IA159 Formal Verification Methods

Partial Order Reduction

Jan Obdržálek
Jan Strejček

Department of Computer Science
Faculty of Informatics
Masaryk University

Focus and sources

Focus

- stuttering principle
- theory of partial order reduction
- heuristics for efficient implementation

Source

- Chapter 10 of *E. M. Clarke, O. Grumberg, and D. A. Peled: Model Checking, MIT, 1999.*

Basic facts on partial order reduction

- compatible with model checking of finite systems against LTL formulae without X operator
- size of the reduced system is 3–99% of the original size
- model checking process for reduced systems is faster and consumes less memory
- best suited for asynchronous systems
- also known as model checking using representatives

Modified definition of Kripke structure

We consider only deterministic systems.

A Kripke structure is a tuple $M = (S, T, S_0, L)$, where

- S is a finite set of states
- T is a set of transitions, each $\alpha \in T$ is a partial function $\alpha : S \to S$.
- $S_0 \subseteq S$ is a set of initial states
- $L : S \to 2^{AP}$ is a labelling function associating to each state $s \in S$ the set of atomic propositions that are true in s.

- a transition α is enabled in s if $\alpha(s)$ is defined
- α is disabled in s otherwise
- $enabled(s)$ denotes the set of transitions enabled in s

More definitions

Let φ be an LTL formula and $K = (S, T, S_0, L)$ be a Kripke structure.

- $AP(\varphi)$ is the set of atomic propositions occurring in φ
- a path in K starting from a state $s \in S$ is an infinite sequence $\pi = s_0, s_1, \ldots$ of states such that $s_0 = s$ and for each i there is a transition $\alpha_i \in T$ such that $\alpha_i(s_i) = s_{i+1}$
- a path starting in a fixed state can be identified with a sequence of transitions
- a path π satisfies φ, written $\pi \models \varphi$, if $w \models \varphi$, where the word $w = w(0)w(1)\ldots$ is defined as $w(i) = L(s_i) \cap AP(\varphi)$ for all $i \geq 0$
- K satisfies φ, written $K \models \varphi$, if all paths starting from initial states of K satisfy φ

Goal of partial order reduction

$\mathrm{LTL}_{-\mathsf{X}}$ denotes LTL formulae without X operator.

Goal

Given a finite Kripke structure K and an $\mathrm{LTL}_{-\mathsf{X}}$ formula φ, we want to find a smaller Kripke structure K' such that

$$K \models \varphi \iff K' \models \varphi.$$

Reduction method

- K' arises from K by disabling some transitions in some states
- as a result, some states may become unreachable in K'
- for each state s, *ample*(s) denotes the set of transitions that are enabled in s in K', $ample(s) \subseteq enabled(s)$
- calculation of ample sets needs to satisfy three goals
  1. K' given by ample sets has to satisfy
  $$K \models \varphi \iff K' \models \varphi$$
  2. K' should be substantially smaller than K
  3. the overhead in calculating ample sets must be small

A base of partial order reduction

Stuttering principle

Stuttering on words

- let $w = w(0)w(1)w(2)\dots$ be an infinite word
- a letter $w(i)$ is called redundant iff $w(i) = w(i+1)$ and there is $j > i$ such that $w(i) \neq w(j)$
- canonical form of w is the word obtained by deleting all redundant letters from w
- infinite words w_1, w_2 are stutter equivalent, written $w_1 \sim w_2$, iff they have the same canonical form

Example

- canonical form of $kk\,k\,oooo\,o\,m\,k\,k.n^\omega$ is $komk.n^\omega$
- canonical form of $k\,oo\,o\,mmmmm\,m\,kkk\,k.n^\omega$ is $komk.n^\omega$
- hence $kkkooooomkk.n^\omega \sim kooommmmmmkkkk.n^\omega$

Stuttering principle

Theorem (Lamport 1983)

Let φ be an $\mathrm{LTL}_{-\mathsf{X}}$ formula and w_1, w_2 be two stutter equivalent words. Then

$$w_1 \models \varphi \iff w_2 \models \varphi.$$

Stuttering on paths

Paths $\pi = s_0 s_1 \ldots$ and $\pi' = s'_0 s'_1 \ldots$ are stutter equivalent with respect to a set $AP' \subseteq AP$, written $\pi \sim_{AP'} \pi'$, iff $w \sim w'$, where w, w' are defined as $w(i) = L(s_i) \cap AP'$ and $w'(i) = L(s'_i) \cap AP'$ for each i.

Kripke structures K, K' are stutter equivalent with respect to AP', written $K \sim_{AP'} K'$, iff

- K and K' have the same set of initial states and
- for each path π of K starting in an initial state s there exists a path π' of K' starting in the same initial state such that $\pi \sim_{AP'} \pi'$ and vice versa.

Stuttering principle for Kripke structures

Corollary

Let φ be an $\mathrm{LTL}_{-\mathsf{X}}$ formula and K, K' be Kripke structures such that $K \sim_{AP(\varphi)} K'$. Then

$$K \models \varphi \iff K' \models \varphi.$$

Stuttering principle for Kripke structures

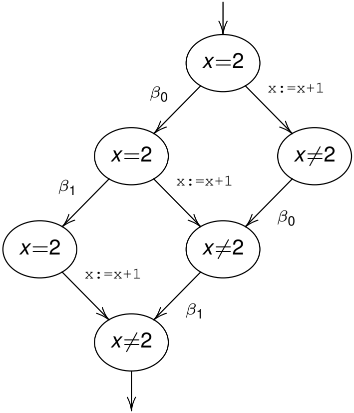
Corollary

Let φ *be an* $\mathrm{LTL}_{-\mathsf{X}}$ *formula and* K, K' *be Kripke structures such that* $K \sim_{AP(\varphi)} K'$. *Then*

$$K \models \varphi \iff K' \models \varphi.$$

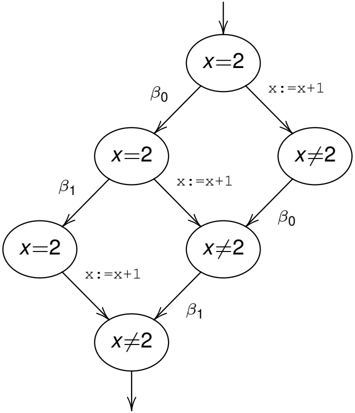
Hence, for every set of stutter equivalent paths (with respect to $AP(\varphi)$) of K it is sufficient to keep at least one representative of these paths in K'.

Example

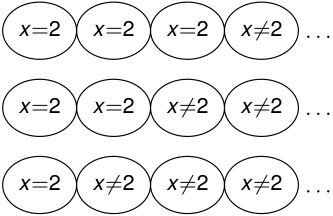


Let $AP(\varphi)$ contain just $x = 2$.

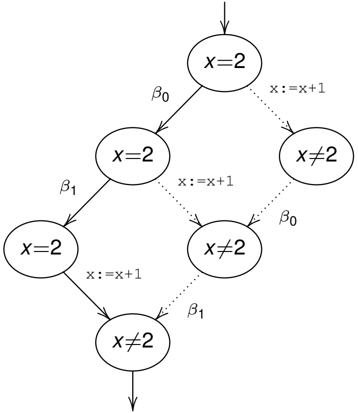
Example



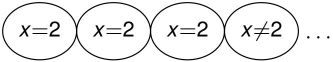
Let $AP(\varphi)$ contain just $x = 2$.



Example



Let $AP(\varphi)$ contain just $x = 2$.



Theory of partial order reduction

Conditions on ample sets

Terminology: (in)visibility and full expansion

A transition $\alpha \in T$ is invisible if for each pair of states $s, s' \in S$ such that $\alpha(s) = s'$ it holds that

$$L(s) \cap AP(\varphi) = L(s') \cap AP(\varphi).$$

A transition is visible if it is not invisible.

Terminology: (in)visibility and full expansion

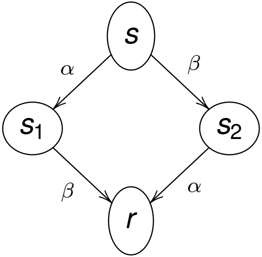
A transition $\alpha \in T$ is invisible if for each pair of states $s, s' \in S$ such that $\alpha(s) = s'$ it holds that

$$L(s) \cap AP(\varphi) = L(s') \cap AP(\varphi).$$

A transition is visible if it is not invisible.

A state s is fully expanded when $ample(s) = enabled(s)$.

Terminology: (in)dependence



An independence relation $I \subseteq T \times T$ is a symmetric and antireflexive relation satisfying the following two conditions for each state $s \in S$ and for each $(\alpha, \beta) \in I$:

1. enabledness: if $\alpha, \beta \in \mathit{enabled}(s)$ then $\alpha \in \mathit{enabled}(\beta(s))$
2. commutativity: if $\alpha, \beta \in \mathit{enabled}(s)$ then $\alpha(\beta(s)) = \beta(\alpha(s))$

The dependency relation D is the complement of I.

Condition C0

If all ample sets satisfy the following conditions C0, C1, C2, and C3, then $K' \sim_{AP(\varphi)} K$.

Condition C0

If all ample sets satisfy the following conditions C0, C1, C2, and C3, then $K' \sim_{AP(\varphi)} K$.

C0

$$\mathit{ample}(s) = \emptyset \iff \mathit{enabled}(s) = \emptyset.$$

Condition C1

C1

Along every path in the original structure that starts in s, the following condition holds: a transition that is dependent on a transition in $\mathit{ample}(s)$ cannot be executed without a transition in $\mathit{ample}(s)$ occurring first.

Condition C1

C1

Along every path in the original structure that starts in s, the following condition holds: a transition that is dependent on a transition in $\mathit{ample}(s)$ cannot be executed without a transition in $\mathit{ample}(s)$ occurring first.

Lemma

If C1 holds, then the transitions in $\mathit{enabled}(s) \setminus \mathit{ample}(s)$ *are all independent of those in* $\mathit{ample}(s)$*.*

Condition C1

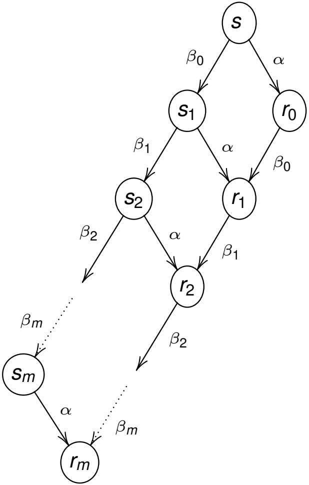
C1

Along every path in the original structure that starts in *s*, the following condition holds: a transition that is dependent on a transition in *ample*(*s*) cannot be executed without a transition in *ample*(*s*) occurring first.

Thanks to C1, all paths of K starting in a state s and not included in K' have one of the following two forms:

- the path has a prefix $\beta_0\beta_1 \ldots \beta_m\alpha$, where $\alpha \in$ *ample*(*s*) and each β_i is independent of all transitions in *ample*(*s*) including α.
- the path is an infinite sequence of transitions $\beta_0\beta_1 \ldots$ where each β_i is independent of all transitions in *ample*(*s*).

Condition C1: consequences



Due to C1, after execution of a sequence $\beta_0\beta_1\ldots\beta_m$ of a transitions not in *ample*(s) from s, all the transitions in *ample*(s) remain enabled. Further, the sequence $\beta_0\beta_1\ldots\beta_m\alpha$ executed from s leads to the same state as the sequence $\alpha\beta_0\beta_1\ldots\beta_m$.

As the sequence $\beta_0\beta_1\ldots\beta_m\alpha$ is not included in the reduced system, we want $\beta_0\beta_1\ldots\beta_m\alpha$ and $\alpha\beta_0\beta_1\ldots\beta_m$ to be prefixes of stutter equivalent paths. This is guaranteed if α is invisible.

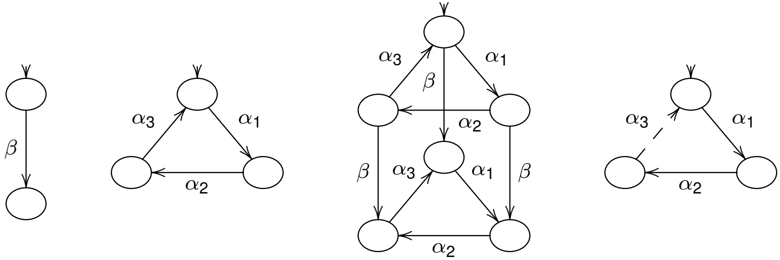
Condition C2

C2 (invisibility)

If s is not fully expanded, then every $\alpha \in$ *ample*(*s*) is invisible.

Condition C3: motivation

Conditions C0, C1, and C2 are not yet sufficient to guarantee that K' is stutter equivalent to K. There is a possibility that some transition will be delayed forever because of a cycle.



β is visible, $\alpha_1, \alpha_2, \alpha_3$ are invisible, β is independent of $\alpha_1, \alpha_2, \alpha_3$, and $\alpha_1, \alpha_2, \alpha_3$ are interdependent

Condition C3

C3 (cycle condition)

A cycle in reduced structure is not allowed if it contains a state in which some transition is enabled, but is never included in *ample*(s) for any state s on the cycle.

Calculating ample sets

Complexity of checking conditions C0–C3

Conditions C0 and C2

C0

$ample(s) = \emptyset \iff enabled(s) = \emptyset$.

C2 (invisibility)

If s is not fully expanded, then every $\alpha \in ample(s)$ is invisible.

- conditions C0 and C2 are local: their validity depends just on *enabled*(s) and *ample*(s), not on the whole structure
- C0 can be checked in constant time
- C2 can be checked in linear time with respect to $|ample(s)|$

Condition C1

C1

Along every path in the original structure that starts in s, the following condition holds: a transition that is dependent on a transition in $\mathit{ample}(s)$ cannot be executed without a transition in $\mathit{ample}(s)$ occurring first.

- checking C1 for a state s and a set $T \subseteq \mathit{enabled}(s)$ is at least as hard as checking reachability for K (reachability problem can be reduced to checking C1)
- we give a procedure computing a set of transitions that is guaranteed to satisfy C1
- computed sets do not have to be optimal: tradeoff efficiency Vs. amount of reduction

Condition C3

C3 (cycle condition)

A cycle in reduced structure is not allowed if it contains a state in which some transition is enabled, but is never included in *ample*(s) for any state s on the cycle.

- C3 is also non-local
- in contrast to C1, C3 refers only to the reduced structure
- instead of checking C3, we formulate a stronger condition which is easier to check

Condition C3

Lemma

Assume that C1 holds for all ample sets along a cycle in a reduced structure. If at least one state along the cycle is fully expanded, then C3 hold for this cycle.

- C1 implies that each $\alpha \in \mathit{enabled}(s) \setminus \mathit{ample}(s)$ is independent of transitions in $\mathit{ample}(s)$
- $\alpha \in \mathit{enabled}(s) \setminus \mathit{ample}(s)$ is also enabled in the next state on the cycle in K'
- if the cycle contains a fully expanded state, then it surely satisfies C3

Condition C3'

If K' is generated using depth-first search strategy, then every cycle in K' has to contain a back edge (i.e. an edge going to a state on the search stack)

C3'

If s is not fully expanded, then no transition in $ample(s)$ may reach a state that is on the search stack.

- C3' can be checked efficiently during nestedDFS algorithm

Calculating ample sets

Algorithm

Basic information

Reduced system is constructed on-the-fly: *ample*(s) is computed only when a model checking algorithm needs to know successors of s.

Algorithm computing ample sets depends on the model of computation. We consider processes with

- shared variables and
- message passing with queues.

Notation

- $pc_i(s)$ denotes the program counter of process P_i in a state s
- $pre(\alpha)$ is a set including all transitions β such that there exists a state s for which $\alpha \notin enabled(s)$ and $\alpha \in enabled(\beta(s))$
- $dep(\alpha)$ is the set of all transitions that are dependent on α
- T_i is the set of transitions of process P_i
- $T_i(s) = T_i \cap enabled(s)$
- $current_i(s)$ is the set of all transitions of P_i that are enabled in some s' such that $pc_i(s) = pc_i(s')$ (note that $T_i(s) \subseteq current_i(s)$)

Tradeoff

We do not compute the sets *pre*(α) and *dep*(α) precisely.
We prefer to efficiently compute over-approximations of these sets.

Computing *pre*(α)

- *pre*(α) includes the transitions of the processes that contain α and that can change a program counter to a value from which α can execute
- if the enabling condition for α involves shared variables, then *pre*(α) includes all other transitions that can change these shared variables
- if α sends or receives messages on some queue *q*, then *pre*(α) includes transitions of other processes that receive or send data through *q*, respectively

Computing *dep*(α)

- pairs of transitions that share a variable, which is changed by at least one of them, are dependent
- pairs of transitions belonging to the same process are dependent
- two receive transitions that use the same message queue are dependent
- two send transitions are also dependent (sending a message may cause the queue to fill)

Note that a pair of send and receive transitions in different processes are independent as they can potentially enable each other, but not disable.

Sketch of the algorithm

- C1 implies that transitions in $\mathit{enabled}(s) \smallsetminus \mathit{ample}(s)$ are independent on those in $\mathit{ample}(s)$
- as transitions in $T_i(s)$ are interdependent, it holds

$$T_i(s) \subseteq \mathit{ample}(s) \;\vee\; T_i(s) \cap \mathit{ample}(s) = \emptyset$$

- hence, $T_i(s)$ is a good candidate for $\mathit{ample}(s)$

Sketch of the algorithm

- C1 implies that transitions in $\mathit{enabled}(s) \smallsetminus \mathit{ample}(s)$ are independent on those in $\mathit{ample}(s)$
- as transitions in $T_i(s)$ are interdependent, it holds

$$T_i(s) \subseteq \mathit{ample}(s) \ \vee \ T_i(s) \cap \mathit{ample}(s) = \emptyset$$

- hence, $T_i(s)$ is a good candidate for $\mathit{ample}(s)$

Idea of the algorithm

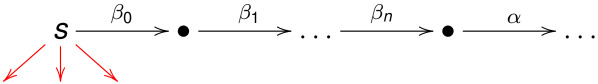
We check whether some $T_i(s) \neq \emptyset$ satisfies the conditions C1, C2, and C3'. If there is no such $T_i(s)$, we set $\mathit{ample}(s) = \mathit{enabled}(s)$.

Checking C1

C1

Along every path in the original structure that starts in s, the following condition holds: a transition that is dependent on a transition in *ample*(s) cannot be executed without a transition in *ample*(s) occurring first.

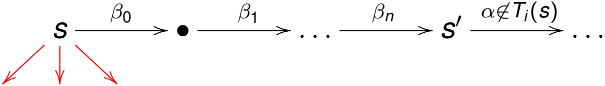
If *ample*$(s) = T_i(s)$ violates C1, then there is a path



where

- $\alpha \notin T_i(s)$ and α is dependent on $T_i(s)$,
- $\beta_0, \ldots, \beta_n$ are independent on $T_i(s)$.

Checking C1



There are two cases.

Case A $\alpha \in T_j$ for some $i \neq j$. Then $dep(T_i(s)) \cap T_j \neq \emptyset$.

Checking C1

$$\begin{tikzcd}
& s \arrow[r, "\beta_0"] \arrow[dl] \arrow[d] \arrow[dr] & \bullet \arrow[r, "\beta_1"] & \dots \arrow[r, "\beta_n"] & s' \arrow[r, "\alpha \notin T_i(s)"] & \dots \\
{} & {} & {} & & &
\end{tikzcd}$$

There are two cases.

Case A $\alpha \in T_j$ for some $i \neq j$. Then $dep(T_i(s)) \cap T_j \neq \emptyset$.

Case B $\alpha \in T_i$.

- $\beta_0, \dots, \beta_n$ are independent on $T_i(s)$ and hence $\beta_0, \dots, \beta_n \notin T_i$ (all transitions of P_i are considered as interdependent).
- Therefore $pc_i(s) = pc_i(s')$ and thus $\alpha \in current_i(s) \setminus T_i(s)$.
- As $\alpha \notin T_i(s)$, some transition of $\beta_0, \dots, \beta_n$ has to be included in $pre(\alpha)$.
- Hence, $pre(current_i(s) \setminus T_i(s)) \cap T_j \neq \emptyset$ for some $j \neq i$.

Algorithm checking C1

```
function checkC1($s, P_i$)
  forall $P_i \neq P_j$ do
    if $dep(T_i(s)) \cap T_j \neq \emptyset \ \vee \ pre(current_i(s) \setminus T_i(s)) \cap T_j \neq \emptyset$ then
      return false
  return true
end function
```

If the function returns true, then C1 holds. It may return false even if $T_i(s)$ satisfies C1.

Algorithm

```
function checkC2($X$)
    forall $\alpha \in X$ do
        if $visible(\alpha)$ then
            return false
    return true
end function
```

```
function checkC3'($s, X$)
    forall $\alpha \in X$ do
        if $onStack(\alpha(s))$ then
            return false
    return true
end function
```

```
function $ample(s)$
  forall $P_i$ such that $T_i(s) \neq \emptyset$ do
    if checkC1($s, P_i$) $\wedge$ checkC2($T_i(s)$) $\wedge$ checkC3'($s, T_i(s)$) then
      return $T_i(s)$
  return $enabled(s)$
end function
```

Partial order reduction

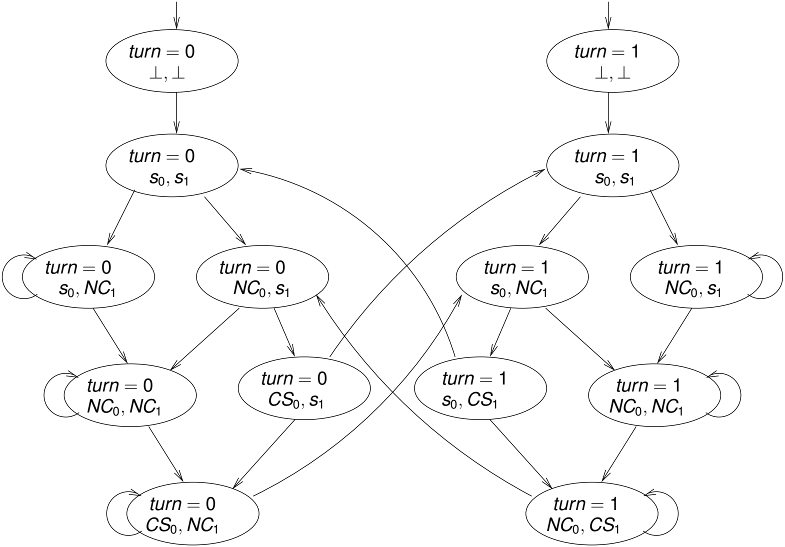
Example

Example: code

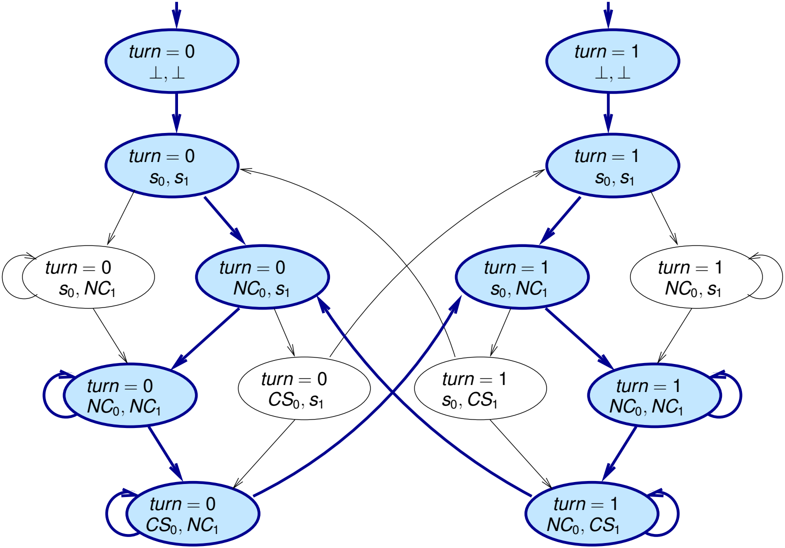
```
$P$ :: $m$ :        cobegin $P_0 \| P_1$ coend

$P_0$ :: $s_0$ :    while true do
       $NC_0$ :         wait($turn = 0$);
       $CS_0$ :         $turn := 1$;
                    endwhile;

$P_1$ :: $s_1$ :    while true do
       $NC_1$ :         wait($turn = 1$);
       $CS_1$ :         $turn := 0$;
                    endwhile;
```

Specification formula $\varphi = \mathrm{G}\neg((pc_0 = CS_0) \land (pc_1 = CS_1))$

Example


$turn = 0$ $\bot, \bot$
$turn = 1$ $\bot, \bot$
$turn = 0$ s_0, s_1
$turn = 1$ s_0, s_1
$turn = 0$ s_0, NC_1
$turn = 0$ NC_0, s_1
$turn = 1$ s_0, NC_1
$turn = 1$ NC_0, s_1
$turn = 0$ NC_0, NC_1
$turn = 0$ CS_0, s_1
$turn = 1$ s_0, CS_1
$turn = 1$ NC_0, NC_1
$turn = 0$ CS_0, NC_1
$turn = 1$ NC_0, CS_1

Example


$turn = 0$ $\bot, \bot$
$turn = 1$ $\bot, \bot$
$turn = 0$ s_0, s_1
$turn = 1$ s_0, s_1
$turn = 0$ s_0, NC_1
$turn = 0$ NC_0, s_1
$turn = 1$ s_0, NC_1
$turn = 1$ NC_0, s_1
$turn = 0$ NC_0, NC_1
$turn = 0$ CS_0, s_1
$turn = 1$ s_0, CS_1
$turn = 1$ NC_0, NC_1
$turn = 0$ CS_0, NC_1
$turn = 1$ NC_0, CS_1

The End

Thank you for your attention!

- Oral exam (subscribe via IS!)
- 30 min per student.
- The order to be determined later.
- Topics
    - Everything we have covered in the course.
    - Including the material not on the slides!