

Specyfikowanie i weryfikowanie

Programy współbieżne

Marek A. Bednarczyk, www.ipipan.gda.pl

Literatura — wiele prac dostępnych w Sieci

np.: <http://www.wikipedia.org/>

PJP — Prosty Język Procesów

Definicje rekursywne

$x = P(x)$ — rekursywna definicja

Składnia PJP

$P ::= 0$	pusty proces
$a.P$	akcja
$P + P$	niedeterministyczny wybór
$P \parallel P$	złożenie równoległe
x	odwołanie do rekursywnej definicji

Przykłady

$0 + 0$ suma dwóch pustych procesów

$a.b.a.0$ wykonaj a, potem b, potem c i skończ

$x = a.x$ wykonuj a nieskończenie wiele razy

$x = a.x \parallel b.x$ generuj współbieżne kopie x

Semantyka operacyjna PJP

Proces **P** może przekształcić się w proces **Q** poprzez wykonanie akcji **a**, notacja

$$P \xrightarrow{a} Q$$

jeśli takie stwierdzenie da się wywieść z podanych dalej reguł

Semantyka operacyjna PJP

$$\frac{}{a.P \xrightarrow{a} P}$$

wykonanie akcji

$$\frac{P \xrightarrow{a} R}{P+Q \xrightarrow{a} R}$$

niedeterministyczny
wybór lewego procesu

$$\frac{Q \xrightarrow{a} R}{P+Q \xrightarrow{a} R}$$

niedeterministyczny
wybór prawego procesu

Semantyka operacyjna PJP (cd)

$$\frac{P \xrightarrow{a} R}{P \parallel Q \xrightarrow{a} R \parallel Q}$$

wybór lewego procesu

$$\frac{Q \xrightarrow{a} R}{P \parallel Q \xrightarrow{a} P \parallel R}$$

wybór prawego procesu

$$\frac{x=P \quad P \xrightarrow{a} Q}{x \xrightarrow{a} Q}$$

odwołanie do definicji

Konsekwencje semantyki operacyjnej

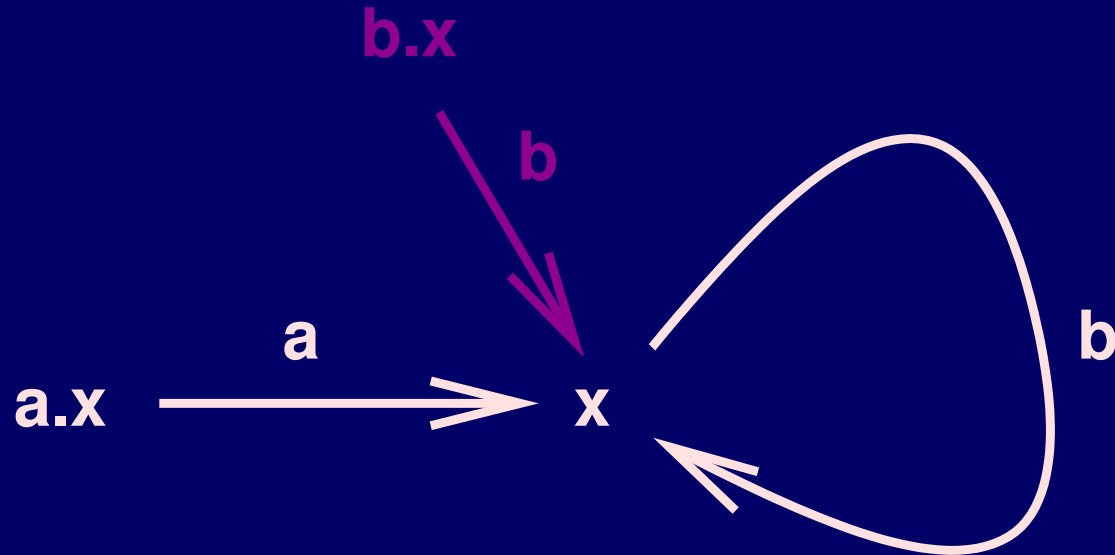
Proces 0 nie może wykonać żadnej akcji: $0 \xrightarrow{a} P$ nie da się wywieść! Podobnie **zablokowane** są procesy: $0+0$, $0 \parallel 0$,

Proces $a.P$ może wykonać tylko jedną akcję: $a.P \xrightarrow{a} P$

Ogólnie, każdy proces P może wykonać skończoną liczbę akcji, to znaczy istnieje skończenie wiele Q oraz a takich, że $P \xrightarrow{a} Q$.

Graf przejść: $a.x$ dla $x = b.x$

$$\frac{}{a.x \xrightarrow{a} x}$$



$$\frac{x = b.x \quad \frac{}{b.x \xrightarrow{b} x}}{x \xrightarrow{b} x}$$

Od procesów do grafów przejść

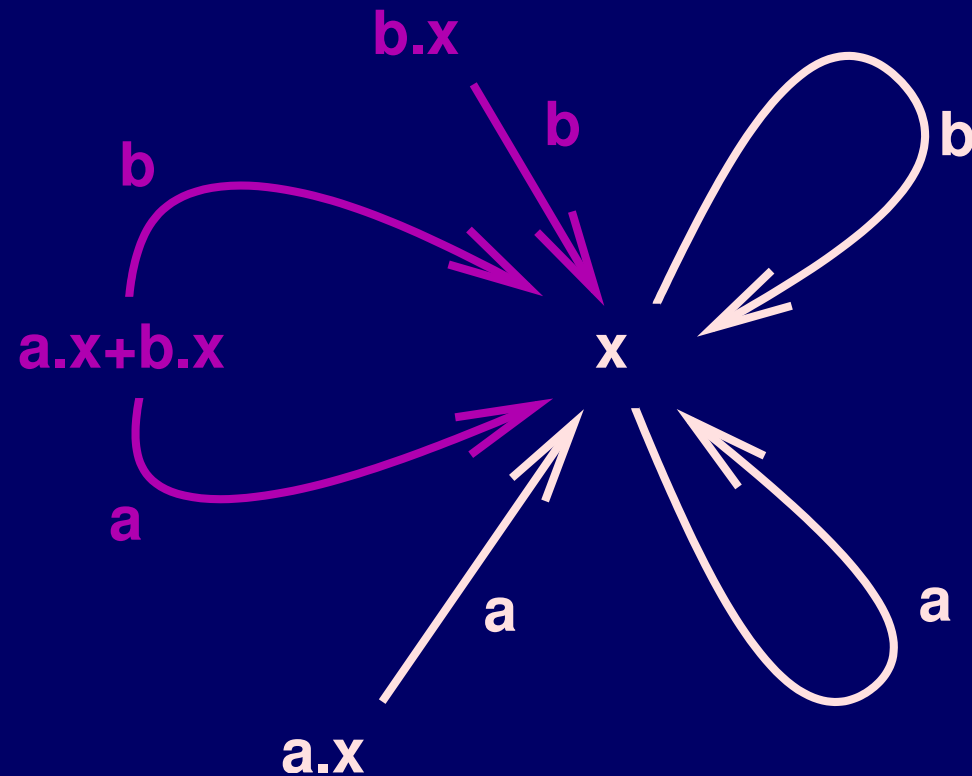
Stany = procesy

Relacja przejścia etykietowana akcjami

$P \xrightarrow{a} Q$ jeśli da się takie stwierdzenie wywieść z reguł semantyki operacyjnej

Graf przejść: $a.x$ dla $x = a.x + b.x$

Graf przejść: $a.x$ dla $x = a.x + b.x$



Graf przejść: $b.x$ dla $x = a.y + a.x$ oraz $y = b.x$

Proces $b.x$ gdzie

$$x = a.y + a.x$$

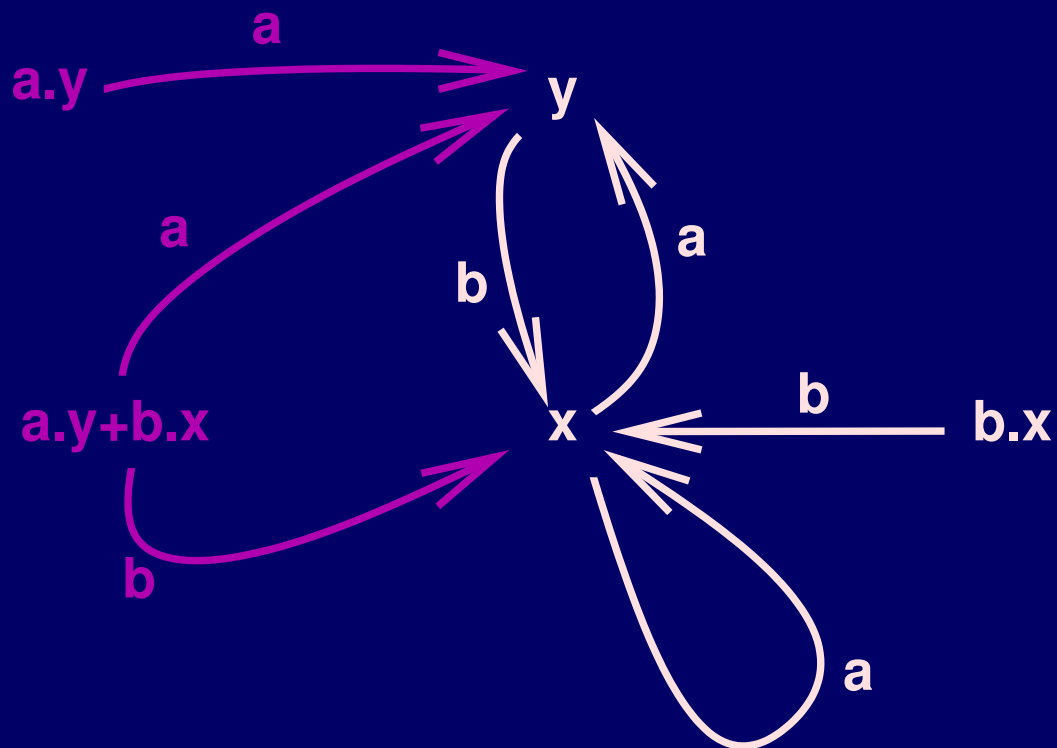
$$y = b.x$$

Graf przejść: $b.x$ dla $x = a.y + a.x$ oraz $y = b.x$

Proces $b.x$ gdzie

$$x = a.y + a.x$$

$$y = b.x$$



Graf przejść: $a.x$ dla $x = a.0 + a.b.x$

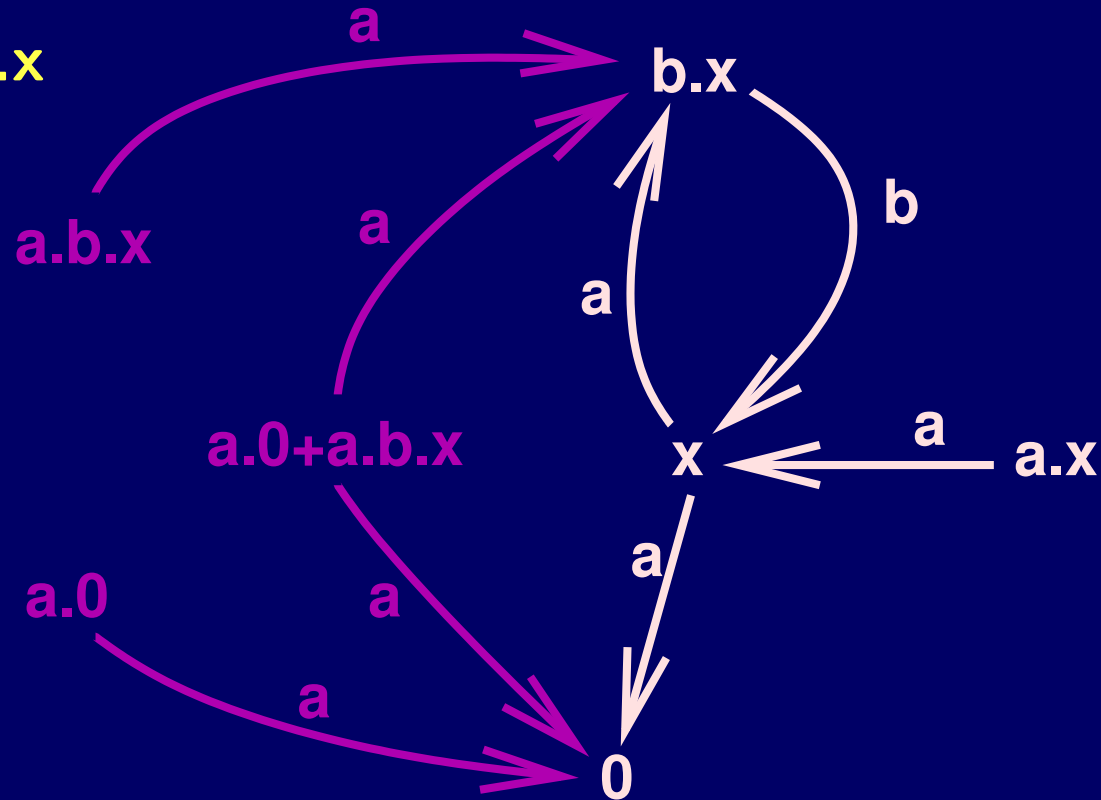
Proces $a.x$ gdzie

$$x = a.0 + a.b.x$$

Graf przejść: $a.x$ dla $x = a.0 + a.b.x$

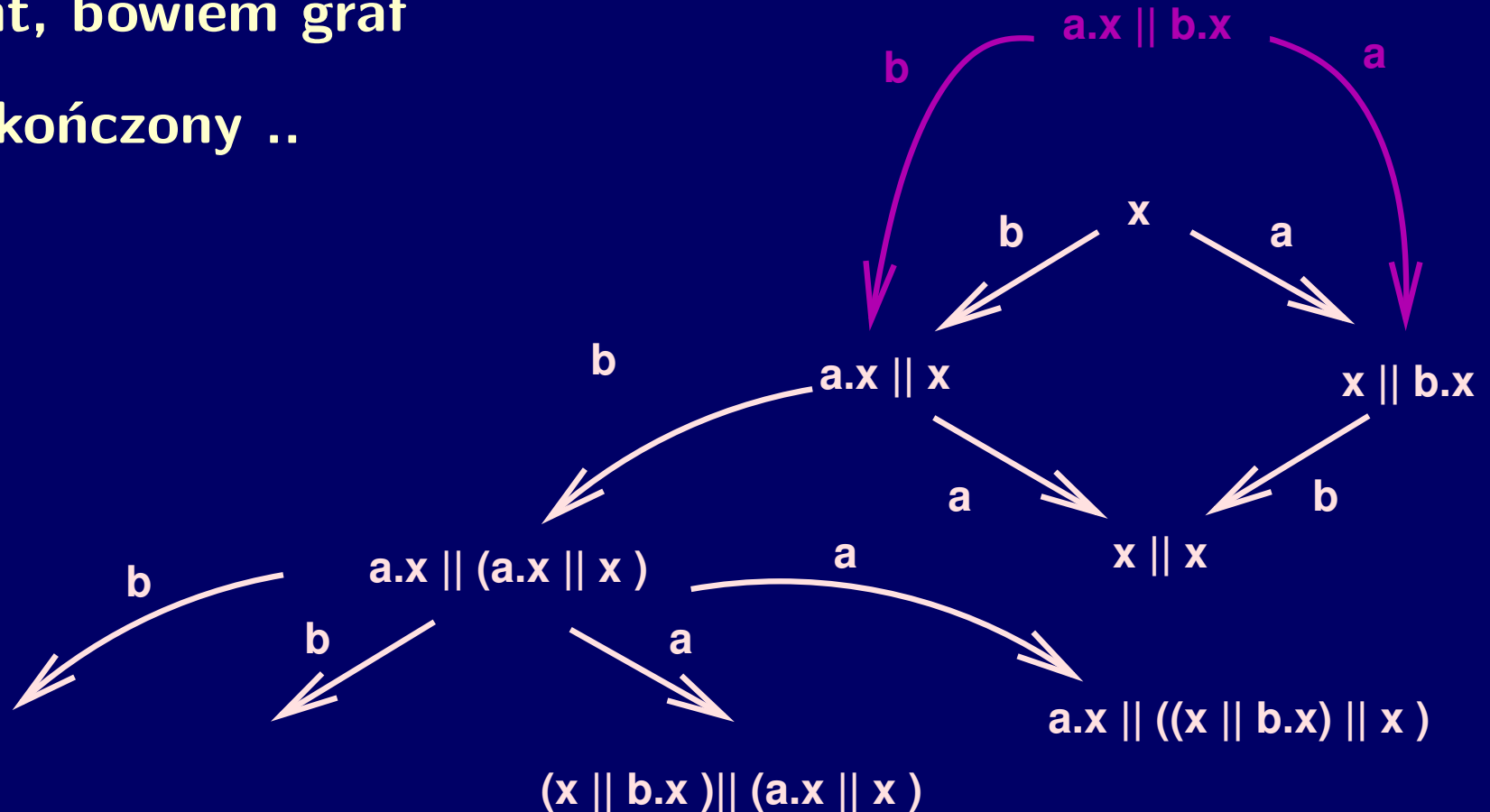
Proces $a.x$ gdzie

$$x = a.0 + a.b.x$$



Graf przejść: $x = a.x \parallel b.x$

Fragment, bowiem graf
jest nieskończony ..



Interesujące własności procesów

Wykluczanie — współbieżne procesy mają wyłączenie na działanie w sekcji krytycznej

Deadlock = blokada = zakleszczenie — stan, w którym proces nie może wykonywać żadnych akcji

Zagłazanie — jeden z procesów jest pozbawiony przez inne dostępu do zasobów

Jak wyrazić takie własności ???

(Wielo-)modalna logika Hennessy-Milner

 $\Phi ::= \mathbf{tt}$ prawda $\Phi \wedge \Psi$ koniunkcja $\neg\Phi$ negacja $\langle a \rangle \Phi$ można wykonać a by osiągnąć Φ $[a]\Phi$ każde wykonanie a prowadzi do Φ fałsz: $\mathbf{ff} \equiv \neg\mathbf{tt}$ dyzjunkcja: $\Phi \vee \Psi \equiv \neg(\neg\Phi \wedge \neg\Psi)$

Semantyka HML

Proces P spełnia formułę Φ : $P \models \Phi$

$P \models \mathbf{tt}$ zawsze

$P \models \Phi \wedge \Psi$ jeśli $P \models \Phi$ oraz $P \models \Psi$

$P \models \neg\Phi$ jeśli $P \not\models \Phi$

$P \models \langle \mathbf{a} \rangle \Phi$ jeśli $P \xrightarrow{\mathbf{a}} Q$ i $Q \models \Phi$

dla pewnego Q

$P \models [\mathbf{a}] \Phi$ jeśli $P \xrightarrow{\mathbf{a}} Q$ implikuje $Q \models \Phi$

dla każdego Q

Przykłady

$P \models \langle a \rangle \mathbf{tt}$ proces P **może** wykonać akcję a

$P \models \langle a \rangle \mathbf{ff}$ równoważne **ff**

$P \models \langle a \rangle \langle b \rangle \mathbf{tt}$

proces P może wykonać akcje a, **poczym** b

$P \models \langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}$

proces P może wykonać akcję a **lub** akcję b

$P \models \langle a \rangle \mathbf{tt} \wedge \langle b \rangle \mathbf{tt}$

proces P może wykonać akcję a **oraz** akcję b

Przykłady (cd)

$P \models [a] \text{ff}$ proces P **nie może** wykonać akcji a

$P \models [a] \text{tt}$ równoważne **tt**

$P \models [a] \langle b \rangle \text{tt}$ zachodzi zawsze, jeśli $P \models [a] \text{ff}$
po każdej akcji a proces P gotów wykonać b

$P \models [a] \text{ff} \vee \langle b \rangle \text{tt}$

P nie może wykonać a lub może akcją b

$P \models [a] \text{ff} \wedge \langle b \rangle \text{tt}$

P może wykonać akcją b oraz nie może a

Przykłady (cd)

Notacja: $[-]\Phi \equiv \bigwedge_{a \in A} [a]\Phi$ $\langle - \rangle \Phi \equiv \bigvee_{a \in A} \langle a \rangle \Phi$

$P \models [-] \text{ff}$

proces P **nie może** wykonać **żadnej** akcji

proces P jest **zablokowany!!!**

$P \models \langle - \rangle \text{tt}$

proces P **może** wykonać **jakąś** akcję

proces P jest **żywy**

Graf przejść: $a.x$ dla $x = a.x + b.x$

$a.x \models \langle a \rangle tt$?

$a.x \models [a] ff$?

$a.x \models \langle a \rangle \langle b \rangle tt$?

$a.x \models \langle a \rangle [b] ff$?

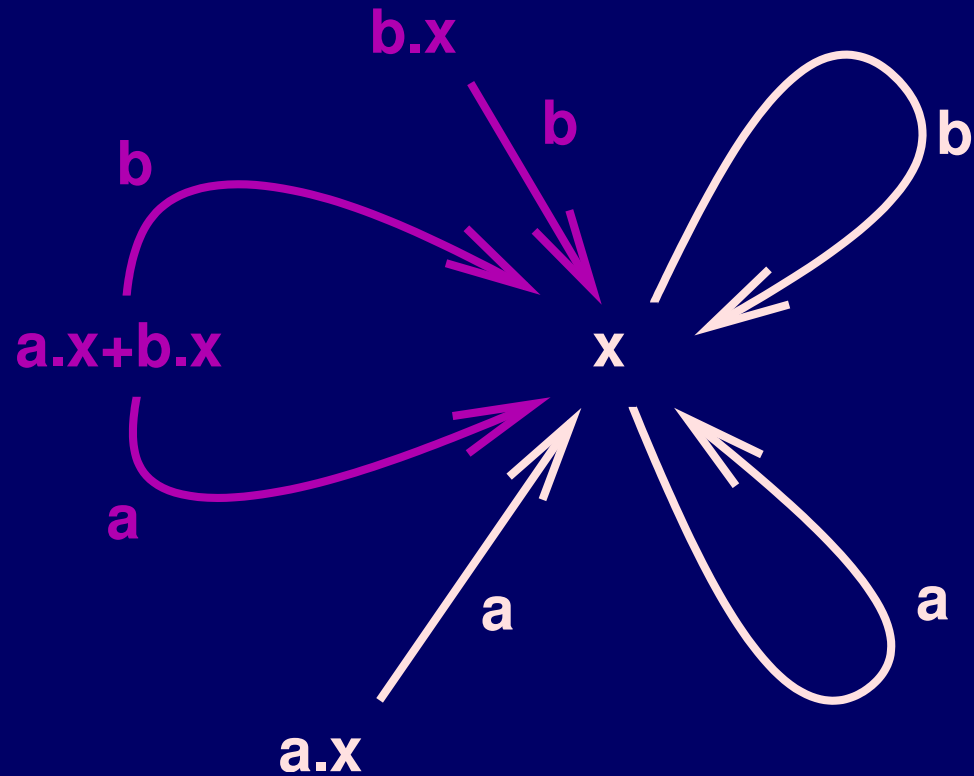
$a.x \models [a] \langle b \rangle tt$?

$a.x \models [a] ff \vee \langle b \rangle tt$?

$a.x \models [a] ff \wedge \langle b \rangle tt$?

$x \models [a] [-] ff$?

$x \models [a] \langle - \rangle tt$?



Graf przejść: $a.x$ dla $x = a.x + b.x$

$a.x \models \langle a \rangle tt$ ✓

$a.x \models [a] ff$ -

$a.x \models \langle a \rangle \langle b \rangle tt$ ✓

$a.x \models \langle a \rangle [b] ff$ -

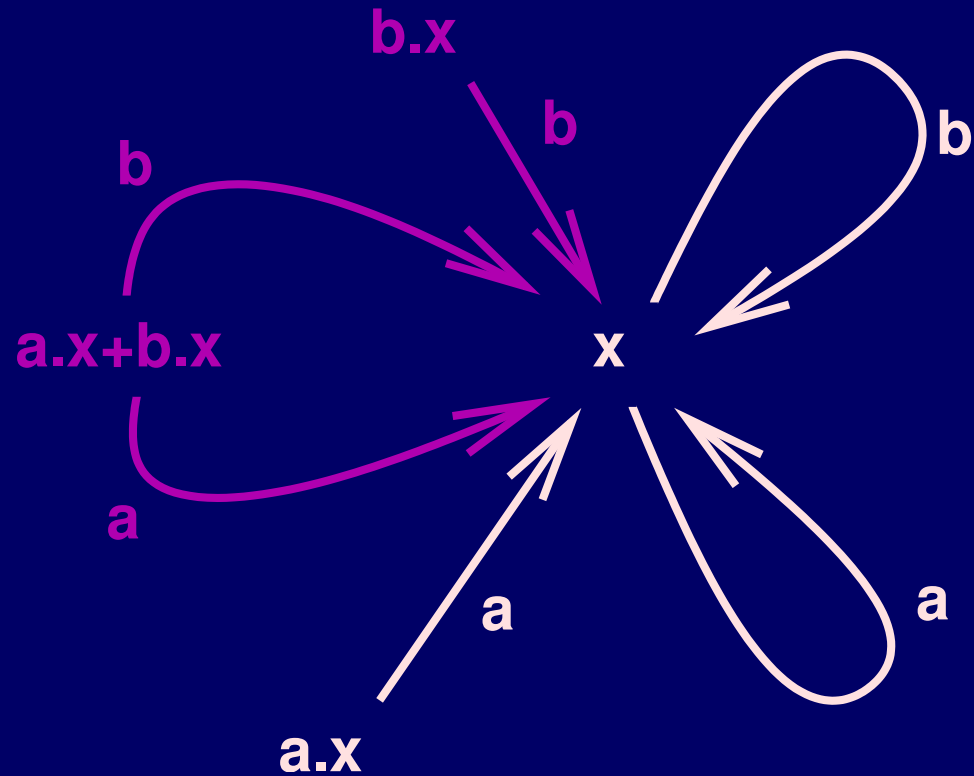
$a.x \models [a] \langle b \rangle tt$ ✓

$a.x \models [a] ff \vee \langle b \rangle tt$ ✓

$a.x \models [a] ff \wedge \langle b \rangle tt$ -

$x \models [a] [-] ff$ -

$x \models [a] \langle - \rangle tt$ ✓



Graf przejść: $b.x$ dla $x = a.y + b.x$ i $y = a.x$

$b.x \models \langle a \rangle tt$?

$b.x \models [a] ff$?

$b.x \models \langle a \rangle \langle b \rangle tt$?

$b.x \models \langle a \rangle [b] ff$?

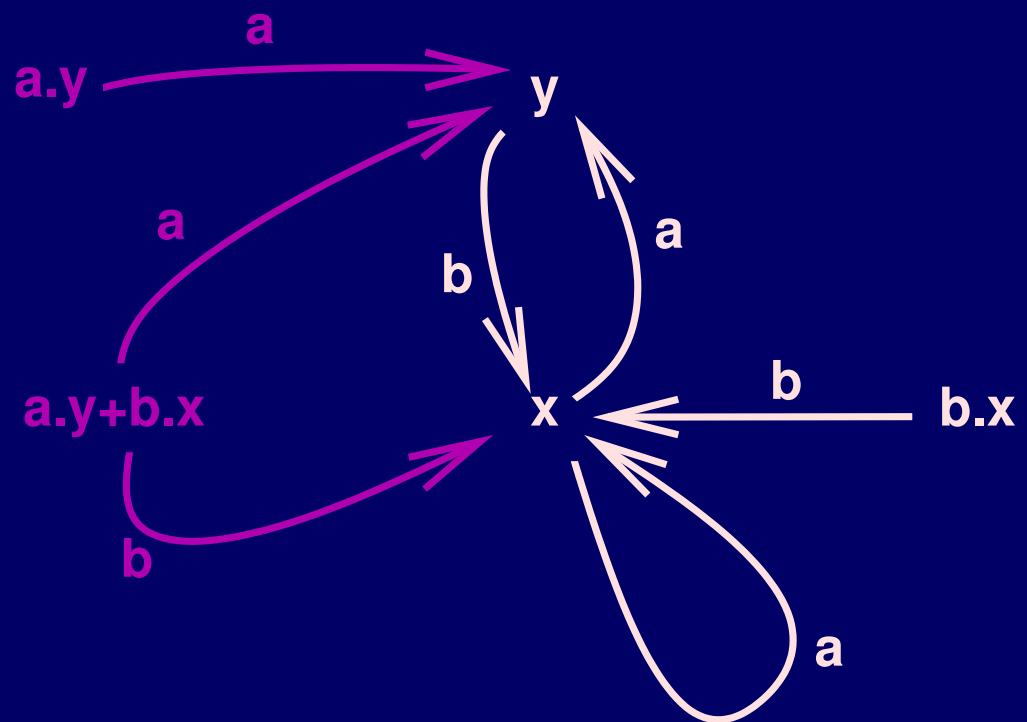
$b.x \models [a] \langle b \rangle tt$?

$b.x \models [a] ff \vee \langle b \rangle tt$?

$b.x \models [a] ff \wedge \langle b \rangle tt$?

$x \models [a] [-] ff$?

$x \models [a] \langle - \rangle tt$?



Graf przejść: $a.x$ dla $x = a.0 + a.b.x$

$a.x \models \langle a \rangle \mathbf{tt}$?

$a.x \models [a] \mathbf{ff}$?

$a.x \models \langle a \rangle \langle b \rangle \mathbf{tt}$?

$a.x \models \langle a \rangle [b] \mathbf{ff}$?

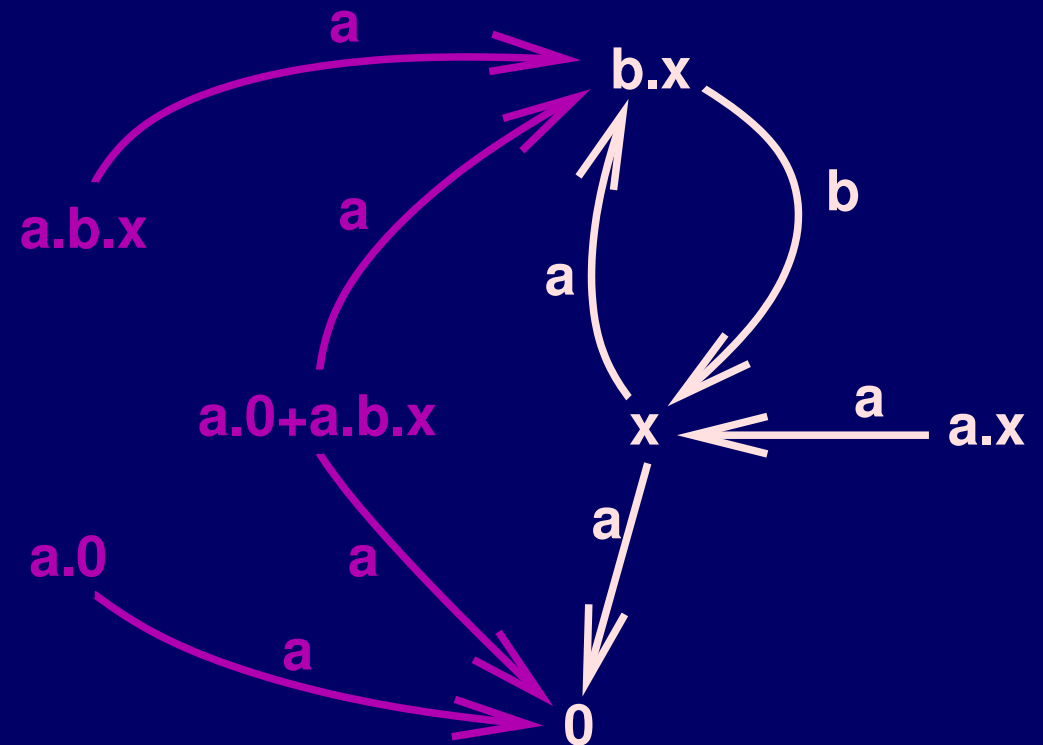
$a.x \models [a] \langle b \rangle \mathbf{tt}$?

$x \models [a][b] \mathbf{ff} \vee [a] \langle b \rangle \mathbf{tt}$?

$x \models \langle a \rangle [b] \mathbf{ff} \wedge [a] \langle b \rangle \mathbf{tt}$?

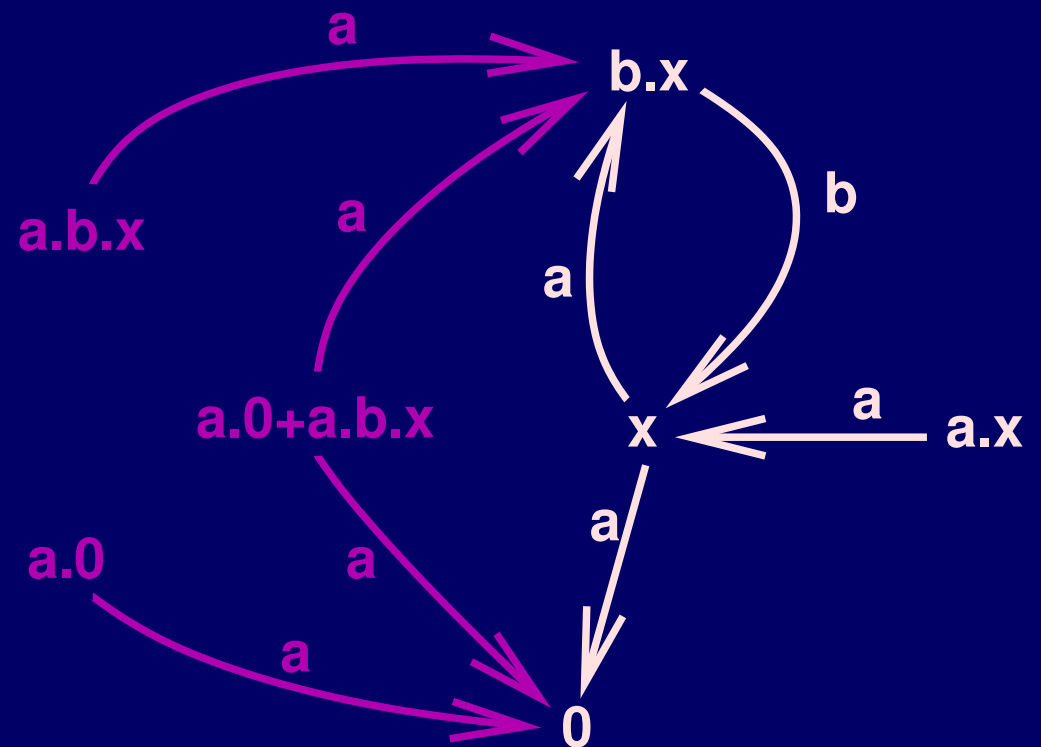
$x \models \langle a \rangle [-] \mathbf{ff}$?

$x \models [a] \langle - \rangle \mathbf{tt}$?



Graf przejść: $a.x$ dla $x = a.0 + a.b.x$

$a.x \models \langle a \rangle \mathbf{tt}$	✓
$a.x \models [a] \mathbf{ff}$	—
$a.x \models \langle a \rangle \langle b \rangle \mathbf{tt}$	—
$a.x \models \langle a \rangle [b] \mathbf{ff}$	✓
$a.x \models [a] \langle b \rangle \mathbf{tt}$	✓
$x \models [a][b] \mathbf{ff} \vee [a] \langle b \rangle \mathbf{tt}$	—
$x \models \langle a \rangle [b] \mathbf{ff} \wedge [a] \langle b \rangle \mathbf{tt}$	✓
$x \models \langle a \rangle [-] \mathbf{ff}$	✓
$x \models [a] \langle - \rangle \mathbf{tt}$	—



Przykłady (cd)

$P \models [-] \text{ff}$ **deadlock** (blokada)

proces P nie może wykonać **żadnej** akcji

$P \models \langle - \rangle \text{tt}$ P jest **żywy**

proces P może wykonać **jakąś** akcję

$P \models \langle - \rangle \text{tt} \wedge \bigwedge_{b \neq a} [b] \text{ff}$

???

$P \models \langle - \rangle \text{tt} \wedge [-] \Phi$

???

Przykłady (cd)

$P \models [-] \text{ff}$ **deadlock** (blokada)

proces P nie może wykonać **żadnej** akcji

$P \models \langle - \rangle \text{tt}$ P jest **żywy**

proces P może wykonać **jakąś** akcję

$P \models \langle - \rangle \text{tt} \wedge \bigwedge_{b \neq a} [b] \text{ff}$

proces P może wykonać **tylko** akcję a

$P \models \langle - \rangle \text{tt} \wedge [-] \Phi$

???

Przykłady (cd)

$P \models [-] \text{ff}$ **deadlock** (blokada)

proces P nie może wykonać **żadnej** akcji

$P \models \langle - \rangle \text{tt}$ P jest **żywy**

proces P może wykonać **jakaś** akcję

$P \models \langle - \rangle \text{tt} \wedge \wedge_{b \neq a} [b] \text{ff}$

proces P może wykonać **tylko** akcję a

$P \models \langle - \rangle \text{tt} \wedge [-] \Phi$

P jest żywy, a cokolwiek zrobi, znajdzie Φ

Negacja w logice HM jest zbędna

$$\neg \mathbf{ff} \equiv \mathbf{tt}$$

$$\neg \mathbf{tt} \equiv \mathbf{ff}$$

$$\neg(\Phi \wedge \Psi) \equiv (\neg\Phi) \vee (\neg\Psi)$$

$$\neg(\Phi \vee \Psi) \equiv (\neg\Phi) \wedge (\neg\Psi)$$

$$\neg \langle \mathbf{a} \rangle \Phi \equiv [\mathbf{a}] (\neg\Phi)$$

$$\neg [\mathbf{a}] \Phi \equiv \langle \mathbf{a} \rangle (\neg\Phi)$$

$$\neg \langle - \rangle \Phi \equiv [-] (\neg\Phi)$$

$$\neg [-] \Phi \equiv \langle - \rangle (\neg\Phi)$$

Prawdziwość, spełnialność, ...

Φ jest **spełnialna** jeśli $P \models \Phi$ dla pewnego procesu P

Φ jest **niespełnialna** jeśli $P \not\models \Phi$ dla żadnego procesu P

Φ jest **tautologią** jeśli $P \models \Phi$ dla każdego procesu P

Prawdziwość, spełnialność, ...

Φ jest spełnialna to $\neg\Phi$ jest niespełnialna ???

Φ jest niespełnialna to $\neg\Phi$ jest tautologią ???

Φ jest tautologią to Φ jest spełnialna ???

Φ jest tautologią to $\neg\Phi$ jest niespełnialna ???

Czy $[a]\Phi \vee [a]\neg\Phi$ jest tautologią?

Prawdziwość, spełnialność, ...

Φ jest spełnialna to $\neg\Phi$ jest niespełnialna ???

Φ jest niespełnialna to $\neg\Phi$ jest tautologią ???

Φ jest tautologią to Φ jest spełnialna ???

Φ jest tautologią to $\neg\Phi$ jest niespełnialna ???

Czy $[a]\Phi \vee [a]\neg\Phi$ jest tautologią?

Nie! $[a]\langle b \rangle \text{tt} \vee [a][b] \text{ff}$ nie jest tautologią!

Spełnialność

Dane:

– formuła Φ

Problem: Czy istnieje P , t.ż. $P \models \Phi$?

Twierdzenie

Problem spełnialności jest NP-zupełny

Model checking

Dane:

- proces P
- formuła Φ

Problem: Czy $P \models \Phi$?

Twierdzenie

Problem model checkingu jest **P**-zupełny

HML za mało ekspresywna!

Żaden z problemów:

- Czy ewolucja procesu P może **kiedyś** doprowadzić do deadlocku?
- Czy w **każdej** ewolucji procesu P mamy zapewnione wykluczanie?

nie daje się wyrazić w HML, bo każda formuła bada tylko skończony początek ewolucji.

Ścieżki

Ścieżka z P to ciąg procesów, (skończony lub nie),

$$\pi = P_0, P_1, \dots, P_n$$

taki, że $P = P_0$ oraz dla wszystkich i zachodzi

$$P_i \xrightarrow{a} P_{i+1} \text{ dla pewnego } a$$

Notacja: $\pi_i = P_i, P_{i+1}, \dots, P_n$

przebieg to ścieżka nieskończona, lub skończona kończąca się w zablokowanym procesie.

LTL — logika czasu liniowego

Logika Czasu Liniowego

$\Phi ::=$	p	zmienna zdaniowa
	tt	prawda
	$\Phi \wedge \Psi$	koniunkcja
	$\neg\Phi$	negacja
	$(-)\Phi$	w jednym kroku można osiągnąć Φ
	F Φ	proces może osiągnąć Φ
	G Φ	proces zawsze będzie spełniać Φ
	Φ U Ψ	proces spełni Ψ a do tego czasu będzie spełniał Φ

Semantyka LTL

Wartościowanie ρ — przypisuje każdej zmiennej zdaniowej p zbiór procesów $\rho(p)$ które ją spełniają.

$\pi, \rho \models \Phi$ **ścieżka** π **przy wartościowaniu** ρ **spełnia** Φ

$P, \rho \models \Phi$ **proces** P **przy wartościowaniu** ρ **spełnia** Φ

jeśli $\pi, \rho \models \Phi$ dla każdego przebiegu π z P , tzn. dla każdej maksymalnej (nieskończonej lub zablokowanej) ścieżki z P

Semantyka LTL (cd)

$\pi = P_0, P_1, \dots, P_n$ — ścieżka z P

ρ — wartościowanie

$\pi, \rho \models \mathbf{p}$ jeśli $P_0 \in \rho(\mathbf{p})$

$\pi, \rho \models \mathbf{tt}$ zawsze

$\pi, \rho \models \Phi \wedge \Psi$ jeśli $\pi \models \Phi$ oraz $\pi, \rho \models \Psi$

$\pi, \rho \models \neg\Phi$ jeśli $\pi \not\models \Phi$

Semantyka LTL (cd)

$\pi, \rho \models (-)\Phi$

jeśli $\pi_1, \rho \models \Phi$

$\pi, \rho \models \mathbf{F}\Phi$

jeśli $\pi_i, \rho \models \Phi$ **dla pewnego** i

$\pi, \rho \models \mathbf{G}\Phi$

jeśli $\pi_i, \rho \models \Phi$ **dla każdego** i

$\pi, \rho \models \Phi \mathbf{U} \Psi$

jeśli $\pi_i, \rho \models \Psi$ **dla pewnego** i

oraz $\pi_j, \rho \models \Phi$ **dla** $j = 0, \dots, i - 1$

Graf przejść: $b.x$ dla $x = a.0 + a.b.x$

Przebieg $\pi = x, b.x, x, bx, \dots$ $\pi' = x, b.x, x, 0$ $\pi'' = x, 0$

ρ — jak na rysunku

$b.x, \rho \models q \wedge p$?

$x, \rho \models q \wedge p$?

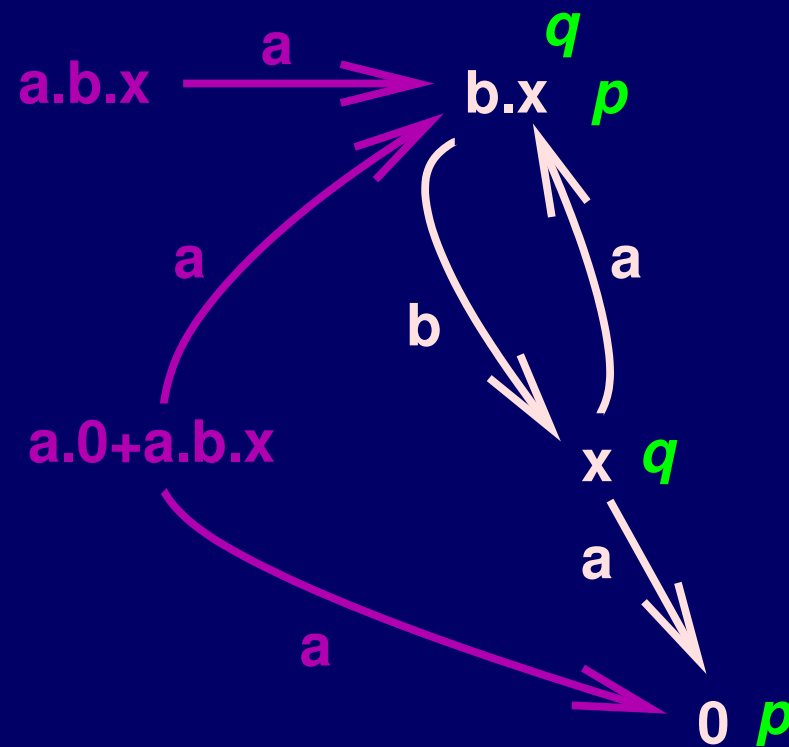
$\pi', \rho \models F(p \wedge q)$?

$\pi'', \rho \models F(p \wedge q)$?

$x, \rho \models F(p \wedge q)$?

$x, \rho \models F(p \Rightarrow q)$?

$x, \rho \models F(q \Rightarrow p)$?



Graf przejść: $b.x$ dla $x = a.0 + a.b.x$

Przebiegi: $\pi = x, b.x, x, bx, \dots$, $\pi' = x, b.x, x, 0$ $\pi'' = x, 0$

ρ — jak na rysunku

$b.x, \rho \models q \wedge p$ ✓

$x, \rho \models q \wedge p$ —

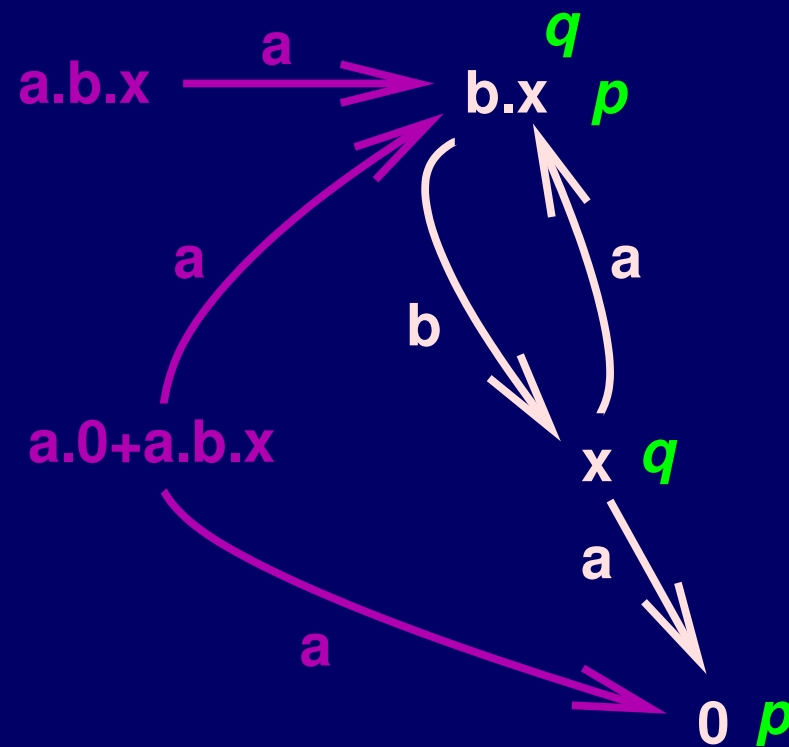
$\pi', \rho \models F(p \wedge q)$ ✓

$\pi'', \rho \models F(p \wedge q)$ —

$x, \rho \models F(p \wedge q)$ —

$x, \rho \models F(p \Rightarrow q)$ ✓

$x, \rho \models F(q \Rightarrow p)$ ✓



Graf przejść: $b.x$ dla $x = a.0 + a.b.x$

Przebieg $\pi = x, b.x, x, bx, \dots$ $\pi' = x, b.x, x, 0$ $\pi'' = x, 0$

ρ — jak na rysunku

$x, \rho \models G(p \vee q)$?

$\pi, \rho \models F(Fq \Rightarrow Gp)$?

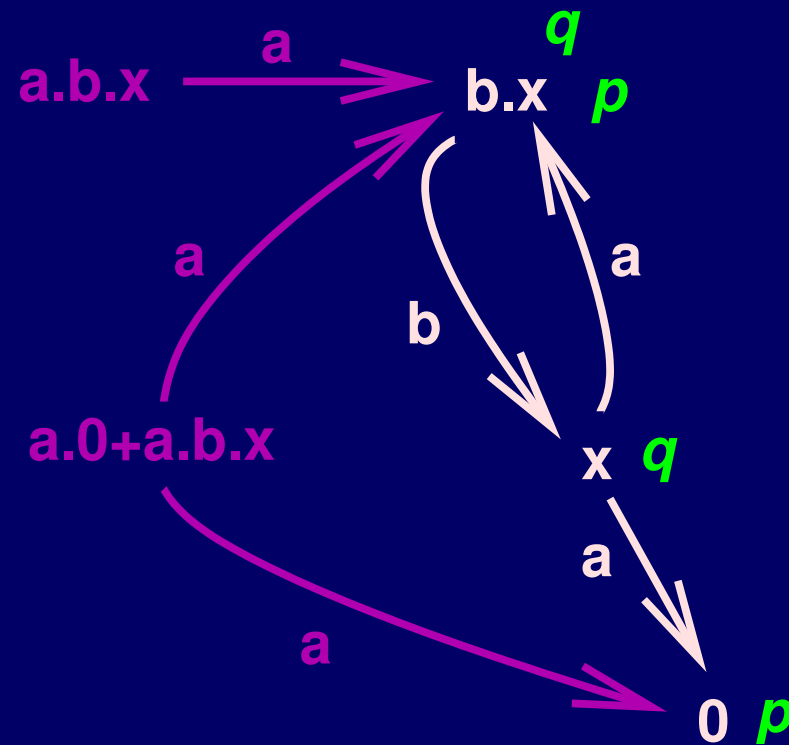
$\pi'', \rho \models F(Fq \Rightarrow Gp)$?

$x, \rho \models q \cup p$?

$x, \rho \models p \cup q$?

$\pi, \rho \models p \cup G(p \wedge q)$?

$\pi, \rho \models q \cup G(p \wedge q)$?



Graf przejść: $b.x$ dla $x = a.0 + a.b.x$

Przebieg $\pi = x, b.x, x, bx, \dots$ $\pi' = x, b.x, x, 0$ $\pi'' = x, 0$

ρ — jak na rysunku

$x, \rho \models G(p \vee q)$ ✓

$\pi, \rho \models F(Fq \Rightarrow Gp)$ -

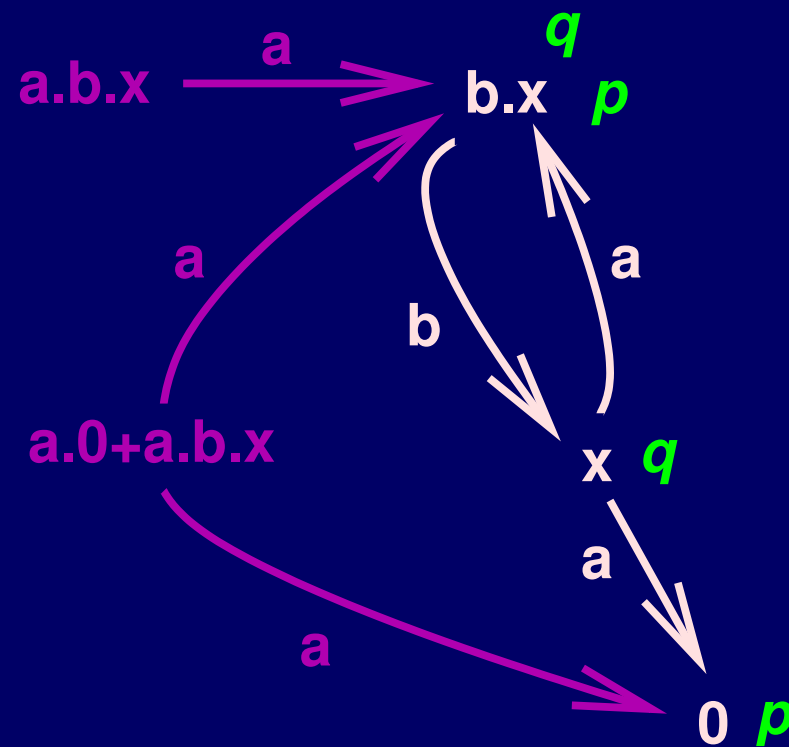
$\pi'', \rho \models F(Fq \Rightarrow Gp)$ ✓

$x, \rho \models q \cup p$ ✓

$x, \rho \models p \cup q$ ✓

$\pi, \rho \models p \cup G(p \wedge q)$ -

$\pi, \rho \models q \cup G(p \wedge q)$ ✓



Spełnialność

Dane:

– formuła Φ LTL

Problem: Czy istnieje P , t.ż. $P \models \Phi$?

Twierdzenie

Problem spełnialności jest **PSPACE**-zupełny

Model checking

Dane:

- proces P
- formuła Φ LTL

Problem: Czy $P \models \Phi$?

Twierdzenie

Problem model checkingu jest **PSPACE**-zupełny

CTL — logika czasu rozgałęzionego

Wracamy do HML i czasu rozgałęzionego

Dla każdego operatora temporalnego z LTL, np. dla **F**, rozważamy dwa warianty

- **AF** Φ dla **każdej** ścieżki **kiedyś** zajdzie Φ
- **EF** Φ dla **pewnej** ścieżki **kiedyś** zajdzie Φ

CTL — logika czasu rozgałęzionego

$\Phi ::=$	tt	prawda
	$\Phi \wedge \Psi$	koniunkcja
	$\neg\Phi$	negacja
	$\langle a \rangle \Phi$	w jakimś a-kroku można osiągnąć Φ
	$[a]\Phi$	każdy a-krok prowadzi do Φ
	$A \Phi \ U \ \Psi$	na każdej ścieżce kiedyś spełni się Ψ a do tego czasu zachodzić będzie Φ
	$E \Phi \ U \ \Psi$	na pewnej ścieżce kiedyś spełni się Ψ a do tego czasu zachodzić będzie Φ

CTL — logika czasu rozgałęzionego

$EF\Phi$ na pewnej ścieżce **kiedyś** spełni się Ψ

$AF\Phi$ na każdej ścieżce **kiedyś** spełni się Ψ

$EG\Phi$ na pewnej ścieżce **zawsze** zachodzi Ψ

$AG\Phi$ na każdej ścieżce **zawsze** zachodzi Ψ

Powyższe są definiowalne przez **Until**:

$$EF\Phi \equiv E(\mathbf{ttU}\Phi) \quad AF\Phi \equiv A(\mathbf{ttU}\Phi)$$

$$EG\Phi \equiv \neg EF\neg\Phi \quad AG\Phi \equiv \neg AF\neg\Phi$$

Semantyka CTL

Nowe klauzule

$P \models \mathbf{A} \Phi \mathbf{U} \Psi$

dla **każdej** ścieżki $P = P_0, P_1, \dots, P_n$

$P_i \models \Psi$ dla pewnego i

oraz $P_j \models \Phi$ dla $j = 0, \dots, i - 1$

$P \models \mathbf{E} \Phi \mathbf{U} \Psi$

istnieje ścieżka $P = P_0, P_1, \dots, P_n$

taka, że $P_i \models \Psi$ dla pewnego i

oraz $P_j \models \Phi$ dla $j = 0, \dots, i - 1$

Wyrażalne własności — Bezpieczeństwo : $AG\Phi$

zła własność $\neg\Phi$ na **żadnej** ścieżce **nigdy** nie zajdzie

Przykłady:

Wykluczanie: $AG([cs1]ff \vee [cs2]ff)$

System nigdy nie będzie gotów do jednoczesnego wykonania akcji cs1 oraz cs2 — gwarancja wyłączonego korzystania z zasobu przez procesy.

Brak deadlocku: $AG\langle-\rangle tt$

System nigdy nie dojdzie do stanu pełnego zablokowania

Wyrażalne własności — Żywotność : $AF\Phi$

dobra własność Φ na **każdej** ścieżce **kiedyś** zajdzie

Przykłady:

Gwarantowana reakcja systemu: $[req]AF(\langle serv \rangle tt)$

Na każde zgłoszenie żądania req proces kiedyś zareaguje akcją obsługi serv tegoż żądania

Wyrażalne własności

Słabe bezpieczeństwo $EG\Phi$

zła własność $\neg\Phi$ na pewnych ścieżkach nie zachodzi

Słaba żywotność $EF\Phi$

dobra własność Φ na pewnych ścieżkach **kiedyś** zajdzie

Graf przejść: $b.x$ dla $x = a.0 + a.b.x$

$x \models \mathbf{AF}(p \wedge q)$?

$x \models \mathbf{EF}(p \wedge q)$?

$x \models \mathbf{AG}(p \vee q)$?

$x \models \mathbf{EG}(p \vee q)$?

$x \models \mathbf{EF}[a]\langle b \rangle \mathbf{tt}$?

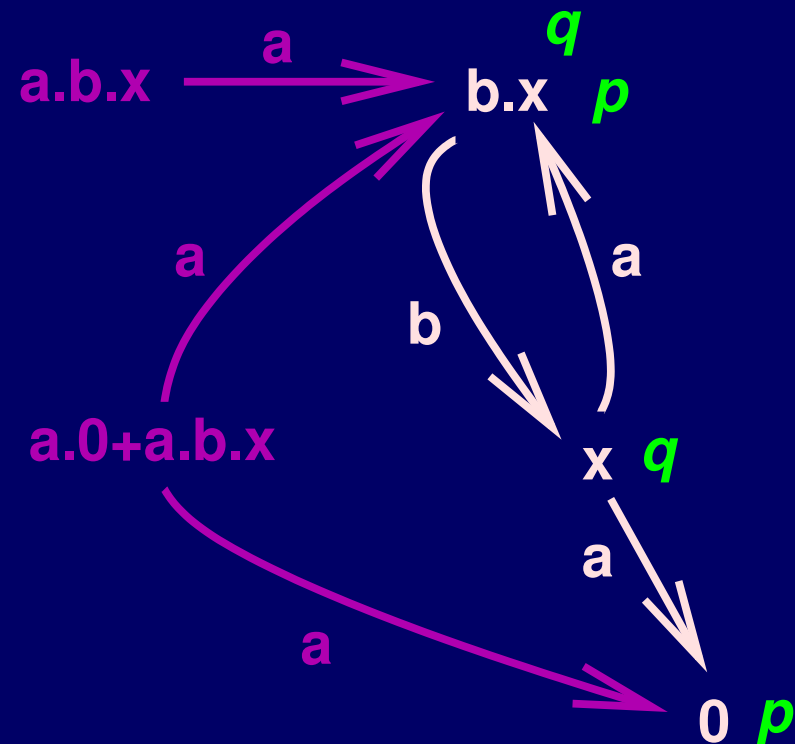
$x \models \mathbf{AF}[a]\langle b \rangle \mathbf{tt}$?

$x \models \mathbf{EG}[a]\langle b \rangle \mathbf{tt}$?

$x \models \mathbf{EG}(\langle a \rangle \mathbf{tt} \Rightarrow \langle a \rangle \langle b \rangle \mathbf{tt})$?

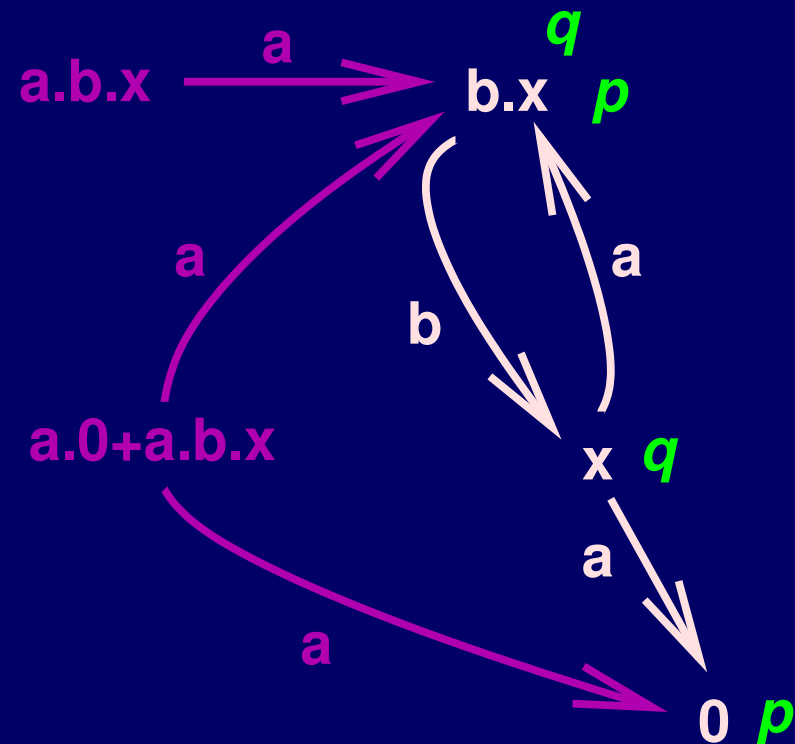
$x \models \mathbf{AG}(\langle a \rangle \mathbf{tt} \Rightarrow \langle a \rangle \langle b \rangle \mathbf{tt})$?

$x \models \mathbf{AG}(\langle b \rangle \mathbf{tt} \Rightarrow \langle b \rangle \langle a \rangle \mathbf{tt})$?



Graf przejść: $b.x$ dla $x = a.0 + a.b.x$

$x \models \mathbf{AF}(p \wedge q)$	—
$x \models \mathbf{EF}(p \wedge q)$	✓
$x \models \mathbf{AG}(p \vee q)$	✓
$x \models \mathbf{EG}(p \vee q)$	✓
$x \models \mathbf{EF}[a]\langle b \rangle \mathbf{tt}$	✓
$x \models \mathbf{AF}[a]\langle b \rangle \mathbf{tt}$	—
$x \models \mathbf{EG}[a]\langle b \rangle \mathbf{tt}$	✓
$x \models \mathbf{EG}(\langle a \rangle \mathbf{tt} \Rightarrow \langle a \rangle \langle b \rangle \mathbf{tt})$	✓
$x \models \mathbf{AG}(\langle a \rangle \mathbf{tt} \Rightarrow \langle a \rangle \langle b \rangle \mathbf{tt})$	—
$x \models \mathbf{AG}(\langle b \rangle \mathbf{tt} \Rightarrow \langle b \rangle \langle a \rangle \mathbf{tt})$	✓



Spełnialność CTL

Dane:

– formuła Φ CTL

Problem: Czy istnieje P , t.ż. $P \models \Phi$?

Twierdzenie

Problem spełnialności jest **EXPTIME**-zupełny

Model checking CTL

Dane:

- skończony proces P
- formuła Φ CTL

Problem: Czy $P \models \Phi$?

Twierdzenie

Problem model checkingu jest **P**-zupełny

CTL z LTL są nieporównywalne

- **EFAGp** tzn., na pewnej ścieżce kiedyś dojdziemy do sytuacji, gdy każda przyszła ewolucja zawsze gwarantować będzie **p**
Nie da się wyrazić równoważną formułą LTL
- **FGp** od pewnego momentu na każdej ścieżce gwarantowane jest **p**
Nie da się wyrazić równoważną formułą CTL

Zawiera CTL oraz LTL

Formuły **ścieżkowe** oraz **stanowe**

Kwantyfikatory **A** i **E** zastosowane do formuły
ścieżkowej dają formułę stanową.

Spełnialność CTL*

Dane:

– formuła Φ CTL*

Problem: Czy istnieje P , t.ż. $P \models \Phi$?

Twierdzenie

Problem spełnialności jest **2EXPTIME**-zupełny

Model checking CTL*

Dane:

- skończony proces P
- formuła Φ CTL*

Problem: Czy $P \models \Phi$?

Twierdzenie

Problem model checkingu jest **PSPACE**-zupełny