

# When Model-Checking Freeze LTL over Counter Machines Becomes Decidable

Stéphane Demri

LSV, ENS Cachan, CNRS, INRIA Saclay IdF

Joint work with Arnaud Sangnier(Università di Genova)

February 17th, 2010

## A fundamental model: data words

- Timed word [Alur & Dill, TCS 94]

<i>a</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>a</i>	<i>b</i>
0	0.3	1	2.3	3.5	3.51

- Runs from counter machines

$q_0$	$q_2$	$q_3$	$q_2$	$q_3$	$q_2$
0	0	1	2	3	4

- Integer arrays [Habermehl & Josif & Vojnar, FOSSACS 08]

$t[0]$   $t[1]$   $t[2]$   $t[3]$   $t[4]$   $t[5]$  ...

- Abstract data words [Bouyer & Petit & Thérien, IC 03]

- Extension to trees, e.g. data trees for XML documents  
[Bojanczyk et al, PODS 06; Jurdzinski & Lazić, LICS 07]

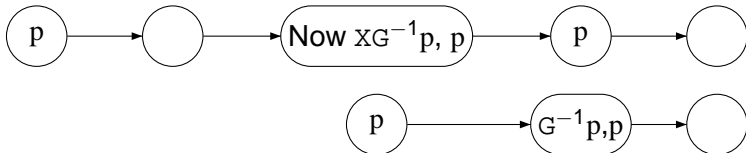
# Specifying classes of data words

- Automata
  - Register automata [Kaminski & Francez, TCS 94]
  - Data automata [Bouyer & Petit & Thérien, IC 03]
  - See the survey [Segoufin, CSL 06]
- First-order languages [Bojańczyk et al., LICS 06]
- Temporal logics
  - Real-time logic TPTL [Alur & Henzinger, JACM 94]
  - LTL with freeze [Demri & Lazić & Nowak, TIME 05]
- Many other formalisms
  - Rewriting systems with data [Bouajjani et al., FCT 07]
  - Hybrid logics [Schwentick & Weber, STACS 07]
  - ...

# Memoryful temporal logics

- Real-time logic TPTL [Alur & Henzinger, JACM 94]
- MTL [Koymans, RTS 90]
  - Fin. MTL is decidable [Ouaknine & Worrell, LICS 05]
  - Inf. MTL is undecidable [Ouaknine & Worrell, FOSSACS 06]
- LTL with forgettable past [Laroussinie & Markey & Schnoebelen, LICS 02]

Effect of Now  $\phi$ : register the current position as the origin and then evaluate  $\phi$ .



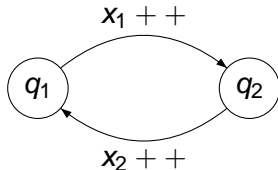
# Motivations

- Model-checking with focus on data values
  - 1 To analyze runs of operational models with focus on data values (beyond control-state reachability).
  - 2 Model-checking rather than satisfiability.
- Current instance:
  - Operational models: classes of counter machines for which the reachability problem is decidable.  
(most often, the reachability sets are definable in Presburger arithmetic.)
  - Specification language: LTL with registers.
- The models can be quite simple but memoryful logics are expressive, see e.g. results on one-counter machines.

# Outline

- 1 LTL with registers (a.k.a. Freeze LTL)
- 2 Preliminary results
- 3 Reversal-bounded counter machines
- 4 Flat fragments
- 5 Conclusion

# Counter machines



- $M = (n, Q, \Delta, q_i)$ 
  - Finite set of control states  $Q$  and initial control state  $q_i$ .
  - Set of transitions  $\Delta \subseteq Q \times G \times A \times Q$  with  $G = \{\text{zero}, \text{true}\}^n$  and  $A = \{-1, 0, 1\}^n$ .

- Runs of the form

$$\rho = \begin{array}{l} q_0 = q_i \\ \mathbf{v}_0 = \mathbf{0} \end{array} \rightarrow \begin{array}{l} q_1 (\in Q) \\ \mathbf{v}_1 (\in \mathbb{N}^n) \end{array} \rightarrow \begin{array}{l} q_2 \\ \mathbf{v}_2 \end{array} \rightarrow \dots$$

- We consider all infinite runs (no accepting conditions) but formulae will constraint them.

# LTL with registers

- $LTL^\downarrow[Q, n]$  formulae:

$$\phi ::= q \mid \downarrow_r^c \phi \mid \uparrow_r^c \phi \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid X\phi \mid \phi U \phi \mid \phi R \phi$$

where  $c$  is a counter and  $r \in \mathbb{N} \setminus \{0\}$  is a register.

- Models of  $LTL^\downarrow[Q, n]$  are infinite data words with finite alphabet  $Q$  and infinite domain  $\mathbb{N}^n$ .

$$\begin{array}{ccccccccc} q_0 & q_1 & q_2 & q_3 & q_4 & q_5 & \cdots \\ \mathbf{0} & \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 & \mathbf{v}_4 & \mathbf{v}_5 & \cdots \end{array}$$

- Register valuation  $f$ : (partial) map from  $\mathbb{N} \setminus \{0\}$  to  $\mathbb{N}$ .

# Satisfaction relation (standard for temporal part)

$$\begin{array}{ll}
 \rho, i \models_f q & \stackrel{\text{def}}{\Leftrightarrow} q_i = q \\
 \rho, i \models_f \downarrow_r^c \phi & \stackrel{\text{def}}{\Leftrightarrow} \rho, i \models_{f[r \mapsto \mathbf{v}_i(c)]} \phi \\
 \rho, i \models_f \uparrow_r^c & \stackrel{\text{def}}{\Leftrightarrow} r \in \text{dom}(f) \text{ and } f(r) = \mathbf{v}_i(c) \\
 \rho, i \models_f \mathbf{X}\phi & \stackrel{\text{def}}{\Leftrightarrow} i + 1 < |\rho| \text{ and } \rho, i + 1 \models_f \phi \\
 \rho, i \models_f \phi_1 \mathbf{U} \phi_2 & \stackrel{\text{def}}{\Leftrightarrow} \text{for some } i \leq j < |\rho|, \rho, j \models_f \phi_2 \\
 & \text{and for all } i \leq j' < j, \text{ we have } \rho, j' \models_f \phi_1 \\
 \rho, i \models_f \phi_1 \mathbf{R} \phi_2 & \stackrel{\text{def}}{\Leftrightarrow} \text{for all } i \leq j < |\rho|, \rho, j \models_f \phi_2 \\
 & \text{or for some } i \leq j < |\rho|, \rho, j \models_f \phi_1 \\
 & \text{and for all } i \leq k \leq j, \rho, k \models_f \phi_2
 \end{array}$$

Standard abbreviations  $\mathbf{F}$ ,  $\mathbf{G}$ , etc.

## Examples with one-counter machines

- There is a suffix such that all counter values are different

$$FG(\downarrow_1^1 \ XG\neg \uparrow_1^1)$$

$q_0$	$q_2$	$q_3$	$q_2$	$q_3$	$q_2$	$q_2 \dots$
0	0	1	2	3	4	5...

- Whenever location  $q$  is reached with current counter value  $n$  and next current counter value  $m$ , if there is a next occurrence of  $q$ , the two consecutive counter values are also  $n$  and  $m$

$$G(q \Rightarrow \downarrow_1^1 \ X \downarrow_2^1 \ XG(q \Rightarrow \uparrow_1^1 \ \wedge \ X \uparrow_2^1))$$

$q$	$q'$	$q'$	$q$	$q'$	$q''$	$q'' \dots$
50	60	1	50	60	4	5...

# Model checking problems

- Infinitary model-checking problem  $\text{MC}^\omega(\text{LTL}^\downarrow[\cdot, \cdot])$ :  
**Input:**  $M = (n, Q', \Delta, q_i)$ , sentence  $\phi \in \text{LTL}^\downarrow[Q, n]$   
with  $Q \subseteq Q'$ ;  
**Question:** Is there an infinite run  $\rho$  such that  $\rho, 0 \models \phi$ ?
- A value is repeated infinitely often in all counters:

$$\downarrow_1^1 \left( \text{GF} \bigwedge_{i=1}^{i=n} \uparrow_1^i \right)$$

- $\text{MC}^\omega(\text{LTL}^{\downarrow, s}[\cdot, \cdot])$ : restriction to formulae for which each register is attached to a unique counter.
- $\text{MC}^\omega(\text{LTL}[\cdot])$ : restriction to formulae with no registers.

# Complexity of satisfiability problems

- LTL with registers [Demri & Lazić, LICS 06]
  - $LTL_1^\downarrow$  restricted to  $X$  and  $F$  is undecidable over infinite data words.
  - $LTL_1^\downarrow$  is decidable over finite data words.  
(but non-primitive recursive using [Schnoebelen, IPL 02])
  - $LTL_2^\downarrow$  is undecidable over finite data words.
  - See preliminary undecidability results in  
[(Demri & Lazić & Nowak; Lisitsa & Potapov), TIME 05]
- FO over data words [Bojanczyk et al., LICS 06]
  - $FO3(\sim, <, +1)$  is undecidable.
  - $FO2(\sim, <, +1)$  is decidable over finite/infinite data words.  
(roughly equivalent to reachability problem for Petri nets)

# Preliminary results

# Complexity results for one-counter machines

[Demri & Lazić & Sangnier, FOSSACS 08]

- Deterministic one-counter machines:  $\text{MC}(\text{FO})$  and  $\text{MC}(\text{LTL})$  are PSPACE-complete.
- Undecidability for nondeterministic one-counter machines:
  - $\text{MC}^{<\omega}(\text{LTL}_1^\downarrow(X, F))$  and  $\text{MC}(\text{FO})_2^{<\omega}$  are  $\Sigma_1^0$ -complete.
  - $\text{MC}^\omega(\text{LTL}_1^\downarrow(X, F))$  and  $\text{MC}(\text{FO})_2^\omega$  are  $\Sigma_1^1$ -complete.
- Reachability sets are semilinear but universal problem for one-counter machines with alphabet is undecidable.

# Classes with decidable reachability problem

- One-counter machines (with semilinear reachability sets).
- Flat counter machines (with semilinear reachability sets):
  - Flatness: each control state belongs to at most one simple cycle.
  - At most one transition between two control states.

[Finkel & Leroux, FSTTCS 02]

- Vector addition systems with states.

[Mayr, STOC 81; Kosaraju, STOC 82; Reutenauer, 89]

See also [Leroux, LICS 09]

## (Ibarra) Reversal-bounded counter machines

- Reversal: Alternation from nonincreasing mode to nondecreasing mode and vice-versa.
- Sequence with 3 reversals:

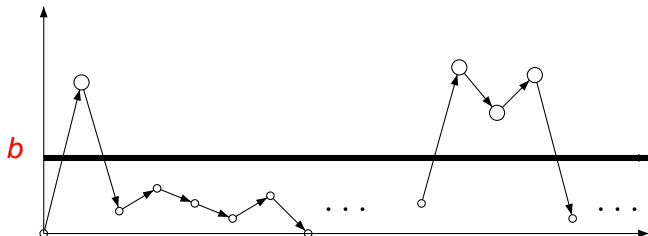
0011223334444 $\bar{3}$ 33222 $\bar{3}$ 33444455555 $\bar{4}$

- Ibarra reversal-bounded counter machines: each run has a bounded number of reversals [Ibarra, JACM 78].
- Reachability and generalized repeated control state reachability are decidable problems.

[Dang & Ibarra & San Pietro, FSTTCS 01]

# Reversal-bounded counter machines

[Finkel & Sangnier, MFCS 08]



- Reversal-bounded counter machines: bounded number of reversals above a bound. [Finkel & Sangnier, MFCS 08]
- Reachability and generalized repeated control state reachability are decidable problems. [Sangnier, PhD 08]  
(below  $b$ , counter values are encoded in control states)

## Standard restriction with no registers

$MC^\omega(\text{LTL}[\cdot])$  restricted to one-counter machines, VASS, and reversal-bounded counter machines is decidable.

- Proof sketch (with standard technique):
  - Make product between the counter machine and the LTL formula.
  - The generalized repeated control state reachability problem is known to be decidable for these classes.
- $MC^\omega(\text{LTL}[\cdot])$  for VASS is EXPSPACE-complete.  
[Habermehl, ICATPN 97]
- $MC^\omega(\text{LTL}[\cdot])$  for 1CM is PSPACE-complete.  
See e.g. [Demri & Gascon, TIME 07]

## Another restriction: flat counter machines

$MC^\omega(\text{LTL}^\downarrow[\cdot, \cdot])$  restricted to flat CM is decidable.

- Flat CM  $M = (n, Q, \Delta, q_0)$ ,  $\phi \in \text{LTL}^\downarrow[Q, n]$ .
- Decidability by translating  $\phi$  into temporal logic FOCTL<sup>\*</sup>(Pr) and then use [Demri et al., ATVA 06].
- $E \text{ t}(\phi; (z_1, \dots, z_N))$ 
  - $\text{t}(\cdot)$  is homomorphic for connectives,
  - $\text{t}(\uparrow_r^c, (z_1, \dots, z_N)) \stackrel{\text{def}}{=} (z_r = x_c)$ ,  
( $x_c$  is variable associated to counter  $c$ )
  - $\text{t}(\downarrow_r^c \psi; (z_1, \dots, z_N)) \stackrel{\text{def}}{=} \exists z'_r (z'_r = x_c \wedge \text{t}(\psi; (z_1, \dots, z'_r, \dots, z_N)))$ .
- $M \models^\omega \phi$  iff  $M \models^\omega \phi'$ .

# Reversal-bounded counter machines

# Undecidability for RB

$MC^\omega(\text{LTL}^\downarrow[\cdot, 4])$  restricted to reversal-bounded CM and to formulae with at most one register is undecidable.

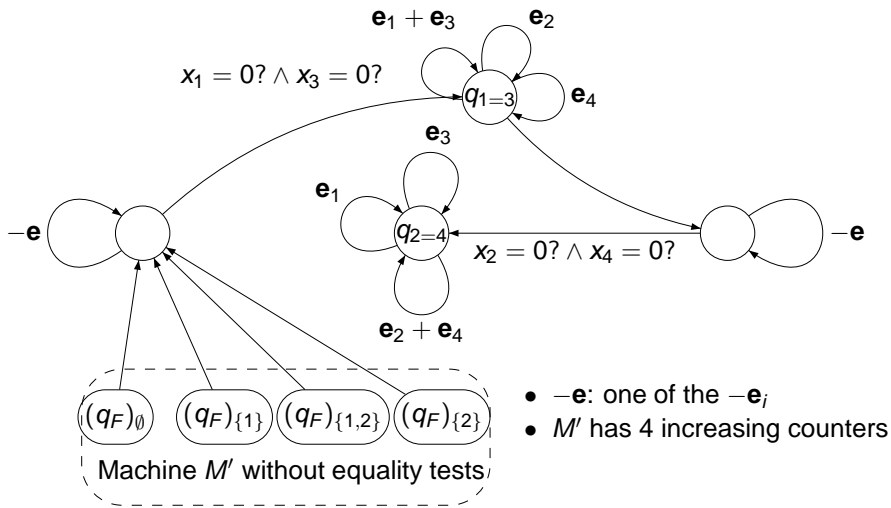
- Similar to proof for undecidability of reachability problem for reversal-bounded counter machines augmented with guards  $c = c'$ ,  $c \neq c'$  [Ibarra et al., TCS 02].
- Each counter  $c$  from Minsky machine provides two increasing counters  $c^{inc}$  and  $c^{dec}$ .
- Zero-test for  $c$  is performed by a test  $c^{inc} = c^{dec}$ , logically equivalent to  $\downarrow_1^{c^{dec}} \uparrow_1^{c^{inc}}$ .
- What about undecidability for strict fragment?  
(each register is attached to a unique counter)

# Undecidability with strict fragment

$MC^\omega(\text{LTL}^{\downarrow, s}[\cdot, 4])$  restricted to reversal-bounded counter machines is undecidable too.

- Let us encode halting problem for Minsky machine  $M$  with counters 1 and 2.
- Counter  $i$  uses two increasing counters  $i$  and  $i + 2$  as in the previous proof.
- Equality tests are performed after reaching the final state.

# 4-reversal-bounded counter machine



# Specifications

$$\phi' = \mathbb{F}q_{2=4} \wedge \bigwedge_{c \in \{1,2\}} \mathbb{G} \left( \downarrow_c^c \downarrow_{c+2}^{c+2} (\text{zerotest}(c) \Rightarrow \mathbb{F}(q_{c=c+2} \wedge \uparrow_c^c \wedge \uparrow_{c+2}^{c+2})) \right)$$

$$\wedge \phi_{\text{dec}} \wedge \phi_{\text{fair}}$$

( $\Downarrow \psi$  stands for  $\downarrow_1^1 \downarrow_2^2 \downarrow_3^3 \downarrow_4^4 \psi$ )

$$\phi_{\text{fair}} \stackrel{\text{def}}{=} \mathbb{G} \bigwedge_{q \in Q'} (q \Rightarrow \Downarrow (\mathbb{F}(q_{1=3} \wedge \uparrow_2^2 \wedge \uparrow_4^4 \wedge \uparrow_1^1) \wedge \mathbb{F}(q_{2=4} \wedge \uparrow_1^1 \wedge \uparrow_3^3 \wedge \uparrow_2^2))))$$

$$\phi_{\text{dec}} = \bigwedge_{c \in \{1,2\}} \mathbb{G} \left( \bigwedge_{(q, \text{true}, -\mathbf{e}_c, q') \in \Delta} q_{\emptyset} \wedge \mathbb{X} \phi_{q'} \Rightarrow \Downarrow \neg \mathbb{F}(q_{c=c+2} \wedge \uparrow_1^1 \cdots \wedge \uparrow_4^4) \right)$$

# Flat fragments

## Flat fragment of $LTL^{\downarrow}[Q, n]$

- Pos. occurrence of  $\phi_1 U \phi_2$  implies  $\downarrow$  does not occur in  $\phi_1$ .  
Neg. occurrence of  $\phi_1 U \phi_2$  implies  $\downarrow$  does not occur in  $\phi_2$ .  
(similar conditions with  $R$ )
- $\neg(q U \downarrow_1^1 \phi)$  is not a flat formula.
- A formula is positively flat when it is flat and no occurrence of  $\uparrow$  is negative (no inequality tests).
- Example:  $F \downarrow_1^1 [(GF \uparrow_1^2 \Leftrightarrow GF \uparrow_1^3) \wedge FG \uparrow_1^4]$ .
- Flatness is a standard means to regain decidability for memoryful linear-time temporal logics.

## We need CM with parameterized tests!

- $M = (n, Q, \Delta, q_0, Z)$  with  $Z$  a finite set of integer variables.
- Set of guards:

$$(\{\text{zero}, \text{true}\} \cup \{=(z), \neq(z), >(z), <(z) \mid z \in Z\})^n$$

- Concretization  $C: Z \rightarrow \mathbb{N}$ .
- Each concretization  $C$  provides a transition system  $TS(M, C)$  and runs.
- Restricted counter machines with parameterized tests: no guard of the form either  $\neq(z)$  or  $<(z)$ .

# Reachability problems

- Parameterized reachability problem (PRP):
  - Input:** parameterized counter machine  $M$  and  $\langle q, \mathbf{v} \rangle$ .
  - Question:** is there  $C$  s.t.  $\langle q_0, \mathbf{0} \rangle \xrightarrow{*} \langle q, \mathbf{v} \rangle$  in  $TS(M, C)$ ?
- PRP for Ibarra reversal-bounded parameterized counter machines is decidable. [Ibarra et al., TCS 02]
- PRP for restricted parameterized 1CM is decidable. [Haase et al., CONCUR 09]
- Parameterized generalized repeated reachability problem:
  - Input:** parameterized CM  $M, F_1, \dots, F_N$ .
  - Question:** are there  $C$  and an infinite run of  $TS(M, C)$  s.t. for  $1 \leq i \leq N$ , one control state in  $F_i$  is repeated  $\infty$  often?

# Parameterized generalized repeated reachability problem is decidable ...

- 1 for restricted parameterized 1CM, use [Haase et al., CONCUR 09] and Dickson's Lemma.
- 2 for Ibarra reversal-bounded parameterized CM, use [Ibarra et al., TCS 02] and Dickson's Lemma.
- 3 for reversal-bounded parameterized CM, use simulation from [Sangnier, PhD 08] and point (2).

## When flatness meets parameterization

There is a reduction from  $MC^\omega(LTL^\downarrow[\cdot, \cdot])$  restricted to flat formulae to the parameterized generalized repeated reachability problem for counter machines.

- Flatness guarantees that only a bounded amount of counter values need to be stored.
- These values are captured by a concretization (via parameters).
- A product is done between the counter machine and the Büchi automaton obtained from flat formula.
- The reduction is in polynomial-space and the number of parameters is linear in the size of the flat formula.

## Final reward

- Exponential-time reduction from  $MC^\omega(LTL^\downarrow[\cdot, \cdot])$  restricted to reversal-bounded CM into  $MC^\omega(LTL^\downarrow[\cdot, \cdot])$  restricted to Ibarra reversal-bounded CM and it preserves flatness.

$MC^\omega(LTL^\downarrow[\cdot, \cdot])$  restricted to reversal-bounded CM and to flat formulae is decidable.

$MC^\omega(LTL^\downarrow[\cdot, \cdot])$  restricted to 1CM and to positively flat formulae is decidable.

(decidability status of PRP for parameterized 1CM is open)

# Summary

	Det.	NDet.	Flatness	No $\uparrow_r^c$
RB	<b>D</b>	<b>U</b> (strict)	<b>D</b>	<b>D</b>
1CM	PSPACE-C.	U (1 reg.)	?   <b>D</b> with positivity	PSPACE-C.
Flat CM	<b>D</b>	<b>D</b>	<b>D</b>	<b>D</b>
VASS	<b>EXPSpace</b>	<b>U</b> (1 reg.)	<b>U</b>	<b>EXPSpace-C.</b>

## Concluding remarks

- A few rules of thumb :
  - 1 Determinism, flat CM and no freeze lead to decidability.
  - 2 Flat formulae often guarantee decidability (except for VASS).
  - 3 Throwing away the atomic formulae made of control states does not help for decidability (a.k.a. purification).
- Open problems:
  - 1 Complete the complexity characterization.
  - 2 Is  $MC^\omega(\text{LTL}^\downarrow[\cdot, \cdot])$  restricted to 1CM and flat formulae decidable?
  - 3 Probably, related to decidability status of PRP for parameterized 1CM.
  - 4 Analysis for other classes of models.