Weryfikacja wspomagana komputerowo

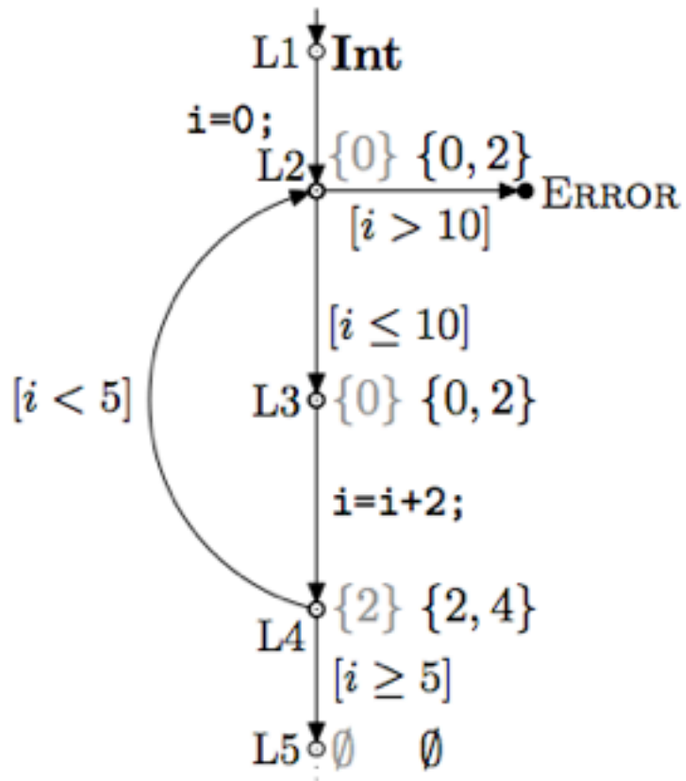
wykład 12

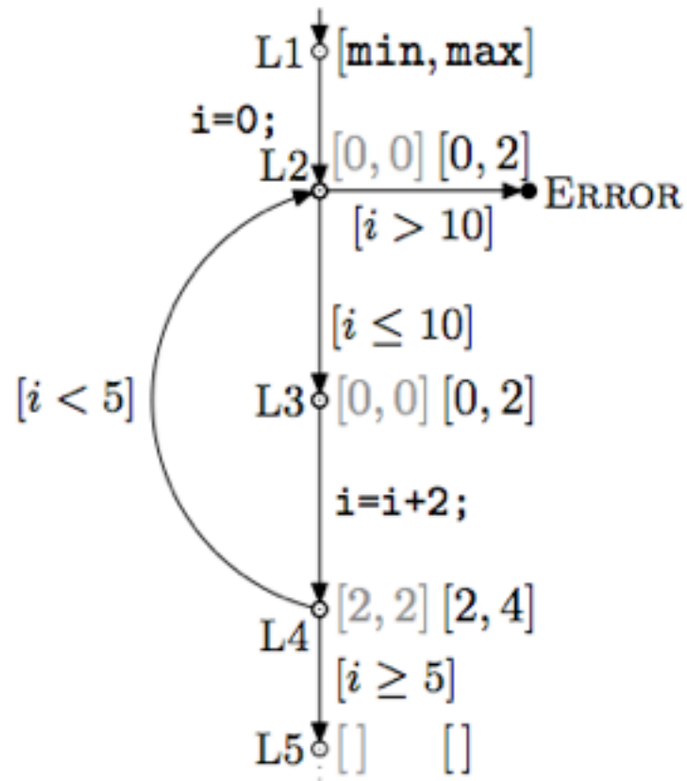
Interpretacja abstrakcyjna II

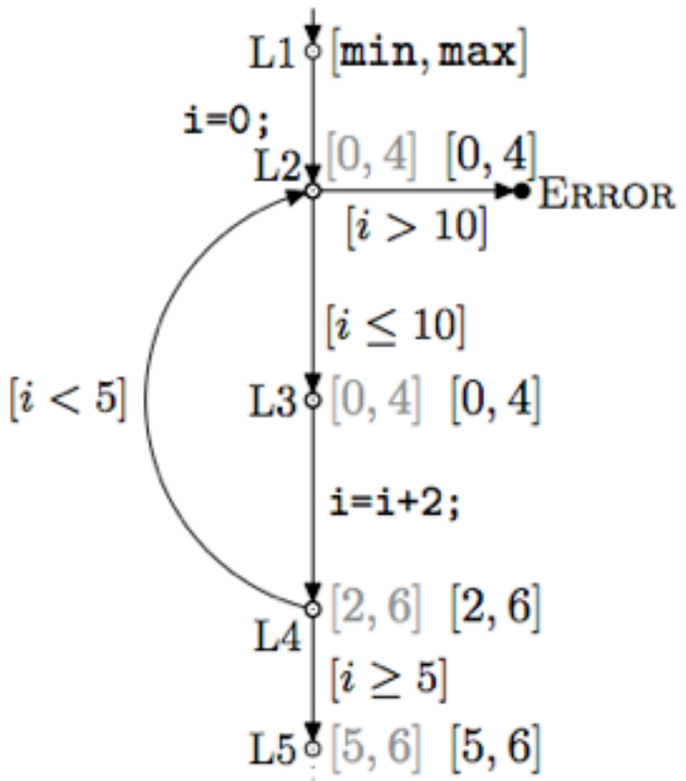
Źródła

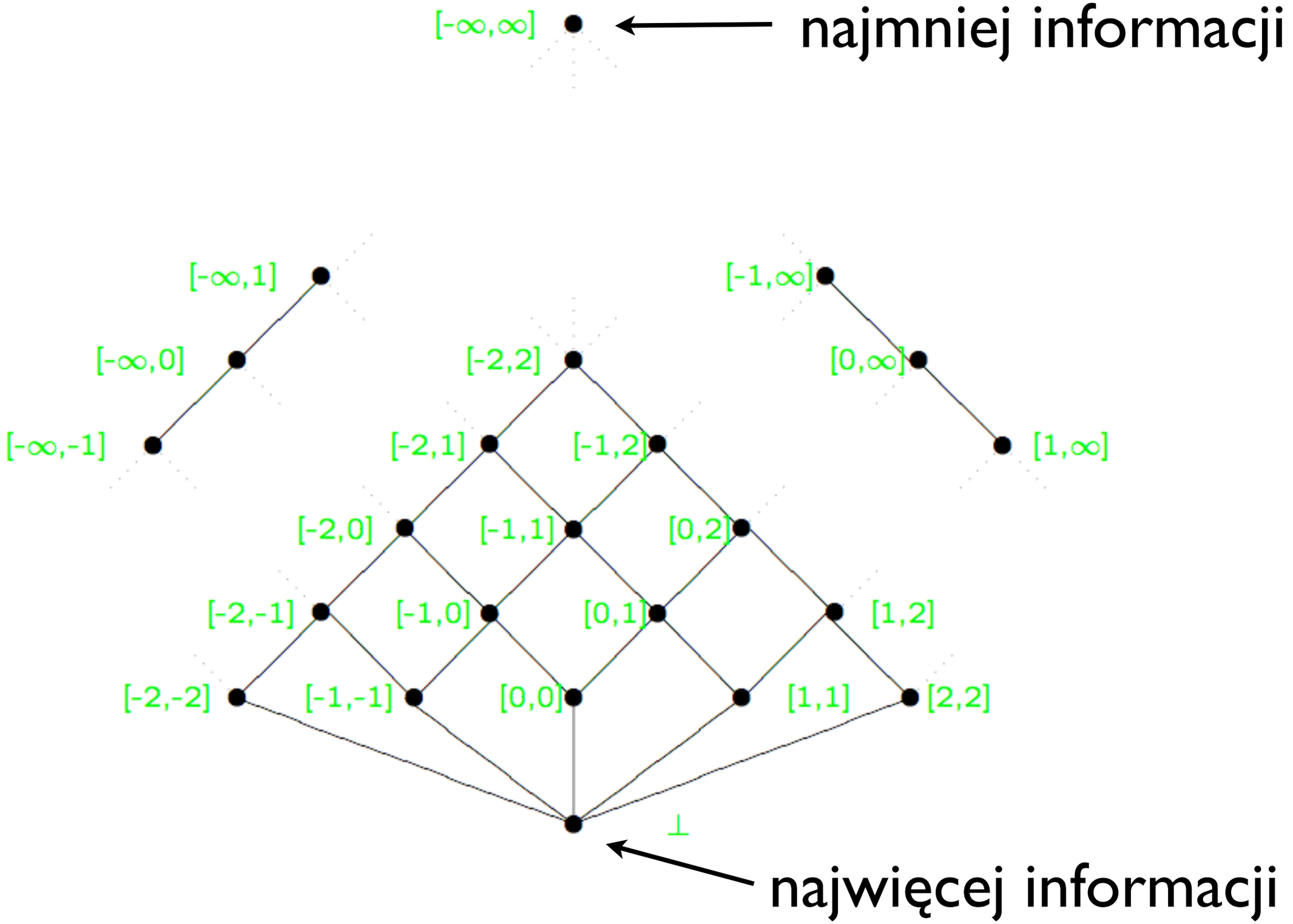
- F. Nielson, H.R. Nielson, C. Hankin, Principles of Program Analysis, Springer, 2005.
- http://www.imm.dtu.dk/~riis/PPA/slides4.pdf
- N. D. Jones, F. Nielson, Interpretation: a Semantics-Based Tool for Program Analysis. Handbook of Logic in Computer Science, tom 4, str. 527-636, 1995.
- V. D'Silva, D. Kroening, G. Weissenbacher, A Survey of Automated Techniques for Formal Software Verification. IEEE Trans. on CAD of Integrated Circuits and Systems 27 (7):1165-1178, 2008.

```
int i = 0;
do {
   assert(i <= 10);
   i = i+2;
} while (i < 5);
```





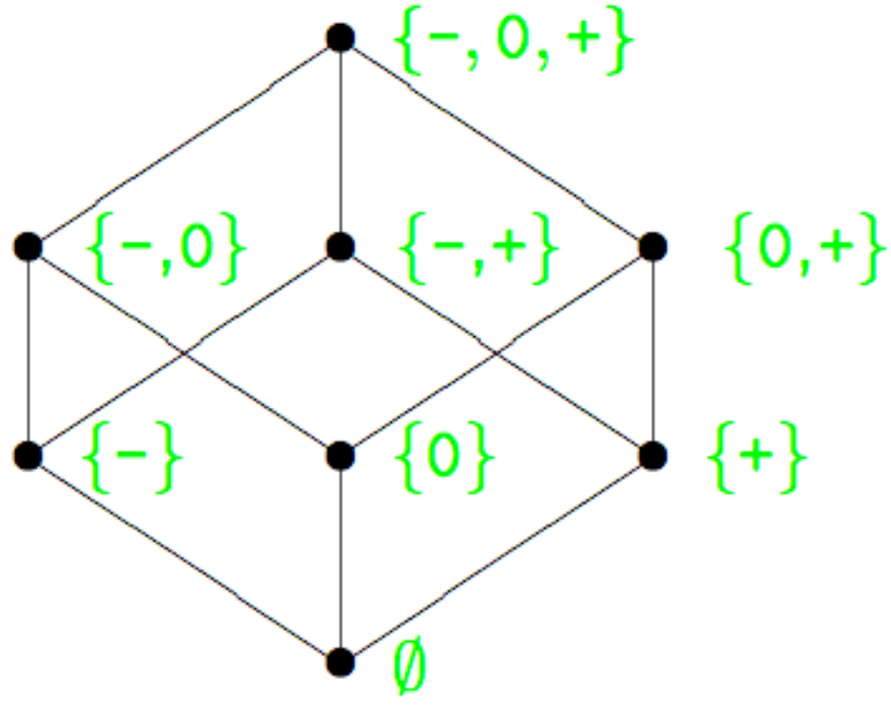



[-∞,∞]
najmniej informacji
[-∞,1]
[-∞,0]
[-∞,-1]
[-2,2]
[-2,1]
[-1,2]
[-2,0]
[-1,1]
[0,2]
[-2,-1]
[-1,0]
[0,1]
[1,2]
[-2,-2]
[-1,-1]
[0,0]
[1,1]
[2,2]
[-1,∞]
[0,∞]
[1,∞]
⊥
najwięcej informacji

Dziedziny abstrakcyjne

Dziedziny nie-relacyjne

- znaki $\mathcal{P}(-, 0, +)$
- przedzialy $[n, m]$
- parzystość
- kongruencja modulo *k*



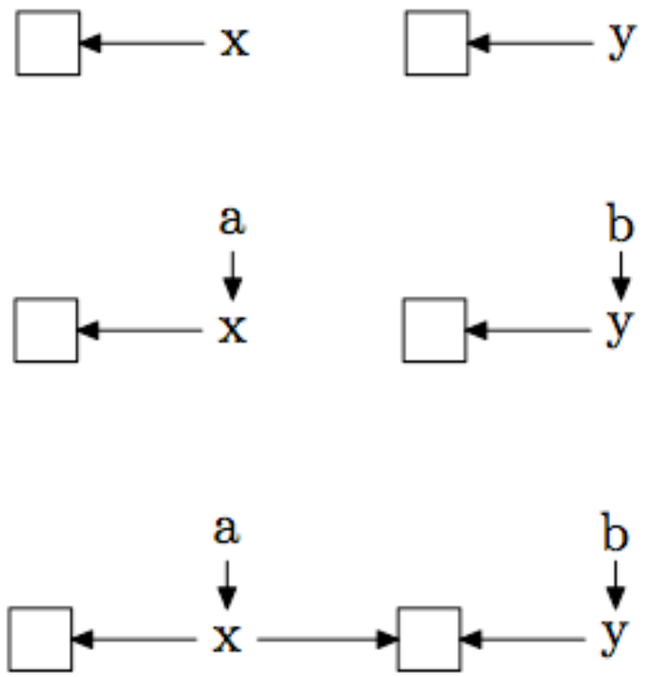
Dziedziny relacyjne

precyzja ↓

- DBM (macierze ograniczeń różnic) $x - y \leq c$
- ośmiokąty $\overset{+}{-} x \overset{+}{-} y \leq c$
- ośmiościany $\overset{+}{-} x_1 \ldots \overset{+}{-} x_n \leq c$
- wielościany $a_1 x_1 + \ \ldots \ + a_n x_n \leq c$
- ...
- grafy

Analiza kształtu

```
int **a, **b, *x, *y;
x = (int*) malloc(sizeof(int));
y = (int*) malloc(sizeof(int));
a = &x;
b = &y;
*a = y;
```



a i b nie wskazują tej samej lokacji

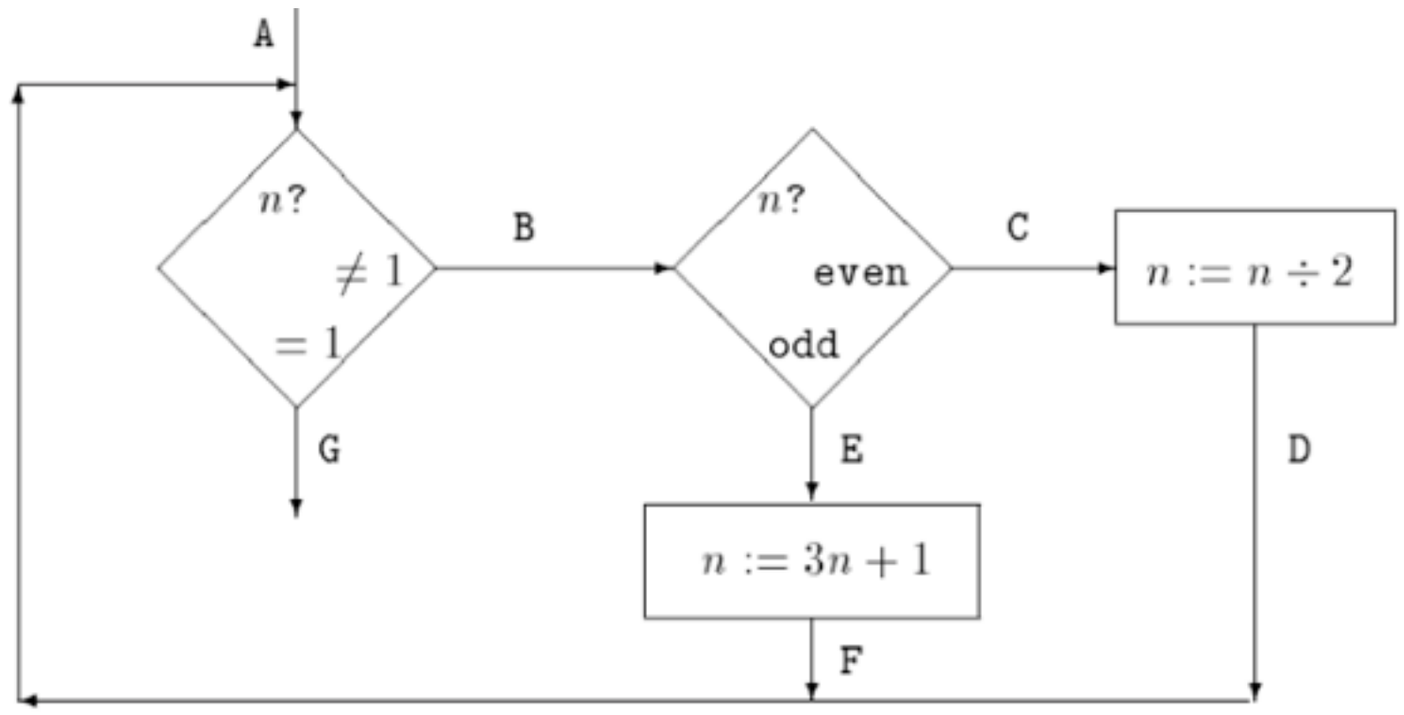
x i y mogą wskazywać tę samą lokację

Składanie analiz

- złożenie
- produkt
- tensor
- przestrzenie funkcyjne

Semantyka abstrakcyjna

A: **while** $n \neq 1$ **do**
  B: **if** n even
    then (C: $n := n \div 2$; D:)
    else (E: $n := 3 * n + 1$; F:)
  fi
od
G:

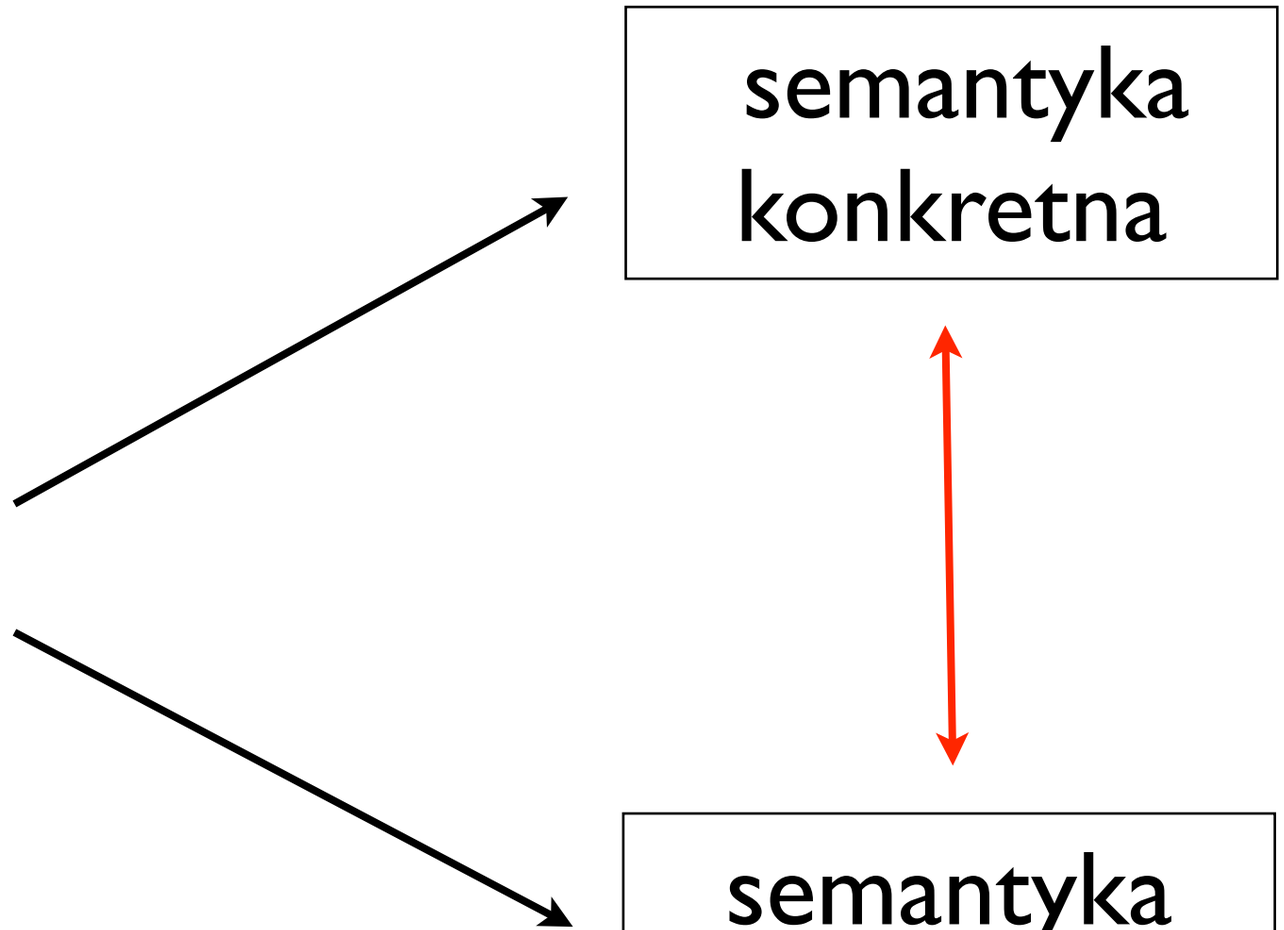


$S = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}, \mathrm{G}\}$

$$\mathrm{State} = S \times \mathrm{Store}$$

$$\mathrm{Store} = \mathrm{Var} \to \mathrm{Val}$$

A: **while** $n \neq 1$ **do**
  B: **if** n even
    then (C: $n := n \div 2$; D:)
    else (E: $n := 3 * n + 1$; F:)
  fi
od
G:



jak skonstruować semantykę abstrakcyjną?

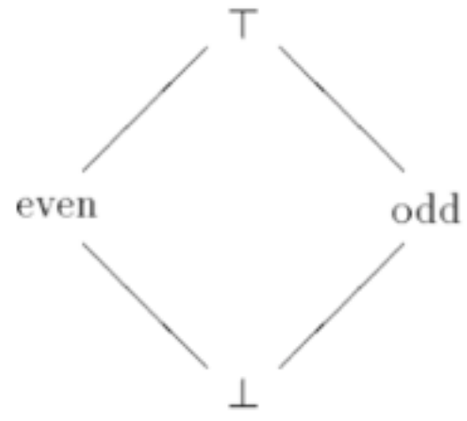
Dziedziny

semantyka konkretna

$$V = \text{Store} = \text{Var} \to \mathbb{Z}$$

semantyka abstrakcyjna

$$L = \text{Var} \to \{\bot, \text{even}, \text{odd}, \top\}$$



Semantyka abstrakcyjna

$n := n \div 2;$

$$\bot \mapsto \bot$$

$$\text{odd}, \text{even}, \top \mapsto \top$$

$n := 3 * n + 1;$

$$\bot \mapsto \bot$$

$$\text{odd} \mapsto \text{even}$$

$$\text{even} \mapsto \text{odd}$$

$$\top \mapsto \top$$

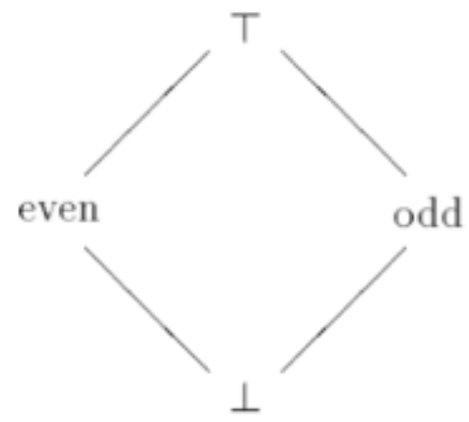
semantyka konkretna

$$V = \text{Store} = \text{Var} \to \mathbb{Z}$$

chcemy uzyskać zgodność semantyk

semantyka abstrakcyjna

$$L = \text{Var} \to \{\bot, \text{even}, \text{odd}, \top\}$$



Funkcja reprezentacji

semantyka konkretna

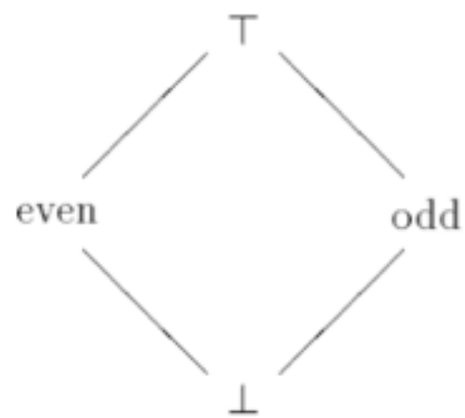
$$V = \text{Store} = \text{Var} \to \mathbb{Z}$$

$\beta : V \to L$

monotoniczna

semantyka abstrakcyjna

$$L = \text{Var} \to \{\bot, \text{even}, \text{odd}, \top\}$$



Funkcja reprezentacji

semantyka konkretna

najlepsze przybliżenie

$$V = \text{Store} = \text{Var} \to \mathbb{Z}$$

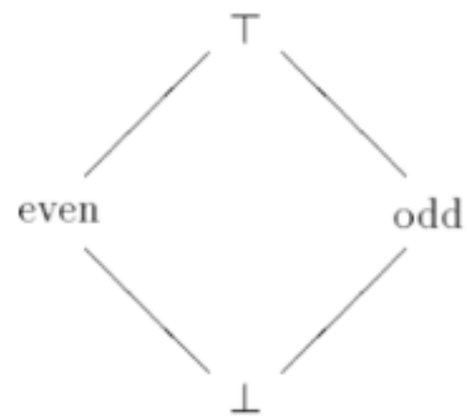
$\beta : V \to L$

monotoniczna

$$\beta(z) = \begin{cases} \text{even} & \text{jeśli } z \text{ parzyste} \\ \text{odd} & \text{jeśli } z \text{ nieparzyste} \end{cases}$$

semantyka abstrakcyjna

$$L = \text{Var} \to \{\bot, \text{even}, \text{odd}, \top\}$$



Funkcja reprezentacji

semantyka konkretna

$$V = \text{Store} = \text{Var} \to \mathbb{Z}$$

$\beta : V \to L$

monotoniczna

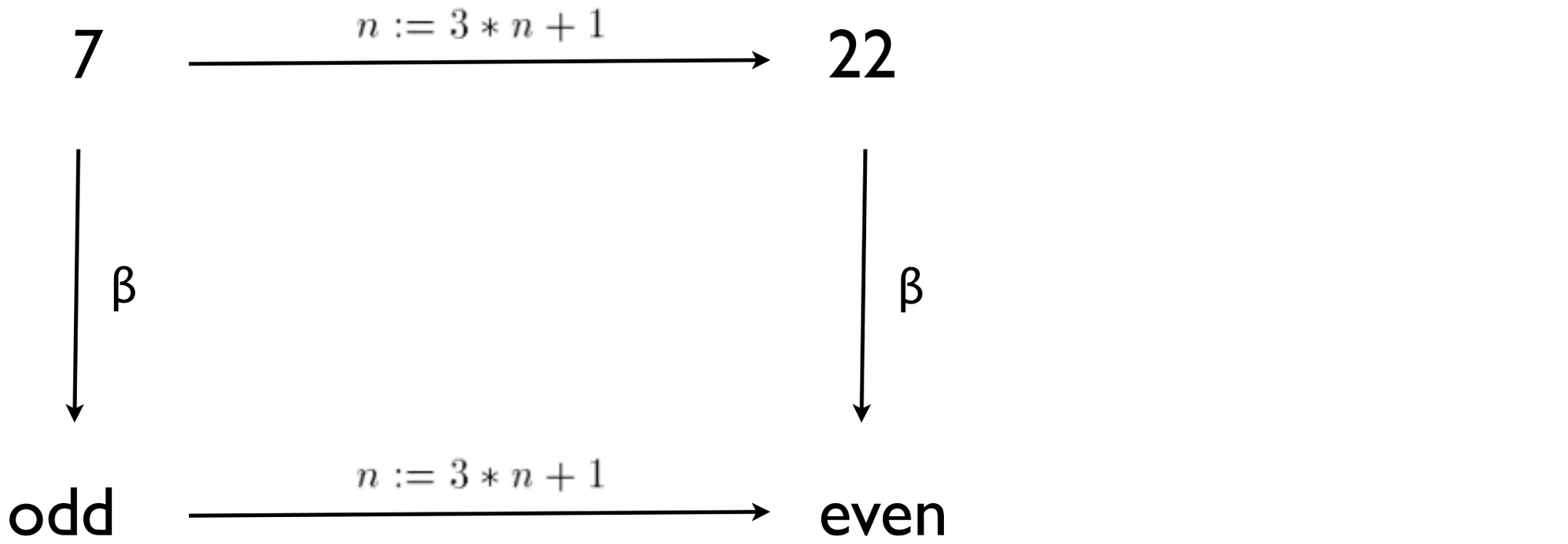
$$\beta(z) = \begin{cases} \{\text{even}\} & \text{jeśli } z \text{ parzyste} \\ \{\text{odd}\} & \text{jeśli } z \text{ nieparzyste} \end{cases}$$

semantyka abstrakcyjna

$$L = \text{Var} \to \{\bot, \text{even}, \text{odd}, \top\}$$

$$|||$$

$$\mathcal{P}(\text{even}, \text{odd})$$



β nie zawsze jest homomorfizmem!

β nie zawsze jest homomorfizmem!

$$[n \mapsto 1, m \mapsto -2] \xrightarrow{m := n + m} [n \mapsto 1, m \mapsto -1]$$

$$\downarrow \beta \qquad\qquad \downarrow \beta$$

$$[n \mapsto +, m \mapsto -] \xrightarrow{m := n + m} [n \mapsto +, m \mapsto \top]$$

Funkcja abstrakcji

semantyka konkretna

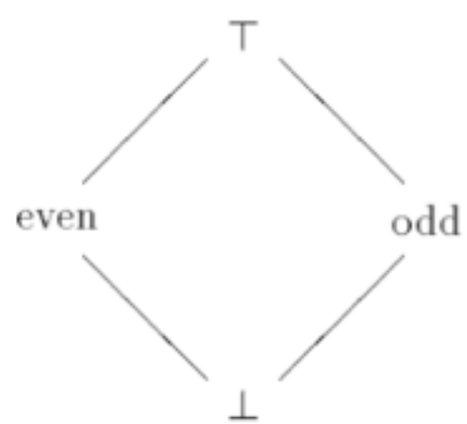
$\mathcal{P}(V)$

abstrakcja

$\alpha : \mathcal{P}(V) \to L$

semantyka abstrakcyjna

$L = \mathrm{Var} \to \{\bot, \mathrm{even}, \mathrm{odd}, \top\}$



A: **while** $n \neq 1$ **do**
  B: **if** n even
    then (C: $n := n \div 2$; D:)
    else (E: $n := 3 * n + 1$; F:)
  fi
od
G:

standardowa semantyka

semantyka abstrakcyjna

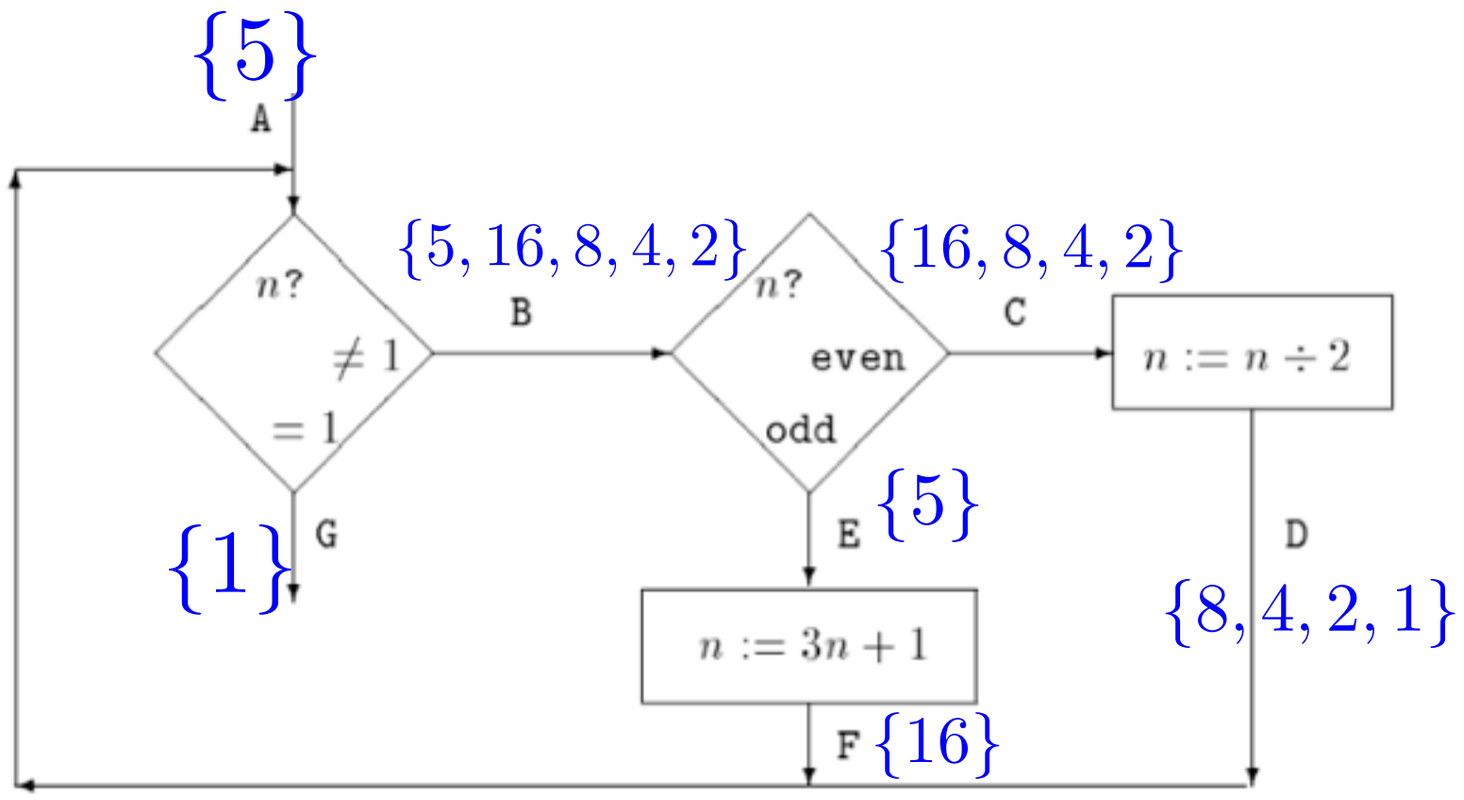
semantyka
akumulacyjna

standardowa
semantyka

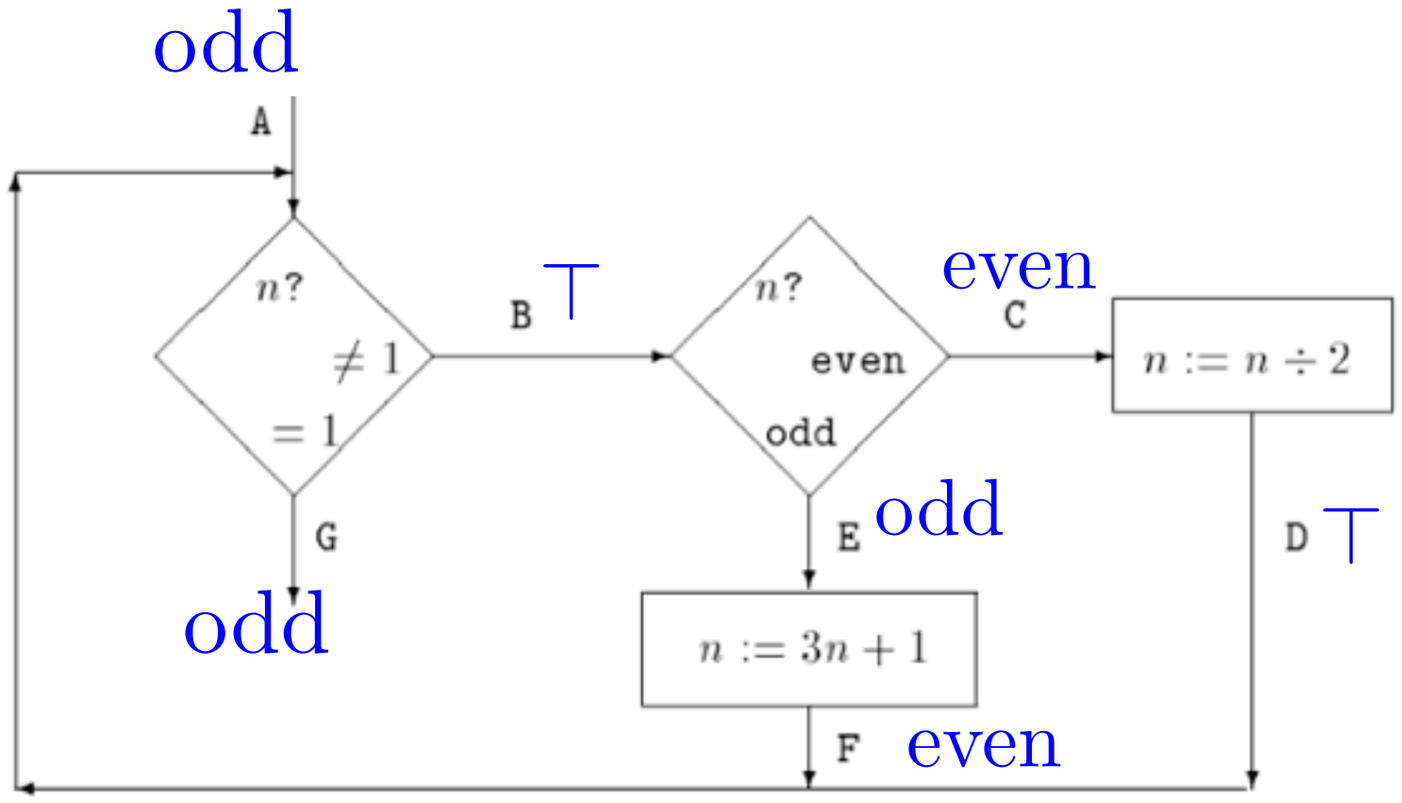
A: **while** $n \neq 1$ **do**
  B: **if** n even
    then (C: $n := n \div 2$; D:)
    else (E: $n := 3 * n + 1$; F:)
  fi
od
G:

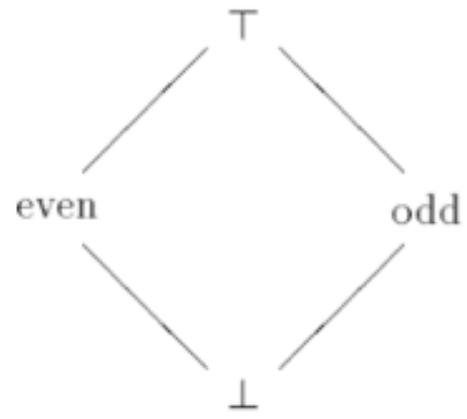
semantyka
abstrakcyjna

A: **while** $n \neq 1$ **do**
    B: **if** n even
        then (C: $n := n \div 2$; D:)
        else (E: $n := 3 * n + 1$; F:)
    fi
od
G:



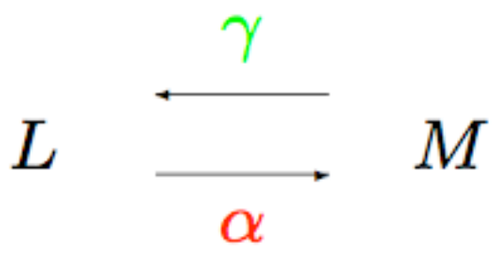
A: **while** $n \neq 1$ **do**
  B: **if** n even
    then (C: $n := n \div 2$; D:)
    else (E: $n := 3 * n + 1$; F:)
  fi
od
G:





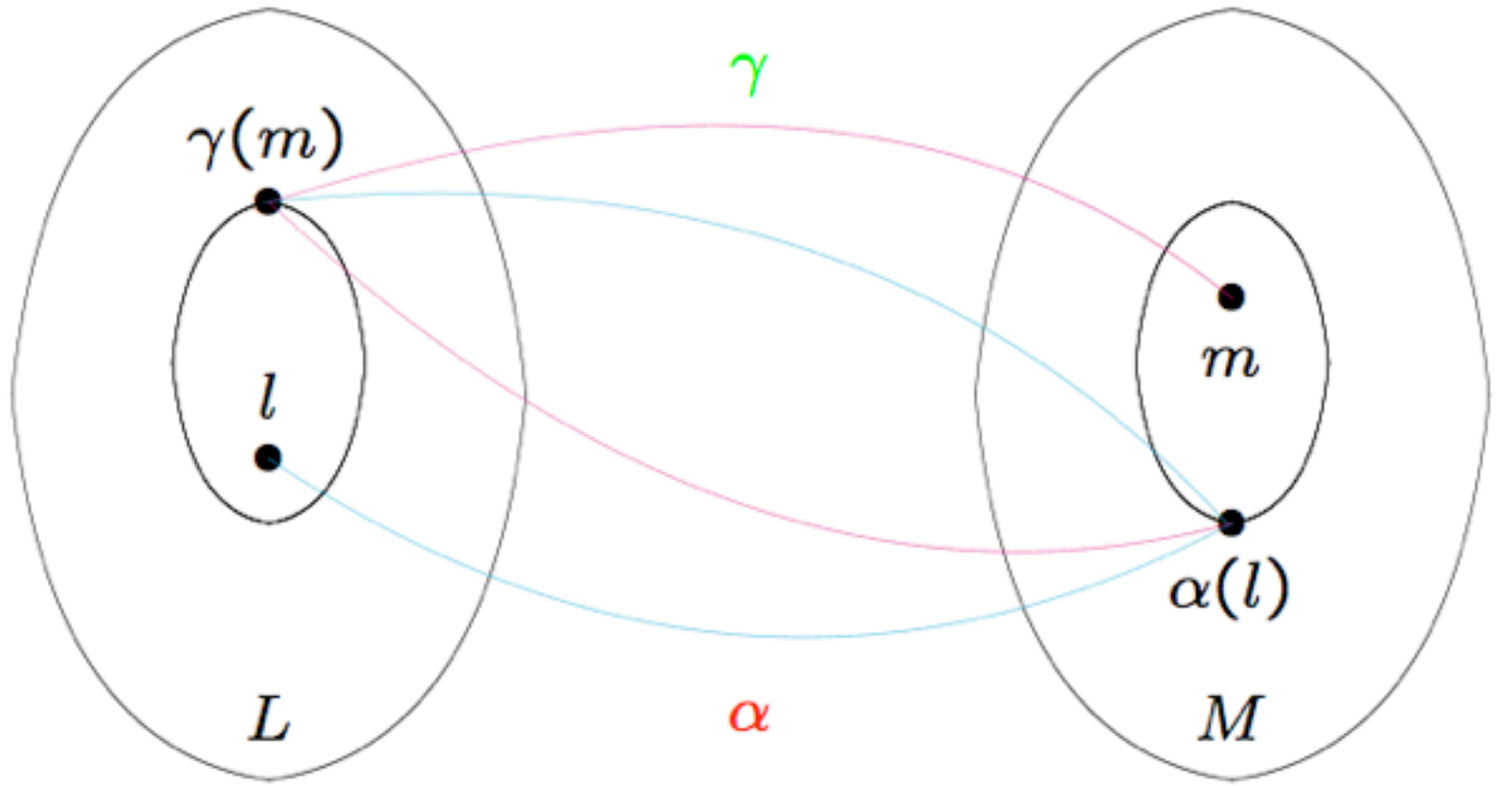
Sprzężenie Galois

Sprzężenie Galois



α - funkcja abstrakcji

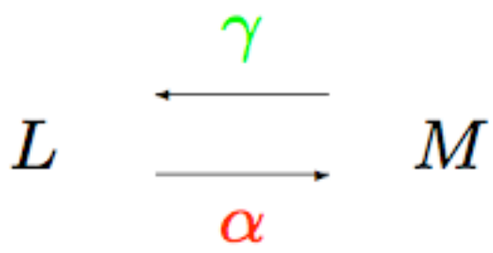
γ - funkcja konkretyzacji



$$l \sqsubseteq \gamma(\alpha(l))$$

$$\alpha(\gamma(m)) \sqsubseteq m$$

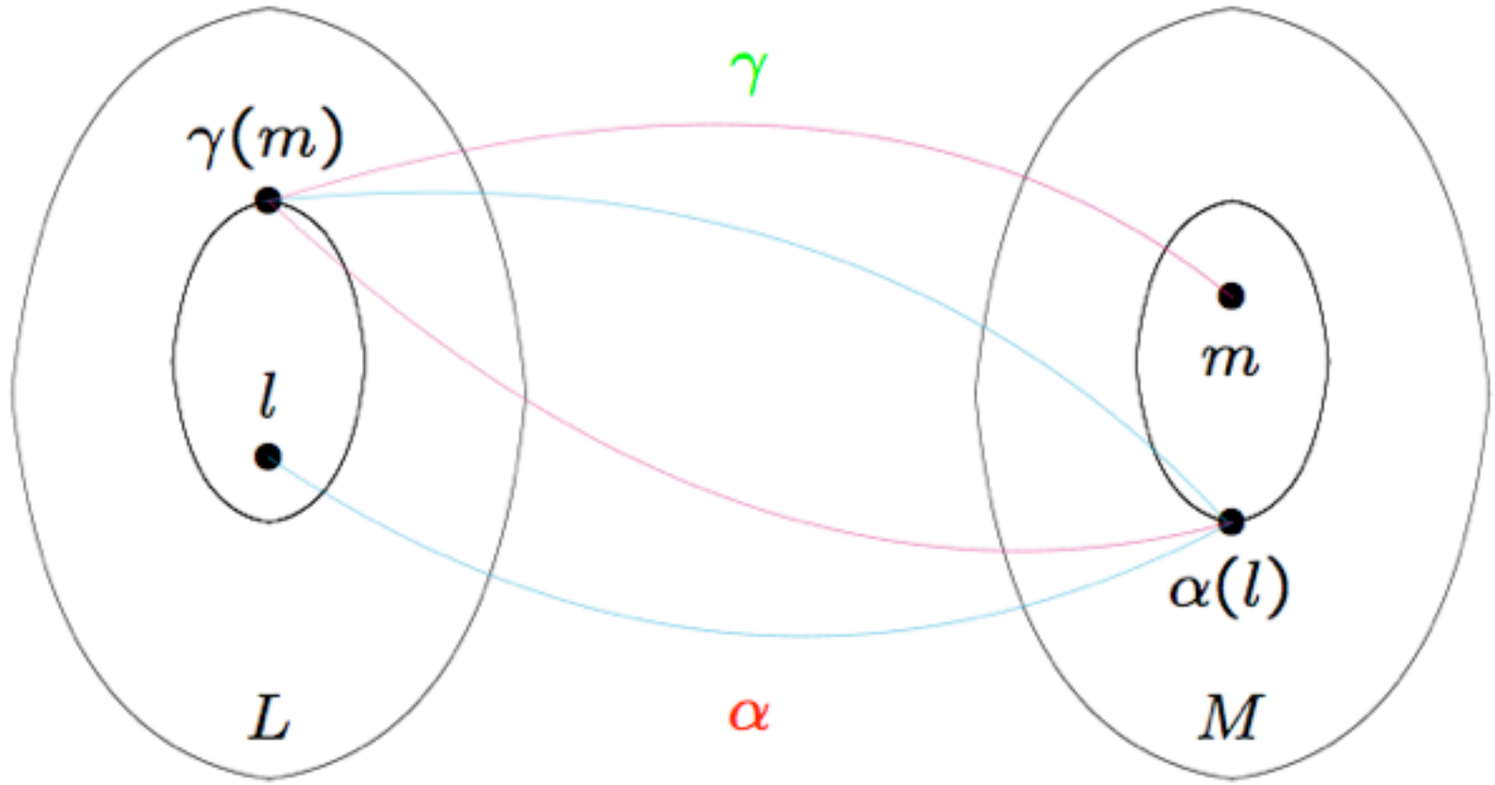
Sprzężenie Galois



α - funkcja abstrakcji

γ - funkcja konkretyzacji

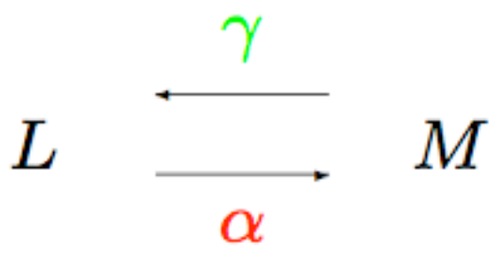
monotoniczne



$$l \sqsubseteq \gamma(\alpha(l))$$

$$\alpha(\gamma(m)) \sqsubseteq m$$

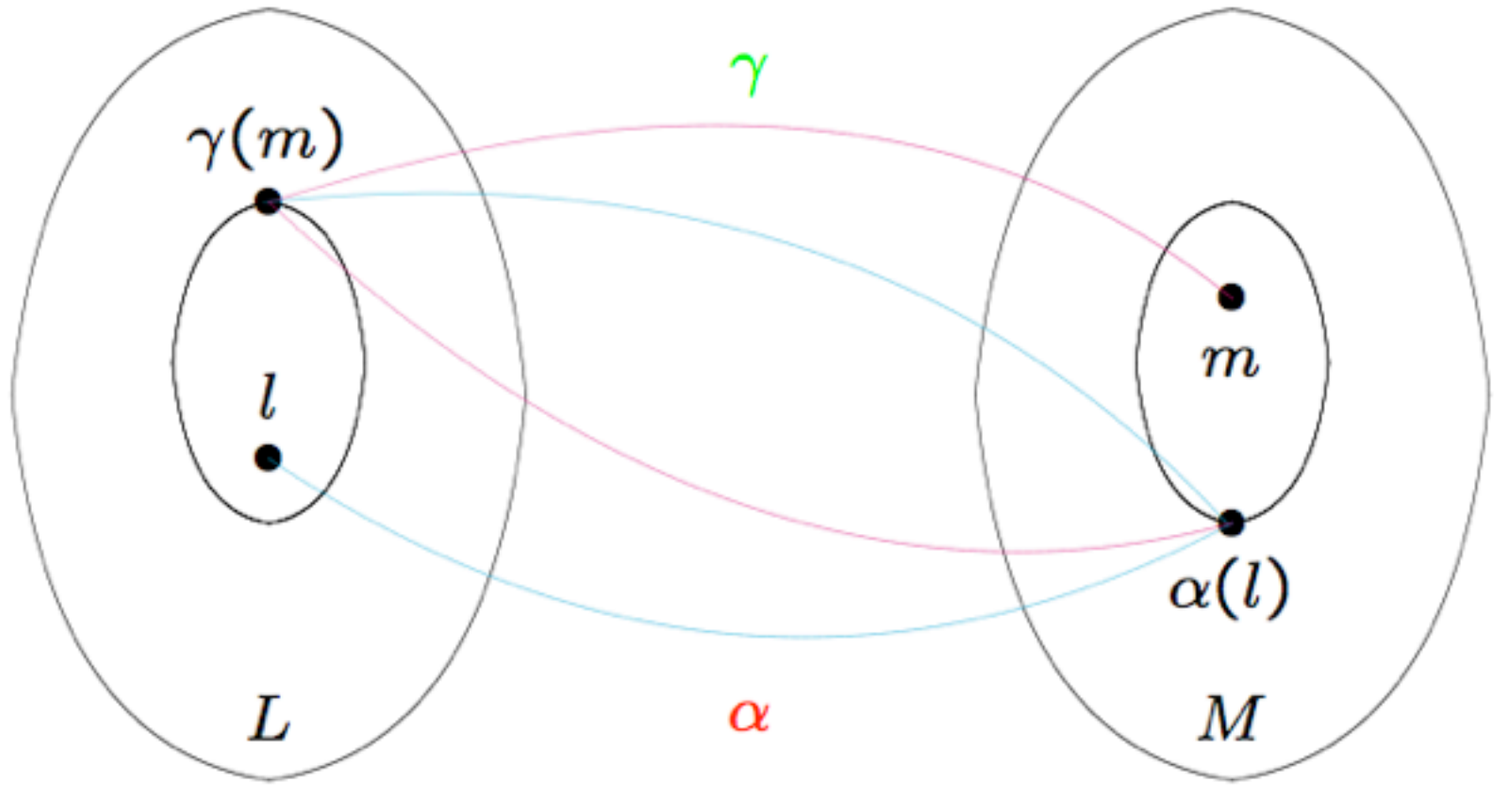
Sprzężenie Galois



α - funkcja abstrakcji

γ - funkcja konkretyzacji

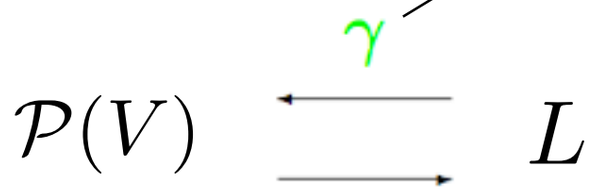
monotoniczne



$$l \sqsubseteq \gamma(m) \iff \alpha(l) \sqsubseteq m$$

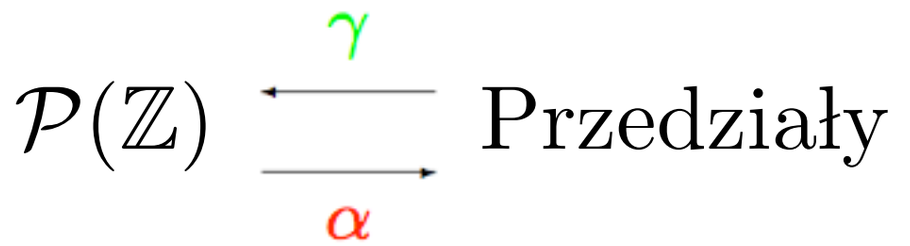
Dziedzina abstrakcyjna i konkretna

zbiór wartości reprezentowanych



najdokładniejsza abstrakcja

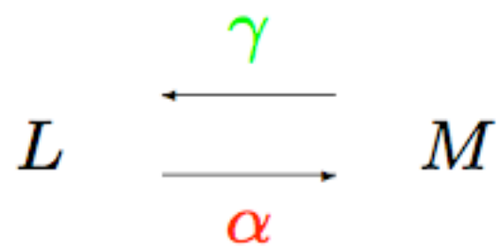
Przykład



$\alpha(X) =$ najmniejszy przedział zawierający X

$$\gamma(I) = I$$

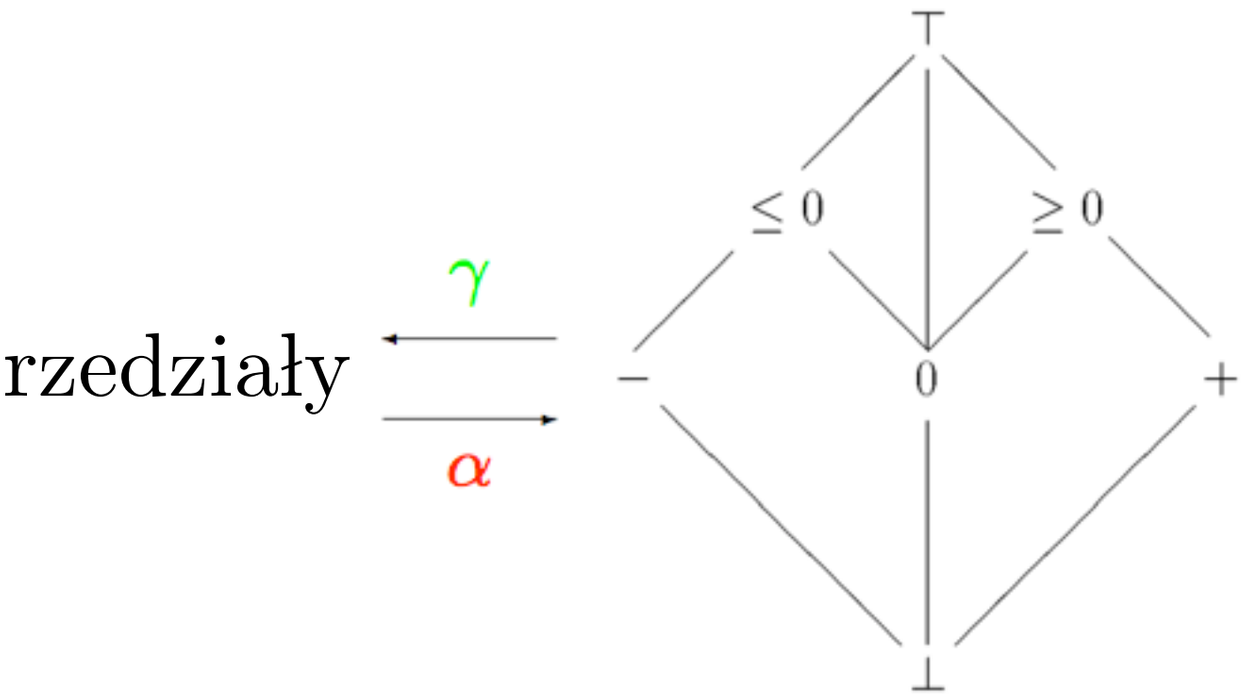
Różne dziedziny abstrakcyjne



Dziedzina *M* jest bardziej abtrakcyjna (mniej dokładna) niż *L*

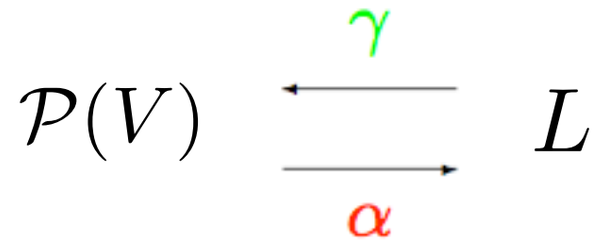
Przykład

Przedziały



brakuje -+

Funkcja reprezentacji β indukuje sprzężenie



$$\alpha(X) = \sqcup\{\beta(v) \mid v \in X\}$$

$$\gamma(l) = \{v \in V \mid \beta(v) \sqsubseteq l\}$$

Przykład

$$\beta : \mathbb{Z} \to \{-, 0, +\}$$

$$\mathcal{P}(V) \underset{\alpha}{\overset{\gamma}{\rightleftarrows}} \mathcal{P}(\{-, 0, +\})$$

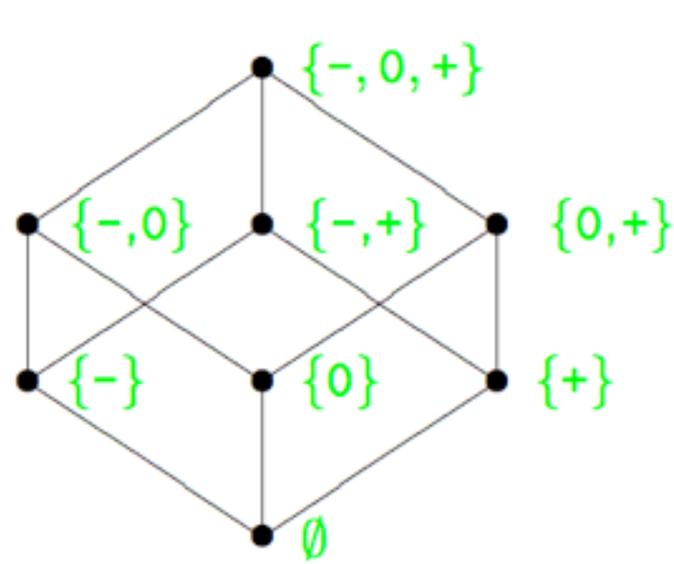
$$\alpha(X) = \{\beta(z) \mid z \in X\}$$

$$\gamma(S) = \{z \in \mathbb{Z} \mid \beta(z) \in S\}$$

Przykład

$$\beta : \mathbb{Z} \to \{-, 0, +\} \quad \subseteq \mathcal{P}(\{-, 0, +\})$$

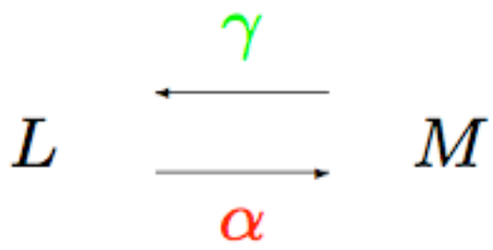
$$\mathcal{P}(V) \underset{\alpha}{\overset{\gamma}{\rightleftarrows}} \mathcal{P}(\{-, 0, +\})$$



$$\alpha(X) = \{\beta(z) \mid z \in X\}$$

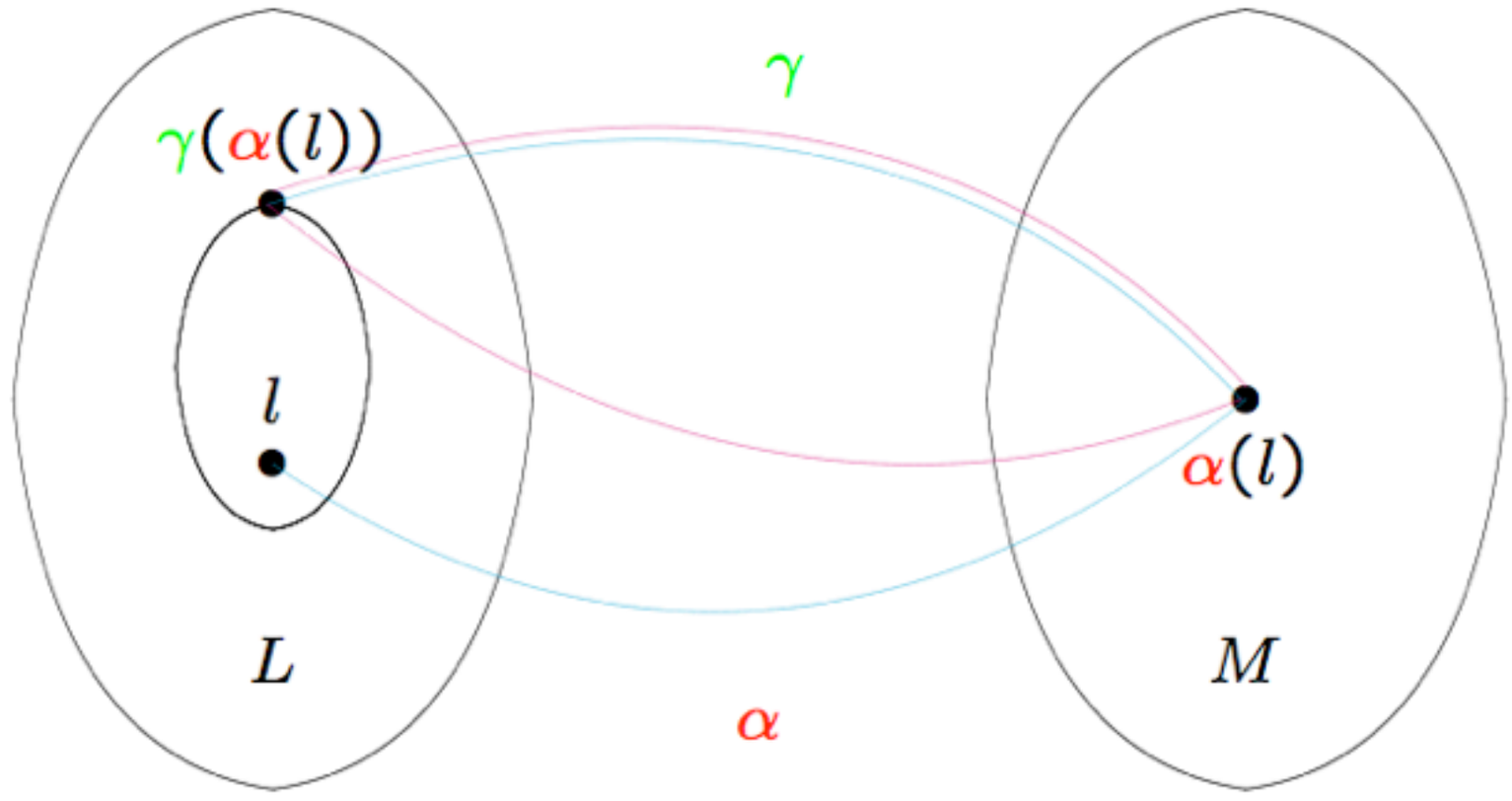
$$\gamma(S) = \{z \in \mathbb{Z} \mid \beta(z) \in S\}$$

Włożenie Galois



α - funkcja abstrakcji

γ - funkcja konkretyzacji

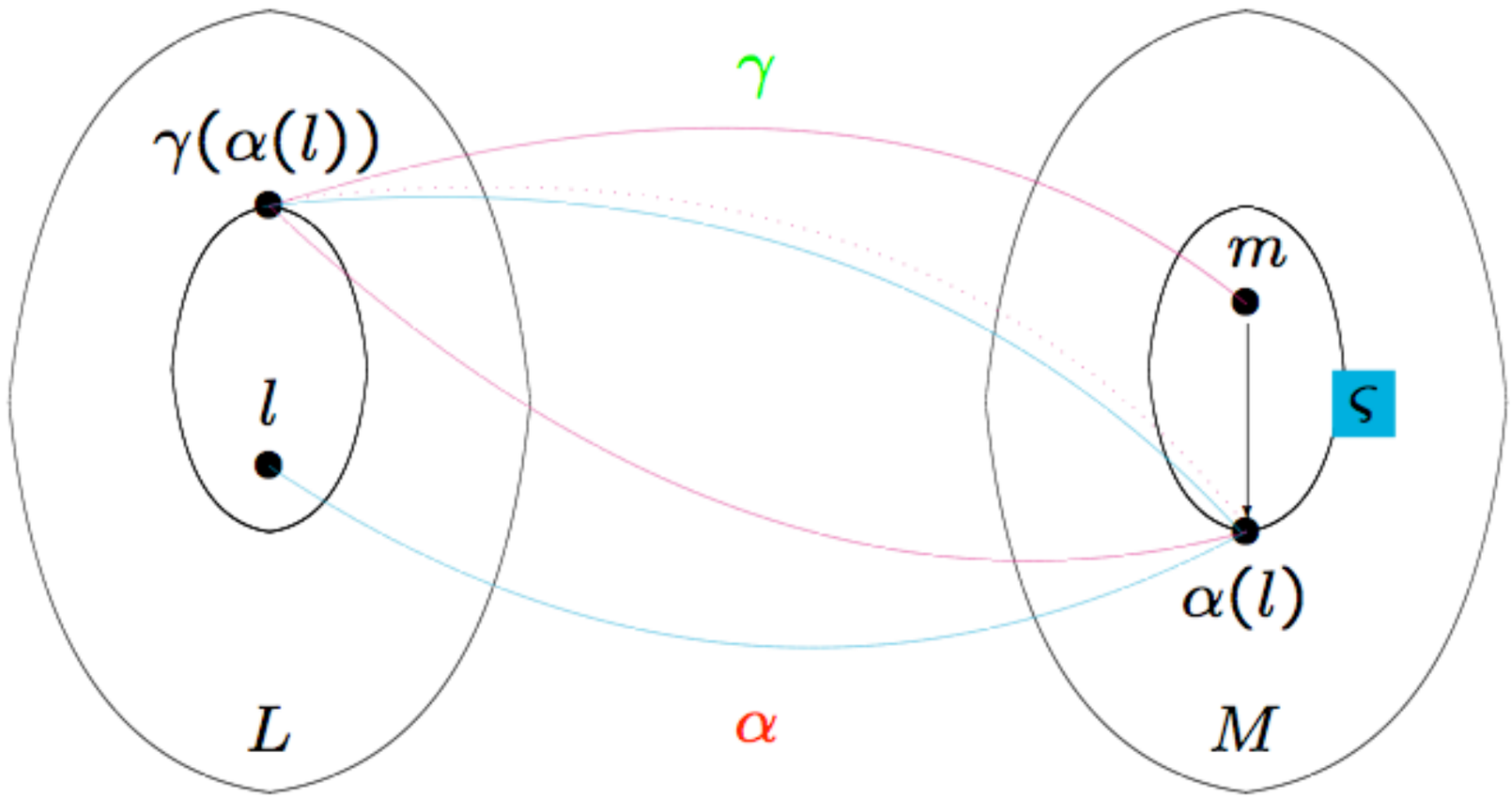


$$l \sqsubseteq \gamma(\alpha(l))$$

$$\alpha(\gamma(m)) = m$$

Redukcja

eliminacja zbędnych elementów abstrakcyjnych



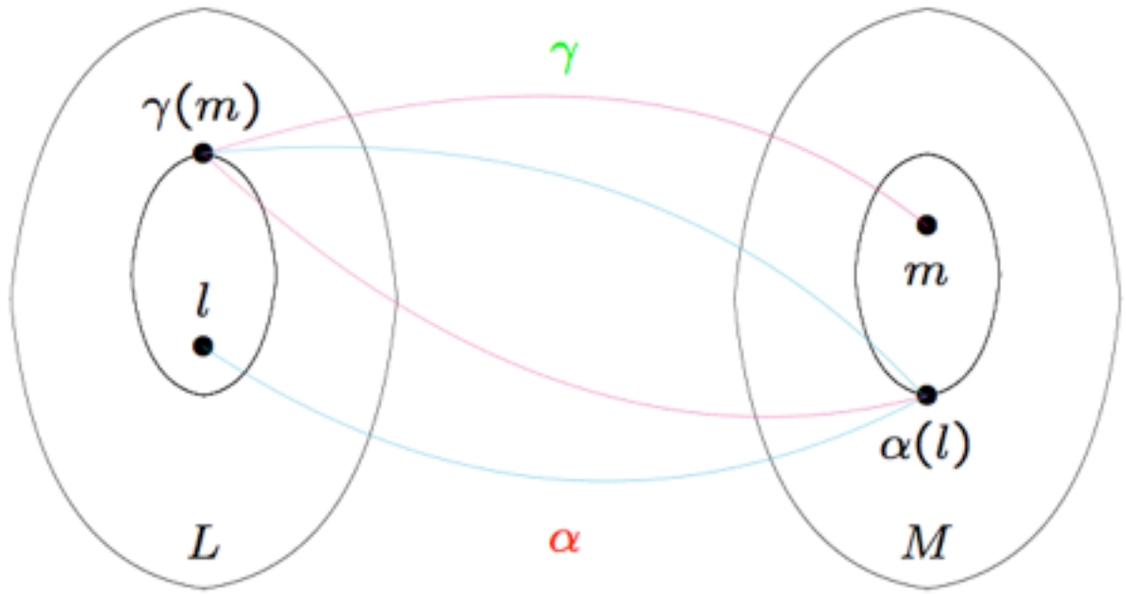
$$\zeta(m) = \sqcap\{m' \mid \gamma(m') = \gamma(m)\}$$

Właściwe pojęcie

- dobre własności matematyczne
    - lewy sprzężony zachowuje kresy górne
    - prawy sprzężony zachowuje kresy dolne
    - jednoznaczność
    - istnienie sprzężonego, gdy funkcja monotoniczna zachowuje kresy górne/dolne

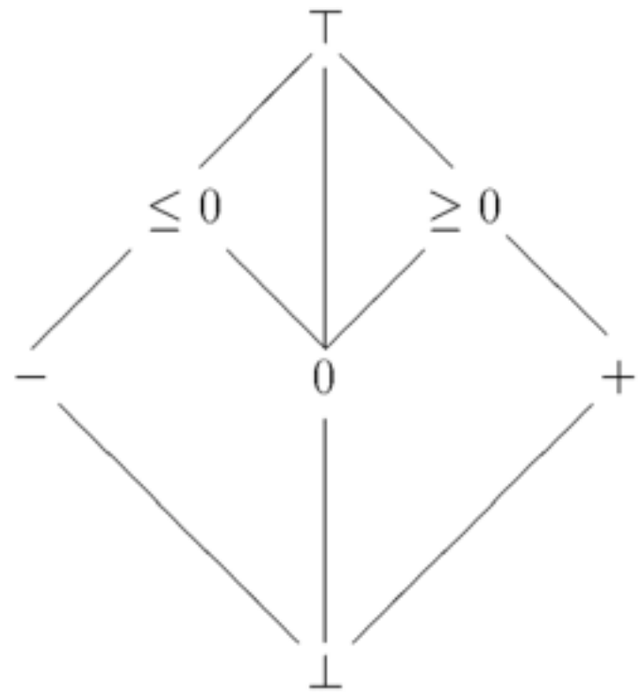
Właściwe pojęcie

- równoważne definicje:
  - domknięcie
  - rodziny Moore'a



- sprzężenia dobrze się składają
  - co pozwala budować dokładniejsze analizy z prostszych analiz składowych
- sprzężenie indukuje najdokładniejszą semantykę abstrakcyjną

$$\mathcal{P}(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \text{Przedziały} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}}$$



$$\alpha(S) = \begin{cases} \bot & \text{if } S = \{\} \text{ else} \\ + & \text{if } S \subseteq \{1, 2, 3, ...\} \text{ else} \\ \geq 0 & \text{if } S \subseteq \{0, 1, 2, 3, \ldots\} \text{ else} \\ - & \text{if } S \subseteq \{\text{-}1, \text{-}2, \text{-}3, \ldots\} \text{ else} \\ \leq 0 & \text{if } S \subseteq \{0, \text{-}1, \text{-}2, \text{-}3, \ldots\} \text{ else} \\ \top & \end{cases}$$

$$\begin{aligned} \gamma(0) &= \{0\} \\ \gamma(+) &= \{1, 2, 3, ...\} \\ \gamma(-) &= \{-1, -2, -3, \ldots\} \\ \gamma(\bot) &= \{\} \\ \gamma(\geq 0) &= \{0, 1, 2, 3, ...\} \\ \gamma(\leq 0) &= \{0, -1, -2, -3, ...\} \\ \gamma(\top) &= \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\} \end{aligned}$$

Bezpieczna aproksymacja

$$\mathrm{op} : \mathbb{Z} \to \mathbb{Z}$$

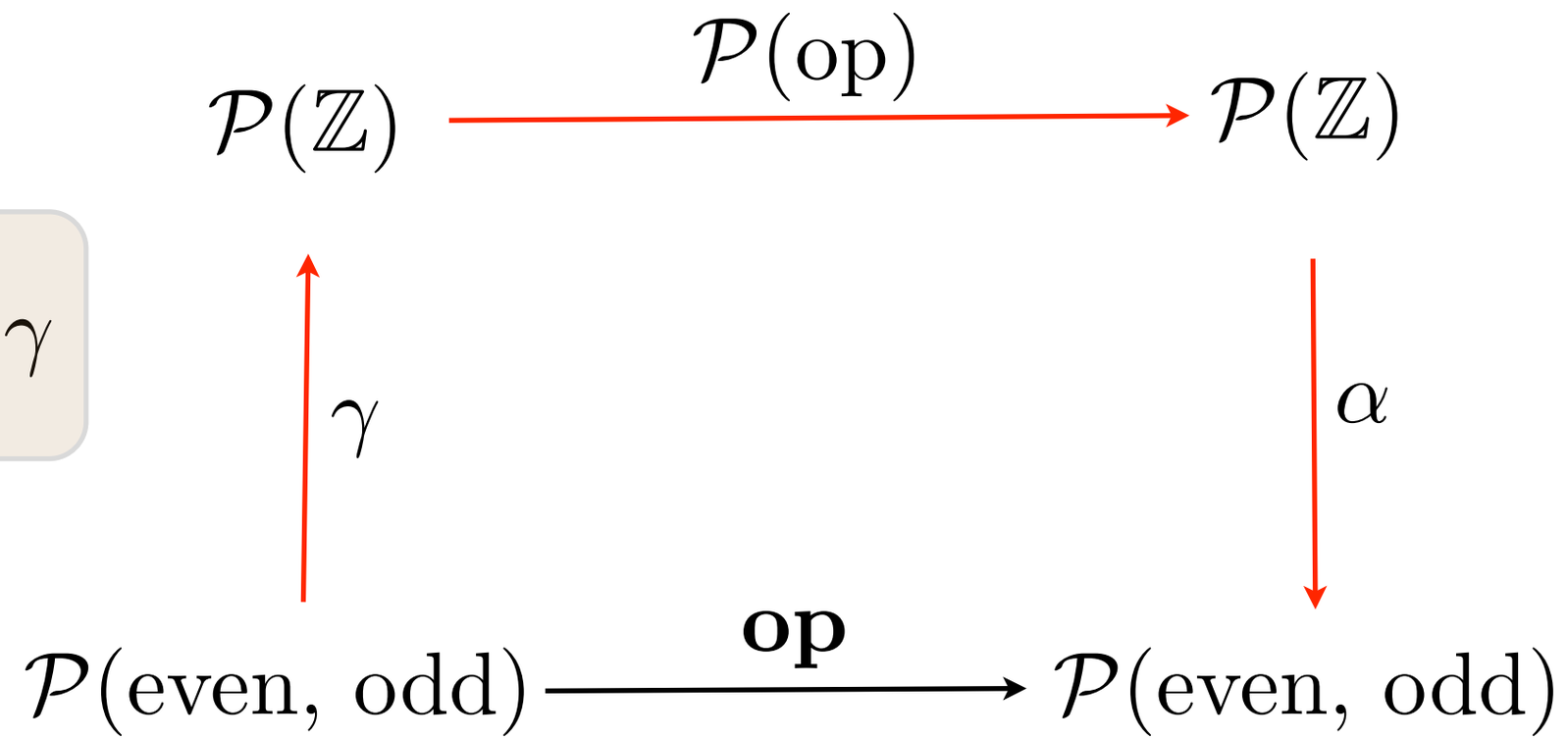
$$\mathcal{P}(\mathrm{op}) : \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$$

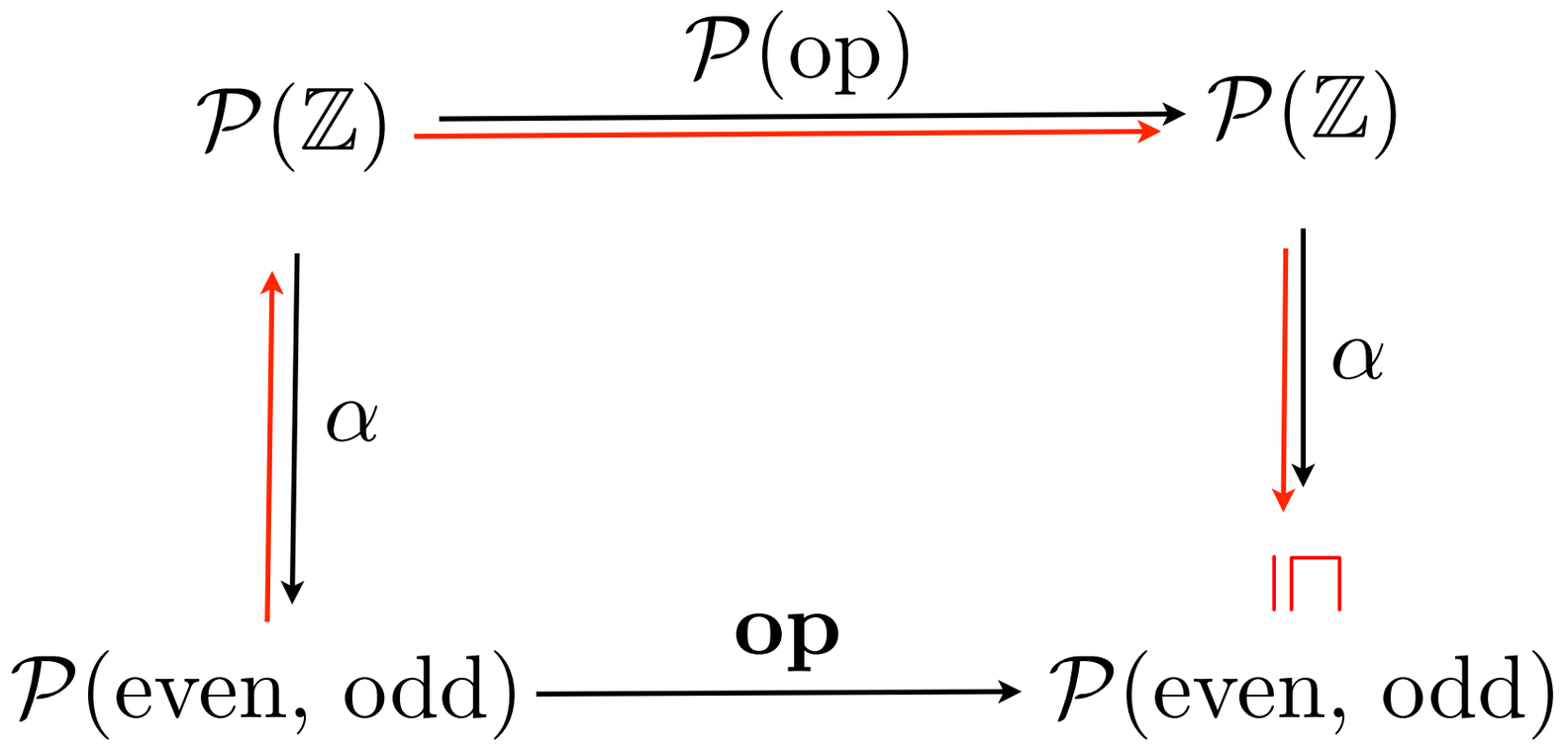
$$\begin{array}{ccc}
\mathcal{P}(\mathbb{Z}) & \xrightarrow{\mathcal{P}(\mathrm{op})} & \mathcal{P}(\mathbb{Z}) \\
\Big\downarrow \alpha & & \Big\uparrow \gamma \\
\mathcal{P}(\text{even, odd}) & \xrightarrow{\mathbf{op}} & \mathcal{P}(\text{even, odd})
\end{array}$$

$$\begin{array}{ccc}
\mathcal{P}(\mathbb{Z}) & \xrightarrow{\mathcal{P}(\mathrm{op})} & \mathcal{P}(\mathbb{Z}) \\
\Big\downarrow \alpha & & \Big\downarrow \alpha \\
\mathcal{P}(\text{even, odd}) & \xrightarrow{\mathbf{op}} & \mathcal{P}(\text{even, odd})
\end{array}$$

Najdokładniejsza aproksymacja

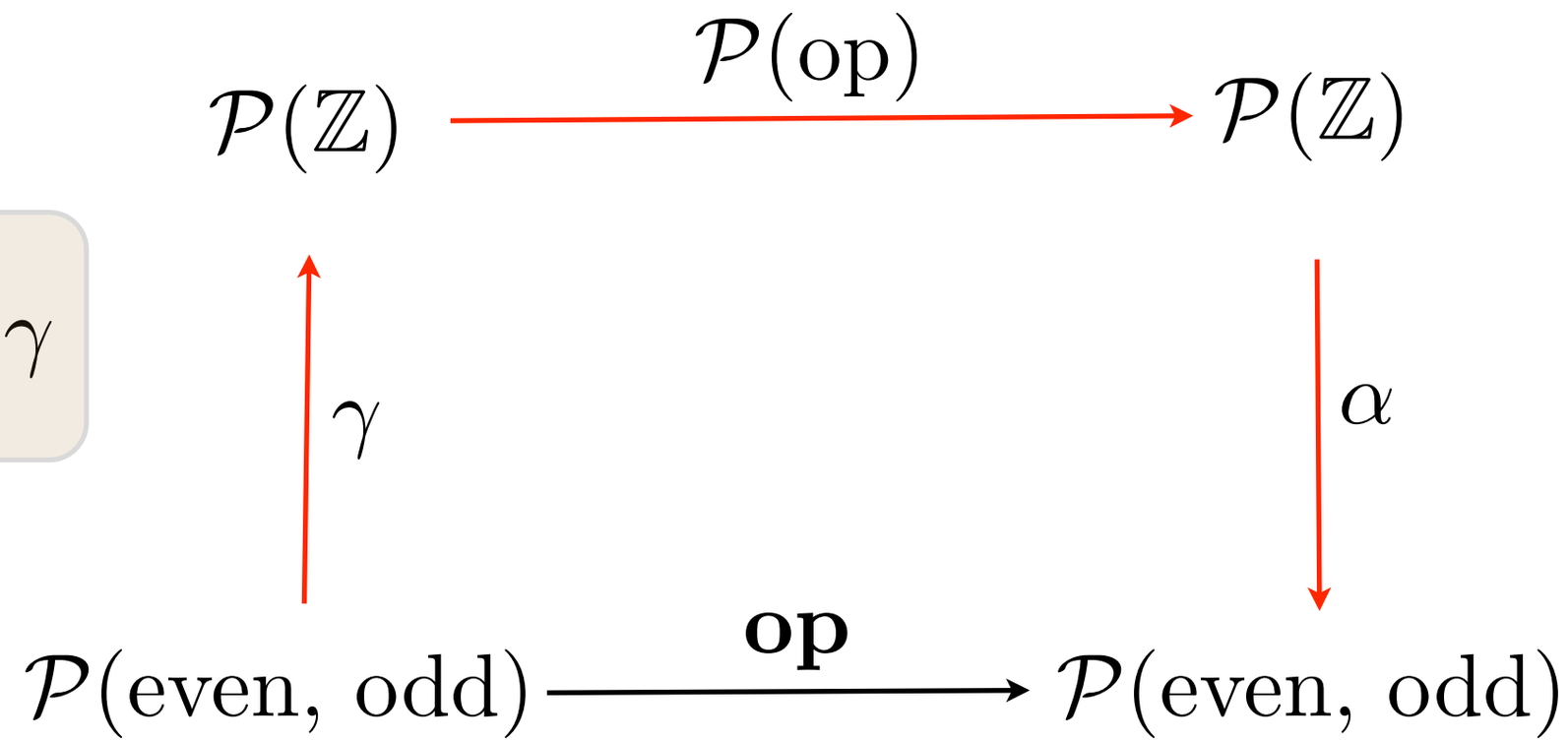
$$\mathbf{op} \;:=\; \alpha \circ \mathcal{P}(\mathrm{op}) \circ \gamma$$



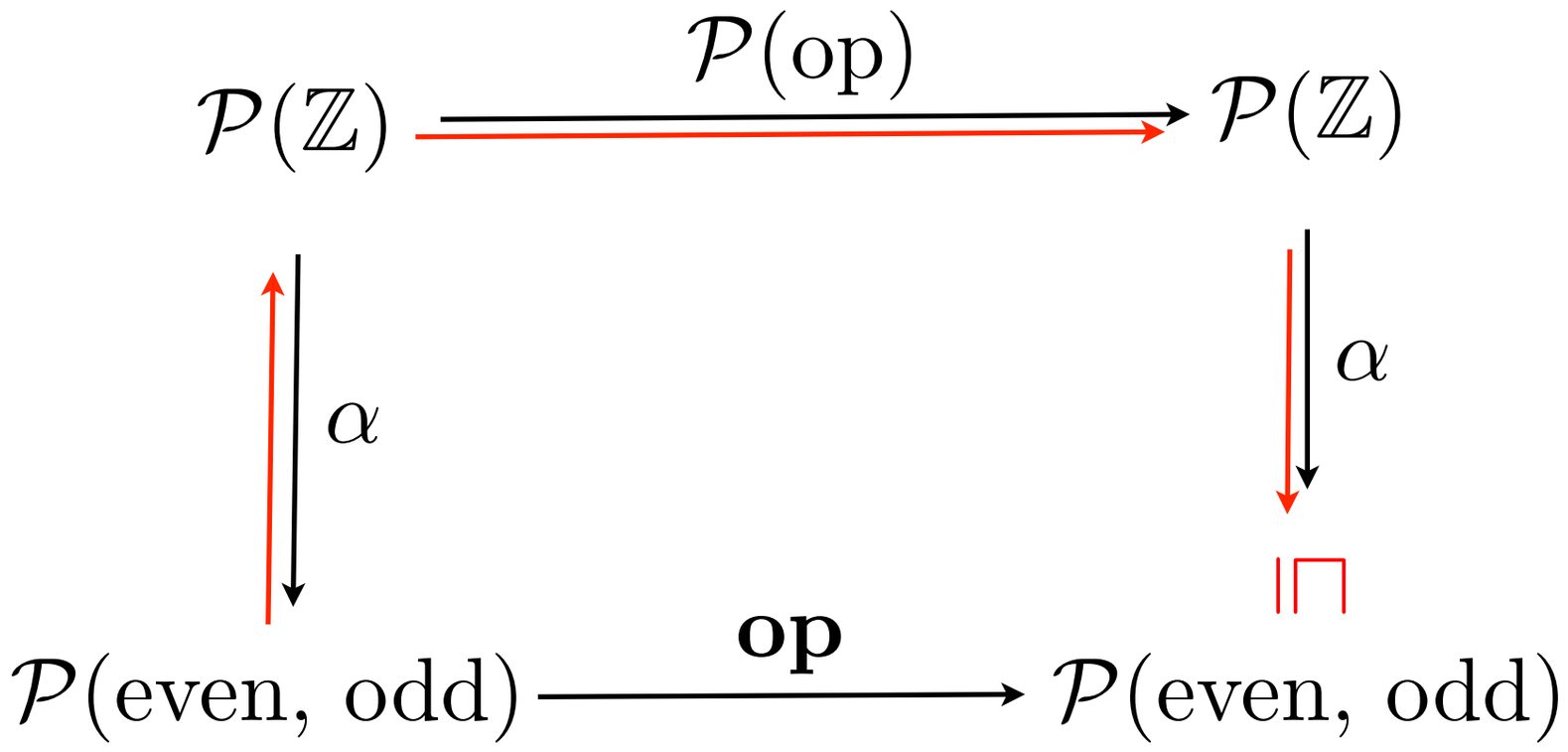


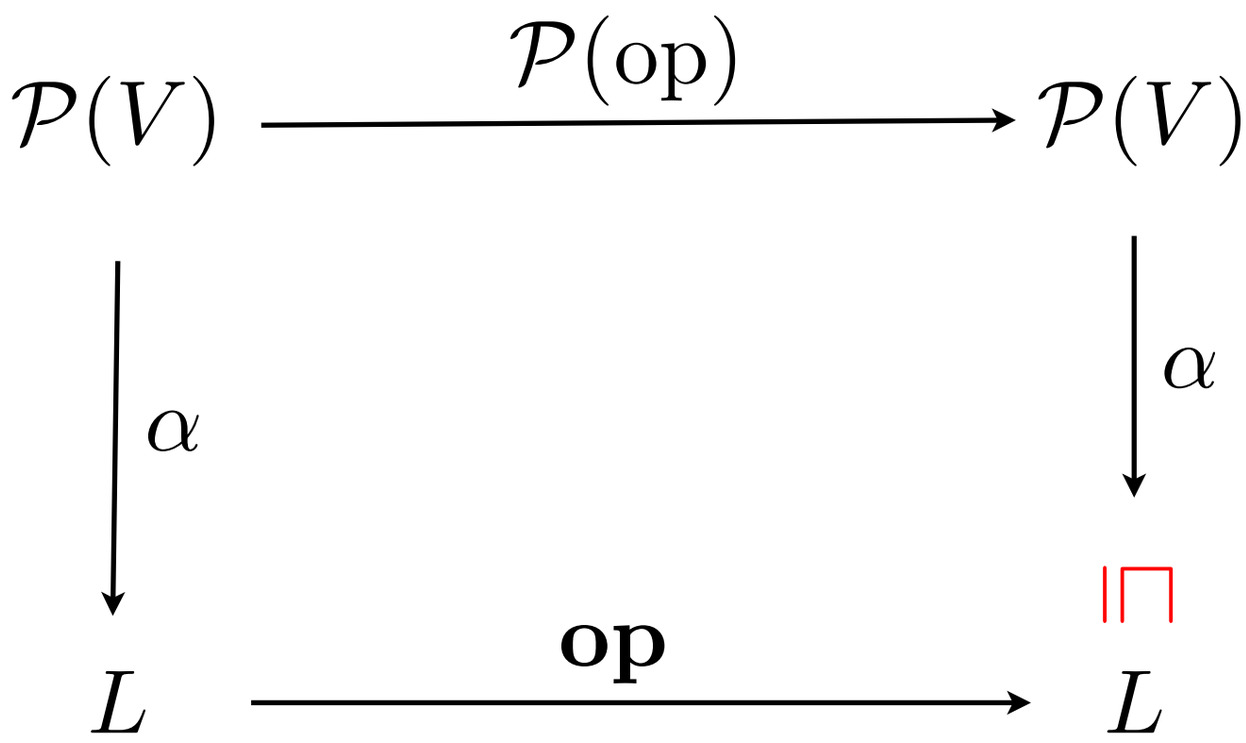
Najdokładniejsza aproksymacja

$$\mathbf{op} \;:=\; \alpha \circ \mathcal{P}(\mathrm{op}) \circ \gamma$$

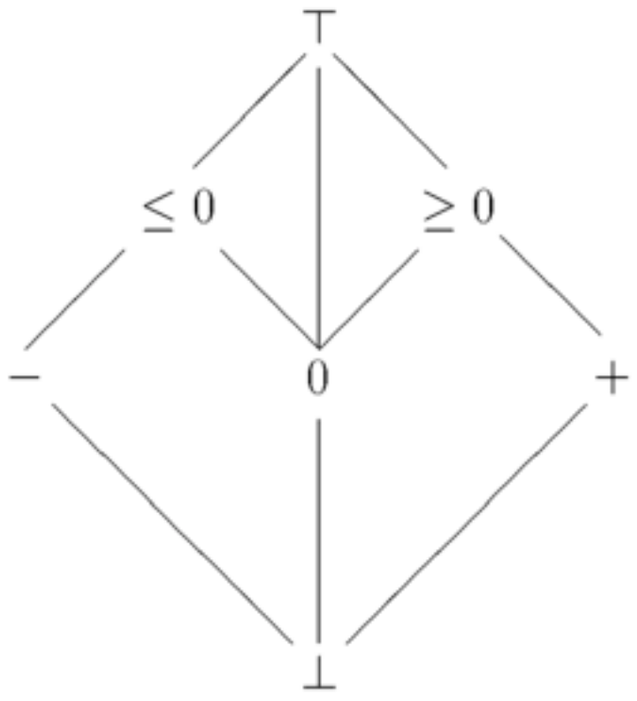


jak obliczyć op ?




$\mathcal{P}(V)$
$\mathcal{P}(\mathrm{op})$
$\mathcal{P}(V)$
α
α
L
$\mathbf{op}$
L

Przykład

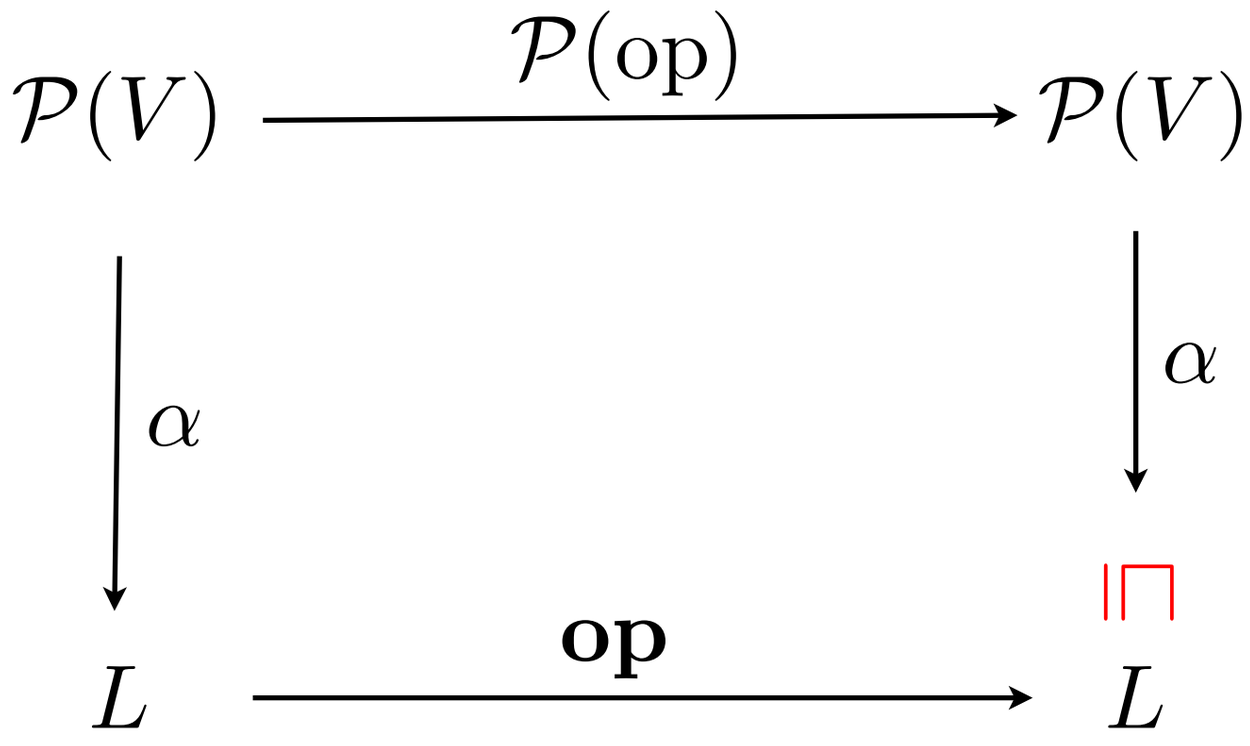


$$
\begin{aligned}
\gamma(0) &= \{0\} \\
\gamma(+) &= \{1, 2, 3, ...\} \\
\gamma(-) &= \{-1, -2, -3, \ldots\} \\
\gamma(\bot) &= \{\} \\
\gamma(\geq 0) &= \{0, 1, 2, 3, ...\} \\
\gamma(\leq 0) &= \{0, -1, -2, -3, ...\} \\
\gamma(\top) &= \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}
\end{aligned}
$$

$$
\alpha(S) = \begin{cases}
\bot & \text{if } S = \{\} \text{ else} \\
+ & \text{if } S \subseteq \{1, 2, 3, ...\} \text{ else} \\
\geq 0 & \text{if } S \subseteq \{0, 1, 2, 3, \ldots\} \text{ else} \\
- & \text{if } S \subseteq \{\text{-}1, \text{-}2, \text{-}3, \ldots\} \text{ else} \\
\leq 0 & \text{if } S \subseteq \{0, \text{-}1, \text{-}2, \text{-}3, \ldots\} \text{ else} \\
\top &
\end{cases}
$$

$$+ \;:\; \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

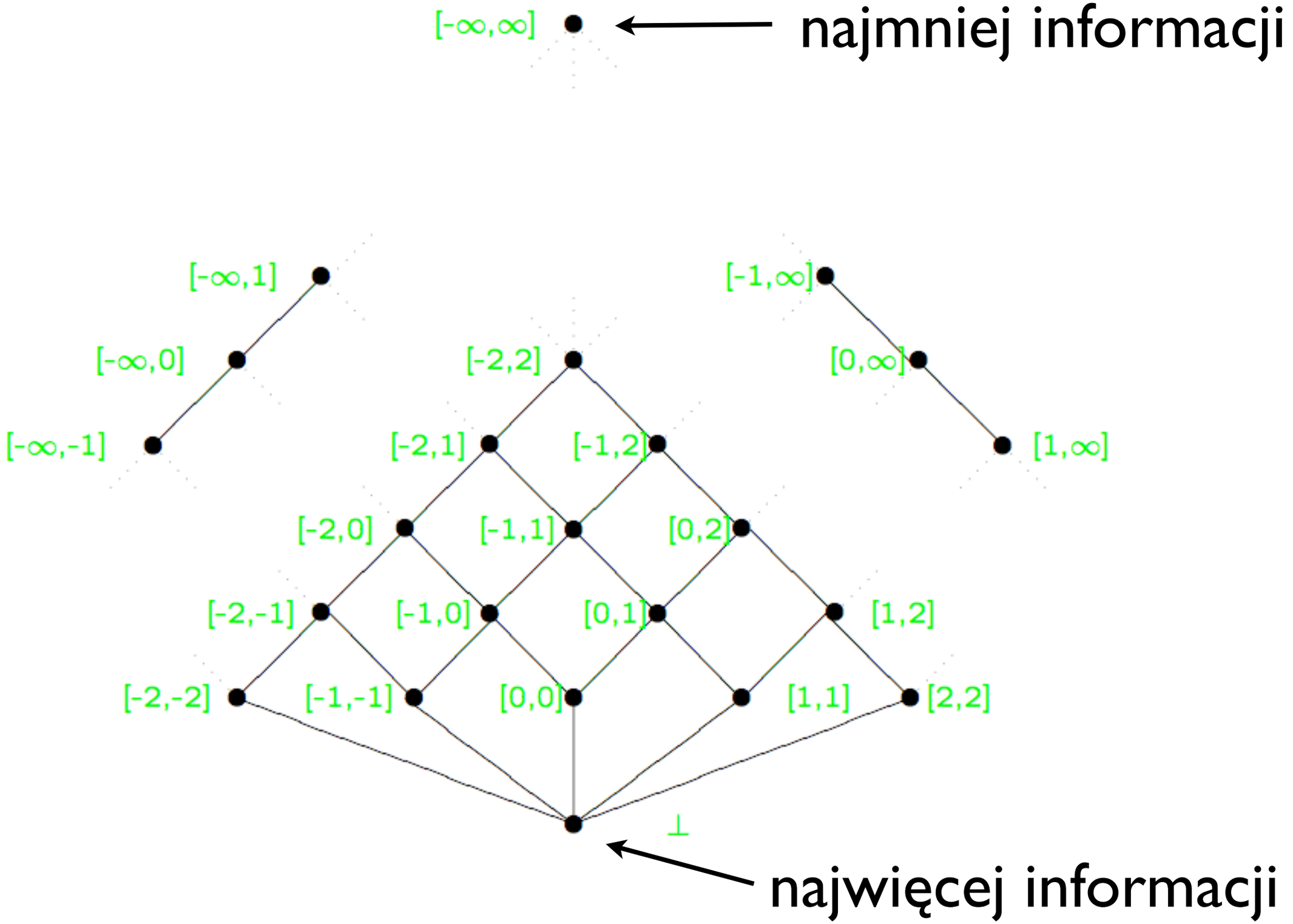
$+'$	$\bot$	$-$	0	$+$	≥ 0	≤ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$-$	$\bot$	$-$	$-$	$\top$	$\top$	$-$	$\top$
0	$\bot$	$-$	0	$+$	≥ 0	≤ 0	$\top$
$+$	$\bot$	$\top$	$+$	$+$	$+$	$\top$	$\top$
≥ 0	$\bot$	$\top$	≥ 0	$+$	≥ 0	$\top$	$\top$
≤ 0	$\bot$	$-$	≤ 0	$\top$	$\top$	≤ 0	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$



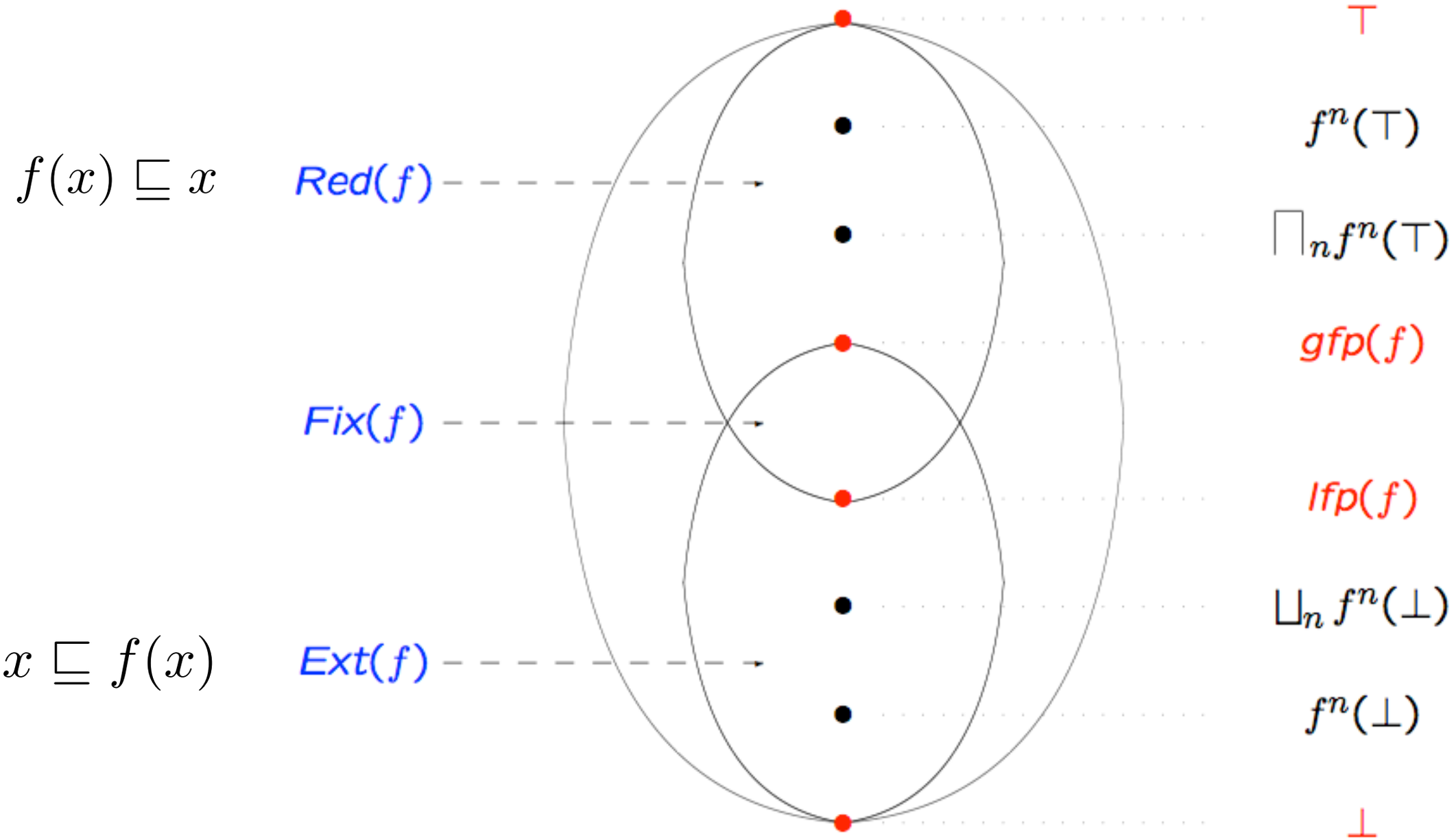
Poszerzanie/zwężanie

Krata zupełna L^S

$$f : L^S \to L^S$$

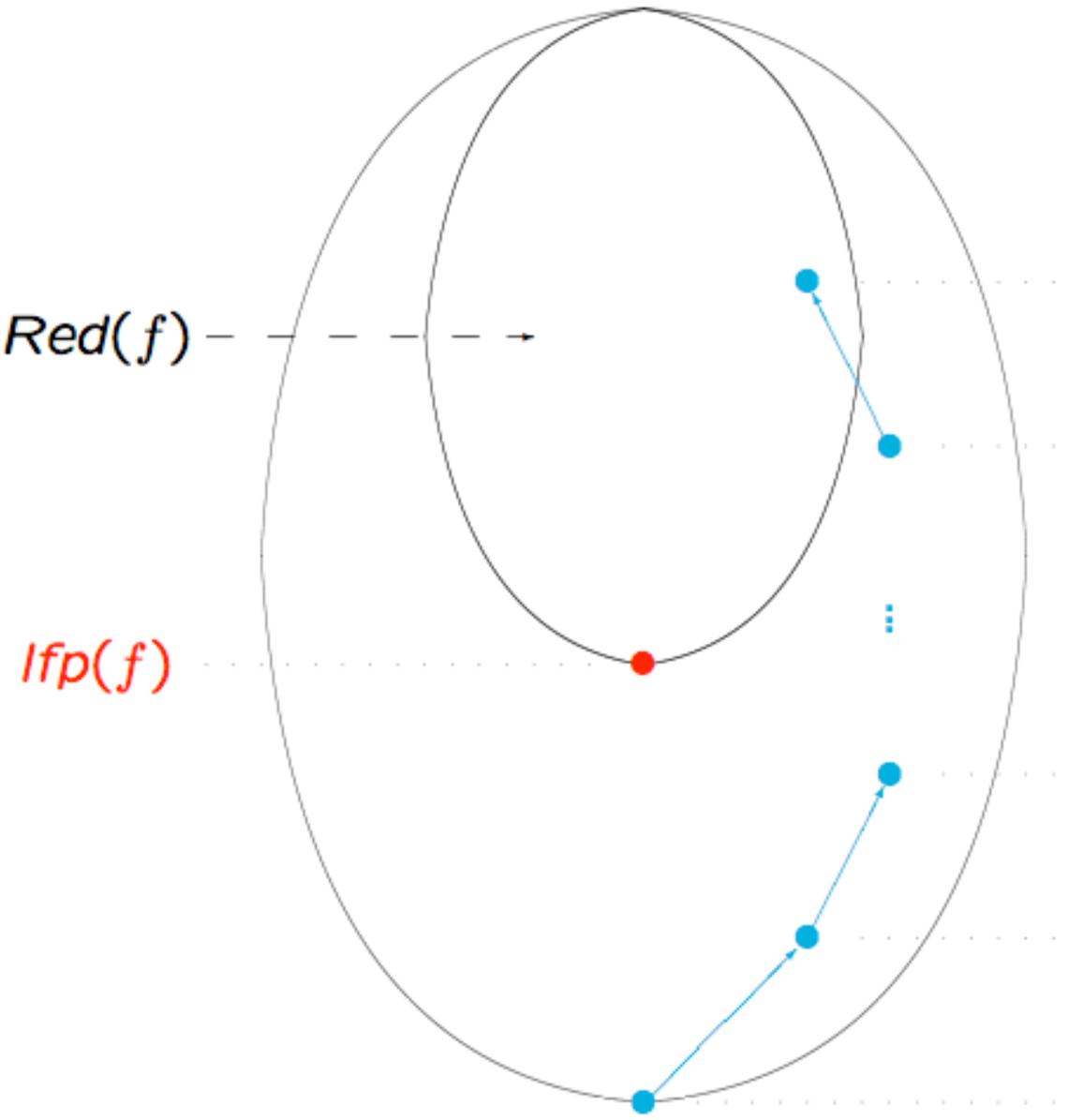

[-∞,∞]
najmniej informacji
[-∞,1]
[-∞,0]
[-∞,-1]
[-2,2]
[-2,1]
[-1,2]
[-2,0]
[-1,1]
[0,2]
[-2,-1]
[-1,0]
[0,1]
[1,2]
[-2,-2]
[-1,-1]
[0,0]
[1,1]
[2,2]
[-1,∞]
[0,∞]
[1,∞]
⊥
najwięcej informacji

Punkty stałe



Poszerzanie

$f(x) \sqsubseteq x$



$$a, b \sqsubseteq a \nabla b$$

(a_n) jest skończony

$$\ldots$$

$$a_3 = a_2 \nabla f(a_2)$$

$$\ldots \; f(a_i) \sqsubseteq a_i$$

$$f(a_2)$$

$$a_2 = a_1 \nabla f(a_1)$$

$$\ldots$$

$$f(a_1)$$

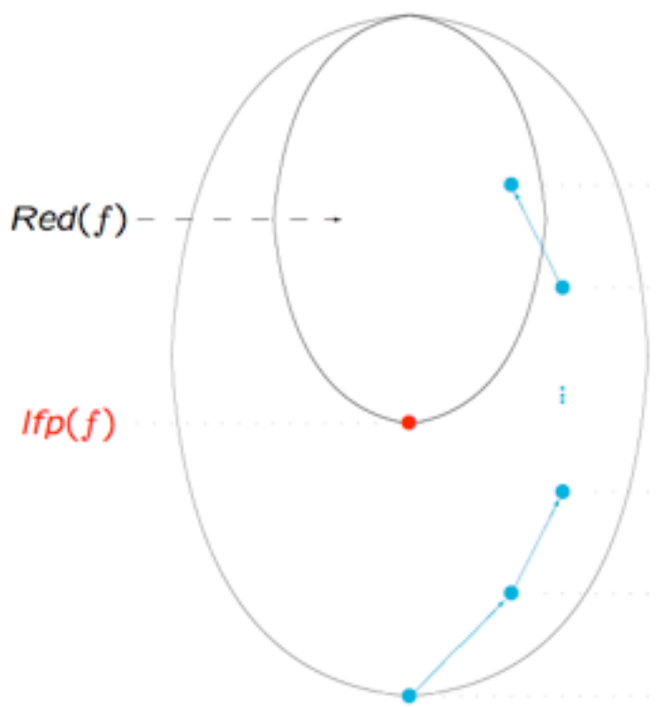
$$f^3(\bot)$$

$$a_1 = \bot \nabla f(\bot)$$

$$f^2(\bot)$$

$$f(\bot)$$

$$\bot$$



Przykład

K - stałe liczbowe występujące w programie

$$[z_1, z_2] \nabla [z_3, z_4] \quad = \quad [\ \mathsf{LB}(z_1, z_3)\ ,\ \mathsf{UB}(z_2, z_4)\ ]$$

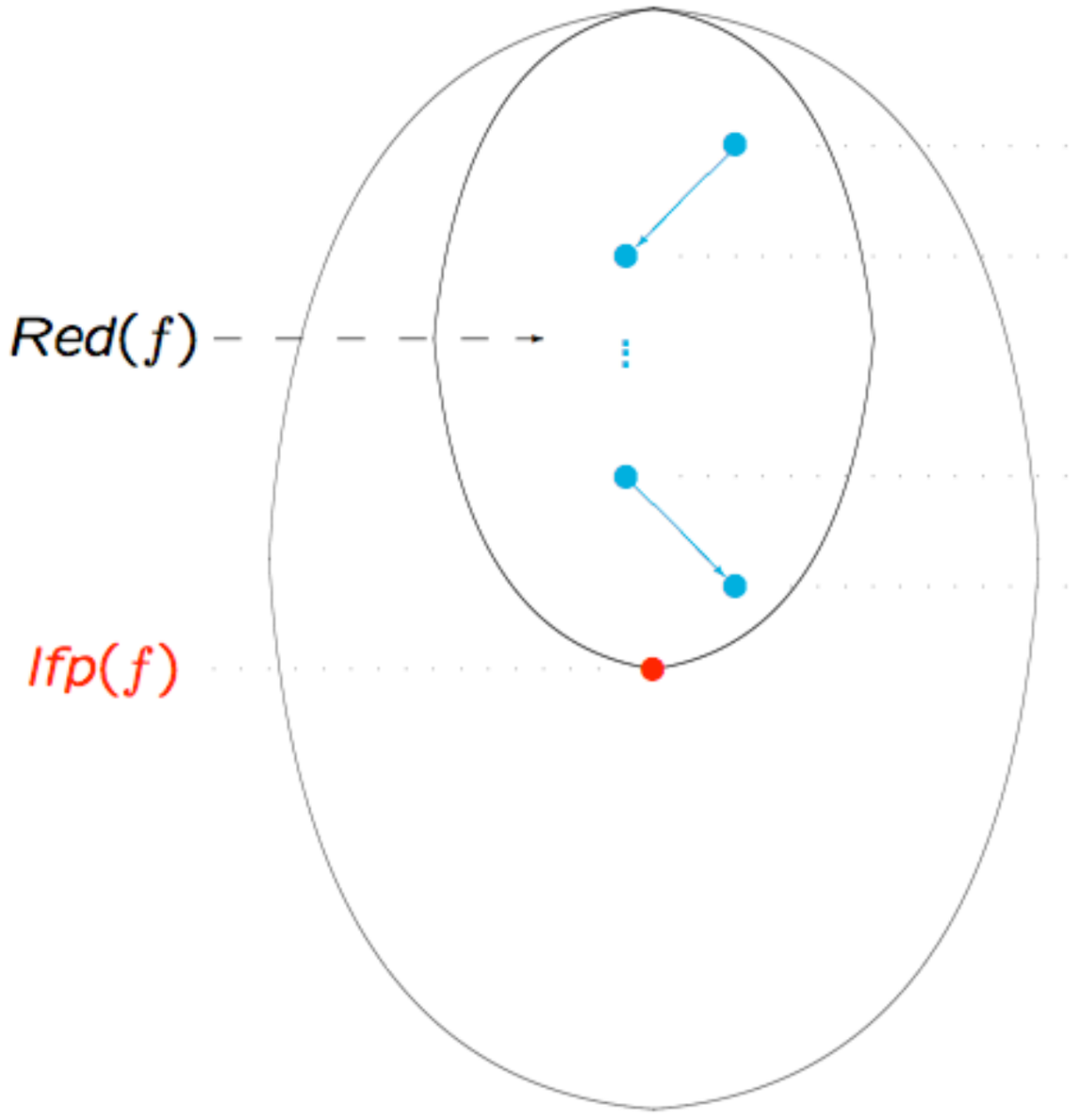
$$\mathsf{LB}(z_1, z_3) \in \{z_1\} \cup K \cup \{-\infty\}$$

$$\mathsf{UB}(z_2, z_4) \in \{z_2\} \cup K \cup \{\infty\}$$

$$\mathsf{LB}_K(z_1, z_3) = \begin{cases} z_1 & \text{if } z_1 \leq z_3 \\ k & \text{if } z_3 < z_1 \ \wedge\ k = \max\{k \in K \mid k \leq z_3\} \\ -\infty & \text{if } z_3 < z_1 \ \wedge\ \forall k \in K : z_3 < k \end{cases}$$

$$\mathsf{UB}_K(z_2, z_4) = \begin{cases} z_2 & \text{if } z_4 \leq z_2 \\ k & \text{if } z_2 < z_4 \ \wedge\ k = \min\{k \in K \mid z_4 \leq k\} \\ \infty & \text{if } z_2 < z_4 \ \wedge\ \forall k \in K : k < z_4 \end{cases}$$

Zwężanie



$$[z_1, \infty], [z_3, \infty], [z_3, \infty], \ldots \qquad z_1 < z_2 < z_3 < \ldots$$