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

https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:c-2-9-1

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:

$$\mathrm{x}{+}{+} \;\approx\; \mathrm{x}' = \mathrm{x} + 1$$

$$\mathrm{x}_1 + \mathrm{x}_2 = \mathrm{x}_B \;\wedge\; \mathrm{x}_1 < 36$$

- Nondeterministic update in a lossy counter machine:

$$\mathrm{x}' \leq \mathrm{x} + 1$$

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

$$\mathsf{x} \leq \mathsf{y} \text{ can be interpreted as } \{\langle n, m \rangle \in \mathbb{N}^2 \;\mid\; n \leq m\}$$

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 $\varphi_1(\mathrm{x}, \mathrm{y})$ interpreted as

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

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

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

- 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.
  - $X_1 \subseteq X_2$.
  - $\varphi_1(\mathrm{x}, \mathrm{y}) \Rightarrow \varphi_2(\mathrm{x}, \mathrm{y})$ 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 2EXPSPACE).
- 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 $\langle \mathbb{N}, +, \leq \rangle$:

$$\forall\, \mathsf{x}\ (\exists\, \mathsf{y}\ ((2\mathsf{x} + 8) \leq \mathsf{y})$$

- Atomic formula $((2\mathsf{x} + 8) \leq \mathsf{y})$.
- Term $(2\mathsf{x} + 8)$.
- Variables x and y.
- Given $\mathrm{VAR} = \{\mathsf{x}, \mathsf{y}, \mathsf{z}, \ldots\}$, the terms are of the form

$$a_1 \mathsf{x}_1 + \cdots + a_n \mathsf{x}_n + k$$

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

Valuations

- Valuation $\mathfrak{v}$: $\mathrm{VAR} \to \mathbb{N}$.
- Extending $\mathfrak{v}$ to all terms:
  - $\mathfrak{v}(k) = k$.
  - $\mathfrak{v}(a\mathrm{x}) = a \times \mathfrak{v}(\mathrm{x})$.
  - $\mathfrak{v}(t + t') = \mathfrak{v}(t) + \mathfrak{v}(t')$.
- Satisfaction relation $\models$
  - $\mathfrak{v} \models (2\mathrm{x} + 8) \leq \mathrm{y}$ with $\mathfrak{v}(\mathrm{x}) = 3$ and $\mathfrak{v}(\mathrm{y}) = 27$.
  - $\mathfrak{v} \not\models (2\mathrm{x} + 8) \leq \mathrm{y}$ with $\mathfrak{v}(\mathrm{x}) = 3$ and $\mathfrak{v}(\mathrm{y}) = 13$.

Formulae (1/2)

- Atomic formula $t \ \leq \ t'$.
- $\mathfrak{v} \models \ t \ \leq \ t' \ \stackrel{\text{def}}{\Leftrightarrow} \ \mathfrak{v}(t) \leq \mathfrak{v}(t')$.
- Formulae are built from Boolean connectives and quantifiers.
- Abbreviations:

$$\begin{array}{lcl} t = t' & \stackrel{\text{def}}{=} & (t \leq t') \wedge (t' \leq t) \\ t < t' & \stackrel{\text{def}}{=} & t + 1 \leq t' \\ t \geq t' & \stackrel{\text{def}}{=} & t' \leq t \\ t > t' & \stackrel{\text{def}}{=} & t' + 1 \leq t \end{array}$$

Formulae (2/2)

$$\varphi ::= \top \mid \bot \mid t \leq t' \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists \mathrm{x}\, \varphi \mid \forall \mathrm{x}\, \varphi$$

where t and t' are terms and $\mathrm{x} \in \mathrm{VAR}$.

- Infinite number of multiple of 3:

$$\forall \mathrm{x}\ (\exists \mathrm{y}\ (\mathrm{y} > \mathrm{x}) \wedge (\exists \mathrm{z}\ (\mathrm{y} = 3\mathrm{z}))).$$

- Oddness: $\exists \mathrm{y}\ \mathrm{x} = 2\mathrm{y} + 1$.

Semantics

- $\mathfrak{v} \models \top \overset{\text{def}}{\Leftrightarrow}$ true; $\mathfrak{v} \models \perp \overset{\text{def}}{\Leftrightarrow}$ false,
- $\mathfrak{v} \models t \leq t' \overset{\text{def}}{\Leftrightarrow} \mathfrak{v}(t) \leq \mathfrak{v}(t')$,
- $\mathfrak{v} \models \neg\varphi \overset{\text{def}}{\Leftrightarrow}$ not $\mathfrak{v} \models \varphi$,
- $\mathfrak{v} \models \varphi \wedge \varphi' \overset{\text{def}}{\Leftrightarrow} \mathfrak{v} \models \varphi$ and $\mathfrak{v} \models \varphi'$,
- $\mathfrak{v} \models \varphi \vee \varphi' \overset{\text{def}}{\Leftrightarrow} \mathfrak{v} \models \varphi$ or $\mathfrak{v} \models \varphi'$,
- $\mathfrak{v} \models \exists\, \mathrm{x}\ \varphi \overset{\text{def}}{\Leftrightarrow}$ there is $n \in \mathbb{N}$ such that $\mathfrak{v}[\mathrm{x} \mapsto n] \models \varphi$ where $\mathfrak{v}[\mathrm{x} \mapsto n]$ is equal to $\mathfrak{v}$ except that x is mapped to n,
- $\mathfrak{v} \models \forall\, \mathrm{x}\ \varphi \overset{\text{def}}{\Leftrightarrow}$ for every $n \in \mathbb{N}$, we have $\mathfrak{v}[\mathrm{x} \mapsto n] \models \varphi$.

Standard first-order semantics

- $\mathfrak{v} \models t = t'$ (where '$t = t'$' is an abbreviation) iff $\mathfrak{v}(t) = \mathfrak{v}(t')$.
- φ and ψ are equivalent in $\mathrm{FO}(\mathbb{N}) \overset{\text{def}}{\Leftrightarrow}$ for every valuation $\mathfrak{v}$, we have $\mathfrak{v} \models \varphi$ iff $\mathfrak{v} \models \psi$.
- $\varphi_1 \wedge \varphi_2$ and $\neg(\neg\varphi_1 \vee \neg\varphi_2)$ are equivalent formulae.
- $\exists$ x φ 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

- φ_{tot}: $\langle \mathbb{N}, < \rangle$ is a linearly ordered set:

$$\varphi_{\text{tot}} \stackrel{\text{def}}{=} \forall\, \mathsf{x}\, \forall\, \mathsf{y}\, ((\mathsf{x} = \mathsf{y}) \vee (\mathsf{x} < \mathsf{y}) \vee (\mathsf{x} > \mathsf{y})).$$

- Key argument: for all valuations $\mathfrak{v}$,

$$\mathfrak{v} \models (\mathsf{x} = \mathsf{y}) \vee (\mathsf{x} < \mathsf{y}) \vee (\mathsf{x} > \mathsf{y})$$

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

$$\exists\, x\ (t = kx + t') \vee (t' = kx + t)$$

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

$$\forall\, x, y\ (-2x + 9 \equiv_4 y + 1) \Leftrightarrow (-y \equiv_4 2x - 8)$$

Satisfiability problem

- Satisfiability problem

  Input: a formula φ

  Question: is there a valuation $\mathfrak{v}$ such that $\mathfrak{v} \models \varphi$?

- Satisfiable formula:

$$(\mathsf{x}_1 \geq 2) \wedge (\mathsf{x}_2 \geq 2\mathsf{x}_1) \wedge \cdots \wedge (\mathsf{x}_n \geq 2\mathsf{x}_{n-1})$$

  (take $\mathfrak{v}(\mathsf{x}_i) = 2^i$)

- Validity problem

  Input: a formula φ

  Question: is the case that for every valuation $\mathfrak{v}$, we have $\mathfrak{v} \models \varphi$?

- Valid formula:

$$(\mathsf{x}_1 \geq 2 \wedge \mathsf{x}_2 \geq 2\mathsf{x}_1 \wedge \cdots \wedge \mathsf{x}_n \geq 2\mathsf{x}_{n-1}) \Rightarrow \mathsf{x}_n \geq 2^n$$

Equivalences (1/2)

- φ: formula whose free variables are among $x_1, \ldots, x_n$.
- The propositions below are equivalent:

(I) φ 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)

- φ: formula whose free variables are among $x_1, \ldots, x_n$.
- The propositions below are equivalent:

  (I) φ 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

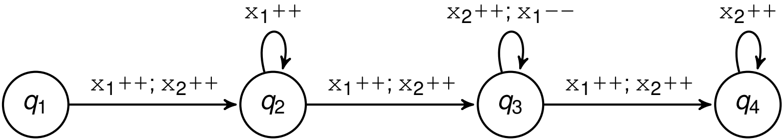
- Formula $\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)$ with n free variables:

$$[\![\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)]\!] \stackrel{\text{def}}{=} \{\langle \mathfrak{v}(\mathsf{x}_1), \ldots, \mathfrak{v}(\mathsf{x}_n)\rangle \in \mathbb{N}^n : \mathfrak{v} \models \varphi\}$$

- $[\![\mathsf{x}_1 < \mathsf{x}_2]\!] = \{\langle n, n'\rangle \in \mathbb{N}^2 : n < n'\}$.
- $[\![\mathsf{x} = \mathsf{x} + \mathsf{x}]\!] = \{0\}$.
- φ is satisfiable iff $[\![\varphi]\!]$ is non-empty.
- φ is valid (with free variables $\mathsf{x}_1, \ldots, \mathsf{x}_n$) iff $[\![\varphi]\!] = \mathbb{N}^n$.

Presburger sets

- $X \subseteq \mathbb{N}^d$ is a Presburger set $\overset{\text{def}}{\Leftrightarrow}$ there is φ with free variables $x_1, \ldots, x_d$ such that $[\![\varphi]\!] = X$.

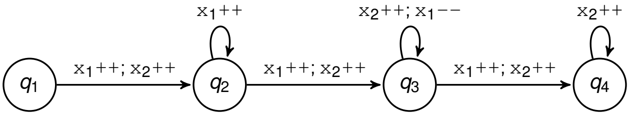


$$[\![x_1 \geq 1 \wedge x_2 \geq 3 \wedge x_1 + x_2 \geq 6]\!]$$

$$=$$

$$\{\langle n, m\rangle \mid \langle q_1, 0, 0\rangle \xrightarrow{*} \langle q_4, n, m\rangle\}$$

A rough analysis



$$[\![x_1 = x_2 = 0]\!] = \{\langle n, m\rangle \mid \langle q_1, 0, 0\rangle \xrightarrow{*} \langle q_1, n, m\rangle\}$$

$$[\![x_2 = 1 \wedge x_1 \geq 1]\!] = \{\langle n, m\rangle \mid \langle q_1, 0, 0\rangle \xrightarrow{*} \langle q_2, n, m\rangle\}$$

$$[\![x_2 \geq 2 \wedge x_1 + x_2 \geq 4]\!] = \{\langle n, m\rangle \mid \langle q_1, 0, 0\rangle \xrightarrow{*} \langle q_3, n, m\rangle\}$$

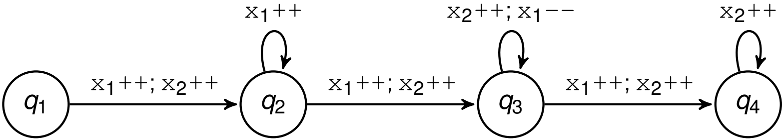
$$[\![x_1 \geq 1 \wedge x_2 \geq 3 \wedge x_1 + x_2 \geq 6]\!] = \{\langle n, m\rangle \mid \langle q_1, 0, 0\rangle \xrightarrow{*} \langle q_4, n, m\rangle\}$$

With quantifiers

$$\exists\, z_1, z_2, z_3\ (x_1 = 3 + z_1 - z_2) \wedge (x_2 = 3 + z_2 + z_3)$$

$$\wedge\ 2 + z_1 - z_2 \geq 0$$

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



Always good to capture the reachability sets

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

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

$$\neg \exists \mathrm{y} \, \forall \mathrm{x}_1, \ldots, \mathrm{x}_n \; \varphi_q(\mathrm{x}_1, \ldots, \mathrm{x}_n) \Rightarrow (\mathrm{x}_1 \leq \mathrm{y} \wedge \cdots \wedge \mathrm{x}_n \leq \mathrm{y})$$

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

$$\varphi_q(\mathrm{x}_1, \ldots, \mathrm{x}_n) \wedge \mathrm{x}_1 = \mathbf{z}(1) \wedge \cdots \wedge \mathrm{x}_n = \mathbf{z}(n),$$

- Control state q can be reached from $\langle q_0, \mathbf{x_0} \rangle$ iff the Presburger formula $\varphi_q(\mathrm{x}_1, \ldots, \mathrm{x}_n)$ is satisfiable.

Refinement: new set of atomic formulae

$$\top \mid \bot \mid t \leq t' \mid t \equiv_k t' \mid t = t' \mid t < t' \mid t \geq t' \mid t > t' \quad \text{(PAF)}$$

- A formula φ is quantifier-free $\overset{\text{def}}{\Leftrightarrow}$ φ is a Boolean combination of atomic formulae (i.e. without quantifiers).

$$(\mathrm{x} + \mathrm{y} \equiv_5 \mathrm{z}) \vee (\mathrm{y} > 23)$$

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

$$\top \mid \bot \mid t \leq t' \mid t = t' \mid t < t' \mid t \geq t' \mid t > t' \qquad \text{(LIN)}$$

More fragments

- Difference fragment: φ is in the difference fragment $\stackrel{\text{def}}{\Leftrightarrow}$ φ belongs to the linear fragment and the terms are of the form either $\mathsf{x} + k$ or k.

$$\begin{aligned} \text{in: } & \neg(\mathsf{x} = \mathsf{y} + 8) \wedge \mathsf{y} \geq 7. \\ \text{out: } & 2\mathsf{x} = 6 \text{ and } \mathsf{x} + \mathsf{y} \geq 3. \end{aligned}$$

- Prenex normal form:

$$\mathcal{Q}_1 \, \mathsf{x}_1 \ \cdots \mathcal{Q}_n \, \mathsf{x}_n \, \psi$$

  with ψ in the linear fragment and $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_n\} \subseteq \{\exists, \forall\}$.

- $\neg(\exists \, \mathsf{x} \; \mathsf{x} \geq 3) \vee (\forall \, \mathsf{y} \; \mathsf{y} \geq 4)$ is equivalent to

$$\forall \, \mathsf{x} \, \forall \, \mathsf{y} \; (\neg(\mathsf{x} \geq 3) \vee \mathsf{y} \geq 4)$$

- Extended prenex normal form:

$$(\mathcal{Q}_1)_{\leq k_1} \, \mathsf{x}_1 \ \cdots (\mathcal{Q}_n)_{\leq k_n} \, \mathsf{x}_n \, \psi$$

  with ψ is in (LIN), $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_n\} \subseteq \{\exists, \forall\}$ 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 $(\sum_i a_i \mathrm{x}_i) + k$ where the a_i's and k belong to $\mathbb{N}$ and the natural numbers are encoded in binary.

- φ quantifier-free formula with variables $\mathrm{x}_1, \ldots, \mathrm{x}_n$ is satisfiable iff there is a valuation

$$\mathfrak{v} : \{\mathrm{x}_1, \ldots, \mathrm{x}_n\} \to [0, 2^{p(|\varphi|)}] \text{ such that } \mathfrak{v} \models \varphi$$

  $p(\cdot)$ is a polynomial independent of φ and $\mathrm{x}_1, \ldots, \mathrm{x}_n$.

- 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 φ 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):
  - φ with propositional variables $p_1, \ldots, p_n$.
  - φ' obtained from φ by replacing p_i by $\mathsf{x}_i^{\mathrm{new}} = \mathsf{y}_i^{\mathrm{new}}$.
  - φ is satisfiable iff φ' is satisfiable.

NP upper bound

- Guess
$$\langle \alpha_1, \ldots, \alpha_n \rangle \in [0, 2^{p(|\varphi|)}]^n$$
- Check that $\mathfrak{v} \models \varphi$ where $\mathfrak{v}(\mathsf{x}_i) = \alpha_i$ 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 $\mathfrak{v}(t)$ for any term t in φ can be done in polynomial time in $|\varphi|$.
  3. Determining the truth value of any atomic formula under $\mathfrak{v}$ can be done in polynomial time in $|\varphi|$.
  4. Replacing all the atomic formulae from φ by either $\top$ or $\perp$ and then simplifying leads to $\top$ or $\perp$ 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 2EXPTIME and 2EXPSPACE.
- 2EXPSPACE is included in 3EXPTIME. [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 φ: eliminate quantifiers in $\exists\, x_1, \ldots, x_d\ \varphi$ and verify it leads to $\top$.

A small model property

- $\varphi = \mathcal{Q}_1 \, \mathsf{x}_1 \, \cdots \, \mathcal{Q}_s \, \mathsf{x}_s \, \psi(\mathsf{x}_1, \ldots, \mathsf{x}_s)$
  - in prenex normal form,
  - of length n and,
  - with m quantifier alternations.

- $w = 2^{\mathrm{C} \times n^{[(s+3)^{m+2}]}}$ for some constant C.

- φ is satisfiable iff

$$(\mathcal{Q}_1)_{\leq w} \, \mathsf{x}_1 \, \cdots \, (\mathcal{Q}_s)_{\leq w} \, \mathsf{x}_s \, \psi(\mathsf{x}_1, \ldots, \mathsf{x}_s)$$

  is satisfiable.

- Decision procedure by trying all the possible values for the variables until w but care is needed because of the quantifier alternations.

$\mathrm{FO}(\mathbb{Z})$

- $\mathrm{FO}(\mathbb{Z})$: variant of $\mathrm{FO}(\mathbb{N})$ in which variables are interpreted in $\mathbb{Z}$.
- $\mathrm{FO}(\mathbb{Z})$ and $\mathrm{FO}(\mathbb{N})$ have the same of formulae.
- The formula $\forall$ x $\exists$ y y $<$ x
  - is valid in $\mathrm{FO}(\mathbb{Z})$
  - but not in $\mathrm{FO}(\mathbb{N})$.
- The satisfiability problem for $\mathrm{FO}(\mathbb{Z})$ 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 $\mathrm{FO}(\mathbb{N})$?
- For instance, disjunction operator $\vee$ can be eliminated in propositional calculus with $\neg$ and $\wedge$ only.
- But NP-completeness of the quantifier-free fragment whereas 2EXPTIME-hardness of the full logic.
- Analogy: linear-time temporal logic LTL and first-order logic on ω-words have the same expressiveness but not the same conciseness and computational complexity.

Simple quantifier eliminations

$\exists\, x\, (x \geq 3)$	is equivalent to	$\top$
$\exists\, z\, (x < z \wedge z < y)$	is equivalent to	$x + 2 \leq y$
$\exists\, z\, (x < z \vee z < y)$	is equivalent to	$\top$
$\forall\, z\, (x \leq z \Rightarrow y \leq z)$	is equivalent to	$y \leq x$
$\exists\, z\, x = 2z$	is equivalent to	$x \equiv_2 0$

What about

$$\exists\, z\, (\neg(x \leq 2z - 1)) \wedge (\exists\, z'\, (z = z') \wedge (0 \leq 2z' - x)) \quad ?$$

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?
- $\mathrm{AT}(\mathsf{x})$: set of atomic formulae of the form
$$a\mathsf{x} + b \leq a'\mathsf{x} + b'$$
where $a, a', b, b' \in \mathbb{N}$.
- Every $a\mathsf{x} + b \leq a'\mathsf{x} + b'$ is equivalent to a formula having one of the forms below:
$$\top \quad \perp \quad \mathsf{x} \leq k \quad \mathsf{x} \geq k$$
where $k \in \mathbb{N}$.
- $3\mathsf{x} + 5 \leq \mathsf{x} + 8$ is logically equivalent to $\mathsf{x} \leq 1$.

Intervals

- Formula ψ = Boolean combination of formulae among $\top$, $\perp$ or $x \leq k$.
- $[\![\psi]\!]$ is a finite union of intervals $\bigcup_i I_i$ such that each I_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 $\bigcup_i I_i$.
- $\exists\ z\ x = 2z$ is not equivalent to a formula in the linear fragment.

Main theorem (QE)

For every formula φ, there exists a quantifier-free formula φ' such that

1. $\mathit{free}(\varphi') \subseteq \mathit{free}(\varphi)$.
2. φ' is logically equivalent to φ.
3. φ' can be effectively built from φ.

- Property (QE*): restriction of (QE) with $\varphi = \exists \mathrm{x}\ \psi$ and ψ 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 (QE*) to eliminate quantifiers

$$\varphi = \exists\, x\ (\psi_0(x) \wedge (\exists\, y\ (\psi_1(x, y) \wedge \exists\, z\ \psi_2(x, y, z, z'))))$$

(the ψ_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 φ is equivalent to

$$\exists\, x\ (\psi_0(x) \wedge (\exists\, y\ (\psi_1(x, y) \wedge \psi_2'(x, y, z'))))$$

- If $\exists\, y\ (\psi_1(x, y) \wedge \psi_2'(x, y, z')$ is equivalent to the QF formula $\psi_1'(x, z')$, then φ is equivalent to

$$\exists\, x\ (\psi_0(x) \wedge \psi_1'(x, z'))$$

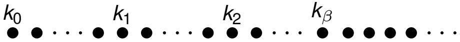
- If $\exists\, x\ (\psi_0(x) \wedge \psi_1'(x, z'))$ is equivalent to the QF formula $\psi_0'(z')$, then φ is equivalent to $\psi_0'(z')$.

Quantifier elimination for φ

1. Replace every $\forall$ x ψ by $\neg \exists$ x $\neg\psi$, leading to φ'.
2. If φ' is quantifier-free, we are done. Otherwise go to 3.
3. Pick an innermost subformula $\exists$ x χ with QF χ and substitute it by an equivalent QF formula thanks to (QE*).
4. Update φ' to be this new formula.
5. The number of quantifiers in φ' has decreased by one.
6. If φ' is quantifier-free, we are done. Otherwise, go to 3.

A simple principle

- $\exists$ x φ with φ 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



- $n \sim n' \overset{\text{def}}{\Leftrightarrow}$ for all $i \in [0, \beta]$, we have $k_i \leq n$ iff $k_i \leq n'$.
- Equivalence classes with its canonical elements:

- $\exists$ x φ is equivalent to $\bigvee_i \varphi(\text{x} \leftarrow k_i)$,

Quantifier elimination with the fragment (†)

- Extended term $(\sum_i a_i \mathsf{x}_i) + k$ with a_i's and k belong to $\mathbb{Z}$.
- $\varphi = \exists\, \mathsf{x}\ \chi$ with χ a QF formula respecting

$$\chi ::= \top \mid \bot \mid t \leq \mathsf{x} \mid t \leq t' \mid \neg\chi \mid \chi \wedge \chi \qquad (\dagger)$$

  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 $t \geq \mathsf{x}$ since that is equivalent to $\neg(t + 1 \leq \mathsf{x})$.
- For instance $\mathsf{y} \leq 2\mathsf{x}$ or $\mathsf{x} \equiv_2 0$ do not belong to (†).

About valuations

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

$$\mathfrak{v}((\sum_i a_i \mathsf{x}_i) + k) \stackrel{\text{def}}{=} (\sum_i a_i \ \mathfrak{v}(\mathsf{x}_i)) + k$$

- Extended terms are interpreted in $\mathbb{Z}$.
- T: set of terms t occurring in some atomic formula $t \leq \mathsf{x}$, and (possibly) augmented with 0.
- So T is non-empty and contains at most $|\chi|$ elements.
- Given $\mathfrak{v} : \mathrm{VAR} \to \mathbb{N}$, there is a term $t_{\mathrm{left}} \in T$ such that
  1. $\mathfrak{v}(t_{\mathrm{left}}) \leq \mathfrak{v}(\mathsf{x})$ and,
  2. there is no $t \in T$ such that $\mathfrak{v}(t_{\mathrm{left}}) < \mathfrak{v}(t) \leq \mathfrak{v}(\mathsf{x})$.
- t_{left} the closest left term (depending on $\mathfrak{v}$).

A key observation

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

Quantifier elimination

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

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

- The disjunction can be computed in polynomial time in $|\varphi|$.
- Existential quantification is replaced by a generalized disjunction, which is conceptually sound.

$$\begin{aligned}
\mathfrak{v} \models \bigvee_{t \in T} \chi(\mathsf{x} \leftarrow t) \quad & \rightarrow \quad \mathfrak{v} \models \chi(\mathsf{x} \leftarrow t) \text{ for some } t \in T \\
& \rightarrow \quad \mathfrak{v}[\mathsf{x} \mapsto \mathfrak{v}(t)] \models \chi(\mathsf{x}) \\
& \rightarrow \quad \mathfrak{v} \models \exists\, \mathsf{x}\ \chi(\mathsf{x})
\end{aligned}$$

The other direction

$$
\begin{aligned}
\mathfrak{v} \models \exists\, \mathsf{x}\ \chi \quad & \to \quad \text{there is } n \in \mathbb{N} \text{ such that } \mathfrak{v}[\mathsf{x} \mapsto n] \models \chi \\
& \to \quad \mathfrak{v}[\mathsf{x} \mapsto \mathfrak{v}(t_{\text{left}})] \models \chi \\
& \to \quad \mathfrak{v} \models \chi(\mathsf{x} \leftarrow t_{\text{left}}) \\
& \to \quad \mathfrak{v} \models \textstyle\bigvee_{t \in T} \chi(\mathsf{x} \leftarrow t)
\end{aligned}
$$

QE for $\exists z\, (x < z \wedge z < y)$

- $\exists z\, (x + 1 \leq z \wedge \neg(y \leq z))$.
- $T = \{x + 1, y, 0\}$.

$$
\begin{gathered}
(\overbrace{x + 1 \leq x + 1}^{\top} \wedge \neg(y \leq x + 1)) \vee \\
(x + 1 \leq y \wedge \underbrace{\neg(y \leq y)}_{\perp}) \vee \\
(\underbrace{x + 1 \leq 0}_{\perp} \wedge \neg(y \leq 0))
\end{gathered}
$$

- Equivalent to $\neg(y \leq x + 1)$ or $x + 2 \leq y$.

Quantifier elimination with the fragment (††)

- $\varphi = \exists\, \mathrm{x}\, \chi$ with χ a QF formula respecting

$$\chi ::= \top \mid \bot \mid t \le a\mathrm{x} \mid t \le t' \mid \neg\chi \mid \chi \wedge \chi \qquad (\dagger\dagger)$$

  where t, t' are extended terms without x and $a \ge 1$.

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

- χ': replace in χ every $t \le a\mathrm{x}$ by $t \times \frac{\ell}{a} \le \ell\mathrm{x}$.

- χ'': replace in χ' every $\ell\mathrm{x}$ by x.

- φ and $\exists\, \mathrm{x}\, (\mathrm{x} \equiv_\ell 0) \wedge \chi''$ are equivalent.

Quantifier elimination with the fragment (†††)

- $\varphi = \exists\, \mathsf{x}\, \chi$ with χ a QF formula respecting

$$\chi ::= \top \mid \bot \mid t \equiv_k t' \mid \mathsf{x} \equiv_k t \mid t \leq \mathsf{x} \mid t \leq t' \mid \neg\chi \mid \chi \wedge \chi \quad (\dagger\dagger\dagger)$$

  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 $a\mathsf{x}$ with $a > 1$.

Preliminary simplifications (again)

- ℓ: lcm of all the coefficients occurring in front of x.
- $a\mathrm{x} \equiv_k t$ is replaced by $\ell\mathrm{x} \equiv_{(k \times \frac{\ell}{a})} \frac{\ell}{a} t$.
- $t \leq \mathrm{x}$ is replaced by $t \times \frac{\ell}{a} \leq \ell\mathrm{x}$.
- Then we proceed as for (††) by introducing the conjunct $\mathrm{x} \equiv_\ell 0$.
- Value ℓ': lcm of all $k_1, \ldots, k_\beta$ such that $\mathrm{x} \equiv_{k_i} t$ occurs in χ.

A key observation (bis)

- For any $n \in \{m \in [\mathfrak{v}(t_{\mathrm{left}}), \mathfrak{v}(\mathsf{x})] : m \equiv_{\ell'} \mathfrak{v}(\mathsf{x})\}$, $\mathfrak{v}$ and $\mathfrak{v}[\mathsf{x} \mapsto n]$ verify exactly the same atomic formulae from χ.
  - Interpretation of the terms t remains unchanged. (so truth of $t \leq t'$ or $t \equiv_k t'$ is unchanged).
  - Truth of $t \leq \mathsf{x}$ is unchanged too (as for ($\dagger$)).
  - Truth of $\mathsf{x} \equiv_{k_i} t$ 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, $\mathfrak{v} \models \chi$ iff $\mathfrak{v}[\mathsf{x} \mapsto n] \models \chi$.

- For the satisfaction of φ, we can assume that x is equal to some term t with $t + j$ such that $t \in T$ and $j \in [0, \ell' - 1]$.

- φ is equivalent to

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

Example

- $\exists\, \mathsf{z}\ \mathsf{x} = 2\mathsf{z}$.
- $\exists\, \mathsf{z}\ (\mathsf{x} \leq 2\mathsf{z}) \wedge (\neg(\mathsf{x} + 1 \leq 2\mathsf{z}))$.
- $\exists\, \mathsf{z}\ (\mathsf{z} \equiv_2 0) \wedge (\mathsf{x} \leq \mathsf{z}) \wedge (\neg(\mathsf{x} + 1 \leq \mathsf{z}))$.
- $T = \{0, \mathsf{x}, \mathsf{x} + 1\}$.
- $\ell' = 2$.

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

$$[(\overbrace{0 \equiv_2 0}^{\top}) \wedge (x \leq 0) \wedge (\overbrace{\neg(x + 1 \leq 0)}^{\top})] \vee$$

$$[(\underbrace{1 \equiv_2 0}_{\perp}) \wedge (x \leq 1) \wedge (\neg x + 1 \leq 1)] \vee$$

$$[(x \equiv_2 0) \wedge (\overbrace{x \leq x}^{\top}) \wedge (\overbrace{\neg(x + 1 \leq x)}^{\top})] \vee$$

$$[(x + 1 \equiv_2 0) \wedge (x \leq x + 1) \wedge (\underbrace{\neg x + 1 \leq x + 1}_{\perp})] \vee$$

$$[(x + 1 \equiv_2 0) \wedge (x \leq x + 1) \wedge (\underbrace{\neg(x + 1 \leq x + 1)}_{\perp})] \vee$$

$$[(x + 2 \equiv_2 0) \wedge (x \leq x + 2) \wedge (\underbrace{\neg(x + 1 \leq x + 2)}_{\perp})]$$

Equivalent to $(x \leq 0) \vee (x \equiv_2 0)$ and therefore to $x \equiv_2 0$.

Corollaries

- $\exists\, \bar{x}\ \varphi(\bar{x})$ 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

From logic to automata

- Automata-based approach consists in reducing logical problems into automata-based decision problems.

- Examples of target problems:
  - $\mathrm{L}(\mathcal{A}) = \emptyset$?
  - $\mathrm{L}(\mathcal{A}) \subseteq \mathrm{L}(\mathcal{B})$?
  - Is $\mathrm{L}(\mathcal{A})$ 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 ω-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 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 $\mathfrak{f} : \mathbb{N} \to \mathcal{P}(\{0,1\}^*)$.
- Extension to $\mathfrak{f} : \mathbb{N}^n \to \mathcal{P}((\{0,1\}^n)^*)$ so that for all $i \in [1,n]$, $\mathbf{x} \in \mathbb{N}^n$ and $\mathbf{y} \in \mathfrak{f}(\mathbf{x})$, the projection of $\mathbf{y}$ on the ith row belongs to $\mathfrak{f}(\mathbf{x}(i))$.
- $\begin{pmatrix} 5 \\ 8 \end{pmatrix}$ represented by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.
- $\mathfrak{f}(0) \stackrel{\text{def}}{=} 0^*$.
- $\mathfrak{f}(k) \stackrel{\text{def}}{=} u_k \cdot 0^*$ where u_k is the shortest binary representation of k (least significant bit first).

Presburger sets are regular

- We aim at $\mathrm{L}(\mathcal{A}) = \mathfrak{f}(\llbracket \varphi \rrbracket)$.
- $\varphi \approx \mathcal{A} \overset{\text{def}}{\Leftrightarrow} \mathrm{L}(\mathcal{A}) = \mathfrak{f}(\llbracket \varphi \rrbracket)$.
- Given φ, we can build a FSA $\mathcal{A}_\varphi$ such that $\varphi \approx \mathcal{A}_\varphi$.
  [Boudet & Comon, CAAP'96]
- $\mathcal{A}_\varphi$ is built recursively on the structure of φ.
  (non-elementary upper bound)

Recursive construction of FSAs

Conjunction If $\varphi \approx \mathcal{A}$ and $\psi \approx \mathcal{B}$, then $\varphi \wedge \psi \approx \mathcal{A} \cap \mathcal{B}$ where $\cap$ is the product construction computing intersection.

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

Quantification If $\varphi \approx \mathcal{A}$, then $\exists\, \mathsf{x}_n\, \varphi \approx \mathcal{A}'$ where $\mathcal{A}'$ is built over the alphabet $\{0, 1\}^{n-1}$ by forgetting the nth component.
$q \xrightarrow{\mathbf{b}} q'$ in $\mathcal{A}'$ whenever there is a transition $q \xrightarrow{\mathbf{b}'} q'$ in $\mathcal{A}$ such that $\mathbf{b}$ and $\mathbf{b}'$ agree on the $n-1$ first bit values.

What about the atomic formulae?

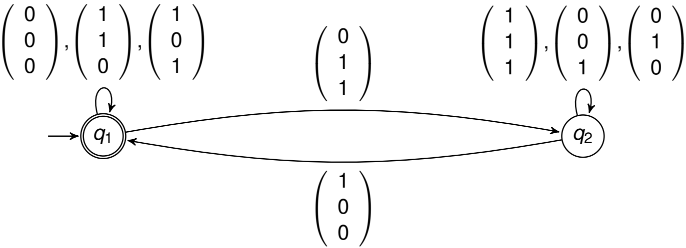
- Atomic formulae of the form $t_1 = t_2 + t_3$ where each t_i is either a variable or a constant.

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

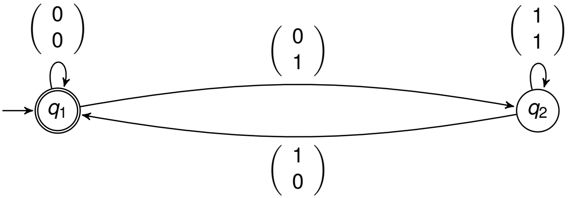
  $$\exists\, z_{2x}, z_{2y}, z_{3x}\ (z_{2x} = x + x \wedge z_{2y} = y + y) \wedge z_{3x} = z_{2x} + x \wedge$$
  $$\exists\, z\ (z_{2y} = z_{3x} + z)$$

  (renaming technique)

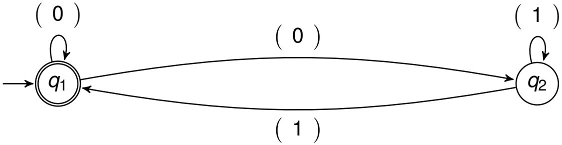
- $x_1 = x_2 + x_3$:



Encoding $x_1 = x_2 + x_2$



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



Final remarks

- When $\varphi \approx \mathcal{A}$, $\psi \approx \mathcal{B}$, 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:

$$[\![\varphi]\!] \subseteq [\![\psi]\!] \quad \text{iff} \quad \mathrm{L}(\mathcal{A}_\varphi) \subseteq \mathrm{L}(\mathcal{A}_\psi)$$

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

$$\varphi ::= \top \mid \bot \mid \mathsf{x} \equiv_k \mathsf{y} \mid \mathsf{x} \equiv_k c \mid \mathsf{x} \leq c \mid \mathsf{x} = \mathsf{y} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists \mathsf{x}\, \varphi$$

x, y are variables, $k \geq 2$ and $c \geq 0$.

1. Show that every formula is equivalent to a Boolean combination of atomic formulae of one of the forms below:
   - $\mathsf{x} \equiv_k c$,
   - $\mathsf{x} \leq c$,
   - $\mathsf{x} = \mathsf{y}$.
2. Show that the satisfiability problem is PSPACE-hard.
3. What about PSPACE-easiness?

Exercise about $\mathrm{FO}(\mathbb{Z})$ (1/2)

- Show in $\mathrm{FO}(\mathbb{Z})$ that every formulae $t \leq t'$ has an equivalent formula that uses only atomic formulae of the form either (1) $\mathsf{x} \geq 0$ or (2) $t = t'$.
- Let $\mathfrak{g}$ be the map restricted to atomic formulae of the form (1) or (2) that is homomorphic for Boolean connectives and quantifiers such that $\mathsf{x} \geq 0$ is translated into $\mathsf{x} \equiv_2 0$.
  An atomic formula of the form

$$\sum_{j \in [1,n]} a_j \mathsf{x}_j = b$$

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

$$\bigvee_{\mathbf{p} \in \{0,1\}^n} \exists\ \mathsf{y}_1, \ldots, \mathsf{y}_n\ (\bigwedge_i \psi(i, \mathbf{p}(i))) \wedge \sum_{j \in [1,n]} \varepsilon(\mathbf{p}(j), a_j) \mathsf{y}_j = b$$

  where
  - $\varepsilon(1, a)$ is equal to a and $\varepsilon(0, a)$ is equal to $-a$.
  - $\psi(j, 0) =$ '$\mathsf{x}_j = 2\mathsf{y}_j + 1$' and $\psi(j, 1) =$ '$\mathsf{x}_j = 2\mathsf{y}_j$'.

  Evaluate the size of $\mathfrak{g}(\varphi)$ with respect to the size of φ.

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

- Given a formula $\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)$ and its translation $\psi(\mathsf{x}_1, \ldots, \mathsf{x}_n)$, show that

$$[\![\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)]\!] = \{\mathfrak{f}(\mathbf{x}) \in \mathbb{Z}^n : \mathbf{x} \in [\![\psi(\mathsf{x}_1, \ldots, \mathsf{x}_n)]\!]\}$$

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

- Conclude that the satisfiability problem for $\mathrm{FO}(\mathbb{Z})$ is decidable.

Exercise about quantifier elimination

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

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