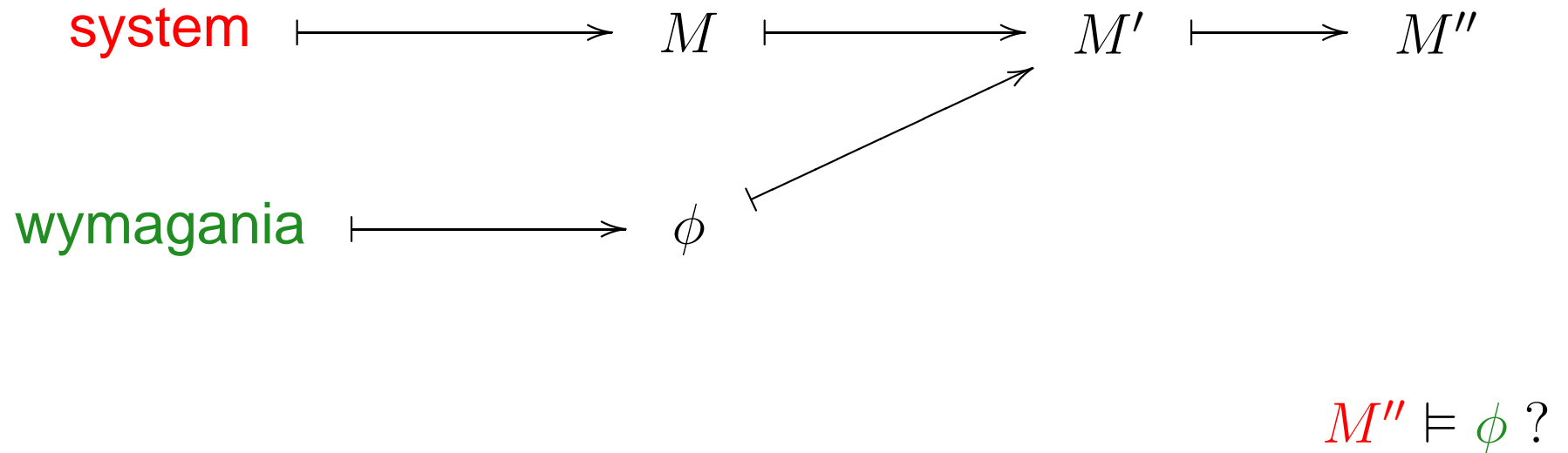


Praktyczne metody weryfikacji

Wykład 12: Abstrakcja

Od rzeczywistości do modelu



Abstrakcja = usuwanie z modelu
zbe, dnej informacji

Metody abstrakcji:

- eliminacja zmiennych
- abstrakcja danych
- abstrakcja oparta na symetrii
- ...

$$M \longmapsto M'$$

Model: $V = \{x_1, \dots, x_n\}, \quad S = D^n$

$$L(d_1 \dots d_n) = \{ "x_1 = d_1", \dots, "x_n = d_n" \}$$

Uwaga: abstrakcja dotyczy opisu modelu

R, S_0 reprezentowane przez formuły

$$(s, s') \in B \implies$$

$$- L(s) = L(s')$$

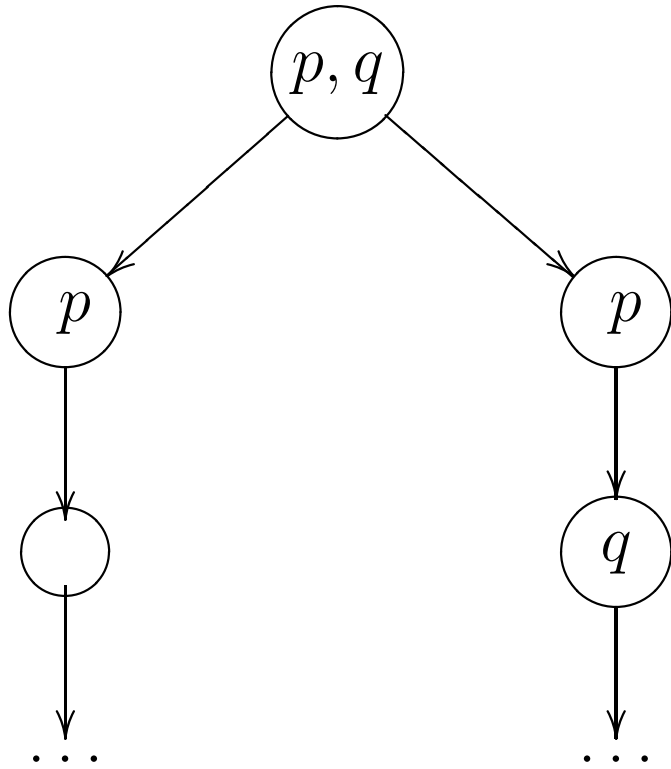
$$- s \rightarrow r \implies \exists r'. s' \rightarrow r', (r, r') \in B$$

$$- s' \rightarrow r' \implies \exists r. s \rightarrow r, (r, r') \in B$$

$s \sim s' \iff (s, s') \in B$ dla pewnej bisymulacji B

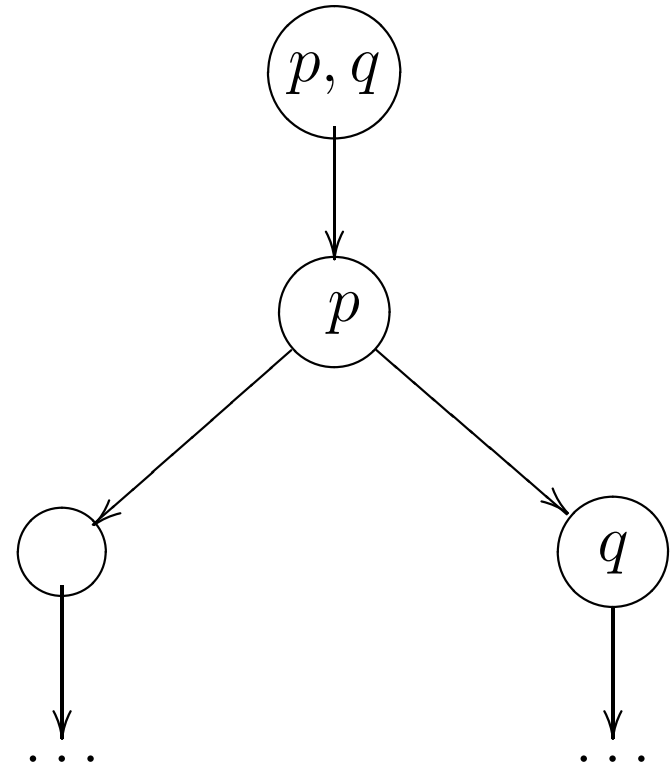
$$M \sim M' \iff s_0 \sim s'_0$$

gra $G_{M \ M'}$



\equiv

\approx



gra $G_{M M'}$

- konfiguracje: $\langle s, s' \rangle$
- konfiguracja pocz.: $\langle s_0, s'_0 \rangle$
- gracz I wybiera stronę i tranzycję $s \rightarrow r$ (lub $s' \rightarrow r'$)
- gracz II odpowiada po drugiej stronie
- itd.

- kto wygrywa?

Tw.: $M \sim M' \implies (\forall \phi \in \text{CTL}^*. M \models \phi \iff M' \models \phi)$

Tw.: $M \sim M' \iff (\forall \phi \in \text{CTL}. M \models \phi \iff M' \models \phi)$

Wn.: $\equiv_{\text{CTL}^*} = \equiv_{\text{CTL}} = \dots = \equiv_{\text{EX}}$

Algorytm symboliczny:

$$B_0 := \{\langle s, s' \rangle \mid L(s) = L'(s')\}$$

powtarzaj

$$B_{i+1} := \{\langle s, s' \rangle \mid s \rightarrow r \implies \exists r'. s' \rightarrow r', (r, r') \in B_i \wedge \\ s' \rightarrow r' \implies \exists r. s \rightarrow r, (r, r') \in B_i\}$$

az $B_{i+1} = B_i$

$$(s, s') \in B \implies$$

- $L(s) = L(s')$
- \forall sprawiedl. Π z $s \exists$ sprawiedl. Π' z s' . $(\Pi, \Pi') \in B$
- \forall sprawiedl. Π' z $s' \exists$ sprawiedl. Π z s . $(\Pi, \Pi') \in B$

$s \sim_F s' \iff (s, s') \in B$ dla pewnej sprawiedl. bisymulacji B

$$M \sim_F M' \iff s_0 \sim_F s'_0$$

Def: $V' \subseteq V$; $C(V') \subseteq V$ zmienne od których zależy V'

Przykład: licznik 3-bitowy

$$\begin{aligned}R_0(\vec{x}, x'_0) &= (x'_0 = \neg x_0) \\R_1(\vec{x}, x'_1) &= (x'_1 = x_0 \text{ XOR } x_1) \\R_2(\vec{x}, x'_2) &= (x'_2 = (x_0 \wedge x_1) \text{ XOR } x_2)\end{aligned}$$

$$C(\{x_i\}) = \{x_0, \dots, x_i\}$$

Eliminacja zmiennych

- $\{x_1, \dots, x_k\} := C(V')$, V' - zmienne w formule
- $S' = D^k$
- $R'(x_1, \dots, x_k, x'_1, \dots, x'_k)$
- $S'_0(x_1, \dots, x_k) \equiv \exists x_{k+1}, \dots, x_n. S_0(x_1, \dots, x_n)$

$$(d_1, \dots, d_n)B(d'_1, \dots, d'_k) \iff d_1 = d'_1 \wedge \dots \wedge d_k = d'_k$$

$$P \supseteq P'$$

$$(s, s') \in S \implies$$

$$- L(s) \cap P' = L(s')$$

$$- s \rightarrow r \implies \exists r'. s' \rightarrow r', (r, r') \in S$$

$$s \preceq s' \iff (s, s') \in S \text{ dla pewnej symulacji } S$$

$$M \preceq M' \iff s_0 \preceq s'_0$$

Tw.: $M \preceq M' \implies (\forall \phi \in \text{ACTL}^*. M' \models \phi \implies M \models \phi)$

Tw.: $M \preceq M' \implies (\forall \phi \in \text{ECTL}^*. M \models \phi \implies M' \models \phi)$

Def.: $\simeq = \preceq \cap \succeq$

Pytanie: Czy $\sim = \simeq$?

\preceq_F, \simeq_F analogicznie

Przykład:

$$h_x(d) = \begin{cases} a_+ & x > 0 \\ a_0 & x = 0 \\ a_- & x < 0 \end{cases} \quad h_x : D \rightarrow A$$

$$\begin{array}{c} x = 5 \\ \downarrow \\ x = 4 \end{array}$$

$$\begin{array}{c} a_+ \\ \downarrow \\ a_+ \text{ czy } a_0? \end{array}$$

- model abstrakcyjny ma więcej zachowań – symulacja
- **niedeterminizm**

$$M \mapsto M' = M / \approx$$

$$\approx = \ker(h)$$

$$S_0(\vec{d}) \implies S'_0([\vec{d}])$$

$$R(\vec{d}_1, \vec{d}_2) \implies R'([\vec{d}_1], [\vec{d}_2])$$

Tw.: $M \preceq M'$

Tw.: $M \sim M'$ gdy \approx jest bisymulacją

Przykładowe abstrakcje:

- znak
- logarytm
- wybrany bit
- kongruencja $\text{mod } m$
- $h = \langle h_1, h_2 \rangle$
- ...

$$h_x : D \rightarrow A$$

$$- S' = A^n$$

$$- R'(y_1, \dots, y_n, y'_1, \dots, y'_n) \equiv \exists x_1 \dots x_n, x'_1, \dots, x'_n.$$

$$R(x_1, \dots, x_n, x'_1, \dots, x'_n) \wedge$$

$$y_1=h(x_1) \wedge \dots \wedge y_n=h(x_n) \wedge y'_1=h(x'_1) \wedge \dots \wedge y'_n=h(x'_n)$$

$$- S'_0(y_1, \dots, y_n) \equiv \exists x_1 \dots x_n. S_0(x_1, \dots, x_n) \wedge y_1=h(x_1) \wedge \dots$$

$$[\phi](\vec{y}) \equiv \exists \vec{x}. \phi(\vec{x}) \wedge y_1=h(x_1) \wedge \dots$$

Obliczamy przybliżenie $[\phi]$

$$- \mathcal{A}(\phi_1 \wedge \phi_2) = \mathcal{A}(\phi_1) \wedge \mathcal{A}(\phi_2)$$

$$- \mathcal{A}(\exists x. \phi) = \exists x. \mathcal{A}(\phi)$$

- ...

$$- \mathcal{A}(x' = x - 1) = (y = a_+ \wedge (y' = a_+ \vee y' = a_0)) \vee \dots$$

Fakt: $[\phi] \implies \mathcal{A}(\phi)$

Tw.: $M \preceq M^{\mathcal{A}}$

Uszczegółowianie abstrakcji

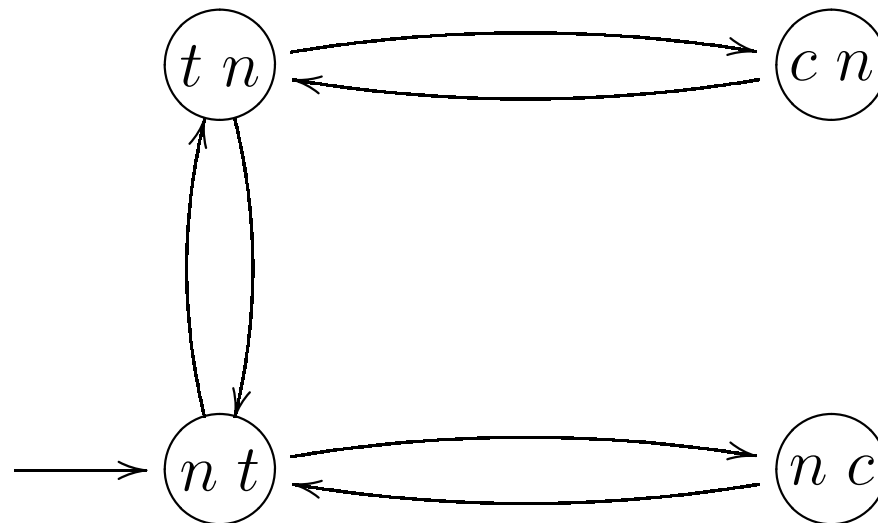
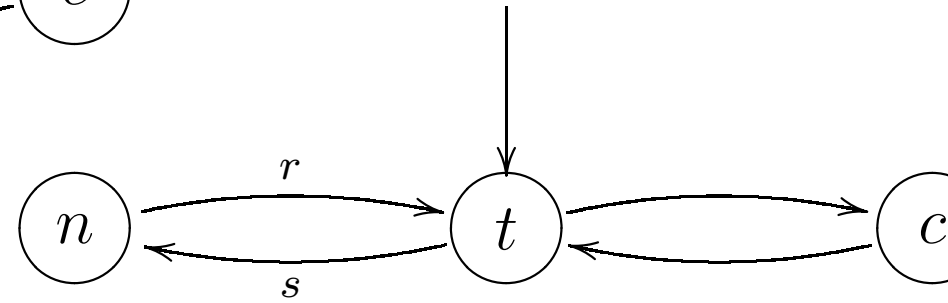
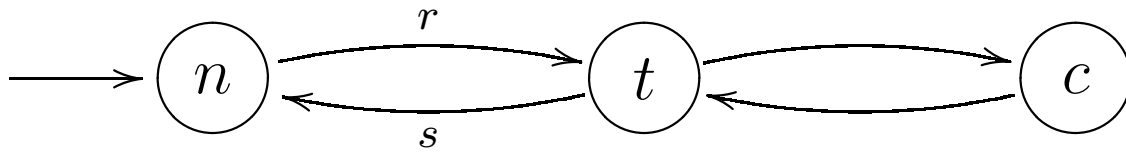
$$M \preceq M' \implies (\forall \phi \in \text{ACTL}^*. M' \models \phi \implies M \models \phi)$$

Powtarzaj:

- weryfikuj model abstrakcyjny
 - jeśli wynik pozytywny – **zakończ**
 - jeśli wynik negatywny – kontrprzykład abstrakcyjny
- jeśli kontrprzykład jest rzeczywisty – **zakończ**
- uszczegółów abstrakcję na podstawie kontrprzykładu

$M \sim M'$	$\forall \phi \in \text{CTL}^*. M \models \phi \iff M' \models \phi$
$M \sim_F M'$	$\forall \phi \in \text{CTL}^*. M \models_F \phi \iff M' \models_F \phi$
$M \preceq M'$	$\forall \phi \in \text{ACTL}^*. M' \models \phi \implies M \models \phi$
$M \preceq_F M'$	$\forall \phi \in \text{ACTL}^*. M' \models_F \phi \implies M \models_F \phi$
$M \simeq M'$	$\forall \phi \in \text{ACTL}^*. M \models \phi \iff M' \models \phi$
$M \simeq_F M'$	$\forall \phi \in \text{ACTL}^*. M \models_F \phi \iff M' \models_F \phi$
$L(M) \subseteq L(M')$	$\forall \phi \in \text{LTL}. M' \models \phi \implies M \models \phi$
$L(M) = L(M')$	$\forall \phi \in \text{LTL}. M \models \phi \iff M' \models \phi$

Symetria – przykład



- $V = \{x_1, \dots, x_n\}$, $S = D^n$
- permutacja $\sigma : \{1 \dots n\} \rightarrow \{1 \dots n\}$ wyznacza permutację $\rho : D^n \rightarrow D^n$:

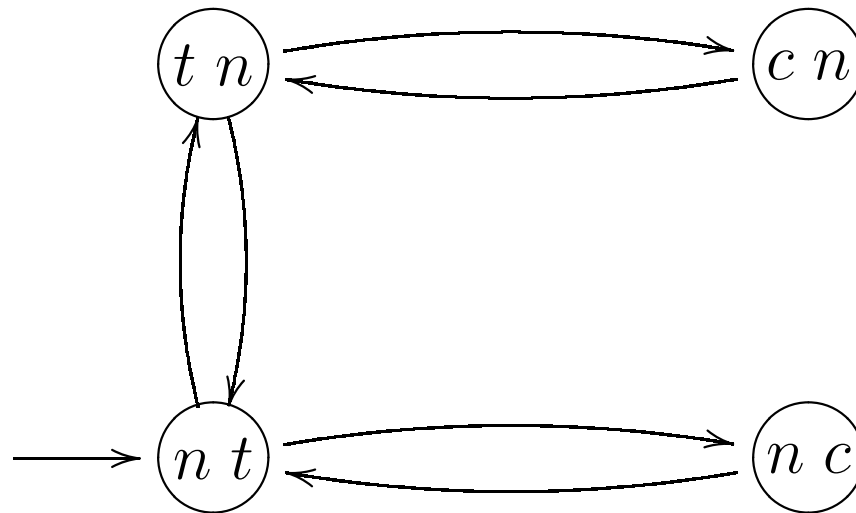
$$\rho(d_1, \dots, d_n) = (d_{\sigma(1)}, \dots, d_{\sigma(n)})$$

- grupa permutacji na $\{1 \dots n\}$ (**strukturze M**) wyznacza grupę permutacji G na D^n (**przestrzeni stanów M**)

Przykład: $D = \{n, t, c\}$

na $\{1, 2, \dots, n\}$: grupa generowana przez $\sigma = (1\ 2 \dots n)$

na D^n : grupa G generowana przez $\rho : \langle d_1 \dots d_n \rangle \mapsto \langle d_2 \dots d_n d_1 \rangle$

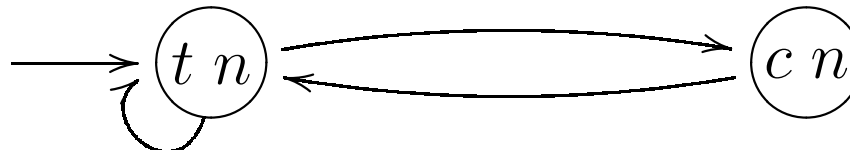


- G – grupa symetrii (automorfizmów) $\rho : D^n \rightarrow D^n$

$$R(\vec{d}, \vec{d}') \implies R(\rho(\vec{d}), \rho(\vec{d}'))$$

- orbita $\theta_G(\vec{d}) = \{\vec{d}' \mid \exists \rho \in G. \rho(\vec{d}) = \vec{d}'\}$
- model ilorazowy M / \approx_G

$$\vec{d} \approx_G \vec{d}' \iff \vec{d} \in \theta_G(\vec{d}')$$



$$\phi \equiv (c_1 \implies \neg c_2) \wedge (c_2 \implies \neg c_1)$$

jest **niezmiennicza** względem G :

$$\vec{d} \models \phi, \rho \in G \implies \rho(\vec{d}) \models \phi$$

Tw.: $M \models \phi \iff M / \approx_G \models \phi,$

o ile ϕ jest niezmiennicza względem G

Tw.: $M \sim M / \approx_G,$

o ile wszystkie $p \in P$ są niezmiennicze względem G

Typowe przypadki:

Pierścień:

grupa generowana przez $\sigma = (1\ 2 \dots n)$

Brak struktury:

grupa wszystkich permutacji

obliczamy \approx_D jako najmniejszy punkt stały:

$$\vec{x} \approx_D \vec{z} \equiv \vec{x} = \vec{z} \vee \exists \vec{y}. \vec{x} \approx_D \vec{y} \wedge \bigvee_i \vec{z} = g_i(\vec{y})$$

$\xi(\vec{d})$ – representant klasy abs. $[\vec{d}]$

obliczamy relację $\vec{y} = \xi(\vec{x})$

$$R_G(\vec{y}, \vec{y}') \equiv \exists \vec{x}, \vec{x}'. R(\vec{x}, \vec{x}') \wedge \vec{y} = \xi(\vec{x}) \wedge \vec{y}' = \xi(\vec{x}')$$