

# Register Minimization of Cost Register Automata over a Field

Yahia Idriss Benalioua

Aix Marseille Univ, CNRS, LIS  
Marseille, France

yahia-idriss.benalioua@univ-amu.fr

Nathan Lhote

Aix Marseille Univ, CNRS, LIS  
Marseille, France

nathan.lhote@lis-lab.fr

Pierre-Alain Reynier

Aix Marseille Univ, CNRS, LIS  
Marseille, France

pierre-alain.reynier@univ-amu.fr

Weighted automata (WA) are an extension of finite automata that defines functions from words to values in a given semi-ring. An alternative model that is deterministic, called Cost Register Automata (CRA), was introduced by Alur et al. It enriches deterministic finite automata with a finite number of registers, which store values, are updated at each transition using the operations of the semi-ring, and are combined to produce the output. The expressiveness of a CRA depends on the number of its registers and the type of register updates allowed for each of its transitions. In particular, the class of functions computable by a CRA with register updates defined by linear (or affine) maps correspond exactly with rational functions (functions computable by a WA). A natural problem for CRA is the register minimization problem : given a function defined by a CRA, what is the minimal number of registers needed to realize this function?

In this paper, we solve the register minimization problem for CRA over a field with linear (or affine) register updates, using an algebraic invariant of a WA introduced recently by Bell and Smertnig, the so-called the linear hull of the automaton. This invariant being computable, we are able to explicitly compute a CRA with linear (or affine) updates, using the minimal number of registers.

Using these techniques, we are also able to solve the more general CRA minimisation problem: given a CRA and integers  $k, d$ , is there an equivalent linear (resp. affine) CRA using at most  $k$  states and  $d$  registers?

## 1 Introduction

**Weighted automata** (WA) are a quantitative extension of finite state automata and have been studied since the sixties ([14]). These automata define functions from words to a given semiring: each transition has a weight in the semiring and the weight of an execution is the product of the weights of the transitions therein; then the weights of the different executions over a word are aggregated using the sum of the semiring.

It turns out that weighted automata over a field enjoy many nice properties: the equivalence of weighted automata is decidable and they can be minimised, and both can be done efficiently (see e.g. [13]). The most studied semirings which are not fields are the tropical semirings and the semiring of languages, and in both cases equivalence is undecidable (see [7, 6]) and no minimisation algorithm is known.

**Cost register automata** (CRA) have been introduced more recently by Alur *et al.* [1]. A cost register automaton is a deterministic finite state automaton endowed with a finite number of registers storing values from the semiring. The register are initialized by some values, then each transition the values are updated using the operations and constants of the semiring. An easy observation is that WA are

exactly CRA with one state and linear updates (the new values of the registers only depend linearly on the previous ones), however adding states does not extend expressiveness.

CRA with polynomial updates have also been studied, and equivalence is decidable (over a field), however the techniques used are more sophisticated and the complexity cost is greater [5], moreover no minimisation results are known.

**The linear hull** of a WA is a notion introduced in a recent article by Bell & Smertnig [3]. This notion is inspired by the algebraic theory needed to study polynomial automata but cast into a linear setting. A linear algebraic set (aka linear Zariski closed set) is a finite union of vector subspaces; then the linear hull of a weighted automaton is the best linear algebraic invariant of the automaton: it is the intersection of all linear algebraic sets which 1) contain the initial vector and 2) are stable under the updates of the automaton. In their articles, Bell & Smertnig show that computing the linear hull of a minimal automaton is enough to decide the following properties: given a WA, is it equivalent to a deterministic (resp. unambiguous) one?

**The register minimisation problem** asks given a CRA and a number  $k$  whether there exists an equivalent CRA with at most  $k$  registers. From a practical point of view, when implementing a CRA, the control part (state of the DFA) requires a bounded amount of memory, while each register may store an unbounded element of the semiring. Hence, reducing the number of registers allows to reduce the worst-case memory usage. From a theoretical point of view, this new problem can be understood as a refinement of the classical problem of minimization of WA. Indeed, a WA can be translated into a linear CRA with a single state, and as many registers as the number of states of the WA. However, it may be possible to build an equivalent CRA with fewer registers, but more states. So there exists a kind of tradeoff between the number of states and the number of registers.

The more general CRA minimization problem asks, given a CRA and integers  $k, d$  whether an equivalent CRA with  $k$  states and  $d$  registers can be constructed. In this framework, the classical minimization of WA corresponds to minimizing the number of registers while using only one state.

**Contributions** A starting observation is that a deterministic WA is a CRA with a single register. Thus one can state the result of Bell & Smertnig as solving the 1-register minimisation problem. Our first contribution is to extend this result by examining the properties of the linear hull, in order to solve the general register minimisation problem, for linear CRA. We then generalise this result in two directions: Firstly we consider affine CRA, which are a very slight extension of CRA which allows to use affine maps in the updates of the registers. Of course affine CRA are not more expressive than linear ones, since one can transform an affine CRA in a linear one with one extra register. Introducing the natural concept of affine hull of a WA we thus show how to minimise the registers of an affine CRA. Secondly, we show how the linear (resp. affine) hull can be used to minimise simultaneously the number of states and registers of a linear (resp. affine) CRA, thus solving the CRA minimisation problem.

## 2 Preliminaries

**Basic concepts and notations** An alphabet  $\Sigma$  is a finite set of letters.  $\Sigma^*$  will denote the set of finite words over  $\Sigma$ ,  $\varepsilon$  the empty word and, for two words  $u$  and  $v$ , their concatenation will be denoted  $uv$ .

For two sets  $X$  and  $Y$ , we denote by  $X \times Y$  their cartesian product and by  $\pi_X$  and  $\pi_Y$  we denote the canonical projection on  $X$  and  $Y$  respectively.

For two integers  $i, j$ ,  $\llbracket i, j \rrbracket$  will denote the interval of integers between  $i$  and  $j$  (both included).

**Algebraic concepts** A *semigroup*  $(S, *)$  is a set  $S$  together with an associative binary operation  $*$ . If  $(S, *)$  has an identity element  $e$ ,  $(S, *, e)$  is called a *monoid* and if, moreover, every element has an inverse,  $(S, *, e)$  is called a *group*. If there is no ambiguity, we will identify algebraic structures with the set that they are defined on. A semigroup (or a monoid/group) is said to be *commutative* if its law is commutative. A sub-semigroup (or sub-monoid/subgroup) of  $S$  is a subset of  $S$  that is a semigroup (or a monoid/group). For all subsets  $E$  of  $S$ ,  $\langle E \rangle$  will denote the smallest sub-semigroup of  $S$  containing  $E$  called the sub-semigroup *generated* by  $E$ .

A *field*  $(\mathbb{K}, +, \cdot)$  is a structure where  $(\mathbb{K}, +, 0)$  and  $(\mathbb{K} \setminus \{0\}, \cdot, 1)$  are commutative groups and multiplication distributes over addition. For all  $n \in \mathbb{N}$ ,  $\mathbb{K}^n$  is an  $n$ -dimensional *vector space* over the field  $\mathbb{K}$ . We will work with row vectors and apply matrices on the right. The set of  $n$  by  $m$  matrices over  $\mathbb{K}$  will be denoted by  $\mathbb{K}^{n \times m}$  and  $\mathbb{K}^{1 \times n}$  (or simply  $\mathbb{K}^n$  when there is no ambiguity) will denote set of  $n$  dimensional vectors. For any matrix  $M$ , we will denote its transpose by  $M^t$ . A *vector subspace* of  $\mathbb{K}^n$  is a subset of  $\mathbb{K}^n$  stable by linear combinations and for all subsets  $E$  of  $\mathbb{K}^n$ ,  $\text{span}(E)$  will denote the smallest vector subspace of  $\mathbb{K}^n$  containing  $E$ .

$\mathbb{K}^n$  can also be seen as an  $n$ -dimensional *affine space*. Affine maps  $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$  are maps of the form  $f(u) = uf^{(l)} + f^{(a)}$  where  $f^{(l)} \in \mathbb{K}^{n \times m}$  and  $f^{(a)} \in \mathbb{K}^{1 \times m}$ . An *affine subspace*  $A$  of  $\mathbb{K}^n$  is a subset of  $\mathbb{K}^n$  of the form  $A = p + V$  with  $p \in A$  and  $V$  a vector subspace of  $\mathbb{K}^n$ . They are also stable by affine combinations (linear combinations with coefficients adding up to 1). For all subsets  $E$  of  $\mathbb{K}^n$ ,  $\text{aff}(E)$  will denote the smallest affine subspace of  $\mathbb{K}^n$  containing  $E$ .

**Weighted Automata and Linear Representations** Let  $\Sigma$  be a finite alphabet and  $(\mathbb{K}, +, \cdot)$  be a field. A *Weighted Automaton* (WA), on  $\Sigma$  over  $\mathbb{K}$ , is a tuple  $\mathcal{W} = (Q, i, t, \Delta)$  where  $Q$  is a finite set of states,  $i, t : Q \rightarrow \mathbb{K}$  are the initial and terminal functions respectively and  $\Delta : Q \times \Sigma \times Q \rightarrow \mathbb{K}$  is the transition function of the automaton.  $|Q|$  will be called the *dimension* of the automaton. Here,  $i, t$  and  $\Delta$  are total maps, the classical setting of partial maps is recovered by assigning a null weight.

For  $p, q \in Q$  and  $a \in \Sigma$ , if  $k = \Delta(p, a, q)$ , the transition will be denoted by  $p \xrightarrow{a:k} q$ . A run of  $\mathcal{W}$  on a word  $w = a_1 \dots a_n \in \Sigma^*$  is a sequence of transitions  $q_0 \xrightarrow{a_1:k_1} q_1 \xrightarrow{a_2:k_2} \dots \xrightarrow{a_n:k_n} q_n$ . The weight of the run is the following product of weights:  $i(q_0)k_1 \dots k_nt(q_n)$ . We say that this run is *accepting* if every weight in this product is non null. The function  $\llbracket \mathcal{W} \rrbracket : \Sigma^* \rightarrow \mathbb{K}$  realized by the WA maps each word  $w$  to the sum of the weights of all the runs of  $\mathcal{W}$  on  $w$ .

A function  $f : \Sigma^* \rightarrow \mathbb{K}$  is said to be *rational* if there exists a WA  $\mathcal{W}$  such that  $f = \llbracket \mathcal{W} \rrbracket$ . Rational functions can also be defined using linear representations :

**Definition 2.1** (Linear Representations). *Let  $f : \Sigma^* \rightarrow \mathbb{K}$  be a rational function.*

*A linear representation of dimension  $n \in \mathbb{N}$  of  $f$  is a triple  $\mathcal{R} = (u, \mu, v)$ , where  $u \in \mathbb{K}^{1 \times n}$ ,  $v \in \mathbb{K}^{n \times 1}$  and  $\mu : \Sigma^* \rightarrow \mathbb{K}^{n \times n}$  is a monoid morphism such that, for all  $w \in \Sigma^*$ ,  $f(w) = u\mu(w)v$ .*

*$f$  will then be denoted as  $\llbracket \mathcal{R} \rrbracket$ .  $u$  and  $v$  will be called the initial and terminal vectors respectively and the  $\mu(a)$ , for  $a \in \Sigma$ , will be called the transition matrices.*

There is a one-to-one correspondance between weighted automata and linear representations (see [13]). We will then use either of those terms and definitions interchangeably.

**Example 2.1.** *We consider the WA depicted on Figure 1, on the alphabet  $\{a\}$  and over the field of real numbers. There are two states  $p$  and  $q$ . We have  $i(p) = 1 = t(p)$ , while  $i(q) = 0 = t(q)$ . Only transitions whose weight is non null are depicted. One can verify that the function realized by this WA maps the*

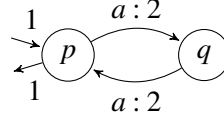


Figure 1: The weighted automaton of Example 2.1.

word  $a^n$  to  $2^n$  if  $n$  is even, and to 0 otherwise. The linear representation  $\mathcal{R} = (u, \mu, v)$  associated with this WA is obtained by taking  $u = (1 \ 0)$ ,  $v = (1 \ 0)^t$ , and  $\mu(a) = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ .

A WA / linear representation of a rational function  $f$  is said to be *minimal* if its dimension is minimal among all the WA / linear representations of  $f$ . We also have the following characterization of minimal representations (see [13] for a proof):

**Proposition 2.1.** *An  $n$ -dimensional linear representation  $\mathcal{R} = (u, \mu, v)$  is minimal if and only if  $\text{span}(u\mu(\Sigma^*)) = \mathbb{K}^{1 \times n}$  and  $\text{span}(\mu(\Sigma^*)v) = \mathbb{K}^{n \times 1}$ .*

**Expressions, substitutions and Cost Register Automata** For a field  $(\mathbb{K}, +, \cdot)$  and a finite set of variables  $\mathcal{X}$  disjoint from  $\mathbb{K}$ , let  $\text{Exp}(\mathcal{X})$  denote the set of expressions generated by the grammar  $e ::= k|X|e + e|e \cdot e$ , where  $k \in \mathbb{K}$  and  $X \in \mathcal{X}$ . An expression is *linear* (resp. *affine*) if it has the form  $\sum_{i=1}^n \alpha_i X_i$  (resp.  $\sum_{i=1}^n \alpha_i X_i + \beta$ ) for some family of  $\alpha_i, \beta \in \mathbb{K}$  and  $X_i \in \mathcal{X}$ . We will denote by  $\text{Exp}_\ell(\mathcal{X})$  (resp.  $\text{Exp}_a(\mathcal{X})$ ) the set of linear (resp. affine) expressions.

A *substitution* over  $\mathcal{X}$  is a map  $s : \mathcal{X} \rightarrow \text{Exp}(\mathcal{X})$ . It can be extended to a map  $\text{Exp}(\mathcal{X}) \rightarrow \text{Exp}(\mathcal{X})$  by substituting each variable  $X$  in the expression given as an input by  $s(X)$ . By identifying  $s$  with its extension, we can then compose substitutions. We call *valuations* the substitutions of the form  $v : \mathcal{X} \rightarrow \mathbb{K}$ . The set of substitutions over  $\mathcal{X}$  will be denoted by  $\text{Sub}(\mathcal{X})$  and the set of valuations  $\text{Val}(\mathcal{X})$ .

**Definition 2.2** (Cost Register Automaton). A cost register automaton (CRA for short), on the alphabet  $\Sigma$  over the field  $\mathbb{K}$ , is a tuple  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$  where  $Q$  is a finite set of states,  $q_0 \in Q$  is the initial state  $\mathcal{X}$  is a finite set of registers (variables),  $v_0 \in \text{Val}(\mathcal{X})$  is the registers' initial valuation,  $o : Q \rightarrow \text{Exp}(\mathcal{X})$  is the output function, and  $\delta : Q \times \Sigma \rightarrow Q \times \text{Sub}(\mathcal{X})$  is the transition function.

We will denote by  $\delta_Q := \pi_Q \circ \delta$  the transition function of the underlying automaton of the CRA and  $\delta_{\mathcal{X}} := \pi_{\text{Sub}(\mathcal{X})} \circ \delta$  its register update function.

$\mathcal{A}$  computes a function  $\llbracket \mathcal{A} \rrbracket : \Sigma^* \rightarrow \mathbb{K}$  defined as follows : the configurations of  $\mathcal{A}$  are pairs  $(q, v) \in Q \times \text{Val}(\mathcal{X})$ . The run of  $\mathcal{A}$  on a word  $w = a_1 \dots a_n \in \Sigma^*$  is the sequence of configurations  $(q_i, v_i)_{i \in [0, n]}$  where,  $q_0$  is the initial state,  $v_0$  is the initial valuation and, for all  $i \in [1, n]$ ,  $q_i = \delta_Q(q_{i-1}, a_i)$  and  $v_i = v_{i-1} \circ \delta_{\mathcal{X}}(q_{i-1}, a_i)$ . We then define  $\llbracket \mathcal{A} \rrbracket(w) = v_n(o(q_n))$ .

$\delta$  can be extended to words by setting, for all  $q \in Q$ ,  $\delta(q, \varepsilon) = (q, \text{id}_{\mathcal{X}})$ , where  $\text{id}_{\mathcal{X}}$  is the substitution such that  $\text{id}_{\mathcal{X}}(X) = X$  for all  $X \in \mathcal{X}$ , and, for all  $a \in \Sigma$  and  $w \in \Sigma^*$ ,  $\delta_Q(q, aw) = \delta_Q(\delta_Q(q, a), w)$  and  $\delta_{\mathcal{X}}(q, aw) = \delta_{\mathcal{X}}(q, a) \circ \delta_{\mathcal{X}}(\delta_Q(q, a), w)$ . We then have

$$\llbracket \mathcal{A} \rrbracket(w) = v_0 \circ \delta_{\mathcal{X}}(q_0, w)(o(\delta_Q(q_0, w)))$$

A CRA  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$  is called *linear* (resp. *affine*) if, for all  $q \in Q, a \in \Sigma$  and  $X \in \mathcal{X}$ ,  $\delta_{\mathcal{X}}(q, a)(X) \in \text{Exp}_\ell(\mathcal{X})$  (resp.  $\text{Exp}_a(\mathcal{X})$ ) and  $o(q) \in \text{Exp}_\ell(\mathcal{X})$  (resp.  $\text{Exp}_a(\mathcal{X})$ ).

**Example 2.2** (Example 2.1 continued). Two CRA are depicted on Figure 2. They are both on the alphabet  $\{a\}$  and over the field of real numbers, and both realize the same function as the WA considered in Example 2.1.

Is there a Cayley-Hamilton theorem for WFA?

i.e. for every  $w \in \Sigma^*$

$$A_w = \sum_{U \in \Sigma^{\leq m}} \alpha_U \cdot A_U$$

5

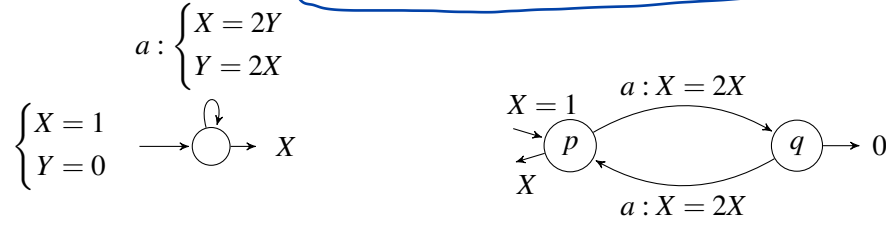


Figure 2: Two CRA detailed in Example 2.2.

The CRA depicted on the left has a single state, and two registers  $X$  and  $Y$ . They are initialised to 1 and 0 respectively, and the output function maps the unique state to the expression  $X$ . Last, the single transition is associated with the substitution  $s$  which maps  $X$  to  $2Y$ , and  $Y$  to  $2X$ , respectively.

The CRA depicted on the right has two states  $p$  and  $q$ , and a single register  $X$ . The initial state is  $p$ , and the output function maps  $p$  to  $X$ , and  $q$  to 0. The two transitions of the CRA apply the same substitution which maps  $X$  to  $2X$ .

It is well-known that linear CRA and WA are equivalent [1]. One can actually directly view a WA as a linear CRA with a single state:

**Proposition 2.2.** *There is a one-to-one correspondence between WA and linear CRA with a single state.*

Given a WA, one can build an equivalent CRA with as many registers as states of the WA. The linear presentation of the WA yields the transitions of the CRA: for each letter  $a$ , the matrix  $\mu(a)$  can be interpreted as a (linear) substitution, associated with the self-loop of label  $a$ .

Conversely, we first observe that, for a (linear) CRA  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$ , we can assume that  $\mathcal{X} = \{X_1, \dots, X_n\}$  is ordered. We then identify any linear expression  $e = \sum_{i=1}^n \alpha_i X_i$  (with the  $\alpha_i$  not present in the expression assumed to be 0) with the linear form  $\underline{e} : \mathbb{K}^n \rightarrow \mathbb{K}$  defined by the column matrix  $(\alpha_1 \dots \alpha_n)^t$ . We can then identify any linear substitution  $s : \mathcal{X} \rightarrow \text{Exp}_{\ell}(\mathcal{X})$  with the linear map  $\underline{s} : \mathbb{K}^n \rightarrow \mathbb{K}^n$  defined by the block matrix  $(\underline{s}(X_1) \mid \dots \mid \underline{s}(X_n))$ , and we can identify any valuation  $v : \mathcal{X} \rightarrow \mathbb{K}$  with the vector  $\underline{v} = (v(X_1) \dots v(X_n))$  of the vector space  $\mathbb{K}^n$ .

The registers of  $\mathcal{A}$  and their updates can then be characterized by the values of  $\underline{v}_0$ ,  $\underline{\delta_{\mathcal{X}}(q, a)}$  and  $\underline{o(q)}$ , for  $q \in Q$  and  $a \in \Sigma$ , and we can check that

$$\llbracket \mathcal{A} \rrbracket(w) = \underline{v}_0 \cdot \underline{\delta_{\mathcal{X}}(q_0, w)} \cdot \underline{o(\delta_Q(q_0, w))}$$

The result easily follows when the CRA has a single state.

**Example 2.3** (Example 2.1 continued). *The CRA depicted on the left of Figure 2 is obtained by the translation of WA into CRA with a single state.*

### 3 Equivalences between WA and CRA

In this section, we survey the known equivalences between subclasses of WA and fragments of CRA, and the known associated decidability results.

We first recall the following classical subclasses of WA:

**Definition 3.1.** *Let  $\mathcal{W} = (Q, i, t, \Delta)$  be a WA, and  $k \in \mathbb{N}$ . We say that:*

- $\mathcal{W}$  is sequential if there is a single state  $q \in Q$  such that  $i(q) \neq 0$ , and for each letter  $\sigma \in \Sigma$  and state  $q \in Q$ , there is at most one state  $q'$  such that  $\Delta(q, \sigma, q') \neq 0$ ,

- $\mathcal{W}$  is multi-sequential if it is defined as the disjoint union of finitely many sequential WA,
- $\mathcal{W}$  is  $k$ -ambiguous if for every word  $w$ , there are at most  $k$  accepting runs of  $\mathcal{W}$  on  $w$ . When  $k = 1$ , we say that  $\mathcal{W}$  is unambiguous. Last,  $\mathcal{W}$  is finitely-ambiguous if it is  $k$ -ambiguous for some  $k$ .

**Remark 3.1.** Observe that a sequential WA is syntactically equivalent to a linear CRA with a single register; as a CRA has an underlying deterministic finite automaton.

**Example 3.1** (Example 2.1 continued). The CRA depicted on the right of Figure 2 is obtained from the (sequential) WA described in Example 2.1.

Now we introduce two classical fragments of CRA. To do so we consider restrictions on updates.

**Definition 3.2** (Copyless CRA). We say that an expression  $e \in \text{Exp}(\mathcal{X})$  is copyless if  $e$  uses every variable from  $\mathcal{X}$  at most once. A substitution  $s$  is copyless if for every  $X \in \mathcal{X}$ , the expression  $s(X)$  is copyless and  $X$  appears in at most one of the expressions  $\{s(Y) \mid Y \in \mathcal{X}\}$ .

We say that a CRA is copyless if for every transition  $\delta(q, a) = (p, s)$ , the substitution  $s$  is copyless, and for every state  $q \in Q$ , the output expression  $o(q)$  is copyless.

**Definition 3.3** (Monomial CRA). Let  $e = \sum_{i=1}^n \alpha_i X_i$  be a linear expression. We say that  $e$  is monomial if the sum contains a single term, i.e. at most one  $\alpha_i$  is not null. A linear CRA is monomial if all its updates use monomial expressions. Last, we say that it is transition-monomial if every update used in a transition is a monomial expression, but updates used in the final output function may not be.

The landscape of the known equivalences between classes of weighted automata, and classes of CRA, is depicted on Figure 3. On this figure, all classes of CRA considered are linear, except affine CRA.

Let us comment briefly on these equivalences. First, the equivalence between linear CRA and Weighted Automata has been proven in the original paper introducing Cost Register automata [1]. In addition, when the WA is unambiguous, then the first law of the semiring, which is used to aggregate the weights of the different runs, becomes useless. This allows to show the equivalence between unambiguous WA and monomial CRA. The other equivalences are rather folklore and not very involved. For instance, the one between sequential WA and CRA has been discussed in Remark 3.1, while the one between unambiguous multi-sequential WA and copyless monomial CRA comes from [8]. As these equivalences do not constitute the main contribution of this paper, we will not develop them further. Observe that all these equivalences are valid for an arbitrary semiring<sup>1</sup>.

We now turn to decidability results for the case of fields. First, Bell and Smertnig have recently shown in [3, 4] that given a WA over a field, one can decide whether there exists an equivalent sequential (resp. unambiguous) WA. These two results are depicted by the dashed arrows.

These two problems are *subclass definability problems*, i.e. they consist in deciding, given an element in some superclass, whether there exists an equivalent element in some subclass.

In this paper, we will focus on a particular instance of such subclass definability problem, which is the problem of *register minimization*. It is defined as follows:

**Definition 3.4** (Register minimization problem). Given a class  $\mathcal{C}$  of CRA, we consider the following decision problem:

- **Input:** a CRA in the class  $\mathcal{C}$ , and an integer  $k \in \mathbb{N}$
- **Question:** Does there exist an equivalent CRA in the class  $\mathcal{C}$  with at most  $k$  registers?

no bound on #states

<sup>1</sup>However, as we lose commutativity, this requires to slightly modify the definitions of expressions, by writing them as  $X\alpha$  instead of  $\alpha X$ .



This constitutes a natural generalization of the classical minimization problem for finite state automata. In the context of implementing CRA, the main resource, regarding memory usage for instance, is the set of registers. It is thus natural to try to minimize it. Unfortunately, this is a hard problem, which has only few positive answers. This problem has been first studied in [2] for so-called additive CRA, *i.e.* monomial CRA over the integers, showing it is PSpace-complete in this case. Then, this problem has been proven to be decidable for semirings satisfying some conditions (fulfilled by fields), for two classes of CRA: copyless monomial CRA [8], and monomial CRA [9]. In Figure 3, this is emphasized by surrounding these two classes with dotted lines. In all these positive results, the CRA considered use only the multiplicative law of the semiring. In this work, we show that this problem is decidable for the general case of linear CRA, and also for affine CRA. This constitutes the first positive results for register minimization in the presence of the two laws of the semiring.

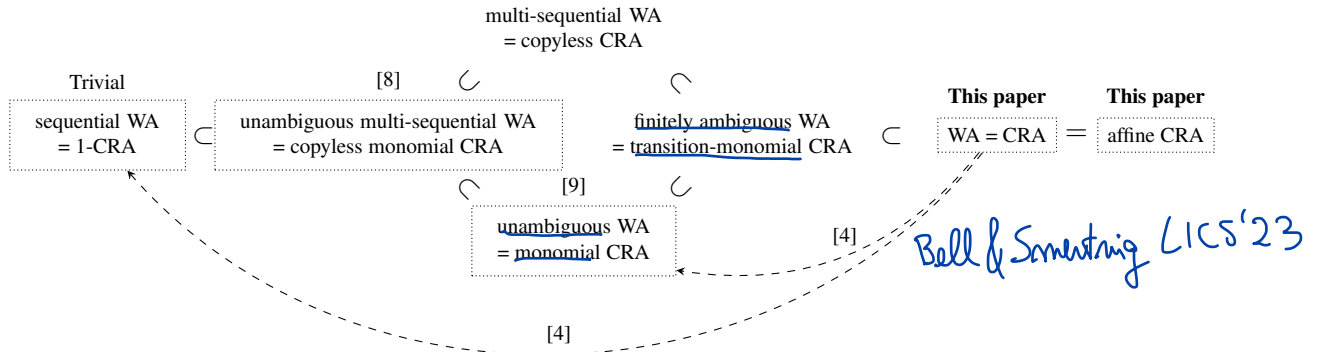


Figure 3: A landscape of equivalences between weighted automata and cost register automata. In this picture, to lighten the names of classes considered, all classes of CRA are linear (except affine CRA). Dashed arrows indicate decidable subclass decision problems. Classes depicted inside a dotted rectangle have a decidable register minimization problem.

## 4 Register minimization for linear CRA

In this section, we introduce the linear hull of a WA and use it to state our main result: the minimal number of registers needed by a CRA to realize a rational function is the dimension of the linear hull of a minimal WA realizing it. To do so, we will need the following topological notions:

Let  $\mathbb{K}$  be a field and  $n \in \mathbb{N}$ . The Zariski topology on  $\mathbb{K}^n$  is defined as the topology whose closed sets are the sets of common roots of a finite collection of polynomials of  $\mathbb{K}[X_1, \dots, X_n]$ . A linear version of this topology, called the linear Zariski topology, was introduced by Bell and Smertnig in [3]. Its closed sets are finite unions of vector subspaces of  $\mathbb{K}^n$ .

For a set  $S \subseteq \mathbb{K}^n$ ,  $\overline{S}^z$  and  $\overline{S}^\ell$  will denote its closure in the Zariski and linear Zariski topologies respectively.

A set  $S \subseteq \mathbb{K}^n$  is called *irreducible* if, for all closed sets  $C_1$  and  $C_2$ , such that  $S \subseteq C_1 \cup C_2$ , we have either  $S \subseteq C_1$  or  $S \subseteq C_2$ . The (linear) Zariski topology is a Noetherian topology in which every closed set can be written as a finite union of irreducible components. In the following we will use (implicitly)

the following properties of irreducible sets : if  $S \subseteq \mathbb{K}^n$  is irreducible and  $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$  is continuous, then  $f(S)$  is irreducible (see [3] for proofs and references).

In the linear Zariski topology on  $\mathbb{K}^n$ , irreducible sets are vector subspaces of  $\mathbb{K}^n$  and linear maps are continuous and closed maps (maps closed sets to closed sets). In particular, for all  $S \subseteq \mathbb{K}^n$  and linear map  $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$ ,  $\overline{f(S)}^\ell = f(\overline{S}^\ell)$ .

Let's now define the algebraic invariant of WA that we will use to solve the register minimization problem for linear CRA:

**Definition 4.1.** Let  $\Sigma$  be a finite alphabet and let  $\mathcal{R} = (u, \mu, v)$  be a linear representation on  $\Sigma$  over  $\mathbb{K}$ .

The (left) reachability set of  $\mathcal{R}$  is defined as  $\text{LR}(\mathcal{R}) = u\mu(\Sigma^*) = \{u\mu(w) \mid w \in \Sigma^*\}$

The (left) linear hull of  $\mathcal{R}$  is the closure of  $\text{LR}(\mathcal{R})$  in the linear Zariski topology. It will be denoted by  $\overline{\text{LR}(\mathcal{R})}^\ell$ . Its dimension  $\dim(\overline{\text{LR}(\mathcal{R})}^\ell)$  is defined as the maximal dimension of its irreducible components. ← vector spaces

(We can dually define the right reachability set and right linear hull of  $\mathcal{R}$  as  $\text{RR}(\mathcal{R}) = \mu(\Sigma^*)v$  and  $\overline{\text{RR}(\mathcal{R})}^\ell$  respectively.)

**Example 4.1** (Example 2.1 continued). The reachability set of the WA considered in example 2.1 is  $\text{LR}(\mathcal{R}) = \{(2^{2n}, 0) \mid n \in \mathbb{N}\} \cup \{(0, 2^{2n+1}) \mid n \in \mathbb{N}\}$ . Its linear hull is then the union of the two coordinate axes of the plane  $\overline{\text{LR}(\mathcal{R})}^\ell = \text{span}(1, 0) \cup \text{span}(0, 1)$ .

Indeed, the inclusion  $\subseteq$  comes from the fact that  $u = (1, 0) \in \text{span}(1, 0)$  and  $\text{span}(1, 0) \cup \text{span}(0, 1)$  is stable by multiplication by  $\mu(a)$  and the inclusion  $\supseteq$  comes from the fact that, for the linear Zariski topology,  $\{(1, 0)\}$  is dense in  $\text{span}(1, 0)$  and  $\{(0, 2)\}$  is dense in  $\text{span}(0, 1)$ .

**Lemma 4.1.** The linear hull of a linear representation is computable.

*Proof sketch.* It was shown in [10] that the Zariski closure of a semigroup generated by a finite set of matrices is computable. This result can be used (as in [11], Proposition 1) to compute their linear Zariski closure: ✓ algebraic variety

For a given finite set of matrices  $S \subseteq \mathbb{K}^{n \times n}$ , let  $\overline{\langle S \rangle}^z = Z_1 \cup \dots \cup Z_r$  with the  $Z_i$  being the irreducible components. We then have  $\overline{\langle S \rangle}^\ell = \text{span}(Z_1) \cup \dots \cup \text{span}(Z_r)$ .

Indeed, let  $W = W_1 \cup \dots \cup W_s$  be a closed set (in the linear Zariski topology) covering  $\langle S \rangle$ . Since, for all  $i \in \llbracket 1, r \rrbracket$ ,  $Z_i \subseteq Z$  and  $Z_i$  is irreducible, then there exists  $j \in \llbracket 1, s \rrbracket$  such that  $Z_i \subseteq W_j$  and since  $W_j$  is a vector subspace, then  $\text{span}(Z_i) \subseteq W_j$ . Finally  $\text{span}(Z_1) \cup \dots \cup \text{span}(Z_r) \subseteq W$ .

For all  $i \in \llbracket 1, r \rrbracket$ ,  $Z_i$  is given by a finite set of polynomial equations. We can then compute a basis of  $\text{span}(Z_i)$  by starting from any vector satisfying the equations defining  $Z_i$  and adding in new vectors, satisfying the equations defining  $Z_i$  and the equations stating their linear independence from the previously computed vectors. This procedure terminates after  $\dim(\text{span}(Z_i))$  vectors are found. The vectors satisfying the given equations are computable using quantifier elimination in the theory of reals.

For a given linear representation  $\mathcal{R} = (u, \mu, v)$ ,  $\overline{\mu(\Sigma^*)}^\ell$  is then computable and so is  $\overline{\text{LR}(\mathcal{R})}^\ell = \overline{u\mu(\Sigma^*)}^\ell = u\overline{\mu(\Sigma^*)}^\ell$ .

Another approach, working directly with the linear Zariski topology, was proposed by Bell and Smertnig in [4]. □

The linear hull of two representations of the same function does not necessarily coincide but, since  $\mathbb{K}$  is a field, it is well known that for every rational function  $f$ , there exists a (computable) minimal linear representation of  $f$  that is unique up to similarity in the following sense (see [13]):



**Definition 4.2.** Let  $\mathcal{R} = (u, \mu, v)$  and  $\mathcal{R}' = (u', \mu', v')$  be  $n$ -dimensional linear representations over  $\mathbb{K}$ .

$\mathcal{R}$  and  $\mathcal{R}'$  are said to be similar if there exists an invertible matrix  $P \in \mathbb{K}^{n \times n}$  such that  $u' = uP$ ,  $\mu'(a) = P^{-1}\mu(a)P$  for all  $a \in \Sigma$  and  $v' = P^{-1}v$ .

We then see that the linear hull of two similar representations only differ by a change of basis. In particular, their dimension and number of components coincide.

Known before

The notion of linear hull was introduced by Bell and Smertnig in [3]. They showed, in [4], that the linear hull is computable and used it to show that determining if a rational function is computable by a sequential (or an unambiguous) WA over a field is decidable.

**Theorem 4.1** ([3]). Let  $f$  be a rational function.

$f$  can be realized by a sequential WA if and only if the linear hull of a minimal linear representation of  $f$  has a dimension of at most 1.

Our main result generalizes this theorem by linking the dimension of the linear hull to the number of registers of a CRA:

**Theorem 4.2.** Let  $f$  be a rational function.

and efficient

The minimal number of registers needed by a linear CRA to realize  $f$  is the dimension of the linear hull of a minimal linear representation of  $f$ .

Moreover, if  $k$  denotes the dimension of this linear hull and  $d$  its number of irreducible components, there exists a (computable) CRA with  $d$  states and  $k$  registers realizing  $f$ .

$d$  is not necessarily minimal

**Corollary 4.1.** The register minimization problem for linear CRA is decidable.

**Example 4.2** (Example 2.1 continued). As we have seen in example 4.1,  $\overline{\text{LR}(\mathcal{R})}^\ell$  is 1-dimensional and has two irreducible components, thus  $\llbracket \mathcal{R} \rrbracket$  can be realized by a CRA with two states and one register (depicted on the right of figure 2).

Let's first show that the dimension of the linear hull of a minimal linear representation is minimal.

**Proposition 4.1.** Let  $\mathcal{R}_{\min}$  be a minimal linear representation of a rational function  $f$ .

If  $\mathcal{R}$  is a linear representation of  $f$ , then  $\dim(\overline{\text{LR}(\mathcal{R}_{\min})}^\ell) \leq \dim(\overline{\text{LR}(\mathcal{R})}^\ell)$ .

In the following, for all  $n \in \mathbb{N}$ , let  $E_n = \{e_1, \dots, e_n\}$  denote the canonical basis of  $\mathbb{K}^n$ . For two bases  $B$  and  $B'$  of the same vector space, let  $P_{B \rightarrow B'}$  denote the change of basis matrix from  $B$  to  $B'$ . And finally, for two integers  $i$  and  $j$ , let  $I_i$  denote the identity matrix of size  $i$  and let  $I_{i \times j}$  denote the  $i$  by  $j$  matrix ( $I_i \mid 0$ ) if  $i \leq j$  and  $I_{j \times i}^t$  otherwise.

**Remark 4.1.** If  $V$  is a  $d$ -dimensional vector subspace of  $\mathbb{K}^n$  and  $B$  is a basis of  $\mathbb{K}^n$  whose first  $d$  vectors form a basis of  $V$ , then, for all  $v \in V$ , since the  $n - d$  last entries of the vector  $vP_{E_n \rightarrow B}$  are all zeros, we note that  $vP_{E_n \rightarrow B}I_{n \times d}I_{d \times n}P_{B \rightarrow E_n} = v$ .

**Lemma 4.2.** Let  $\mathcal{R}$  be a linear representation of a rational function  $f$  and let  $d = \dim(\text{span}(\overline{\text{LR}(\mathcal{R})}^\ell))$  (resp.  $\dim(\text{span}(\overline{\text{RR}(\mathcal{R})}^\ell))$ ).

We can construct a  $d$ -dimensional linear representation  $\mathcal{R}_m$  of  $f$  such that  $\dim(\overline{\text{LR}(\mathcal{R}_m)}^\ell) \leq \dim(\overline{\text{LR}(\mathcal{R})}^\ell)$  and  $\text{span}(\overline{\text{LR}(\mathcal{R}_m)}^\ell) = \mathbb{K}^d$  (resp.  $\text{span}(\overline{\text{RR}(\mathcal{R}_m)}^\ell) = \mathbb{K}^d$ ).

*Proof.* We will prove the lemma for the (left) reachability set. Let  $\mathcal{R} = (u, \mu, v)$ , let  $n$  be the dimension of  $\mathcal{R}$  and let  $B$  be a basis of  $\mathbb{K}^n$  obtained by completing a basis  $\{b_1, \dots, b_d\}$  of  $\text{span}(\overline{\text{LR}(\mathcal{R})}^\ell)$  with arbitrary vectors.

We define  $\mathcal{R}_m$  as  $(u', \mu', v')$  where, for all  $a \in \Sigma$ ,

$$u' = uP_{E_n \rightarrow B}I_{n \times d} \quad \mu'(a) = I_{d \times n}P_{B \rightarrow E_n}\mu(a)P_{E_n \rightarrow B}I_{n \times d} \quad v' = I_{d \times n}P_{B \rightarrow E_n}v$$

We can show by induction, thanks to remark 4.1, that, for all  $w \in \Sigma^*$ ,  $u'\mu'(w) = u\mu(w)P_{E_n \rightarrow B}I_{n \times d}$ . So  $\llbracket \mathcal{R}_m \rrbracket = \llbracket \mathcal{R} \rrbracket$  and, since  $\{b_1, \dots, b_d\}P_{E_n \rightarrow B}I_{n \times d} = \{e_1, \dots, e_d\}I_{n \times d} = E_d$ , then  $\text{span}(\text{LR}(\mathcal{R})_m) = \mathbb{K}^d$ .

Moreover,  $\text{LR}(\mathcal{R}_m) = \text{LR}(\mathcal{R})P_{E_n \rightarrow B}I_{n \times d}$  and, since linear maps are continuous and closed maps in the linear Zariski topology,  $\overline{\text{LR}(\mathcal{R}_m)}^\ell = \overline{\text{LR}(\mathcal{R})}^\ell P_{E_n \rightarrow B}I_{n \times d}$ .

The irreducible components of  $\overline{\text{LR}(\mathcal{R}_m)}^\ell$  are then images of the irreducible components of  $\overline{\text{LR}(\mathcal{R})}^\ell$  by a linear map. Thus  $\dim(\overline{\text{LR}(\mathcal{R}_m)}^\ell) \leq \dim(\overline{\text{LR}(\mathcal{R})}^\ell)$ .

The case of the right reachability set is proven similarly (using a basis of  $\text{span}(\text{RR}(\mathcal{R}))$ ).  $\square$

*Proof of Proposition 4.1.* Alternating the left and right constructions of lemma 4.2 on  $\mathcal{R}$ , we obtain a linear representation  $\mathcal{R}_m$ , that is minimal due to Proposition 2.1, and, since all minimal linear representations are similar, we conclude that  $\dim(\overline{\text{LR}(\mathcal{R}_{\min})}^\ell) = \dim(\overline{\text{LR}(\mathcal{R}_m)}^\ell) \leq \dim(\overline{\text{LR}(\mathcal{R})}^\ell)$ .  $\square$

Let's now show the link between CRA and the linear hulls of WA.

**Proposition 4.2.** *Let  $\mathcal{R}$  be a linear representation and let  $d$  be the dimension of  $\overline{\text{LR}(\mathcal{R})}^\ell$  and  $k$  be the number of its irreducible components.*

*There exists a CRA  $\mathcal{A}$  with  $k$  states and  $d$  registers such that  $\llbracket \mathcal{A} \rrbracket = \llbracket \mathcal{R} \rrbracket$*

*Proof.* Let  $\mathcal{R} = (u, \mu, v)$ , let  $n$  be the dimension of  $\mathcal{R}$  and let  $W_1, \dots, W_k$  be the irreducible components of  $\overline{\text{LR}(\mathcal{R})}^\ell$ . We assume, without loss of generality, that  $u \in W_1$ . For all  $i \in \llbracket 1, k \rrbracket$ , let  $B_i$  be a basis of  $\mathbb{K}^n$  obtained by completing a basis of  $W_i$  with arbitrary vectors.

We define  $\mathcal{A}$  as  $(Q, q_0, \mathcal{X}, v_0, o, \delta)$  where:

- $Q = \llbracket 1, k \rrbracket$  and  $q_0 = 1$ .
- $\mathcal{X} = \{X_1, \dots, X_d\}$ ,  $v_0 = uP_{E_n \rightarrow B_1}I_{n \times d}$  and, for all  $q \in Q$ ,  $o(q) = I_{d \times n}P_{B_q \rightarrow E_n}v$ .
- for all  $q \in Q$  and  $a \in \Sigma$ , let  $p$  be an element of  $\{\underline{p} \in \llbracket 1, k \rrbracket \mid W_q\mu(a) \subseteq W_p\}$  (chosen arbitrarily).  $\delta(q, a)$  will be defined by  $\delta_Q(q, a) = p$  and  $\delta_{\mathcal{X}}(q, a) = I_{d \times n}P_{B_q \rightarrow E_n}\mu(a)P_{E_n \rightarrow B_p}I_{n \times d}$ .

We can show by induction, using remark 4.1, that, for all  $w \in \Sigma^*$ ,  $v_0\delta_{\mathcal{X}}(q_0, w) = u\mu(w)P_{E_n \rightarrow B_{\delta_Q(q_0, w)}}I_{n \times d}$ . Thus  $\llbracket \mathcal{A} \rrbracket = v_0\delta_{\mathcal{X}}(q_0, w)o(\delta_Q(q_0, w)) = \llbracket \mathcal{R} \rrbracket$ .  $\square$

**Proposition 4.3.** *Let  $\mathcal{A}$  be a CRA with  $k$  states and  $d$  registers.*

*There exists a  $kd$ -dimensional linear representation  $\mathcal{R}$  of  $\llbracket \mathcal{A} \rrbracket$  such that  $\dim(\overline{\text{LR}(\mathcal{R})}^\ell) < d$ .*

*Proof.* Let's assume, without loss of generality, that  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$  where  $Q = \llbracket 1, k \rrbracket$ ,  $q_0 = 1$  and  $\mathcal{X} = \{X_1, \dots, X_d\}$ .

We define  $\mathcal{R}$  as  $(u, \mu, v)$ , where  $u = (\underline{v_0} \ 0 \dots 0) \in \mathbb{K}^{1 \times kd}$ ,  $v = \begin{pmatrix} o(1) \\ \vdots \\ o(k) \end{pmatrix} \in \mathbb{K}^{kd \times 1}$  and, for all  $a \in \Sigma$ ,

$$\mu(a) = \begin{pmatrix} \delta_{1,1}(a) & \dots & \delta_{1,k}(a) \\ \vdots & \ddots & \vdots \\ \delta_{k,1}(a) & \dots & \delta_{k,k}(a) \end{pmatrix} \in \mathbb{K}^{kd \times kd} \text{ where, for all } i, j \in \llbracket 1, k \rrbracket, \delta_{i,j}(a) \in \mathbb{K}^{d \times d} \text{ is defined by}$$

$$\delta_{i,j}(a) = \begin{cases} \delta_{\mathcal{X}}(i, a) & \text{if } \delta_Q(i, a) = j \\ 0 & \text{otherwise} \end{cases}.$$

We can show by induction that, for all  $w \in \Sigma^*$ ,  $\mu(w) = \left( \begin{array}{c|c|c} \delta_{1,1}(w) & \dots & \delta_{1,k}(w) \\ \hline \vdots & \ddots & \vdots \\ \hline \delta_{k,1}(w) & \dots & \delta_{k,k}(w) \end{array} \right)$  where, for all  $i, j \in \llbracket 1, k \rrbracket$ ,  $\delta_{i,j}(w) = \begin{cases} \delta_{\mathcal{Q}}(i, w) & \text{if } \delta_{\mathcal{Q}}(i, w) = j \\ 0 & \text{otherwise} \end{cases}$ .

We then have

$$\llbracket \mathcal{R} \rrbracket = u\mu(w)v = \sum_{i=1}^n \underline{v_0} \delta_{1,i}(w) \underline{o(i)} = \underline{v_0} \delta_{1,\delta_{\mathcal{Q}}(1,w)}(w) \underline{o(\delta_{\mathcal{Q}}(1,w))} = \llbracket \mathcal{A} \rrbracket$$

Moreover, since for all  $w \in \Sigma^*$ ,  $u\mu(w) = (\underline{v_0}\delta_{1,1}(w) | \dots | \underline{v_0}\delta_{1,k}(w))$  and only  $\delta_{1,\delta_{\mathcal{Q}}(1,w)}(w)$  is potentially nonzero, then  $\text{LR}(\mathcal{R}) \subseteq \bigcup_{i=1}^k \varphi_i(\mathbb{K}^d)$  where, for all  $i \in \llbracket 1, k \rrbracket$ ,  $\varphi_i : \mathbb{K}^d \rightarrow \mathbb{K}^{kd}$  maps every vector  $v \in \mathbb{K}^d$  to the vector of  $\mathbb{K}^{kd}$  that has  $v$  as its  $i$ -th “block” of size  $d$  and zeros everywhere else. Thus  $\dim(\overline{\text{LR}(\mathcal{R})}^\ell) \leq d$ .  $\square$

We can now show the main result:

*Proof of theorem 4.2.* Let  $f$  be a rational function, let  $d_{\text{CRA}}$  be the minimal number of registers needed by a linear CRA to realize  $f$  and let  $d_{\text{rep}}$  be the dimension of the linear hull of a minimal linear representation of  $f$  and  $k_{\text{rep}}$  the number of its irreducible components.

We will show that  $d_{\text{CRA}} = d_{\text{rep}}$  and construct a CRA with  $d_{\text{rep}}$  registers and  $k_{\text{rep}}$  states.

If  $d_{\text{CRA}} > d_{\text{rep}}$  then Proposition 4.2 shows that there exists a CRA with  $d_{\text{rep}}$  registers realizing  $f$ , contradicting the minimality of  $d_{\text{CRA}}$ . Thus  $d_{\text{CRA}} \leq d_{\text{rep}}$ .

Reciprocally, if  $d_{\text{CRA}} < d_{\text{rep}}$  then Proposition 4.3 gives a linear representation of  $f$  with a  $d_{\text{CRA}}$ -dimensional linear hull, contradicting the minimality of  $d_{\text{rep}}$  given by Proposition 4.1. Thus  $d_{\text{rep}} \leq d_{\text{CRA}}$ .

We can obtain the desired CRA by applying the construction of Proposition 4.2 to a minimal linear representation of  $f$ .  $\square$

Using the minimal number of registers can, however, have a big impact on the number of states of the underlying automaton of the CRA, as shown in the example below:

**Example 4.3.** Let  $n \in \mathbb{N}$ . An  $n$ -dimensional permutation matrix is an  $n$  by  $n$  matrix that has exactly one 1 in each row and each column and zeros everywhere else. The set  $\text{Perm}_n$  of permutation matrices together with matrix multiplication form a group of order  $n!$  and can be generated using two elements.  $\overline{\text{Perm}_n}^\ell$  is one dimensional and has  $n!$  irreducible components, as it is a union of  $n!$  lines.

Using the previous result, we can then show that, a rational function, on a two-letter alphabet, with an  $n$ -dimensional minimal linear representation that has as transition matrices two generators of  $\text{Perm}_n$ , can be realized by a CRA with only one register but  $n!$  states.

flip two rows or two columns

## 5 Tradeoff states/registers

In this section, we consider the more general minimization problem for CRA defined as:

**Definition 5.1** (CRA minimization problem). Given a class  $\mathcal{C}$  of CRA, we consider the following decision problem:

- **Input:** a CRA in the class  $\mathcal{C}$ , and two integers  $k, d \in \mathbb{N}$

- **Question:** Does there exist an equivalent CRA in the class  $\mathcal{C}$  with at most  $k$  states and at most  $d$  registers?

For a linear CRA realizing a rational function with a minimal linear representation  $\mathcal{R}$ , the results of the previous section and the correspondence between linear representations and CRA gives us two possible extreme cases : first, the CRA that has the minimal number of registers (the dimension of  $\overline{\text{LR}(\mathcal{R})}^\ell$ ) and the maximal number of “useful” states (the number of irreducible components of  $\overline{\text{LR}(\mathcal{R})}^\ell$ ) and second, the CRA that has the minimal number of states (one) and the maximal number of “useful” registers (the dimension of  $\mathcal{R}$ ). We show, in this section, the decidability of the minimization problem for linear CRA by giving a procedure to enumerate all the CRA with numbers of states and registers in between these bounds, balancing out the two resources of the machine.

**Definition 5.2** ( $k, d$ -congruences). Let  $\mathcal{R} = (u, \mu, v)$  be a linear representation and let  $\overline{\text{LR}(\mathcal{R})}^\ell = W_1 \cup \dots \cup W_r$  be its linear hull, where the  $W_i$ , for  $i \in \llbracket 1, r \rrbracket$ , are its irreducible components.

A  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^\ell$  is a partition  $\mathcal{P}$  of  $\llbracket 1, r \rrbracket$  into  $k$  parts such that

$i \rightarrow i'$  :

- (1) for all  $C \in \mathcal{P}$  and  $a \in \Sigma$ , there exists  $C' \in \mathcal{P}$  verifying that for all  $i \in C$  there exists  $i' \in C'$  such that  $W_i \mu(a) \subseteq W_{i'}$ . (the set of  $C' \in \mathcal{P}$  verifying this property will be denoted by  $C\mu(a)$ )
- (2) for all  $C \in \mathcal{P}$ ,  $\dim(\text{span}(\bigcup_{i \in C} W_i)) \leq d$ .

$k, d$ -congruences allow to group together components of a linear hull without making the dimension increase beyond  $d$ .

**Theorem 5.1.** Let  $f$  be a rational function.

$f$  is realizable by a CRA with  $k$  states and  $d$  registers if and only if  $f$  has a linear representation  $\mathcal{R}$  with a linear hull that has a  $k, d$ -congruence.

The proof of this theorem generalizes the proofs of Propositions 4.2 and 4.3.

*Proof.* If  $\mathcal{A}$  is a CRA with  $k$  states and  $d$  registers realizing  $f$ , let's consider the same construction and notations of the proof of Proposition 4.3 and let  $\overline{\text{LR}(\mathcal{R})}^\ell = W_1 \cup \dots \cup W_r$ , where the  $W_i$  for  $i \in \llbracket 1, r \rrbracket$  are the irreducible components.

We will show that  $\mathcal{P} = \{C_1, \dots, C_k\}$  with, for all  $j \in \llbracket 1, k \rrbracket$ ,  $C_j = \{i \in \llbracket 1, r \rrbracket \mid W_i \subseteq \varphi_j(\mathbb{K}^d)\}$ , is a  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^\ell$ .

First, since for all  $i \in \llbracket 1, r \rrbracket$ ,  $W_i \subseteq \bigcup_{j=1}^k \varphi_j(\mathbb{K}^d)$  and  $W_i$  is irreducible, then there exists  $j \in \llbracket 1, k \rrbracket$  such that  $W_i \subseteq \varphi_j(\mathbb{K}^d)$ . So the  $C_j$  are well-defined. Then, since for all  $j \in \llbracket 1, k \rrbracket$ ,  $\text{span}(\bigcup_{i \in C_j} W_i)$  is a subspace of  $\varphi_j(\mathbb{K}^d)$  by definition, we have  $\dim(\text{span}(\bigcup_{i \in C_j} W_i)) \leq d$ . Finally, for all  $j \in \llbracket 1, k \rrbracket$  and  $a \in \Sigma$ , by definition of  $\mu(a)$ , there exists  $j' \in \llbracket 1, k \rrbracket$  such that  $\varphi_j(\mathbb{K}^d)\mu(a) \subseteq \varphi_{j'}(\mathbb{K}^d)$ . This implies that, for all  $C_j \in \mathcal{P}$  and  $a \in \Sigma$ , there exists  $C_{j'} \in \mathcal{P}$  verifying that for all  $i \in C_j$  there exists  $i' \in C_{j'}$  such that  $W_i \mu(a) \subseteq W_{i'}$ .

Thus  $\mathcal{P}$  is an  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^\ell$ .

Reciprocally, if  $\mathcal{R} = (u, \mu, v)$  is an  $n$ -dimensional linear representation of  $f$  with  $\mathcal{P}$  a  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^\ell = W_1 \cup \dots \cup W_r$ , let's assume, without loss of generality, that  $u \in W_1$ .

Let, for all  $C \in \mathcal{P}$ ,  $B_C$  be a basis of  $\mathbb{K}^n$  obtained by completing a basis of  $\text{span}(\bigcup_{i \in C} W_i)$  with arbitrary vectors.

We define a CRA  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$  with  $k$  states and  $d$  registers realizing  $f$  with:

- $Q = \mathcal{P}$  and  $q_0 = C_1 \in \mathcal{P}$  where  $C_1$  is the class containing 1.

- $\mathcal{X} = \{X_1, \dots, X_d\}$ ,  $v_0 = uP_{E_n \rightarrow B_{q_0}} I_{n \times d}$  and, for all  $q \in Q$ ,  $o(q) = I_{d \times n} P_{B_q \rightarrow E_n} v$ .
- for all  $q \in Q$  and  $a \in \Sigma$ , let  $p$  be an element of  $q\mu(a)$  (chosen arbitrarily).  $\delta(q, a)$  will be defined by  $\delta_Q(q, a) = p$  and  $\delta_{\mathcal{X}}(q, a) = I_{d \times n} P_{B_q \rightarrow E_n} \mu(a) P_{E_n \rightarrow B_p} I_{n \times d}$ .

We prove that  $\mathcal{A}$  is equivalent to  $\mathcal{R}$  the same way as in the proof of Proposition 4.2.  $\square$

For a CRA with a given number of registers, this result can lead to a big reduction in the number of states, as shown in the example below:

**Example 5.1.** Let  $n \in \mathbb{N}$ . Using an alphabet of size  $n + 1$  and the matrices of Example 4.3 generating  $\text{Perm}_n$ , we can define a 2n-dimensional linear representation with a linear hull that can be written as the union of  $n!$  one-dimensional irreducible component and an  $(n - 1)$ -dimensional one.

Since  $\dim(\text{span}(\text{Perm}_n)) = n - 1$ , we can define on this linear hull a  $2, (n - 1)$ -congruence, merging together the one-dimensional irreducible components without raising the dimension of the linear hull, thus reducing the number of states of the corresponding CRA to 2 while keeping the same number of registers.

See Appendix B for the details of the construction.

We can show that we only need to consider minimal linear representations:

**Proposition 5.1.** If  $\mathcal{R}$  is a linear representation such that  $\overline{\text{LR}(\mathcal{R})}^\ell$  has a  $k, d$ -congruence then any minimal representation of  $\llbracket \mathcal{R} \rrbracket$  has a  $k, d$ -congruence.

The proof of this proposition generalizes the proof of Proposition 4.1. The following lemma gives the left and right constructions needed to obtain the desired minimal representation.

**Lemma 5.1.** Let  $\mathcal{R}$  be a linear representation of a rational function  $f$  and let  $d = \dim(\text{span}(\text{LR}(\mathcal{R})))$  (resp.  $\dim(\text{span}(\text{RR}(\mathcal{R})))$ ).

If  $\overline{\text{LR}(\mathcal{R})}^\ell$  has a  $k, d$ -congruence, we can construct a  $d$ -dimensional linear representation  $\mathcal{R}_m$  of  $f$  such that  $\overline{\text{LR}(\mathcal{R}_m)}^\ell$  has a  $k, d$ -congruence and  $\text{span}(\text{LR}(\mathcal{R}_m)) = \mathbb{K}^d$  (resp.  $\text{span}(\text{RR}(\mathcal{R}_m)) = \mathbb{K}^d$ ).

*Proof.* Let's consider the same construction and notations of the proof of lemma 4.2 and let  $\overline{\text{LR}(\mathcal{R})}^\ell = W_1 \cup \dots \cup W_r$  and  $\overline{\text{LR}(\mathcal{R}_m)}^\ell = W'_1 \cup \dots \cup W'_r$  where, for all  $i \in \llbracket 1, r \rrbracket$ ,  $W'_i = W_i P_{E_n \rightarrow B} I_{n \times d}$ .

If  $\mathcal{P}$  is a  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^\ell$ , we will show that it is also a  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R}_m)}^\ell$ .

Let  $C \in \mathcal{P}$ ,  $a \in \Sigma$  and  $C' \in C\mu(a)$ . Since, for all  $i \in C$  there exists  $i' \in C'$  such that  $W_i \mu(a) \subseteq W_{i'}$ , we then have  $W'_i \mu'(a) = W_i P_{E_n \rightarrow B} I_{n \times d} I_{d \times n} P_{B \rightarrow E_n} \mu(a) P_{E_n \rightarrow B} I_{n \times d} = W_i \mu(a) P_{E_n \rightarrow B} I_{n \times d} \subseteq W_{i'} P_{E_n \rightarrow B} I_{n \times d} = W'_{i'}$ .

Moreover, for all  $C \in \mathcal{P}$ ,  $\text{span}(\bigcup_{i \in C} W'_i) = \text{span}(\bigcup_{i \in C} W_i P_{E_n \rightarrow B} I_{n \times d}) = \text{span}(\bigcup_{i \in C} W_i) P_{E_n \rightarrow B} I_{n \times d}$ . Thus,  $\dim(\text{span}(\bigcup_{i \in C} W'_i)) \leq \dim(\text{span}(\bigcup_{i \in C} W_i)) \leq d$   $\square$

Given a rational function  $f$ , we can then find “every” CRA realizing  $f$  by constructing a minimal linear representation of  $f$  and enumerating all the possible  $k, d$ -congruence on its linear hull and we get the following decidability result:

**Corollary 5.1.** The minimization problem for linear CRA is decidable.

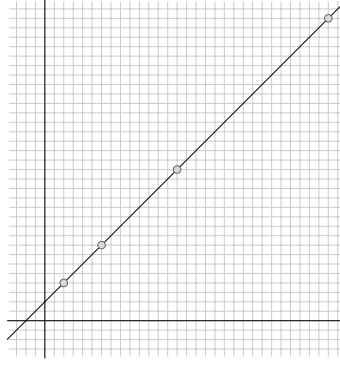


Figure 4: Graphic representation of the reachability set of the WA of Example 6.1.

## 6 Affine CRA

We can naturally extend the results shown in the previous sections on linear CRA to CRA with affine register updates by considering the affine Zariski topology instead of the linear one. This allows to use up to one less register than the minimal number needed in the linear case.

Let  $\mathbb{K}$  be a field and  $n \in \mathbb{N}$ . The *affine Zariski topology* is the topology on  $\mathbb{K}^n$  whose closed sets are finite unions of affine subspaces of  $\mathbb{K}^n$ . This topology has the same properties as the linear Zariski topology. For a set  $S \subseteq \mathbb{K}^n$ ,  $\overline{S}^a$  will denote its closure in the affine Zariski topology.

Similarly to the linear case, we define affine hulls of WA in the natural way, using the affine Zariski topology.

**Definition 6.1.** Let  $\Sigma$  be a finite alphabet and let  $\mathcal{R} = (u, \mu, v)$  be a linear representation on  $\Sigma$  over  $\mathbb{K}$ .

The (left) affine hull of  $\mathcal{R}$  is the closure of  $\text{LR}(\mathcal{R})$  in the affine Zariski topology. It will be denoted by  $\overline{\text{LR}(\mathcal{R})}^a$ . Its dimension  $\dim(\overline{\text{LR}(\mathcal{R})}^a)$  is defined as the maximal dimension of its irreducible components.

(The, dually defined, right affine hull will be denoted by  $\overline{\text{RR}(\mathcal{R})}^a$ )

**Example 6.1.** On the alphabet  $\Sigma = \{a\}$ , let  $\mathcal{R} = (u, \mu, v)$ , where  $u = (1 \ 2)$ ,  $\mu(a) = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$  and  $v = (1 \ 0)^t$ , be a linear representation (over  $\mathbb{R}$ ) of the rational function  $f$  defined by  $f(a^n) = \sum_{i=0}^n 2^i$ .

The reachability set of  $\mathcal{R}$  is  $\text{LR}(\mathcal{R}) = \{(\sum_{i=0}^n 2^i, 2^{n+1}) \mid n \in \mathbb{N}\}$ .

For the linear Zariski topology,  $\text{LR}(\mathcal{R})$  is dense in  $\mathbb{R}^2$ . So the linear hull  $\overline{\text{LR}(\mathcal{R})}^\ell = \mathbb{R}^2$  is two dimensional. However, note that, for all  $(x, y) \in \text{LR}(\mathcal{R})$ ,  $y = x + 1$ . So, by an argument of density in the affine Zariski topology, the affine hull  $\overline{\text{LR}(\mathcal{R})}^a$  is the affine line  $y = x + 1$ , which is one dimensional.

The computability of the affine hull follows from the same arguments as in the linear case.

**Lemma 6.1.** The affine hull of a linear representation is computable.

We can also define  $k, d$ -congruences on the affine hull.

**Definition 6.2.** Let  $\mathcal{R} = (u, \mu, v)$  be a linear representation and let  $\overline{\text{LR}(\mathcal{R})}^a = W_1 \cup \dots \cup W_r$  be its affine hull, where the  $W_i$ , for  $i \in \llbracket 1, r \rrbracket$ , are its irreducible components.

A  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^a$  is a partition  $\mathcal{P}$  of  $\llbracket 1, r \rrbracket$  into  $k$  parts such that

- (1) for all  $C \in \mathcal{P}$  and  $a \in \Sigma$ , there exists  $C' \in \mathcal{P}$  verifying that for all  $i \in C$  there exists  $i' \in C'$  such that  $W_i \mu(a) \subseteq W_{i'}$ . (the set of  $C' \in \mathcal{P}$  verifying this property will be denoted by  $C\mu(a)$ )
- (2) for all  $C \in \mathcal{P}$ ,  $\dim(\text{aff}(\bigcup_{i \in C} W_i)) \leq d$ .



All the previous results obtained in the linear case still hold for the affine case.

**Theorem 6.1.** *Let  $f$  be a rational function.*

*The minimal number of registers needed by an affine CRA to realize  $f$  is the dimension of the affine hull of a minimal linear representation of  $f$ .*

*Moreover,  $f$  is realizable by an affine CRA with  $k$  states and  $d$  registers if and only if  $f$  has a linear representation with an affine hull that has a  $k, d$ -congruence and every possible  $k, d$ -congruence can be found on the affine hull of a minimal representation of  $f$ .*

**Corollary 6.1.** *The minimization and register minimization problems for affine CRA are decidable.*

The proof is the same as in the linear case, replacing vector spaces with affine ones and readjusting the constructions accordingly. For the sake of completeness, it can be found in the appendix.



Figure 5: Two CRA detailed in Example 6.2.

**Example 6.2** (Example 6.1 continued). *The two CRA depicted on Figure 5 realizes the function of the previous example.*

*On the left we have a linear CRA with two registers and, on the right, an affine CRA with only one register. The previous results show that both have the minimal number of register for their respective classes of CRA.*

## 7 Conclusion

We have shown how to decide the CRA minimisation problem, and are thus able to minimise simultaneously the number of states and registers needed to realise a rational function.

An important question which remains is the one of complexity of this procedure: can the linear (resp. affine) hull of a WA be computed in ELEMENTARY complexity. In their article [3] the authors do not give complexity upper bounds for the computation of the linear hull. Similarly, in [10] where the authors show how to compute the best polynomial invariant for an affine program, no complexity is given for their algorithm. In fact one can observe that computing the best algebraic invariant for a polynomial automaton cannot be done in ELEMENTARY complexity, since the zeroness problem for polynomial automata is ACKERMANN-hard [5]. Our problem is however simpler in two crucial ways:

1. the automata we consider are linear and not polynomial, which makes things probably much easier. For instance, if all the register updates are invertible, then computing the best algebraic invariant can be done in ELEMENTARY complexity (see [12]),
2. we do not need to compute the best algebraic invariant, only the best linear one, which may be much coarser and is a fundamentally much simpler object.

*in fact it is skolem hard*

Questions which remain open are the ones given in Fig 3 of register minimisation for subclasses of CRA. Given a copyless CRA (which correspond to multi-sequential WA) can one find an equivalent copyless CRA with fewer registers? Similarly, a register minimization procedure for *transition-monomial* CRA (corresponding to finitely ambiguous WA) is not known. While the techniques used for solving the corresponding unambiguous cases are very different, it is possible that this linear hull approach could be a useful tool to tackle these questions.

A much more ambitious goal would be to consider register minimisation in the context of different semirings, but there, all the linear algebra tools which are crucial to solve these problems completely vanish. Similarly, it seems that register minimisation for polynomial automata would be very difficult. Indeed in both cases no minimal/canonical machine is known to exist, which is a central tool to solving the linear case over fields.

## References

- [1] Rajeev Alur, Loris D'Antoni, Jyotirmoy V. Deshmukh, Mukund Raghothaman & Yifei Yuan (2013): *Regular Functions and Cost Register Automata*. In: *28th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2013, New Orleans, LA, USA, June 25-28, 2013*, IEEE Computer Society, pp. 13–22.
- [2] Rajeev Alur & Mukund Raghothaman (2013): *Decision Problems for Additive Regular Functions*. In: *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part II, Lecture Notes in Computer Science 7966*, Springer, pp. 37–48.
- [3] Jason Bell & Daniel Smertnig (2021): *Noncommutative rational Pólya series*. *Selecta Mathematica* 27, doi:10.1007/s00029-021-00629-2.
- [4] Jason P. Bell & Daniel Smertnig (2023): *Computing the linear hull: Deciding Deterministic? and Unambiguous? for weighted automata over fields*. In: *LICS '23, ACM*. To appear.
- [5] Michael Benedikt, Timothy Duff, Aditya Sharad & James Worrell (2017): *Polynomial automata: Zeroness and applications*. In: *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, IEEE Computer Society, pp. 1–12, doi:10.1109/LICS.2017.8005101. Available at <https://doi.org/10.1109/LICS.2017.8005101>.
- [6] Jean Berstel (1979): *Transductions and context-free languages*. Teubner Studienbücher : Informatik 38, Teubner. Available at <https://www.worldcat.org/oclc/06364613>.
- [7] Laure Daviaud (2020): *Containment and Equivalence of Weighted Automata: Probabilistic and Max-Plus Cases*. In Alberto Leporati, Carlos Martín-Vide, Dana Shapira & Claudio Zandron, editors: *Language and Automata Theory and Applications - 14th International Conference, LATA 2020, Milan, Italy, March 4-6, 2020, Proceedings, Lecture Notes in Computer Science 12038*, Springer, pp. 17–32, doi:10.1007/978-3-030-40608-0\_2. Available at [https://doi.org/10.1007/978-3-030-40608-0\\_2](https://doi.org/10.1007/978-3-030-40608-0_2).
- [8] Laure Daviaud, Ismaël Jecker, Pierre-Alain Reynier & Didier Villevalois (2017): *Degree of Sequentiality of Weighted Automata*. In: *FOSSACS 2017, Lecture Notes in Computer Science 10203*, pp. 215–230.
- [9] Laure Daviaud, Pierre-Alain Reynier & Jean-Marc Talbot (2016): *A Generalised Twinning Property for Minimisation of Cost Register Automata*. In: *LICS '16, ACM*, pp. 857–866.
- [10] Ehud Hrushovski, Joël Ouaknine, Amaury Pouly & James Worrell (2018): *Polynomial Invariants for Affine Programs*. In Anuj Dawar & Erich Grädel, editors: *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, ACM, pp. 530–539, doi:10.1145/3209108.3209142. Available at <https://doi.org/10.1145/3209108.3209142>.
- [11] Engel Lefauchaux, Joël Ouaknine, David Purser & James Worrell (2021): *Porous Invariants*. In Alexandra Silva & K. Rustan M. Leino, editors: *Computer Aided Verification - 33rd International Conference, CAV 2021, Virtual Event, July 20-23, 2021, Proceedings, Part II, Lecture Notes in Computer Science 12760*,

all invertible

- Springer, pp. 172–194, doi:10.1007/978-3-030-81688-9\_8. Available at [https://doi.org/10.1007/978-3-030-81688-9\\_8](https://doi.org/10.1007/978-3-030-81688-9_8).
- [12] Klara Nosan, Amaury Pouly, Sylvain Schmitz, Mahsa Shirmohammadi & James Worrell (2022): On the Computation of the Zariski Closure of Finitely Generated Groups of Matrices. In Marc Moreno Maza & Lihong Zhi, editors: *ISSAC '22: International Symposium on Symbolic and Algebraic Computation*, Villeneuve-d'Ascq, France, July 4 - 7, 2022, ACM, pp. 129–138, doi:10.1145/3476446.3536172. Available at <https://doi.org/10.1145/3476446.3536172>.
- [13] Jacques Sakarovitch (2009): *Elements of Automata Theory*. Cambridge University Press, doi:10.1017/CB09781139195218.
- [14] Marcel Paul Schützenberger (1961): *On the Definition of a Family of Automata*. *Inf. Control*. 4(2-3), pp. 245–270, doi:10.1016/S0019-9958(61)80020-X. Available at [https://doi.org/10.1016/S0019-9958\(61\)80020-X](https://doi.org/10.1016/S0019-9958(61)80020-X).

# Appendices

## A Proof of theorem 6.1

Similarly to the linear case, we identify any affine expression  $e = \sum_{i=1}^n \alpha_i X_i + \beta$  with the affine form  $\underline{e} : \mathbb{K}^n \rightarrow \mathbb{K}$  defined by  $\underline{e}(u) = u\underline{e}^{(l)} + \underline{e}^{(a)}$  with  $\underline{e}^{(l)} = (\alpha_1 \dots \alpha_n)^t$  and  $\underline{e}^{(a)} = \beta$ . We can then identify any affine substitution  $s : \mathcal{X} \rightarrow \text{Exp}_a(\mathcal{X})$  with the affine map  $\underline{s} : \mathbb{K}^n \rightarrow \mathbb{K}^n$  defined by  $\underline{s}(u) = u\underline{s}^{(l)} + \underline{s}^{(a)}$  with  $\underline{s}^{(l)} = (\underline{s}(X_1))^{(l)} \dots \underline{s}(X_n)^{(l)}$  and  $\underline{s}^{(a)} = ((\underline{s}(X_1))^{(a)} \dots \underline{s}(X_n)^{(a)})$ , and we can identify any valuation  $v : \mathcal{X} \rightarrow \mathbb{K}$  with the point  $\underline{v} = (v(X_1) \dots v(X_n))$  of the affine space  $\mathbb{K}^n$ .

And, like in the linear case, the registers of an affine CRA  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$  and their updates can be characterized by the values of  $\underline{v_0}$ ,  $\underline{\delta_{\mathcal{X}}(q, a)}$  and  $\underline{o(q)}$ , for  $q \in Q$  and  $a \in \Sigma$ , and we can check that

$$\llbracket \mathcal{A} \rrbracket(w) = \underline{o(\delta_Q(q_0, w))} \left( \underline{\delta_{\mathcal{X}}(q_0, w)} (\underline{v_0}) \right)$$

### A.1 From linear representations to affine CRA

We tweak the construction of 4.2 to get an affine CRA with  $k$  states and  $d$  registers from a  $k, d$ -congruence on the affine hull of a linear representation:

Let  $\mathcal{R} = (u, \mu, v)$  be a linear representation, let  $n$  be the dimension of  $\mathcal{R}$  and let  $W_1, \dots, W_k$  be the irreducible components of  $\text{LR}(\mathcal{R})^a$ . We assume, without loss of generality, that  $u \in W_1$ .

Let  $\mathcal{P}$  be a  $k, d$ -congruence on  $\text{LR}(\mathcal{R})^a$  and for all  $C \in \mathcal{P}$ , let  $\text{aff}(\bigcup_{i \in C} W_i) = p_C + V_C$  with  $p_C \in \mathbb{K}^n$  and  $V_C$  a vector subspace of  $\mathbb{K}^n$  and let  $B_C$  be a basis of  $\mathbb{K}^n$  obtained by completing a basis of  $V_C$  with arbitrary vectors.

We define  $\mathcal{A}$  as  $(Q, q_0, \mathcal{X}, v_0, o, \delta)$  where:

- $Q = \mathcal{P}$  and  $q_0 = C_1 \in \mathcal{P}$  where  $C_1$  is the class containing 1.
- $\mathcal{X} = \{X_1, \dots, X_d\}$  and  $\underline{v_0} = (u - p_{q_0}) P_{E_n \rightarrow B_{q_0}} I_{n \times d}$
- for all  $q \in Q$  and  $x \in \mathbb{K}^d$ ,  $\underline{o(q)}(x) = (p_q + x I_{d \times n} P_{B_q \rightarrow E_n}) v$ .
- for all  $q \in Q$  and  $a \in \Sigma$ , let  $q'$  be an element of  $\{p \in \llbracket 1, k \rrbracket \mid W_q \mu(a) \subseteq W_p\}$  (chosen arbitrarily).  $\delta(q, a)$  will be defined by  $\delta_Q(q, a) = q'$  and, for all  $x \in \mathbb{K}^d$ ,

$$\underline{\delta_{\mathcal{X}}(q, a)}(x) = ((p_q + x I_{d \times n} P_{B_q \rightarrow E_n}) \mu(a) - p_{q'}) P_{E_n \rightarrow B_{q'}} I_{n \times d}$$

We can show by induction that, for all  $w \in \Sigma^*$ ,

$$\underline{\delta_{\mathcal{X}}(q_0, w)} (\underline{v_0}) = \left( u \mu(w) - p_{\delta_Q(q_0, w)} \right) P_{E_n \rightarrow B_{\delta_Q(q_0, w)}} I_{n \times d}$$

Thus  $\llbracket \mathcal{A} \rrbracket = \llbracket \mathcal{R} \rrbracket$ .

Taking a trivial partition, we also obtain an affine version of Proposition 4.2.

### A.2 From affine CRA to linear representations

We tweak the construction of 4.3 to get a linear representation with an affine hull that has an  $k, d$ -congruence from a CRA with  $d$  registers and  $k$  states:

Let  $\mathcal{A} = (Q, q_0, \mathcal{X}, v_0, o, \delta)$  be an affine CRA where, we assume without loss of generality that,  $Q = \llbracket 1, k \rrbracket$ ,  $q_0 = 1$  and  $\mathcal{X} = \{X_1, \dots, X_d\}$ .

We define  $\mathcal{R}$  as  $(u, \mu, v)$ , where:

- $u = (\underline{v_0} \ 1 \ 0 \dots 0) \in \mathbb{K}^{1 \times k(d+1)}$
- $v = \begin{pmatrix} o_1 \\ \vdots \\ o_n \end{pmatrix} \in \mathbb{K}^{k(d+1) \times 1}$ . where, for all  $i \in \llbracket 1, k \rrbracket$ ,  $o_i = \begin{pmatrix} \underline{o(i)^{(l)}} \\ \underline{o(i)^{(a)}} \end{pmatrix}$ .
- for all  $a \in \Sigma$ ,  $\mu(a) = \left( \begin{array}{c|c|c} \delta_{1,1}(a) & \dots & \delta_{1,k}(a) \\ \vdots & \ddots & \vdots \\ \delta_{k,1}(a) & \dots & \delta_{k,k}(a) \end{array} \right) \in \mathbb{K}^{k(d+1) \times k(d+1)}$  where, for all  $i, j \in \llbracket 1, k \rrbracket$ ,  

$$\delta_{i,j}(a) = \begin{pmatrix} \underline{\delta_{\mathcal{Q}}(i,a)^{(l)}} & 0 \\ \underline{\delta_{\mathcal{Q}}(i,a)^{(a)}} & 1 \end{pmatrix} \text{ if } \delta_{\mathcal{Q}}(i,w) = j \text{ and } 0 \text{ otherwise.}$$

Like in the linear case, we show by induction that the definition of the  $\delta_{i,j}$  extends to words and proves that  $\llbracket \mathcal{R} \rrbracket = \llbracket \mathcal{A} \rrbracket$ .

We observe that, for all  $w \in \Sigma^*$ ,  $u\mu(w) = ((\underline{v_0} \ 1)\delta_{1,1}(w) | \dots | (\underline{v_0} \ 1)\delta_{1,k}(w))$  and only  $\delta_{1,\delta_{\mathcal{Q}}(1,w)}(w)$  is potentially nonzero, then  $\text{LR}(\mathcal{R}) \subseteq \bigcup_{i=1}^k \psi_i(\mathbb{K}^d)$  where, for all  $i \in \llbracket 1, k \rrbracket$ ,  $\psi_i : \mathbb{K}^d \rightarrow \mathbb{K}^{k(d+1)}$  maps every vector  $v \in \mathbb{K}^d$  to the vector of  $\mathbb{K}^{k(d+1)}$  that has  $(v \ 1)$  as its  $i$ -th “block” of size  $d+1$  and zeros everywhere else.

Note that the  $\psi_i$  are affine maps. So,  $\dim(\overline{\text{LR}(\mathcal{R})^a}) \leq d$  and we can show, like in the linear case, that  $\mathcal{P} = \{C_1, \dots, C_k\}$  with, for all  $j \in \llbracket 1, k \rrbracket$ ,  $C_j = \{i \in \llbracket 1, r \rrbracket \mid W_i \subseteq \psi_j(\mathbb{K}^d)\}$ , is a  $k, d$ -congruence on  $\overline{\text{LR}(\mathcal{R})^a}$ .

### A.3 Left and right minimization

The proof of lemma 4.2 and 5.1 remains the same for their affine versions. The key point is that linear maps are a particular case of affine maps and the properties used in these two proof remain true. Thus, Proposition 4.1 and 5.1 still hold for the affine hull.

## B Details of Example 5.1

The symmetric group can be generated using the cycle  $(1 \ 2 \dots n)$  and the transposition  $(1 \ 2)$ . Let  $C$  and  $T$  be their respective corresponding matrices in  $\text{Perm}_n$ .

For all  $i \in \llbracket 1, n-1 \rrbracket$ , let  $M_i = \left( \begin{array}{c|c} I_{n-1} & 0 \\ \hline e_i & 1 \end{array} \right)$ , where  $I_{n-1}$  is the identity matrix of size  $n-1$  and  $e_i$  is the  $i$ -th vector of the canonical basis of  $\mathbb{K}^{n-1}$ .

Let  $\Sigma = \{a, b, c_1, c_2, \dots, c_{n-1}\}$  be an alphabet of size  $n+1$ .

Let  $\mathcal{R} = (u, \mu, v)$  be the  $2n$ -dimensional linear representation, on  $\Sigma$ , defined by:

- $u = (1 \ 2 \dots n \mid 0 \dots 0 \ 1) \in \mathbb{K}^{1 \times 2n}$
- $\mu(a) = \left( \begin{array}{c|c} C & 0 \\ \hline 0 & I_n \end{array} \right)$ ,  $\mu(b) = \left( \begin{array}{c|c} T & 0 \\ \hline 0 & I_n \end{array} \right)$  and, for all  $i \in \llbracket 1, n-1 \rrbracket$ ,  $\mu(c_i) = \left( \begin{array}{c|c} 0 & 0 \\ \hline 0 & M_i \end{array} \right)$ .
- $v \in \mathbb{K}^{n \times 1}$  can be arbitrary.

Note that  $\langle \mu(a), \mu(b) \rangle = \left\{ \left( \begin{array}{c|c} P & 0 \\ \hline 0 & I_n \end{array} \right) \mid P \in \text{Perm}_n \right\}$  and, for all vector  $(k_1 \dots k_n \mid l_1 \dots l_{n-1} \ 1) \in \mathbb{K}^{1 \times 2n}$ ,  
 $(k_1 \dots k_n \mid l_1 \dots l_{n-1} \ 1)\mu(c_i) = (0 \dots 0 \mid l_1 \dots l_i + 1 \dots l_{n-1} \ 1)$ .

The reachability set of  $\mathcal{R}$  is then the union of the two sets  $S_1 = \left\{ \left( (12 \dots n)P \mid 0 \dots 01 \right) \mid P \in \text{Perm}_n \right\}$  and  $S_2 = \left\{ \left( 0 \dots 0 \mid l_1 \dots l_{n-1} 1 \right) \mid l_1, \dots, l_{n-1} \in \mathbb{N} \right\}$ . Thus,  $\overline{\text{LR}(\mathcal{R})}^\ell$  is the union of  $\text{span}(S_2)$  and the  $n!$  lines, going through the origin, directed by the vectors of  $S_1$ .

Since  $\dim(\text{span}(S_1)) = n - 1$  and, for all  $\sigma \in \Sigma$  and  $i \in \{1, 2\}$ , there exists  $j \in \{1, 2\}$  such that  $S_i \mu(\sigma) \subseteq S_j$ , we can define a  $2, (n - 1)$ -congruence on  $\overline{\text{LR}(\mathcal{R})}^\ell$  by grouping together all the irreducible components corresponding to the lines.