ABSTRACT INTERPRETATION:
THEORY AND APPLICATIONS

P. Cousot

Patrick.Cousot@ens.fr http://www.di.ens.fr/~cousot

Second International Summer School in Computational Logic, ISCL 2002

25th—30th August 2002, Acquafredda di Maratea (Basilicata, Italy)

1. Abstract Interpretation told with flowers

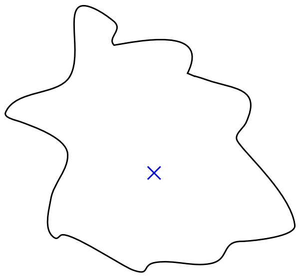
A little graphical language :

- objects;
- operations on objects.

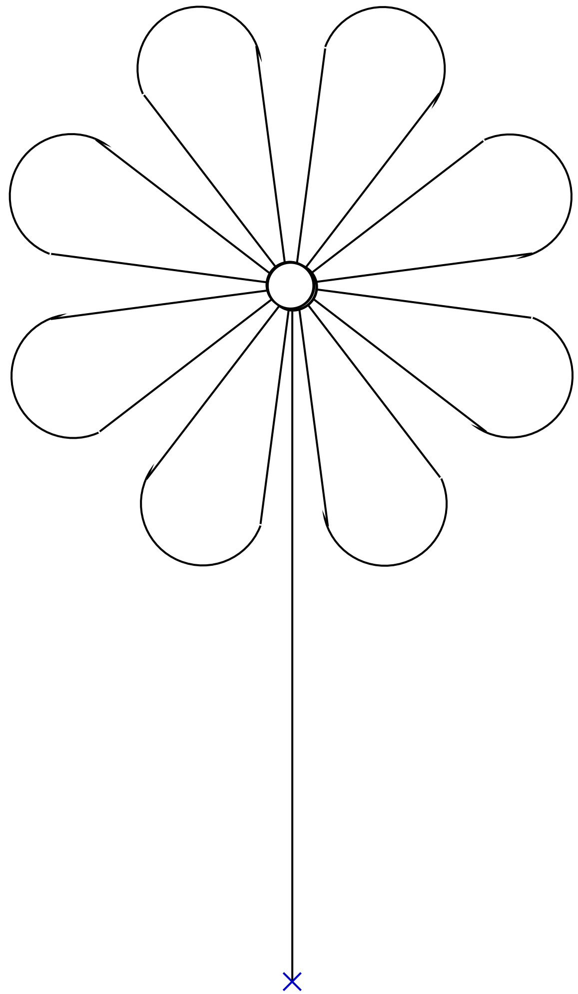
OBJECTS:

An object is a pair:

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



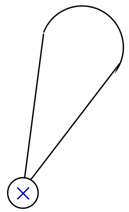
Example of an object: a flower



Operations on objects : constants

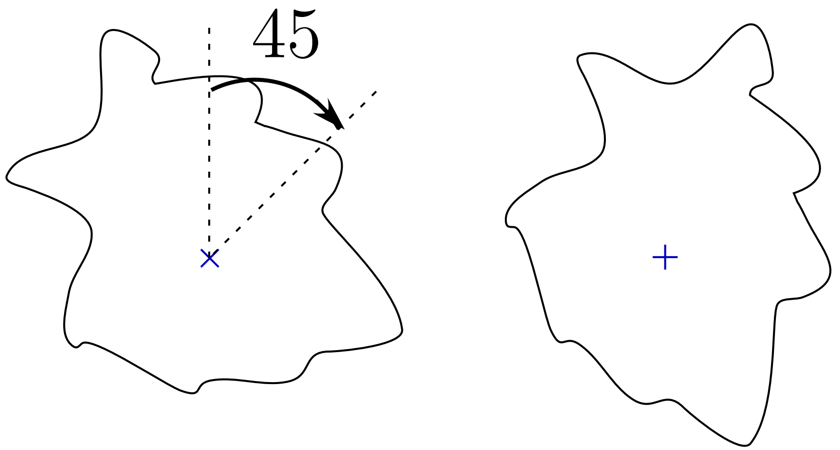
- constant objects;

  for example:

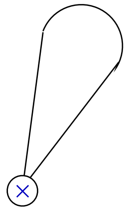
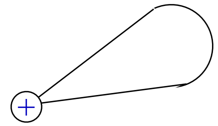
petal = 

Operations on objects : rotation

- rotation $\mathrm{r}[a](o)$ of objects o (of some angle a around the origin):

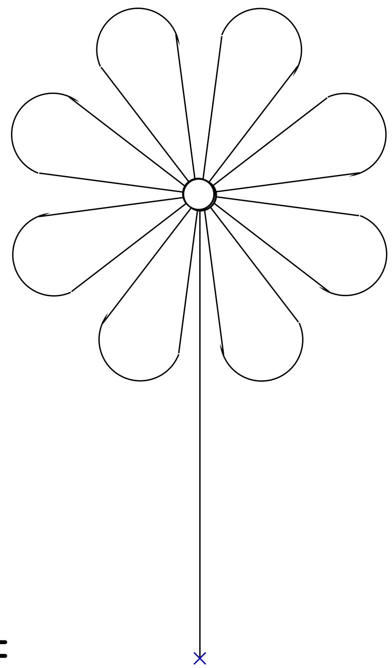


Example 1 of rotation:

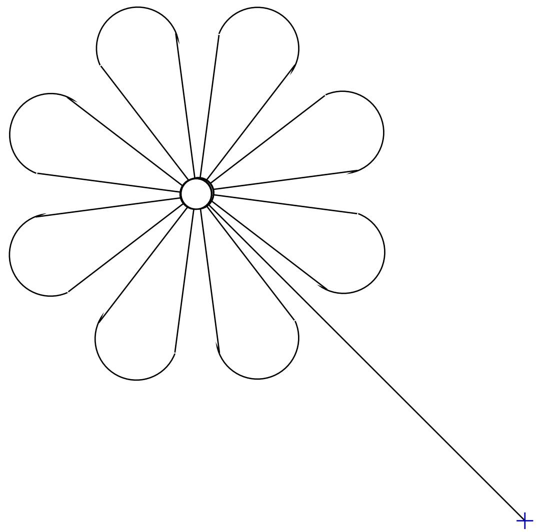
petal =    r[45](petal) = 

Example 2 of rotation:

flower =



r[-45](flower) =

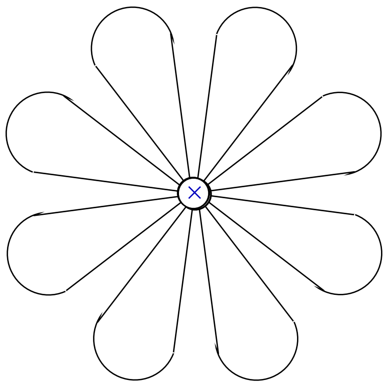


Operations on objects : union

- union $o_1 \cup o_2$ of objects o_1 and o_2 = superposition at the origin;

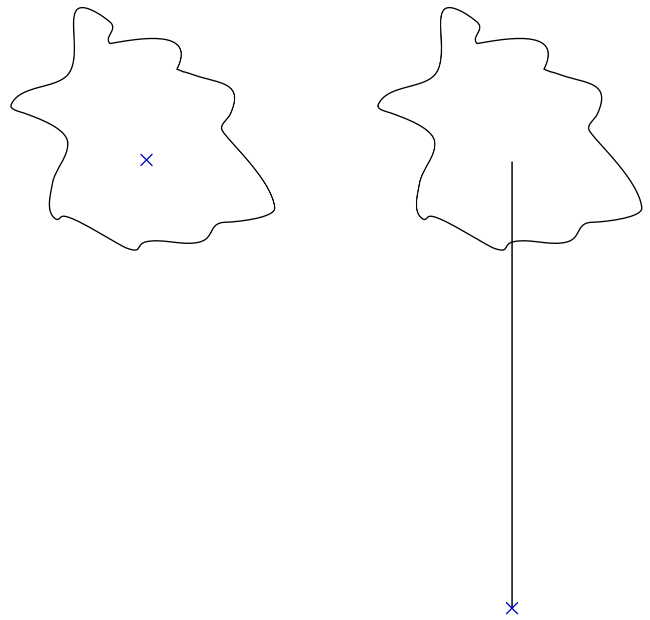
  for example:

  $$\text{corolla} = \text{petal} \cup \text{r}[45](\text{petal}) \cup \text{r}[90](\text{petal}) \cup \text{r}[135](\text{petal}) \cup \text{r}[180](\text{petal}) \cup \text{r}[225](\text{petal}) \cup \text{r}[270](\text{petal}) \cup \text{r}[315](\text{petal})$$



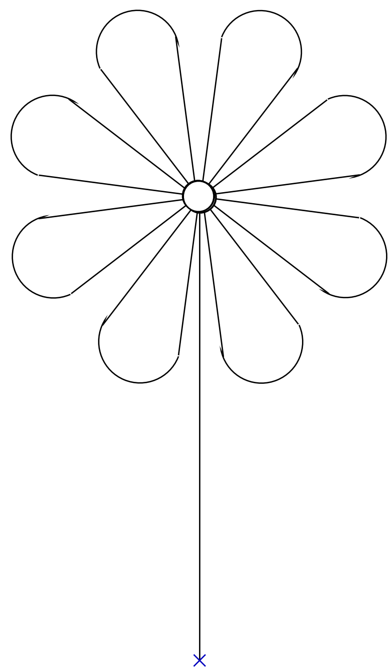
Operations on objects : add a stem

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



Flower:

flower = stem(corolla)



Fixpoints

- $\text{corolla} = \text{lfp}^{\subseteq}\ F$

  $F(X) = \text{petal} \cup \text{r}[45](X)$

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 degres:

  $$\text{r}[45](X) \subseteq X$$

- Or, equivalently [1]:

  $$F(X) \subseteq X, \qquad \text{where} \qquad F(X) = \text{petal} \cup \text{r}[45](X)$$

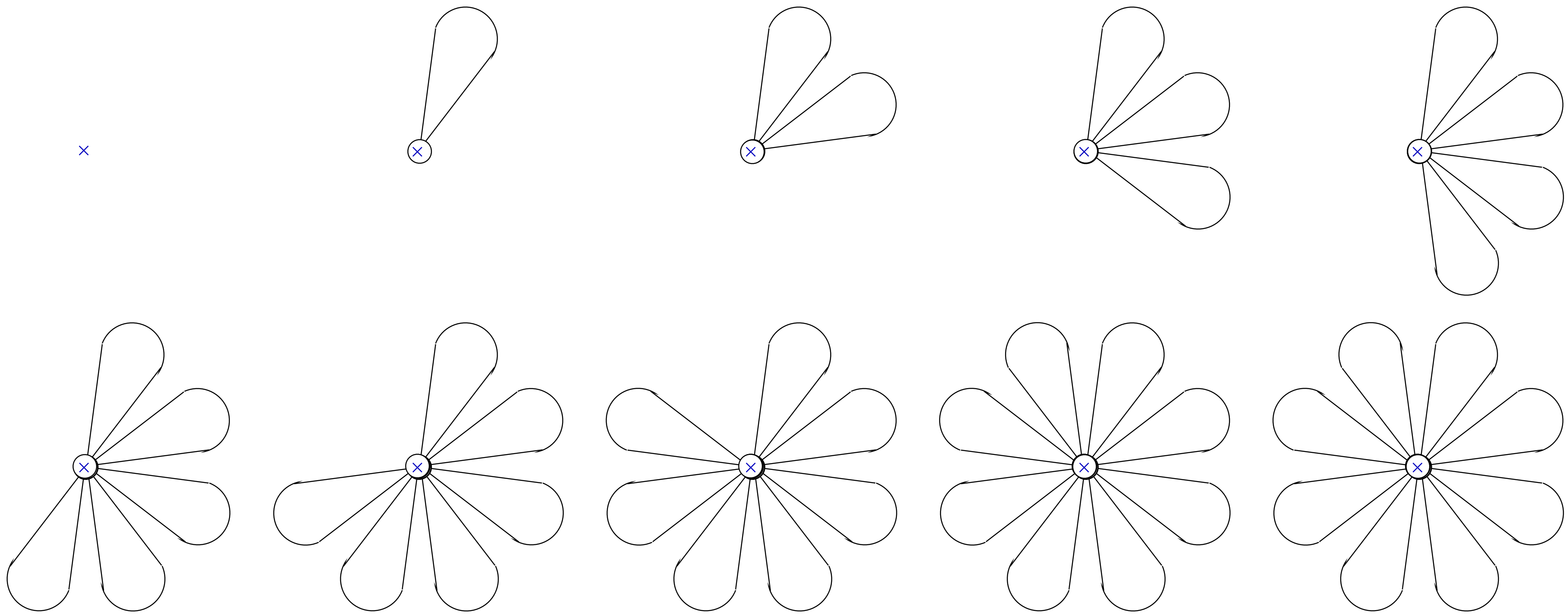
[1] By Tarski's fixpoint theorem, the least solution is $\text{lfp}^{\subseteq} F$.

Iterates to fixpoints

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

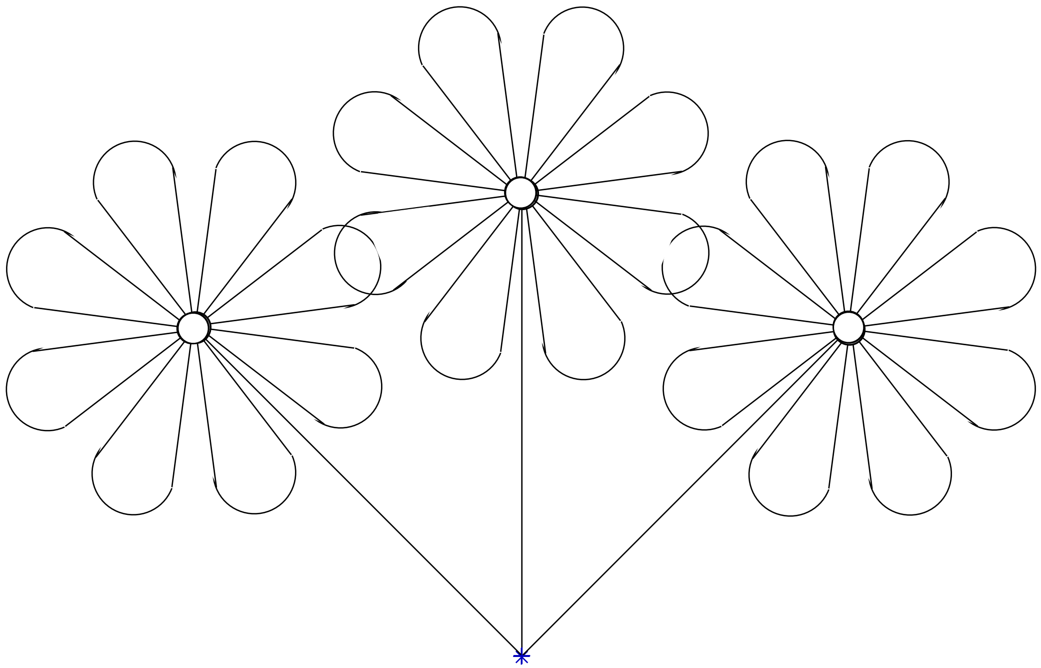
$$\begin{aligned} X^0 &= \emptyset \ , \\ X^1 &= F(X^0) \ , \\ \ldots &\ \ldots\ \ldots, \\ X^{n+1} &= F(X^n) \ , \\ \ldots &\ \ldots\ \ldots \ , \\ \operatorname{lfp}^{\subseteq} F &= X^\omega = \bigcup_{n \geq 0} X^n \ . \end{aligned}$$

ITERATES FOR THE COROLLA



The bouquet:

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



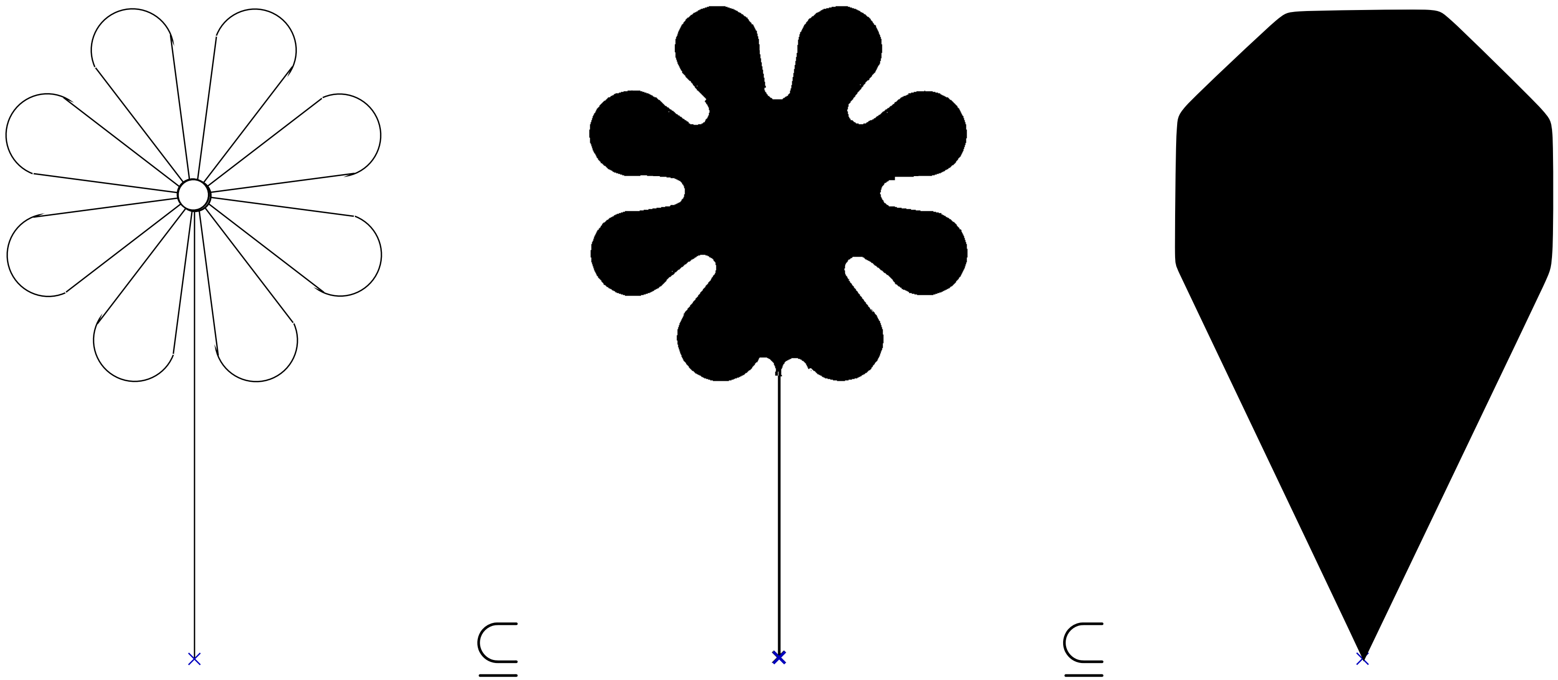
Upper-approximation

- An upper-approximation of an object is a object with:

  same origin;

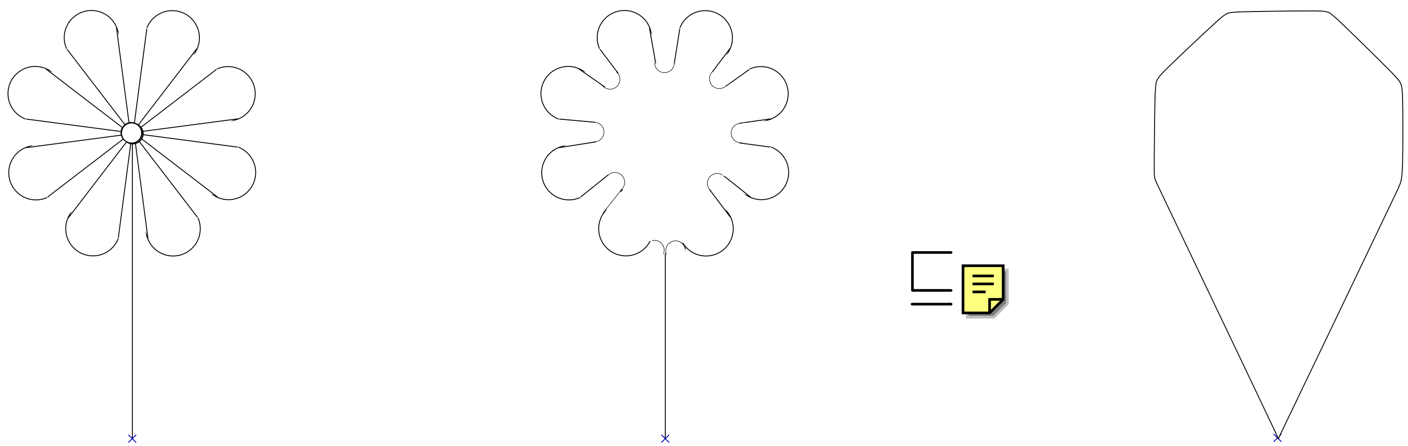
  more pixels.

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 more abstract object

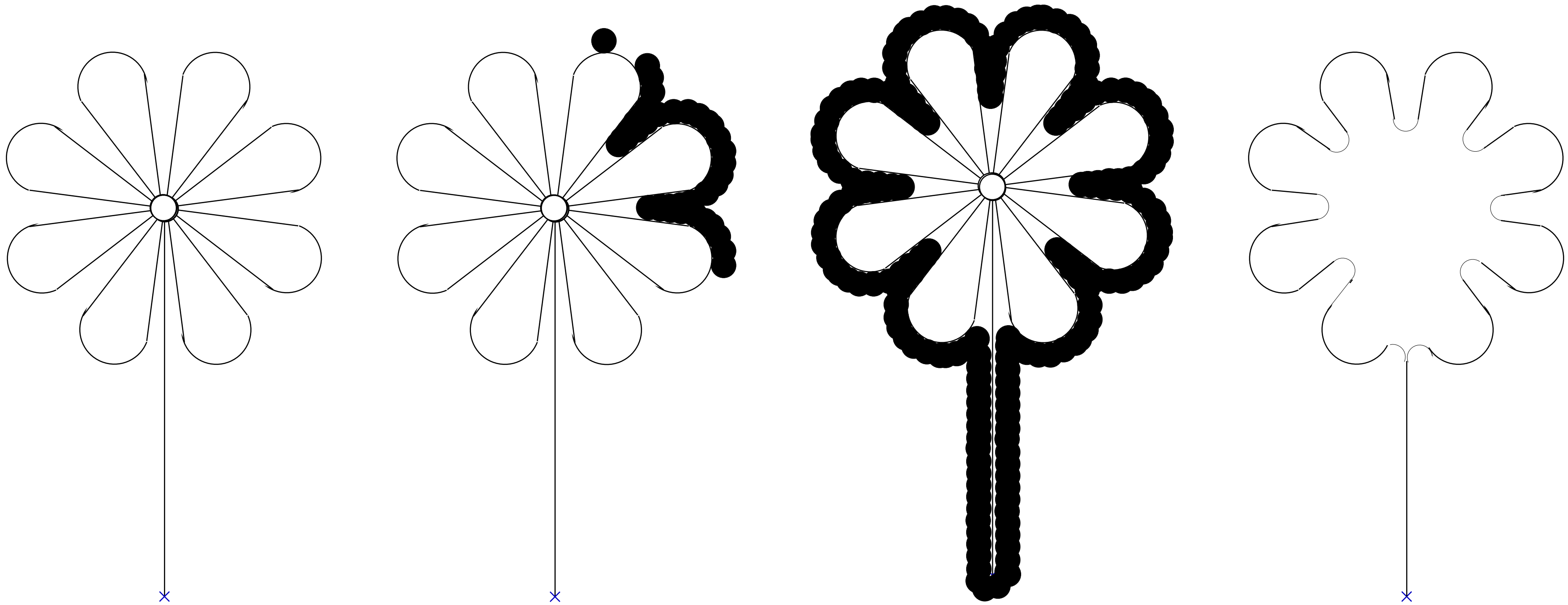
Abstract domain:

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

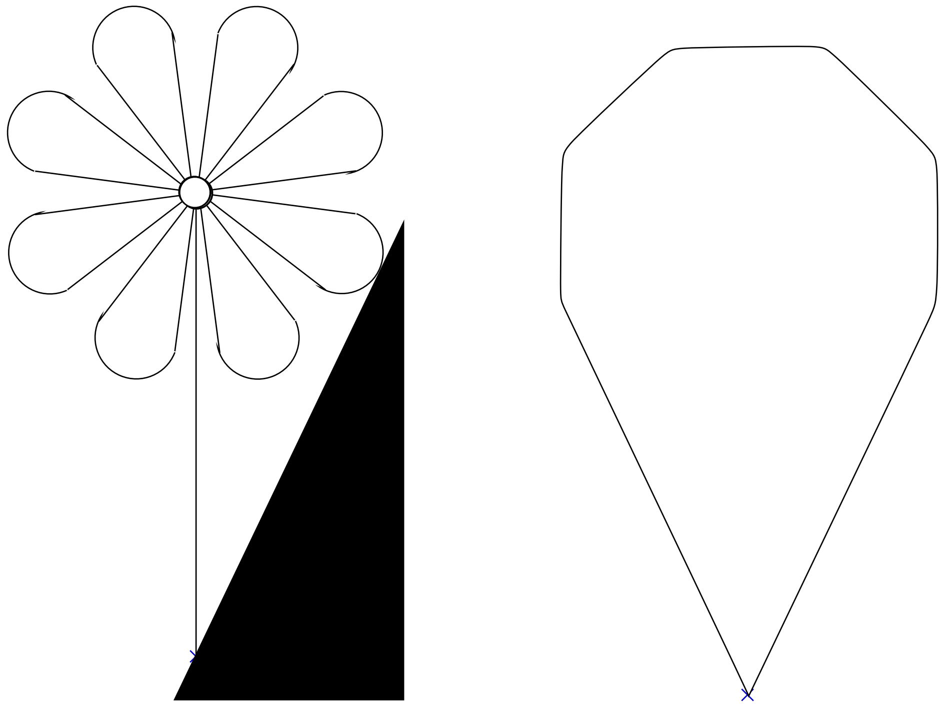
Abstraction:

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

Example of abstraction 1:



Example of abstraction 2:



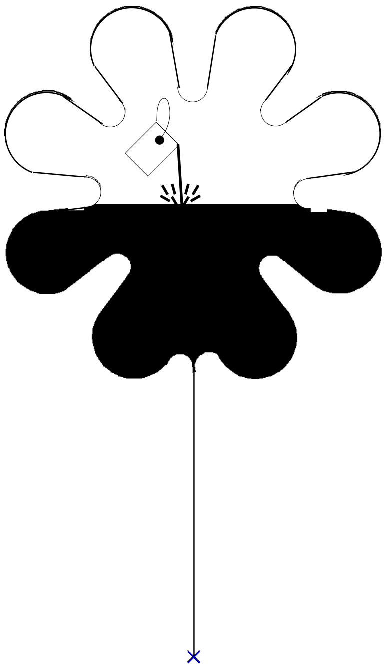
Comparing abstractions:

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

Concretization:

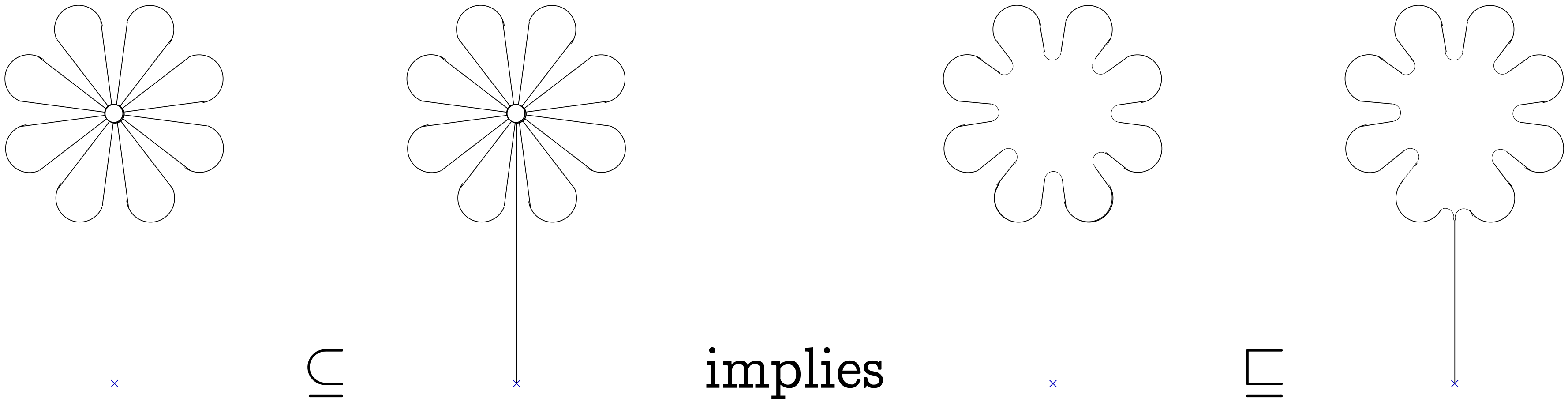
- a concretization function γ maps an abstract object $\overline{o}$ to the concrete object $\gamma(\overline{o})$ that is represents (that is to its concrete meaning/semantics).

Example of concretization:



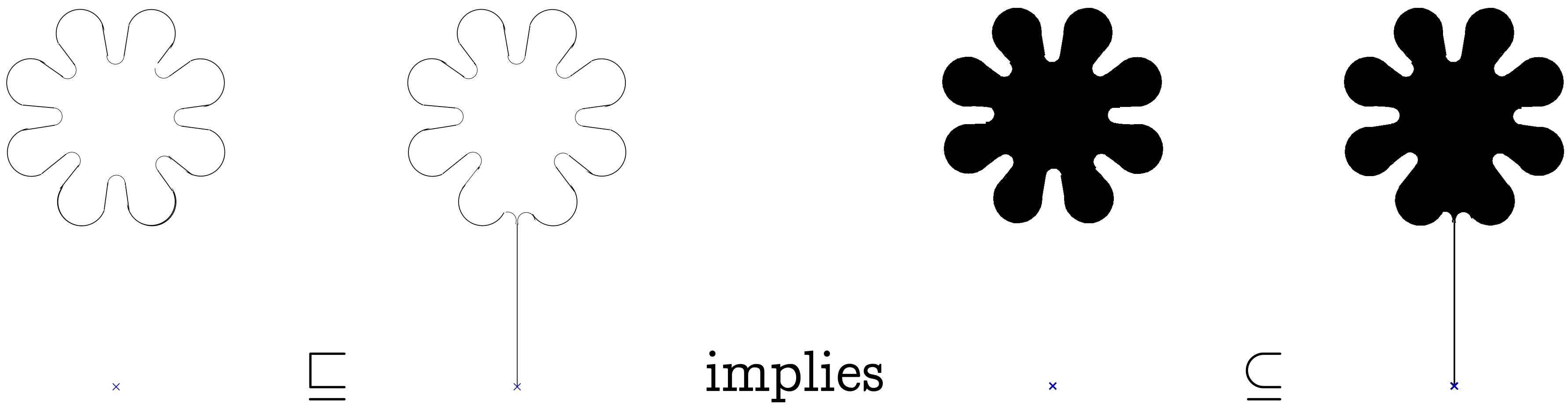
GALOIS CONNECTION 1/4:

- α is monotonic.



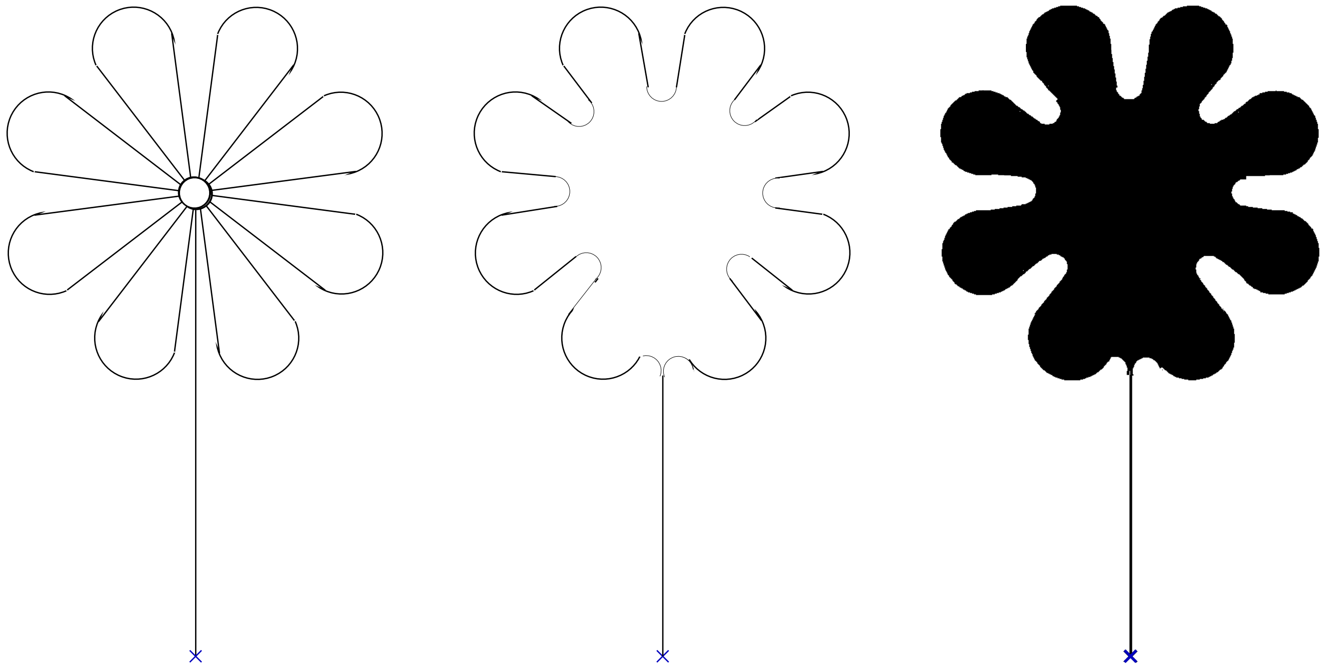
GALOIS CONNECTION 2/4:

- γ is monotonic.



Galois connection 3/4:

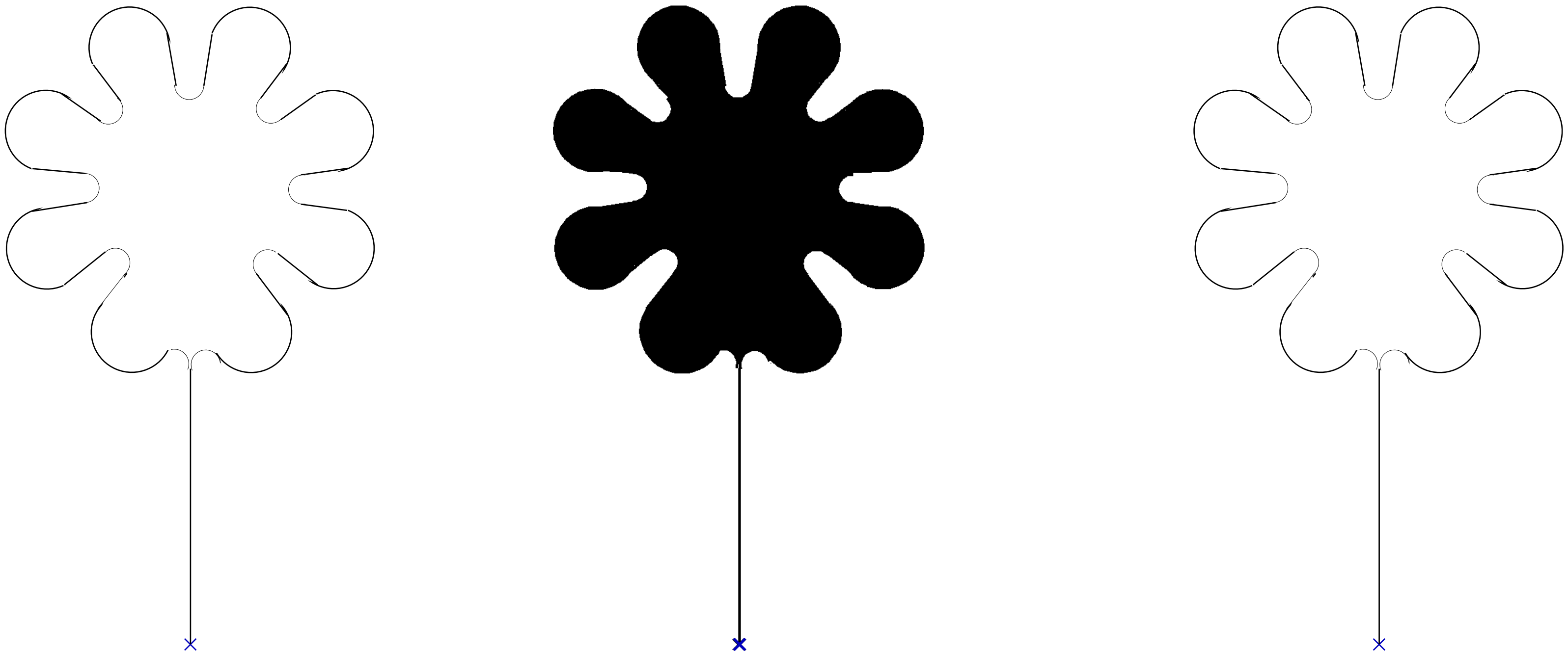
- for all concrete objects x, $\gamma \circ \alpha(x) \subseteq x$.



flower $\qquad$ α(flower) $\qquad$ $\gamma(\alpha$(flower))

Galois connection 4/4:

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



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

Galois connections

$$\langle \mathcal{D}, \subseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \overline{\mathcal{D}}, \sqsubseteq \rangle$$

iff $\quad \forall x, y \in \mathcal{D} : x \subseteq y \Longrightarrow \alpha(x) \sqsubseteq \alpha(y)$

$\wedge \; \forall \overline{x}, \overline{y} \in \overline{\mathcal{D}} : \overline{x} \sqsubseteq \overline{y} \Longrightarrow \gamma(\overline{x}) \subseteq \gamma(\overline{y})$

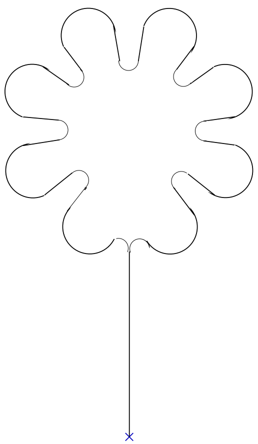
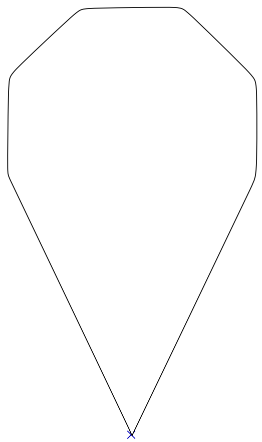
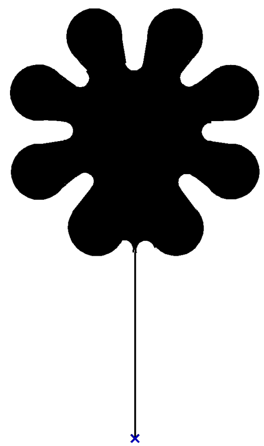
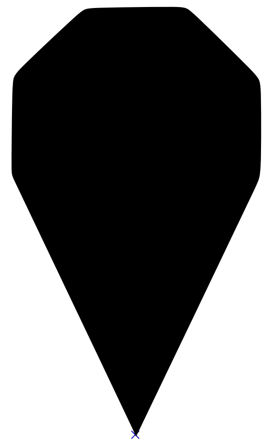
$\wedge \; \forall x \in \mathcal{D} : x \subseteq \gamma(\alpha(x))$

$\wedge \; \forall \overline{y} \in \overline{\mathcal{D}} : \alpha(\gamma(\overline{y})) \sqsubseteq \overline{x}$

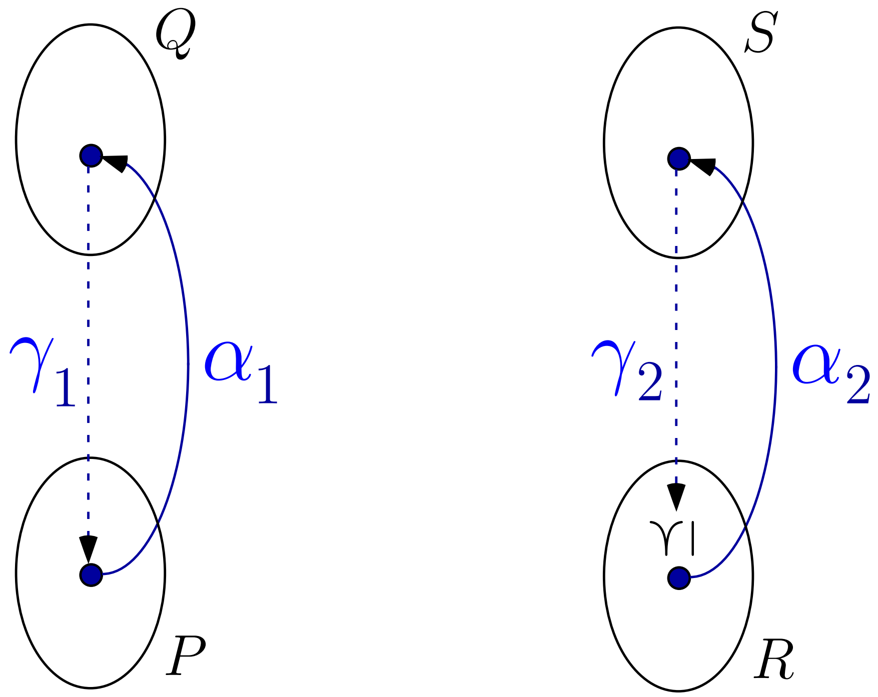
iff $\quad \forall x \in \mathcal{D}, \overline{y} \in \overline{\mathcal{D}} : \alpha(x) \sqsubseteq y \Longleftrightarrow x \subseteq \gamma(y)$

ABSTRACT ORDERING:

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

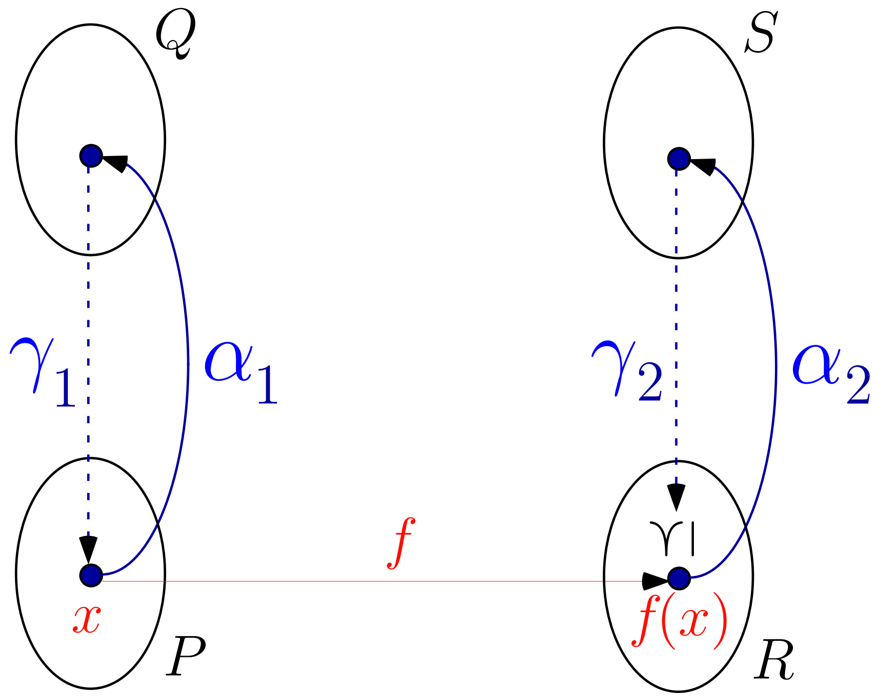
 $\sqsubseteq$  since  $\subseteq$ 

Function Abstraction (2)



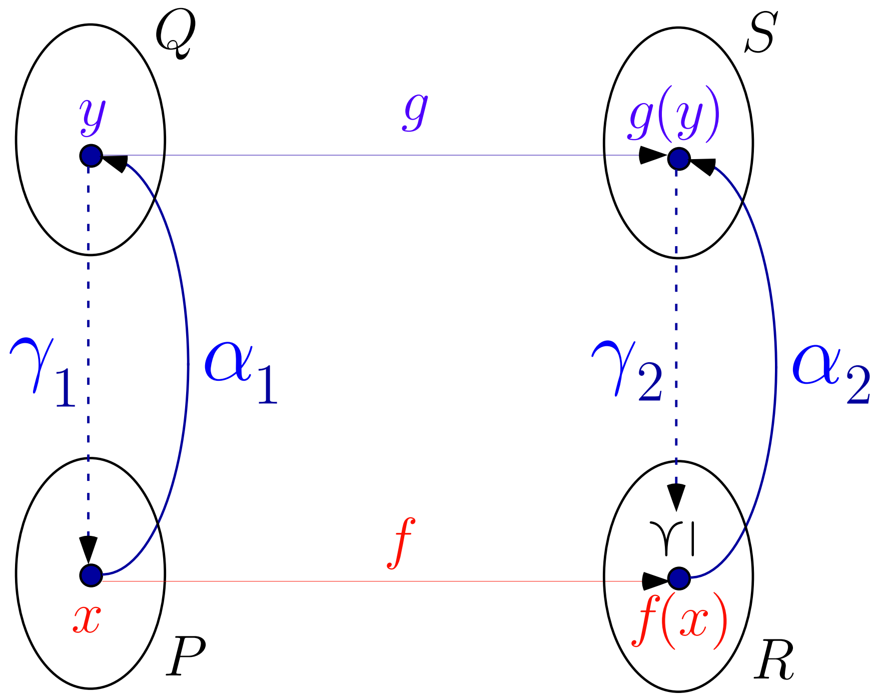
$$\langle P, \leq \rangle \xleftarrow[\alpha_1]{\gamma_1} \!\!\!\!\!\!\!\!\!\! \xrightarrow{} \langle Q, \subseteq \rangle \qquad \langle R, \preceq \rangle \xleftarrow[\alpha_2]{\gamma_2} \!\!\!\!\!\!\!\!\!\! \xrightarrow{} \langle S, \sqsubseteq \rangle$$

Function Abstraction (2)



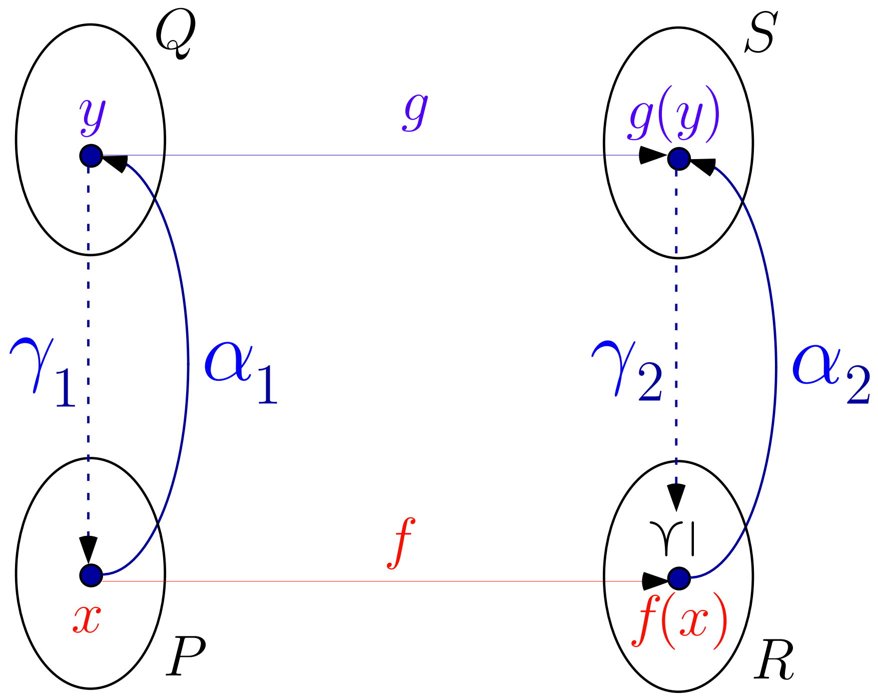
$$\langle P, \leq \rangle \xleftarrow[\alpha_1]{\gamma_1} \langle Q, \subseteq \rangle \qquad \langle R, \preceq \rangle \xleftarrow[\alpha_2]{\gamma_2} \langle S, \sqsubseteq \rangle$$

Function Abstraction (2)



$$\langle P, \leq \rangle \xrightleftharpoons[\alpha_1]{\gamma_1} \langle Q, \subseteq \rangle \qquad \langle R, \preceq \rangle \xrightleftharpoons[\alpha_2]{\gamma_2} \langle S, \sqsubseteq \rangle$$

Function Abstraction (2)



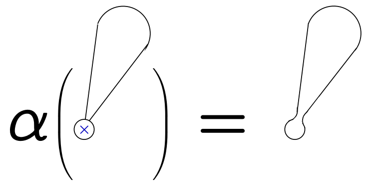
- If $\langle P, \leq\rangle \xrightleftharpoons[\alpha_1]{\gamma_1} \langle Q, \subseteq\rangle$ and $\langle R, \preceq\rangle \xrightleftharpoons[\alpha_2]{\gamma_2} \langle S, \sqsubseteq\rangle$ then

$$\langle P \overset{m}{\longmapsto} R, \dot{\subseteq}\rangle \xrightleftharpoons[\boldsymbol{\lambda} f \cdot \alpha_2 \circ f \circ \gamma_1]{\boldsymbol{\lambda} g \cdot \gamma_2 \circ g \circ \alpha_1} \langle Q \overset{m}{\longmapsto} S, \dot{\sqsubseteq}\rangle$$

Specification of abstract operations:

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

Abstract petal

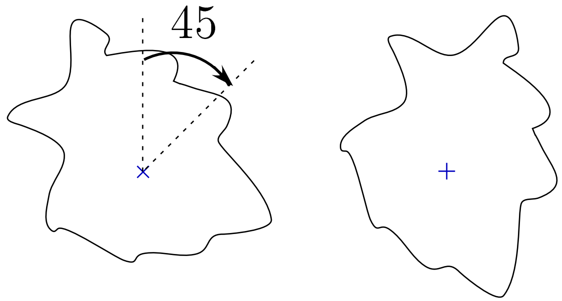


Abstract rotations:

- $\overline{\mathrm{r}}[a](y) = \alpha(\mathrm{r}[a](\gamma(y)))$

Abstract rotations:

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

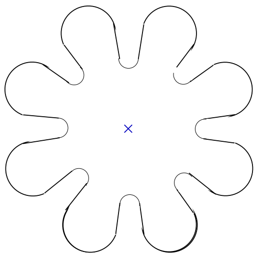


A <u>commutation theorem</u> on abstract rotations:

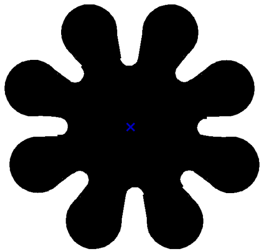
- $\alpha(\mathrm{r}[a](x))$
  $= \alpha(\gamma(\alpha(\mathrm{r}[a](x))))$
  $= \alpha(\gamma(\mathrm{r}[a](\alpha(x))))$
  $= \alpha(\mathrm{r}[a](\gamma(\alpha(x))))$
  $= \overline{\mathrm{r}}[a](\alpha(x))$

ABSTRACT STEMS:

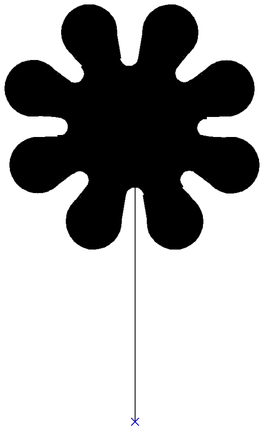
- $\overline{\text{stem}}(y) = \alpha(\text{stem}(\gamma(y)))$



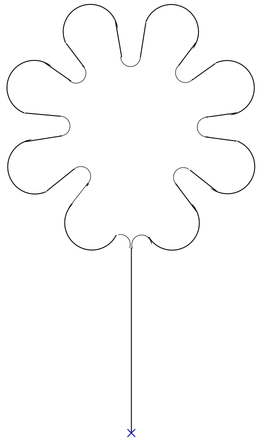
abstract corolla



γ(abstract corolla)



stem(γ(abstract corolla))



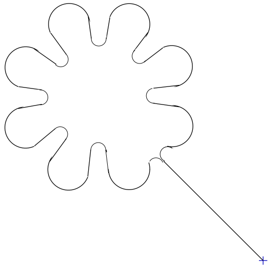
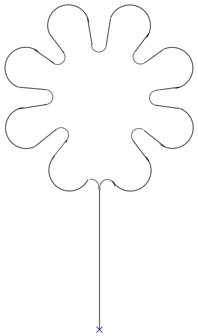
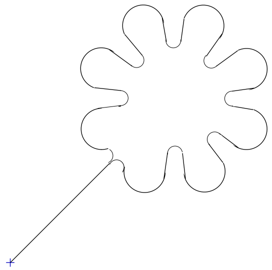
α(stem(γ(abstract corolla)))

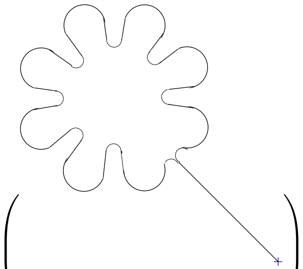
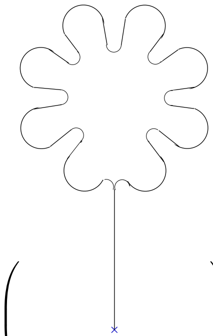
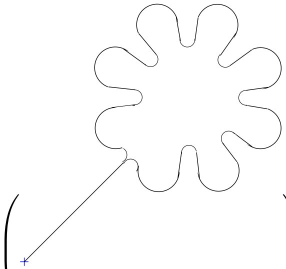
Abstract union:

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

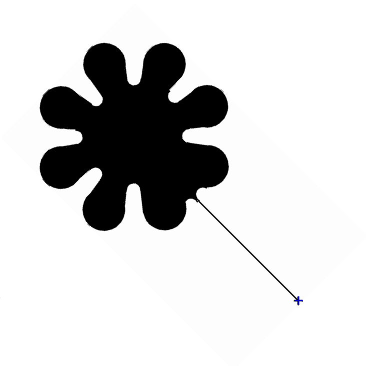
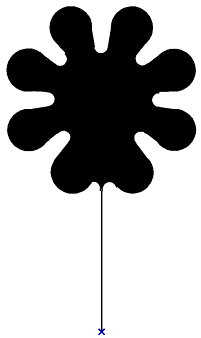
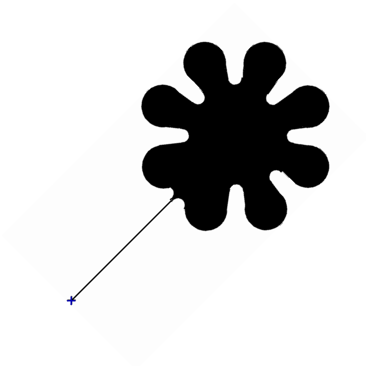
Abstract bouquet:

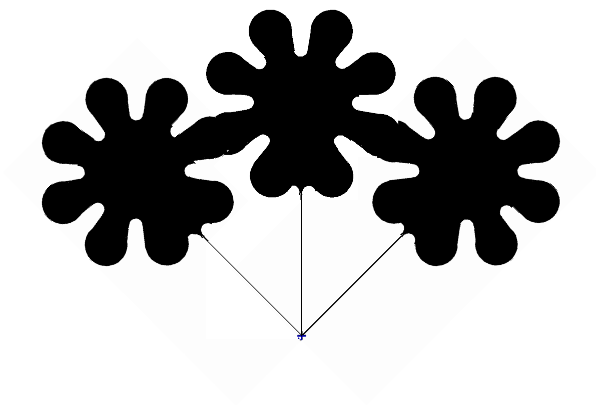
abstract bouquet

$=$  $\sqcup$  $\sqcup$ 

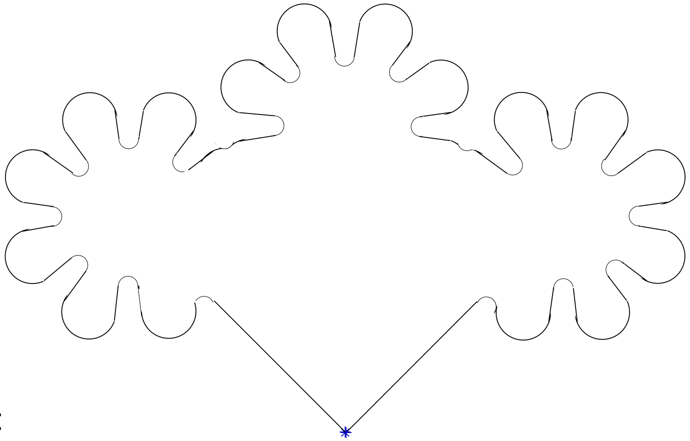
$= \alpha\Big(\gamma\Big($  $\Big) \cup \gamma\Big($  $\Big) \cup \gamma\Big($  $\Big)\Big)$

Abstract bouquet: (cont'd)

$= \alpha\Big($  $\cup$  $\cup$  $\Big)$

$= \alpha($  $)$

Abstract bouquet: (end)

$=$ 

A THEOREM ON THE ABSTRACT BOUQUET

abstract flower $= \alpha($concrete flower$)$

abstract bouquet

$= \bar{\text{r}}[\text{-}45](\text{abstract flower}) \sqcup \text{abstract flower} \sqcup \bar{\text{r}}[+45](\text{abstract flower})$

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

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

$= \alpha(\text{r}[\text{-}45](\text{concrete flower}) \cup \text{concrete flower} \cup \text{r}[+45](\text{concrete flower}))$

$= \alpha(\text{concrete bouquet})$

Fixpoint Approximation

Let $F \in L \stackrel{m}{\longmapsto} L$ and $\overline{F} \in \overline{L} \stackrel{m}{\longmapsto} \overline{L}$ be respective monotone maps on the cpos $\langle L, \bot, \sqsubseteq\rangle$ and $\langle \overline{L}, \overline{\bot}, \overline{\sqsubseteq}\rangle$ and $\langle L, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{L}, \overline{\sqsubseteq}\rangle$ such that $\alpha \circ F \circ \gamma \;\dot{\overline{\sqsubseteq}}\; \overline{F}$. Then [14]:

- $\forall \delta \in \mathbb{O}\colon\ \alpha(F^\delta) \mathrel{\overline{\sqsubseteq}} \overline{F}^\delta$ (iterates from the infimum);
- The iteration order of $\overline{F}$ is $\leq$ to that of F;
- $\alpha(\mathrm{lfp}^{\sqsubseteq} F) \mathrel{\overline{\sqsubseteq}} \mathrm{lfp}^{\overline{\sqsubseteq}} \overline{F}$;

[14] P. Cousot & R. Cousot. *Systematic design of program analysis frameworks.* ACM POPL'79, pp. 269–282, 1979. Numerous variants!

Fixpoint Approximation

Let $F \in L \stackrel{m}{\longmapsto} L$ and $\overline{F} \in \overline{L} \stackrel{m}{\longmapsto} \overline{L}$ be respective monotone maps on the cpos $\langle L, \bot, \sqsubseteq\rangle$ and $\langle \overline{L}, \overline{\bot}, \overline{\sqsubseteq}\rangle$ and $\langle L, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{L}, \overline{\sqsubseteq}\rangle$ such that $\alpha \circ F \circ \gamma \mathrel{\dot{\overline{\sqsubseteq}}} \overline{F}$. Then [14]:

- $\forall \delta \in \mathbb{O}\colon\ \alpha(F^{\delta}) \mathrel{\overline{\sqsubseteq}} \overline{F}^{\delta}$ (iterates from the infimum);
- The iteration order of $\overline{F}$ is $\leq$ to that of F;
- $\alpha(\mathrm{lfp}^{\sqsubseteq} F) \mathrel{\overline{\sqsubseteq}} \mathrm{lfp}^{\overline{\sqsubseteq}} \overline{F}$;

Soundness: $\mathrm{lfp}^{\overline{\sqsubseteq}} \overline{F} \mathrel{\overline{\sqsubseteq}} \overline{P} \Rightarrow \mathrm{lfp}^{\sqsubseteq} F \sqsubseteq \gamma(\overline{P})$.

14 P. Cousot & R. Cousot. *Systematic design of program analysis frameworks*. ACM POPL'79, pp. 269–282, 1979. Numerous variants!

Fixpoint Abstraction

Moreover, the *commutation condition* $\overline{F} \circ \alpha = \alpha \circ F$ implies[15]:

- $\overline{F} = \alpha \circ F \circ \gamma$, and
- $\alpha(\mathrm{lfp}^{\sqsubseteq} F) = \mathrm{lfp}^{\overline{\sqsubseteq}} \overline{F}$;

[15] P. Cousot & R. Cousot. *Systematic design of program analysis frameworks*. ACM POPL'79, pp. 269–282, 1979. Numerous variants!

Fixpoint Abstraction

Moreover, the *commutation condition* $\overline{F} \circ \alpha = \alpha \circ F$ implies[15]:

- $\overline{F} = \alpha \circ F \circ \gamma$, and
- $\alpha(\mathrm{lfp}^{\sqsubseteq} F) = \mathrm{lfp}^{\overline{\sqsubseteq}} \overline{F}$;

Completeness: $\mathrm{lfp}^{\sqsubseteq} F \sqsubseteq \gamma(\overline{P}) \Rightarrow \mathrm{lfp}^{\overline{\sqsubseteq}} \overline{F} \mathrel{\overline{\sqsubseteq}} \overline{P}$.

15 P. Cousot & R. Cousot. *Systematic design of program analysis frameworks*. ACM POPL'79, pp. 269–282, 1979. Numerous variants!

Abstract fixpoint

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

Abstract transformer $\overline{F}$

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

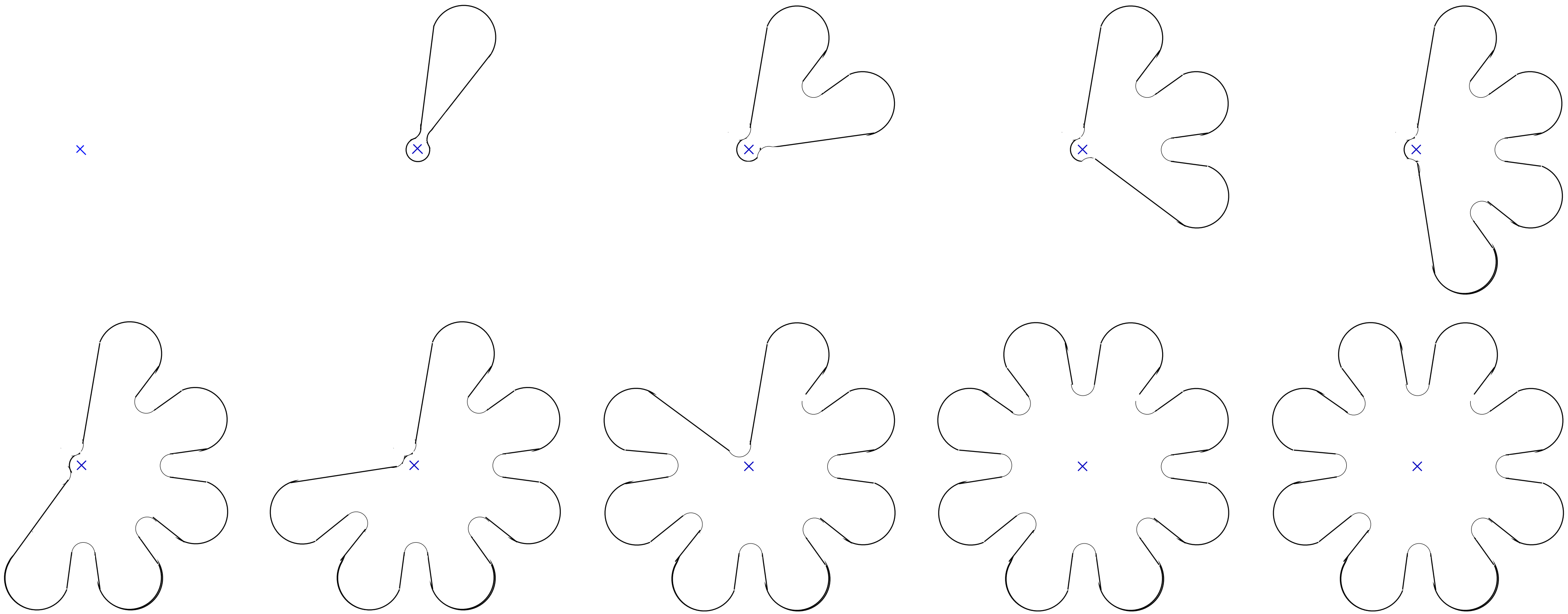
by defining

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

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

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

On abstracting properties of graphic objects

- 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?

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

$$\langle \wp(\wp(\mathcal{P})), \subseteq \rangle \xrightleftharpoons[\alpha_0]{\gamma_0} \langle \wp(\mathcal{P}), \subseteq \rangle$$

where:

$\mathcal{P}$ is a set of pixels (e.g. pairs of coordinates)

$\alpha_0(X) = \cup X$

$\gamma_0(Y) = \{G \in \mathcal{P} \mid G \subseteq Y\}$

$\wp(\mathcal{P})$

Composing Galois Connections

- If $\langle P, \leq \rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q, \sqsubseteq \rangle$ and $\langle Q, \sqsubseteq \rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle R, \preceq \rangle$ then

$$\langle P, \leq \rangle \underset{\alpha_2 \circ \alpha_1}{\overset{\gamma_1 \circ \gamma_2}{\leftrightarrows}} \langle R, \preceq \rangle$$ [13]

13 This would not be true with the original definition of Galois correspondences.

Is it for fun (only)?

- 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.