FAKULTA
INFORMATIKY
Masarykova univerzita

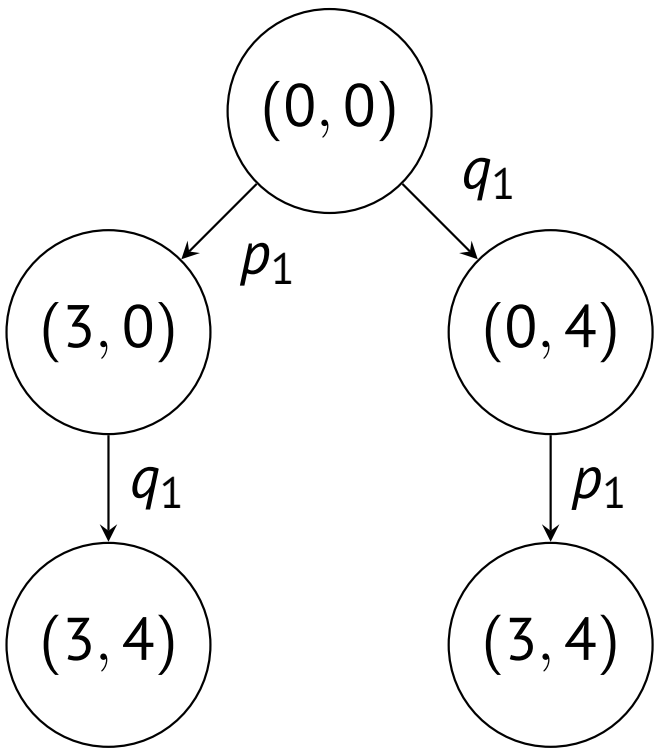
Context-Sensitive Dynamic Partial Order Reduction

Jan Tušil

26. března 2018

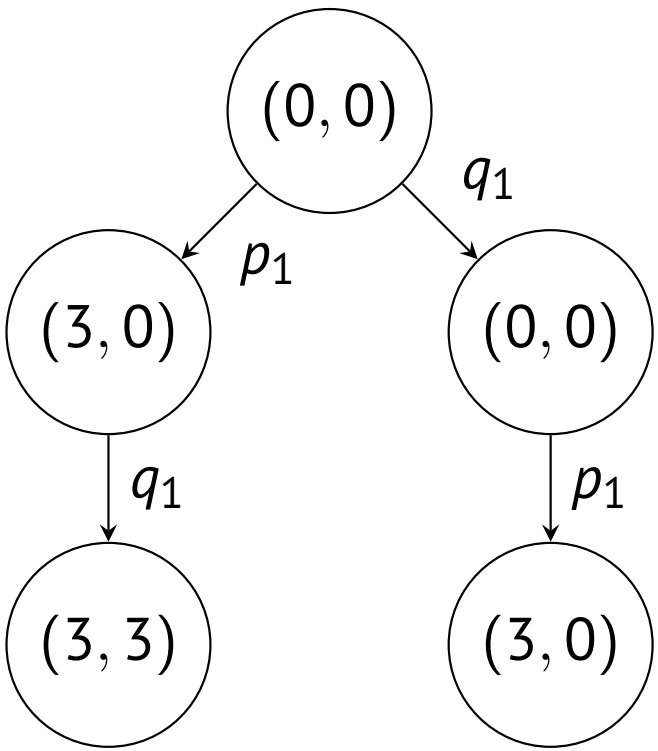
Example 1

```
p: x := 3      q: y := 4
```



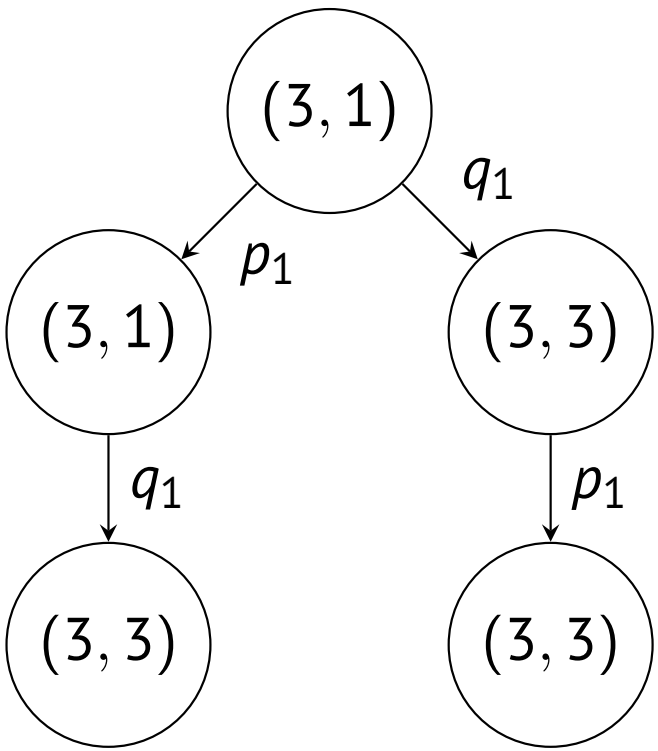
Example 2

```
p: x := 3      q: y := x
```



Example 3

```
p: x := 3      q: y := x
```



Happens-Before

Program

```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Happens-Before

Program

```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Konkrétní běh:

```
p1: write(x);
q1: read(y);
q2: read(x);
r1: read(z);
r2: read(x);
```

Happens-Before

Program

```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Konkrétní běh:

```
p1: write(x);
q1: read(y);
q2: read(x);
r1: read(z);
r2: read(x);
```

Happens-Before tohoto běhu:

Happens-Before

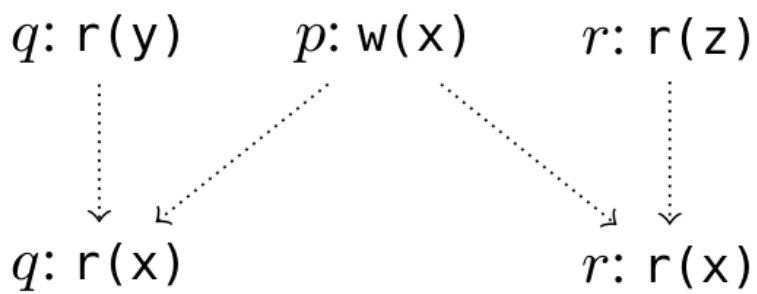
Program

```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Konkrétní běh:

```
p1: write(x);
q1: read(y);
q2: read(x);
r1: read(z);
r2: read(x);
```

Happens-Before tohoto běhu:



Happens-Before

Program

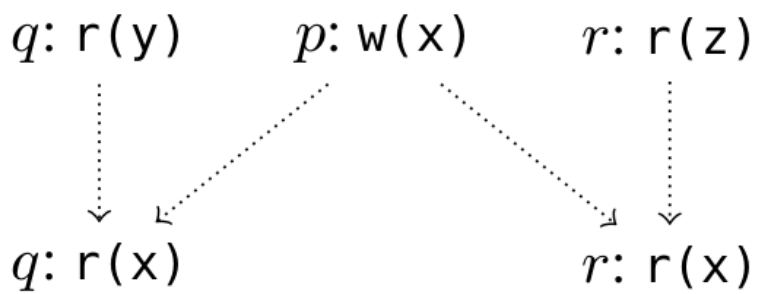
```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Jaké jsou jiné běhy se stejnou Happens-Before relací?

Konkrétní běh:

```
p1: write(x);
q1: read(y);
q2: read(x);
r1: read(z);
r2: read(x);
```

Happens-Before tohoto běhu:



Happens-Before

Program

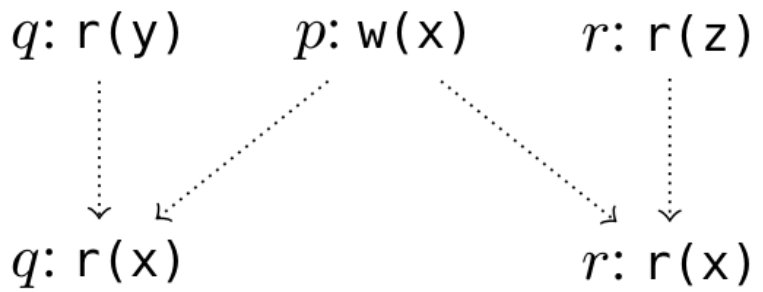
```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Jaké jsou jiné běhy se stejnou Happens-Before relací?
Není ale třeba je zkoumat.

Konkrétní běh:

```
p1: write(x);
q1: read(y);
q2: read(x);
r1: read(z);
r2: read(x);
```

Happens-Before tohoto běhu:



Notace

Notace

val Event $\leftarrow$ Process $\times\mathbb{N}$

Notace

val Event $\leftarrow$ Process $\times\mathbb{N}$
val s : State

Notace

val Event $\leftarrow$ Process $\times \mathbb{N}$
val s : State ▷ Iniciální stav

Notace

val Event $\leftarrow$ Process $\times \mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State

Notace

val Event $\leftarrow$ Process $\times\mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State ▷ Stav, do něhož doběhne stopa z s

Notace

val Event $\leftarrow$ Process $\times \mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State ▷ Stav, do něhož doběhne stopa z s
val enabled : State -> Set<Process>

Notace

val Event $\leftarrow$ Process $\times \mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State ▷ Stav, do něhož doběhne stopa z s
val enabled : State -> Set<Process>
var Sleep : Trace -> Set<Trace>

Notace

val Event $\leftarrow$ Process $\times\mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State ▷ Stav, do něhož doběhne stopa z s
val enabled : State -> Set<Process>
var Sleep : Trace -> Set<Trace> ▷ Navazující stopy jež netřeba řešit

Notace

val Event $\leftarrow$ Process $\times\mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State ▷ Stav, do něhož doběhne stopa z s
val enabled : State -> Set<Process>
var Sleep : Trace -> Set<Trace> ▷ Navazující stopy jež netřeba řešit
var backtrack : Trace -> Set<Process>

Notace

val Event $\leftarrow$ Process $\times\mathbb{N}$
val s : State ▷ Iniciální stav
val s[_] : Trace -> State ▷ Stav, do něhož doběhne stopa z s
val enabled : State -> Set<Process>
var Sleep : Trace -> Set<Trace> ▷ Navazující stopy jež netřeba řešit
var backtrack : Trace -> Set<Process>
val dom : Trace -> Set<Event>

Source DPOR (1)

function ExploreSource(E : Trace, $Sleep$: Set<Trace>)
    $sleep(E) \leftarrow Sleep$
    choose process $p \in enabled(s[e]) \setminus Sleep$ **or return**
    $backtrack(E) \leftarrow \{p\}$;
    while $\exists p \in backtrack(E) \setminus sleep(E)$ **do**
        DetectRacesSource(E, p)
        $Sleep' \leftarrow \{v \mid v \in sleep(E) \wedge E \vDash p \diamond v\}$
        Explore($E.p$, $Sleep'$)
        $sleep(E) \leftarrow sleep(E) \cup \{p\}$
    end while
end function

Source DPOR (2)

function DetectRacesSource(E : Trace, p: Process)
    val e_p : Event $\leftarrow$ $next_E(p)$
    for all $e \in dom(E)$ **such that** e is in reversible race with e_p **do**
        val $E' \leftarrow prefixBefore(E, e)$ ▷ does not include e
        val v : Trace $\leftarrow indepSuffixAfter(e, E).p$ ▷ does not include e
        if the first event of v is not in $backtrack(E')$ **then**
            add it there
        end if
    end for
end function

Source DPOR (2)

function DetectRacesSource(E : Trace, p: Process)
  val e_p : Event $\leftarrow$ $next_E(p)$
  for all $e \in dom(E)$ **such that** e is in reversible race with e_p **do**
    val $E' \leftarrow prefixBefore(E, e)$ ▷ does not include e
    val v : Trace $\leftarrow$ $indepSuffixAfter(e, E).p$ ▷ does not include e
    if $I_{E'}(v) \cap backtrack(E') \neq \emptyset$ **then**
      add some $q' \in I_{E'}(v)$ to $backtrack(E')$
    end if
  end for
end function

Výraz $I_{E'}(v)$ označuje procesy, které mají v posloupnosti v nějakou událost, která nenastává po (ve smyslu happens-before) žádné jiné události ve v.

Source DPOR - příklad

```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Source DPOR - příklad

```
p: write(x);
q: read(y); read(x);
r: read(z); read(x);
```

Na tabuli

Source DPOR není citlivé na kontext

```
p: write(x = 5);
q: write(x = 5);
r: read(x)
```

Source DPOR není citlivé na kontext

```
p: write(x = 5);
q: write(x = 5);
r: read(x)
```

Na tabuli

Context-Sensitive DPOR

function ExploreCS(E : Trace, $Sleep$: Set<Trace>)
    $sleep(E) \leftarrow Sleep$
    choose process $p \in enabled(s[e]) \setminus Sleep$ **or return**
    $backtrack(E) \leftarrow \{p\}$;
    while $\exists p \in backtrack(E) \setminus sleep(E)$ **do**
        DetectRaces(E, p)
        $Sleep' \leftarrow \{v \mid v \in sleep(E) \wedge E \vDash p \diamond v\}$
        $Sleep' \leftarrow Sleep' \cup \{v \mid p.v \in sleep(E)\}$
        Explore($E.p$, $Sleep'$)
        $sleep(E) \leftarrow sleep(E) \cup \{p\}$
    end while
end function

DetectRaces

function DetectRacesCS(E : Trace, p: Process)
    val e_p : Event $\leftarrow$ $next_E(p)$
    for all $e \in dom(E)$ **such that** e is in reversible race with e_p **do**
        val $E' \leftarrow prefixBefore(E, e)$ ▷ does not include e
        val v : Trace $\leftarrow indepSuffixAfter(e, E).p$ ▷ does not include e
        if the first event of v is not in $backtrack(E')$ **then**
            add it there
        end if
        suspendSomething(E, p, e, E', v)
    end for
end function

DetectRaces

function DetectRacesCS(E : Trace, p: Process)
  val e_p : Event $\leftarrow$ $next_E(p)$
  for all $e \in dom(E)$ **such that** e is in reversible race with e_p **do**
    val $E' \leftarrow prefixBefore(E, e)$ ▷ does not include e
    val v : Trace $\leftarrow$ $indepSuffixAfter(e, E).p$ ▷ does not include e
    if $I_{E'}(v) \cap backtrack(E') \neq \emptyset$ **then**
      add some $q' \in I_{E'}(v)$ to $backtrack(E')$
    end if
    suspendSomething(E, p, e, E', v)
  end for
end function

Výraz $I_{E'}(v)$ označuje procesy, které mají v posloupnosti v nějakou událost, která nenastává po (ve smyslu happens-before) žádné jiné události ve v.

suspendSomething

function suspendSomething(E, p, e : Event, E' : Trace, v : Trace)
    val $u \leftarrow depSuffixFrom(e, E)$

        if $s[E.p] = s[E'.v.u]$ **then** ▷ commutativity
            $sleep(E) \leftarrow sleep(E) \cup \{v.u\}$
        end if

end function

suspendSomething

function suspendSomething(E, p, e : Event, E' : Trace, v : Trace)
    val $u \leftarrow depSuffixFrom(e, E)$
    if $\nexists w \in sleep(E')$ **where** $w \leq v.u$ **then** ▷ redundancy check
        if $s[E.p] = s[E'.v.u]$ **then** ▷ commutativity
            $sleep(E) \leftarrow sleep(E) \cup \{v.u\}$
        end if
    end if
end function

Příklad

```
p: write(x = 5);
q: write(x = 5);
r: read(x)
```

Příklad

```
p: write(x = 5);
q: write(x = 5);
r: read(x)
```

Na tabuli

Proč to funguje

Proč to funguje

Definice

Mazurkiewiczova stopa je happened-before relace úplné výpočetní posloupnosti.

Proč to funguje

Definice

Mazurkiewiczova stopa je happened-before relace úplné výpočetní posloupnosti.

Tvrzení

Pro každou Mazurkiewiczovu stopu T, ExploreSourcePOR$(\epsilon, \emptyset)$ prozkoumá nějakou výpočetní sekvenci E, která stopu T implementuje.

Proč to funguje

Definice

Mazurkiewiczova stopa je happened-before relace úplné výpočetní posloupnosti.

Tvrzení

Pro každou Mazurkiewiczovu stopu T, ExploreSourcePOR$(\epsilon, \emptyset)$ prozkoumá nějakou výpočetní sekvenci E, která stopu T implementuje.

Tvrzení

Pro každou Mazurkiewiczovu stopu T, ExploreCS$(\epsilon, \emptyset)$ prozkoumá nějakou výpočetní sekvenci E, která buď implementuje stopu T, nebo dosáhne stejného stavu jako nějaká jiná sekvence E', která stopu T implementuje.