Verification and Model checking
DBMA-spring 2016

Håkon Normann

May 8, 2016

Overview

- Soundness

Overview

- Soundness
- Deadlock/livelock

Overview

- Soundness
- Deadlock/livelock
- State machines/Transition systems

Overview

- Soundness
- Deadlock/livelock
- State machines/Transition systems
- Finding deadlocks/livelocks in Transition systems.

Need something fitting here

- Soundness
  1. Option to complete

Need something fitting here

- Soundness
  1. Option to complete
  2. Proper completion

Need something fitting here

- Soundness
  1. Option to complete
  2. Proper completion
  3. No dead activities.

Need something fitting here

- Soundness
  1. Option to complete
  2. Proper completion
  3. No dead activities.
- Data Flow Correctness
  1. No missing data

Need something fitting here

- Soundness
  1. Option to complete
  2. Proper completion
  3. No dead activities.
- Data Flow Correctness
  1. No missing data
 2. No dead activities

Need something fitting here

- Soundness
  1. Option to complete
  2. Proper completion
  3. No dead activities.
- Data Flow Correctness
  1. No missing data
  2. No dead activities
  3. No lost updates

Option to Complete

A process instance, once started, can always complete.
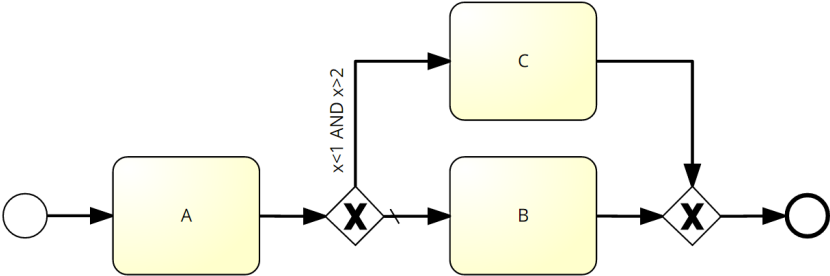Require that the process is free of Deadlocks and Livelocks.

Proper completion

When a process instance completes there is no related activity of this instance which is still running or enabled.
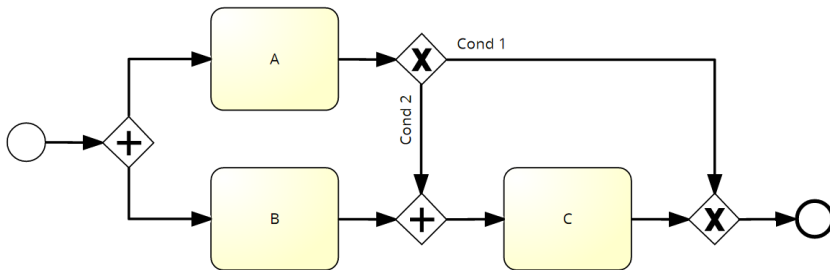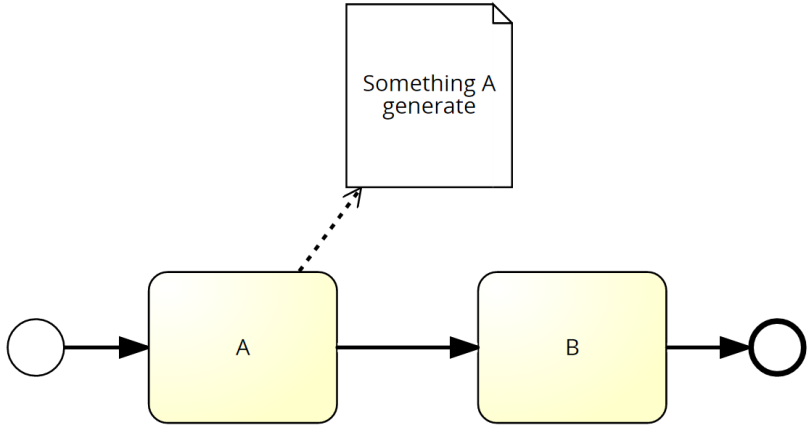
Dead Activity

For each activity there exists at least one completed trace producible on that model and containing this activity.

Unnecessary Data

A data object written by an activity of process model is called unnecessary if it is not read by any subsequent activity or transition condition or passed to the outside environment via an end message.

Missing Data

The data flow schema of a process model might cause missing data at run-time if a data object exists which can be read during run-time without having been written by any preceding activity or provided by the outside environment (i.e., by a start message).
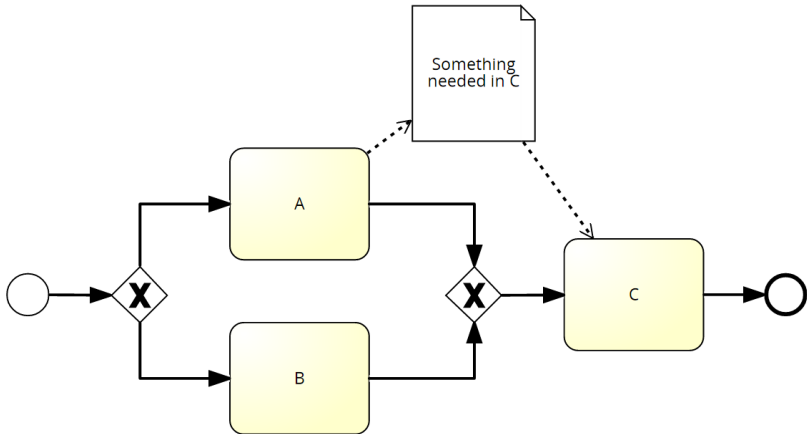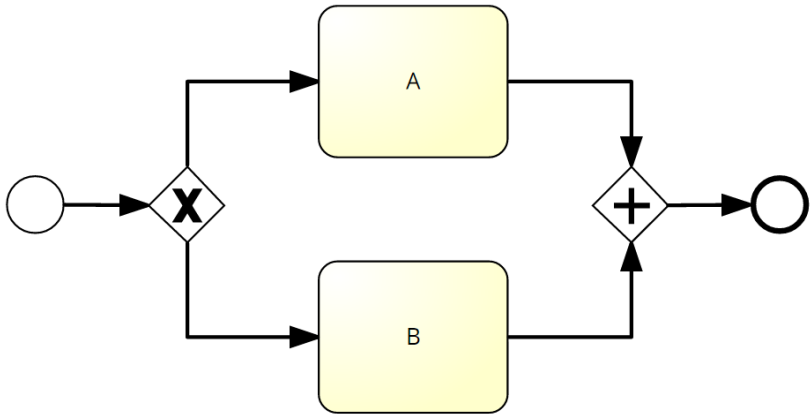
Lost Update

The data flow schema of a process model might cause lost data at run-time if a data object, which is written by an activity, is updated by a subsequent activity, but without reading the data object in between.
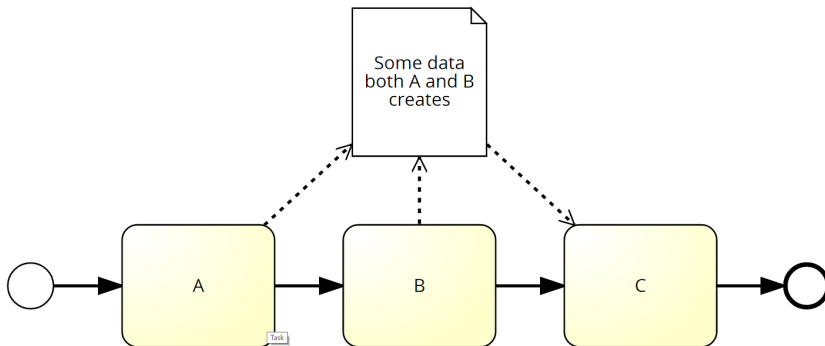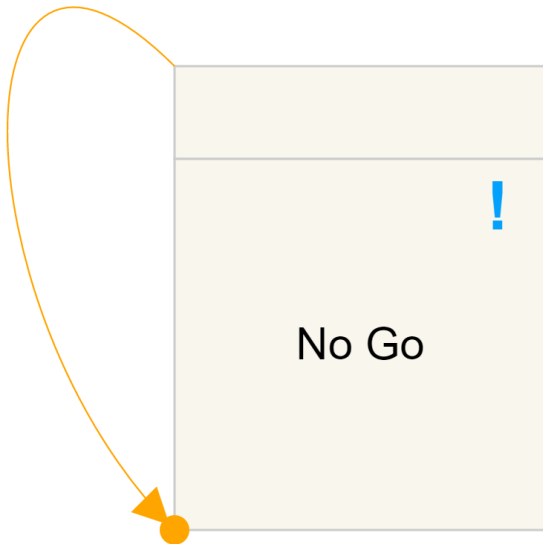
Deadlocks

There process is in a state where no activity is enabled, and the process is not completed.
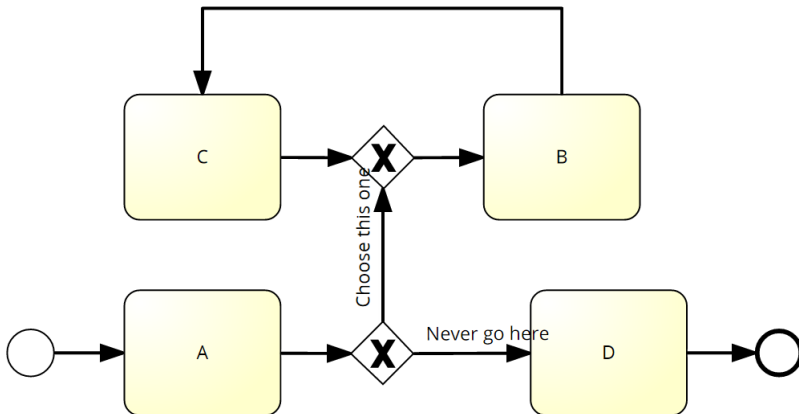
Deadlocks in DCR's

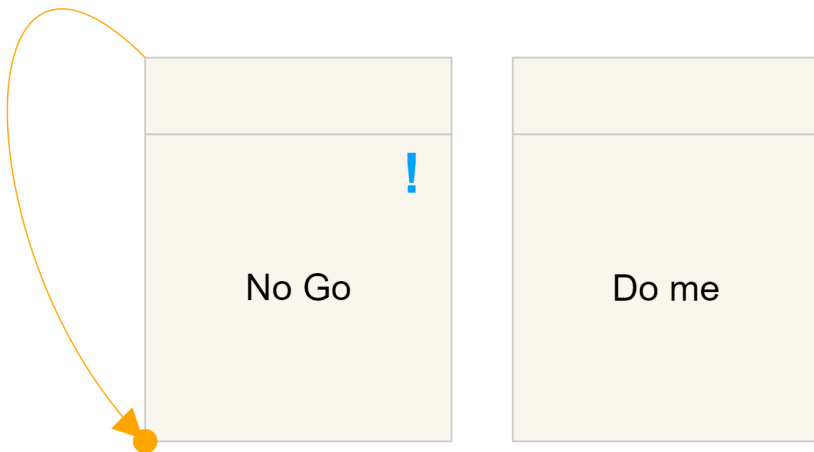There are a reachable state no enabled events, and there exist at least one included pending event.

livelock

The process continuously is able to perform some activity but never reach a completed state.

Livelock in DCR's

For all states reachable from the current state, there exists an enabled event and at least one included pending event.

Exercise

The models in the exercises file, which ones violates soundness and data flow, and how?

Unstructured vs Structured processes

- A well-structured or block-structured process model is composed of blocks (Single-Entry Single-Exit fragments), which can be nested, but must not overlap

Unstructured vs Structured processes

- A well-structured or block-structured process model is composed of blocks (Single-Entry Single-Exit fragments), which can be nested, but must not overlap
- Blocks can be single activities, sequences, parallel branchings, alternative branchings, loop blocks or the entire process model
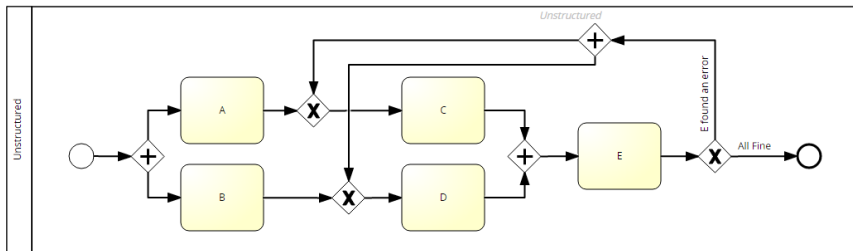
Unstructured vs Structured processes

- A well-structured or block-structured process model is composed of blocks (Single-Entry Single-Exit fragments), which can be nested, but must not overlap
- Blocks can be single activities, sequences, parallel branchings, alternative branchings, loop blocks or the entire process model
- Unstructured models require advanced verification techniques

Unstructured vs Structured processes

- A well-structured or block-structured process model is composed of blocks (Single-Entry Single-Exit fragments), which can be nested, but must not overlap
- Blocks can be single activities, sequences, parallel branchings, alternative branchings, loop blocks or the entire process model
- Unstructured models require advanced verification techniques
- Unstructured models are more difficult to understand and are a considerable source of errors

Unstructured vs Structured processes

Unstructured vs Structured processes
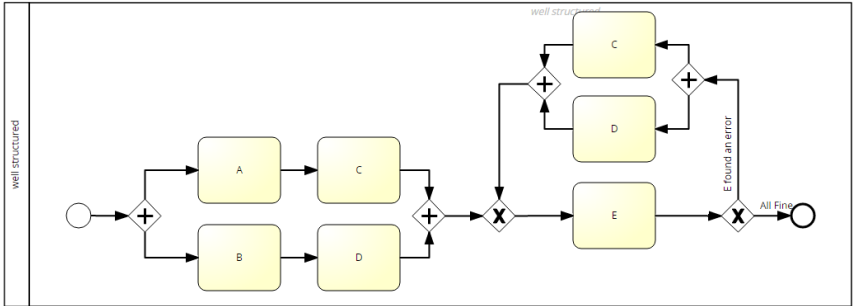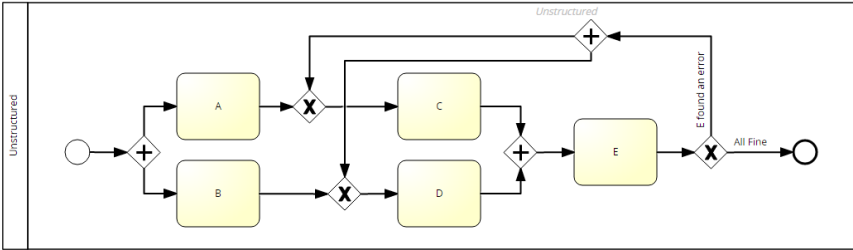
Transition Systems

- A Transition system, is a model where one model transitions between states of a process.

Transition Systems

- A Transition system, is a model where one model transitions between states of a process.
- A state is a snapshot of the process including which values each data object may have, and what state each activity/event have.

Transition Systems

- A Transition system, is a model where one model transitions between states of a process.
- A state is a snapshot of the process including which values each data object may have, and what state each activity/event have.
- States can also be marked as initial (the state the process starts in) or accepting (a state which allows the process to end).

Transition Systems

- A Transition system, is a model where one model transitions between states of a process.
- A state is a snapshot of the process including which values each data object may have, and what state each activity/event have.
- States can also be marked as initial (the state the process starts in) or accepting (a state which allows the process to end).
- Transitions are when activities in the process is executed. The execution of an activity may cause a transition to a new state or to the same state.

State space explosion

- As a state is a snapshot of a process, does it means that all possible snapshots are possible states.

State space explosion

- As a state is a snapshot of a process, does it means that all possible snapshots are possible states.

- For a dcr-graph each event may have 8 different states. This makes it so that for a full graph we MAY have up to 8^n states, where n is the number of events in the graph.

State space explosion

- As a state is a snapshot of a process, does it means that all possible snapshots are possible states.

- For a dcr-graph each event may have 8 different states. This makes it so that for a full graph we MAY have up to 8^n states, where n is the number of events in the graph.

- In a transition system not all states are reachable.

Checking for deadlocks and livelocks

- Deadlocks
  - From an initial state do a breadth-first search over states reachable by transitions from the initial state. to look for states with no outgoing transition

Checking for deadlocks and livelocks

- Deadlocks
  - From an initial state do a breadth-first search over states reachable by transitions from the initial state. to look for states with no outgoing transition
- Livelocks
  - Do a breadth-first search to look for loop backs to earlier visited states.

Signavio checks

Signavio checks