A Scalable Incomplete Boundedness Test for CFSM Languages

Wei Wei

Software Engineering Group
Department of Computer and Information Science
University of Konstanz
Germany

- It is a joint work with
  - Stefan Leue
  - Richard Mayr

Publications

- Stefan Leue, Richard Mayr, and Wei Wei: *A Scalable Incomplete Test for the Boundedness of UML RT Models*, Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems TACAS 2004.

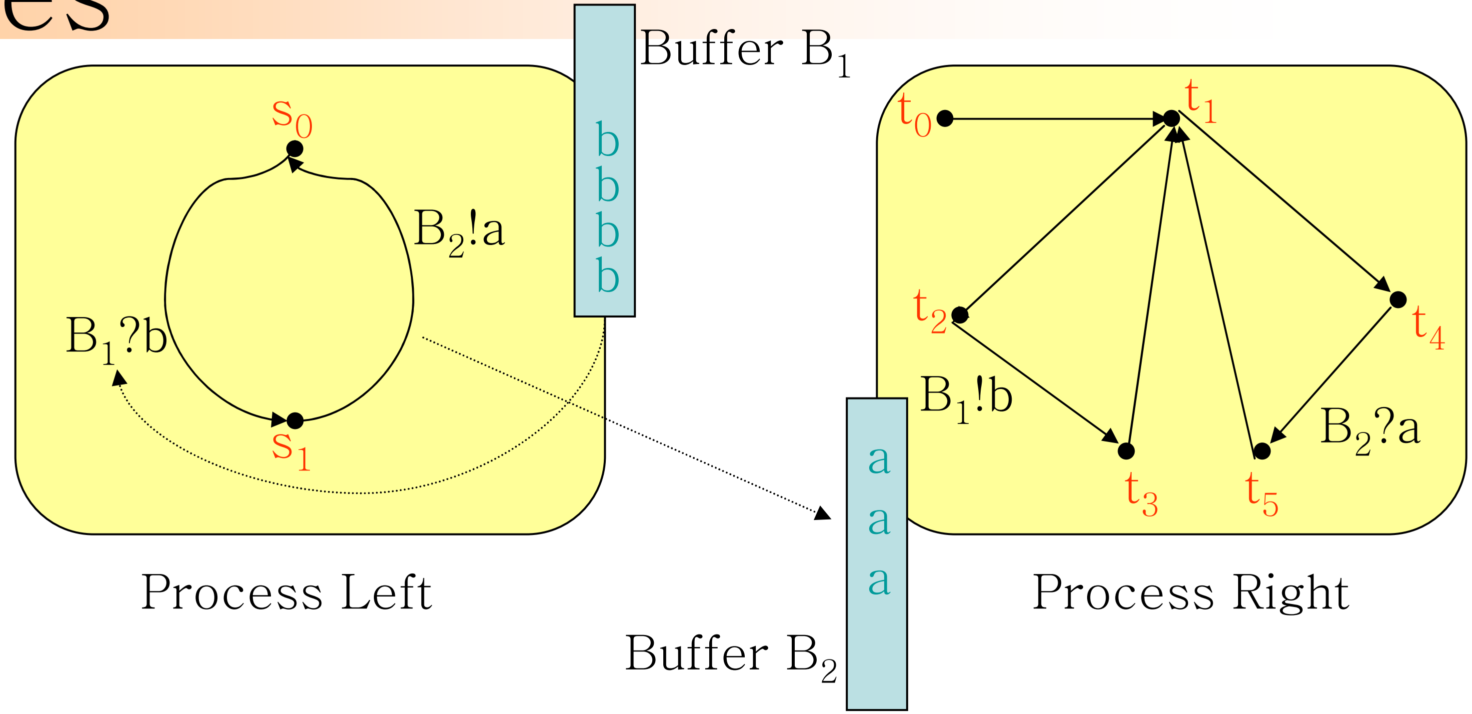
- Stefan Leue, Richard Mayr, and Wei Wei: *A Scalable Incomplete Test for Message Buffer Overflow in Promela Models*, Proceedings of the 11th International SPIN Workshop on Model Checking Software SPIN 2004.

- Stefan Leue and Wei Wei: *Counterexample-based Refinement for a Boundedness Test for CFSM Languages*, Proceedings of 12th International SPIN Workshop on Model Checking of Software SPIN 2005.

Outline

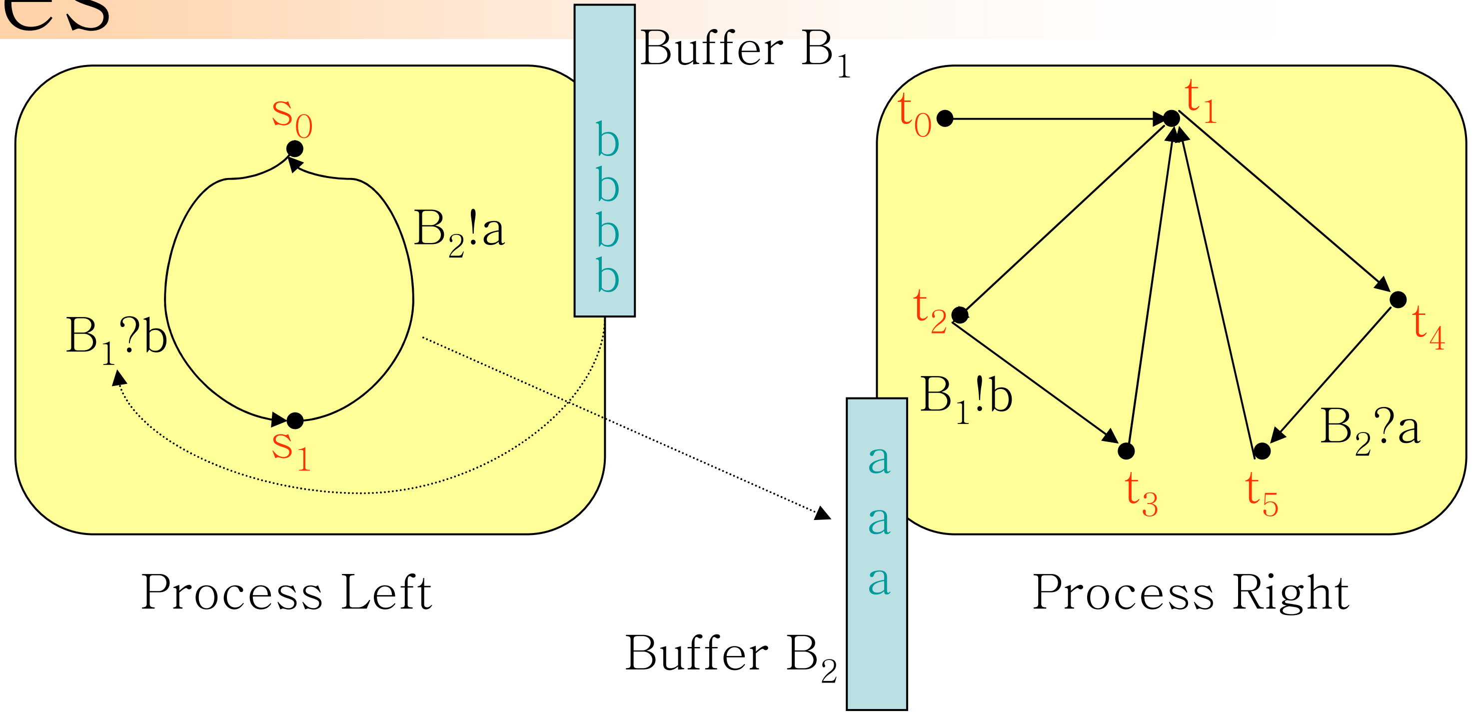
- Communicating Finite State Machines
- Boundedness
- Abstraction
- Verification
- Counterexamples and Refinement
- Conclusion

Communicating Finite State Machines



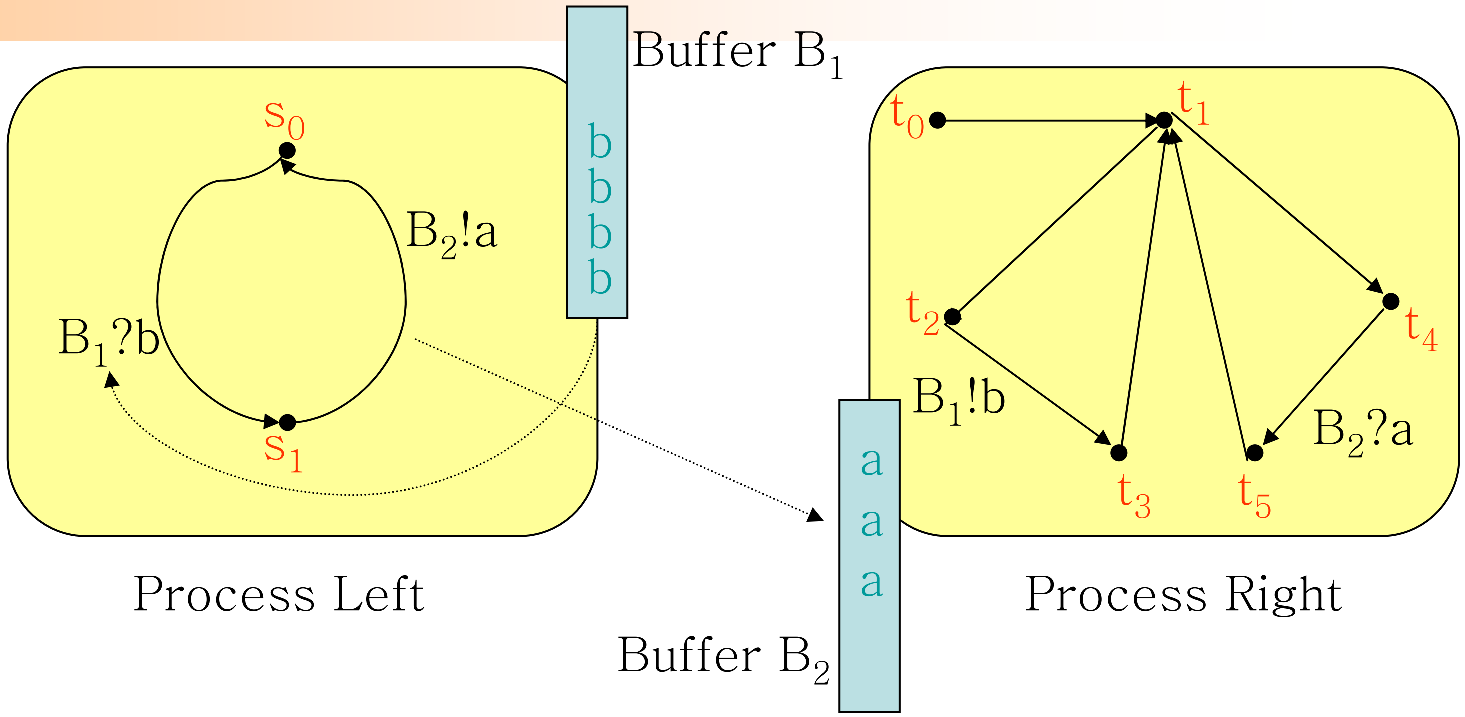
- Brand and Zafiropulo, 1983
- Keywords: finite state machines, asynchronous message exchanging, unbounded buffers

Communicating Finite State Machines



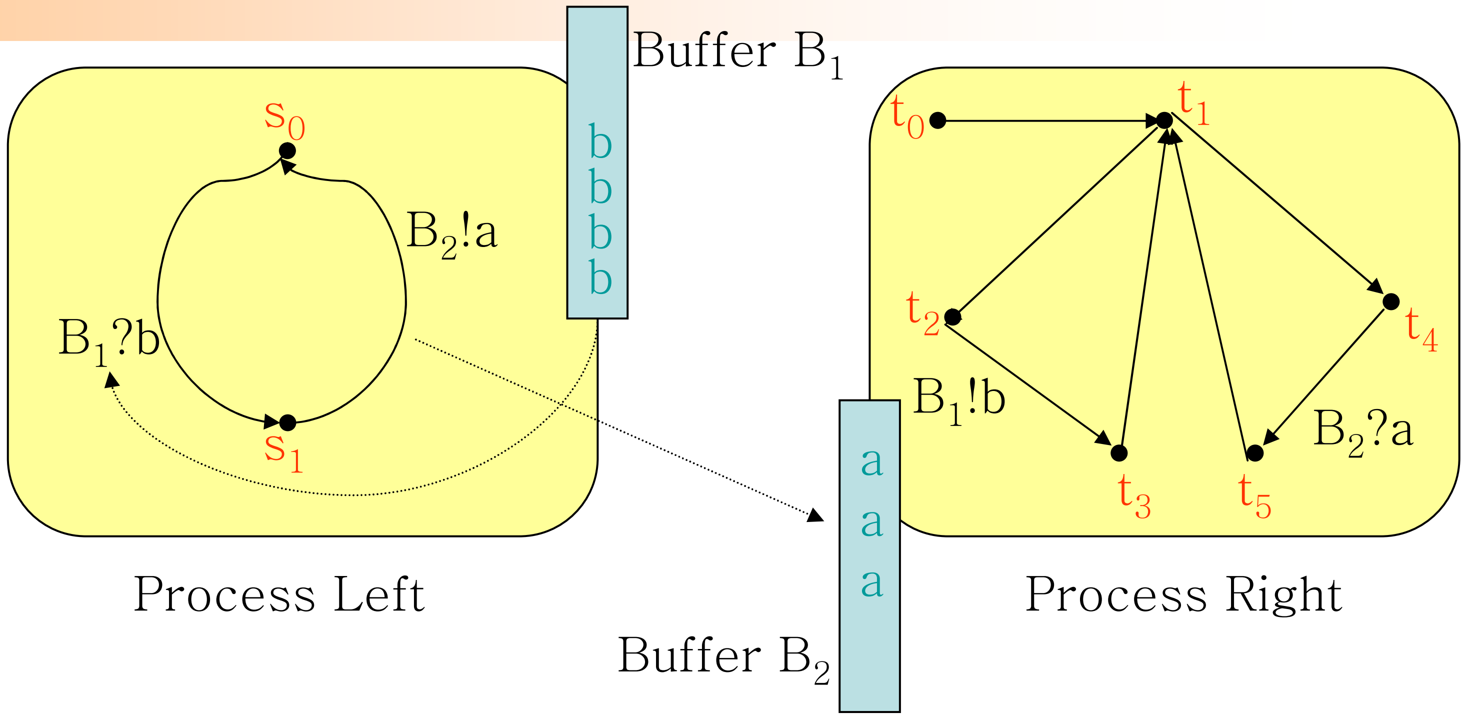
- UML RT, SPIN/Promela, SDL, …

Unboundedness



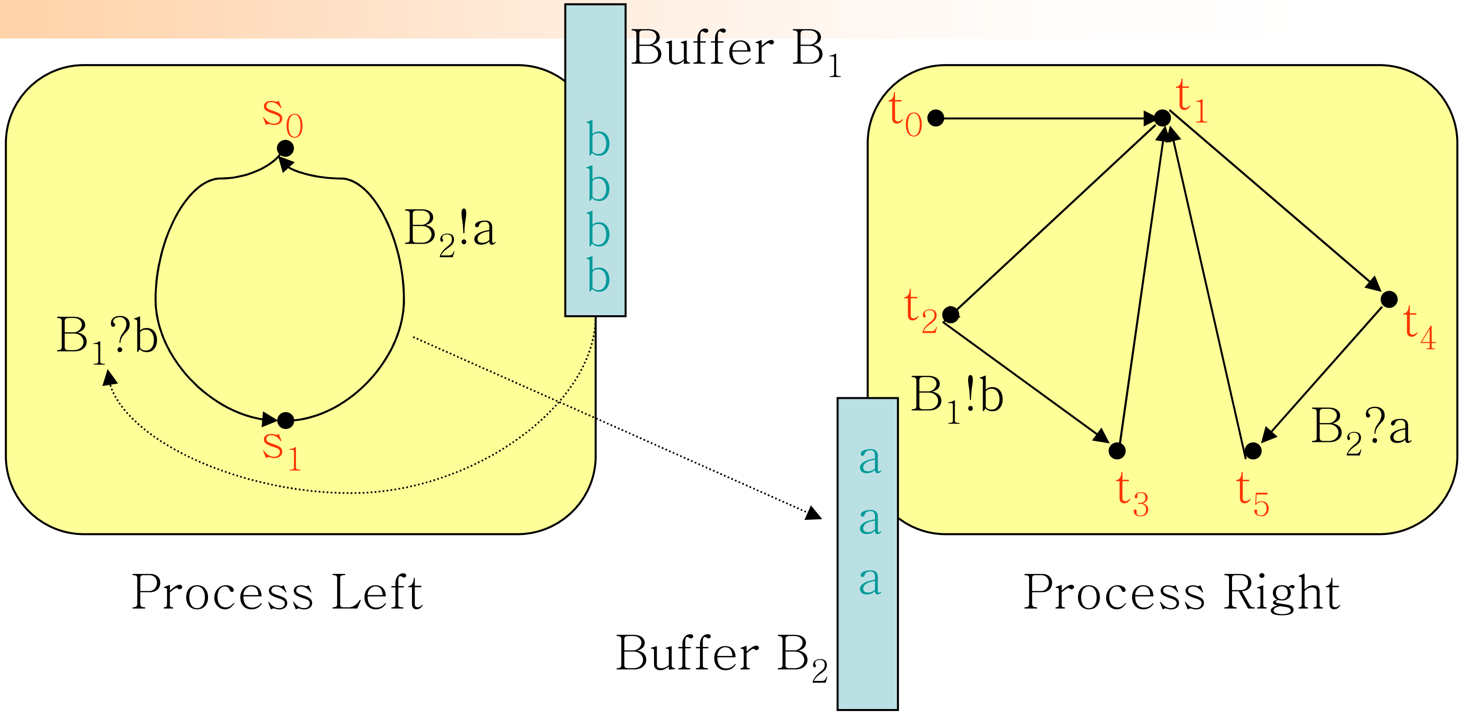
- Unbounded buffer filling is undesirable
  - Implementation: limited resources
  - Verification: impedes reachability analyses

Boundedness



A buffer is bounded if, at any time, the number of messages stored in the buffer is bounded.

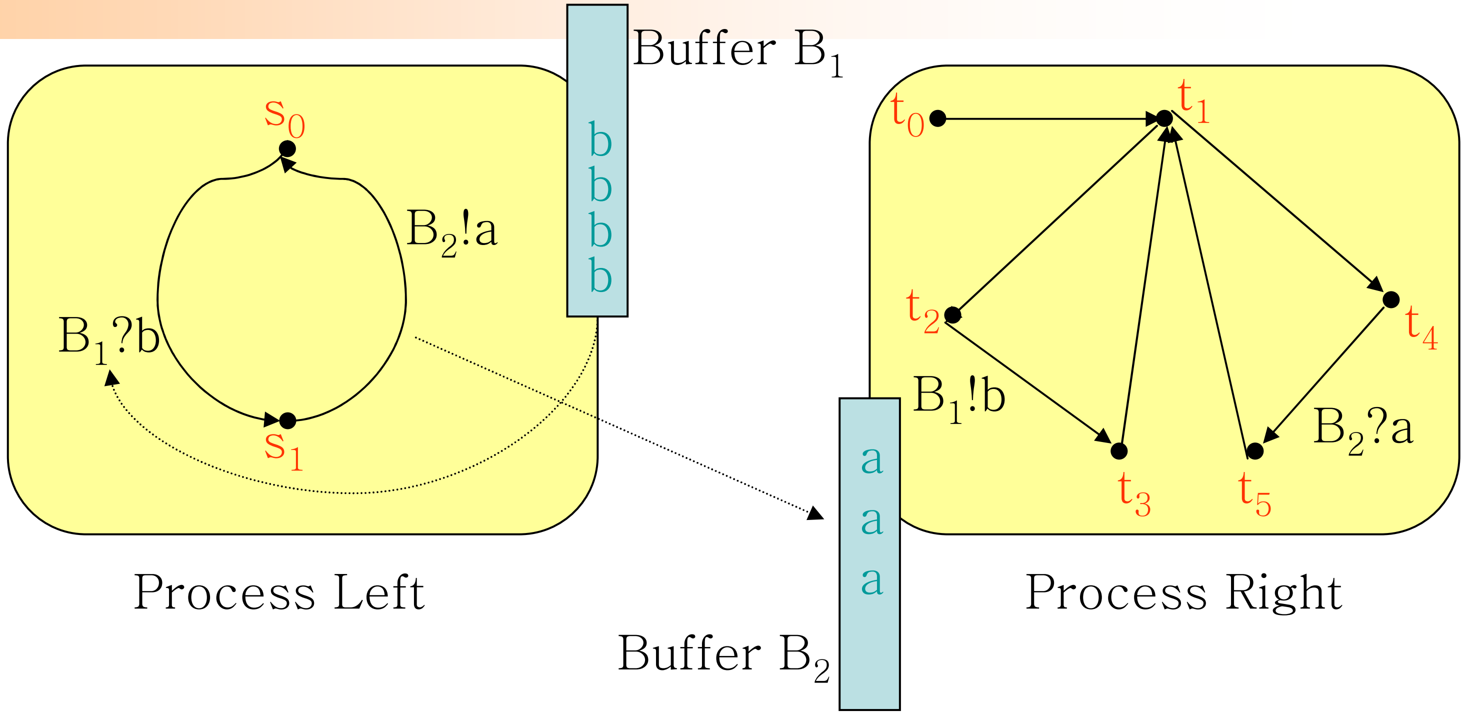
Boundedness



Boundedness is undecidable.

- Any determination algorithm is incomplete
- Abstract! -> construct overapproximations.

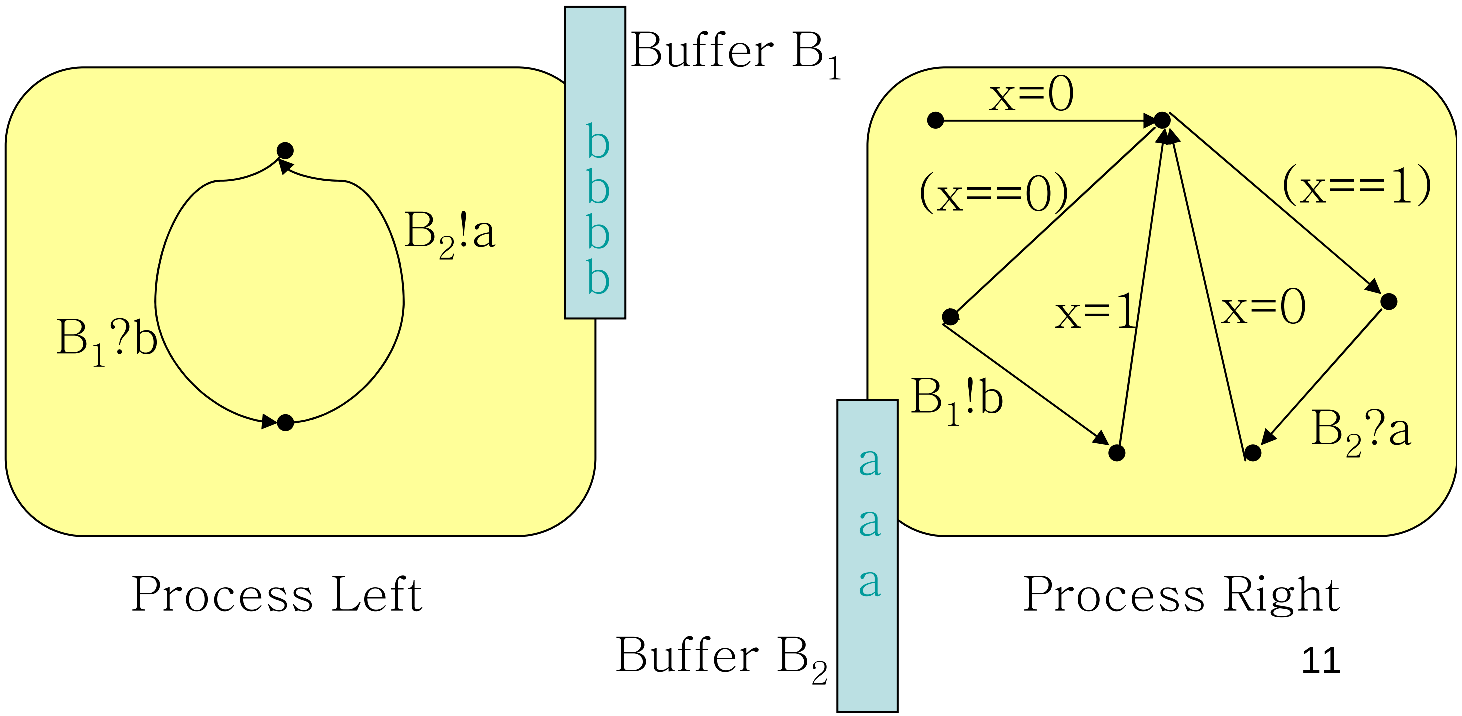
Boundedness Test



Cyclic behaviors: control flow cycles!

Abstraction

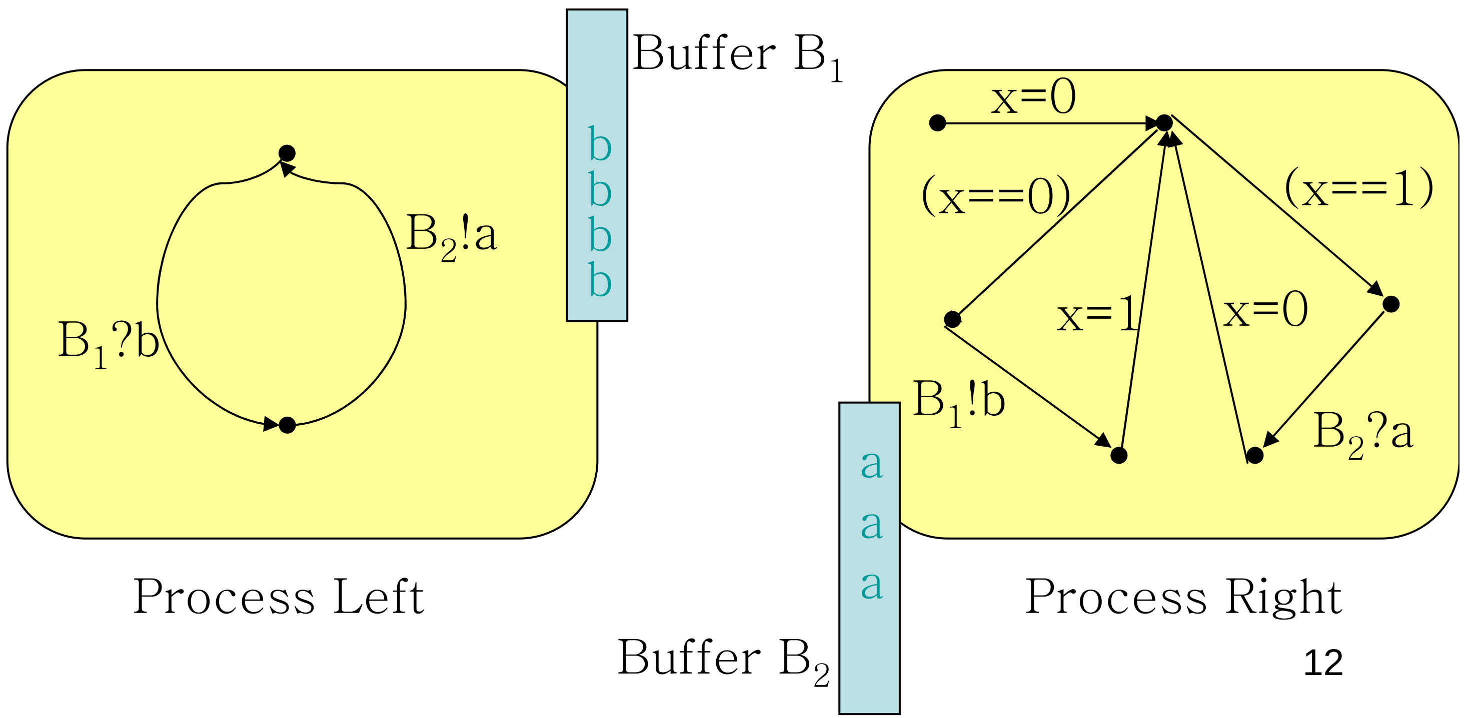
Level 0: A real model (Undecidable)



Abstraction

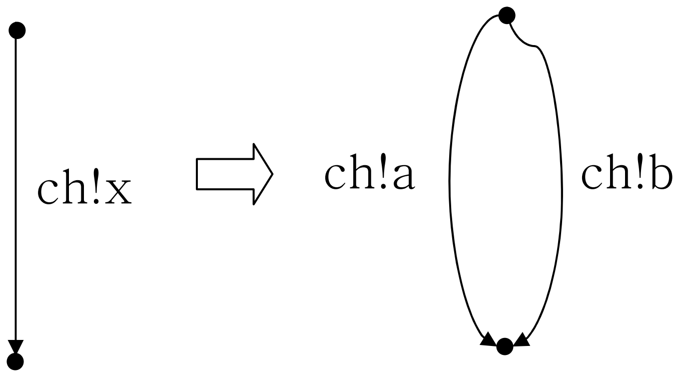
Level 0: A real model (Undecidable)

Abstracting program code

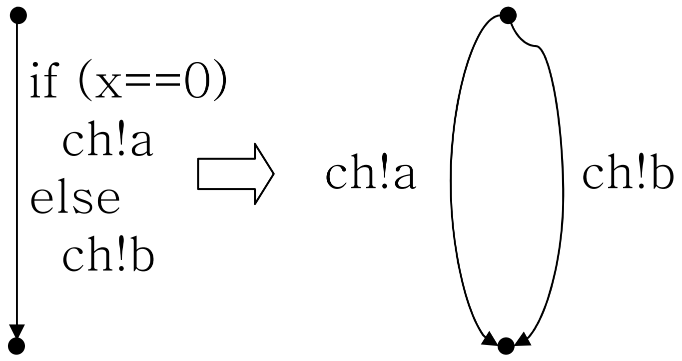


Code Abstraction

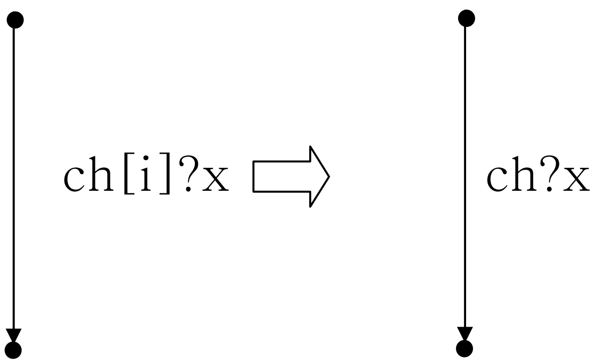
Variables



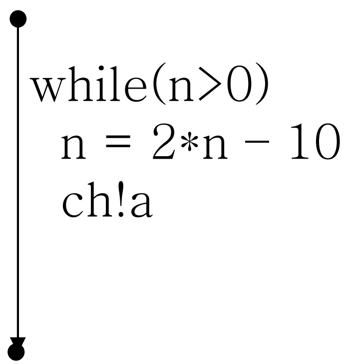
Branching



Buffer arrays



Loops

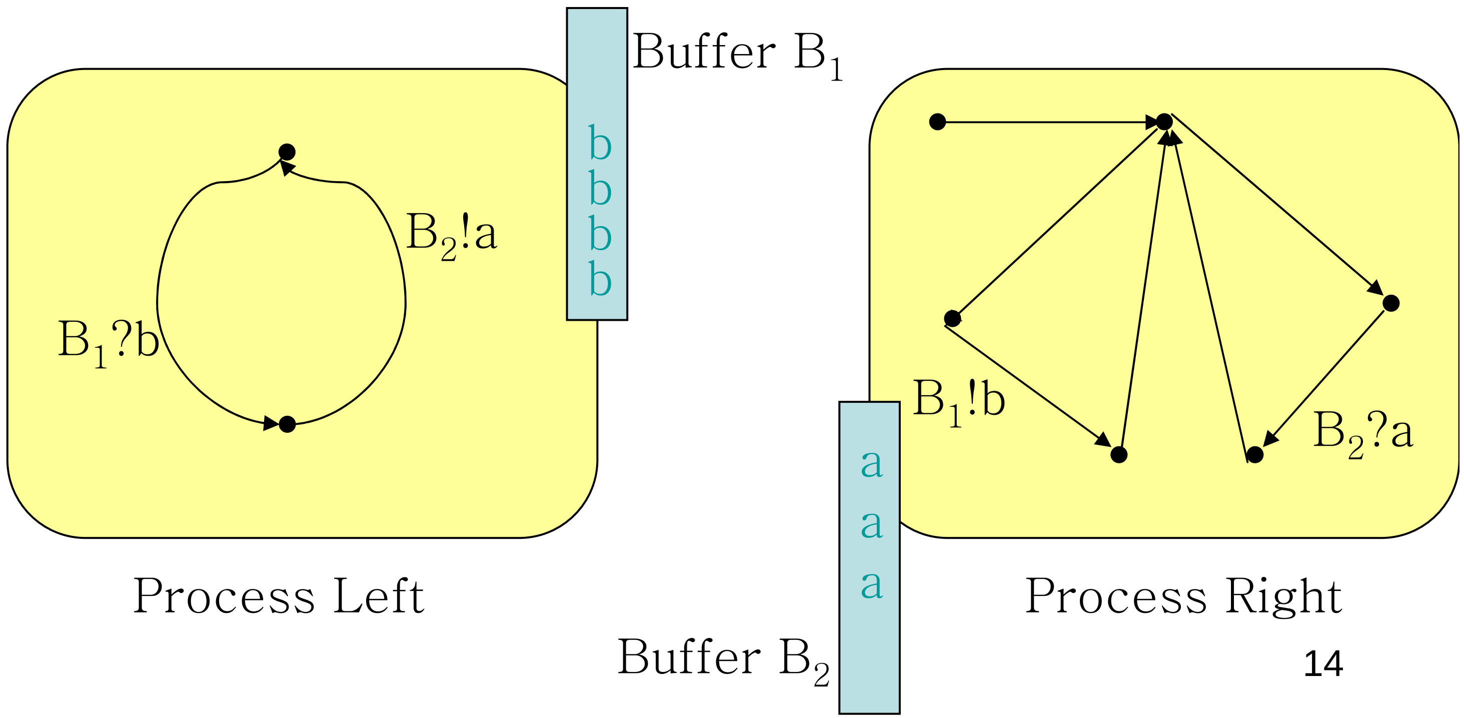


Abstraction

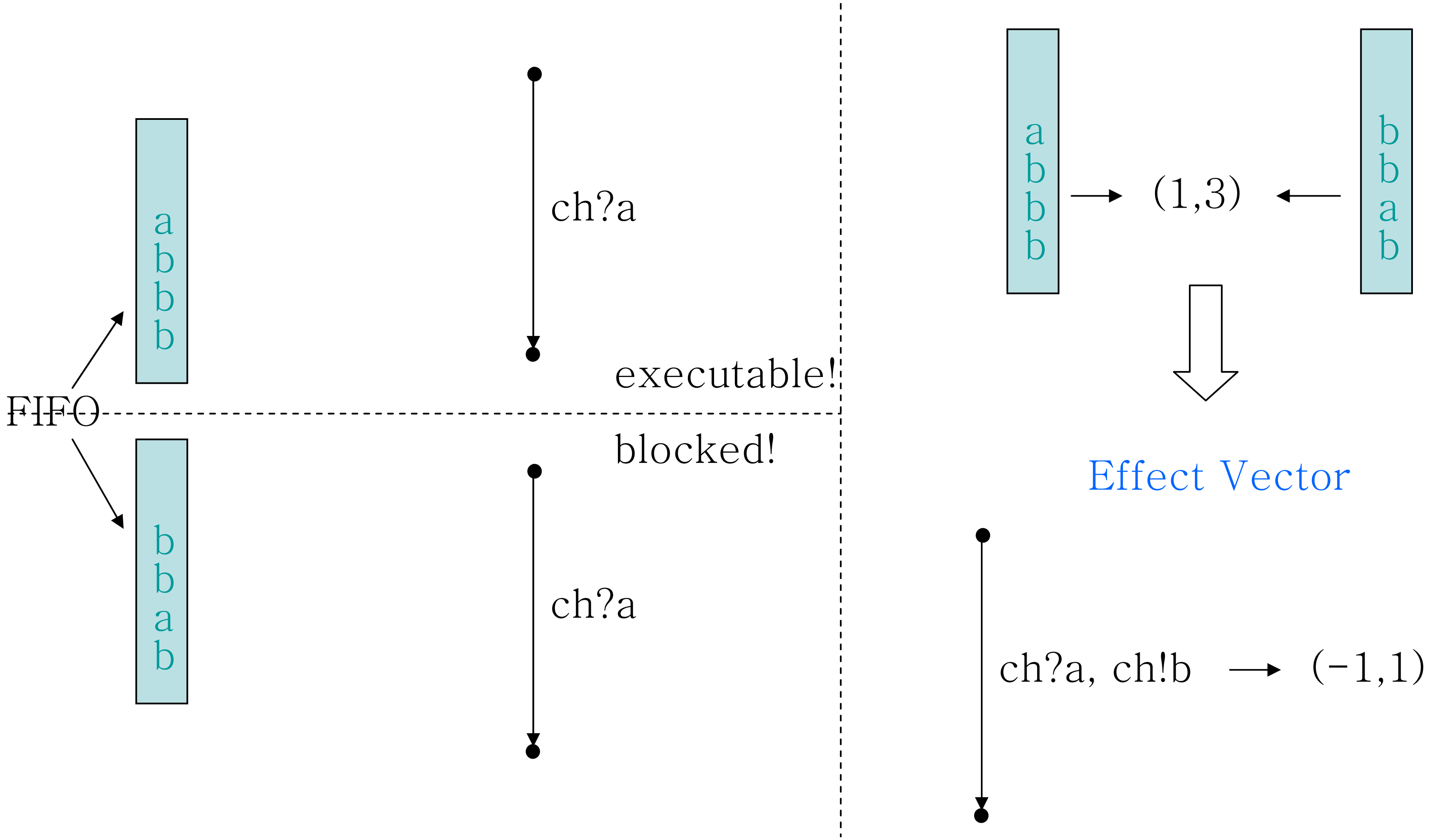
Level 0: A real model (Undecidable)

  Abstracting program code

    Level 1: CFSMs (Undecidable)



Message Orders

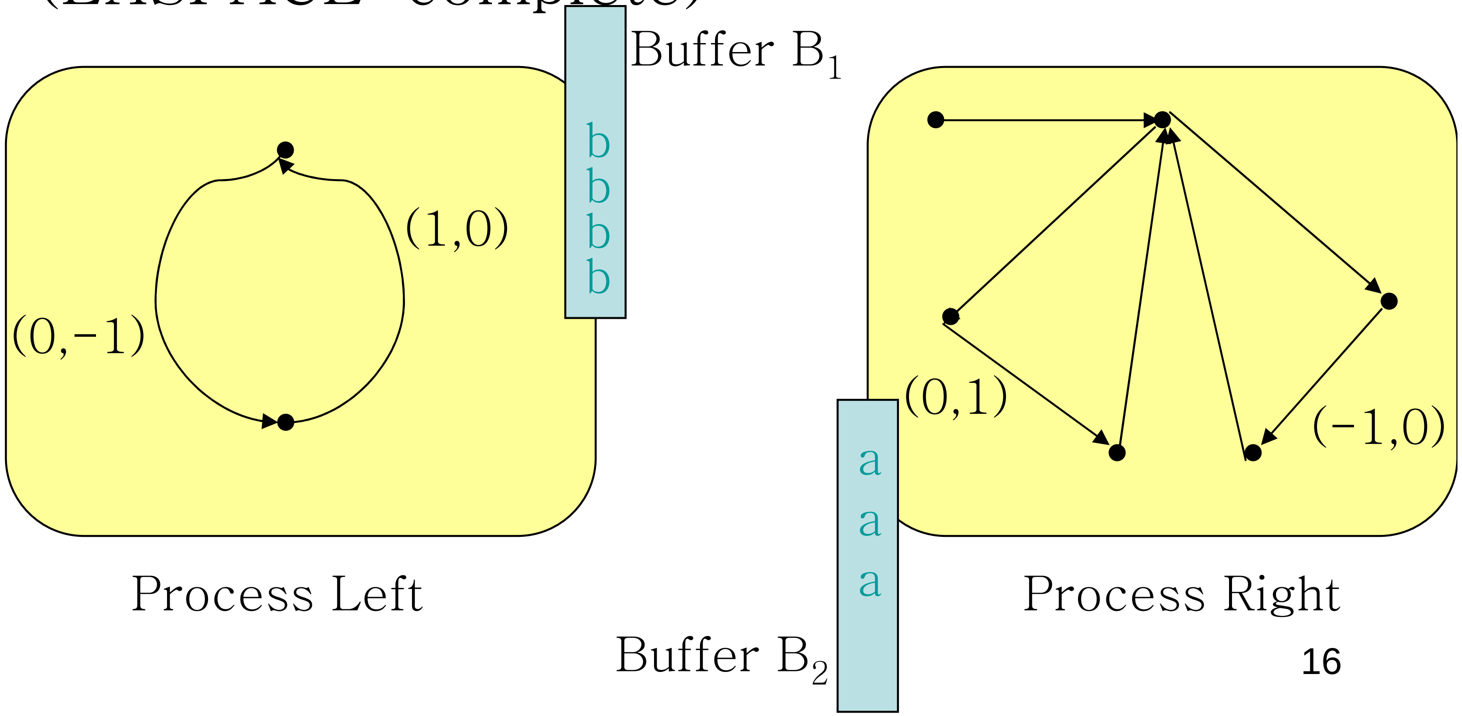


Abstraction

Level 1: CFSMs (Undecidable)

Abstracting message orders

Level 2: Vector addition systems with states (EXSPACE-complete)



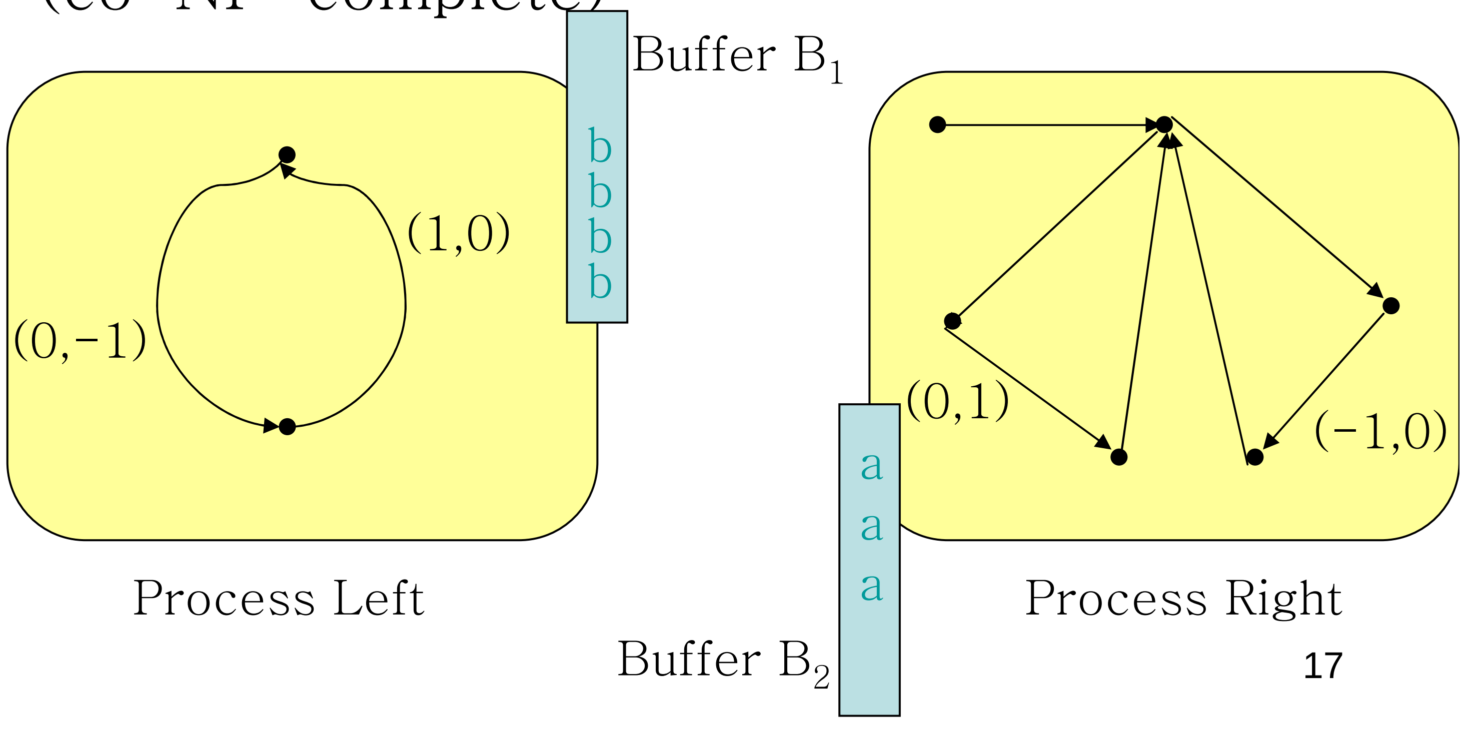
Abstraction

Level 2: VASS (EXSPACE-complete)

Abstracting activation conditions of cycles

Level 3: VASS with arbitrary inputs

(co-NP-complete)

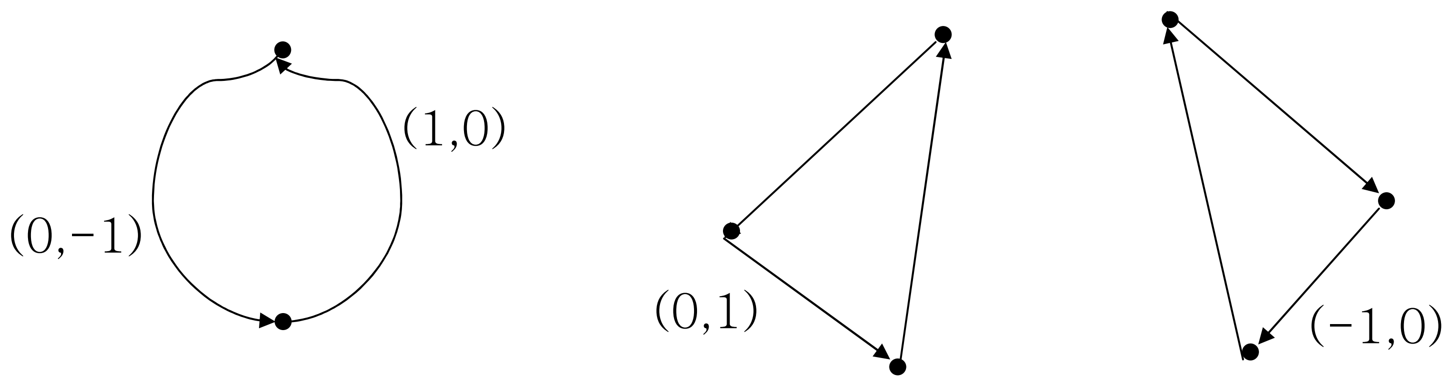


Abstraction

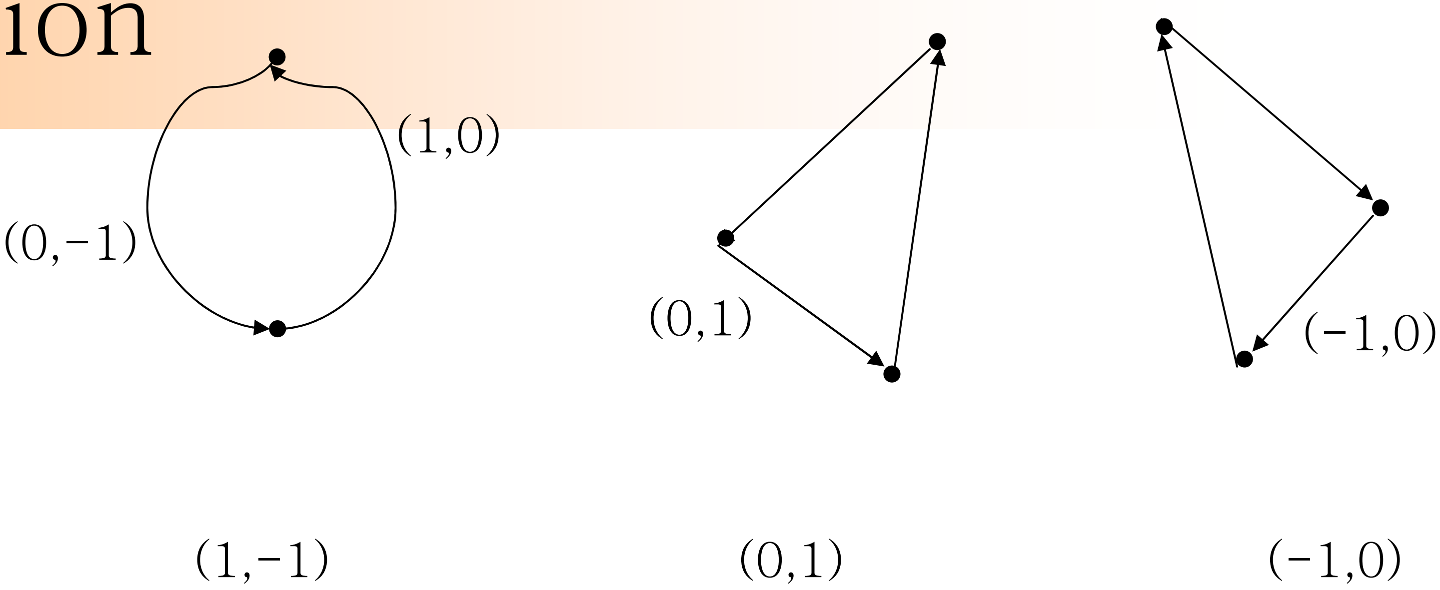
Level 3: VASS with arbitrary inputs(co-NP-complete)

Abstracting cycle dependencies

Level 4: Independent cycle system(polynomial)

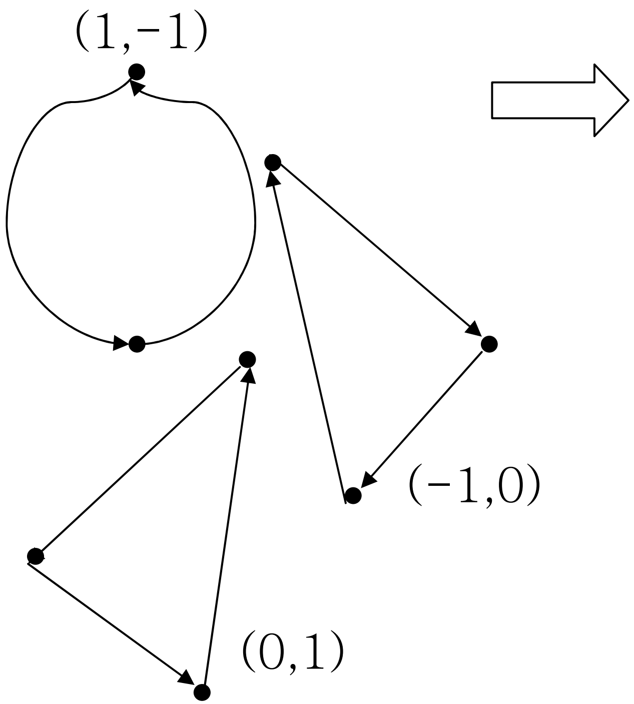


Verification



- Assign to each cycle an integer variable to denote how many times it is repeated
  - Check all the linear combinations of cycle effect vectors

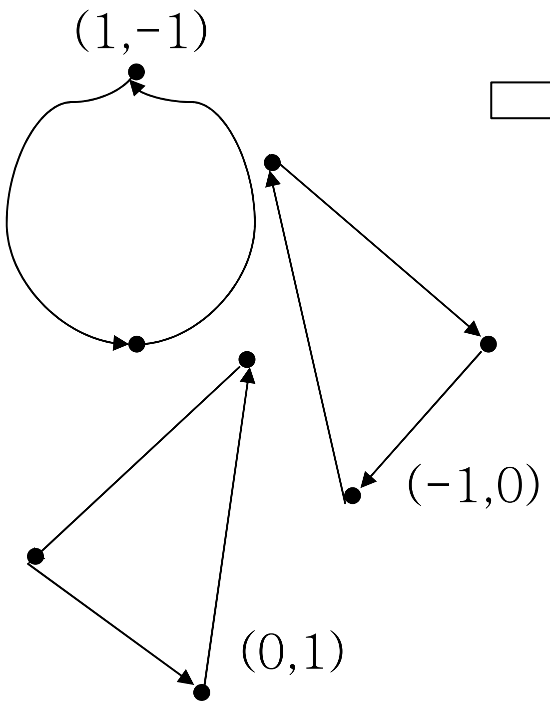
Verification



$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}=\begin{pmatrix}?\\?\end{pmatrix}$$

- A linear combination: only nonnegative components and at least one positive component.
  - The abstract model is unbounded. $\begin{pmatrix}0\\1\end{pmatrix}$
- No such combination.
  - The abstract and the concrete model are both bounded.

Verification



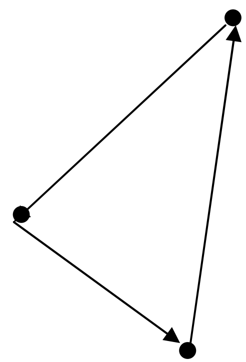
$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix}$$

- Encoded into an integer programming problem.
  - homogeneous
- No solution means „Bounded“. Otherwise, „Unknown“.

Counterexamples

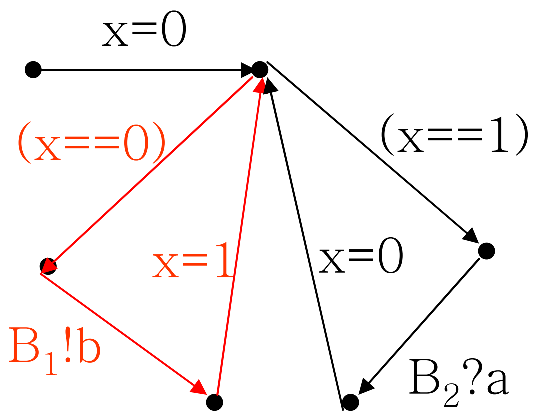
$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix}$$

A solution: $x_1 = 0$; $x_2 = 1$; $x_3 = 0$

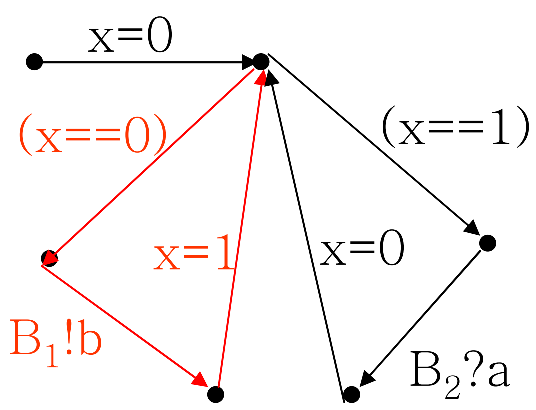


(0,1)

Spurious Counterexamples

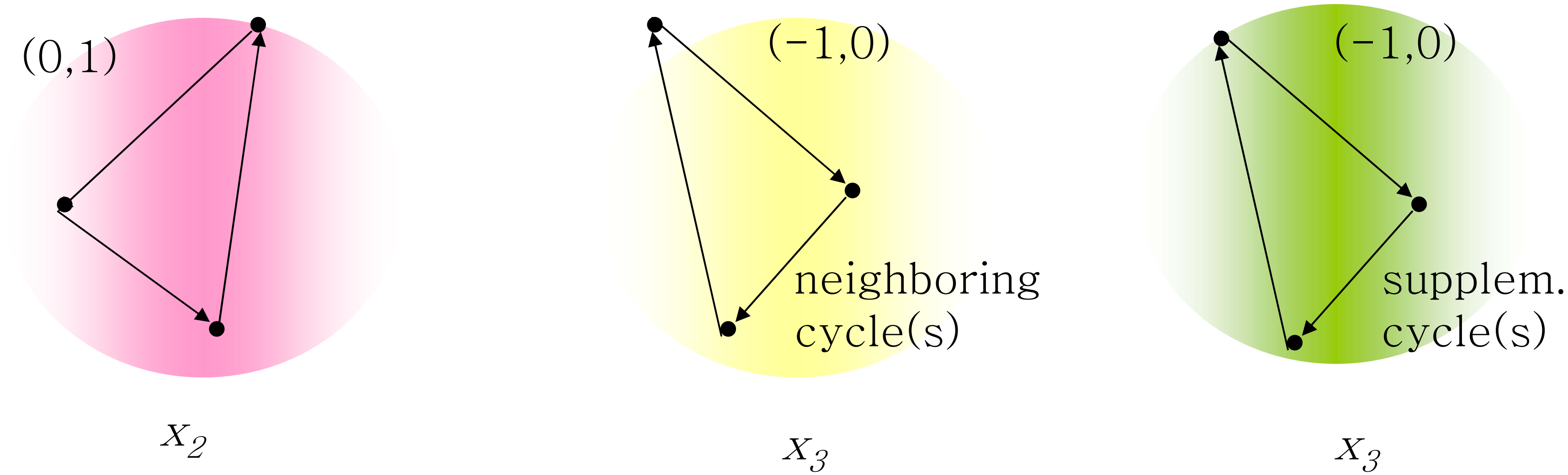


Cycle Code Analysis



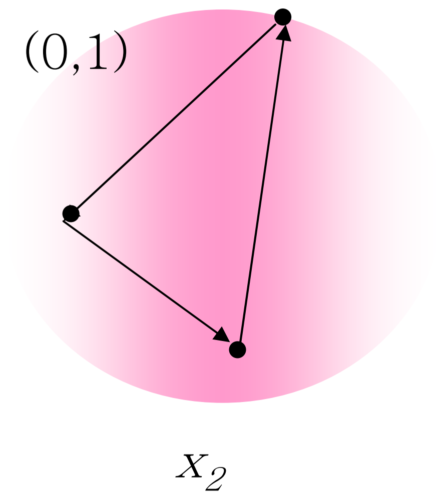
- Neighboring cycles.
- Supplementary cycles with respect to (x==0).

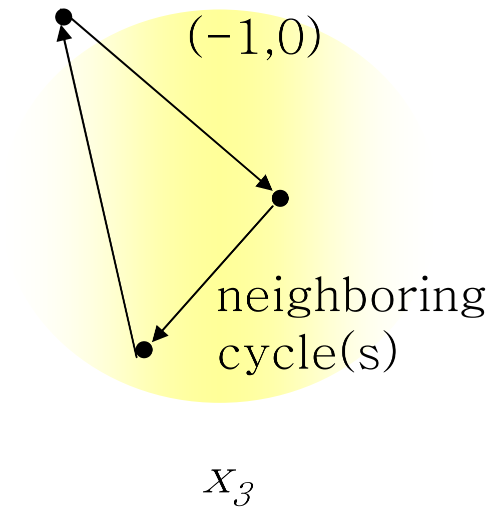
Refinement

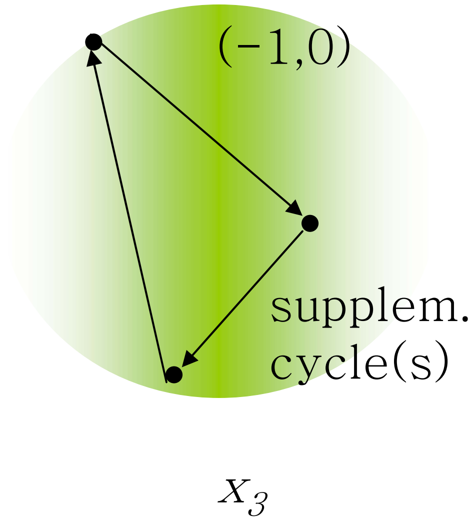


- Every time that the left cycle is executed,
  - at least one neighboring cycle must be executed
    $x_2 \leq 1*x_3$
  - at least one supplementary cycle must be executed
    $x_2 \leq 1*x_3$

Refinement



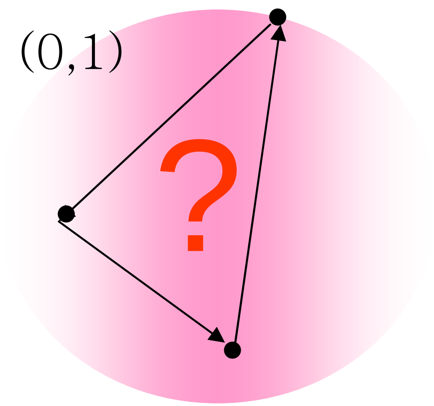




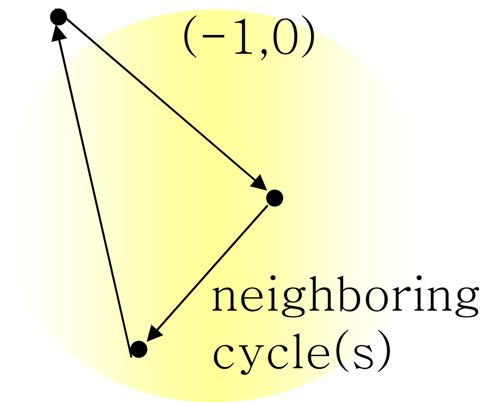
$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix}$$

$$x_2 \le x_3$$

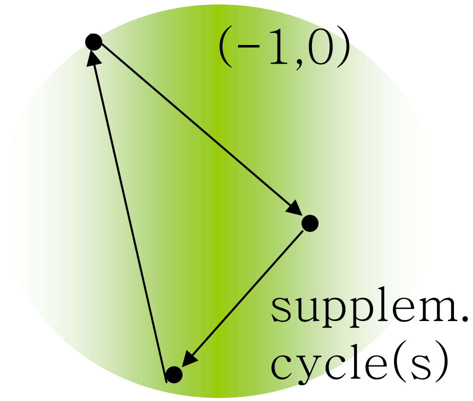
Refinement



x_2

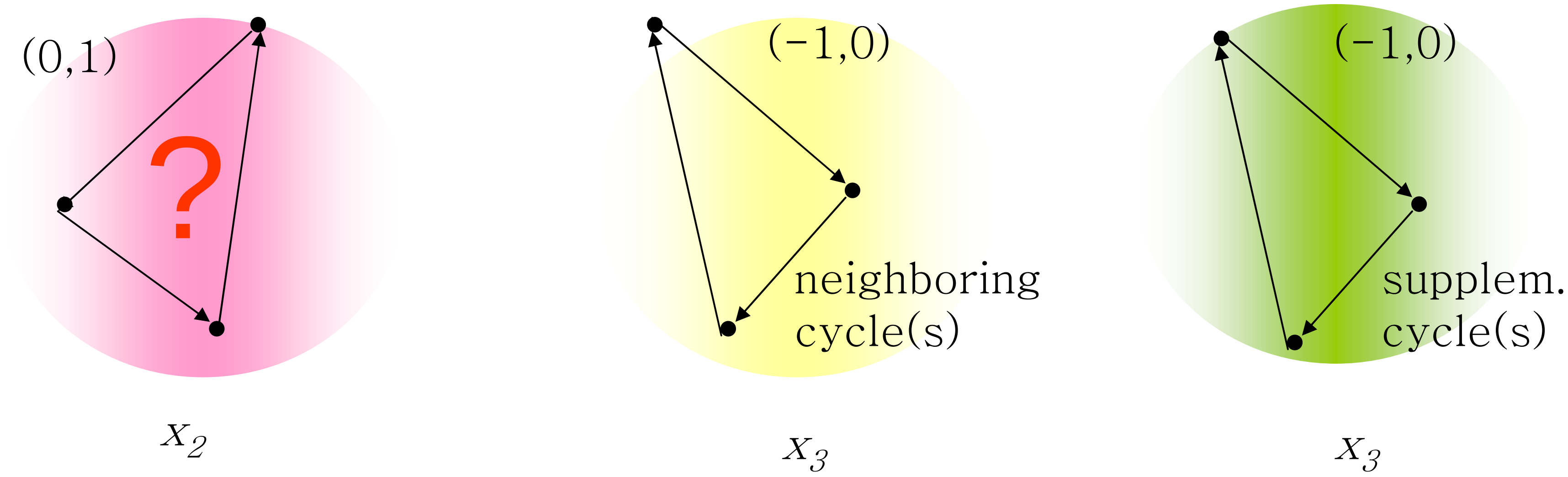


x_3



x_3

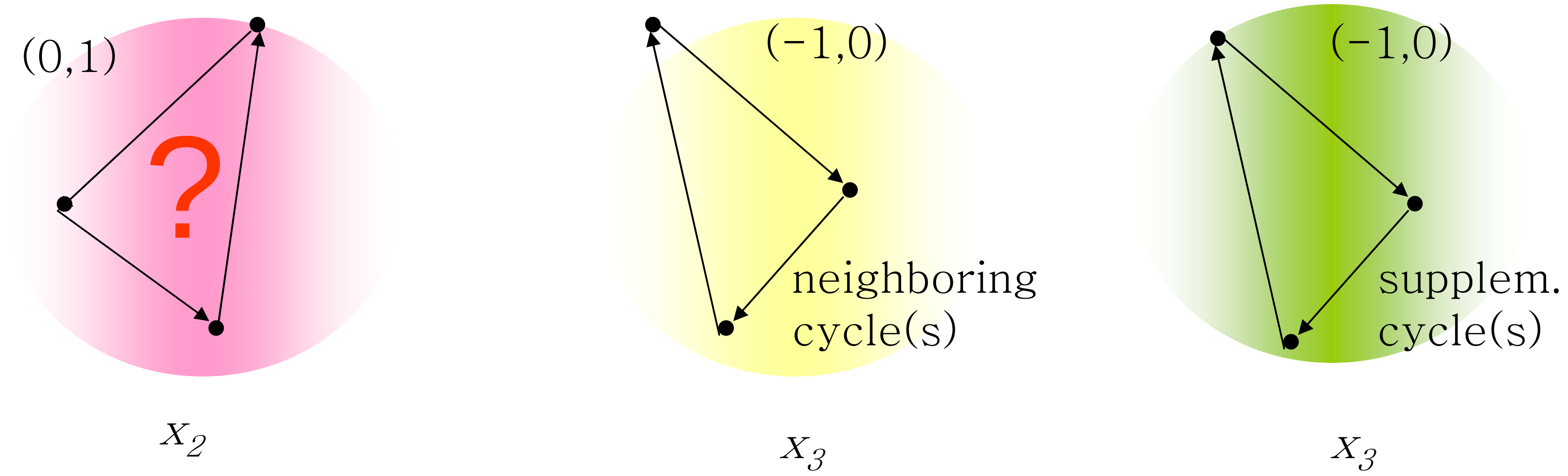
Refinement



Two possibilities:

- $x_2 = 0$
- $x_2 > 0 \land x_3 > 0 \land x_3 > 0$

Refinement



$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix}$$

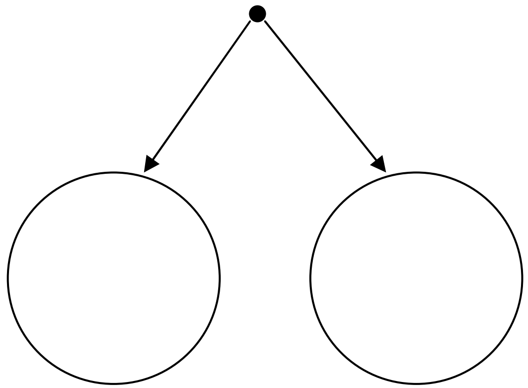
$$x_2=0$$

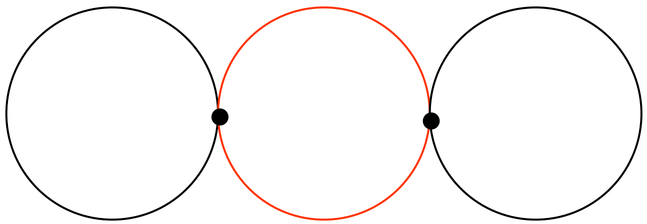
$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix}$$

$$x_2>0$$

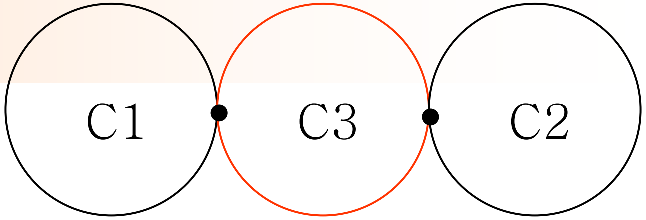
$$x_3>0$$

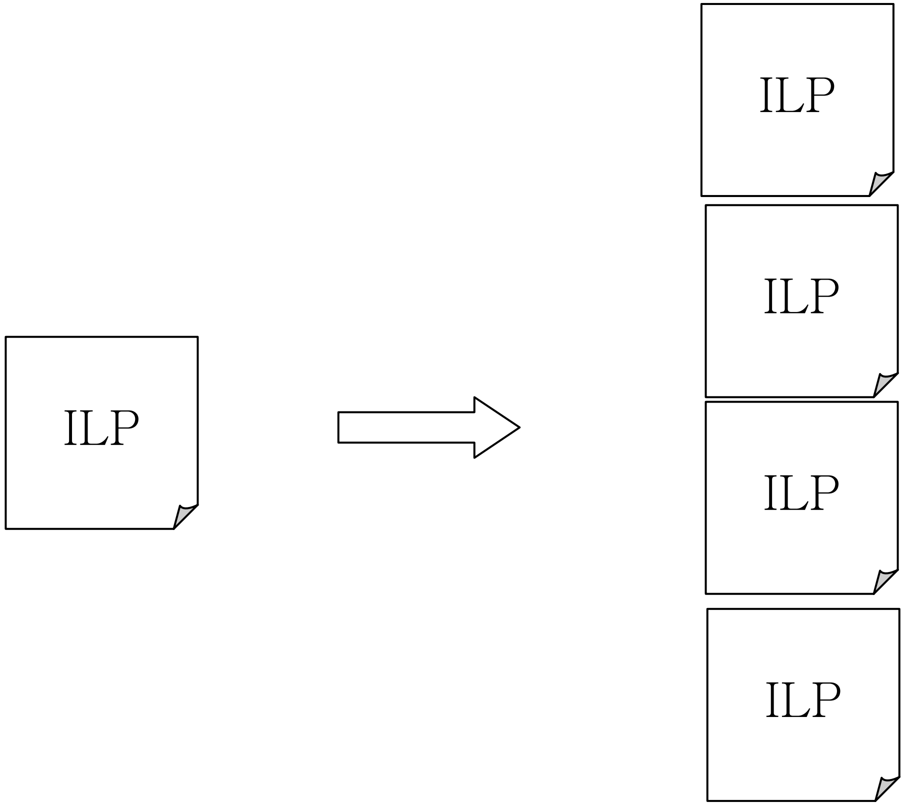
Graph Structure Analysis





Refinement





+ $x_1 = 0 \wedge x_2 = 0$

+ $x_1 > 0 \wedge x_2 = 0$

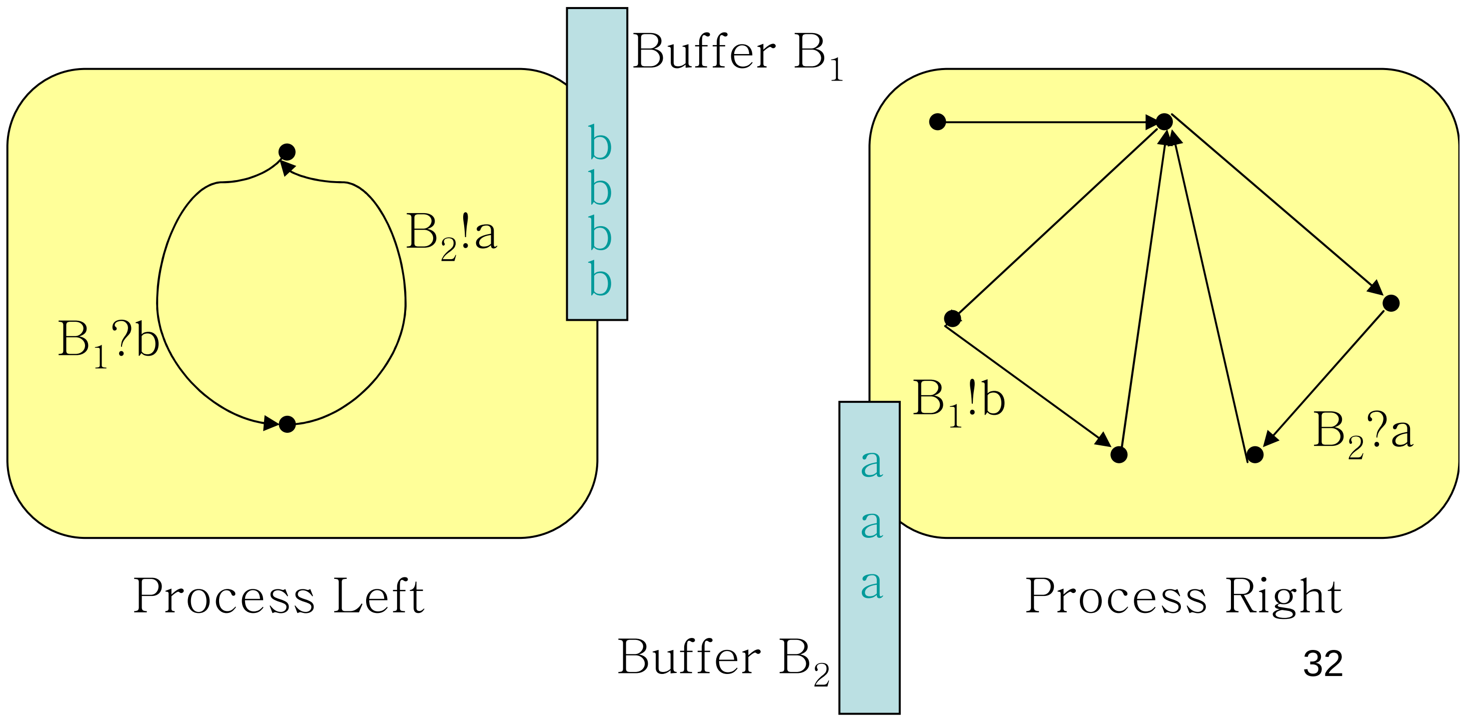
+ $x_1 = 0 \wedge x_2 > 0$

+ $x_1 > 0 \wedge x_2 > 0 \wedge x_3 > 0$

Buffer Bound Estimate

$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix}$$

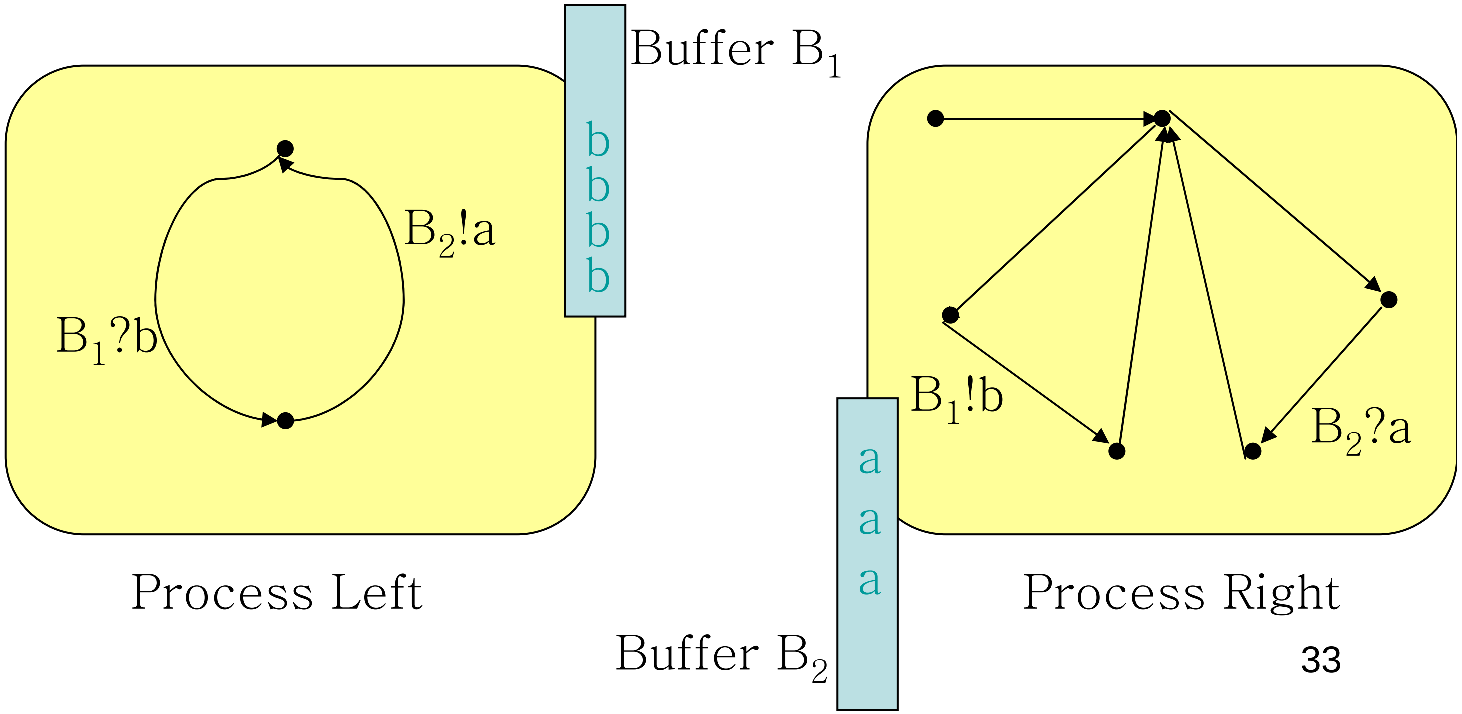
$$x_2 \le x_3$$



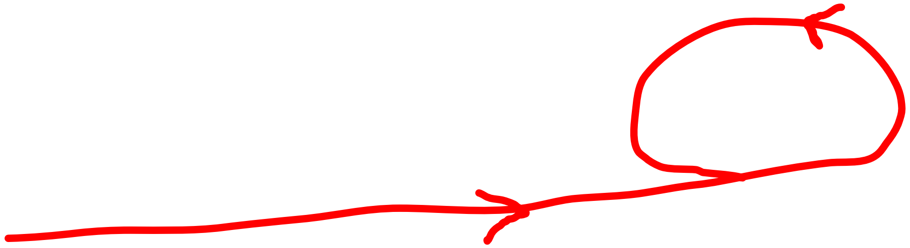
Buffer Bound Estimate

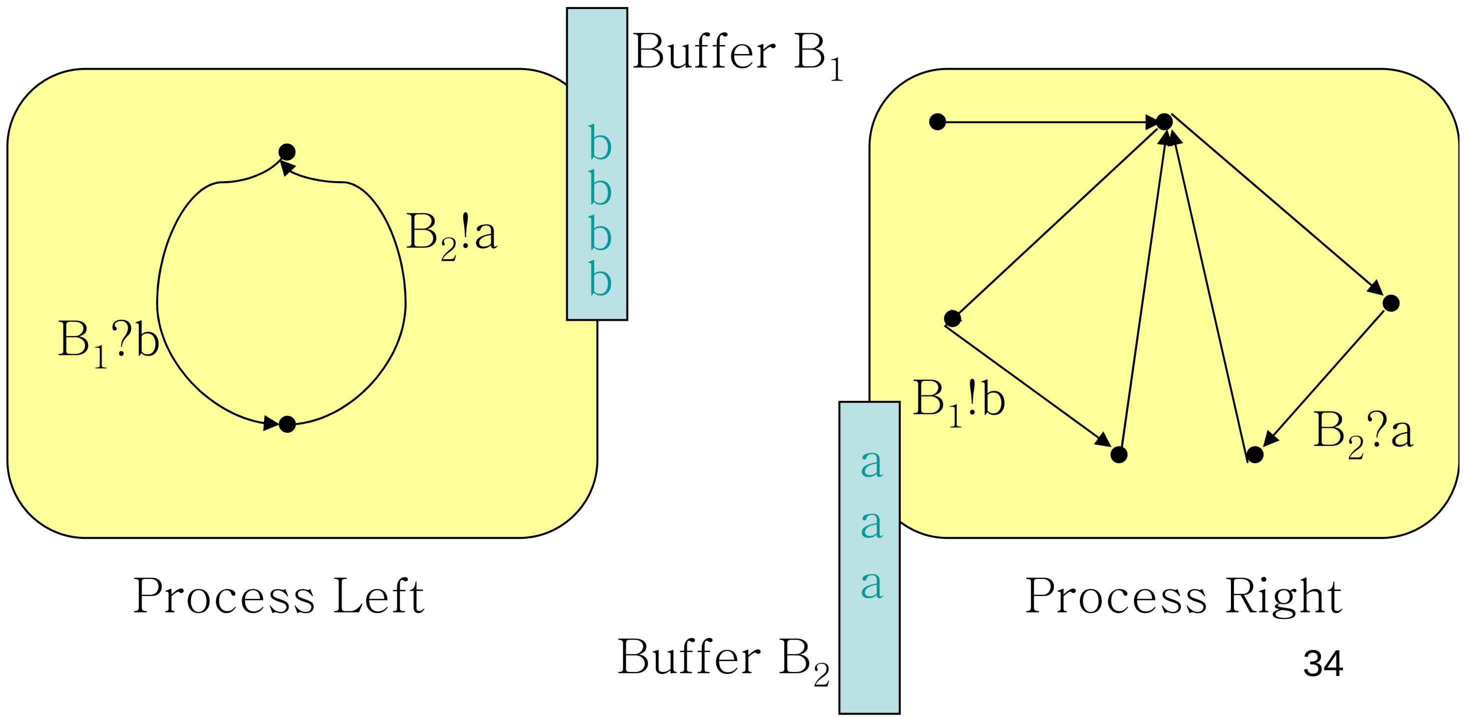
$$x_1\begin{pmatrix}1\\-1\end{pmatrix}+x_2\begin{pmatrix}0\\1\end{pmatrix}+x_3\begin{pmatrix}-1\\0\end{pmatrix}>\begin{pmatrix}0\\0\end{pmatrix} \longrightarrow$$ No solution! -> Bounded!

$$x_2 \le x_3$$



Buffer Bound Estimate



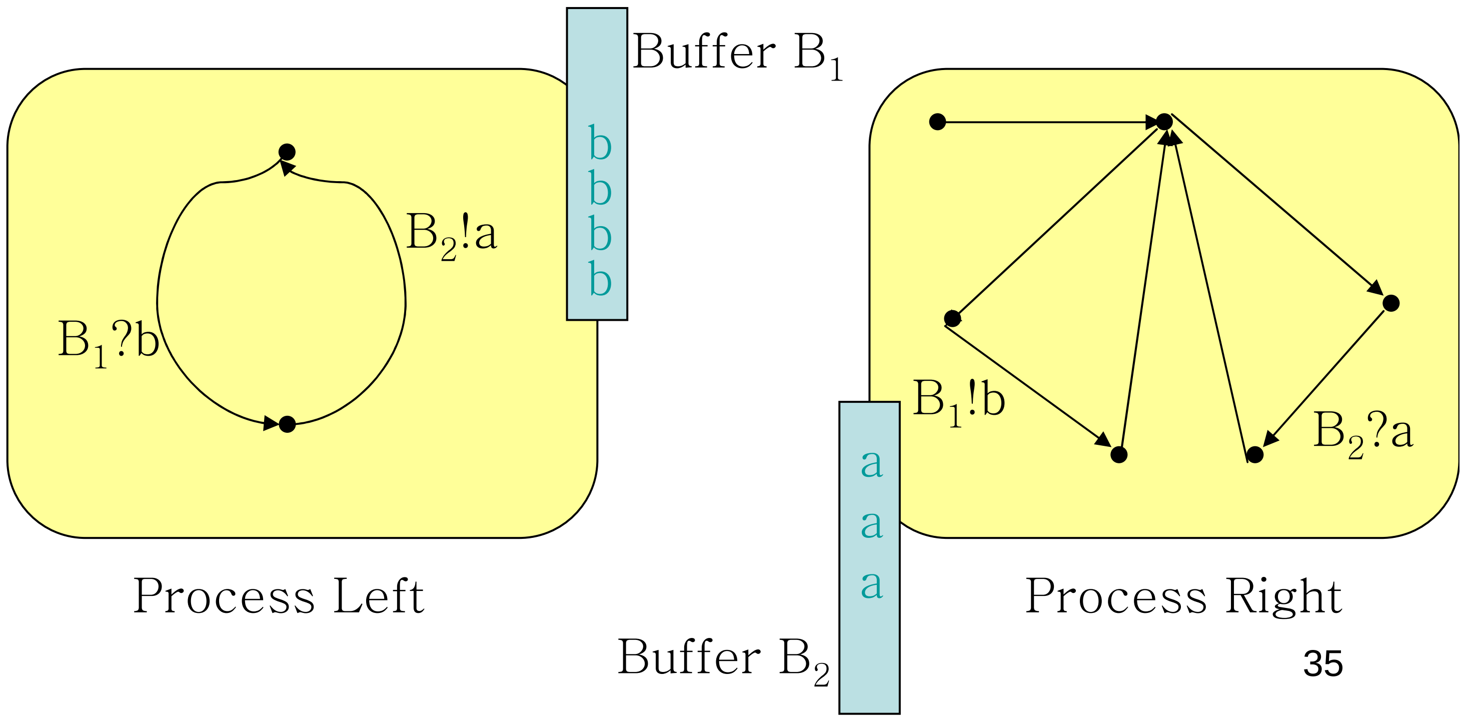


Buffer Bound Estimate

$$\max: ae_a + x_1 \times 1 + x_2 \times 0 + x_3 \times (-1)$$

$$\begin{pmatrix} ae_a \\ ae_b \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} -1 \\ 0 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$x_2 \leq x_3$$

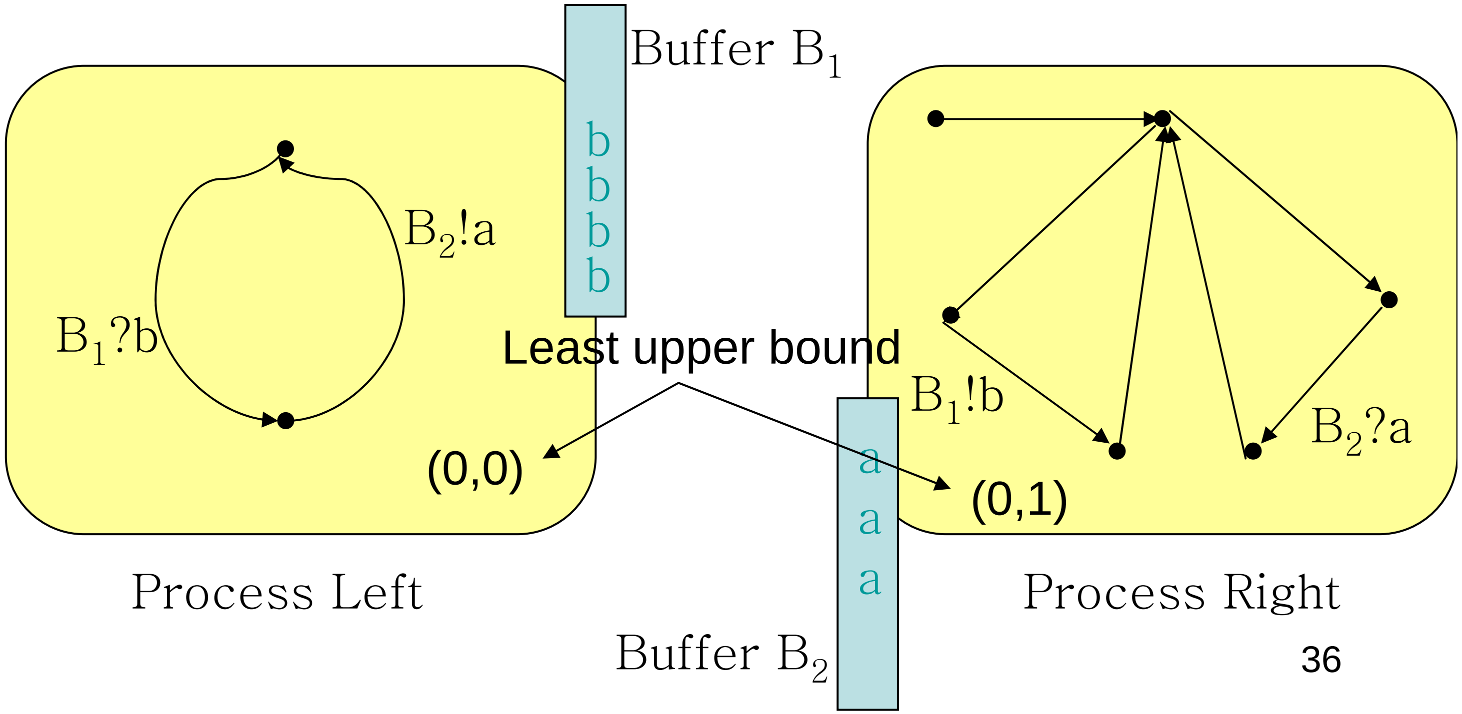


Buffer Bound Estimate

$$\max: ae_a + x_1 \times 1 + x_2 \times 0 + x_3 \times (-1)$$

$$\begin{pmatrix} ae_a \\ ae_b \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} -1 \\ 0 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$x_2 \leq x_3$$

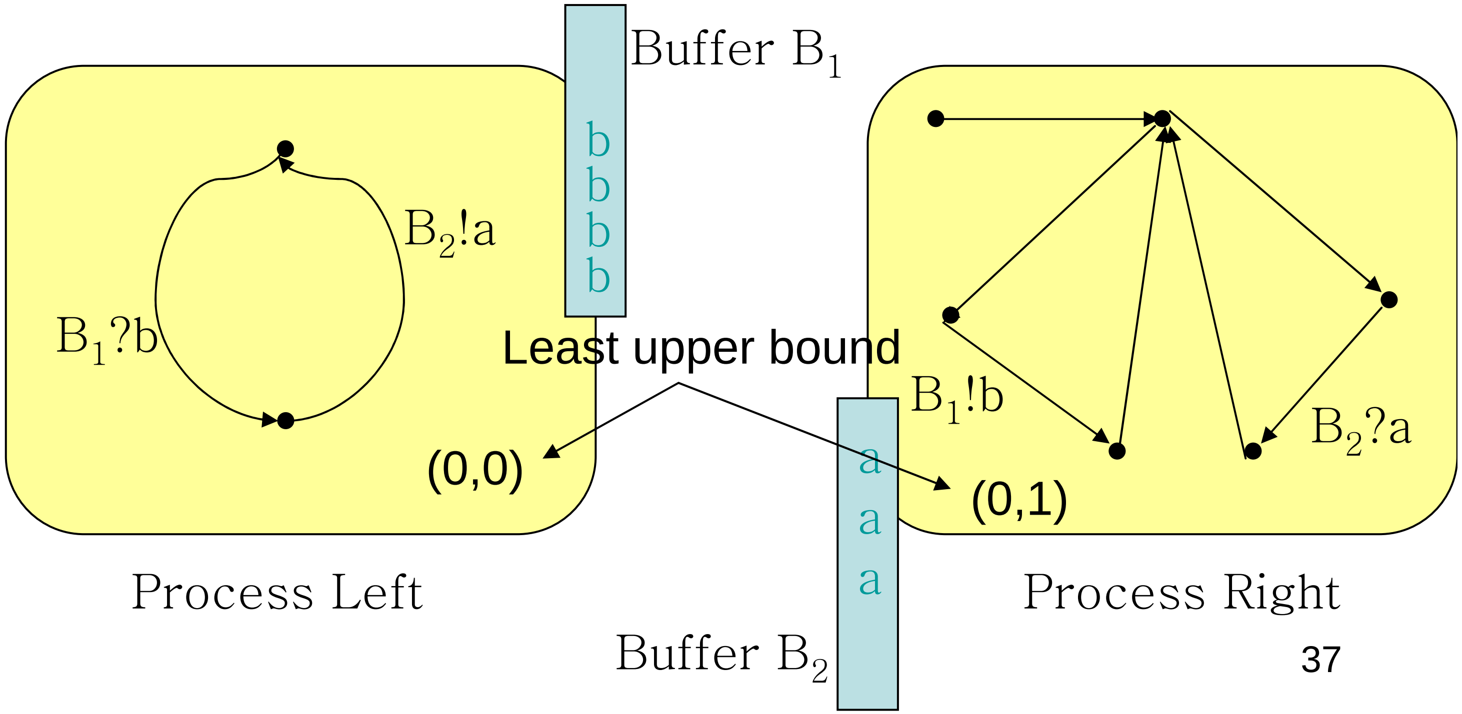


Buffer Bound Estimate

$$\max : 0 + x_1 \times 1 + x_2 \times 0 + x_3 \times (-1)$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} -1 \\ 0 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$x_2 \leq x_3$$



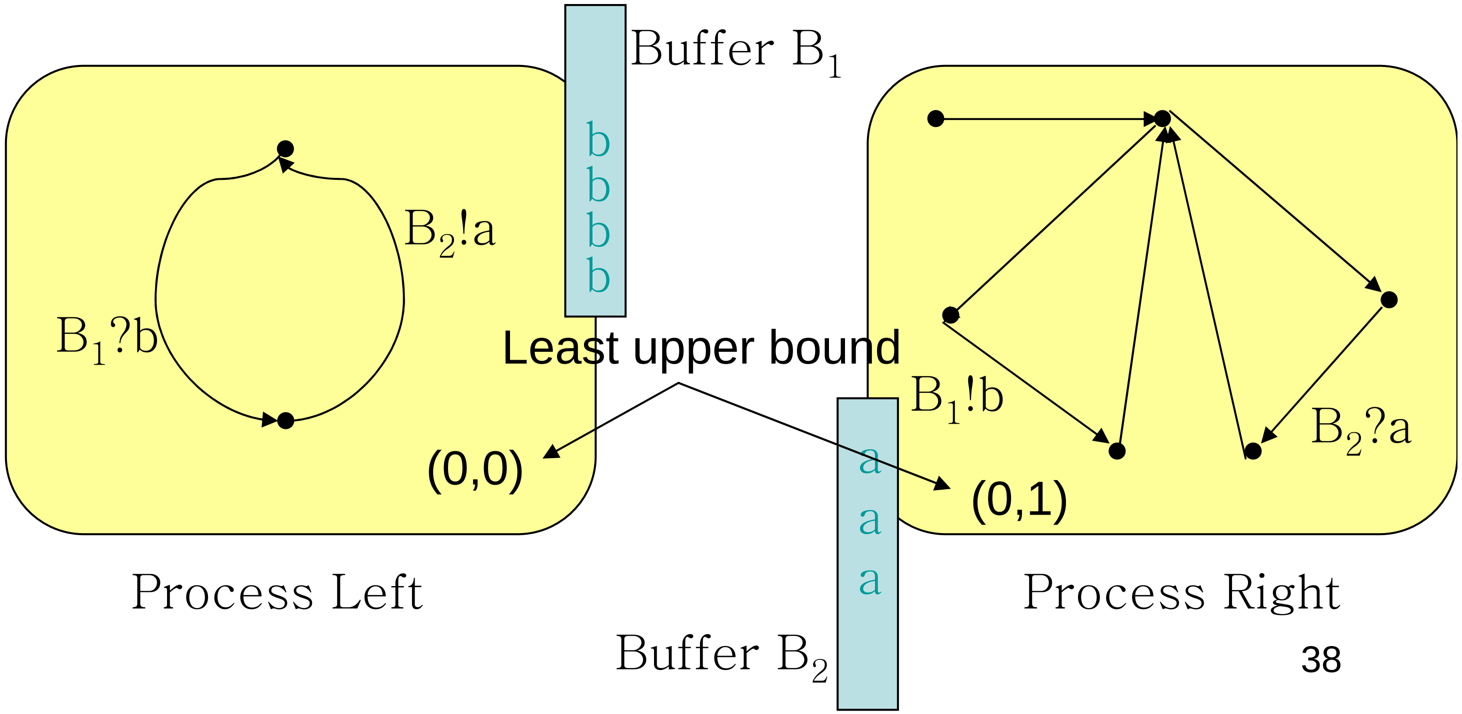
Buffer Bound Estimate

$$\max : x_1 - x_3$$

$$\begin{pmatrix}0\\1\end{pmatrix} + x_1\begin{pmatrix}1\\-1\end{pmatrix} + x_2\begin{pmatrix}0\\1\end{pmatrix} + x_3\begin{pmatrix}-1\\0\end{pmatrix} \geq \begin{pmatrix}0\\0\end{pmatrix}$$

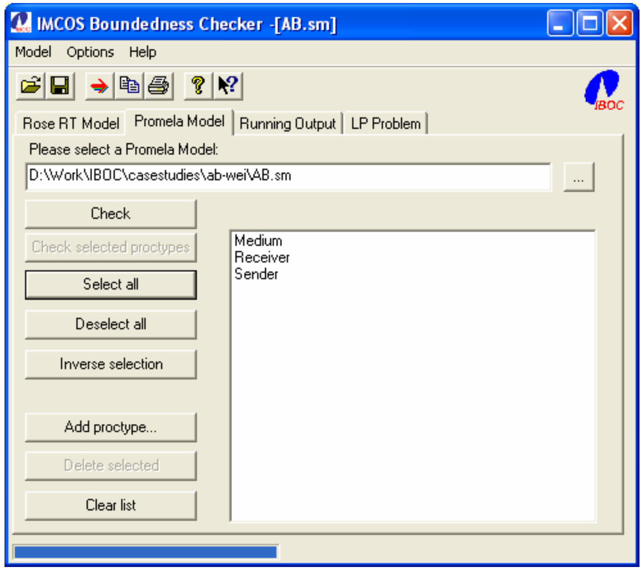
1

$$x_2 \leq x_3$$



Experimental Results

- IBOC (IMCOS Boundedness Checker)
- Tests on 31 models:
  - 8 of 31 are proved bounded without counterexamples reported.
  - 2 of 31 are proved bounded after refinement.
  - IBOC returned „UNKNOWN“ for 21 of 31.
    - 12 of 21 are truly unbounded.



Conclusion

- Buffer boundedness determination
  - Fully automated
  - Abstraction based
  - Incomplete
  - Scalable and efficient
  - Able to estimate buffer bounds
- Counterexample analyses and abstraction refinement
  - Currently only applies to Promela code

Future Work

- Improve precision of the boundedness test.
- Static code analyses for UML RT models.
- Heap boundedness for programming languages.

Thank you!