

## LOGICS

### TD 4 : Presburger Arithmetics

#### Exercice 4.1 Automata construction

1- Construct finite automata for the following languages :

$$\nu^{-1}(\{(x, y) \in \mathbb{N}^2 \mid 2x = y\}); \quad \nu^{-1}(\{(x, y) \in \mathbb{N}^2 \mid x \leq y\})$$

2- Let  $\alpha \in \mathbb{N}$  be some fixed integer. Describe some finite automaton recognizing

$$\nu^{-1}(\{(x, y) \in \mathbb{N}^2 \mid \alpha x = y\})$$

#### Exercice 4.2 Linear equations

We consider the following system of equations (and inequations) over natural integers :

$$2x + y = z, x \leq y$$

1- How can we describe its set of solutions by means of a finite automaton ?

2- Let us assume we aim at solving a system of equations and inequations over  $\mathbb{N}$  by means of automata theory.

2.1 How much time will it take to decide whether there exists some solution ?

2.2 Give an upper-bound on the minimal size of a solution (if some exists).

#### Exercice 4.3 Language of squares

Let us consider the predicate defined by :

$$C(n) \Leftrightarrow \exists y, x = y \times y$$

1- Show that the predicate  $x \times y = z$  is definable within the language  $\mathcal{L}_1(+, =, C)$ .

2- Conclude that the first-order theory of  $\langle \mathbb{N}, +, =, C \rangle$  is undecidable.

3- Show that the language

$$\{u \in \Sigma_2^* \mid \nu(u) \text{ is a square} \}$$

is not rational.

#### Exercice 4.4 Algebraic integers

Show that the first-order theory of

$$\langle \mathbb{Z}, +, 0, 1, \leq, = \rangle$$

is decidable.

#### Exercice 4.5 Skolem arithmetics

Show, by an adequate use of the closure and decidability properties of term automata, that the first-order theory of

$$\langle \mathbb{N}, \times, = \rangle$$

is decidable.

**Exercice 4.6** Logics over words

1- Show, by an adequate use of the closure and decidability properties of word automata, that the first-order theory of

$$\langle X^*, \approx, \preceq, (S_x)_{x \in X} \rangle$$

[where  $u \approx v$  means  $|u| = |v|$ ,  $\preceq$  denotes the prefix ordering and  $u = S_x(v)$  means  $u = v \cdot x$ ] is decidable.

2- Is every rational language over  $X^*$  *definable* within this logics ?

**Exercice 4.7** Logics over the free monoid

Using the undecidability of the Post Correspondence Problem, show that the first-order theory of

$$\langle \{a, b, c\}^*, a, b, c, \cdot, = \rangle$$

is undecidable.