_1 (the property of being "positive")

A_2 (the property of being "zero")

A_3 (the property of being "negative")

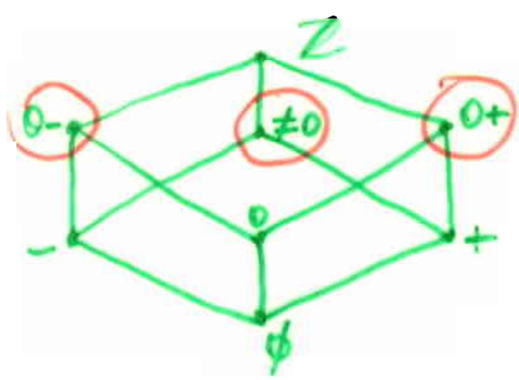
2. Refined domains

$A_4 = A_1 \sqcap A_3$



$A_5 = A_4 \sqcap A_2$

$A_6 = \mathcal{R}_v(A_5)$



HOW TO MODEL DEPENDENCIES IN LOGIC
(towards a logical characterization of reduced cardinal power)

- the interesting logical operator is "implication"

  given properties φ and ψ,

  $\varphi \to \psi$ tells us that whenever φ holds, then ψ holds too

  $\Downarrow$

- enhance a given abstract domain of properties to include the space of all the above implications built from every pair of its elements

- if a, b are elements of the abstract domain A

  the enhancement of A should contain relational objects (implications) $a \to b$, with the following property

  $a \wedge (a \to b)$ is approximated by b ($\approx$ modus ponens)

  $$a \wedge \boxed{(a \to b)} \leq b$$

  - we have many choices for an element c representing the implication $a \to b$
  - a best choice exists if the complete lattice is a Heyting algebra
    - models of intuitionistic logic
  - the implication has to be understood as intuitionistic implication

    $a \to b$ means that a proof for a can be transformed into a proof for b

HEYTING COMPLETION

C : concrete domain

$a\ b \in C$

$$a \to b = lub_C \{ d \mid glb_C(a,d) =_C b \}$$

$A, B \subseteq C$ Moore families (set of fixpoints of two closure operators on C)

$$A \to B = \{ a \to b \mid a \in A,\ b \in B \}$$

this is not necessarily a Moore family

- the Heyting completion

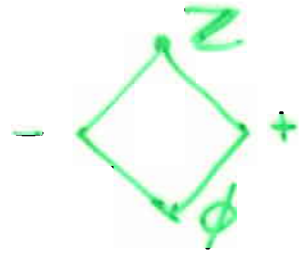
$$A \stackrel{\wedge}{\to} B =$$ the most abstract Moore family containing $A \to B$

the Moore completion of $A \to B$

AN EXAMPLE

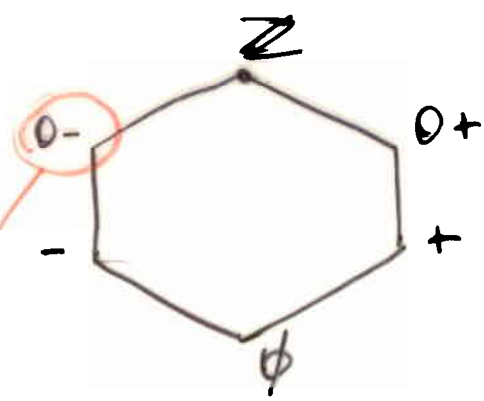
$= \wp(Z), \subseteq$

A



is a Moore family

$A \to A$



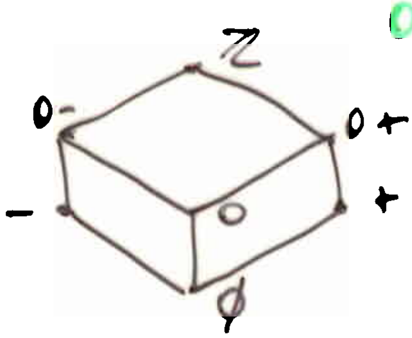
not a Moore family

$a = +$
$b = \emptyset$

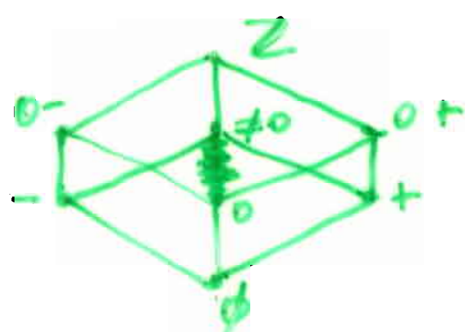
$\bigcup\{d \mid \sqcap(+,d) \subseteq \emptyset\}$

0−

$A \xrightarrow{\wedge} A$



$(A \xrightarrow{\wedge} A) \xrightarrow{\wedge} (A \xrightarrow{\wedge} A)$



HEYTING COMPLETION AND REFINEMENTS

- reduced cardinal power

$$B^A \equiv A \xrightarrow{\lambda} B$$

- nice algebraic properties relate the various refinements - completions

algebra of domain operators

APPLICATIONS TO LOGIC PROGRAMS

- groundness

  $$DEF = G \xrightarrow{\sim} G$$
  $$POS = DEF \xrightarrow{\sim} DEF$$
  $$POS = POS \xrightarrow{\sim} POS$$

- (polymorphic) types
  - similar hierarchy modeling "directional types"

- sharing & freeness

  NS   simple non pair-sharing
  F   freeness
  - a powerful and precise new domain

  $$(NS \sqcap F) \xrightarrow{\sim} (NS \sqcap F)$$