Abstraction I

Informal Introduction to Abstract Interpretation

(based on Patrick Cousout's 2005 course "Abstract Interpretation")

UNI FREIBURG

Albert-Ludwigs-Universität Freiburg

Manuel Geffken

2014-06-04

A little graphical language

UNI FREIBURG

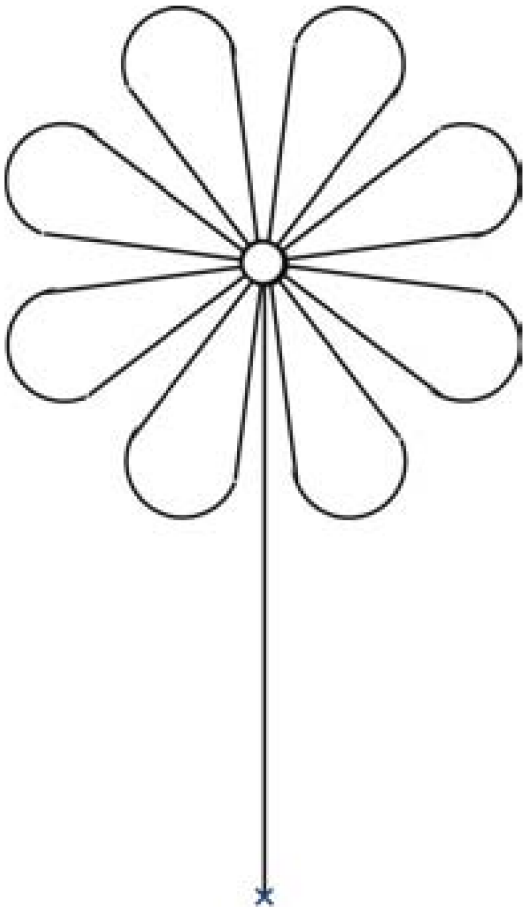
- objects;
- operations on objects.

Objects

An object is a pair

- an origin (a reference point $\times$);
- a finite set of black pixels (on a white background).

Example of an object: a flower



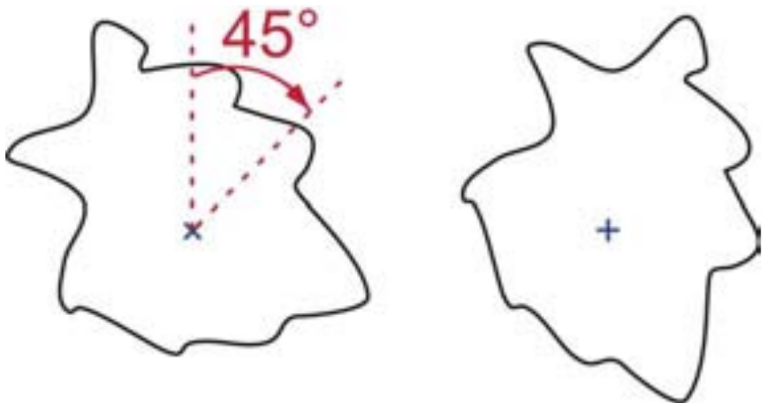
Operations on objects: constants

- constant objects;
  for example

petal $=$ 

Operations on objects: rotation

- rotation r[a](o) of object o of some angle a around the origin):

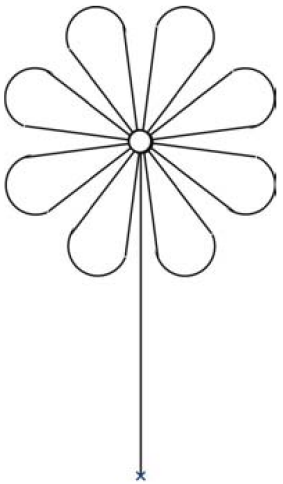


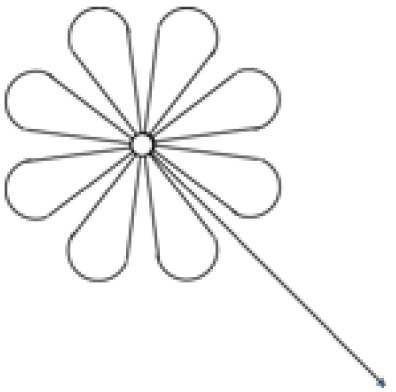
Example 1 of rotation

petal = 

r[45](petal) = 

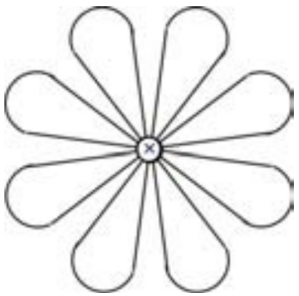
Example 2 of rotation

flower $=$ 

r[−45](petal) $=$ 

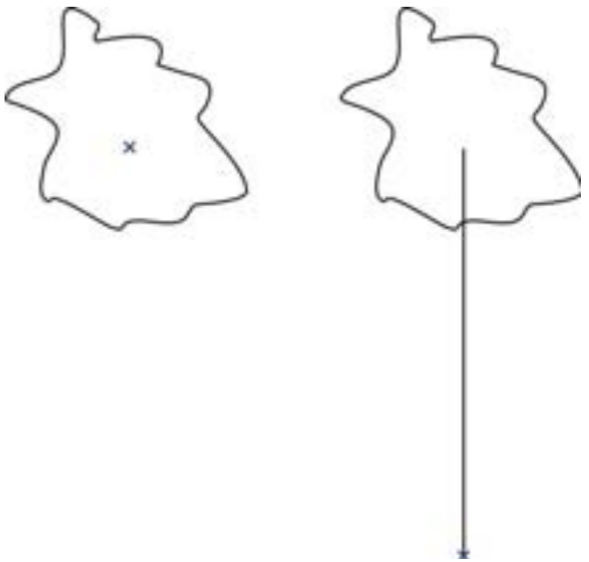
Operations on objects : union

- union $o_1 \cup o_2$ of objects o_1 and o_2 = superposition at the origin;
  for example:
  corolla = petal ∪ r[45](petal) ∪ r[90](petal) ∪ r[135](petal) ∪ r[180](petal) ∪ r[225](petal) ∪ r[270](petal) ∪ r[315](petal)



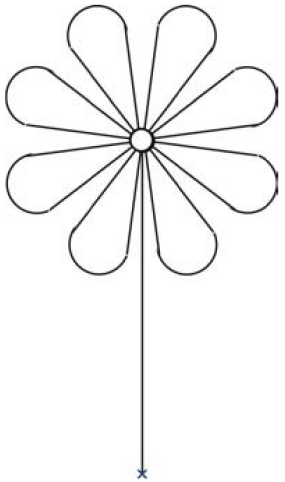
Operations on objects : add a stem

- stem(o) adds a stem to an object o (up to the origin, with new origin at the root);



Flower

$$\text{flower} = \text{stem}(\text{corolla})$$



Fixpoints

UNI FREIBURG

- $\mathsf{corolla} = \mathsf{lfp}^{\subseteq} F$
  $F(X) = \mathsf{petal} \cup \mathsf{r}[45](X)$

Contraints

- A corolla is the $\subseteq$-least object X satisfying the two constraints:
  - A corolla contains a petal:
    $$\text{petal} \subseteq X$$
  - and, a corolla contains its own rotation by 45 degrees:
    $$\text{r}[45](X) \subseteq X$$
- Or, equivalently [1]:
  $$F(X) \subseteq X, \quad \text{where} \quad F(X) = \text{petal} \cup \text{r}[45](X)$$

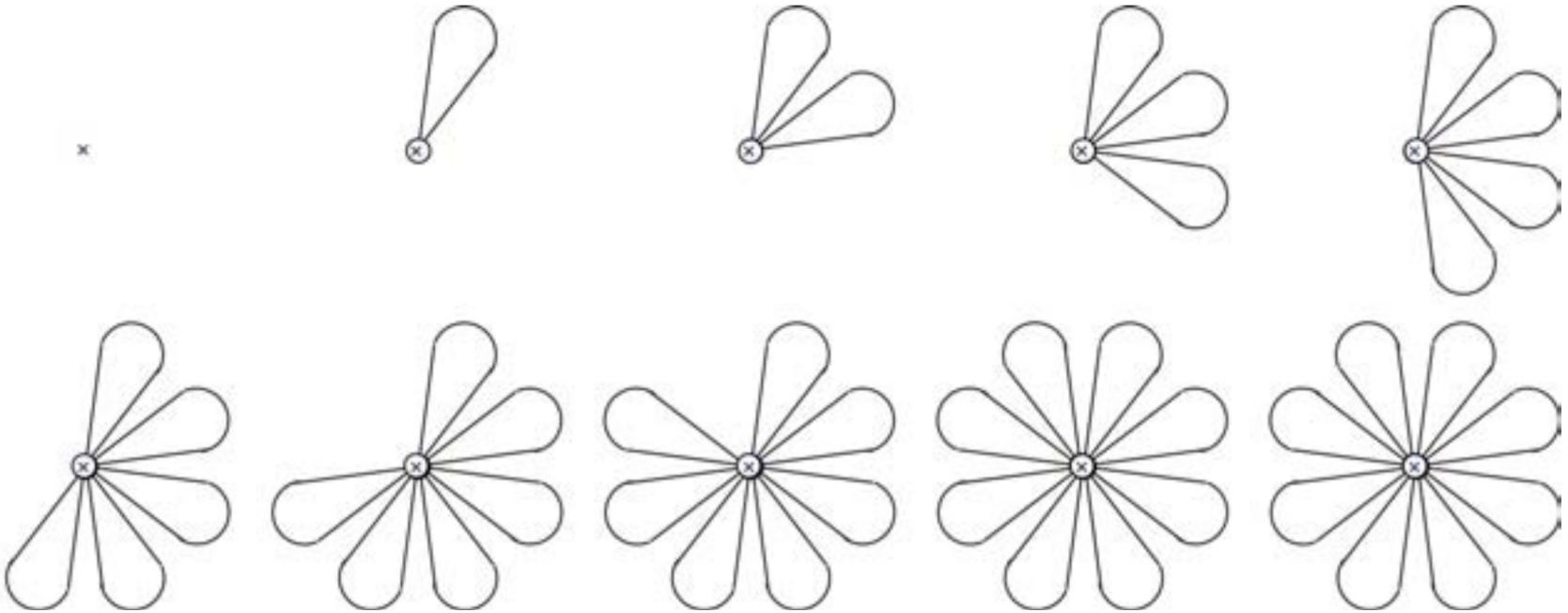
[1] By Tarski's fixpoint theorem, the least solution is $\text{lfp}^{\subseteq} F$.

Iterates to fixpoints

- The iterates of F from the bottom $\emptyset$ are:

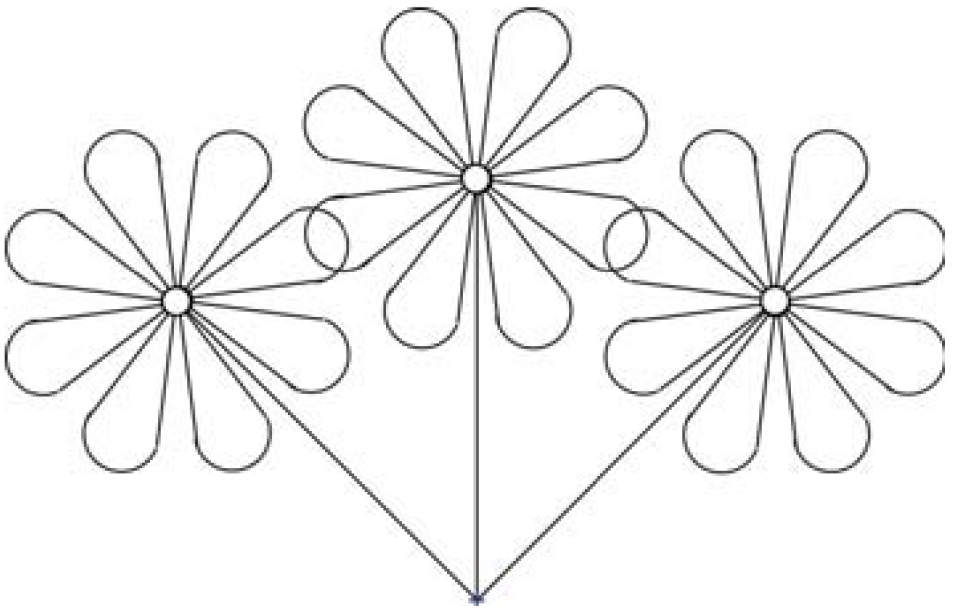
$$
\begin{aligned}
X^0 &= \emptyset, \\
X^1 &= F(\emptyset), \\
&\dots\ \dots\ \dots, \\
X^{n+1} &= F(X^n), \\
&\dots\ \dots\ \dots, \\
\mathsf{lfp}^{\subseteq} F = X^\omega &= \bigcup_{n \leq 0} X^n.
\end{aligned}
$$

Iterates for the corolla



The bouquet

- bouquet = r[-45](flower) ∪ flower ∪ r[45](flower)
- The bouquet:

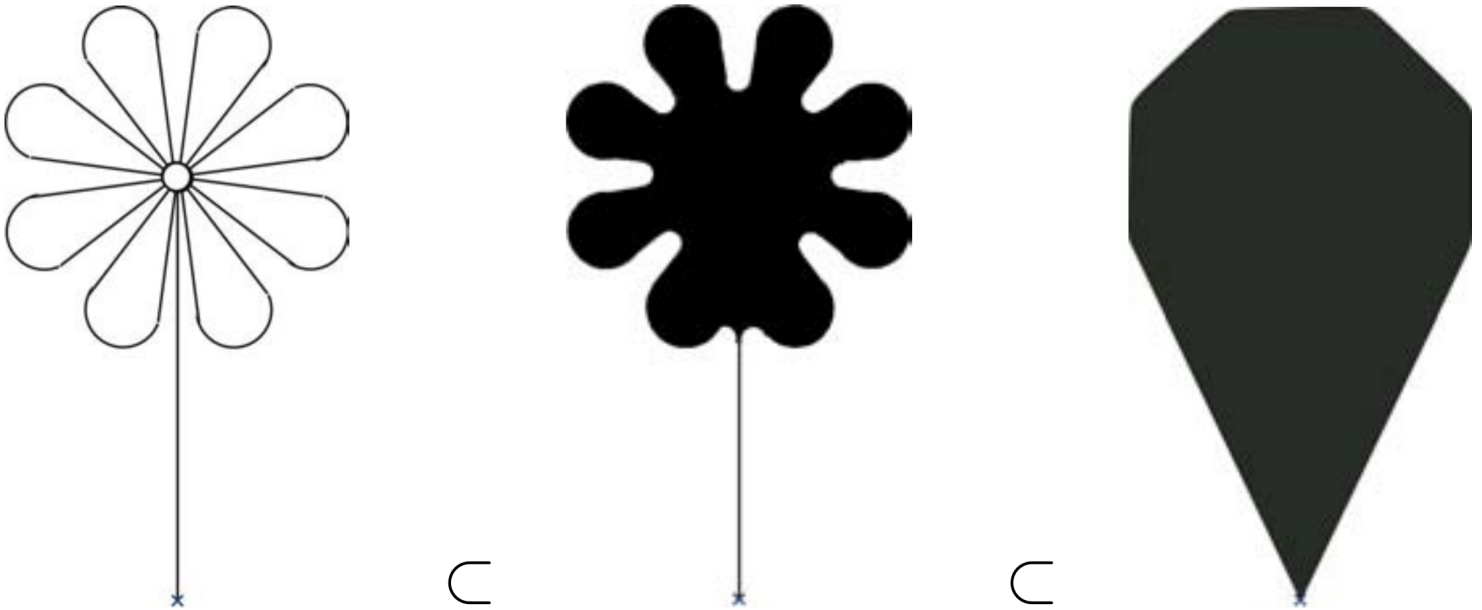


Upper-approximation

UNI FREIBURG

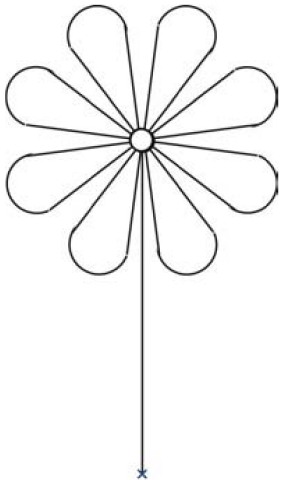
- An upper-approximation of an object is an object with:
  - same origin;
  - more pixels.

Examples of upper-approximations of flowers

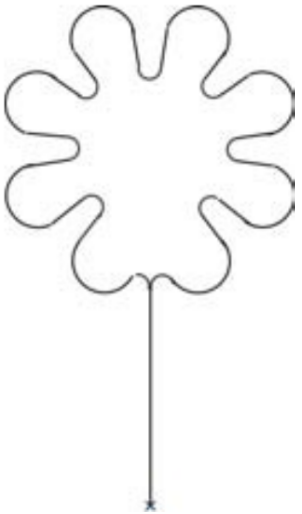


Abstract objects

- an abstract object is a mathematical/computer representation of an approximation of a concrete object;



concrete object



abstract object

$\sqsubseteq$

more abstract object

Abstract domain

UNI FREIBURG

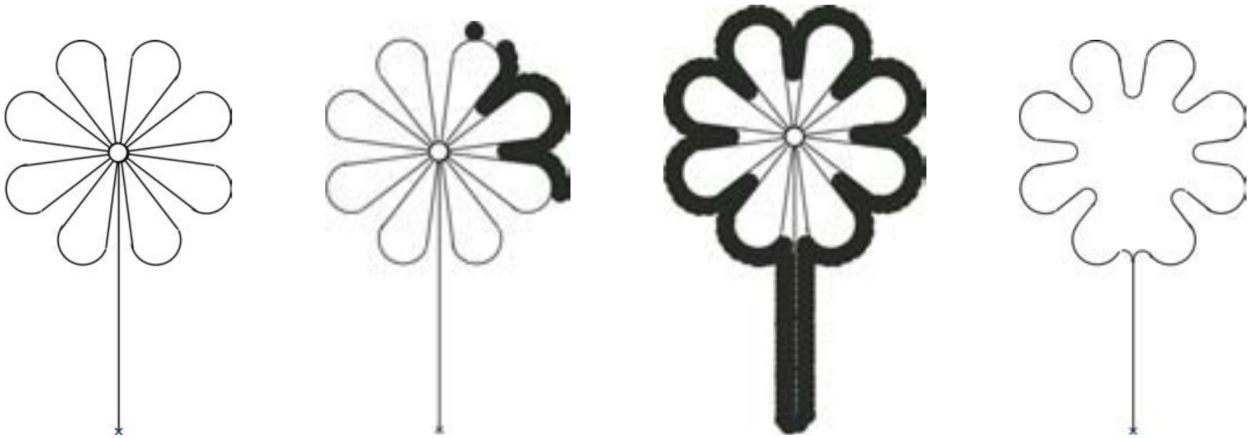
- an abstract domain is a set of abstract objects plus abstract operations (approximating the concrete ones);

Abstraction

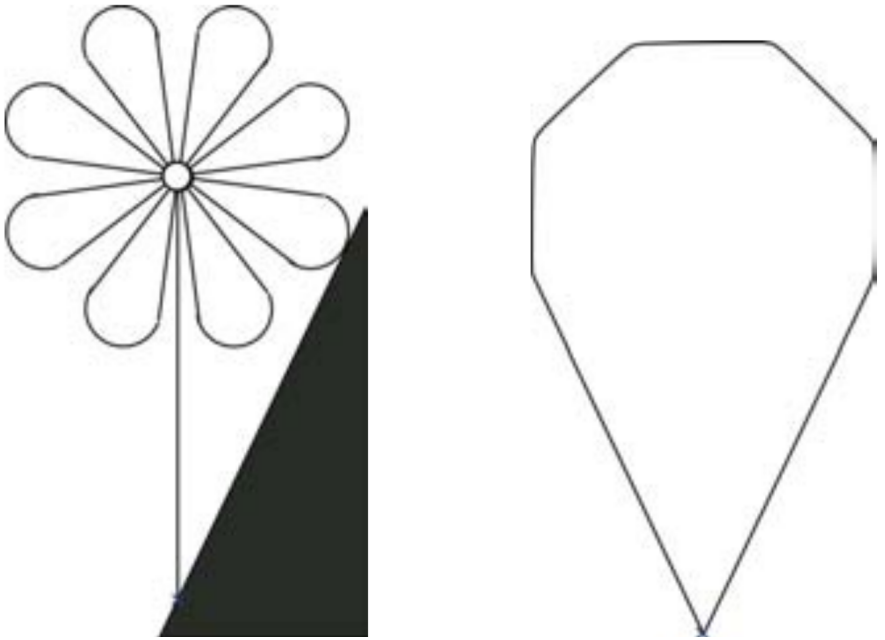
UNI FREIBURG

- an abstraction function α maps a concrete object o to an approximation represented by an abstract object $\alpha(o)$.

Example 1 of abstraction



Example 2 of abstraction



Comparing abstractions

UNI FREIBURG

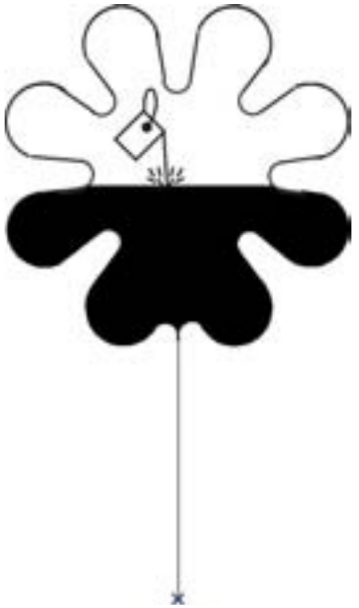
- larger pen diameters: more abstract;
- different pen shapes: may be non comparable abstractions

Concretization

UNI FREIBURG

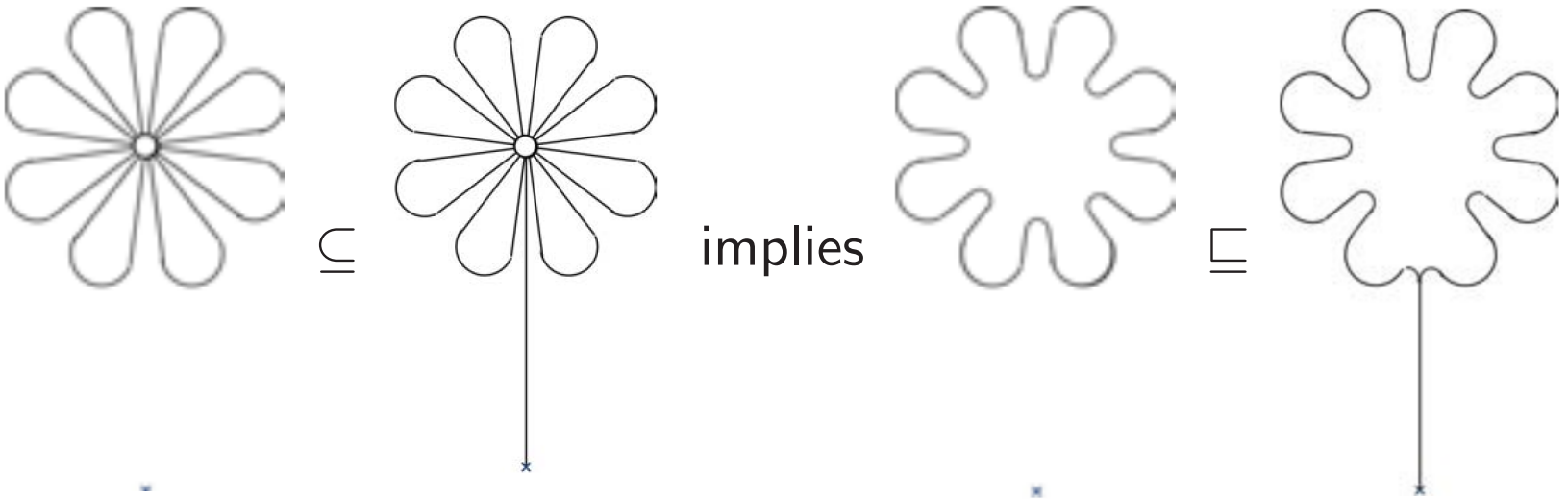
- a concretization function γ maps an abstract object $\overline{o}$ to the concrete object $\gamma(\overline{o})$ that it represents (that is to its concrete meaning/semantics).

Example of concretization



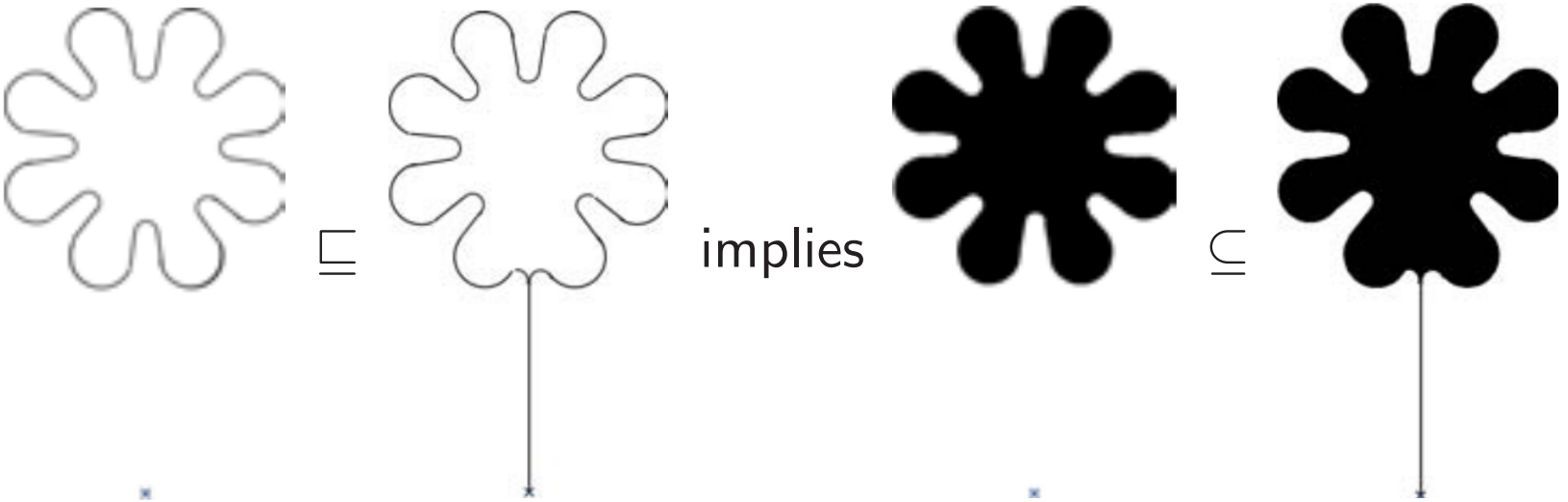
Galois connection 1/4

- α is monotonic.



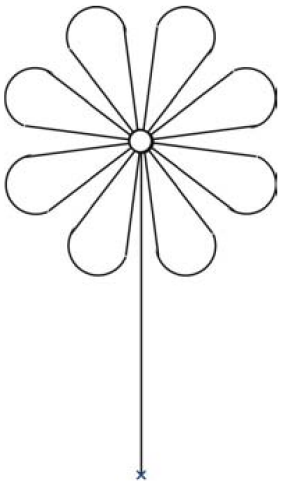
Galois connection 2/4

- γ is monotonic.

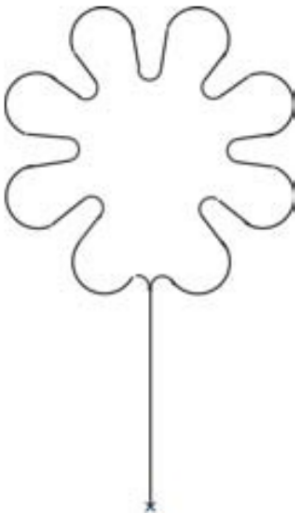


Galois connection 3/4

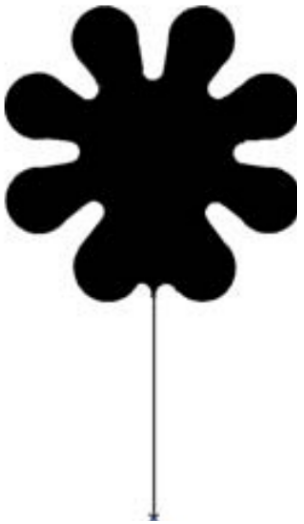
- for all concrete objects $x, \gamma \circ \alpha(x) \supseteq x$.



flower



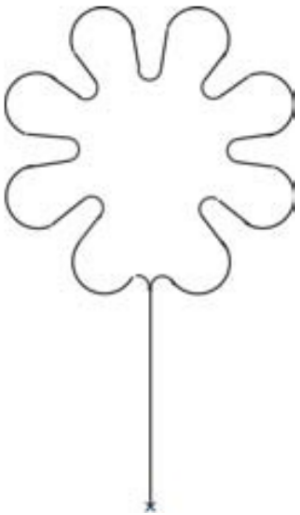
α(flower)



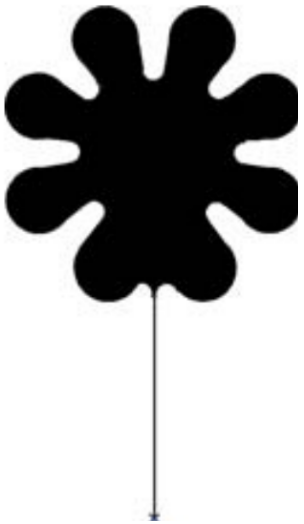
$\gamma(\alpha$(flower))

Galois connection 4/4

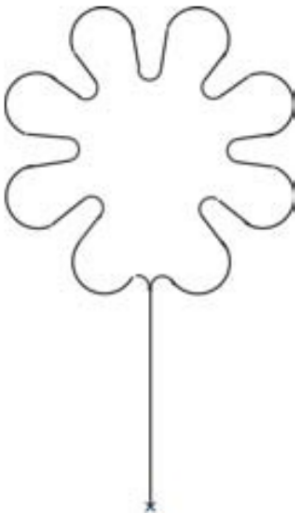
- for all abstract objects $y, \alpha \circ \gamma(y) \sqsubseteq y$.



abstract flower



γ(abstract flower)



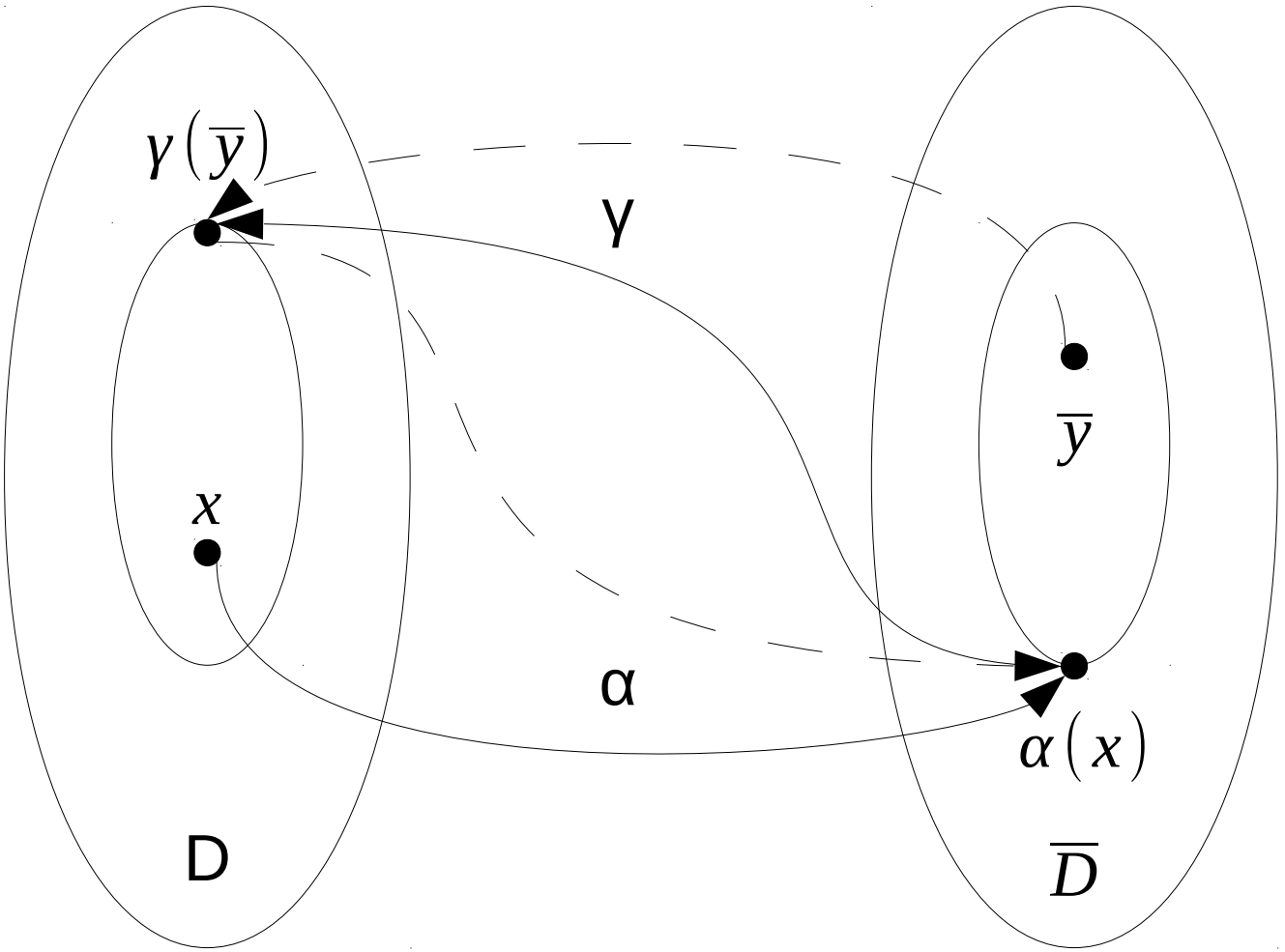
$\alpha(\gamma$(abstract flower))

Galois connections

$$\langle \mathcal{D}, \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{\mathcal{D}}, \sqsubseteq \rangle$$

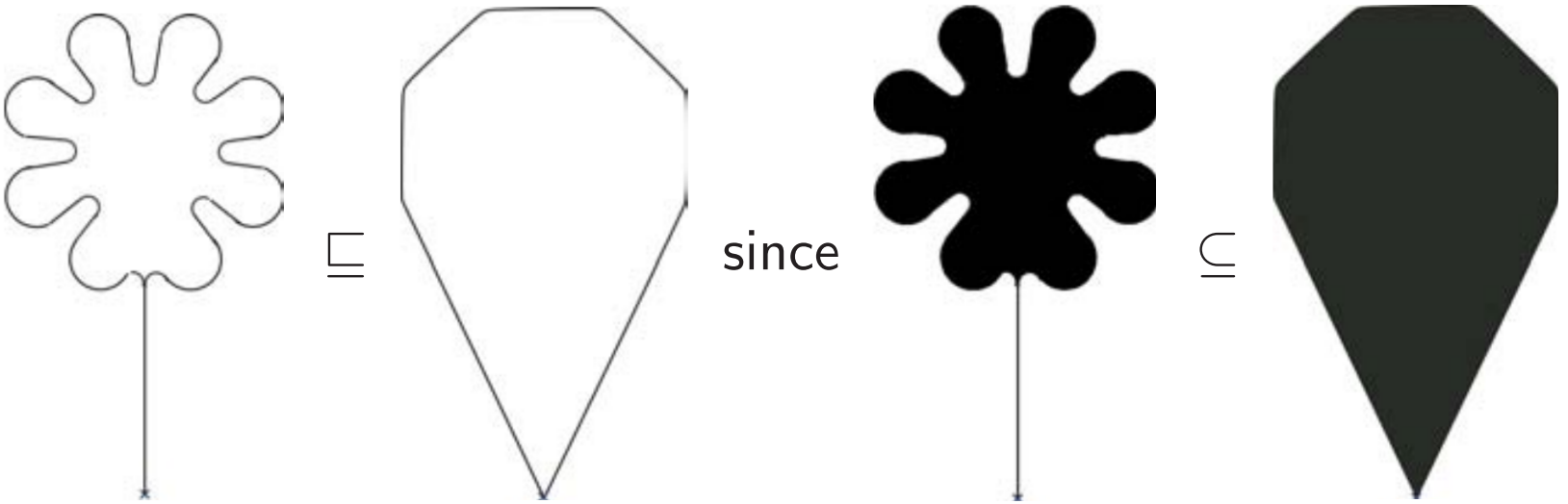
$$\begin{aligned}
\text{iff} \quad & \forall x, y \in \mathcal{D} : x \subseteq y \Rightarrow \alpha(x) \sqsubseteq \alpha(y) \\
& \wedge \forall \overline{x}, \overline{y} \in \overline{\mathcal{D}} : \overline{x} \sqsubseteq \overline{y} \Rightarrow \gamma(\overline{x}) \subseteq \gamma(\overline{y}) \\
& \wedge \forall x \in \mathcal{D} : x \subseteq \gamma(\alpha(x)) \\
& \wedge \forall \overline{y} \in \overline{\mathcal{D}} : \alpha(\gamma(\overline{y})) \subseteq \overline{y} \\
\text{iff} \quad & \forall x \in \mathcal{D}, \overline{y} \in \overline{\mathcal{D}} : \alpha(x) \sqsubseteq \overline{y} \Leftrightarrow x \subseteq \gamma(\overline{y})
\end{aligned}$$

Galois connections (illustrated)



Abstract ordering

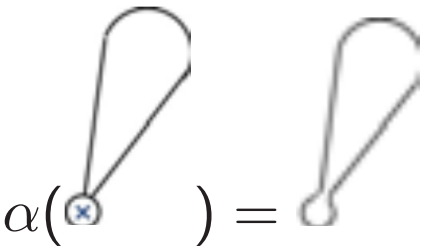
- $x \sqsubseteq y$ is defined as $\gamma(x) \subseteq \gamma(y)$



Specification of abstract operations

- $\overline{op/0} \stackrel{def}{=} \alpha(op/0)$ 0-ary
- $\overline{op/1}(y) \stackrel{def}{=} \alpha(op/1(\gamma(y)))$ unary
- $\overline{op/2}(z) \stackrel{def}{=} \alpha(op/2(\gamma(y), \gamma(z)))$ binary
- ...

Abstract petal



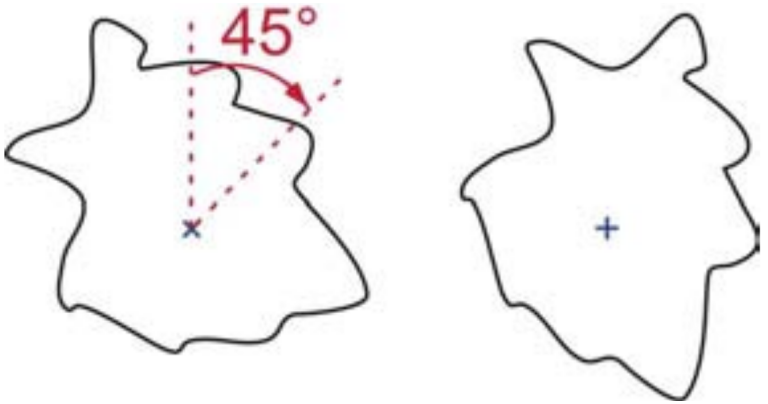
Abstract rotations

UNI FREIBURG

- $\bar{\mathsf{r}}[a](y) = \alpha(\mathsf{r}[a](\gamma(y)))$

Abstract rotations

- $\bar{\mathsf{r}}[a](y) = \alpha(\mathsf{r}[a](\gamma(y)))$
  $= \mathsf{r}[a](y)$



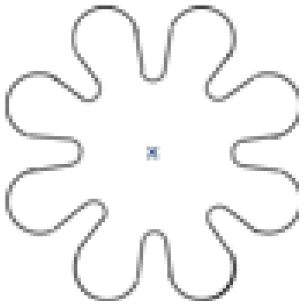
A commutation theorem on abstract rotations

UNI FREIBURG

- $\alpha(\mathsf{r}[a](x))$
  $= \alpha(\gamma(\alpha(\mathsf{r}[a](x))))$
  $= \alpha(\gamma(\mathsf{r}[a](\alpha(x))))$
  $= \alpha(\mathsf{r}[a](\gamma(\alpha(x))))$
  $= \bar{\mathsf{r}}[a](\alpha(x))$

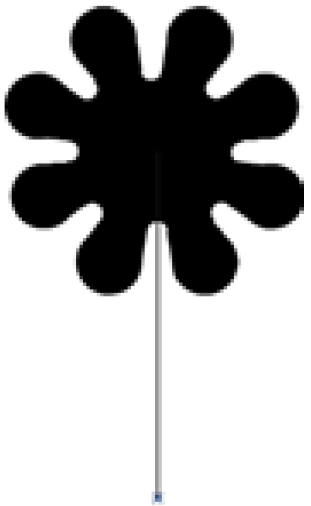
Abstract stems

- $\overline{\text{stem}}(y) = \alpha(\text{stem}(\gamma(y)))$

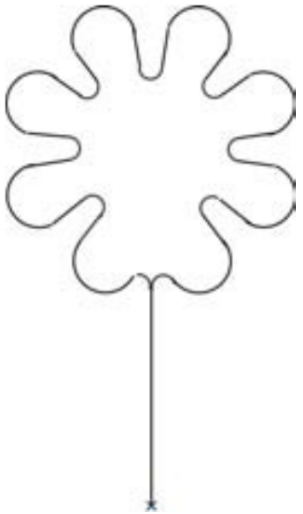


abstract corolla

γ(abstract corolla)



stem(γ(abstract corolla))



α(stem(γ(abstract corolla)))

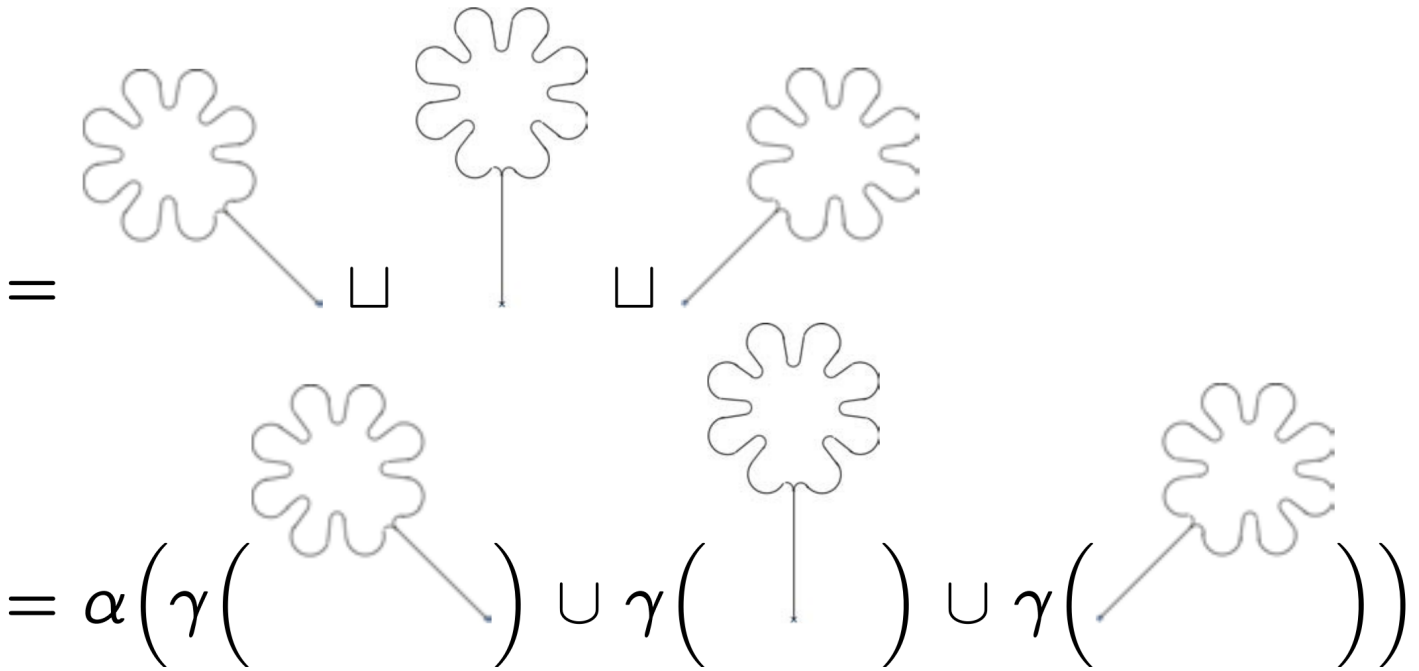
Abstract stems

UNI FREIBURG

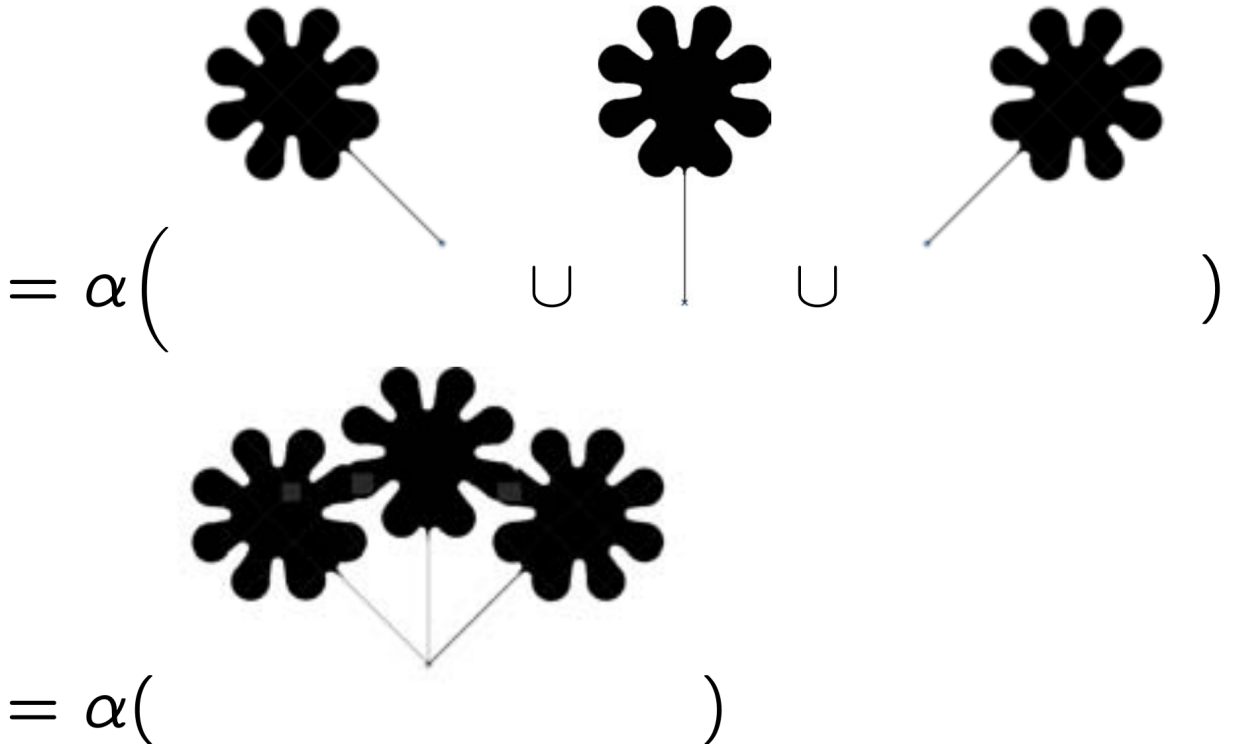
- $x \sqcup y = \alpha(\gamma(x) \cup \gamma(y))$

Abstract bouquet

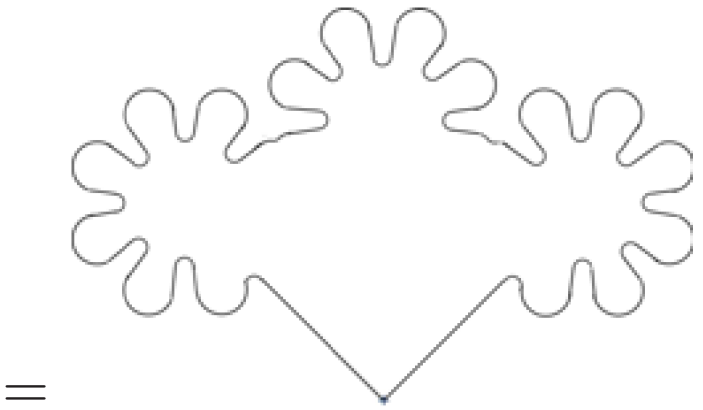
abstract bouquet



Abstract bouquet: (continued)



Abstract bouquet: (end)



A theorem on the abstract bouquet

UNI FREIBURG

abstract flower $= \alpha$(concrete flower)

abstract bouquet

$= \bar{r}[-45]$(abtract flower) $\sqcup$ abtract flower $\sqcup \bar{r}[45]$(abtract flower)

$= \bar{r}[-45](\alpha$(concrete flower)) $\sqcup \alpha$(concrete flower) $\sqcup$ $\bar{r}[45](\alpha$(concrete flower))

$= \alpha$(r[-45](concrete flower)) $\sqcup \alpha$(concrete flower) $\sqcup$ α(r[45](concrete flower))

$= \alpha$(r[-45](concrete flower) $\cup$ concrete flower $\cup$ r[45](concrete flower))

$= \alpha$(concrete bouquet)

Abstract fixpoint

UNI FREIBURG

- abstract corolla $= \alpha(\text{concrete corolla}) = \alpha(\text{lfp}^{\subseteq} F)$
  where $F(X) = \text{petal} \cup \text{r}[45](X)$

Abstract transformer $\overline{F}$

- $\alpha(F(X))$
  $= \alpha(\text{petal} \cup \text{r}[45](X))$
  $= \alpha(\text{petal}) \sqcup \alpha(\text{r}[45](X))$
  $= \alpha(\text{petal}) \sqcup \bar{\text{r}}[45](\alpha(X))$
  $= \text{abstract petal} \sqcup \bar{\text{r}}[45](\alpha(X))$
  $= \overline{F}(\alpha(X))$

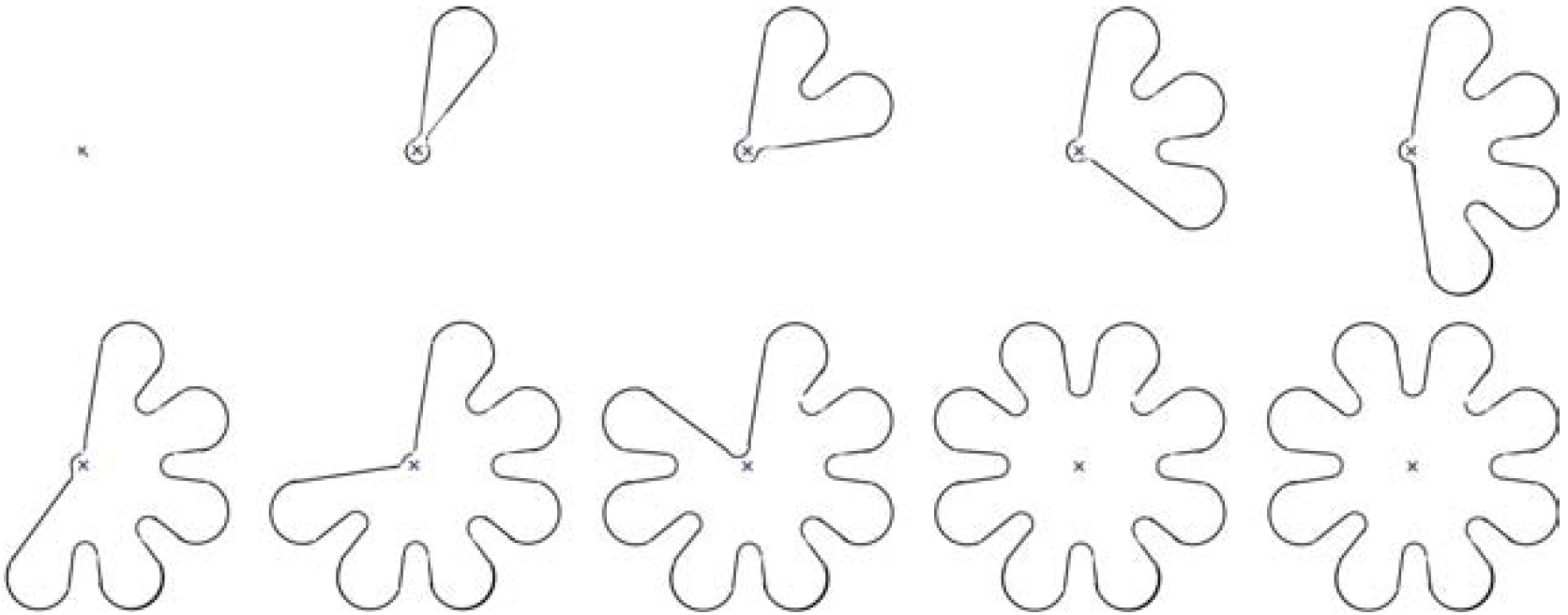
by defining

$$\overline{F}(X) = \text{abstract petal} \sqcup \bar{\text{r}}[45](X)$$

and so:

- abstract corolla $= \alpha(\text{concrete corolla}) = \alpha(\text{lfp}^{\subseteq} F) = \text{lfp}^{\sqsubseteq} \overline{F}$

Iterates for the abstract corolla



Abstract interpretation of the (graphic) language

UNI FREIBURG

- Similar, but by syntactic induction on the structure of programs of the language;

On abstracting properties of graphic objects

UNI FREIBURG

- A graphic object is a set of (black) pixels (ignoring the origin for simplicity);
- So a property of graphic objects is a set of graphic objects that is a set of sets of (black) pixels (always ignoring the set of origins for simplicity);
- Was there something wrong?

On abstracting properties of graphic objects

UNI FREIBURG

- No, because we implicitly used the following implicit initial abstraction:

$$\langle \wp(\wp(\mathcal{P})), \subseteq \rangle \underset{\alpha_0}{\overset{\gamma_0}{\leftrightarrows}} \langle \wp(\mathcal{P}), \subseteq \rangle$$

where:
$\mathcal{P}$ is a set of pixels (e.g. pairs of coordinates)
$\alpha_0(X) = \bigcup X$
$\gamma_0(Y) = \{G \in \mathcal{P} \mid G \subseteq Y\}$

Is it for fun (only)?

UNI FREIBURG

- Yes, but see image processing by morphological filtering:

  J. Serra. Morphological filtering: An overview,
  Signal Processing 38 (1994) 3–11.

  It can be entirely formalized by abstract interpretation.