Reversal-bounded Counter Machines

Definition (Counter machine)

Let $C = \{c_1, \dots, c_n\}$ be a finite set of counters.

- A *counter machine* is a finite automaton
  $M = (\Sigma, Q, q_0, \to)$ // no final states
  with $\Sigma = \{\text{inc}, \text{dec}, \text{zero}\} \times C$.
- A *configuration* of M is a pair (q, v) with $v : C \to \mathbb{N}$.
  The *initial configuration* is $(q_0, 0)$.
- We have the following transition relation
  $\to \subseteq (Q \times \mathbb{N}^C) \times (Q \times \mathbb{N}^C)$
  between configurations:

  $(q, v) \to (q', v[c := c+1])$, if $q \xrightarrow{\text{inc}(c)} q'$.

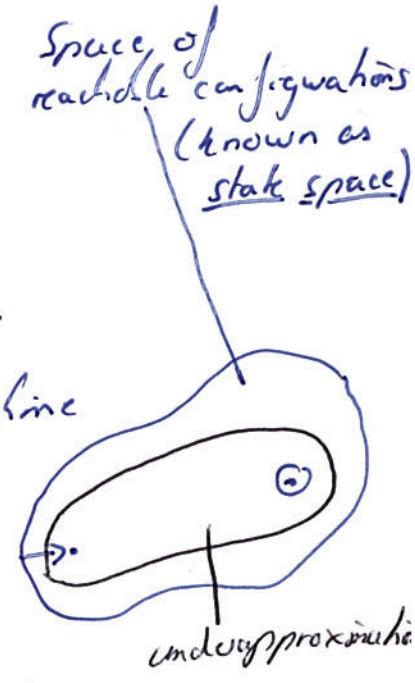
  $(q, v) \to (q', v[c := c-1])$, if $q \xrightarrow{\text{dec}(c)} q'$ and $c > 0$.

  $(q, v) \to (q', v)$, if $q \xrightarrow{\text{zero}(c)} q'$ and $c = 0$.

Note:
Counter machines are Petri nets that can actively test for zero.

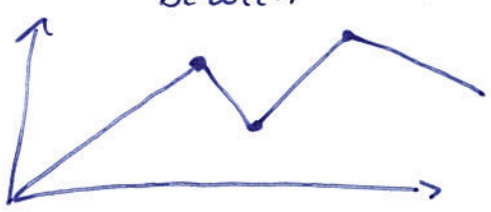
Theorem (Minsky '67)

2-counter machines are Turing-complete.

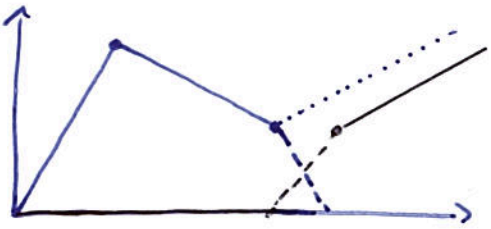


Goal: Underapproximate behaviour of a counter machine
↳ Good for bug hunting in verification
↳ Habermehl et al. CAV '06:
Programs with lists are counter automata

Idea for underapproximation: Consider only few *reversals* between increment and decrement phases.



Trick 1:
- Consider the 2-reversal behaviour of a 1-counter machine
- We compute a new machine with 2-counters having 1-reversal each.



Technically, we use states

$$Q \times \{pi, pd\} \times \{c_1, c_2\}$$

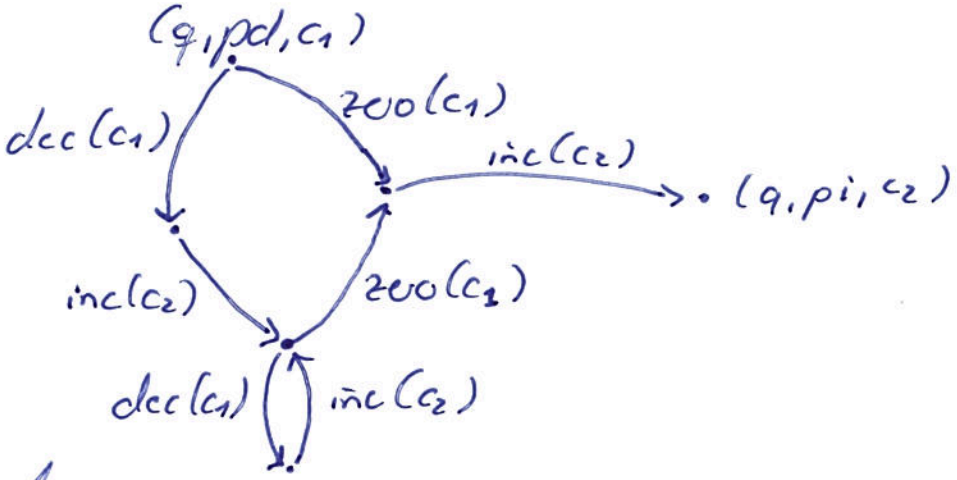
with the following meaning:

(q, pi, c_1) = increment phase of c_1, no reversal happened so far
(q, pd, c_2) = decrement phase of c_1, 1-reversal happened so far
(q, pi, c_2) = increment phase of c_2, 2-reversals happened so far

↳ To mimic a transition

$q \xrightarrow{inc(c)} q'$ in state (q, pd, c_2),

use following gadget:



In general:

Theorem (Ibarra '79)

Consider an n-counter machine where all counters do r-reversals. Then there is an $n \cdot (1 + \lfloor \frac{r}{2} \rfloor)$-counter machine so that

$(q_0, \vec{0}) \xrightarrow[r\text{-bounded}]{}^{*} (q, \vec{x})$ iff $(\tilde{q}_0, \vec{0}) \xrightarrow[1\text{-bounded}]{}^{*} (\tilde{q}, \vec{x'})$.

Idea, $x'(i, 1+\lfloor \frac{r}{2} \rfloor) = x(i)$ for all $1 \leq i \leq n$.

Moreover, $\widehat{q}$ contains pi or pd, depending on r.

Trick 2:
- Let A be an n-counter machine where all counters do 1 reversal.
- Goal is to check reachability of $(q, \bar{x})$.
- The idea is to understand A as finite automaton with initial state q_0 and final state q.
- Then
$$\mathcal{L}_{q_0,q}(A) \cap z_{00}^* . inc^* . dec^* . z_{00}^*)$$
is regular.
- So
$$\Psi(\mathcal{L}_{q_0,q}(A)) \text{ is } \exists PA\text{-definable}.$$
Moreover, the corresponding formula
$$\mathcal{C}(x_{inc(c_1)}, x_{dec(c_1)}, \ldots, x_{inc(c_n)}, x_{dec(c_n)})$$
can be computed in linear-time.
- The final configuration contains $\bar{x}$ iff
$$x_c = x_{inc(c)} - x_{dec(c)}.$$

Theorem (Ibarra '78)

A reaches $(q, \bar{x})$ iff

$$\exists x_{inc(c_1)}, x_{dec(c_1)}, \ldots, x_{inc(c_n)}, x_{dec(c_n)}:$$
$$\left(\mathcal{C}(x_{inc(c_1)}, \ldots, x_{dec(c_n)}) \wedge \bar{x} = \overline{x_{inc}} - \overline{x_{dec}}\right)$$
is satisfiable.