Plan of the talk

- Yesterday’s lecture:
  - Counter systems, Presburger arithmetic.
  - Linear-time temporal logics.

- Today’s lecture:
  - Simple undecidability proof for $\text{CLTL}_3^1(\text{DL})$ satisfiability.
  - Repeated reachability problem.
  - Plain LTL for several classes of counter systems.
    (use of automata)
  - $\text{LTL}^\text{CS}(\text{PrA})$ for admissible counter systems.
    (use of Presburger arithmetic)
$\text{CLTL}^1_3(\text{DL})$ satisfiability is undecidable
Recall

- Atomic formulae in $\text{CLTL}_3(\text{DL})$ include the following $(1 \leq i \leq 3, k \in \mathbb{N})$:

  \[ X x_i = x_i + 1 \quad X x_i = x_i - 1 \quad x_i = k \]

- Simple reduction from halting problem for Minsky machines.

- A Minsky machine can be viewed as a counter automaton with two counters.

- Operations on counters:
  - Check whether the counter is zero.
  - Increment the counter by one.
  - Decrement the counter by one if nonzero.
2-counter Minsky machines

- Set of $n$ instructions.

- The $l$th instruction has one of the forms below ($i \in \{1, 2\}$, $l' \in \{1, \ldots, n\}$):
  
  $l$: $C_i := C_i + 1$; goto $l'$
  
  $l$: if $C_i = 0$ then goto $l'$ else $C_i := C_i - 1$; goto $l''$.

- Configurations are elements of $\{1, \ldots, n\} \times \mathbb{N} \times \mathbb{N}$.

- Initial configuration: $(1, 0, 0)$. 
A computation is a sequence of configurations starting from the initial configuration and such that two successive configurations respect the instructions.

The Minsky machine

1: $C_1 := C_1 + 1$; goto 2
2: $C_2 := C_2 + 1$; goto 1

has unique computation

$(1, 0, 0) \rightarrow (2, 1, 0) \rightarrow (1, 1, 1) \rightarrow (2, 2, 1) \rightarrow (1, 2, 2) \rightarrow (2, 3, 2) \ldots$
Halting problem

- Halting problem:
  \textbf{input:} a 2-counter Minsky machine $M$;
  \textbf{question:} is there a finite computation that ends with location equal to $n$?
  ($n$ may also be a special instruction that halts the machine)

- Theorem: The halting problem is undecidable. [Minsky, 67]
Satisfiability problem for $\text{CLTL}^1_3(\text{DL})$ is undecidable

- Formulae in $\text{CLTL}^1_3(\text{DL})$ can easily internalize the instructions of Minsky machines.

- $S$ has $n$ instructions, the $n$th one halts.

- $x_1$ and $x_2$ encode counter values, $x_3$ encodes the instruction ordinal.

- $S$ does not halt iff formula below is satisfiable:

$$
(\bigwedge_{i \in [1,n]} \psi_i) \land G \neg q_{halt} \land \underbrace{x_1 = 0 \land x_2 = 0 \land x_3 = 1}_{\text{initial configuration}}
$$
Internalizing instructions from Minsky machines

- For “i: increment counter j and goto i’”

\[ \psi_i \overset{\text{def}}{=} G(x_3 = i \Rightarrow (Xx_3 = i') \land (x_j + 1 = Xx_j) \land (x_{3-j} = Xx_{3-j})) \].

- For “i: if counter j equals zero then goto i’ else (decrement counter j; goto i’’):”

\[ G(x_3 = i \Rightarrow ((x_j = 0 \Rightarrow (Xx_3 = i') \land (x_j = Xx_j) \land (x_{3-j} = Xx_{3-j}))) \land (x_j \neq 0 \Rightarrow (Xx_3 = i'') \land (x_j - 1 = Xx_j) \land (x_{3-j} = Xx_{3-j})))) \]

- Satisfiability problem for $\text{CLTL}_2^1(DL)$ is undecidable too.
LTL and Control State Repeated Reachability
**LTL(\(Q\))**

- **LTL(\(Q\))**: fragment where atomic formulae are restricted to control states. Example: \(G(q_1 \Rightarrow x q_2)\).

- **LTL(\(Q\))** does not speak about counter values but counter values constrain the runs.

- **Existential Model-Checking Problem for LTL(\(Q\))**:  
  **Input**: CS \(S = (Q, n, \delta), (q_0, \vec{x}_0)\) and \(\varphi \in \text{LTL}(\(Q\))\).  
  **Question**: Is there an infinite run \(\rho\) from \((q_0, \vec{x}_0)\) s.t. \(\rho, 0 \models \varphi\)?

- In this part, we present a sufficient condition for deciding the model-checking problem for LTL(\(Q\)) restricted to subclasses of counter systems.

- Problem restricted to CA is already undecidable.
Projection on runs

- Counter system $S$, configuration $(q_0, \overrightarrow{x_0})$ and $\varphi$ in $\text{LTL}(Q)$.

- $\rho, 0 \models \varphi$ implies $\text{proj}_Q(\rho), 0 \models \varphi$, where $\text{proj}_Q(\rho) \in Q^\omega$ is obtained from $\rho$ by erasing the counter values.

- One can effectively construct a Büchi automaton $A_\varphi$ over $Q$ such that:
  - $\text{L}(A_\varphi)$ is the set of models of $\varphi$.
  - Size of $A_\varphi$ is at most exponential in size of $\varphi$.
  (see lecture 4 slides)

- In $A_\varphi$, there is a successful run of the form

  \[
  \rho' = X_0 \xrightarrow{\text{proj}_Q(\rho)(0)} X_1 \xrightarrow{\text{proj}_Q(\rho)(1)} X_2 \xrightarrow{\text{proj}_Q(\rho)(2)} X_3 \cdots
  \]

  (recall that states of $A_\varphi$ are sets of formulae)
Synchronized product

- Satisfaction of $\rho, 0 \models \varphi$ and $\text{proj}_Q(\rho), 0 \models \varphi$ can be represented by two synchronized sequences:

  $$(q_0, x_0) \rightarrow (q_1, x_1) \rightarrow (q_2, x_2) \rightarrow (q_3, x_3) \rightarrow \cdots \models \varphi$$

  $$X_0 \xrightarrow{q_0} X_1 \xrightarrow{q_1} X_2 \xrightarrow{q_2} X_3 \xrightarrow{q_3} \models \varphi$$

- To design a unique counter system synchronizing $S$ and $A_{\varphi}$ with control states of the form $(q_i, X_i)$.

- To update the counter values according to the transitions from $S$.

- $S = (Q, n, \delta), A = (\Sigma, Q', Q'_0, \delta', F)$ with $\Sigma = Q$. Synchronized product $S \otimes A = (Q'', n, \delta'')$:

  - $Q'' = Q \times Q'$,

  - $(q_0, q'_0) \varphi (q_1, q'_1) \defeq q_0 \varphi q_1 \in \delta$ and $q'_0 \xrightarrow{q_0} q'_1 \in \delta'$. 
Reduction to repeated reachability

- CS $S$, $(q, \bar{x})$ and formula $\varphi \in \text{LTL}(Q)$.

- BA $A_{\varphi} = (\Sigma, Q', Q'_0, \delta', F)$ s.t. $\text{Models}(\varphi) = L(A_{\varphi})$.

- Equivalence between (I) and (II):
  
  (I) $\exists$ infinite run $\rho$ from $(q, \bar{x})$ s.t. $\rho, 0 \models \varphi$.

  (II) For some $q_i \in Q'_0$ and $(q'', q_f) \in Q \times F$, there is an infinite run in $S \otimes A_{\varphi}$ from $((q, q_i), \bar{x})$ such that $(q'', q_f)$ is repeated infinitely often.

- Model-checking is reduced to a finite number of instances of the control state repeated reachability problem.
Decidability

- Let $C$ be a class of counter systems such that
  1. the control state repeated reachability problem is decidable,
  2. $C$ is closed under synchronized products with BA.

Then, existential model-checking problem restricted $\text{LTL}(\mathcal{Q})$ and to counter systems in $C$ is decidable.
Proof

- There is an infinite run $\rho$ with initial configuration $(q, \vec{x})$ such that $\rho, 0 \models \varphi$ iff for some $q_i \in Q_0'$ and $(q'', q_f) \in Q \times F$, there is an infinite run in $S \otimes A_\varphi$ with initial configuration $((q, q_i), \vec{x})$ such that $(q'', q_f)$ is repeated infinitely often.

- Since both $Q_0'$ and $Q \times F$ are finite sets, the existence of a finite run $\rho$ such that $\rho, 0 \models \varphi$ can be verified by checking at most $\operatorname{card}(Q_0') \times \operatorname{card}(Q \times F)$ instances of the control state repeated reachability problem on the system $S \otimes A_\varphi$.

- By condition (2), such a system belongs also to $C$ and the target problem is decidable by condition (1).
What about VASS?
• Control state repeated reachability problem restricted to VASS can be solved in exponential space. [Habermehl, ICATPN 97]

• Adaptation of Rackoff’s proof for solving boundedness and covering in exponential space.

• Equivalence between the propositions below.
  • There is an infinite run with initial configuration \((q, \vec{x})\) such that the control state \(q_f\) is repeated infinitely often.
  • there is a finite run \((q_0, \vec{x}_0), \ldots, (q_k, \vec{x}_k)\) such that
    • \((q_0, \vec{x}_0) = (q, \vec{x})\),
    • there is \(k' < k\) such that \(\vec{x}_{k'} \preceq \vec{x}_k\),
    • \(q_k = q_{k'} = q_f\).
Use of Dickson’s Lemma: for any infinite sequence $\vec{y}_0, \vec{y}_1, \ldots$ of tuples in $\mathbb{N}^n$, there are $i < j$ such that $\vec{y}_i \preceq \vec{y}_j$.

The key argument to get the $\text{EXPSPACE}$ upper bound is to show that $k$ can be at most double-exponential in the size of the instance $S, (q, \vec{x}), q'$.

Model-checking problem restricted to $\text{LTL}(Q)$ and to VASS is $\text{EXPSPACE}$-complete [Habermehl, ICATPN 97].
Another logic expressing fairness

- TLF formulae ($q \in Q$ and $c \in \mathbb{N}$):
  \[ q \mid x_i \geq c \mid \neg(x_i \geq c) \mid \varphi \lor \varphi \mid \varphi \land \varphi \mid GF \varphi \]

- TLF formulae are not closed under negations and the temporal properties are intersection or union of fairness conditions.

- Existential model-checking problem for TLF restricted to VASS is decidable [Jančar, TCS 90].

- Addition of $F$ may lead to undecidability. [Howell & Rosier, TCS 89]

- Decidability/undecidability results for linear-time temporal logic on Petri nets can be found in [Esparza, CAAP’94]; e.g., $\text{LTL}(Q) + x_i = 0$ is undecidable.
- 6 phases, 3 biphases, and 5 reversals.

- Initialized CA \( (S, (q, \vec{x})) \) is \( r \)-reversal-bounded \( \iff \) every run from \( (q, \vec{x}) \) has strictly less than \( r + 1 \) reversals. [Ibarra, JACM 78]

- \( S \) is uniformly reversal-bounded \( \iff \) there is \( r \) such that every initialized CA defined from \( S \) is \( r \)-reversal-bounded.
About reachability and repeated reachability

• Theorem: [Ibarra, JACM 78] Let \((S, (q_0, \vec{x}_0))\) be \(r\)-reversal-bounded. For each \(q \in Q\), the set \(\{\vec{x} \in \mathbb{N}^n : (q_0, \vec{x}_0) \xrightarrow{*} (q, \vec{x})\}\) is effectively semilinear: one can construct \(\varphi\) such that

\[
\text{REL}(\varphi) = \{\vec{x} \in \mathbb{N}^n : (q_0, \vec{x}_0) \xrightarrow{*} (q, \vec{x})\}
\]

• This is not sufficient to deduce that control state repeated reachability problem is decidable.

• Nevertheless, control state repeated reachability problem is decidable as shown now.
Decidability

- Control state repeated reachability problem restricted to reversal-bounded counter automata is decidable.
  [Dang & Ibarra & San Pietro, FSTTCS’01]

- A stronger result is shown since Presburger-definable atomic properties can be included while preserving decidability.

- **Corollary**: Existential model-checking problem restricted to LTL(\(Q\)) and to reversal-bounded CA is decidable.
Idea of the proof

- $r$-reversal-bounded initialized CA $(S, (q_0, \vec{x}_0))$ and $q_f \in Q$.

- Property ($\star$): there is an infinite run from $(q_0, \vec{x}_0)$ such that $q_f$ is repeated infinitely often.

- We reduce ($\star$) to a reachability question for a new reversal-bounded counter automaton $S'$.

- Property ($\star\star$): there exist

  $\rho = (q_0, \vec{x}_0) \xrightarrow{t_1} (q_1, \vec{x}_1) \cdots \xrightarrow{t_l} (q_l, \vec{x}_l)$ and $l' \in [0, l - 1]$ s.t.

  1. $q_l = q_{l'} = q_f$,
  2. $\vec{x}_{l'} \preceq \vec{x}_l$,
  3. if $X$ is the set of counters tested to zero between $(q_l, \vec{x}_l)$ and $(q_{l'}, \vec{x}_{l'})$, then $\vec{x}_{l'}(X) = \vec{x}_l(X) = \vec{0}$.
Equivalence

- (⋆) is equivalent to (⋆⋆).

- (⋆⋆) shall provide a characterization with a finite witness run that can be encoded as a reachability question.

- (⋆⋆) implies (⋆):
  - $\rho = (q_0, \vec{x}_0) \xrightarrow{t_1} (q_1, \vec{x}_1) \cdots \xrightarrow{t_l} (q_l, \vec{x}_l)$.
  - $\rho'$ is defined with $t_1 \cdots t_{l'}(t_{l'+1} \cdots t_l)\omega$.
  - $q_f$ is repeated infinitely often.
  - Zero-tests are also successful.
(⋆) implies (⋆⋆)

• \( \rho = (q_0, \vec{x}_0) \xrightarrow{t_1} (q_1, \vec{x}_1) \xrightarrow{t_2} (q_2, \vec{x}_2) \cdots \) with \( q_f \) repeated infinitely often.

• \( X \): set of counters that are successfully tested to zero in \( \rho \) infinitely often.

• By reversal-boundedness, there is \( I \geq 0 \) s.t. for \( k \geq I \), we have \( \vec{x}_k(X) = \vec{0} \).

• There exists \( I \leq k_1 < k_2 < k_3 < \ldots \) s.t. for \( 1 \leq j < j' \), we have \( q_{k_j} = q_f \) and between \( (q_{k_j}, \vec{x}_{k_j}) \) and \( (q_{k_j'}, \vec{x}_{k_j'}) \), exactly the counters in \( X \) are tested to zero.

• By Dickson’s Lemma, there exists \( J < J' \) such that \( \vec{x}_{k_j} \preceq \vec{x}_{k_j'} \).
Reduction to a reachability question

\[ S' = (Q', q_0, 3 \times n, \delta') \text{ s.t. (**) iff } (q_0, \vec{x}_0) \overset{*}{\rightarrow} (q_{\text{new}}, \vec{0}) \text{ in } S'. \]
Construction of $S'$

- Let $S' = (Q', q_0, 3 \times n, \delta')$ s.t. $(\ast \ast)$ iff $(q_0, \vec{x}_0)^* \rightarrow (q_{\text{new}}, \vec{0})$ in $S'$.

- One can effectively build $\varphi$ s.t.
  $$\text{REL}(\varphi) = \{\vec{x} : (q_0, \vec{x}_0)^* \rightarrow (q_{\text{new}}, \vec{x})\}$$

- $S'$ is made of $2^n + 1$ copies of $S$ plus some extra control states such as $q_{\text{new}}$.

- It includes an initial distinguished copy of $S$.

- For $X \subseteq [1, n]$, the control states of the $X$-copy are among $Q \times \{X\} \times \mathcal{P}(X)$.

- Third component records the counters that have been tested to zero since the run has entered in the $X$-copy.
Entering into the $X$-copy

- For $X \subseteq [1, n]$, we consider a sequence of transitions from $q_f$ to $(q_f, X, \emptyset)$ whose effect is to perform a zero-test on counters in $X$ and to copy the value of each counter $i \in X$ into the counter $n + i$.

- $\text{copy } x_i \rightarrow x_{i+n}$:
  1. Decrement the counter $i$ until zero and for each decrement, the counters $n + i$ and $2n + i$ are incremented.
  2. When counter $i$ is equal to zero, decrement the counter $2n + i$ until zero while incrementing the counter $i$ at each step.
  3. The number of reversals is at most augmented by 2.
Transitions in the $X$-copy

• $(q, X, Y) \xrightarrow{\varphi} (q', X, Y')$ is a transition whenever there is a transition $q \xrightarrow{\varphi'} q'$ in $S$ for which
  • $\varphi$ performs the same instruction as $\varphi'$,
  • for $i \in \overline{X}$, $\varphi'$ is a not a zero-test on $i$,
  • if $\varphi = \text{zero}(j)$, then $Y' = Y \cup \{j\}$ otherwise $Y' = Y$.

• When all the counters in $X$ have been tested to zero at least once and $q_f$ is reached, we may jump to $q_{new}$. 
Final step

- Consider a sequence of transitions from \((q_f, X, X)\) to \(q_{new}\) performing the following tasks:

  1. for \(i \in X\), perform a zero-test on counter \(i\),

  2. for \(i \in \overline{X}\), test whether the counter value for \(i\) is greater or equal to the counter value for \(n + i\),

  3. empty all the counters.

- check \(x_{i+n} \leq x_i\): decrement \(i\) and \(n + i\) simultaneously and nondeterministically test whether the counter \(n + i\) has value zero.

- \((S', (q_0, \vec{x}_0))\) is \((r + 3)\)-reversal-bounded.
What about gainy counter automata?
Gainy counter automata

- Gainy counter automaton: standard counter automaton $(Q, n, \delta)$ such that for $q \in Q$ and $i \in [1, n]$, $q \xrightarrow{\text{inc}(i)} q \in \delta$.

- Alternative definition: to modify the one-step relation

  \[(q, \vec{x}) \xrightarrow{t} g (q', \vec{x}') \iff \text{there are } \vec{y} \text{ and } \vec{y}' \text{ in } \mathbb{N}^n \text{ such that } \vec{x} \preceq \vec{y} \text{ and } (q, \vec{y}) \xrightarrow{t} (q', \vec{y}') \text{ – perfect step – and } \vec{y}' \preceq \vec{x}'\].

- The control state reachability problem for gainy counter automata is decidable but with nonprimitive recursive complexity [Schnoebelen, IPL 02].

- The control state repeated reachability problem restricted to gainy counter automata is undecidable.

- Hence, model-checking problem restricted to $\text{LTL}(Q)$ and to gainy counter automata is undecidable.
Undecidability proof – Step I

- Minsky machine $S = (Q, 2, \delta)$ with halting control state $q_h$.
- We have seen that the halting problem is undecidable.
- First, we build a CA $S' = (Q', 3, \delta')$ that behaves exactly as $S$ as far as the counters 1 and 2 are concerned.
- Counter 3 is incremented after each instruction of $S$.
- Control state $q_h$ cannot be reached in $S$ iff for the unique run of $S'$, the counter 3 has no bounded value.
Step II

- Gainy counter automaton $S''$ with 6 counters:
  - The counters 1, 2 and 3 roughly behave as the 3 respective counters in $S'$.  
  - Counter 4 is the global budget that is progressively incremented.
  - Counter 5 is the current budget. It records how many increments on one of the counters 1, 2 or 3 can be still performed. E.g., increment of counter 3 is followed by decrement of counter 5.
  - Counter 6 is auxiliary.

- We shall implement two subroutines: $\text{copy}(4, 5)$ and $\text{transfer}(1 + 2 + 3, 5)$
copy(4, 5) and transfer(1 + 2 + 3, 5)
(incrementating errors can occur)
Gainy counter automata $S''$

Simulation of $S'$

MO: Memory Overflow

transfer($1 + 2 + 3, 5$)
Simulation of $S'$

- A transition $q \xrightarrow{\text{dec}(i)} q'$ is simulated by $q \xrightarrow{\text{dec}(i)} \circ \xrightarrow{\text{inc}(5)} q'$. The location $\circ$ is an arbitrary new location only used to simulate this transition.

- A transition $q \xrightarrow{\text{zero}(i)} q'$ is simulated by itself.

- A transition $q \xrightarrow{\text{inc}(i)} q'$ is simulated by $q \xrightarrow{\text{inc}(i)} \circ \xrightarrow{\text{dec}(5)} q'$ and $\circ \xrightarrow{\text{zero}(5)} \text{MO}$. 


Non-reachability and repeated reachability

- One shall show that $S$ cannot reach $q_h$ iff $S''$ visits infinitely often the control state (1).
- $S$ cannot reach $q_h$ iff $S'$ cannot reach $q_h$.
- If $S'$ cannot reach $q_h$, then an error-free run of $S''$ visits infinitely often (1).
Converse direction

- Converse direction uses these facts:
  - In (A), the only way to decrement counter 5 is to simulate exactly $S'$. 
  - In order to reach (1), in the part between $q_i$ and (A), counter 5 is decremented regularly.
  - If $S''$ visits infinitely often (1) and $S'$ can reach some configuration $(q_h, \vec{x})$, then at some point an error-free simulation of $S'$ shall be done with value for counter 5 greater than $\vec{x}(1) + \vec{x}(2) + \vec{x}(3)$, a contradiction.

- **Theorem**: control state repeated reachability problem restricted to gainy counter automata is undecidable.
Affine Counter Systems with Finite Monoids
Overview

- Introduction to the class of admissible counter systems.
- Reachability relation is effectively semilinear.
- Existential model-checking problem for $\text{LTL}^{\text{CS}}(\text{PrA})$ restricted to such counter systems is decidable.
Affine functions

• Binary relation of dimension \( n \): relation \( R \subseteq \mathbb{N}^{2n} \).

• \( R \) is Presburger definable \( \iff \) there is a Presburger formula \( \varphi(x_1, \ldots, x_n, x'_1, \ldots, x'_n) \) such that \( R = \text{REL}(\varphi) \).

\[
\left( \text{REL}(\varphi(x_1, \ldots, x_k)) \right) \overset{\text{def}}{=} \{ (v(x_1), \ldots, v(x_k)) \in \mathbb{N}^k : v \models \varphi \}.
\]

• Partial function \( f : \mathbb{N}^n \to \mathbb{N}^n \) is affine \( \iff \) there exist a matrix \( A \in \mathbb{Z}^{n \times n} \) and \( \vec{b} \in \mathbb{Z}^n \) such that for every \( \vec{a} \in \text{dom}(f) \),

\[
f(\vec{a}) = A\vec{a} + \vec{b}
\]

• \( f \) is Presburger definable \( \iff \) the graph of \( f \) is a Presburger definable relation.
Affine counter systems

- Affine counter system $\mathcal{S} = (Q, n, \delta)$: for every transition $q \xrightarrow{\varphi} q' \in \delta$, $\text{REL}(\varphi)$ is affine.

- $\varphi$ can be encoded by a triple $(A, \vec{b}, \psi)$ such that
  1. $A \in \mathbb{Z}^{n \times n}$,
  2. $\vec{b} \in \mathbb{Z}^n$,
  3. $\psi$ has free variables $x_1, \ldots, x_n$,
  4. $\text{REL}(\varphi) = \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \vec{x}' = A\vec{x} + \vec{b} \text{ and } \vec{x} \in \text{REL}(\psi)\}$.

- Guard $\psi$ and deterministic update function $(A, \vec{b})$. 
Composing two affine updates

Let \((A_1, \vec{b}_1, \psi_1)\) and \((A_2, \vec{b}_2, \psi_2)\) be two affine updates. There is \((A, \vec{b}, \psi)\) such that

\[
\text{REL}((A, \vec{b}, \psi)) = \{(\vec{x}, \vec{x'}) \in \mathbb{N}^{2n} : \exists \vec{y} \in \mathbb{N}^n (\vec{x}, \vec{y}) \in \text{REL}((A_1, \vec{b}_1, \psi_1)) \\
\text{and } (\vec{y}, \vec{x'}) \in \text{REL}((A_2, \vec{b}_2, \psi_2))\}
\]

- \(A = A_2A_1\).
- \(\vec{b} = A_2\vec{b}_1 + \vec{b}_2\).
- \(\psi = \exists \vec{y} \psi_1(\vec{x}) \land \vec{y} = A_1\vec{x} + \vec{b}_1 \land \psi_2(\vec{y})\).
Loop effect

\[(A, \vec{b}, \psi)\]

- How to represent symbolically
  \[X = \{(\vec{x}, \vec{x}^\prime) \in \mathbb{N}^{2n} : (q, \vec{x}) \rightarrow (q, \vec{x}^\prime)\} \]

- Is \(X\) definable in Presburger arithmetic?

- Reflexive and transitive closure \(R^* \subseteq \mathbb{N}^{2n}\) of \(R \subseteq \mathbb{N}^{2n}\):
  \[(\vec{y}, \vec{y}^\prime) \in R^* \text{ iff there are } \vec{x}_1, \ldots \vec{x}_k \in \mathbb{N}^n \text{ such that}\]
  - \(\vec{x}_1 = \vec{y}\),
  - \(\vec{x}_k = \vec{y}^\prime\),
  - for \(i \in [1, k - 1]\), we have \((\vec{x}_i, \vec{x}_{i+1}) \in R\).
Loop effect (II)

• If $R$ is Presburger definable, this does not imply that $R^*$ is Presburger definable too.

• $R = \{(\alpha, 2\alpha) \in \mathbb{N}^2 : \alpha \in \mathbb{N}\}$.
  • $R^* = \{(\alpha, 2^\beta \alpha) \in \mathbb{N}^2 : \alpha, \beta \in \mathbb{N}\}$.
  • If $R^*$ is Presburger definable, then so is $\{2^\beta \in \mathbb{N} : \beta \in \mathbb{N}\}$.
  • Semilinear subset of $\mathbb{N}$ are ultimately periodic.
  • $\rightarrow R^*$ is not Presburger definable.

• If $S = \{(\alpha, \alpha + 1) \in \mathbb{N}^2 : \alpha \in \mathbb{N}\}$ then
  $S^* = \{(\alpha, \beta) \in \mathbb{N}^2 : \alpha < \beta, \alpha, \beta \in \mathbb{N}\}$ is Presburger definable.
Presburger counting iteration

- The counting iteration of $R \subseteq \mathbb{N}^{2n}$ is $R_{\text{CI}} \subseteq \mathbb{N}^n \times \mathbb{N} \times \mathbb{N}^n$ such that $(\vec{a}, i, \vec{b}) \in R_{\text{CI}}$ iff $(\vec{a}, \vec{b}) \in R^i$.

- $R$ has a Presburger counting iteration if its counting iteration is Presburger definable.

- $\{ (\alpha, \alpha + 1) \in \mathbb{N}^2 : \alpha \in \mathbb{N} \}$ has a Presburger counter iteration.

- For $A \in \mathbb{Z}^{n \times n}$, $A^*$ denotes the monoid generated from $A$ with $A^* = \{ A^i : i \in \mathbb{N} \}$.

- The identity element is $A^0 = I$.

- Given $A \in \mathbb{Z}^{n \times n}$, checking whether the monoid generated by $A$ is finite, is decidable [Mandel & Simon, TCS 77].
Main result

- Let $R = \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \vec{x}' = A\vec{x} + \vec{b} \text{ and } \vec{x} \in \text{REL}(\psi)\}$.

- **Theorem:** If $A^*$ is finite, then $R$ has a Presburger counting iteration.

  [Boigelot, PhD 98; Finkel & Leroux, FSTTCS’02]

- In CA, $A$ is the identity and therefore $A^*$ is finite.

- General theme in the literature to determine when Presburger definable relations admit Presburger definable reflexive and transitive closure.
Admissible counter systems

• A loop in an affine counter system has the finite monoid property $\text{def} \iff A^* \text{ is finite for its corresponding affine update } (A, \vec{b}, \psi)$.

• Admissible counter system $S$:
  1. $S$ is an affine counter system,
  2. there is at most one transition between two control states,
  3. its control graph is flat,
  4. each loop has the finite monoid property.

• Consequently, the effect of each loop can be defined in Presburger Arithmetic.
A CS is flat if every control state belongs to at most one simple cycle. Moreover, there is at most one transition between two control states.
Reachability is semilinear!

Let $S$ be an admissible counter system and $q, q' \in Q$. One can effectively compute $\varphi$ such that for every $v$, we have $v \models \varphi$ iff $(q, (v(x_1), \ldots, v(x_n))) \xrightarrow{*} (q', (v(x'_1), \ldots, v(x'_n)))$. [Finkel & Leroux, FSTTCS’02; Leroux, PhD 03]

First, build FSA $A$ that overapproximates the language of transitions between $q$ and $q'$ (ignore counter values).
Decidable model-checking problem

- \( \text{LTL}^{\text{CS}}(\text{PrA}) \) formulae:
  \[
  \varphi ::= \psi \mid q \mid \varphi \land \varphi \mid \neg \varphi \mid X\varphi \mid \varphi U \varphi \mid \exists y \varphi
  \]

- **Theorem:** Existential model-checking problem for \( \text{LTL}^{\text{CS}}(\text{PrA}) \) restricted to admissible counter systems is decidable.

- The proof partly uses that the reachability relation for admissible counter systems is effectively semilinear . . .

- . . . but this is not sufficient to show the result.
Proof – Showing a stronger property

- Instance: $S = (Q, n, \delta), (q, \vec{x}), \varphi$.

- W.l.o.g., $\varphi$ has no control states as atomic formulae.

- We wish to check whether there is an infinite run $\rho$ from $(q, \vec{x})$ such that $\rho, 0 \models \varphi$.

- We build $\psi$ such that for every $v$, propositions below are equivalent:
  1. $v \models \psi$.
  2. $\exists$ an infinite run $\rho$ from $(q, (v(x_1), \ldots, v(x_n)))$ s.t. $\rho, 0 \models \varphi$.

- It remains to test the satisfaction of $\psi \land (\bigwedge_{i\in[1,n]} x_i = \vec{x}(i))$. 
Proof – Run schemata

- Run schemata:
  \[ t_1 t_3 (t_4 t_2 t_3)^* t_5 t_6^\omega, t_1 t_3 (t_4 t_2 t_3)^\omega, t_7 t_8 (t_{10} t_9)^* t_{11} t_6^\omega, t_7 t_8 (t_{10} t_9)^\omega. \]

- Number of run schemata is at most exponential in \( \text{card}(Q) \).

- The run schemata can be effectively computed.
Quantifying over runs with natural numbers

• From \( L = u_1(v_1)^* u_2(v_2)^* \cdots (v_k)^\omega \) and \( m_1, \ldots, m_{k-1} \in \mathbb{N} \), we get the sequence

\[
u_1(v_1)^{m_1} u_2(v_2)^{m_2} \cdots (v_k)^\omega\]

• The sequence may correspond to an infinite run from \((q, \vec{x})\) (but not necessarily).

• With \( L \) and \( m_1, \ldots, m_{k-1} \), there is at most one infinite run from \((q, \vec{x})\) respecting \( u_1(v_1)^{m_1} u_2(v_2)^{m_2} \cdots (v_k)^\omega \).

• Indeed, update functions in affine CS are deterministic.
Proof – Auxiliary formulae

- Auxiliary Presburger formulae such that for every $v$,
  - $v \models \exists^L(z_1, \ldots, z_{k-1}, \bar{x})$ iff there is an infinite run from $(q, (v(x_1), \ldots, v(x_n)))$ resp. $u_1(v_1)v(z_1)u_2(v_2)v(z_2)\ldots(v_k)^\omega$.
  - $v \models \chi^\text{steps}_L(z_1, \ldots, z_{k-1}, \bar{x}, z, \bar{x}')$ iff $v \models \exists^L(z_1, \ldots, z_{k-1}, \bar{x})$ and the $v(z)$th tuple of counter values is $(v(x'_1), \ldots, v(x'_n))$.

- $\psi$ defined as a disjunction:

$$\bigvee_{L = u_1(v_1)^*u_2(v_2)^*\ldots(v_k)^\omega} (\exists z_1, \ldots, z_{k-1}, z_0 \chi^L(z_1, \ldots, z_{k-1}, \bar{x}) \land z_0 = 0 \land t_L(z_0, \varphi))$$
From FO-definable temporal operators to FO on \((\mathbb{N}, +)\)

- \(t_L\) is homomorphic for Boolean connectives.
- \(t_L(z, x\psi') \overset{\text{def}}{=} \exists z' (z' = z + 1) \land t_L(z', \psi')\).
- The definition of \(t_L(z, \psi_1 \cup \psi_2)\) is analogous.
- \(t_L(z, \forall y \psi') \overset{\text{def}}{=} \forall y t_L(z, \psi')\).
- \(t_L(z, \psi'(\vec{y}, \vec{x})) \overset{\text{def}}{=} \forall \vec{x'} (\chi_L^{\text{steps}}(z_1, \ldots, z_{k-1}, \vec{x}, z, \vec{x'}) \Rightarrow \psi'(\vec{y}, \vec{x'}))\) where \(\psi'(\vec{y}, \vec{x})\) is an atomic formula with a tuple \(\vec{y}\) of variables from \(\text{VAR}^p\).
Open problems

- Computational complexity of the model-checking problem for LTLCS(PrA) restricted to ACS is still open.

- Decidability extends to a CTL* extension of LTLCS(PrA). What about the linear $\mu$-calculus extension?

- Which conditions in the definition of admissible counter systems can be relaxed so that the model-checking problem for LTLCS(PrA) remains decidable?

- ...but a slight relaxation can lead to undecidability.
Undecidable model-checking problem

\[
x_1' = x_1 + 1 \quad x_2' = x_2 + 1 \quad x_3' = x_3 + 1
\]

- Existential model-checking problem for \( \text{LTL}^{CS}(\text{PrA}) \) restricted to the affine counter system \( S_u \) is undecidable.
- Reduction from the recurrence problem for ND Minsky machines.
Concluding remarks

- Today’s lecture:
  - Repeated reachability problem for several classes.
  - Plain LTL for several classes of counter systems.
  - $LTL^{CS}(PrA)$ for admissible counter systems.

- We have illustrated two proof techniques:
  1. Combining repeated reachability with standard automata-based approach for temporal logics.
  2. Translation into the decidable Presburger Arithmetic.