Reasoning about data repetitions with counter systems

S. Demri

Joint work with D. Figueira and M. Praveen

Workshop LIA INFINIS, IRIF, Nov. 2016
Logics for Data Words
A fundamental model: data words

- Timed words

  $a \ b \ c \ a \ a \ b$
  $0 \ 0.3 \ 1 \ 2.3 \ 3.5 \ 3.51$

- Runs from counter machines

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

- Integer arrays


- Abstract data words

  [Bouyer & Petit & Thérien, IC 03]

- Extension to trees, e.g. data trees for XML documents

  [Bojańczyk et al., PODS’06; Jurdziński & Lazić, LICS’07]
Specifying classes of data words

- **Automata**
  - Register automata [Kaminski & Francez, TCS 94]
  - Data automata [Bouyer & Petit & Thérien, IC 03]
  - EES automata [Choffrut & Grigorieff, TCS 09]
  - See the survey [Segoufin, CSL’06]

- **First-order languages** [Bojańczyk et al., LICS’06]

- **Temporal logics**
  - Temporal logic with $\lambda$-abstraction [Lisitsa & Potapov, TIME’05]
  - Freeze LTL [Demri & Lazić & Nowak, IC 07]
  - BD-LTL [Kara & Schwentick & Zeume, FSTTCS’10]

- **Many other formalisms**
  - Rewriting systems with data [Bouajjani et al., FCT’07]
  - Hybrid logics [Areces & Blackburn & Marx, JSL 01]
  - Memory logics [Areces et al., TABLEAUX’09; Mera, PhD thesis 2009]
  - ...
A mechanism for handling data

- A register can store a data value and equality tests are performed between registers and current data values.

- Storing the value of $x$ in a register:

  $$\downarrow_r \phi \approx \exists y_r (y_r = x) \land \phi$$

- Equality test between a register and a value: $\uparrow_r \approx y_r = x$.

- Generalisation with memory logics, e.g. memory bags have operations “register”, “forget” and “erase”.

  \[ \models \downarrow_r F(a \land \uparrow_r \land XF \uparrow_r) \]

[Mera, PhD thesis 09]
Ubiquity of the freeze operator

▶ Freeze quantifier in hybrid logics.
   [Goranko 94; Blackburn & Seligman, JOLLI 95]

▶ Temporal semantics of imperative programs.
   [Manna & Pnueli, 1992]
   Program variable $x$ never decreases below its initial value:
   $$\exists y \ (x = y) \land G(x \geq y)$$

▶ Freeze quantifier in real-time logics.
   [Alur & Henzinger, JACM 94]
   $y \cdot \phi(y)$ binds the variable $y$ to the current time $t$.

▶ Predicate $\lambda$-abstraction.
   [Fitting, JLC 02]
   $\langle y \cdot F P(y) \rangle(c)$: current value of constant $c$ satisfies the predicate $P$. 
Freeze LTL: $\text{LTL}^\downarrow$

- **LTL$^\downarrow$ formulae:**

  $$\phi ::= a \mid \uparrow_r \mid \neg \phi \mid \phi \land \phi \mid \phi \lor \phi \mid \phi U \phi \mid X \phi \mid \downarrow_r \phi$$

  where $a \in \Sigma$ and $r \in \mathbb{N}^+$. 

- **Register valuation $f$:** finite partial map from $\mathbb{N}^+$ to $\mathbb{N}$.

- **Models:** finite or infinite data words over the alphabet $\Sigma$.

- **Satisfaction relation:**

  $$\mathcal{d}w, i \models_f \uparrow_r \iff r \in \text{dom}(f) \text{ and } f(r) = \mathcal{d}_i$$

  $$\mathcal{d}w, i \models_f \downarrow_r \phi \iff \mathcal{d}w, i \models_f[r \mapsto \mathcal{d}_i] \phi$$

  ($\mathcal{d}_i$: data value at position $i$)
Complexity of satisfiability problems

- Finitary and infinitary satisfiability problem for LTL are \( \text{PSPACE-complete} \).  
  \[ \text{[Sistla & Clarke, JACM 85]} \]

- Infinitary satisfiability problem for \( \text{LTL} \downarrow \) restricted to \( X \) and \( F \) and to a single register is undecidable.

- Finitary satisfiability problem for \( \text{LTL} \downarrow \) restricted to a single register is decidable but nonprimitive recursive.  
  \[ \text{[Demri & Lazić, TOCL 09]} \]
  (nonprimitive recursiveness uses \[ \text{[Schnoebelen, IPL 02]} \])

- Finitary satisfiability problem for \( \text{LTL} \downarrow \) restricted to \( F \) and to a single register is nonprimitive recursive too.
  - to a single register is nonprimitive recursive too.
  - to two registers is undecidable.  
  \[ \text{[Figueira & Segoufin, MFCS’09]} \]
A Logic for Repeating Values
Models & basic constraints

- \( \sigma : [0, \ell - 1] \rightarrow (\text{VAR} \rightarrow \mathbb{N}) \), \( \ell \geq 1 \):

\[
\begin{array}{cccccccccc}
x & 9 & 0 & 4 & 8 & 4 & 4 & 4 & 2 & 1 \\
y & 7 & 9 & 7 & 5 & 7 & 5 & 4 & 2 & 9 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
z & 8 & 4 & 2 & 4 & 8 & 4 & 2 & 4 & 4 \\
\end{array}
\]

- Local constraints:

\[
x \approx X_y \quad \neg(x \approx X^2_y) \quad \neg(z \approx Xz)
\]

\[
\downarrow^x_1 X \uparrow^y_1 \quad \neg \downarrow^x_1 X^2 \uparrow^y_1 \quad \neg \downarrow^z_1 X \uparrow^z_1
\]

- Global (repeating) constraints:

\[
x \approx \langle \top? \rangle_y \quad y \approx \langle \phi? \rangle_y
\]

\[
\downarrow^x_1 XF(\top \land \uparrow^y_1) \quad \downarrow^y_1 XF(\phi \land \uparrow^y_1)
\]

- + standard LTL operators.
Syntax & semantics

$$\phi ::= x \approx X^i_y \mid x \approx \langle \phi? \rangle_y \mid x \not\approx \langle \phi? \rangle_y \mid \phi \land \phi \mid \neg \phi \mid X\phi \mid \phi \cup \phi \mid X^{-1}\phi \mid \phi S \phi$$

$$\sigma, i \models x \approx X^i_y \text{ iff } i + j < |\sigma| \text{ and } \sigma(i)(x) = \sigma(i + j)(y)$$

$$\sigma, i \models x \approx \langle \phi? \rangle_y \text{ iff } \text{there exists } j \text{ such that } i < j < |\sigma|, \sigma(i)(x) = \sigma(j)(y) \text{ and } \sigma, j \models \phi$$

$$\sigma, i \models x \not\approx \langle \phi? \rangle_y \text{ iff } \text{there exists } j \text{ such that } i < j < |\sigma|, \sigma(i)(x) \neq \sigma(j)(y) \text{ and } \sigma, j \models \phi$$

$$\sigma, i \models X\phi \text{ iff } i + 1 < |\sigma| \text{ and } \sigma, i + 1 \models \phi$$

$$\sigma, i \models \phi S \phi' \text{ iff } \text{there is } 0 \leq j \leq i \text{ such that } \sigma, j \models \phi' \text{ and for every } j < l \leq i \text{ we have } \sigma, l \models \phi.$$
Related work

- Decidability of SAT(LRV\(\top\)) by translation into the reachability problem for VASS.  
  [Demri & D’Souza & Gascon, JLC 09]

- Satisfiability for FO2 “equivalent” to the reachability problem for VASS.  
  [Bojańczyk et al., LICS’06]

- Satisfiability of basic data LTL “equivalent” to the reachability problem for VASS.  
  [Kara & Schwentick & Zeume, FST&TCS’10]

- Basic data LTL BD-LTL\(^+\) extends LRV and in 2\(\text{EXPSPACE}\).  
  [Decker et al., CONCUR’14]
Repeating Values and Counting
Restricting test formulae to $\top$

- There is a polynomial-time reduction from $\text{SAT}(\text{LRV})$ into $\text{SAT}(\text{LRV} \approx)$.

- Introduction of variables to eliminate the subformulae of the form $x \not\approx \langle \psi \rangle_y$ and $\neg(x \not\approx \langle \psi \rangle_y)$.

- There is a polynomial-time reduction from $\text{SAT}(\text{LRV} \approx)$ to $\text{SAT}(\text{LRV}^\top)$. 
From satisfiability to reachability

- Vector addition systems with states (VASS).

Reachability problem: \( \langle q_0, 0 \rangle \rightarrow^* \langle q_f, 0 \rangle \)?
Control state reachability: \( \langle q_0, 0 \rangle \rightarrow^* \langle q_f, x \rangle \) for some \( x \)?

- \( \phi \in \text{LRV}^\top \) is satisfiable iff \( \langle q_0, 0 \rangle \rightarrow^* \langle q_f, 0 \rangle \) in \( A_\phi \).

- \( x \approx \langle \top\rangle_y \wedge x \approx \langle \top\rangle_z \wedge \neg(x \approx X_y) \wedge \neg(x \approx X_z) \) creates an obligation for the current value of \( x \) to appear on \( y \) and on \( z \).

- Increment the counter \( \{y, z\} \).

- Decrement the counter \( \{y, z\} \) when the obligation is satisfied, even partially.
From reachability to control state reachability

- \( \phi \in LRV^T \) is satisfiable iff \( \langle q_0, 0 \rangle \xrightarrow{*} \langle q_f, 0 \rangle \) in \( A_\phi \).
  (bookkeeping of obligations)

- \( \langle q_0, 0 \rangle \xrightarrow{*} \langle q_f, 0 \rangle \) in \( A_\phi \) iff \( \langle q_0, 0 \rangle \xrightarrow{\text{gainy}} \langle q_f, 0 \rangle \) in \( A_{\text{inc}} \).
  (structural properties of \( A_\phi, A_{\text{inc}} \) slight variant of \( A_\phi \))

- \( \langle q_0, 0 \rangle \xrightarrow{\text{gainy}} \langle q_f, 0 \rangle \) in \( A_{\text{inc}} \) iff \( \langle q_f, 0 \rangle \xrightarrow{\text{lossy}} \langle q_0, 0 \rangle \) in \( A_{\text{dec}} \).
  = reverse of \( A_{\text{inc}} \). –by the reverse construction.

- \( \langle q_f, 0 \rangle \xrightarrow{\text{lossy}} \langle q_0, 0 \rangle \) in \( A_{\text{dec}} \) \( \langle q_f, 0 \rangle \xrightarrow{*} \langle q_0, x \rangle \) in \( A_{\text{dec}} \) for some \( x \).
  –losses can be moved to the end.

- \( 2\text{EXPSPACE} \): control state reachability for VASS is in \( \text{EXPSPACE} \) and \( |A_{\text{dec}}| \in \mathcal{O}(2^p(|\phi|)) \) – use of [Rackoff, TCS 78].
Counter systems with chained counters

- VASS $\approx$ FSA with $n$ counters, no zero-tests but increments and decrements.

- Chain system $\approx$ FSA with $n$ chains of counters of exponential length and access to counters via pointers.

\[ C_0 \ C_1 \ \cdots \ C_{i-1} \ C_i \ C_{i+1} \ \cdots \ C_{2^N-1} \]

- Updates and guards on transitions ($\alpha \in [1, n]$):
  \{inc($\alpha$), dec($\alpha$), next($\alpha$), prev($\alpha$), first($\alpha$)?, first($\overline{\alpha}$)?, last($\alpha$)?, last($\overline{\alpha}$)?\}

- Control-state reachability problem for chain systems is in $2\text{EXPSPACE}$. (EXPSPACE-complete for VASS)

- Chain system $\approx$ VASS with a succinct representation of an exponential number of counters.
2EXPSPACE lower bound

- EXPSPACE-hardness of the control state reachability problem for VASS.  
  - Reduction from the halting problem for counter automata with counters bounded doubly exponentially.

- CA has zero-tests, VASS has no such tests.

- Each counter $c$ in CA is simulated by $c$, $\overline{c}$ with the invariant
  
  $$c + \overline{c} = 2^{2N^K}$$

  - $\mathcal{O}(N^K)$ auxiliary counters ($2^{2i+1} = 2^{2i} \times 2^{2i}$).

- 2EXPSPACE-hardness for chain systems by adapting Lipton’s proof.

  - $\mathcal{O}(N^K)$ chains (instead of $\mathcal{O}(2^{N^K})$ counters with VASS).

- To factorize the encoding for all counters by just moving pointers.
SAT(LRV) is $2\text{EXPSPACE}$-hard (ideas)

- Chain system $\mathcal{A}$ with $n$ chains of size $2^N$.
- We build a formula over the alphabet of transitions. (model = accepting run)
- Standard counter-blind conditions easily expressible.
- Variables $x$ and $x^\alpha_{inc}$, $x^\alpha_{dec}$, $x^\alpha_i$ for every chain $\alpha$ and for every $i \in [1, N]$.
- The values for $x$ and for the $x^\alpha_i$’s determine a counter $c$ in $[0, 2^N - 1]$. 
Any two positions have different values of $x_{inc}^{\alpha}$.

For each position operating on $c$ containing an instruction ‘first($\alpha$)?’ , we have $c = 0$.

For each position operating on $c$, if it contains an instruction ‘next($\alpha$)’ , then the next position operates on $c + 1$. 
Past obligations – PLRV

\[
\begin{array}{cccccccc}
  x & 0 & 0 & 4 & 8 & 4 & 4 & 4 & 2 & 1 \\
  y & 0 & 9 & 0 & 5 & 7 & 5 & 4 & 2 & 9 \\
  \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
  z & 8 & 7 & 4 & 4 & 8 & 4 & 2 & 4 & 4 \\
\end{array}
\]

\[\models y \approx \langle \top? \rangle^{-1} z\]

- There is a polynomial-time reduction from SAT(PLRV) into SAT(PLRV\(^\top\)).

- SAT(PLRV\(^\top\)) is decidable \cite{DemriDS09}.

- Polynomial-space reduction from Reach(VASS) into SAT(PLRV).

- Same proof as the one in \cite{Bojanczyketal06} for FO\(^2(\sim, <, +1)\) except that PLRV is used.
Robustness

- $\text{SAT}_\omega(\text{LRV})$ is $2\text{EXPSPACE}$-complete.

- $\text{SAT}_\omega(\text{PLRV})$ is decidable.

- For every $k \geq 1$, $\text{SAT}(\text{LRV}_k^\top)$ is $\text{PSPACE}$-complete.
  (use of Rackoff’s result on the covering problem for VASS)

- $\text{SAT}(\text{LRV}_1)$ is $2\text{EXPSPACE}$-hard.

- $\text{SAT}(\text{LRV}_{vec}(X, U))$ is undecidable.

\[
\sigma, i \models (x_1, x_2) \approx \langle \varphi? \rangle (y_1, y_2) \quad \text{iff} \quad \text{there exists } j \text{ s.t. } i < j < |\sigma|, \sigma, j \models \varphi,
\]
\[
\sigma(i)(x_1) = \sigma(j)(y_2) \& \sigma(i)(x_2) = \sigma(j)(y_2)
\]
Concluding remarks

$LRV_k^T$: PSPACE-complete

$LRV \equiv LRV^T \equiv LRV_1 \equiv LRV + \{\oplus_1, \ldots, \oplus_k\}: 2\text{EXPSPACE}-complete$

$PLRV \equiv PLRV^T \equiv PLRV_1 \equiv \text{Reach}(VASS)$

$LRV_{vec}^T$: undecidable