Verification of temporal logics on infinite-state systems

Lecture 4.1
Temporal logics for counter systems

Stéphane Demri and Valentin Goranko

ESSLLI 2007, Trinity College, August 2007
Overview

Counter Logic
  Relational counter automata
  Definition
  Flat fragment
  Model-checking

Presburger LTL
  Fragments of Presburger LTL
  Model-checking problems
  Summary
  A $\text{PSPACE}$-complete problem
  Nonemptiness test
  Qualitative constraints

Fairness conditions in VASS
  Temporal logic on VASS
  Results on Petri nets

Model Checking Lossy VASS
  Constraints
  Closure properties
  Automata logic
  Global model-checking is decidable
Counter Logic

Presburger LTL

Fairness conditions in VASS

Model Checking Lossy VASS

Relational counter automata

Definition

Flat fragment

Model-checking

Counter Logic
Relational counter automata with alphabet

- A relational counter automata with alphabet is a structure \( \mathcal{A} = (\Sigma, Q, I, C, \delta, F) \) such that
  - \( Q \) is a finite set of locations,
  - \( I \subseteq Q \) (initial locations), \( F \subseteq Q \) (final locations),
  - \( C \) is a finite set of counters,
  - \( \delta \subseteq Q \times \text{guards}(C) \times \Sigma \times Q \) is the transition relation.

- A guard in \( \text{guards}(C) \) is a conjunction of expressions of the form
  \[ x \sim y + c, \quad x \sim c \]
  where \( x, y \in C \cup C', \ c \in \mathbb{Z} \) and \( \sim \in \{\geq, \leq, =, >, <\} \).

- Acceptance of words in \( \Sigma^* \) by final location and words in \( \Sigma^\omega \) by Büchi acceptance condition.
Example: pay phone controller [Comon & Cortier, CSL 00]

- $x$ is the number of quarters which have been inserted.
- $y$ measures the total communication time.
- $x'$ [resp. $y'$] is the new value of $x$ [resp. $y$].
- The controller interacts with the environment. Messages followed by a question mark are received by the controller and messages followed by an exclamation mark are sent by the controller.
Counter Logic
Presburger LTL
Fairness conditions in VASS
Model Checking Lossy VASS

Relational counter automata
Definition
Flat fragment
Model-checking

\[
q_1 \xrightarrow{x = y = 0, \text{lift?}} q_2 \xrightarrow{dial?} q_3 \xrightarrow{x > 0, \text{connected?}} q_4
\]

\[
x = y, x' = y' = 0
\]

\[
ym' \leq x, y + +, \text{quarter!}
\]

\[
x + +, \text{quarter?}
\]

\[
y \leq x, \text{signal?}, y +
\]

\[
x + +, \text{quarter?}
\]

\[
q_6 \xrightarrow{\text{busy?}} q_5 \xrightarrow{\text{hang?}} q_4
\]

\[
q_4 \xrightarrow{y \leq x}
\]
Properties

- Communication time is never greater than the number of inserted quarters: $A \text{ G } \neg(y > x)$.

- The number of quarters is infinitely often equal to zero: $A \text{ GF } x = 0$.

- There is an execution of the controller such that the communication time is always equal to zero: $E \text{ G } y = 0$.

- Whenever the communication is over, the controller regains the initial configuration: $A \text{ G } (q_5 \Rightarrow Fq_1)$.

- Whenever the control state $q_1$ is reached, $x = y = 0$ and conversely: $A \text{ G } (q_1 \iff (x = 0 \land y = 0))$. 
CLTL (LTL with counters) [Comon & Cortier, CSL 00]

- Models of CLTL represent runs of relational counter automata.
- Models $\pi$ are elements of $(\mathcal{P}(PROP) \times \mathbb{N}^{VAR})^\omega$ where
  - $PROP = \{p_1, p_2, \ldots\}$ is a countably infinite set of propositional variables.
  - $VAR = \{x_1, x_2, \ldots\}$ is a countably infinite set of variables interpreted in $\mathbb{N}$.
- Formulae
  \[
  \phi ::= p \mid g \mid \neg \phi \mid \phi \land \phi \mid X\phi \mid \phi U \phi
  \]
  with $p \in PROP$ and $g \in guards(C)$ for some $C \subseteq VAR$.
- Standard abbreviations:
  \[
  F\phi \equiv \top U \phi \quad G\phi \equiv \neg F \neg \phi
  \]
Satisfaction relation

- $\pi, i \models p$ iff $p \in X$ with $\pi(i) = (X, v)$.

- $\pi, i \models g$ iff $m_1, \ldots, m_k, m'_1, \ldots, m'_k \models g$ with
  - $g$ belongs to $\text{guards}({x_1, \ldots, x_k})$,
  - $m_j$ is $v(x_j)$ and $m'_j$ is $v'(x_j)$ with $\pi(i + 1) = (X', v')$.

- Boolean operators are interpreted as usual.
Standard clauses for temporal operators

- $\pi, i \models X\phi$ iff $\pi, i + 1 \models \phi$.

- $\pi, i \models \phi_1 U \phi_2$ iff there is $j \geq i$ such that $\pi, i \models \phi_2$ and for every $i \leq k < j$, $\pi, j \models \phi_1$. 
CLTL satisfiability is $\Sigma_1^1$-complete

- Reduction from the recurrence problem for nondeterministic Minsky machines.
- $\Sigma_1^1$-hardness from [Alur & Henzinger, JACM 94].
- The instruction "$l : C_1 := C_1 + 1; \text{goto either } l_1 \text{ or } l_2$" is encoded by
  \[ G(x_{\text{inst}} = l \Rightarrow (x'_1 = x_1 + 1 \land x'_2 = x_2 \land (x'_{\text{inst}} = l_1 \lor x'_{\text{inst}} = l_2))) \]
- Recurring condition: $GF(x_{\text{inst}} = 1)$. 
Flat fragment of CLTL

- Elementary formula: Boolean combination of constraints in $\text{guards}(C)$.

- Flat fragment of CLTL

  $\phi ::= \phi_{el} \mid \phi \land \phi \mid \phi \lor \phi \mid X\phi \mid g U \phi \mid G g$

  where $\phi_{el}$ is an elementary formula and $g$ is a guard in some $\text{guards}(C)$.

- Flat fragment of CLTL is not closed under negation.
Automata-based approach

- Automata-based approach for LTL [Vardi & Wolper, IC 94]:
  \[ \phi \mapsto A_\phi \]
  - models of \( \phi = L(A_\phi) \).
  - \( |A_\phi| \) is in \( 2^{O(|\phi|)} \).

- For every flat formula \( \phi \), there is a flat relational counter automaton whose accepting runs are exactly the models of \( \phi \). [Comon & Cortier, CSL 00]

- The proof is by structural induction on \( \phi \).

- Existence of accepting runs for flat relational counter automata is decidable by [Comon & Jurski, TR 98].
Sketch of the proof

- Elementary formulae are equivalent to disjunctions
  \[ g_1 \lor \cdots \lor g_m \]

- For \( \phi_1 \land \phi_2 \), we consider the synchronized product between \( A_{\phi_1} \) and \( A_{\phi_2} \) since
  - guards are closed under conjunctions,
  - flatness is preserved.

- For \( \phi_1 \lor \phi_2 \), we consider the “disjoint union” of \( A_{\phi_1} \) and \( A_{\phi_2} \).
Construction for $gU\phi$

\[ A_\phi \]
Model checking

- Problem
  
  input: relational counter automaton $A$ and formula $\phi$; 
  question: is there an accepting run of $A$ satisfying $\phi$?

- The model-checking problem restricted to flat automata and to the flat fragment of CLTL is decidable. 
  
  [Comon & Cortier, CSL 00]

- Nonemptiness testing for $L(A) \cap L(A_\phi)$.

- This result can be extended to a fragment of CLTL containing full LTL. See details in [Comon & Cortier, CSL 00].
Presburger LTL
Fragments of Presburger arithmetic

- Difference logic DL

\[ E ::= x \sim y + d \mid x \sim d \mid E \land E \mid \neg E \]

with \( d \in \mathbb{Z} \), \( \sim \in \{<, >, =\} \)

- \( DL^+ \): DL + \( x \equiv_k c \), \( x \equiv_k y + c \) (\( c, k \in \mathbb{N} \)).

- Quantifier-free Presburger arithmetic QFP:

\[ E ::= \sum_{i \in I} a_i x_i \sim d \mid \sum_{i \in I} a_i x_i \equiv_k c \mid E \land E \mid \neg E \]

with \( a_i \in \mathbb{Z} \)
Syntax for **CLTL(L)**

- **L** is a fragment of Presburger arithmetic (e.g. DL, DL\(^+\), QFP).

- **Formulae:**

\[
\phi ::= E[x_1 \leftarrow X^{l_1}x_{j_1}, \ldots , x_n \leftarrow X^{l_n}x_{j_n}] \mid \phi \land \phi \mid \neg \phi \mid X\phi \mid \phi U \phi
\]

\((E \in L)\)

- \(i\) times

- \(XX \cdots Xx\) interpreted as the value of \(x\) at the \(i\)th next position.

- **Definitions**

  - One-step constraint: \(l_1, \ldots , l_n \leq 1\).
  - \(X\)-length of \(\phi\): maximal \(i\) such that \(X^i x\) occurs in \(\phi\).
Semantics for Presburger LTL

- **Models:** $\omega$-sequences of valuations of the form $\text{VAR} \to \mathbb{Z}$.

- **Satisfaction relation:**
  - $\sigma, i \models E[x_1 \leftarrow X^l_1 x_{j_1}, \ldots , x_n \leftarrow X^l_n x_{j_n}]$ iff $(\sigma(i + l_1)(x_{j_1}), \ldots , \sigma(i + l_n)(x_{j_n})) \models E$ in PA,
  - $\sigma, i \models X\phi$ iff $\sigma, i + 1 \models \phi$,
  - $\sigma, i \models \phi U \phi'$ iff there is $j \geq i$ such that $\sigma, j \models \phi'$ and for every $i \leq k < j$, we have $\sigma, k \models \phi$. 

![Diagram]

Stéphane Demri and Valentin Goranko
Verification of temporal logics on infinite-state systems
Fragments $\text{CLTL}^l_k(L)$

- $\text{CLTL}^l_k(L)$ is the fragment of $\text{CLTL}(L)$ with
  - atomic formulae built from constraints in $L$,
  - formulae use variables from $\{x_1, \ldots, x_k\}$,
  - the term $X^i x$ can occur only if $i \leq l$.

**Examples**

- $x_1 = X^8 x_2 + 1$ belongs to $\text{CLTL}^8_2(\text{DL})$,
- $XXX(5Xx_1 + 2x_2 \geq 27)$ belongs to $\text{CLTL}^1_2(\text{QFP})$.

- $\text{CLTL}$ from [Comon & Cortier, CSL 00] is $\text{CLTL}^1_\omega(\text{DL})$ with variables interpreted over $\mathbb{N}$. 
(Relational) $k$-variable $L$-automata

- **Definition:**
  - Transitions of the form $q \xrightarrow{E} q'$ for one-step constraint $E$ in $L$.
  - Examples: $q \xrightarrow{x > y + 1} q'$, $q_0 \xrightarrow{x = 0 \land y = 0} q$, $q \xrightarrow{\top} q$.
  - Standard Büchi acceptance condition.
  - Accepting runs of the form $\mathbb{N} \rightarrow Q \times \mathbb{Z}^k$.
  - $\sigma$ realizes $E_0 \cdot E_1 \cdots$ iff for every $i$, we have $\sigma, i \models E_i$. 
**k-\(\mathbb{Z}\)-counter automata**

- Restriction of \(k\)-variable DL-automaton with constraints

\[
\bigwedge_{i \in \{1...k\}} E_{test}^i \land \bigwedge_{i \in \{1...k\}} E_{update}^i
\]

with

- \(E_{test}^i \in \{\top\} \cup \{x_i \sim 0 \mid \sim \in \{<, >, =, \neq\}\}\),

- \(E_{update}^i \in \{Xx_i = x_i + u \mid u \in \mathbb{Z}\}\)

- Initial values of the counters are zero.

- Simple \(\mathbb{Z}\)-counter automata: updates in \(\{0, -1, 1\}\).
Model checking problems

- Model-checking $\mathrm{CLTL}_k^l(L)$ formulae over a class $\mathcal{C}$ of automata:
  
  **input:** a $k$-variable automaton $\mathcal{A}$ in $\mathcal{C}$ and a formula in $\mathrm{CLTL}_k^l(L)$.
  
  **question:** Is there a model $\sigma$ that realizes a word accepted by $\mathcal{A}$ and such that $\sigma, 0 \models \phi$?

- We have seen that model-checking $\mathrm{CLTL}_3^1(DL)$ over the class of $3-\mathbb{N}$-automata is $\Sigma_1^1$-complete [Alur & Henzinger, JACM 94].
Summary of results

\( \text{CLTL}^I_k(L) \): \( k \) variables, “next length” \( \leq l \), fragment \( L \)

<table>
<thead>
<tr>
<th></th>
<th>MC (DL)</th>
<th>SAT</th>
<th>MC (CA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{CLTL}^1_3(DL)</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>\text{CLTL}^\omega_2(DL)</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>\text{CLTL}^2_1(DL)</td>
<td>U</td>
<td>U</td>
<td>\text{PSPACE}-c</td>
</tr>
<tr>
<td>\text{CLTL}^1_2(DL)</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>\text{CLTL}^1_1(DL \text{ or DL}^+)</td>
<td>\text{PSPACE}-c.</td>
<td>\text{PSPACE}-c.</td>
<td>\text{PSPACE}-c</td>
</tr>
<tr>
<td>\text{CLTL}^1_1(QFP)</td>
<td>U</td>
<td>U</td>
<td>\text{PSPACE}-c</td>
</tr>
<tr>
<td>\text{CLTL}^\omega_1(QFP)</td>
<td>U</td>
<td>U</td>
<td>\text{PSPACE}-c</td>
</tr>
</tbody>
</table>

\textbf{Corollary:} The model-checking problem and satisfiability problem for CLTL restricted to one variable are \text{PSPACE}-complete [Demri & Gascon, TIME 07].
Symbolic model-checking for $\text{CLTL}_1^1(\text{DL})$

- Model-checking for $\text{CLTL}_1^1(\text{DL}^+)$ reduces to satisfiability for $\text{CLTL}_1^1(\text{DL}^+, \text{PROP})$ (addition of propositions).

- Maps $\{x, Xx\} \rightarrow \mathbb{Z}$ are abstracted by finite sets of constraints depending on the syntactic resources of the formula to be checked.

- Symbolic models are $\omega$-sequences of symbolic valuations.

- Satisfiability is reduced to nonemptiness problem for simple $1-\mathbb{Z}$-counter automata over the alphabet of symbolic valuations.
Symbolic valuation

- \((E_x, E_m, E'_x, E'_m, E_s) \in C_x \times \text{Mod}_x \times C_{Xx} \times \text{Mod}_{Xx} \times C_{\text{step}}.\)

- For \(t \in \{x, Xx\}\)
  - \(C_t:\)
    - \((d_i < t) \land (t < d_{i+1})\) for \(i \in \{\min, \ldots, \max - 1\},\)
    - \(t = d_i\) for \(i \in \{\min, \ldots, \max\} + t < d_{\min}\) and \(d_{\max} < t,\)
  - \(\text{Mod}_t: t \equiv_K c\) for \(c \in \{0, \ldots, K - 1\},\)
  - \(C_{\text{step}}:\)
    - \(x + e_i < Xx \land Xx < x + e_{i+1}\) for \(i \in \{\min', \ldots, \max' - 1\},\)
    - \(Xx = x + e_i\) for \(i \in \{\min', \ldots, \max'\} + Xx < x + e_{\min'}\) and \(x + e_{\max'} < Xx.\)
Satisfiability and symbolic models

- Symbolic model \((\sigma, \rho)\):
  - \(\sigma : \mathbb{N} \rightarrow \text{PROP}\),
  - \(\rho : \mathbb{N} \rightarrow \Sigma\) (alphabet of symbolic valuations)

- \(\phi\) is satisfiable iff there is a symbolic model \((\sigma, \rho)\) such that
  1. \((\sigma, \rho) \models_{\text{symb}} \phi\) (as for LTL)
  2. \(\rho\) is realized in some concrete model.

- Construction of
  - a Büchi automaton for (a) (almost as for LTL).
  - a simple \(1-\mathbb{Z}\)-counter automata over \(\Sigma\) for (b).

- Synchronization and nonemptiness checking can be done on the fly in \(\text{PSPACE}\).
Nonemptiness of simple 1-$\mathbb{Z}$-counter automata

- Büchi acceptance condition, interpretation in $\mathbb{Z}$, alphabet, zero and sign tests.

- **Theorem:** The nonemptiness problem for simple 1-$\mathbb{Z}$-counter automata is $\text{NLOGSPACE}$-complete.

- **Structure of the proof:**
  - Reduction to the nonemptiness problem for simple 1-$\mathbb{N}$-counter automata without alphabet and test $x \neq 0$.
  - Nonemptiness for this class of automata amounts to check the existence of paths of polynomial length.
Qualitative constraints

- Fragment IPC* (integer periodicity constraints)

\[
E ::= x \sim d \mid x \sim y \mid x \equiv_k k' \mid \neg E \mid E \land E
\]

with \( d \in \mathbb{Z}, \; k' < k \in \mathbb{N}, \; \sim \in \{<, >, =, \leq, \geq\} \).

- Ubiquity of periodicity constraints
  - Formalisms dealing with calendars.
  - DATALOG with integer periodicity constraints

- \( \nu \models x \equiv_k k' \) iff there is \( z \in \mathbb{Z} \) such that \( \nu(x) = z \times k + k' \).
Complexity of model-checking

- Model-checking and satisfiability problems for CLTL(IPC*) are PSPACE-complete.
  
  [D. & D’Souza, FSTTCS 02, D. & Gascon, CONCUR 05]

- The proof is by using symbolic valuations that form a finite alphabet for a fixed formula.

- Difficulty of the proof comes from the fact that the sets of symbolic models that admit concrete models are not necessarily $\omega$-regular, i.e. definable by a Büchi automaton.

- Open problem Is CLTL($\{0, 1\}^*, \preceq, =$) decidable?
Fairness conditions in VASS
Notations for VASS

- A VASS of dimension $k$: $\mathcal{A} = (Q, q_0, \delta)$
  - $Q$ is a finite set of locations.
  - $q_0 \in Q$.
  - $\delta$ is a finite subset of $Q \times \mathbb{Z}^k \times Q$.

- Infinite computation of $\mathcal{A}$:

\[ (q_0, c_0) \rightarrow (q_1, c_1) \rightarrow (q_2, c_2) \rightarrow (q_3, c_3) \rightarrow \ldots \]

with $q_0$ initial location and $c_0 = 0 \in \mathbb{N}^k$.

- VASS = counter automata without zero-tests.

- Fairness conditions:
  - Infinitely often the location is $q$.
  - Infinitely often the value of the $i$th counter is greater than 3.
Temporal logic with fairness [Jančar, TCS 90]

- For simplicity, we assume a fixed VASS of dimension $k \geq 1$.

- Atomic formulae:
  \[ q \mid i \geq c \mid \neg(i \geq c) \]
  with $q \in Q$, $i \in \{1, \ldots, k\}$, $c \in \mathbb{N}$.

- Formulae:
  \[ \phi ::= p \mid \phi \lor \phi \mid \phi \land \phi \mid GF\phi \]

- In [Jančar, TCS 90], the logic is defined for Petri nets.
Satisfaction relation

- Computation $\sigma = (q_0, c_0) \rightarrow (q_1, c_1) \rightarrow \ldots$.

- $\sigma, i \models q$ iff $q_i = q$.

- $\sigma, i \models j \geq c$ iff $c_i(j) \geq c$.

- $\sigma, i \models \text{GF} \phi$ iff $\{j \geq i : \sigma, j \models \phi\}$ is infinite.
Model-checking problem and decidability

- Model-checking problem:

  input: a VASS $\mathcal{A}$ and a temporal formula $\phi$;
  question: Is there a computation $\sigma$ of $\mathcal{A}$ such that
  $\sigma, 0 \models \phi$?

- Decidability is shown in [Jančar, TCS 90] by reduction into the
  reachability problem for Petri nets.
  (the proof is difficult)

- See also fairness conditions in VASS in [German & Sistla, JACM 92].
Petri nets

- Petri net $N = (S, T, W, M_0)$
  - $S$ is the finite set of places.
  - $T$ is the finite set of transitions.
  - $W : (S \times T) \cup (T \times S) \rightarrow \mathbb{N}$ is the weight function.
  - Initial marking $M_0 \in \mathbb{N}^S$.

- $M [t > t']$ iff for $s \in S$,
  - $M(s) \geq W(s, t)$,
  - $M'(s) = M(s) - W(s, t) + W(t, s)$. 

```plaintext
Petri net N = (S, T, W, M_0)

- S is the finite set of places.
- T is the finite set of transitions.
- W : (S x T) U (T x S) -> N is the weight function.
- Initial marking M_0 in N^S.

M[t > t'] iff for s in S,
- M(s) >= W(s, t),
- M'(s) = M(s) - W(s, t) + W(t, s).
```
From VASS to Petri nets

- \( A = (Q, q_0, \delta) \mapsto N = (S, T, W, M_0) \).

- For each \( q \in Q \), \( N \) has a place \( s_q \).

- For each counter \( i \leq k \), \( N \) has a place \( s_i \).

- For each transition \( q \xrightarrow{d} q' \) in \( A \) we consider a transition in \( N \) that
  - consumes a token \( s_q \),
  - produces a token in \( s_{q'} \),
  - consumes \( d(i) \) tokens in the place \( s_i \) when \( d(i) < 0 \),
  - produces \( d(i) \) tokens in the place \( s_i \) when \( d(i) \geq 0 \).
Temporal logics in Petri nets

- Temporal logic on Petri nets [Jančar, TCS 90]:
  \[ \phi ::= s \geq c \mid \neg(s \geq c) \mid \phi \lor \phi \mid \phi \land \phi \mid GF\phi \]

- Reduction from VASS to Petri nets guarantees that decidability on Petri nets implies decidability on VASS.

- Undecidability of a linear-time temporal logic for Petri nets [Howell & Rosier, TCS 89] with
  - temporal operator F and Boolean connectives,
  - atomic formulae \( s \geq c \) and “transition \( t \) is the next one in the sequence”.

- Decidability/undecidability results for linear-time temporal logic on Petri nets. [Esparza, ICALP 94]
  - e.g. linear \( \mu \)-calculus with propositions \( s = 0 \) is undecidable.
Model Checking Lossy Vector Addition Systems
Lossy VASS

- A $n$-dim Lossy VASS (with alphabet) $A$ is a structure $(\Sigma, Q, C, \delta)$ where
  - $Q$ is a finite set of locations,
  - $C$ is a set of counters of cardinal $n$,
  - $\delta$ is a finite set of transitions among $Q \times \Sigma \times \mathbb{Z}^n \times Q$.

- $(q, v) \xrightarrow{a}_{\text{lossy}} (q', v')$ iff there are $v_- \leq v$ and $v'_+ \geq v'$ such that $(q, v_-) \xrightarrow{a}_{\text{perf}} (q', v'_+)$. 

- Finite run of $A$ from configuration $(q, v)$:
  
  $$(q_0, v_0) \xrightarrow{a_0} (q_1, v_1) \xrightarrow{a_1} (q_2, v_2) \xrightarrow{a_2} (q_3, v_3) \xrightarrow{a_3} (q_4, v_4) \ldots$$
  
  with $(q_0, v_0) = (q, v)$.

- The control-state reachability problem and the reachability problem for lossy VASS are decidable.
Ordering on \((\mathbb{N} \cup \{\infty\})^n\)

- \(u, v \in (\mathbb{N} \cup \{\infty\})^n\): \(u \leq v\) iff for every \(i \in \{1, \ldots, n\}\), \(u(i) \leq v(i)\).

- \(X \subseteq \mathbb{N}^n\) is upward closed \(\iff\) for \(u \in X\), \(v \in \mathbb{N}^n\), \(u \leq v\) implies \(v \in X\).

- \(X \subseteq \mathbb{N}^n\) is downward closed \(\iff\) for \(u \in X\), \(v \in \mathbb{N}^n\), \(v \leq u\) implies \(v \in X\).

- By Dickson’s Lemma, any set \(X \subseteq \mathbb{N}^n\) has a finite number of minimal elements.

- Downward or upward closed set are closed under union and intersection.
Constraints

- Simple constraint: Boolean combination of constraints of the form $x \geq d$ with $d \in \mathbb{N} \cup \{\infty\}$.

- Upward closed constraint: positive Boolean combination of constraints of the form $x \geq d$ with $d \in \mathbb{N} \cup \{\infty\}$.

- Downward closed constraints: positive Boolean combination of constraints of the form $x < d$ with $d \in \mathbb{N} \cup \{\infty\}$.

- Every simple constraint $E$ built over $\{x_1, \ldots, x_n\}$ defines a subset $[E] \subseteq \mathbb{N}^n$.

- $X$ is SC [resp. UC, DC] definable $\iff$ there is an SC [resp. UC, DC] $E$ such that $[E] = X$. 
Constraints in normal form

- Products $(\vec{l} \in \mathbb{N}^n$ and $\vec{u} \in (\mathbb{N} \cup \{\infty\})^n)$:
  - Canonical product: $\vec{l} \leq \vec{x} \leq \vec{u}$
  - Canonical upward closed product: $\vec{l} \leq \vec{x}$
  - Canonical downward closed product: $\vec{x} \leq \vec{u}$

- A SC [resp. UC, DC] in normal form is a finite disjunction of canonical [resp. canonical upward closed, canonical downward closed] products (possibly empty).

- Every SC [resp. UC, DC] is equivalent to a SC [resp. UC, DC] in normal form.

- $X$ is SC definable iff it is the Boolean combinations of upward closed sets.

- $X$ is UC definable iff $X$ is an upward closed set.
Closure properties

- In order to deal with configurations, the canonical products are extended: \((q, \vec{l} \leq \vec{x} \leq \vec{u})\).

- \(\text{SC}(Q,C), \text{UC}(Q,C), \text{DC}(Q,C)\).

- The class SC is effectively closed under the operations of post and pre for any lossy VASS.
  - e.g. \(\text{post}_t((q, \vec{l} \leq \vec{x} \leq \vec{u})) = (q', \vec{x} \leq \vec{u} + d)\) with \(t = q \xrightarrow{a,d} q'\).

- For every \(n\)-dim lossy VASS and SC definable set \(X\), \(\text{pre}^\ast(X)\) is UC definable and effectively computable. Consequence of a construction from [CéCé & Finkel & Purushothaman Iyer, IC 96].

- For every \(n\)-dim lossy VASS and SC definable set \(X\), \(\text{post}^\ast(X)\) is DC definable and effectively computable.
**EF logic** [Bouajjani & Mayr, STACS 99]

- **Formulae**

\[
\phi ::= E \mid \neg \phi \mid \phi \land \phi \mid \phi \lor \phi \mid EX\phi \mid EF\phi
\]

with \(E\) in \(SC(Q,C)\).

- **EX \equiv \langle R \rangle, EF \equiv \langle R^* \rangle.**

- **Satisfaction relation**
  - \((q', v') \models (q, \bar{t} \leq \bar{x} \leq \bar{u})\) iff \(q = q'\) and \(\bar{t} \leq v' \leq \bar{u}\).
  - \((q', v') \models EX\phi\) iff there is a configuration \((q, v)\) such that \((q', v') \in pre((q, v))\) and \((q, v) \models \phi\).
  - \((q', v') \models EF\phi\) iff there is a configuration \((q, v)\) such that \((q', v') \in pre^*((q, v))\) and \((q, v) \models \phi\).

- **Richer logics are considered in** [Bouajjani & Mayr, STACS 99] with Wolper-like temporal operators.
Model-checking problems

- Local model-checking problem:
  - input: a lossy VASS, a configuration \((q, v)\) and \(\phi \in EF\);
  - question: does \((q, v) \models \phi\) hold true?

- Global model-checking problem:
  - input: a lossy VASS \(A\), \(\phi \in EF\);
  - question: compute the symbolic representation for \(\{(q, v) : (q, v) \models \phi\}\).
Computations of representations

- The global model-checking for lossy VASS and the logic EF is decidable [Bouajjani & Mayr, STACS 99].

- \( \{(q, v) : (q, v) \models \phi\} \) is effectively computable.

- The proof is by structural induction.
  - The base case with \( E \in SC(Q, C) \) is immediate.
  - Formulae with outermost Boolean operators easy to deal with since SC definable sets are closed under Boolean operations.
  - Constraints for \( EX\phi \) can be computed since SC is effectively closed under the \( pre \) operation for lossy VASS:
    - \( pre_t((q, \vec{1} \leq \vec{x} \leq \vec{u})) = (q', \vec{1} \cdot d \leq \vec{x}) \) with \( t = q' \xrightarrow{a,d} q \) and \( (\vec{1} - d)(i) = \max(0, \vec{1}(i) - d(i)) \) for \( i \in \{1, \ldots, n\} \).
  - Constraints for \( EF\phi \) can be computed since SC is effectively closed under the \( pre^* \) operation for lossy VASS.
Extensions and related work.

- The results for EF are extended in [Bouajjani & Mayr, STACS 99] in various directions:
  - Automata-based operators with Büchi acceptance condition and universal quantification on paths.
  - Decidability results for model-checking problems over non-lossy VASS.

- General unboundedness problem for lossy counter automata is undecidable (boundedness for every configuration) [Mayr, TCS 03].

- See also the decidability results for lossy channel systems with regular guards in [Baier & Bertrand & Schnoebelen, LPAR 06].
Proof techniques for temporal logics

- Automata-based approach extending [Vardi & Wolper, IC 94]
  See e.g. counter logic CLTL.

- Reduction to reachability questions
  See e.g. temporal logic with fairness condition in [Jančar, TCS 90].

- Symbolic representation of configurations.
  See e.g. decidable fragments of Presburger LTL.

- Well structure of transitions systems.
  See e.g. [Bouajjani & Mayr, STACS 99; Finkel & Schnoebelen, TCS 01]
Incomplete bibliography

A. Bouajjani and R. Mayr.
Model checking lossy vector addition systems.

H Comon and V. Cortier.
Flatness is not a weakness.

J. Esparza.
On the decidability of model checking for several \( \mu \)-calculi and Petri nets.

P. Jančar.
Decidability of a temporal logic problem for petri nets.

M. Vardi and P. Wolper.
Reasoning about infinite computations.