Rudiments of Presburger Arithmetic

Stéphane Demri (demri@lsv.fr)

October 9th, 2015
Slides and lecture notes

http://www.lsv.fr/~demri/notes-de-cours.html

About the lectures 1, 2 & 3

- Theory of well-quasi orderings.
- Presburger counter machines.
- Motivations for a logical formalisms about arithmetical constraints.
- Basis of the theory of well-structured transition systems.
- Covering problem for lossy counter machines is Ackermann-hard.
Plan of the talk

- Introduction to Presburger arithmetic.
- Decidability and quantifier elimination.
- Decidability by the automata-based approach.
A Formalism for Arithmetical Constraints
A fundamental decidable theory

- First-order theory of \( \langle \mathbb{N}, +, \leq \rangle \) introduced by Mojcesz Presburger (1929).

- Handy to express guards and updates in counter machines:
  \[
  x++ \approx x' = x + 1 \\
  x_1 + x_2 = x_B \land x_1 < 36
  \]

- Nondeterministic update in a lossy counter machine:
  \[
  x' \leq x + 1
  \]

- Formulae are viewed as symbolic representations for (infinite) sets of tuples of natural numbers.

  \[
  x \leq y \text{ can be interpreted as } \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n \leq m \}
  \]
Symbolic representation in counter machines

- Counter machine with two counters and with at least the locations $q_0$ (initial), $q_1$ and $q_2$.

- Suppose $\varphi_1(x, y)$ interpreted as

$$X_1 = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid \langle q_0, 0, 0 \rangle \rightarrow^* \langle q_1, n, m \rangle \}$$

- Suppose $\varphi_2(x, y)$ interpreted as

$$X_2 = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid \langle q_0, 0, 0 \rangle \rightarrow^* \langle q_2, n, m \rangle \}$$

- Equivalence between the statements below:
  
  - Every pair of counter values from a reachable configuration with location $q_1$ is also a pair of counter values from a reachable configuration with location $q_2$.
  
  - $X_1 \subseteq X_2$.

  - $\varphi_1(x, y) \Rightarrow \varphi_2(x, y)$ is always true.
Essential properties for formal verification

- Rich logical language: captures most standard updates and guards in counter machines (and more).

- Decidability of the satisfiability and validity problems. Worst-case complexity characterised (below $2 \exp^{\exp^{\text{SPACE}}}$).

- Handy language with unrestricted quantifications but those quantifications can be viewed as concise macros.

- Expressive power of the language is known: Presburger sets = semilinear sets.

- Formalism also used to express constraints on graphs, on number of events, etc.

  See e.g., [Seidl & Schwentick & Muscholl, chapter 07]
Presburger arithmetic [Presburger, 29]

- “First-order theory of $\langle \mathbb{N}, +, \leq \rangle$” (no multiplication).

- A property about the structure $\langle \mathbb{N}, +, \leq \rangle$:

  $$\forall x \ (\exists y ((2x + 8) \leq y))$$

- Atomic formula $((2x + 8) \leq y)$.

- Term $(2x + 8)$.

- Variables $x$ and $y$.

- Given $\text{VAR} = \{x, y, z, \ldots\}$, the terms are of the form

  $$a_1x_1 + \cdots + a_nx_n + k$$

  with $a_1, \ldots, a_n, k \geq 0$. 
Valuations

- Valuation $\nu$: $\text{VAR} \rightarrow \mathbb{N}$.

- Extending $\nu$ to all terms:
  - $\nu(k) = k$.
  - $\nu(ax) = a \times \nu(x)$.
  - $\nu(t + t') = \nu(t) + \nu(t')$.

- Satisfaction relation $\models$
  - $\nu \models (2x + 8) \leq y$ with $\nu(x) = 3$ and $\nu(y) = 27$.
  - $\nu \not\models (2x + 8) \leq y$ with $\nu(x) = 3$ and $\nu(y) = 13$. 
Formulae (1/2)

- Atomic formula $t \leq t'$.

- $v \models t \leq t' \overset{\text{def}}{\iff} v(t) \leq v(t')$.

- Formulae are built from Boolean connectives and quantifiers.

- Abbreviations:
  
  $t = t' \overset{\text{def}}{=} (t \leq t') \land (t' \leq t)$
  
  $t < t' \overset{\text{def}}{=} t + 1 \leq t'$
  
  $t \geq t' \overset{\text{def}}{=} t' \leq t$
  
  $t > t' \overset{\text{def}}{=} t' + 1 \leq t$
Formulae (2/2)

\[ \varphi ::= \top | \bot | t \leq t' | \neg \varphi | \varphi \land \varphi | \varphi \lor \varphi | \exists x \varphi | \forall x \varphi \]

where \( t \) and \( t' \) are terms and \( x \in \text{VAR} \).

- Infinite number of multiple of 3:
  \[ \forall x (\exists y (y > x) \land (\exists z (y = 3z))). \]

- Oddness: \( \exists y x = 2y + 1 \).
Semantics

▶ $v \models T \iff \text{true}; v \models \bot \iff \text{false},$

▶ $v \models t \leq t' \iff v(t) \leq v(t'),$

▶ $v \models \neg \varphi \iff \text{not } v \models \varphi,$

▶ $v \models \varphi \land \varphi' \iff v \models \varphi \text{ and } v \models \varphi',$

▶ $v \models \varphi \lor \varphi' \iff v \models \varphi \text{ or } v \models \varphi',$

▶ $v \models \exists x \varphi \iff \text{there is } n \in \mathbb{N} \text{ such that } v[x \mapsto n] \models \varphi \text{ where } v[x \mapsto n] \text{ is equal to } v \text{ except that } x \text{ is mapped to } n,$

▶ $v \models \forall x \varphi \iff \text{for every } n \in \mathbb{N}, \text{ we have } v[x \mapsto n] \models \varphi.$
Standard first-order semantics

- $v \models t = t'$ (where $t = t'$ is an abbreviation) iff $v(t) = v(t')$.

- $\varphi$ and $\psi$ are equivalent in $\text{FO}(\mathbb{N})$ $\text{def}$ for every valuation $v$, we have $v \models \varphi$ iff $v \models \psi$.

- $\varphi_1 \land \varphi_2$ and $\neg(\neg \varphi_1 \lor \neg \varphi_2)$ are equivalent formulae.

- $\exists x \varphi$ and $\neg \forall x \neg \varphi$ are equivalent formulae.

- $\forall x \exists y (y < x)$ and $\forall x \exists y (x < y)$ are not equivalent.
Total ordering

- $\varphi_{\text{tot}}$: $\langle \mathbb{N}, \prec \rangle$ is a linearly ordered set:
  \[
  \varphi_{\text{tot}} \overset{\text{def}}{=} \forall x \forall y ((x = y) \lor (x < y) \lor (x > y)).
  \]

- Key argument: for all valuations $\nu$,
  \[
  \nu \models (x = y) \lor (x < y) \lor (x > y)
  \]
Standard notations

- $\forall x_1 \cdots \forall x_n \varphi$ is also written

  $\forall x_1, \ldots, x_n \varphi$

- $\forall x \ (x \leq k) \Rightarrow \varphi$ is also written

  $\forall_{\leq k} x \varphi$

- $3y \leq 7x + 8$ is also written

  $-2x + 3y - 8 \leq 5x$
Modulo constraints

▶ $x \equiv_k 0$ is an abbreviation for $\exists y \ (x = ky)$.

▶ $t \equiv_k t'$ is an abbreviation for

$$\exists x \ (t = kx + t') \lor (t' = kx + t)$$

▶ Example of formula in $\mathsf{FO(\mathbb{N})}$ (with various abbreviations):

$$\forall x, y \ (-2x + 9 \equiv_4 y + 1) \iff (-y \equiv_4 2x - 8)$$
Satisfiability problem

Input: a formula $\varphi$
Question: is there a valuation $v$ such that $v \models \varphi$?

Satisfiable formula:

$$(x_1 \geq 2) \land (x_2 \geq 2x_1) \land \cdots \land (x_n \geq 2x_{n-1})$$
(take $v(x_i) = 2^i$)

Validity problem

Input: a formula $\varphi$
Question: is the case that for every valuation $v$, we have $v \models \varphi$?

Valid formula:

$$(x_1 \geq 2 \land x_2 \geq 2x_1 \land \cdots \land x_n \geq 2x_{n-1}) \implies x_n \geq 2^n$$
Equivalences (1/2)

▶ \( \varphi \): formula whose free variables are among \( x_1, \ldots, x_n \).

▶ The propositions below are equivalent:

   (I) \( \varphi \) is valid.

   (II) \( \forall x_1, \ldots, x_n \varphi \) is valid.

   (III) \( \forall x_1, \ldots, x_n \varphi \) is satisfiable.

   (IV) \( \forall x_1, \ldots, x_n \varphi \) is equivalent to \( \top \).
Equivalences (2/2)

- $\varphi$: formula whose free variables are among $x_1, \ldots, x_n$.

- The propositions below are equivalent:
  
  (I) $\varphi$ is satisfiable.

  (II) $\exists x_1, \ldots, x_n \varphi$ is valid.

  (III) $\exists x_1, \ldots, x_n \varphi$ is satisfiable.

  (IV) $\exists x_1, \ldots, x_n \varphi$ is equivalent to $\top$. 
Defining sets of tuples

- Formula $\varphi(x_1, \ldots, x_n)$ with $n$ free variables:

  \[
  \llbracket \varphi(x_1, \ldots, x_n) \rrbracket \overset{\text{def}}{=} \{ \langle v(x_1), \ldots, v(x_n) \rangle \in \mathbb{N}^n : v \models \varphi \} 
  \]

- $\llbracket x_1 < x_2 \rrbracket = \{ \langle n, n' \rangle \in \mathbb{N}^2 : n < n' \}$.

- $\llbracket x = x + x \rrbracket = \{ 0 \}$.

- $\varphi$ is satisfiable iff $\llbracket \varphi \rrbracket$ is non-empty.

- $\varphi$ is valid (with free variables $x_1, \ldots, x_n$) iff $\llbracket \varphi \rrbracket = \mathbb{N}^n$. 
Presburger sets

- $X \subseteq \mathbb{N}^d$ is a Presburger set $\iff$ there is $\varphi$ with free variables $x_1, \ldots, x_d$ such that $\llbracket \varphi \rrbracket = X$.

$$\llbracket x_1 \geq 1 \land x_2 \geq 3 \land x_1 + x_2 \geq 6 \rrbracket = \{ \langle n, m \rangle \mid \langle q_1, 0, 0 \rangle \xrightarrow{*} \langle q_4, n, m \rangle \}$$
A rough analysis

\[ \begin{align*}
[x_1 = x_2 = 0] &= \{ \langle n, m \rangle \mid \langle q_1, 0, 0 \rangle \xrightarrow{*} \langle q_1, n, m \rangle \} \\
[x_2 = 1 \land x_1 \geq 1] &= \{ \langle n, m \rangle \mid \langle q_1, 0, 0 \rangle \xrightarrow{*} \langle q_2, n, m \rangle \} \\
[x_2 \geq 2 \land x_1 + x_2 \geq 4] &= \{ \langle n, m \rangle \mid \langle q_1, 0, 0 \rangle \xrightarrow{*} \langle q_3, n, m \rangle \} \\
[x_1 \geq 1 \land x_2 \geq 3 \land x_1 + x_2 \geq 6] &= \{ \langle n, m \rangle \mid \langle q_1, 0, 0 \rangle \xrightarrow{*} \langle q_4, n, m \rangle \}
\end{align*} \]
With quantifiers

\[ \exists z_1, z_2, z_3 \ (x_1 = 3 + z_1 - z_2) \land (x_2 = 3 + z_2 + z_3) \land 2 + z_1 - z_2 \geq 0 \]

(equivalent to add \((x_1 \geq 1)\))

---

Diagram:

- **q₁** \(\xrightarrow{x_1++; \ x_2++} q₂\)
- **q₂** \(\xrightarrow{x_1++; \ x_2++;} q₃\)
- **q₃** \(\xrightarrow{x_1++; \ x_2++;} q₄\)
- **q₄** \(\xrightarrow{x_2++} q₁\)
Always good to capture the reachability sets

- Suppose $\llbracket \varphi_q \rrbracket = \{x \in \mathbb{N}^n : \langle q_0, x_0 \rangle \xrightarrow{*} \langle q, x \rangle \}$ for every control state/location $q$.

- $\{x \in \mathbb{N}^n : \langle q_0, x_0 \rangle \xrightarrow{*} \langle q, x \rangle \}$ is infinite iff the formula below is satisfiable:

  $$\neg \exists y \forall x_1, \ldots, x_n \varphi_q(x_1, \ldots, x_n) \Rightarrow (x_1 \leq y \land \cdots \land x_n \leq y)$$

- $\langle q_0, x_0 \rangle \xrightarrow{*} \langle q, z \rangle$ iff the formula below is satisfiable:

  $$\varphi_q(x_1, \ldots, x_n) \land x_1 = z(1) \land \cdots \land x_n = z(n),$$

- Control state $q$ can be reached from $\langle q_0, x_0 \rangle$ iff the Presburger formula $\varphi_q(x_1, \ldots, x_n)$ is satisfiable.
Refinement: new set of atomic formulae

\[ \top \mid \bot \mid t \leq t' \mid t \equiv_k t' \mid t = t' \mid t < t' \mid t \geq t' \mid t > t' \] (PAF)

- A formula \( \varphi \) is quantifier-free \( \iff \) \( \varphi \) is a Boolean combination of atomic formulae (i.e. without quantifiers).

\[(x + y \equiv_5 z) \lor (y > 23)\]

- Linear fragment (LIN) –i.e. \( = \) (PAF) \( \setminus \) modulo constraints

\[ \top \mid \bot \mid t \leq t' \mid t = t' \mid t < t' \mid t \geq t' \mid t > t' \] (LIN)
More fragments

Difference fragment: \( \phi \) is in the difference fragment \( \iff \phi \) belongs to the linear fragment and the terms are of the form either \( x + k \) or \( k \).

\[
\text{in: } \neg(x = y + 8) \land y \geq 7.
\]

\[
\text{out: } 2x = 6 \text{ and } x + y \geq 3.
\]

Prenex normal form:

\[
Q_1 x_1 \cdots Q_n x_n \psi
\]

with \( \psi \) in the linear fragment and \( \{Q_1, \ldots, Q_n\} \subseteq \{\exists, \forall\} \).

\[\neg(\exists \ x \ x \geq 3) \lor (\forall \ y \ y \geq 4) \text{ is equivalent to } \forall \ x \ \forall \ y \ (\neg(x \geq 3) \lor y \geq 4)\]

Extended prenex normal form:

\[
(Q_1)_{\leq k_1} x_1 \cdots (Q_n)_{\leq k_n} x_n \psi
\]

with \( \psi \) is in (LIN), \( \{Q_1, \ldots, Q_n\} \subseteq \{\exists, \forall\} \) and \( k_1, \ldots, k_n \in \mathbb{N} \).
The difficulty of the satisfiability problem

- Obviously the domain of the quantified variables is infinite.

- Assume that terms in quantifier-free formulae can be written as \((\sum_i a_i x_i) + k\) where the \(a_i\)'s and \(k\) belong to \(\mathbb{N}\) and the natural numbers are encoded in binary.

- \(\varphi\) quantifier-free formula with variables \(x_1, \ldots, x_n\) is satisfiable iff there is a valuation

\[
v : \{x_1, \ldots, x_n\} \rightarrow [0, 2^{p(|\varphi|)}]
\]

such that \(v \models \varphi\).

- \(p(\cdot)\) is a polynomial independent of \(\varphi\) and \(x_1, \ldots, x_n\).

- The theorem exists in many variants: it is possible to refine this bound by taking into account in a more precise way,
  - the number of variables,
  - the maximal size of a constant occurring in \(\varphi\) or,
  - the number of connective occurrences with the a conjunctive polarity.
NP-completeness

- The satisfiability problem for the quantifier-free fragment is NP-complete.

- NP-hardness (straightforward):
  - $\varphi$ with propositional variables $p_1, \ldots, p_n$.
  - $\varphi'$ obtained from $\varphi$ by replacing $p_i$ by $x_i^{\text{new}} = y_i^{\text{new}}$.
  - $\varphi$ is satisfiable iff $\varphi'$ is satisfiable.
NP upper bound

- Guess
  \[ \langle \alpha_1, \ldots, \alpha_n \rangle \in [0, 2^{p(|\varphi|)}]^n \]

- Check that \( v \models \varphi \) where \( v(x_i) = \alpha_i \) for every \( i \in [1, n] \).

- Can be done in polynomial time in the size of the formula:
  1. \( \langle \alpha_1, \ldots, \alpha_n \rangle \) is of polynomial size in \( |\varphi| \).
  2. Computing \( v(t) \) for any term \( t \) in \( \varphi \) can be done in polynomial time in \( |\varphi| \).
  3. Determining the truth value of any atomic formula under \( v \) can be done in polynomial time in \( |\varphi| \).
  4. Replacing all the atomic formulae from \( \varphi \) by either \( \top \) or \( \bot \) and then simplifying leads to \( \top \) or \( \bot \) and can be done in polynomial time.
Decidability and quantifier elimination

- **Theorem**: The satisfiability problem for Presburger arithmetic is decidable. [Presburger, 29]

- Every Presburger formula is effectively equivalent to a Presburger formula without first-order quantification. [Presburger, 29]
  
  (periodicity atomic formulae are needed here)

- Satisfiability problem for quantifier-free formulae is NP-complete. [Papadimitriou, JACM 81]

  See also [Borosh & Treybig, AMS 76]

- About other first-order theories
  
  - Skolem arithmetic $\langle \mathbb{N}, 0, 1, \times \rangle$ is decidable.
  
  - $\langle \mathbb{Z}, \leq, + \rangle$ is decidable.

  - $\langle \mathbb{N}, \leq, \times, + \rangle$ is undecidable.
A few words about the computational complexity

- Satisfiability problem is between $2\text{EXP TIME}$ and $2\text{EXP SPACE}$.

- $2\text{EXP SPACE}$ is included in $3\text{EXP TIME}$. [Oppen, JCSS 78]

- More precisely: completeness for the class of alternating Turing machines working in double exponential time with at most a linear amount of alternations. [Berman, TCS 80]

- Satisfiability checking for $\varphi$: eliminate quantifiers in $\exists x_1, \ldots, x_d \varphi$ and verify it leads to $\top$. 
A small model property

\[ \varphi = \forall_1 x_1 \cdots \forall_s x_s \psi(x_1, \ldots, x_s) \]

\[ \text{in prenex normal form,} \]
\[ \text{of length } n \text{ and,} \]
\[ \text{with } m \text{ quantifier alternations.} \]

\[ w = 2^{C \times n^{(s+3)m+2}} \]

for some constant \( C \).

\[ \varphi \text{ is satisfiable iff} \]
\[ \left( \forall_1 \right)_{\leq w} x_1 \cdots \left( \forall_s \right)_{\leq w} x_s \psi(x_1, \ldots, x_s) \]

is satisfiable.

Decision procedure by trying all the possible values for the variables until \( w \) but care is needed because of the quantifier alternations.
**FO(\mathbb{Z})**

- **FO(\mathbb{Z})**: variant of FO(\mathbb{N}) in which variables are interpreted in \mathbb{Z}.

- **FO(\mathbb{Z})** and FO(\mathbb{N}) have the same of formulae.

- The formula \( \forall x \exists y \ y < x \)
  - is valid in FO(\mathbb{Z})
  - but not in FO(\mathbb{N}).

- The satisfiability problem for FO(\mathbb{Z}) is decidable.

- Proof idea: encode the negative integers \( n \) by \(-2n + 1\) and the positive integers \( m \) by \( 2m \).
Quantifier Elimination
QE: good or bad?

- Quantification elimination means that quantifications are dummy logical operators for $\text{FO}(\mathbb{N})$?

- For instance, disjunction operator $\lor$ can be eliminated in propositional calculus with $\neg$ and $\land$ only.

- But NP-completeness of the quantifier-free fragment whereas 2$\text{E}XP\text{TIME}$-hardness of the full logic.

- Analogy: linear-time temporal logic LTL and first-order logic on $\omega$-words have the same expressiveness but not the same conciseness and computational complexity.
Simple quantifier eliminations

\[ \exists x \ (x \geq 3) \quad \text{is equivalent to} \quad \top \]
\[ \exists z \ (x < z \land z < y) \quad \text{is equivalent to} \quad x + 2 \leq y \]
\[ \exists z \ (x < z \lor z < y) \quad \text{is equivalent to} \quad \top \]
\[ \forall z \ (x \leq z \Rightarrow y \leq z) \quad \text{is equivalent to} \quad y \leq x \]
\[ \exists z \ x = 2z \quad \text{is equivalent to} \quad x \equiv_2 0 \]

What about

\[ \exists z \ (\neg(x \leq 2z - 1)) \land (\exists z' \ (z = z') \land (0 \leq 2z' - x)) \]
Why periodicity constraints are needed?

- $t \equiv_2 0$ is simple enough but hides an existential quantification.
- Is there a quantifier-free formula equivalent to $\exists z \ x = 2z$ in the linear fragment?
- $\mathcal{AT}(x)$: set of atomic formulae of the form
  $$ax + b \leq a'x + b'$$
  where $a, a', b, b' \in \mathbb{N}$.
- Every $ax + b \leq a'x + b'$ is equivalent to a formula having one of the forms below:
  $$\top \quad \bot \quad x \leq k \quad x \geq k$$
  where $k \in \mathbb{N}$.
- $3x + 5 \leq x + 8$ is logically equivalent to $x \leq 1$. 

Formula $\psi = \text{Boolean combination of formulae among } \top, \bot \text{ or } x \leq k$.

$[\psi]$ is a finite union of intervals $\bigcup_i l_i$ such that each $l_i$ is of the form either $[k_1, k_2]$ or $[k_1, +\infty[$ with $k_1, k_2 \in \mathbb{N}$.

$[\exists z \; x = 2z]$ is obviously not equal to a finite union of intervals of the form $\bigcup_i l_i$.

$\exists z \; x = 2z$ is not equivalent to a formula in the linear fragment.
Main theorem (QE)

For every formula $\varphi$, there exists a quantifier-free formula $\varphi'$ such that

1. $\text{free}(\varphi') \subseteq \text{free}(\varphi)$.

2. $\varphi'$ is logically equivalent to $\varphi$.

3. $\varphi'$ can be effectively built from $\varphi$.

Property (QE*): restriction of (QE) with $\varphi = \exists x \psi$ and $\psi$ is a Boolean combination of formulae of the form either $t \leq t'$ or $t \equiv_k t'$.

It is sufficient to show (QE*) to get (QE).
How to use \((\text{QE}^*)\) to eliminate quantifiers

\[
\varphi = \exists x (\psi_0(x) \land (\exists y (\psi_1(x, y) \land \exists z \psi_2(x, y, z, z')))\\
\]

(the \(\psi_i\)'s are quantifier-free formulae)

- If \(\exists z \psi_2(x, y, z, z')\) is equivalent to the QF formula \(\psi'_2(x, y, z')\), then \(\varphi\) is equivalent to
  \[
  \exists x (\psi_0(x) \land (\exists y (\psi_1(x, y) \land \psi'_2(x, y, z'))))\\
  \]

- If \(\exists y (\psi_1(x, y) \land \psi'_2(x, y, z'))\) is equivalent to the QF formula \(\psi'_1(x, z')\), then \(\varphi\) is equivalent to
  \[
  \exists x (\psi_0(x) \land \psi'_1(x, z'))\\
  \]

- If \(\exists x (\psi_0(x) \land \psi'_1(x, z'))\) is equivalent to the QF formula \(\psi'_0(z')\), then \(\varphi\) is equivalent to \(\psi'_0(z')\).
Quantifier elimination for $\varphi$

1. Replace every $\forall x \psi$ by $\neg \exists x \neg \psi$, leading to $\varphi'$.

2. If $\varphi'$ is quantifier-free, we are done. Otherwise go to 3.

3. Pick an innermost subformula $\exists x \chi$ with QF $\chi$ and substitute it by an equivalent QF formula thanks to (QE$^*$).

4. Update $\varphi'$ to be this new formula.

5. The number of quantifiers in $\varphi'$ has decreased by one.

6. If $\varphi'$ is quantifier-free, we are done. Otherwise, go to 3.
A simple principle

- $\exists x \varphi$ with $\varphi$ a Boolean combination of formulae of the form $k \leq x$ with $k \in \{k_0, \ldots, k_\beta\}$ and $k_0 = 0$.

- Successive constants

$$
\begin{array}{cccc}
  k_0 & \cdots & k_1 & \cdots & k_2 & \cdots & k_\beta \\
  \bullet & \cdots & \bullet & \cdots & \bullet & \cdots & \bullet
\end{array}
$$

- $n \sim n'$ $\overset{\text{def}}{\iff}$ for all $i \in [0, \beta]$, we have $k_i \leq n$ iff $k_i \leq n'$.

- Equivalence classes with its canonical elements:

$$
\begin{array}{cccc}
  k_0 & \cdots & k_1 & \cdots & k_2 & \cdots & k_\beta \\
  \circ & \cdots & \bullet & \cdots & \bullet & \cdots & \bullet
\end{array}
$$

- $\exists x \varphi$ is equivalent to $\bigvee_i \varphi(x \leftarrow k_i)$,
Quantifier elimination with the fragment ($\dagger$)

- Extended term ($\sum_i a_i x_i + k$) with $a_i$'s and $k$ belong to $\mathbb{Z}$.

- $\varphi = \exists x \chi$ with $\chi$ a QF formula respecting

$$\chi ::= \top \mid \bot \mid t \leq x \mid t \leq t' \mid \neg \chi \mid \chi \land \chi \quad (\dagger)$$

where $t$, $t'$ are extended terms without $x$.

- Variable $x$ has been isolated on one side of the inequalities.

- No atomic formula of the form $t \geq x$ since that is equivalent to $\neg(t + 1 \leq x)$.

- For instance $y \leq 2x$ or $x \equiv_2 0$ do not belong to ($\dagger$).
About valuations

- Any valuation $v : \text{VAR} \rightarrow \mathbb{N}$, can be generalized to extended terms such that

\[
v((\sum_i a_i x_i) + k) \overset{\text{def}}{=} (\sum_i a_i v(x_i)) + k
\]

- Extended terms are interpreted in $\mathbb{Z}$.

- $T$: set of terms $t$ occurring in some atomic formula $t \leq x$, and (possibly) augmented with 0.

- So $T$ is non-empty and contains at most $|\chi|$ elements.

- Given $v : \text{VAR} \rightarrow \mathbb{N}$, there is a term $t_{\text{left}} \in T$ such that
  1. $v(t_{\text{left}}) \leq v(x)$ and,
  2. there is no $t \in T$ such that $v(t_{\text{left}}) < v(t) \leq v(x)$.

- $t_{\text{left}}$ the closest left term (depending on $v$).
A key observation

- For any \( n \in [v(t_{\text{left}}), v(x)] \), \( v \) and \( v[x \mapsto n] \) verify exactly the same atomic formulae from \( \chi \).
  - Interpretation of the terms \( t \) remains unchanged.
    (so truth of \( t \leq t' \) is unchanged).
  - Truth of \( t \leq x \) is unchanged too.
- So, \( v \models \chi \) iff \( v[x \mapsto n] \models \chi \).
- For the satisfaction of \( \varphi \), we can assume that \( x \) is equal to some term \( t \) with \( t \in T \).
Quantifier elimination

- $\varphi = \exists x \, \chi$ is replaced by

$$\bigvee_{t \in T} \chi(x \leftarrow t)$$

- The disjunction can be computed in polynomial time in $|\varphi|$.

- Existential quantification is replaced by a generalized disjunction, which is conceptually sound.

$$\models v \models \bigvee_{t \in T} \chi(x \leftarrow t) \quad \rightarrow \quad v \models \chi(x \leftarrow t) \text{ for some } t \in T$$

$$\rightarrow \quad v[x \mapsto v(t)] \models \chi(x)$$

$$\rightarrow \quad v \models \exists x \, \chi(x)$$
The other direction

\[ v \models \exists x \chi \quad \rightarrow \quad \text{there is } n \in \mathbb{N} \text{ such that } v[x \mapsto n] \models \chi \]

\[ \rightarrow \quad v[x \mapsto v(t_{\text{left}})] \models \chi \]

\[ \rightarrow \quad v \models \chi(x \leftarrow t_{\text{left}}) \]

\[ \rightarrow \quad v \models \bigvee_{t \in T} \chi(x \leftarrow t) \]
QE for $\exists z \ (x < z \land z < y)$

- $\exists z \ (x + 1 \leq z \land \neg(y \leq z))$.

- $T = \{x + 1, y, 0\}$.

\[
\begin{align*}
\top &= (x + 1 \leq x + 1 \land \neg(y \leq x + 1)) \lor \\
&\quad (x + 1 \leq y \land \neg(y \leq y)) \lor \\
&\quad (x + 1 \leq 0 \land \neg(y \leq 0)) \\downarrow \\
\bot &= \neg(y \leq x + 1) \lor x + 2 \leq y.
\end{align*}
\]
Quantifier elimination with the fragment (††)

- \( \varphi = \exists x \chi \) with \( \chi \) a QF formula respecting

\[
\chi ::= \top \mid \bot \mid t \leq ax \mid t \leq t' \mid \neg \chi \mid \chi \land \chi \quad (††)
\]

where \( t, t' \) are extended terms without \( x \) and \( a \geq 1 \).

- \( \ell \): the least common multiple (lcm) of all the coefficients occurring in front of \( x \).

- \( \chi' \): replace in \( \chi \) every \( t \leq ax \) by \( t \times \frac{\ell}{a} \leq \ell x \).

- \( \chi'' \): replace in \( \chi' \) every \( \ell x \) by \( x \).

- \( \varphi \) and \( \exists x (x \equiv \ell 0) \land \chi'' \) are equivalent.
Quantifier elimination with the fragment (††††)

- $\varphi = \exists x \chi$ with $\chi$ a QF formula respecting

$$\chi ::= \top \mid \bot \mid t \equiv_k t' \mid x \equiv_k t \mid t \leq x \mid t \leq t' \mid \neg \chi \mid \chi \land \chi \ (†††)$$

where $t, t'$ are extended terms without $x$, and $k \geq 1$.

- QF formulae in (††††) are almost of the general form except that modulo constraints or inequalities may involve the terms $ax$ with $a > 1$. 
Preliminary simplifications (again)

- $\ell$: lcm of all the coefficients occurring in front of $x$.

- $ax \equiv_k t$ is replaced by $\ell x \equiv (k \times \frac{\ell}{a}) \frac{\ell}{a} t$.

- $t \leq x$ is replaced by $t \times \frac{\ell}{a} \leq \ell x$.

- Then we proceed as for $(††)$ by introducing the conjunct $x \equiv_\ell 0$.

- Value $\ell'$: lcm of all $k_1, \ldots, k_\beta$ such that $x \equiv_{k_i} t$ occurs in $\chi$. 
A key observation (bis)

For any $n \in \{ m \in [v(t_{left}), v(x)] : m \equiv_{\ell'} v(x) \}$, $v$ and $v[x \mapsto n]$ verify exactly the same atomic formulae from $\chi$.

- Interpretation of the terms $t$ remains unchanged. (so truth of $t \leq t'$ or $t \equiv_k t'$ is unchanged).

- Truth of $t \leq x$ is unchanged too (as for ($\dagger$)).

- Truth of $x \equiv_{k_i} t$ is unchanged.

Consequence of the Chinese Remainder Theorem: $n \equiv_{\ell'} n'$ iff ($n \equiv_{k_1} n'$ and $\cdots$ and $n \equiv_{k_\beta} n'$)

- So, $v \models \chi$ iff $v[x \mapsto n] \models \chi$. 
For the satisfaction of $\varphi$, we can assume that $x$ is equal to some term $t$ with $t + j$ such that $t \in T$ and $j \in [0, \ell - 1]$.

$\varphi$ is equivalent to

$$\bigvee_{t \in T, j \in [0, \ell - 1]} \chi(x \leftarrow t + j)$$
Example

- $\exists z \ x = 2z$.

- $\exists z \ (x \leq 2z) \land (\neg (x + 1 \leq 2z))$.

- $\exists z \ (z \equiv_2 0) \land (x \leq z) \land (\neg (x + 1 \leq z))$.

- $T = \{0, x, x + 1\}$.

- $\ell' = 2$. 
\[
\bigvee_{t \in T, j \in [0, \ell' - 1]} \chi(x \leftarrow t + j)
\]

\[
\begin{align*}
\top &\quad \top \\
[&(0 \equiv_2 0) \land (x \leq 0) \land (\neg(x + 1 \leq 0))] \lor \\
[&(1 \equiv_2 0) \land (x \leq 1) \land (\neg x + 1 \leq 1)] \lor \\
\bot &
\end{align*}
\]

\[
\begin{align*}
\top &\quad \top \\
[&(x \equiv_2 0) \land (x \leq x) \land (\neg(x + 1 \leq x))] \lor \\
[&(x + 1 \equiv_2 0) \land (x \leq x + 1) \land (\neg x + 1 \leq x + 1)] \lor \\
\bot &
\end{align*}
\]

\[
\begin{align*}
\top &\quad \top \\
[&(x + 1 \equiv_2 0) \land (x \leq x + 1) \land (\neg(x + 1 \leq x + 1))] \lor \\
\bot &
\end{align*}
\]

\[
\begin{align*}
\top &\quad \top \\
[&(x + 2 \equiv_2 0) \land (x \leq x + 2) \land (\neg(x + 1 \leq x + 2))] \\
\bot &
\end{align*}
\]

Equivalent to \((x \leq 0) \lor (x \equiv_2 0)\) and therefore to \(x \equiv_2 0\).
Corollaries

- $\exists \overline{x} \varphi(\overline{x})$ is equivalent to either $\top$ or $\bot$.

- Decidability is a consequence of quantifier elimination.

- Exponential blow-up while quantifiers are eliminated.
Decision procedures and tools

- **Quantifier elimination and refinements**
  [Cooper, ML 72; Reddy & Loveland, STOC’78]

- **Tools dealing with quantifier-free PA, full PA or quantifier elimination: Z3, CVC4, Alt-Ergo, Yices2, Omega test.**

- **Automata-based approach.**
  [Büchi, ZML 60; Boudet & Comon, CAAP’96]

- **Automata-based tools for Presburger arithmetic: LIRA, suite of libraries TAPAS, MONA, and LASH.**
Automata-Based Approach
Automata-based approach consists in reducing logical problems into automata-based decision problems.

Examples of target problems:
- \( L(A) = \emptyset \)?
- \( L(A) \subseteq L(B) \)?
- Is \( L(A) \) the universal language?

Pioneering work by Büchi [Büchi, 62].
- MSO over \( \langle \mathbb{N}, < \rangle \).
- Models of a formula over \( P_1, \ldots, P_N \) are \( \omega \)-sequences over the alphabet \( \mathcal{P}(\{P_1, \ldots, P_N\}) \).
- Büchi automata are equivalent to MSO formulae.
Desirable properties

- **Reduction is simple.**
  ex: LTL formula $\mapsto$ alternating automaton

- **Complexity** of the automata-based target problem is well-characterised.
  ex: PDL formula $\mapsto$ nondeterministic Büchi tree automaton.

- Reduction allows to obtain the **optimal** complexity of the source logical problem.
  ex: CTL model-checking is in $\text{PTIME}$ by reduction into hesitant alternating automata (HAA).
A few words about regular model-checking

- To represent sets of configurations by regular sets of finite words (or infinite words, trees, etc.)

- Transducers encode the transition relations of the systems.

- Regularity is typically captured by finite-state automata.
Tuples of natural numbers as finite words

- To represent $[\varphi] \subseteq \mathbb{N}^n$ by a (regular) set of finite words over the alphabet $\{0, 1\}^n$.

- Encoding map $f : \mathbb{N} \rightarrow \mathcal{P}(\{0, 1\}^*)$.

- Extension to $f : \mathbb{N}^n \rightarrow \mathcal{P}((\{0, 1\}^n)^*)$ so that for all $i \in [1, n]$, $x \in \mathbb{N}^n$ and $y \in f(x)$, the projection of $y$ on the $i$th row belongs to $f(x(i))$.

- $(\begin{array}{c} 5 \\ 8 \end{array})$ represented by $(\begin{array}{c} 1 \\ 0 \end{array}) (\begin{array}{c} 0 \\ 0 \end{array}) (\begin{array}{c} 1 \\ 0 \end{array}) (\begin{array}{c} 0 \\ 1 \end{array}) (\begin{array}{c} 0 \\ 0 \end{array})$.

- $f(0) \overset{\text{def}}{=} 0^*$.

- $f(k) \overset{\text{def}}{=} u_k \cdot 0^*$ where $u_k$ is the shortest binary representation of $k$ (least significant bit first).
Presburger sets are regular

- We aim at $L(A) = f([\varphi])$.

- $\varphi \equiv A \overset{\text{def}}{\iff} L(A) = f([\varphi])$.

- Given $\varphi$, we can build a FSA $A_\varphi$ such that $\varphi \equiv A_\varphi$.

[Boudet & Comon, CAAP’96]

- $A_\varphi$ is built recursively on the structure of $\varphi$.
  (non-elementary upper bound)
Recursive construction of FSAs

Conjunction: If \( \varphi \approx A \) and \( \psi \approx B \), then \( \varphi \land \psi \approx A \cap B \) where \( \cap \) is the product construction computing intersection.

Negation: If \( \varphi \approx A \), then \( \neg \varphi \approx \overline{A} \) where \( \overline{\cdot} \) performs complementation, which may cause an exponential blow-up.

Quantification: If \( \varphi \approx A \), then \( \exists x_n \varphi \approx A' \) where \( A' \) is built over the alphabet \( \{0, 1\}^{n-1} \) by forgetting the \( n \)th component.

\( q \xrightarrow{b} q' \) in \( A' \) whenever there is a transition \( q \xrightarrow{b'} q' \) in \( A \) such that \( b \) and \( b' \) agree on the \( n - 1 \) first bit values.
What about the atomic formulae?

- Atomic formulae of the form $t_1 = t_2 + t_3$ where each $t_i$ is either a variable or a constant.

- $3x \leq 2y$ is equivalent to

$$\exists z_{2x}, z_{2y}, z_{3x} \ (z_{2x} = x + x \land z_{2y} = y + y) \land z_{3x} = z_{2x} + x \land \exists z \ (z_{2y} = z_{3x} + z)$$

(renaming technique)

- $x_1 = x_2 + x_3$:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$
Encoding $x_1 = x_2 + x_2$

By projection, encoding for $\exists x_2 \ (x_1 = x_2 + x_2)$
Final remarks

- When $\varphi \approx A$, $\psi \approx B$, and the two formulae have distinct free variables, we add dummy bits in the automata before performing the operations on automata.

- The automata-based approach can be extended to $\langle \mathbb{R}, \mathbb{N}, + \rangle \leq$ (with Büchi automata).

  [Boigelot & Wolper, ICLP’02]

- The above construction also verifies:

  $$[\varphi] \subseteq [\psi] \iff L(A_\varphi) \subseteq L(A_\psi)$$
Content of the next lecture on October 16th

- Presburger sets are the semilinear sets.
- Parikh images about regular languages.
- Introduction to reversal-bounded counter machines.
- Reachability relations are Presburger sets.
Exercise

\[ \varphi ::= \top \mid \bot \mid x \equiv_k y \mid x \equiv_k c \mid x \leq c \mid x = y \mid \neg \varphi \mid \varphi \land \varphi \mid \exists x \, \varphi \]

1. Show that every formula is equivalent to a Boolean combination of atomic formulae of one of the forms below:
   - \( x \equiv_k c \)
   - \( x \leq c \)
   - \( x = y \)

2. Show that the satisfiability problem is PSPACE-hard.

3. What about PSPACE-easiness?
Exercise about $\text{FO}(\mathbb{Z})$ (1/2)

- Show in $\text{FO}(\mathbb{Z})$ that every formulae $t \leq t'$ has an equivalent formula that uses only atomic formulae of the form either (1) $x \geq 0$ or (2) $t = t'$.

- Let $g$ be the map restricted to atomic formulae of the form (1) or (2) that is homomorphic for Boolean connectives and quantifiers such that $x \geq 0$ is translated into $x \equiv_2 0$. An atomic formula of the form

$$\sum_{j \in [1,n]} a_j x_j = b$$

with $a_j \in \mathbb{Z}$ and $b \in \mathbb{Z}$ is encoded by

$$\bigvee_{p \in \{0,1\}^n} \exists y_1, \ldots, y_n (\bigwedge_i \psi(i, p(i))) \land \sum_{j \in [1,n]} \varepsilon(p(j), a_j)y_j = b$$

where

- $\varepsilon(1, a)$ is equal to $a$ and $\varepsilon(0, a)$ is equal to $-a$.
- $\psi(j, 0) = 'x_j = 2y_j + 1'$ and $\psi(j, 1) = 'x_j = 2y_j'$. 

Evaluate the size of $g(\varphi)$ with respect to the size of $\varphi$. 

Exercise about FO(\mathbb{Z}) (2/2)

Given a formula \( \varphi(x_1, \ldots, x_n) \) and its translation \( \psi(x_1, \ldots, x_n) \), show that

\[
[\varphi(x_1, \ldots, x_n)] = \{ f(x) \in \mathbb{Z}^n : x \in [\psi(x_1, \ldots, x_n)] \}
\]

where \( f(x)(i) = \frac{x(i)}{2} \) if \( x(i) \) is even, otherwise \( f(x)(i) = -\frac{x(i)-1}{2} \).

Conclude that the satisfiability problem for FO(\mathbb{Z}) is decidable.
Exercise about quantifier elimination

Following the procedure to eliminate quantifiers, compute a quantifier-free formula equivalent to the formula below:

$$\exists z_1, z_2, z_3 \ (x_1 = 3 + z_1 - z_2) \land (x_2 = 3 + z_2 + z_3) \land (2 + z_1 - z_2 \geq 0).$$