Representations of Reversible Automata and State Graphs of Vector Addition Systems

Eric Badouel

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Representations of Reversible Automata and State Graphs of Vector Addition Systems

Eric Badouel

N ° 3490

septembre 1998

THÈME 1

ISSN 0249-6399

Representations of Reversible Automata and State Graphs of Vector Addition Systems

Eric Badouel *

Thème 1 — Réseaux et systèmes
Projet Paragraphe

Rapport de recherche n3490 — septembre 1998 — 50 pages

Abstract: Using the interpretation of a place of a vector addition system as a synchronic constraint we derive a characterization of the state graphs of vector addition systems as the maximal quotients of polyhedral automata. We give a classification of the representations of reversible automata (automata in which events are local bijections on states) as full subgraphs of Schreier graphs. We describe the computation of the canonical representation of a commutative automaton (automaton that fully embedds in the Cayley graph of an abelian group). We suggest on that basis an algorithm to decide whether a finite automaton is isomorphic to the state graph of a vector addition system. The correction of this algorithm however relies on the conjecture that the state graphs of vector addition systems are torsion-free.

Key-words: Reversible Automata, Vector Addition Systems

(Résumé : tsvp)

* Email: Eric.Badouel@irisa.fr

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu, 35042 RENNES Cedex (France)
Téléphone : 02 99 84 71 00 - International : +33 2 99 84 71 00
Télécopie : 02 99 84 71 71 - International : +33 2 99 84 71 71

Représentations des automates réversibles et graphes d'états des systèmes d'addition de vecteurs

Résumé : En interprétant une place d'un système d'addition de vecteurs comme une contrainte synchronique on caractérise les graphes de marquage des systèmes d'addition de vecteurs comme les graphes réduits des graphes polyèdriques. Nous indiquons une classification des représentations des automates réversibles (c.à d. des automates dans lesquels chaque action induit une bijection partielle de l'ensemble des états) comme sous graphes pleins de graphes de Schreier. On décrit le calcul de la représentation canonique d'un automata commutatif (c.à d. d'un automate qui se plonge dans le graphe de Cayley d'un groupe commutatif). On suggère à partir de là un algorithme qui décide si un automate fini est isomorphe au graphe de marquage d'un système d'addition de vecteurs. La correction de cet algorithme repose sur la conjecture que le graphe de marquage d'un système d'addition de vecteurs est sans torsion.

Mots-clé : Automates réversibles, systèmes d'addition de vecteurs

1 Introduction

States graphs of various kind of nets are reversible automata which means that events induce local bijections on the set of states. This property greatly simplifies the study of the algebraic properties of these automata as notions borrowed from the litterature on combinatorial group theory, see [11, 19, 18, 27], like the notions of coverings, group acting on graph, and homology are well investigated and more easy to manipulate than their counterparts used in the more general context of transformation monoids. In section (2) we give a review of this theory a variant of which is known as the study of *inverse monoids* (see [21, 26]). In section (3) we give a classification of the representations of reversible automata as full subgraphs of Schreier graphs (also called coset graphs of groups). The condition that should be fufilled by the representing groups are very similar to the separation properties discovered by Ehrenfeucht and Rozenberg in their study of elementary transition systems [9, 10] (see also [6]). We also describe the computation of the canonical representation of a commutative automaton (automaton that fully embedds in the Cayley graph of an abelian group).

A place of a vector addition system (or a pure Petri net) is a synchronic constraint on the events occurring in the system, namely it constraints the relative frequence of execution of the transitions affecting that place. If the place is bounded its range of variation that is, the difference between its minimum and maximum values, is a measure of the reciprocal independence: higher values mean looser constraints. This is in agreement with the interpretation of a place as abstract resource shared by the transitions connected to that place.

The notion of synchronic distance was introduced, in the context of net theory, by C.A. Petri as a tool to measure the relative degree of freedom between sets of transitions in a concurrent system. It has been used in [2] to define a notion a *generalized regions* allowing to adapt the representation theorem of Ehrenfeucht and Rozenberg to the context of vector addition systems. A slightly different approach to synchronic relations in Petri nets was set out in [25], where linear programming techniques are used to compute upper bounds of synchronic invariants in a given net. In [1] the use of linear algebraic techniques provides a polynomial time algorithm solving the synthesis problem of vector addition systems.

Using the interpretation of a place of a vector addition system as a synchronic constraint we derive a characterization of the state graphs of vector addition systems as the maximal quotients of polyhedral automata. They are commutative automata and we conjecture that they are torsion-free, i.e. that their canonical representation does not contain torsion element. Under this assumption and using the canonical representations of commutative automata we derive an algorithm which decide whether a finite automaton is isomorphic to the state graph of a vector addition system.

2 Reversible Automata

A *transition system* is a triple (S, E, T) consisting of a set of *states* S, a set of *events* E, and a transition relation $T \subseteq S \times E \times S$. We shall write $s \xrightarrow{e} s'$ as an abbreviation for $(s, e, s') \in T$. The transition system is said to be *deterministic* (respectively *co-deterministic*) if $s \xrightarrow{e} s_1 \wedge s \xrightarrow{e} s_2 \Rightarrow s_1 = s_2$ (resp. if $s_1 \xrightarrow{e} s \wedge s_2 \xrightarrow{e} s \Rightarrow s_1 = s_2$).

Definition 1 *A reversible transition system is a deterministic and co-deterministic transition system.*

2.1 Permutation Transition Systems

A permutation transition system is a transition system in which each event induces a permutation on the set of states. It is therefore a *complete* reversible transition system. If G is a group, H a subgroup of G, and E a subset of G (usually a set of generators), the Schreier graph $S(G, H, E)$ is the permutation transition system whose states are the right-cosets $H\backslash G = \{Hg | g \in G\}$ and whose transitions are the triples (Hg, e, Hge). The Cayley graph $C(G, E)$ is $S(G, 1, E)$ where 1 is the trivial subgroup; more generally if H is a normal subgroup of G and if not two distinct generators in E are equivalent modulo H, then the Schreier graph $S(G, H, E)$ is isomorphic to the Cayley graph $C(G/H, E/H)$. Any permutation transition system (S, E, T, s_0) whose underlying graph is connected is isomorphic to the Schreier graph $S(G, H, E)$ where G is the group generated by the permutations in E and $H = G_{s_0} = \{g \in G | s_0 \cdot g = s_0\}$ is the stabiliser of the initial state. Indeed each state

$s \in S$ can be univocally encoded by the set $G_{s_0,s} = \{g \in G \mid s_0 * g = s\}$ which is a H right-coset and this correspondance is an isomorphism of transition systems. The stabilisers of the states of a connected permutation transition system are conjugate (if $s' = s * u$ then $G_{s'} = u^{-1}G_s u$), and the map $S(G, G_s, E) \stackrel{\sim}{\to} S(G, G_{s'}, E) \ : \ G_s v \mapsto G_{s'} u^{-1} v$ is an isomorphism between the respective Schreier graphs. Conversely $S(G, H, E) \cong S(G, K, E)$ implies that the groups H and K are conjugate in G. [1]

2.2 Reversible Automata

Let $\overline{E}$ be an isomorphic copy of E consisting of formal inverses $\overline{e}$ of events $e \in E$. We recall that the free group generated by E is the group with presentation $F(E) = \mathbf{gp}(E \cup \overline{E}; e \cdot \overline{e}, \overline{e} \cdot e (e \in E))$. A word in $F(E)$ is a word $u \in (E \cup \overline{E})^*$; in order to ease notation we shall usually make no distinction between a word in $F(E)$ and the actual element of $F(E)$ that it represents. A word in $F(E)$ is termed *reduced* if it contains no subwords of the form $e \cdot \overline{e}$ or $\overline{e} \cdot e$ for some $e \in E$. A reduced word is therefore the canonical form of an element of $F(E)$. The free group $F(E)$ has a partially defined action on the set of states of a reversible transition system (S, E, T) given by letting $s * e = s'$ and $s' * \overline{e} = s$ when $s \stackrel{e}{\to} s'$. A is said to be *connected* when $F(E)$ acts transitively on S: $\forall s, s' \in S \ \exists u \in F(E) \quad s * u = s'$.

Definition 2 *A reversible automaton is a connected reversible transition system together with an initial state.*

2.3 Fundamental Group and Coverings

The *fundamental group* of transition system T in state $s \in S$ is $\pi_1(T, s) = \{u \in F(E) \mid s * u = s\}$. An element of $\pi_1(T, s)$ is called a *closed path* based on s. If the automaton is connected all fundamental groups are conjugate in

[1] In fact the Schreier graph $S(G, H, E)$ is a graphical representation of the coset space cos(G:H), i.e. the set of right cosets $H\backslash G$ on which G acts by right mutiplication and the results mentioned above are the graph theoretic counterparts of the fact that any *transitive* G-space is isomorphic to a coset space cos(G:H) for some subgroup H of G and that one has therefrom a bijective correspondance between the isomorphic classes of transitive G-spaces and the conjugacy class of subgroups of G.

$F(E)$ hence isomorphic: $\pi_1(T,s') = u^{-1} \cdot \pi_1(T,s) \cdot u$ when $s * u = s'$. We let $\pi_1(A) = \pi_1(T, s_0)$ denote the fundamental group of reversible automaton $A = (S, E, T, s_0)$. Let $U \subseteq T$ be some spanning tree of the automaton A. Let u_s be the (reduced) word labelling the (unique) path in U from the initial state s_0 to state s. Each chord $t \in T \setminus U$ where $t = s \xrightarrow{e} s'$ determines a closed path $c_t = u_s \cdot e \cdot u_{s'}^{-1}$ based on s_0. The fundamental group $\pi_1(A)$ is the group freely generated by the closed paths c_t associated with the chords of some spanning tree of A.

There is a bijective correspondance between the subgroups H of $F(E)$ and the right congruences of $F(E)$ given by $u \equiv v \Leftrightarrow u \cdot v^{-1} \in H$, and $\equiv$ is a congruence if and only if H is a normal subgroup of $F(E)$. We say that a subgroup H of $F(E)$ saturates a language $L \subseteq F(E)$ when its associated right congruence does, i.e. when L is a union of right cosets of H. The *language* of a reversible automaton $A = (S, E, T, s_0)$, let $L(A) = \{u \in F(E) \mid \exists s \in S \quad s_0 * u = s\}$ is saturated by its fundamental group, indeed $L(A) = \bigcup_{s \in S} \pi_1(A) u_s$ where u_s is the (reduced) word labelling the path in some fixed spanning tree of A from s_0 to s. Conversely, if H is a subgroup of $F(E)$ and $L \subseteq F(E)$ a prefix-closed language saturated by H, we let $S(L, H, E)$ be the subautomaton of the Schreier graph $S(F(E), H, E)$ induced by the vertices (H right cosets) included in L; i.e. $S(L, H, E) = (E, S, T, s_0)$ where $S = \{Hu \mid u \in F(E) \quad Hu \subseteq L\}$ and $T = \{(Hu, e, Hue) \mid u \in F(E) \quad e \in E \quad Hu \subseteq L \quad Hue \subseteq L\}$, and $s_0 = H$. Notice that $\pi_1(S(L, H, E)) = H$ and $L(S(L, H, E)) = L$ and $A \cong S(L(A), \pi_1(A), E)$. We have therefrom bijective correspondances between the set of right congruences saturating a prefix-closed language $L \subseteq F(E)$, the set of subgroups of $F(E)$ saturating L and the set of isomorphic classes of reversible automata recognizing L.

Dual to the inclusion of their fundamental groups is the covering of reversible automata: a *covering* of a reversible automaton A is another reversible automaton $\tilde{A}$ together with a map $f : \tilde{S} \to S$ between their respective set of states such that $\forall s \in S \quad \forall \tilde{s} \in \tilde{S} \quad f(\tilde{s}) = s \Rightarrow (\forall u \in F(E) \quad s * u \Leftrightarrow \tilde{s} * u)$. Therefore if $\tilde{A}$ and A are reversible automata there exists a covering from $\tilde{A}$ to A if and only if they have the same language and $\pi_1(\tilde{A}) \subseteq \pi_1(A)$ and such a covering is *uniquely* determined by $f(\tilde{s}_0 * u) = s_0 * u$. We write $A \leq \tilde{A}$ when this happens and said that $\tilde{A}$ *covers* A. We deduce that the set of isomorphic classes of reversible automata recognizing $L \subseteq F(E)$ ordered by the covering

relation is dually-isomorphic to the set of subgroups of $F(E)$ saturating L and ordered by inclusion.

Notice that if $\pi_1(\tilde{A}) \subseteq \pi_1(A)$ then $\pi_1(\tilde{A})$ saturates every language saturated by $\pi_1(A)$ and thus the coverings $\tilde{A}$ of A can be classified up to isomorphism by the subgroups of $\pi_1(A)$; in particular there is a maximal covering corresponding to the trivial subgroup. Symmetrically the *quotients* of A correspond up to isomorphism to the groups H saturating the language of A and including its fundamental group.

A covering $f : \tilde{A} \to A$ is termed a *Galois covering* if $\pi_1(\tilde{A})$ is a normal subgroup of $\pi_1(A)$. The *Galois group* of the Galois covering f is the quotient group $\pi_1(A)/\pi_1(\tilde{A})$. A *path* in a reversible automaton $A = (S, E, T, s_0)$ is a pair $(s, u) \in S \times F(E)$ such that $s * u$ is defined, it is a *closed* based on s, noted $(s, u) \in C(s)$, if moreover $s * u = s$ (thus $\pi_1(T, s) = \{u \in F(E) \mid (s, u) \in C(s)\}$). Two closed paths $(\tilde{s}, u)$ and $(\tilde{s}', u')$ of $\tilde{A}$ are *conjugate* in the covering $f : \tilde{A} \to A$ if they have the same f-image, i.e. $f(\tilde{s}) = f(\tilde{s}')$ and $u = u'$. Then a covering $f : \tilde{A} \to A$ between reversible automata is a Galois covering if and only if every path of $\tilde{A}$ conjugate to a closed path is closed.

The *Nerode equivalence* associated with a language $L \subseteq F(E)$ is $u \equiv v \Leftrightarrow [\forall w \in F(E) \quad u \cdot w \in L \Leftrightarrow v \cdot w \in L]$, i.e. $u \equiv v$ if and only if $u^{-1}L = v^{-1}L$. It is the greatest right congruence saturating L, i.e. the Nerode group $N_L = \{u \in F(E) \mid u^{-1}L = L\}$ is the greatest subgroup of $F(E)$ saturating L.

3 Representations of Reversible Automata

3.1 Extensions of Reversible Automata

Definition 3 *An* extension *of a reversible automaton $A = (S, E, T, s_0)$ is any complete reversible automaton (i.e. permutation automaton) isomorphic to some $A' = (E, S', T', s_0)$ such that $S \subseteq S'$ and $T = T' \cap (S \times E \times S)$. The inclusion of S into S' is termed a* full embedding *of A into A'.*

If $U \subseteq T$ is some spanning tree of a reversible automaton A, we let $\Delta(A, U)$ denote the following subset of $F(E)$:

$$\Delta(A, U) = \{u_s \cdot u_{s'}^{-1} \mid \forall s, s' \in S \quad s \neq s'\} \cup \{u_s \cdot e \cdot u_{s'}^{-1} \mid \forall s, s' \in S \quad s \overset{e}{\not\to} s'\}$$

The word $u_s \cdot u_{s'}^{-1}$ is said to separate states s and s', and the word $u_s \cdot e \cdot u_{s'}^{-1}$ is said to inhibit the transition $s \xrightarrow{e} s'$. The following result gives a classification of the extensions of a reversible automaton, the conditions that a representing group should satisfy are analogues to the separation axioms introduced by Ehrenfeucht and Rozenberg for elementary transition systems. By Hrushovski's theorem [14] (see also [12]) we already know that any finite reversible automaton has a finite extension and the use of Hall's theorem in order to prove the existence of this finite extension is taken from the proof of Hrushovski's theorem given by Lascar and Herwig [13].

Proposition 4 *Every reversible automaton $A = (S, E, T, s_0)$ has an extension $A' = (E, S', T', s'_0)$ with the same fundamental group: $\pi_1(A') = \pi_1(A)$. If A is finite it has a finite extension. Up to isomorphism the extensions of a connected reversible automaton A are in bijective correspondance with the subgroups H of $F(E)$ such that $\pi_1(A) \subseteq H$ and $H \cap \Delta(A, U) = \emptyset$ where U is some spanning tree of A. The extension associated with H is $A_H = S(F(E), H, E)$ with full embedding $S \hookrightarrow H\backslash F(E) \ : \ s \mapsto Hu$ where $s_0 * u = s$. A can be fully embedded in a Cayley graph if and only if $N(\pi_1(A)) \cap \Delta(A, U) = \emptyset$ where $N(\pi_1(A))$ is the normaliser of the fundamental group in $F(E)$. Such a Cayley graph is then $C(G, E)$ where G is the group with presentation $G = \mathbf{gp}(E, B)$ where $B = \{c_t \mid t \in T \setminus U\}$ is the base of $\pi_1(A)$ derived from some spanning tree U of A.*

Proof: We have a partial right action of $F(E)$ on the product $S \times F(E)$ given by $(s, u) \bullet w = (s * w, w^{-1}u)$. We define a complete reversible automaton $A = (E, S', T, s'_0)$ by letting S' be the set of orbits $[s, u]$ of $(s, u) \in S \times F(E)$ under this action, the set of transition T' is given by $[s, u] * e = [s, ue]$, and the initial state is $s'_0 = [s_0, 1]$. the map $j : S \to S' : s \mapsto [s, 1]$ is injective because $[s, 1] = [s', 1] \Leftrightarrow (\exists w \in F(E) \quad s' = s * w \ \wedge \ 1 = w) \Rightarrow s' = s$. Now $s \xrightarrow{e} s' \Rightarrow [s, 1] * e = [s, e] = [s * e, 1]$ i.e. $[s, 1] \xrightarrow{e} [s', 1]$. Conversely if $[s, 1] \xrightarrow{e} [s', 1]$, i.e. $[s', 1] = [s, e]$ then there exists $w \in F(E)$ such that $s = s' * w$ and $1 = ew$. Since w is a reduced word, this word should start by, and in fact be reduced to, the letter $\overline{e}$, and thus $s \xrightarrow{e} s'$. Therefore A' is an extension of A termed the *canonical* extension of A. Generally the canonical extension is not finite even for finite A. Its fundamental group $\pi_1(A')$ is the set of reduced words u such that $[s_0, 1] * u = [s_0, u] = [s_0, 1]$, then there exists $w \in F(E)$

such that $s_0 = s_0 * w$ (i.e. $w \in \pi_1(A)$) and $1 = w \cdot u$ (i.e. $w = u^{-1}$); thus $\pi_1(A') = \pi_1(A)$.

Let H be a subgroup of $F(E)$ such that $\pi_1(A) \subseteq H$ and $H \cap \Delta(A,U) = \emptyset$, then the map $\rho : S \to H\backslash F(E) \ : s \mapsto Hu$ where $s_0 * u = s$ is well defined because $\pi_1(A) \subseteq H$ and injective because $H \cap D(A,U) = \emptyset$. If $s \xrightarrow{e} s'$ then $u_s \cdot e \cdot u_{s'}^{-1} \in H$ because $\pi_1(A) \subseteq H$; hence $\rho(s) \xrightarrow{e} \rho(s')$ in $S(F(E),H,E)$. Conversely assume that $\rho(s) \xrightarrow{e} \rho(s')$ in $S(F(E),H,E)$, i.e. $u_s \cdot e \cdot u_{s'}^{-1} \in H$, then $s \xrightarrow{e} s''$ for some state $s'' \in S$ since $H \cap \Delta(A,U) = \emptyset$. Then necessarily $s'' = s'$ by determinacy of $A_H = S(F(E),H,E)$ and injectivity of ρ. Therefore $\rho : A \to A_H$ is an extension of A.

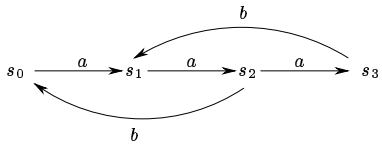
Since every connected complete reversible automaton is isomorphic to a Schreier graph $S(F(E),H,E)$ for H some subgroup of the free group $F(E)$, any extension of A is a morphism of the form $\rho : A \to S(F(E),H,E)$. Thus $\rho(s) = Hvu$ where $\rho(s_0) = Hv$ and $s_0 * u = s$. It follows that $u \cdot u'^{-1} \in \pi_1(A) \Rightarrow Hvu = Hvu' \Leftrightarrow vuu'^{-1}v^{-1} \in H$ i.e. $\pi_1(A) \subseteq v^{-1}Hv$. Now since ρ is injective $s \neq s' \Rightarrow Hvu_s \neq Hvu_{s'} \Leftrightarrow vu_su_{s'}^{-1} \notin H$, thus $v^{-1}Hv \cap \{u_s \cdot u_{s'}^{-1} \mid \forall s, s' \in S \quad s \neq s'\} = \emptyset$. Now $s \not\xrightarrow{e} s' \Rightarrow Hvu_se \neq Hvu_{s'} \Leftrightarrow vu_seu_{s'}^{-1}v^{-1} \notin H \Leftrightarrow u_seu_{s'}^{-1} \notin v^{-1}Hv$. Altogether $H' = v^{-1}Hv$ satisfies $\pi_1(A) \subseteq H'$ and $H' \cap \Delta(A,U) = \emptyset$ and we have an extension $\rho' : A \to S(F(E),H',E) \ : s \mapsto H'u$. Now ρ is the composition of ρ' with the isomorphism $S(F(E),H',E) \xrightarrow{\sim} S(F(E),H,E) \ : H'u \mapsto Hvu$.

If A is finite, $\pi_1(A)$ is a finitely generated subgroup of the free group $F(E)$ and by Hall's theorem $\pi_1(A)$ is the intersection of all the subgroup H of $F(E)$ of finite index such that $\pi_1(A) \subseteq H$. Since a finite intersection of subgroups of finite index is a subgroup of finite index and $\Delta(A,U)$ is finite, we deduce that A has a finite extension.

Finally $S(F(E),H,E)$ is isomorphic to a Cayley graph if and only if H is a normal subgroup of $F(E)$, in which case $S(F(E),H,E) \cong C(G,E)$ where G is the group presented by $G = \mathbf{gp}(E;K)$ where K is a set of generators of H. Now $\pi_1(A) \subseteq H \lhd F(E)$ and $H \cap \Delta(A,U) = \emptyset$ implies that $\Delta(A,U) \cap N(\pi_1(A)) = \emptyset$. Conversely if $\Delta(A,U) \cap N(\pi_1(A)) = \emptyset$ then A fully embeds in the Cayley graph $A_{N(\pi_1(A))} = S(F(E),N(\pi_1(A)),E) \cong C(G,E)$ where $G = \mathrm{gp}(E;B)$ with $B = \{c_t \mid t \in T \setminus U\}$ the base of $\pi_1(A)$ derived from some spanning tree U of A. ∎

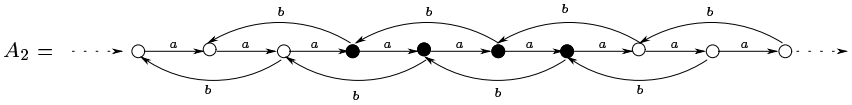
Corollary 5 $\pi_1(A) \cap \Delta(A, U) = \emptyset$.

Let A_1 be the following reversible automaton



Its fundamental group $\pi_1(A_1)$ is the subgroup of $F(E)$ generated by the elements aab and $aaaba^{-1}$ the normal closure of which is the group generated by the elements $uaabu^{-1}$ for $u \in F(E)$. Thus

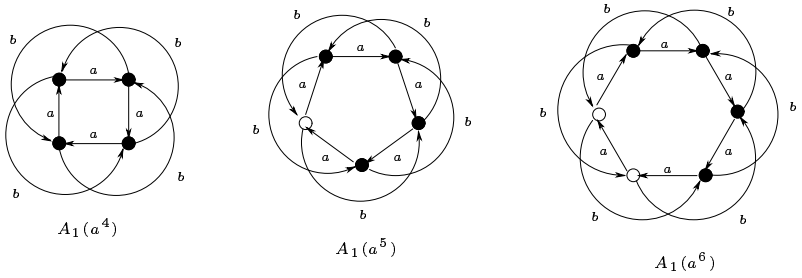
$$F(E)/N(\pi_1(A_1)) = \mathbf{gp}(\{a; b\}; aab) \cong \mathbb{Z}$$



If U is the spanning tree of A, consisting of the a-labelled transitions,

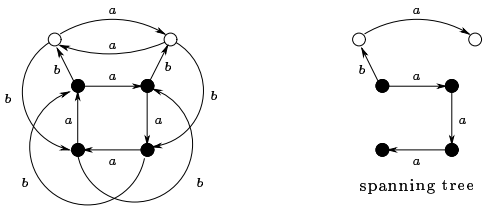
$$\Delta(A_1, U) = \{a; a^2; a^3; a^4; ab; aba^{-1}; aba^{-2}; aba^{-3}; b; ba^{-1}; ba^{-2}; ba^{-3}\}$$

$\Delta(A_1, U) \cap N(\pi_1(A_1)) = \emptyset$ because none of the elements of $\Delta(A_1, U)$ maps to $0 \in \mathbb{Z}$. Thus the cayley graph A_2 is an extension of A_1. If $X \subseteq F(E)$, we let $A_1(X)$ denote the automaton $S(F(E), H(X), E)$ where $H(X)$ is the normal closure of the subgroup of $F(E)$ generated by a^2b and the words in X. Then $A_1(a^6)$ is a finite extension of A_1.



$A_1(a^4)$ is not an extension of A_1 because $a^4 \in \Delta(A_1, U)$ which corresponds to the adjunction of the extra transition $s_3 \xrightarrow{a} s_0$. Similarly $A_1(a^5)$ is not an

extension of A_1 because $ba^{-3} = [a^{-2} \cdot (a^2b) \cdot a^2] \cdot a^{-5} \in \Delta(A_1, U) \cap H(a^5)$, which corresponds to the adjunction of the transition $s_0 \xrightarrow{b} s_3$. Let A_3 the automaton obtained by adding the transition $s_3 \xrightarrow{a} s_0$ to A_1, then $\pi_1(A_3)$ is the subgroup of $F(E)$ generated by the elements aab, $aaaba^{-1}$ and a^4, and $\Delta(A_3, U) = \Delta(A_1, U) \setminus \{a^4\}$. A_3 does not fully embed in $S(F(E), N(\pi_1(A_3), E) = A_1(a^4)$ because of the two extra transitions $s_1 \xrightarrow{b} s_3$ and $s_0 \xrightarrow{b} s_2$ which correspond respectively to the elements $aba^{-3} = a^{-1} \cdot (a^2b \cdot a^{-4}) \cdot a$ and $ba^{-2} = a^2 \cdot (a^{-4} \cdot a^2b) \cdot a^{-2}$ of $N(\pi_1(A_3)) \cap \Delta(A_3, U)$. Thus A_3 has no extension which is a Cayley graph. A finite extension of A_3 is the following:



It corresponds to the group H_3 generated by a^4, a^2b, a^3ba^{-1}, ba^2b^{-1}, $aba^{-1}b^{-1}$, b^2a^{-3}, and ab^2a^{-2} (associated with the chords of the spanning tree indicated in the figure).

3.2 Parikh Automata

The *Parikh mapping* is the (unique) morphism of groups $\psi : F(E) \to \mathbb{Z}^E$ such that $\pi(e)(e') = 1 \quad \text{if } e = e' \text{ else } 0$. We write elements of the free abelian group as formal sums: $V = \sum V(e) \cdot e$, so that for instance $\psi(aba^{-2}) = -a + b$ and $\psi(ab^{-1}a^2b^2a) = 4a + b$. We term *commutative image* of an element $u \in F(E)$ or of a set $L \subseteq F(E)$ their respective images by the Parikh mapping, i.e. the vector $\psi(u) \in \mathbb{Z}^E$ and set of vectors $\psi(L) \subseteq \mathbb{Z}^E$ respectively. We let $V_A = \psi(L_A)$ denote the commutative image of the language of A.

Recall that the abelianization of a group G is the quotient of G by its commutator group $[G, G] = \{aba^{-1}b^{-1} | a, b \in G\}$. It is indeed an abelian group and the canonical projection $G \to G/[G, G]$ is universal among the morphisms $G \to A$ where A is abelian. If $G \subseteq F(E)$ is a subgroup of a free group its abelianization is isomorphic to its commutative image $\psi(G)$ which is a subgroup of $\mathbb{Z}^E$. Moreover if G is the subgroup of $F(E)$ generated by words $u_1, \ldots, u_n$

then $\psi(G)$ is the subgroup of $\mathbb{Z}^E$ generated by the vectors $\psi(u_1), \ldots, \psi(u_n)$; i.e. $\psi(G) = \{\sum_{i=1}^{n} \lambda_i \psi(u_i) | \lambda_i \in \mathbb{Z}\}$. The *first homology group* $H_1(A)$ of a reversible automaton is the abelianization $\psi(\pi_1(A))$ of its fundamental group. It therefore consists of the commutative images of the closed paths based on its initial state. But since the underlying graph is connected the initial state does not matter and the first homology group thus contains the commutative images of all closed paths. Notice that $V_A = \bigcup_{s \in S} \psi(u_s) + H_1(A)$. A *Parikh automaton* is a reversible automaton in which any two co-initial paths with the same Parikh image leads to the same state: $\forall u, v \in F(E) \quad \forall s, s_1, s_2 \in S \quad (s_1 = s * u \ \wedge \ s_2 = s * v \ \wedge \ \psi(u) = \psi(v)) \Rightarrow s_1 = s_2$.

Proposition 6 *The following three conditions are equivalent*

$$\begin{array}{ll} (i) & [s \xrightarrow{u} s' \ \wedge \ u \in H_1(A)] \Rightarrow s = s' \\ (ii) & H_1(A) \cap \{\psi(u_s) - \psi(u_{s'}) \mid \forall s, s' \in S \quad s \neq s'\} = \emptyset \\ (iii) & A \text{ is a Parikh automaton} \end{array}$$

Proof:

- $(i) \Rightarrow (ii)$: Let $s, s' \in S$ such that $\psi(u_s) - \psi(u_{s'}) \in H_1(A)$, then $s \xrightarrow{u} s'$ with $u = u_s^{-1} \cdot u_{s'}$, whence $\psi(u) \in H_1(A)$ and $s = s'$.
- $(ii) \Rightarrow (iii)$: Let $s \xrightarrow{u_1} s_1$ and $s \xrightarrow{u_2} s_2$ with $\psi(u_1) = \psi(u_2)$, then $u_{s_1} \cdot u_1^{-1} \cdot u_2 \cdot u_{s_2}^{-1} \in \pi_1(A)$ hence $\psi(u_{s_1}) - \psi(u_1) + \psi(u_2) - \psi(u_{s_2}) = \psi(u_{s_1}) - \psi(u_{s_2}) \in H_1(A)$ and $s_1 = s_2$.
- $(iii) \Rightarrow (i)$: Let $s \xrightarrow{u} s'$ with $u \in H_1(A)$ i.e. $\exists v \in \pi_1(A) \quad \psi(u) = \psi(v)$. Thus $s_0 \xrightarrow{\mathrm{U}} s$ and $s_0 \xrightarrow{\mathrm{V}} s'$ with $\mathrm{U} = v \cdot u_s$ and $\mathrm{V} = u_s \cdot u$. Now $\psi(\mathrm{U}) = \psi(v) + \psi(u_s) = \psi(u) + \psi(u_s) = \psi(\mathrm{V})$ proving that $s = s'$.

∎

A Parikh automaton is termed *free* or *unfolded* if the converse implication holds: $\forall u, v \in F(E) \quad \forall s \in S \quad s * u = s * v \Rightarrow \psi(u) = \psi(v)$. A language $L \subseteq F(E)$ is termed a *Parikh language* if the Parikh equivalence is coarser than its Nerode equivalence: $\forall u, v \in L \quad \psi(u) = \psi(v) \Rightarrow [\forall w \in F(E) \quad uw \in L \Leftrightarrow vw \in L]$. Recall that the Nerode group $N_L = \{u \in F(E) \mid u^{-1}L = L\}$ is the maximal subgroup of $F(E)$ saturating $L \subseteq F(E)$ and thus corresponds to the minimal automaton (w.r.t. the covering relation) recognizing L.

Proposition 7 *A reversible automaton is a Parikh automaton if and only if its right congruence is finer than the Parikh equivalence:* $\psi_{L(A)} \subseteq \pi_1(A)$ *where* $\psi_L = \{vu^{-1} \mid u, v \in L, \quad \psi(u) = \psi(v)\}$. *A reversible automaton is a free Parikh automaton if and only if* $\psi_{L(A)} = \pi_1(A)$. *Thus any quotient of a Parikh automaton is a Parikh automaton. A language* $L \subseteq F(E)$ *is a Parikh language if and only if the minimal automaton recognizing* L *is a Parikh automaton (i.e. equivalently if it is the language of some Parikh automaton). If* L *is a Parikh language, then* $\psi_L = ker(\psi) \cap N_L$ *and it is a normal subgroup of* N_L. *More generally the fundamental group of any Parikh automaton is a normal subgroup of* $N_{L(A)}$. *The set of Parikh automata recognizing a (Parikh) language* $L \subseteq F(E)$ *is anti-isomorphic to the lattice of the subgroups* H *of* $F(E)$ *such that* $\psi_L \subseteq H \subseteq N_L$.

Let A be a Parikh automaton and let u and v be words in $L(A)$ such that $\psi(u) = \psi(v)$, then $s_0 * u = s_0 * v$ i.e. $uv^{-1} \in \pi_1(A)$. Conversely assume $\psi_L(A) \subseteq \pi_1(A)$ and let $s \xrightarrow{u} s_1$ and $s \xrightarrow{v} s_2$ where $\psi(u) = \psi(v)$. Let $\mathrm{U} = u_s \cdot u$ and $\mathrm{V} = u_s \cdot v$ where u_s is some word such that $s_0 \xrightarrow{u_s} s$. U and V are words of $L(A)$ which are Parikh equivalent and thus $\mathrm{V}\mathrm{U}^{-1} = u_s v u^{-1} u_s^{-1} \in \pi_1(A)$ from which it follows $vu^{-1} \in \pi_1(T, s)$ hence $s \xrightarrow{u} s * v = s_2$ and thus $s_1 = s_2$ by determinacy. Therefore a reversible automaton is a Parikh automaton if and only if $\psi_{L(A)} \subseteq \pi_1(A)$. If A is a free automaton, then $u \in \pi_1(A)$ i.e. $s_0 * u = s_0$ entails $\psi(u) = 0$ and thus the converse implication holds. Conversely suppose $\psi_{L(A)} = \pi_1(A)$ and let $u, v \in F(E)$ and $s \in S$ such that $s * u = s * v$ this means $u_s u v^{-1} u_s^{-1} \in \pi_1(A) = \psi_{L(A)}$ where u_s is some word such that $s_0 \xrightarrow{u_s} s$, in particular $\pi(u_s u v^{-1} u_s^{-1}) = \pi(uv^{-1}) = 0$ and thus $\psi(u) = \psi(v)$ which shows that A is a free Parikh automaton. We recall that B is a quotient of A if and only if $\pi_1(A) \subseteq \pi_1(B)$ thus B is a Parikh automaton if A is.

The minimal automaton recognizing a language $L \subseteq F(E)$ is a Parikh automaton if and only if $\psi_L \subseteq N_L$ i.e. $\{vu^{-1} \mid u, v \in L \quad \psi(u) = \psi(v)\} \subseteq \{u \mid u^{-1}L = L\}$ which is equivalent to $\forall u, v \in L \quad \psi(u) = \psi(v) \Rightarrow u^{-1}L = v^{-1}L$ i.e. L is a Parikh language.

By definition of ψ_L one has $ker(\psi) \cap L \subseteq \psi_L \subseteq ker(\psi)$ for every language $L \subseteq F(E)$. If L is a Parikh language $u, v \in L$ and $\psi(u) = \psi(v)$ entails $vu^{-1} \in L$ (because $uu^{-1} = 1 \in L$) and thus $\psi_L = ker(\psi) \cap L$ in that case. If L is a Parikh language we have $\psi_L \subseteq ker(\psi) \cap N_L$, now $N_L \subseteq L$ and thus $ker(\psi) \cap N_L \subseteq ker(\psi) \cap L = \psi_L$ showing the converse implication. Therefore ψ_L

is a subgroup of N_L. Let $u \in N_L$ and $v \in \psi_L$, then $uvu^{-1} \in ker(\psi) \cap N_L = \psi_L$ and thus ψ_L is a normal subgroup of N_L. More generally the fundamental group of a Parikh automaton A is a normal subgroup of $N_{L(A)}$: let $v \in \pi_1(A)$ and $u \in N_{L(A)}$, $(u \in N_{L(A)} \wedge v \in L(A)) \Rightarrow uv \in L(A)$, since $\psi(uv) = \psi(vu)$ we deduce $s_0 * uv = s_0 * vu = s_0 * u$ and thus $uvu^{-1} \in \pi_1(A)$ as required.

The set of Parikh automata recognizing a (Parikh) language $L \subseteq F(E)$ is thus a lattice anti-isomorphic to the lattice of the subgroups H of $F(E)$ such that $\psi_L \subseteq H \subseteq N_L$ where $\psi_L = ker(\pi) \cap L$ and $N_L = \{u \in F(E) \mid u^{-1}L = L\}$. ∎

Thus any Parikh automaton is a regular quotient of a free Parikh automaton and any quotient of a Parikh automaton is a regular quotient.

3.3 Commutative Automata

Definition 8 *A reversible automaton A is a commutative automaton if and only if it satisfies the two following conditions:*

1. $\forall s, s' \in S \quad \forall u \in F(E) \qquad [s \xrightarrow{u} s' \ \wedge \ \psi(u) \in H_1(A)] \Rightarrow s = s'$
2. $\forall s, s' \in S \quad \forall u \in F(E) \quad \forall e \in E \qquad [s \xrightarrow{u} s' \ \wedge \ \psi(u) = e] \Rightarrow s \xrightarrow{e} s'$

Proposition 9 *A reversible automaton is a commutative automaton if and only if*

1. $\forall s, s' \in S \qquad \psi(u_s) - \psi(u_{s'}) \in H_1(A) \Rightarrow s = s'.$
2. $\forall s, s' \in S \quad \forall e \in E \qquad \psi(u_s) - \psi(u_{s'}) + e \in H_1(A) \Rightarrow s \xrightarrow{e} s'.$

where u_s is the unique path from s_0 to s in some fixed spanning tree U.

Proof: The equivalence of condition (1) in Prop. 9 and condition (1) in Def. 8 was proved in Prop. 6. Let us now prove that if A is a Parikh automaton condition (2) in Prop. 9 and condition (2) in Def. 8 are equivalent. For the one direction, suppose that condition (2) in Def. 8 holds and let $s, s' \in S$ such that $\psi(u_s) + e - \psi(u_{s'}) \in H_1(A)$, i.e. $\psi(u_s) + e - \psi(u_{s'}) = \psi(v)$ for some $v \in \pi_1(A)$. Thus $s \xrightarrow{\mathrm{U}} s'$ with $\mathrm{U} = u_s^{-1} \cdot v \cdot u_{s'}$. Now $\psi(\mathrm{U}) = e$ which implies $s \xrightarrow{e} s'$. Conversely assume that condition (2) in Prop. 9 holds and let $s \xrightarrow{u} s'$ with $\psi(u) = e$, then

$v = u_s \cdot u \cdot u_{s'}^{-1} \in \pi_1(A)$, therefore $\psi(u_s) + e - \psi(u_{s'}) \in H_1(A)$ which implies $s \xrightarrow{e} s''$ for some $s'' \in S$. Now $s' \xrightarrow{\mathrm{U}} s''$ with $\mathrm{U}{=}u^{-1} \cdot e$ entails $s' = s''$ because $\psi(\mathrm{U}) = 0$. ∎

We say that a reversible automaton A divises a reversible automaton B if there exists some reversible automaton C that covers A and fully embedds in B; in notation $A|B \Leftrightarrow \exists C \quad A \leq C \hookrightarrow B$. For instance state graphs of vector addition systems divise the Cayley graph of $\mathbb{Z}^E$.

Proposition 10 *Let $A = (E, S, T, s_0)$ be a reversible automaton, then the following conditions are equivalent:*

1. *A is a commutative automaton,*
2. *A divides the Cayley graph of $\mathbb{Z}^E$,*
3. *A fully embeds in a Cayley graph of a finitely generated abelian group.*

Commutative automata with set of events E are in bijective correspondance with the pairs (V, H) where $V \subseteq \mathbb{Z}^E$ is a connected set of vectors and H is a subgroup of the group $I(V)$ of invariants of V: $H \subseteq I(V) = \{u \in \mathbb{Z}^E \mid u+V = V\}$. H is then the first homology group and V the commutative image of the language of the associated commutative automaton. A commutative automaton is reduced if and only if its first homology group coincides with its group of invariants.

Proof: The fact that the reversible automaton A fully embeds in the Cayley graph of an abelian group means that it has a normal extension with an abelian factor group ; i.e. there exists a normal subgroup H of $F(E)$ such that $H \cap \Delta(A, U) = \emptyset$ for U a fixed spanning tree of A, and $\forall a, b \in E \quad [a, b] = aba^{-1}b^{-1} \in H$. Now since $ker(\psi) \subseteq H$, the map $Hu \mapsto K\psi(u)$ defines an isomorphism $F(E)/H \cong \mathbb{Z}^E/K$ where $K = \psi(H)$. Under the assumption that $ker(\psi) \subseteq H$ one has $H = \psi^{-1}(K)$ and the condition $H \cap \Delta(A, U) = \emptyset$ is equivalent to $K \cap \Lambda(A, U) = \emptyset$ where $\Lambda(A, U) = \psi(\Delta(A, U)) = \{\psi(u_s) - \psi(u_{s'}) \mid \forall s, s' \in S \quad s \neq s'\} \cup \{\psi(u_s) + e - \psi(u_{s'}) \mid \forall s, s' \in S \quad s \overset{e}{\not\to} s'\}$. Therefore A fully embeds in the Cayley graph of an abelian group if and only if $H_1(A) \cap \Lambda(A, u) = \emptyset$. This condition corresponds by Prop. 6 to the conjunction of the two following conditions:

1. $s \xrightarrow{u} s' \ \wedge \ u \in H_1(A) \Rightarrow s = s'$,
2. $s \xrightarrow{u} s' \wedge \ \pi(u) = e \Rightarrow s \xrightarrow{e} s'$

which in turn expresses by Prop. 9 that A is a commutative automaton. Thus a reversible automaton embeds in the Cayley graph of an abelian group if and only if it is a commutative automaton.

Suppose that A is a commutative automaton. Let $\alpha : T \to H_1(A)$ be the regular voltage assignment given by $\alpha(t) = 0$ if $t \in U$ and $\alpha(t) = \psi(u_t)$ if $t \notin U$ where $u_t = u_s \cdot e \cdot u_{s'}^{-1} \in \pi_1(A)$ is the fundamental closed path associated with the chord $t = s \xrightarrow{e} s'$. We term the derived automaton A^α the *Parikh unfolding* of A. We recall that the derived automaton A^α is the Galois covering of A whose states are the pairs $(s, x) \in S \times H_1(A)$ (with initial state (s_0, ϵ)) and whose transitions are given by $(s, x) \xrightarrow{e} (s', x') \Leftrightarrow t = s \xrightarrow{e} s' \in T \wedge x' = x + \alpha(t)$. The map Ψ that takes $(s, x) \in \tilde{S}$ to $\psi(u_s) + x \in \mathbb{Z}^E$ is a morphism of transition system from $\tilde{A}$ to the Cayley graph of $\mathbb{Z}^E$. Indeed, since $u_{s'} = u_s \cdot e$ if $t = s \xrightarrow{e} s' \in U$ and $u_{s'} = u_s \cdot e \cdot u_t$ if $t \notin U$ it follows that $\psi(u_s) + e - \psi(u_{s'}) = \alpha(t)$ and then $(s, x) \xrightarrow{e} (s', x')$ implies $\Psi(s', x') = \Psi(s, x) + e$.

Let us prove that Ψ is a full embedding if and only if A is a commutative automaton. First we prove that Ψ is injective if and only if *(i)* $\psi(u_s) - \psi(u_{s'}) \in H_1(A) \Rightarrow s = s'$. $\Psi(s, x) = \Psi(s', x')$ is equivalent to $\psi(u_s) - \psi(u_{s'}) = x' - x$, thus if Condition *(i)* is satisfied $\Psi(s, x) = \Psi(s', x')$ entails $s = s'$ and therefore also $x = x'$. Conversely, assume that Condition *(i)* does not hold, i.e. there exist distinct states s and s' such that $y = \psi(u_s) - \psi(u_{s'}) \in H_1(A)$, then $\Psi(s, 1) = \Psi(s', y)$ which shows that Ψ is not injective. Second we prove that Condition *(ii)* : $\psi(u_s) - \psi(u_{s'}) + e \in H_1(A) \Rightarrow s \xrightarrow{e} s'$ is equivalent to Condition *(ii)'* :$\Psi(s', x') = \Psi(s, x) + e \Rightarrow (s, x) \xrightarrow{e} (s', x')$. For the one direction, let us assume Condition *(ii)* and $\Psi(s', x') = \Psi(s, x)$, then $\psi(u_s) - \psi(u_{s'}) + e = x' - x \in H_1(A)$ and therefore $s \xrightarrow{e} s'$. Now $x' = \psi(u_s) + e - \pi(u_{s'}) = x + \alpha_t$ where $t = s \xrightarrow{e} s'$ and then $(s, x) \xrightarrow{e} (s', x')$. Conversely, assume that Condition *(ii)* does not hold, i.e. there exists s, s' and e such that $y = \psi(u_s) - \psi(u_{s'}) + e \in H_1(A)$ and $s \overset{e}{\not\to} s'$. Then $\Psi(s, 1) + e = \Psi(s', y)$ and if Condition *(ii)'* were to hold we would have $(s, 1) \xrightarrow{e} (s', y)$ and thus in particular $s \xrightarrow{e} s'$ which leads to a contradiction.

Let A and B be reversible automata such that $A \leq B \hookrightarrow C(\mathbb{Z}^E, E)$. The states of B corresponds (via the embedding) to the vectors V_A. Thus any such

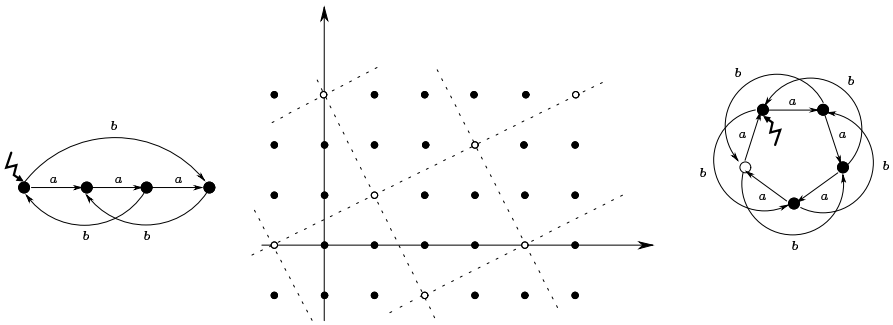


Figure 1: a commutative automaton

automaton B is uniquely determined up to isomorphism hence is isomorphic to the Parikh unfolding of A. This shows that the first two conditions of the proposition are equivalent. Moreover $B \cong \tilde{A} \to A$ is a Galois covering with Galois group $H_1(A)$ thus $A \cong \tilde{A}/H_1(A)$ is characterized by the (full) image of $\tilde{S}$ in $\mathbb{Z}^E$ i.e. by the set of vectors V_A and by its Galois group $H_1(A)$. Now $H_1(A) \subseteq \{u \in \mathbb{Z}^E \mid u + V_A = V_A\}$ and the set of reversible automata with a given unfolding ordered by the covering relation is dual-isomorphic to the set of sets of linear invariants of V_A ordered by inclusion. ∎

In fact the conditions in Def. 8 state that the map $s \mapsto \psi(u_s) + H_1(A)$ is a full embedding of the automaton into the Cayley graph of $\mathbb{Z}^E/H_1(A)$. Consider the reversible automaton of Fig. 1, $H_1(A)$ is the group generated by $3a - b$ and $2a + b$, and $V_A = U_A + H_1(A)$ where $U_A = \{0; a; 2a; 3a\}$ (using the set of a-labelled transitions as spanning tree). The embedding of A into the Cayley graph of the group $\mathbb{Z}^E/H_1(A)$ takes a state s to the coset $\psi(u_s) + H_1(A)$; i.e. the orbits of $\psi(u_s)$ in $V_A \subseteq \mathbb{Z}^E$ for the action of $H_1(A)$. Now $H_1(A)$ is also generated by $5a$ and $3a - b$ (because $5a = (3a - b) + (2a + b)$) and thus $\mathbb{Z}^E/H_1(A)$ is isomorphic to the cyclic group $\mathbb{Z}/5\mathbb{Z}$ with a identified to 1 and b to $3 = -2$. The embedding of A into $\mathbb{Z}^E/H_1(A)$ is shown on the right of Fig. 1. We shall term the factor group $\mathcal{C}(A) = \mathbb{Z}^E/H_1(A)$ the *canonical group* of the reversible automaton $A = (E, S, T, s_0)$. The embedding of A into the Cayley graph of $\mathcal{C}(A)$ which takes a state s to the coset $\psi(u_s) + H_1(A)$ and an event e to its coset $e + H_1(A)$ is termed the *canonical representation* of A. We recall that any abelian group $\mathcal{C}(A)$ has an explicit representation

of the form $\mathcal{C}(A) \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^m$ where $1 \leq n_i | n_{i+1}$ and $m \geq 0$. The coefficients n_i and m are characteristic of $\mathcal{C}(A)$ even though the isomorphism may not be uniquely determined. By abuse of notation we shall term *a canonical representation* for A any composition of its canonical representation with such an isomorphism. We describe in the next section how such canonical representations can be explicitely computed using some Smith normalization of a matrix associated with $\mathcal{C}(A)$.

3.4 Canonical Embeddings of a Commutative Automaton

If H is a subgroup of $\mathbb{Z}^n$ and $G = \mathbb{Z}^n/H$ is the factor group then G, as any commutative group, has a canonical decomposition $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^m$ where $1 \leq n_i | n_{i+1}$ and $m \geq 0$. These numbers called respectively the *torsion coefficients* and the *Betti number* are characteristic of G. They can be computed using the Smith normal form of a matrix associated with a presentation of G(see [19] page 140–150). Let us recall some facts about Smith normal forms of integral matrices [20]. Let $M \in \mathbb{Z}^{n,m}$ be a matrix of rank r, the whole numbers $f_0, f_1, \ldots, f_r$, where $f_0 = 1$ and f_k for $1 \leq k \leq r$ is the greatest common divisor of all nonzero determinants of k^{th} order submatrices of M are termed the *determinantal divisors* of M. Then $f_{k-1} | f_k$, the quotients q_k defined by $f_k = q_k f_{k-1}$ are the *invariant factors* of M. Matrix M is equivalent to a matrix S called its *Smith normal form* such that $S(i,i) = q_i$ for $i = 1, \ldots r$ and $S(i,j) = 0$ otherwise; i.e. M is of the form $M = RSC$ where S is in Smith normal form and R and C are elementary matrices corresponding respectively to a sequence of elementary row operations on M (interchanging rows or adding a multiple of a row to another row) and a sequence of elementary column operations on M. The Smith normal form of a matrix M is unique but not the elementary matrices R and C that may depend on the order in which the elementary operations needed to reach the normal form are performed.

Let $G = Ab(E, W)$ denote the group $\mathbb{Z}^E/H$ where H is the subgroup of $\mathbb{Z}^E$ generated by the elements of $W \subseteq \mathbb{Z}^E$. The pair (E, W) can be represented as a matrix, called the *relation matrix* of G, whose columns corresponds to the relators. We then compute the Smith normal form of this matrix. For instance the relation matrix for the group $G = Ab(a, b; 3a - b, 2a + b)$ associated with the

commutative automaton of Fig. 1 is $M = \begin{pmatrix} 3 & 2 \\ -1 & 1 \end{pmatrix}$ and its Smith normal form is computed as follows:

$$\begin{pmatrix} 3 & 2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $R_{i,j}$ and $R_{(i)\leftarrow(i)+c(j)}$ be the matrices the left multiplication by which amounts respectively to exchange rows i and j and to add c times row j to row i. The matrices $C_{i,j}$ and $C_{(i)\leftarrow(i)+c(j)}$ encoding elementary operations on columns are defined similarly. These matrices are nonsingular with inverses $R_{i,j}^{-1} = R_{i,j}$ and $R_{(i)\leftarrow(i)+c(j)}^{-1} = R_{(i)\leftarrow(i)-c(j)}$ (similarly for the C matrices). In the previous exemple

$$R^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$$

and similarly $C^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$; and thus

$$\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Therefore when computing the Smith normal form of a matrix we memorize the sequences of elementary operations performed on the sets of rows and columns from which the matrices R and C and their inverses can be obtained. Now the important property is the following.

Proposition 11 *Let $M \in \mathbb{Z}^{n,m}$ be the relation matrix of a group $G = Ab(E, W)$ (where $E = \{e_1, \ldots, e_n\}$ and $W = \{w_1, \ldots, w_m\}$) and $R \in \mathbb{Z}^{n,n}$ and $C \in \mathbb{Z}^{m,m}$ be respectively elementary row and column matrices. Then $N = RMC$ is the relation matrix of a group $G' = Ab(E', W')$ (where $E' = \{e'_1, \ldots, e'_n\}$ and $W' = \{w'_1, \ldots, w'_m\}$) isomorphic to G. The isomorphism takes the element $\sum_{i=1}^n \lambda_i e_i$ of G to the element $\sum_{i=1}^n \mu_i e'_i$ of G' where $\mu = R\lambda$.*

Let $M = RSC$ be the Smith normalisation of a relation matrix M of a group G, let $d_i = S(i,i)$ if $i \leq m$ and 0 if $i > m$ (this latter case can only occur if $m < n$ which can always be avoided up to the addition of redundant relators). Then by the preceding proposition we have an isomorphism $\varphi : \mathbb{Z}^n/G \to \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_n\mathbb{Z}$ where $\psi(\sum_{i=1}^n \lambda_i e_i + G) = \sum_{i=1}^n (\mu_i \bmod d_i) e'_i$ with $\mu = R^{-1}\lambda$ and $e_i(j) = e'_i(j) = \delta_{i,j}$ (where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise). Notice that if $d = 1$ then the factor group $\mathbb{Z}/d\mathbb{Z}$ is the trivial group and may be omitted from the product and if $d = 0$ then factor group $\mathbb{Z}/d\mathbb{Z}$ is the infinite cyclic group $\mathbb{Z}$. The first k coefficients $d_1, \ldots, d_k$ (maybe $k = 0$) are equal to 1 and corresponds to the linear part that disappears, the last m coefficients are zeros where m is the Betti number, the intermediate values (distinct to 0 and 1) are the torsion coefficients. In our previous example we obtain an isomorphism $G \cong \mathbb{Z}/5\mathbb{Z}$ that takes $\lambda a + \mu b + H_1(A)$ to $\lambda - 2\mu \bmod 5$.

Corollary 12 *Let $\Psi : \mathcal{C}(A) \to \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ be the isomorphism induced from some Smith normalisation of some relation matrix for the canonical group $\mathcal{C}(A) = \mathbb{Z}^E/H_1(A)$ of a reversible automaton A, and let $\lambda(s) = \Psi(\psi(u_s) + H_1(A))$, then the automaton A is commutative if and only if*

1. $\forall s, s' \in S \quad s \neq s' \Rightarrow \lambda(s) \neq \lambda(s')$,
2. $\forall s, s' \in S \;\; \forall e \in E \quad s \overset{e}{\not\to} s' \;\Rightarrow \lambda(s) + \lambda(e) \neq \lambda(s')$.

the embedding λ is then called a canonical representation *of the commutative automaton.*

3.5 Torsion-Free Commutative Automata

A commutative automaton A is termed *torsion-free* if its canonical group $\mathcal{C}(A) = \mathbb{Z}^E/H_1(A)$ is acyclic.

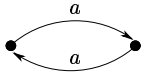
Observation 13 *If $s \xrightarrow{u} s$ is a closed path in a torsion-free commutative automaton whose commutative image is a multiple of some vector $V \in \mathbb{Z}^E$, i.e. $\psi(u) = \ell V$ where $\ell \in \mathbb{N} \setminus \{0\}$, then there exists a closed path $s \xrightarrow{v} s$ in A such that $\psi(v) = V$.*

Proposition 14 *The first homology group of a finite torsion-free commutative automaton coincides with its group of invariants: $H_1(A) = \{u \in \mathbb{Z}^E | u + V_A = V_A\}$.*

Proof: $V_A = U_A + H_1(A)$ where $U_A = \{\psi(u_s) | s \in S\}$ is finite. $H_1(A) + V_A = V_A$ because $H_1(A)$ is a group, and then $H_1(A) \subseteq \{u \in \mathbb{Z}^E | u + V_A = V_A\}$. Conversely let $u \in \mathbb{Z}^E$ such that $u + V_A = V_A$, then $u = u_0 + u'_0$ where $u_0 \in U_A$ and $u'_0 \in H_1(A)$. Suppose that $u_0 \notin H_1(A)$ and consider the sequence $v_n = u + nu_0$ for $n \in \mathbb{N}$. $v_n = u_n + u'_n$ where $u_n \in U_A$ and $u'_n \in H_1(A)$. Since U_A is finite there exists some indices n and m with $n < m$ and $u_n = u_m$, then $v_m - v_n = (m - n)u_0 = u'_m - u'_n \in H_1(A)$ which contradicts the acyclicity of G. Therefore u_0 and thus u are elements of $H_1(A)$. ∎

By Prop. 10, we deduce

Corollary 15 *Any finite torsion-free commutative automaton is reduced.*

Observe that the reversible automaton A= 

which is neither torsion-free nor reduced is such that V_A coincides with its group of linear invariants (isomorphic to $\mathbb{Z}$) while $H_1(A)$ is its subgroup $2\mathbb{Z}$.

Proposition 16 *Let I be a subgroup of $\mathbb{Z}^n$, $G = \mathbb{Z}^n/I$ be the corresponding factor group and $M \in \mathbb{Z}^{n \times k}$ be the matrix whose columns form a basis $u_1, \ldots, u_k$ of I. Then the following conditions are equivalent :*

1. *G is acyclic,*
2. *I is convex,*
3. *the greatest common divisor of the subdeterminants of M of order k is 1,*
4. *for each vector y if My is integral then y is integral.*

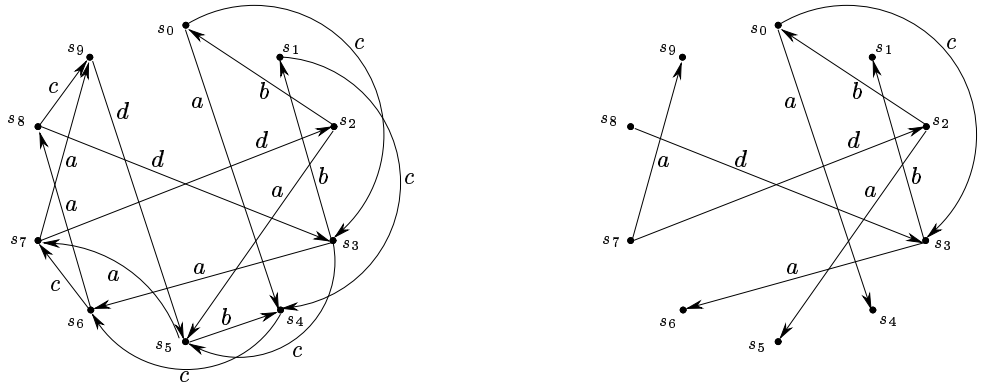


Figure 2: a reversible automaton and one of its spanning tree

Proof: Conditions 1 and 3 are equivalent because the greatest common divisor of the subdeterminants of M is the product of the torsion coefficients. Now $u \in \mathbb{Z}^n$ is a cyclic element of G if and only there exists some positive integer ℓ such that $u \notin I$ whereas $\ell u \in I$, i.e. there exists an integral vector z such that $\ell u = Mz$ (hence $u = M\frac{1}{\ell}z$) and $y = \frac{1}{\ell}z$ is not integral. Thus conditions 1 and 4 are equivalent. Assume now that condition 4 holds and $x \in \mathbb{Z}^n$ belongs to the convex hull of I, then $x = \sum_i \lambda_i My_i$ for some $\lambda_i \in \mathbb{Q}$, $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$ and $y_i \in \mathbb{Z}^k$. Since $x = Mz$ (where $z = \sum_i \lambda_i y_i$) is integral we deduce by condition 4 that z itself is integral and thus $x \in I$ proving that I is convex. Conversely assume that I is convex and My is integral. Without loss of generality we can assume that each y_i is non negative (if not we replace the corresponding vector u_i of the basis by the opposite vector). If $y \neq 0$, let $z = \frac{1}{\sigma}y$ where $\sigma = \sum_i y_i$; $Mz \in I$ because I is convex. Therefore $Mz = Mz'$ for some integral vector z', now $z = z'$ because M is of full column rank and therefore z and $y = \sigma z$ are integral vectors. ∎

3.6 An Example

Let us consider the reversible automaton of Fig. 2. The vectors $\psi_s = \psi(u_s)$ associated with the choice of spanning tree shown on the right of Fig. 2 are

given in the following table.

	ψ_{s_0}	ψ_{s_1}	ψ_{s_2}	ψ_{s_3}	ψ_{s_4}	ψ_{s_5}	ψ_{s_6}	ψ_{s_7}	ψ_{s_8}	ψ_{s_9}
a	0	0	0	0	1	1	1	0	0	1
b	0	1	-1	0	0	-1	0	-1	0	-1
c	0	1	0	1	0	0	1	0	1	0
d	0	0	0	0	0	0	0	-1	-1	-1

The Parikh images of the fundamental cycles are given in the following table.

$t = s \xrightarrow{e} s'$	$\psi_t = \psi(c_t) = \psi_s + e - \psi_{s'}$
$s_1 \xrightarrow{c} s_4$	$-a + b + 2c$
$s_3 \xrightarrow{c} s_5$	$-a + b + 2c$
$s_4 \xrightarrow{c} s_6$	0
$s_5 \xrightarrow{b} s_4$	0
$s_6 \xrightarrow{c} s_7$	$a + b + 2c + d$
$s_6 \xrightarrow{a} s_8$	$2a + d$
$s_8 \xrightarrow{c} s_9$	$-a + b + 2c$
$s_9 \xrightarrow{d} s_5$	0

The relation matrix is therefore $M = \begin{pmatrix} -1 & 1 & 2 \\ 1 & 1 & 0 \\ 2 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ and we compute its Smith normal form:

$$\begin{pmatrix} -1 & 1 & 2 \\ 1 & 1 & 0 \\ 2 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix} = R_{1,4} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \\ 2 & 1 & -1 \end{pmatrix} \cdot C_{1,3}$$

$$= \underbrace{R_{1,4} \cdot R^{-1}_{(4)\leftarrow(4)-2(1)}}_{R_1} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & -1 & -1 \end{pmatrix} \cdot \underbrace{C^{-1}_{(2)\leftarrow(2)-(1)} \cdot C_{1,3}}_{C_1}$$

$$= R_1 \cdot R^{-1}_{(3)\leftarrow(3)-2(2)} \cdot R^{-1}_{(4)\leftarrow(4)+(2)} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot C^{-1}_{(3)\leftarrow(3)-(2)} \cdot C_1$$

And thus

$$R^{-1} = R_{(4)\leftarrow(4)+(2)} \cdot R_{(3)\leftarrow(3)-2(2)} \cdot R_{(4)\leftarrow(4)-2(1)} \cdot R_{1,4}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -2 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 1 & 1 & 0 & -2 \end{pmatrix}$$

The factor of the free abelian group $\mathbb{Z}^E \cong \mathbb{Z}^4$ by the first homology group of A has no torsion coefficient, its Betti number is 2. The canonical projection is

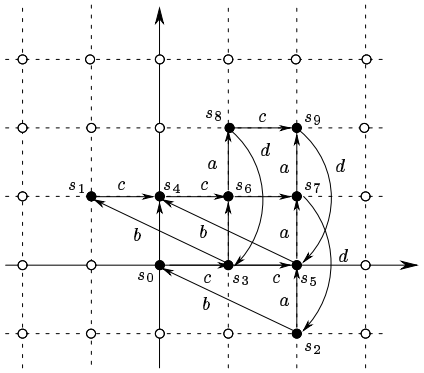


Figure 3: embedding of the automaton of Fig. 2 in $\mathbb{Z}^2$

given by the matrix Λ consisting of the last two rows of matrix R^{-1}:

$$\Lambda = \begin{pmatrix} 0 & -2 & 1 & 0 \\ 1 & 1 & 0 & -2 \end{pmatrix}$$

We introduce two symbols e and f associated with the dimensions of the quotient space, then matrix Λ gives a change of variables from the old alphabet $\{a; b; c; d\}$ to the new one $\{e; f\}$.

Λ	λ_a	λ_b	λ_c	λ_d
e	0	-2	1	0
f	1	1	0	-2

Similarly the states s are represented as $\lambda_s = \Lambda\psi_s$.

	λ_{s_0}	λ_{s_1}	λ_{s_2}	λ_{s_3}	λ_{s_4}	λ_{s_5}	λ_{s_6}	λ_{s_7}	λ_{s_8}	λ_{s_9}
e	2	1	2	1	2	0	1	2	-1	0
f	2	2	1	1	0	1	0	-1	1	0

Every state is represented by a distinct vector and thus λ gives an embedding, shown on Fig. 3, of the automaton in the Cayley graph $C(\mathbb{Z}^2, \{\lambda_e | e \in E\})$. We readily verify that λ is a full embedding as it happens that $\lambda_{s'} = \lambda_s + \lambda_e$ only if $s \xrightarrow{e} s'$.

4 State Graphs of Vector Addition Systems

A place of a vector addition system is a synchronic constraint on the events occurring in the system, namely it constraints the relative frequence of execution of the transitions affecting that place. If the place is bounded its range of variation that is, the difference between its minimum and maximum values, is a measure of the reciprocal independence: higher values mean looser constraints. This is in agreement with the interpretation of a place as abstract resource shared by the transitions connected to that place.

This observation allows us to characterize the state graphs of vector addition systems as the maximal quotients of polyhedral automata. They are commutative automata and we conjecture that they are torsion-free, i.e. that their canonical representation does not contain torsion element. We give an algorithm for the synthesis of vector addition systems which relies on that conjecture.

4.1 Vector Addition Systems

A *vector addition system* [17] is a triple $N = (P, E, \mu)$ consisting of a finite set of *places* $P = \{p_1, \ldots, p_m\}$, a finite set of *events* $E = \{e_1, \ldots, e_n\}$, and a matrix $\mu : P \times E \to \mathbb{Z}$. A *marking* is any vector $M \in \mathbb{N}^m$, and the *state graph* of N is the transition system $N^* \subseteq \mathbb{N}^m \times E \times \mathbb{N}^m$ given by $(M, e, M') \in N^* \Leftrightarrow M' = M + \mu \cdot e$. We often write $M[e>M'$ as an abbreviation for $(M, e, M') \in N^*$, and $M[e>$ when $M[e>M'$ for some M' in which case event e is said to be *enabled* in marking M.

The transition system induced by a reversible transition system $\mathbf{T} = (S, E, T)$ on a subset of states $S' \subseteq S$ is the reversible transition system defined by $\mathbf{T} \restriction S' = (S', E, T \cap (S' \times E \times S'))$.

Observation 17 *The state graph of a vector addition system is the reversible transition system induced by the Cayley graph of a power of $\mathbb{Z}$ on the set of vectors of non negative entries.*

But of course not all induced sub-transition systems of a Cayley Graph of $\mathbb{Z}^n$ are state graphs of vector addition systems. The main purpose of this study is to search for an effective procedure that decides whether a given finite

reversible transition system is an induced sub-transition system of a Cayley Graph of $\mathbb{Z}^n$ and whether it is isomorphic to the state graph of some vector addition system.

If $s \in S$ is some state of a reversible transition system $\mathbf{T} = (S, E, T)$ we let $(\mathbf{T}, s)$ denote the reversible automaton whose transition relation is induced by T on the connected component of s. For instance if M_0 is some marking of a vector addition system $N = (P, E, \mu)$, the reversible automaton (N^*, M_0) will be termed the state graph of the marked vector addition system (P, E, μ, M_0).

4.2 Polyhedral Graphs

State graphs of (marked) vector addition systems are commutative automata. We introduce a class of automata, termed polyhedral, that are their abelian unfoldings.

A $\mathbb{Z}$-polyhedron is a set of vectors of $\mathbb{Z}^n$ defined by a finite set of affine inequalities. All polyhedra that we consider in this document contain the origin and therefore are of the form $\{x \in \mathbb{Z}^n \mid Ax + b \geq 0\}$ for some matrix $A \in \mathbb{Z}^{m,n}$ and vector $b \in \mathbb{N}^m$. Such a polyhedron may be viewed as a reversible transition system, termed a *polyhedral transition system*, whose states are the vectors of the polyhedron, whose events are given by $e_i(j) = 1 \quad \text{if } i = j \quad \text{else } 0$, and whose transition relation $T \subseteq S \times E \times S$ is given by $s \xrightarrow{e} s' \Leftrightarrow s' = s + e$.

A *polyhedral automaton* is a reversible automaton of the form $(\mathbf{T}, 0)$ where $\mathbf{T}$ is a polyhedral transition system, i.e. it is the connected component of the origin in some polyhedron of $\mathbb{Z}^n$. One should pay attention to the fact that polyhedral automaton is not synonymous to connected polyhedral transition system as it may happen, as shown in Fig. 4, that a connected component of the set of integral elements of a convex of $\mathbb{R}^n$ be strictly included in the set of integral elements of its convex hull. We call a *polyhedral graph* the undirected graph associated with a polyhedral transition system, i.e. it is an undirected graph whose vertices are the integral vectors of a polyhedron and such that any two vertices are connected by an edge if and only if their euclidean distance is 1. Thus the above example shows that a connected component of a polyhedral graph may not be a polyhedral graph.

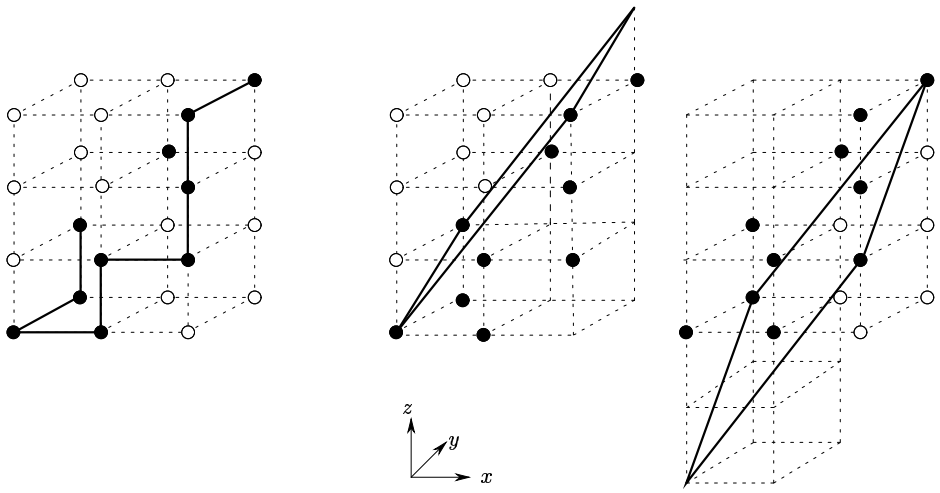


Figure 4: the set X of points of the three dimensional grid indicated by black dots is the set of integral elements of its convex hull K . As shown by the two right-hand side figures, this convex K is the polyhedron obtained by intersecting the paralleliped ($0 \leq x \leq 2$, $0 \leq y \leq 1$, and $0 \leq z \leq 3$) with two half spaces ($3x + 2y - 2z \geq 0$ and $-3x - 4y + 2z + 4 \geq 0$). Now set X has two connected components one of which is an isolated point that belongs to the convex hull of the other one

4.3 Places as Synchronic Constraints

A place $p \in P = \{p_1, \ldots, p_n\}$ of a (marked) vector addition system $N = (P, E, \mu, M_0)$ is a synchronic constraint on the language of N. To make that fact clear, let us recall that $M \xrightarrow{e} M'$, where M and M' are markings and $e \in E$ an event, if and only if $M' = M + \mu \cdot e$; from which it follows that $M \xrightarrow{u} M'$, where M and M' are markings and $u \in F(E)$ is a (reduced) word, if and only if $M' = M + \mu \cdot \psi(v)$ for all prefixes v of u. We can decompose the equation in matrix form $M' = M + \mu \cdot \psi(v)$ into the set of linear equations $M'(p_i) = M(p_i) + \mu_i \cdot \psi(v)$ indexed by places $p_i \in P$. Then $M_0 \xrightarrow{u} M$ for some marking M if and only if all prefixes v of u satisfies the set of linear constraints $\{M_0(p_i) + \mu_i \cdot \psi(v) \geq 0 \mid p_i \in P\}$ i.e. if and only $0 \xrightarrow{u} \psi(u)$ in the polyhedral automaton corresponding to the $\mathbb{Z}$-polyhedron $\{x \in \mathbb{Z}^m \mid \mu \cdot x + M_0 \geq 0\}$, where $E = \{e_1, \ldots, e_m\}$. Conversely each $\mathbb{Z}$-polyhedron presented as $\{x \in \mathbb{Z}^m \mid A \cdot x + b \geq 0\}$ where $A \in \mathbb{Z}^{m,n}$ and $b \in \mathbb{N}^m$ can be viewed as a vector addition system whose places are given by the synchronic constraints $A(i, \cdot) \cdot M + b(i) \geq 0$. To sum up:

a place of a vector addition system	$\equiv$	a synchronic constraint
	$\equiv$	an affine hyperplan

a vector addition system	$\equiv$	a set of synchronic constraints
	$\equiv$	a (presentation of) $\mathbb{Z}$-polyhedron

Now by the previous discussion, the map $x \mapsto \mu \cdot x + M_0$ which takes a vector of the $\mathbb{Z}$-polyhedron $\{x \in \mathbb{Z}^m \mid \mu \cdot x + M_0 \geq 0\}$, associated with the vector addition system $N = (P, E, \mu, M_0)$, to the vector of "distances" of x to each of the hyperplanes bording the polyhedron is a *covering* from the polyhedral automaton to the marking graph of N.

Proposition 18 *A reversible automaton is isomorphic to the state graph of a (marked) vector addition system if and only if it is a reduced commutative automaton the commutative image of whose language is a connected component of a polyhedral graph.*

Proof: Let us prove that the state graph of a vector addition system is a minimal reversible automaton. Suppose by way of contradiction there exists two

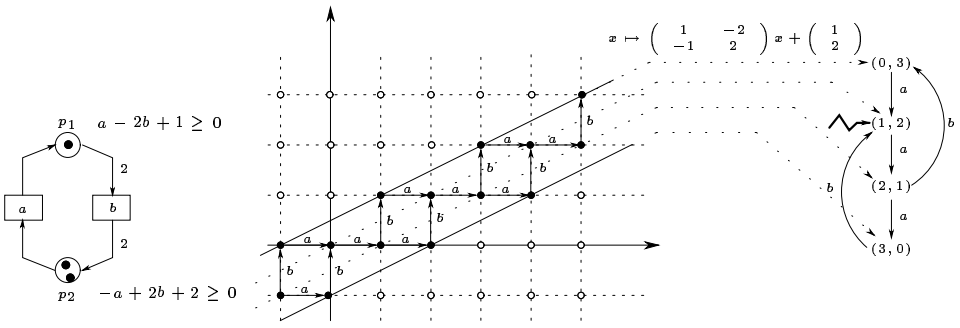


Figure 5: a vector addition system with two events a and b and two places p_1 and p_2 corresponding to the synchronic constraints $a - 2b + 1 \geq 0$ and $-a + 2b + 2 \geq 0$, its marking graph (shown on the right) is a quotient of the corresponding polyhedral automaton.

distinct markings M and M' which are Nerode equivalent: $\forall u \in F(E) \quad M * u \Leftrightarrow M' * u$. Since $M \neq M'$ there exists some place $p \in P$ with $M(p) \neq M'(p)$ e.g. $M(p) > M'(p)$. Let $v \in F(E)$ such that $M * v = M'$, then $\mu(p, \cdot) \cdot \psi(v) = M'(p) - M(p) < 0$. Now since M and M' are Nerode equivalent, we deduce $M * v^n$ for every $n \in \mathbb{N}$ and thus $M(p) + n \cdot (\mu(p, \cdot) \cdot \psi(v)) \geq 0$ for every n, which leads to a contradiction. Conversely if a reversible automaton is the maximal quotient of a polyhedral automaton, then (by unicity of the maximal quotient) it is isomorphic to the state graph of the (marked) vector addition system associated with the polyhedral automaton. ∎

4.4 An Algorithm

By Prop. 9 the state graph of a (marked) vector addition system is then characterized by the commutative image of its language, which is by Prop. 18 a connected component of a polyhedral graph, and its first homology group. If $V \subseteq \mathbb{Z}^n$, let $I(V)$ denote its group of invariants, i.e. $I(V) = \{u \in \mathbb{Z}^n | u + V = V\}$; and let $G(V) = \mathbb{Z}^n / I(V)$ denote the corresponding factor group.

Observation 19 *If V is the set of vertices of a polyhedral graph, then $G(V)$ is acyclic.*

Proof: Let u be a vector and ℓ a positive integer such that $\ell u \in I(V)$, then $V + \ell u = V$ and by convexity of V it follows that $v + u$ and $v - u$ belong to V for every $v \in V$ and thus $u + V = V$ which proves that $u \in I(V)$ and therefore that $G(V)$ is acyclic. ∎

We conjecture that $G(V)$ is also acyclic if V is a connected component of a polyhedral graph, i.e.

Conjecture 20 *State graphs of vector addition systems are torsion-free commutative automaton.*

If A is the marking graph of a vector addition system (P, E, μ, M_0), then $u \in H_1(A)$ if and only if $\mu u = 0$ and there exists a path labelled u. Thus Conjecture 20 may be reformulated as

Conjecture 21 *If there exists a path between two vertices of a polyhedral graph of the form u and $u + \ell v$ where v is an invariant and ℓ is a positive integer, then there exists a path between u and $u + v$.*

Another conjecture (stronger than the previous ones) is the following:

Conjecture 22 *If V is a connected component of a polyhedral graph whose set of vertices $P = \{x \in \mathbb{Z}^n | \mu x + b \geq 0\}$ (where μ and b are a matrix and a vector with integral entries) is the set of integral elements of the convex hull of V, then V and P have the same group of invariants: $I(V) = I(P)$.*

Remark 23 *Since $K(u + V) = u + K(V)$ where $K(V)$ denote the convex hull of V we deduce that $I(V) \subseteq I(P)$ so we only have to prove the converse implication, i.e. $\mu \cdot u = 0 \Rightarrow \exists v_1, v_2 \in V \quad v_2 - v_1 = u$.*

Conjecture 22 implies Conjecture 20: If $u \in \mathbb{Z}^n$ and $\ell \in \mathbb{N}$ are such that $\ell u \in I(V)$, then $\ell u \in I(P)$; by the above remark, $u \in I(P)$ by Obs. 19, and $u \in I(V)$ by Conjecture 22. ∎

Since finite torsion-free commutative automata are reduced a consequence of Conjecture 20 is

Corollary 24 *A finite reversible automaton is isomorphic to the state graph of a vector addition system if and only if it is a torsion-free commutative automaton the commutative image of whose language is a connected component of a polyhedron.*

Proposition 25 *Let $V \subseteq \mathbb{Z}^n$ be a set of vectors with invariants $I = \{u \in \mathbb{Z}^n \mid u + V = V\}$ and $G = \mathbb{Z}^n/I$ be the corresponding factor group.If G is acyclic then V is convex in $\mathbb{Z}^n$ if and only if its image V' is convex in $G \cong \mathbb{Z}^m$; moreover $H \subseteq \mathbb{Z}^n$ is a bounding hyperplane of V if and only if its image $H' \subseteq \mathbb{Z}^m$ is a bounding hyperplane of V'.*

Proof: Let $M = RSC$ be the Smith normalization of the relation matrix M of G associated with a base $u_1, \ldots, u_k$ of I. Suppose that G is acyclic, since M is of full column rank its Smith normal form is $S = \begin{pmatrix} I_k \\ 0_{m,k} \end{pmatrix}$ where I_k is the identity matrix of rank k and $O_{m,k} \in \mathbb{Z}^{m,k}$ is the matrix all of whose entries are null. The canonical projection is given as the composition $\Psi = \mathbb{Z}^n \xrightarrow{\varphi} \mathbb{Z}^{k+m} \xrightarrow{p} \mathbb{Z}^m$ of the isomorphism φ with matrix R^{-1} and of the projection p on the last m components. Since R and R^{-1} are integral matrices and since $\varphi(V)$ is saturated by the projection p (because $V + I = V$) we deduce that if V is convex, i.e. is the set of all integral elements of its convex hull $K(V) \subseteq \mathbb{R}^n$, then the elements of V' are the integral elements of the image of $K(V)$ which is a convex of $\mathbb{R}^m$ hence V' is convex. Similarly if V' is convex then the elements of V are the integral elements of the inverse image of the convex hull of V and thus is also convex.

The last assertion of the proposition holds true for the projection $\mathbb{Z}^n \to \mathbb{Z}^m$, because it holds for each of its components: the former is a bijective linear map while the latter is a projection with respect to which V is saturated. ∎

The matrix $\Lambda \in \mathbb{Z}^{m,n}$ of the projection consists of the last m rows of matrix R^{-1}, the map that takes the hyperplane of $\mathbb{R}^m$ of equation $u_1x_1 + \cdots + u_mx_m + b = 0$ to the hyperplane of $\mathbb{R}^n$ of equation $v_1y_1 + \ldots + v_ny_n + b = 0$ where $v = \Lambda^t u$ gives a bijective correspondance between the respective sets of bounding hyperplanes of V and of its projection.

As we already noticed however, the Parikh image of the language of a vector addition system is not necessarily convex. If $X \subseteq \mathbb{Z}^n$ we let $K(X) \subseteq \mathbb{R}^n$

denotes the convex hull of X (in $\mathbb{R}^n$) and $K_I(X) = K(X) \cap \mathbb{Z}^n$ the set of integral elements of the convex hull of X.

Proposition 26 *Let Ψ be a canonical representation of a torsion-free commutative automaton A, then $K_I(V_A) = \Psi^{-1}(K_I(\Psi(V_A)))$.*

Proof: Let us use the same notation for the representation $\Psi : \mathbb{Z}^n \to \mathbb{Z}^m$ and for its associated linear map $\Psi : \mathbb{R}^n \to \mathbb{R}^m$. We first prove $K(V_A) = \Psi^{-1}(K(\Psi(V_A)))$ (in $\mathbb{R}^m$). Ψ is the composition of an isomorphism and of a projection with respect to which V is saturated, we can then assume without loss of generality that $\Psi : \mathbb{R}^{k+m} \to \mathbb{R}^m$ is the projection on the last m components and that $V_A = \Psi^{-1}(\Psi(V_A)) \cap \mathbb{Z}^n$. By linearity of Ψ we have $\Psi(K(V_A)) = K(\Psi(V_A))$ and then the condition $K(V_A) = \Psi^{-1}(K(\Psi(V_A)))$ is equivalent to the fact that $K(V_A)$ be saturated for the projection, i.e. that $K(V_A) = \Psi^{-1}(\Psi(K(V_A)))$. Let us therefore assume $x \in \mathbb{R}^n$ such that $\Psi(x) = \sum_{i=1}^{\ell} \lambda_i \Psi(x_i)$ where $\lambda_i > 0$, $\sum_{i=1}^{\ell} \lambda_i = 1$ and $x_i \in V_A$. Let $\chi : \mathbb{R}^n = \mathbb{R}^{k+m} \to \mathbb{R}^k$ be the projection on the k first components, and for each $v \in \mathbb{R}^k$ let $\varphi_v : \mathbb{R}^m \to \mathbb{R}^n$ be the section of Ψ, i.e. $\Psi \circ \varphi_v = id$, given by $\varphi_v(u) = (v, u) \in \mathbb{R}^k \times \mathbb{R}^m = \mathbb{R}^n$. Then $x = \sum_{i=1}^{\ell} \lambda_i \varphi_v \Psi(x_i)$ where $v = \chi(x)$ because the right-hand side and the left hand side of this identity are elements of $\mathbb{R}^n$ having the same image by both projection χ and Ψ because $\Psi \circ \varphi_v = id$ and $\Psi(\varphi_v(u)) = v$. Since V_A is saturated by Ψ it follows that $\varphi_v(\Psi(x_i)) \in V_A$ (it is an integral vector) and thus $x \in K(V_A)$ as required.

Since Ψ is the composition of an isomorphism φ and of a projection where both φ and its inverse isomorphism φ^{-1} are represented by a matrix with integral entries, it follows that $\Psi(X \cap \mathbb{Z}^n) = \Psi(X) \cap \mathbb{Z}^m$ for every set $X \subseteq \mathbb{R}^n$ saturated by Ψ. Thus $K_I(V_A) = K(V_A) \cap \mathbb{Z}^n = \Psi^{-1}(\Psi(K(V_A)) \cap \mathbb{Z}^m) = \Psi^{-1}(K(\Psi(V_A)) \cap \mathbb{Z}^m) = \Psi^{-1}(K_I(\Psi(V_A)))$. ∎

If state graph of vector addition systems prove to be torsion-free the following is an algorithm which decides whether a given finite reversible automaton is isomorphic to the marking graph of a vector addition system and which construct such a system when it exists.

1. Choose some spanning tree U of the graph of the automaton $A = (E, S, T, s_0)$. Let u_s denote the (reduced) word labelling the (unique)

path in U from the initial state s_0 to state s, and let $c_t = u_s \cdot e \cdot u_{s'}^{-1}$ be the cycle associated with the chord $t = s \xrightarrow{e} s'$. Compute the commutative images of the chains u_s and of the cycles c_t: let $\psi_s = \psi(u_s)$ and $\psi_t = \psi(c_t)$.

2. Form the relation matrix M associated with the presentation $H_1(A) = Ab(E, \{\pi_t | t \in T \setminus U\})$ of the first homology group of the automaton given by the choice of the spanning tree; i.e. the columns of M are the Parikh images of the fundamental cycles associated with U. Compute the Smith normal form of this relation matrix $M = RSC$ (we recall that matrix R^{-1} is computed along this normalization process).

3. If $G = \mathbb{Z}^E / H_1(A)$ has torsion coefficients (i.e. S contains entries distinct from 0 and 1) then the automaton is not isomorphic to the state graph of a vector addition system else proceed to the following steps.

4. If $n = |E|$ is the size of the alphabet and m is the Betti number of G, let $\Lambda \in \mathbb{Z}^{m,n}$ be the matrix consisting of the last m rows of matrix R^{-1}. The columns of Λ are indexed by the elements of the alphabet, let λ_e denote the column associated with $e \in E$. Compute $\lambda_s = \Lambda \psi_s$.

5. Check that the mapping λ represents the automaton as the subgraph of the Cayley graph $C(\mathbb{Z}^m, \{\lambda_e | e \in E\})$ induced on the subset of nodes $\lambda_S = \{\lambda_s | s \in S\}$. This amounts to verify the following two conditions

   (a) $\forall s, s' \in S \quad s \neq s' \Rightarrow \lambda_s \neq \lambda_{s'}$.

   (b) $\forall s, s' \in S \ \ \forall e \in E \quad s \overset{e}{\not\to} s' \ \Rightarrow \lambda_s + \lambda_e \neq \lambda_{s'}$.

   If one of the above conditions is not satisfied then the automaton is not isomorphic to the state graph of a vector addition system else proceed to the following steps.

6. Compute a polyhedral presentation $\{x \in \mathbb{Z}^m | \ \Pi x + b \geq 0\}$ (with $\Pi \in \mathbb{Z}^{r,m}$ and $b \in \mathbb{N}^m$) of the convex hull of the set λ_S. Its inverse image is the polyhedron $\{y \in \mathbb{Z}^n | \ \Pi \Lambda x + b \geq 0\}$ which is associated with the marked vector addition system $N = (P, E, \mu, M_0)$ with places $P = \{p_1, \ldots, p_r\}$ and such that $\mu(p, e) = p^t \Pi \Lambda e$, and $M_0(p) = p^t b$. Then the automaton A

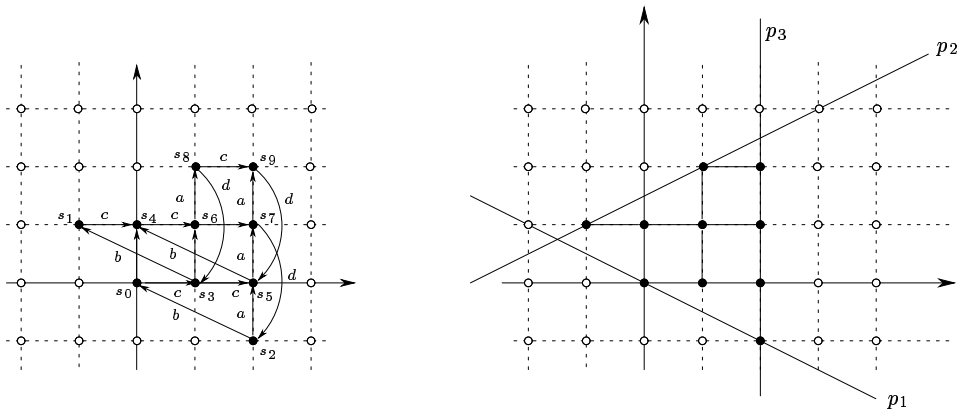


Figure 6: embedding of the automaton of Fig. 2 in $\mathbb{Z}^2$

is isomorphic to the state graph of some vector addition vector systems if and only if it is isomorphic to the state graph of N if and only there is no element $v \in K(\lambda_S) \setminus \lambda_S$ of the form $v = \lambda_s + \lambda_e$ or $v = \lambda_s - \lambda_e$.

Let us consider the commutative automaton of section 3.6, it fully embedds in the Cayley graph of $\mathbb{Z}^2$ as shown on the left of Fig. 6. The image of this embedding is the set of integral points of the polytope delimited by three hyperplanes p_1, p_2 and p_3 as shown on the right of Fig. 6. This polytope is represented by the system

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; \begin{pmatrix} 1 & 2 \\ 1 & -2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

whose inverse image by λ is the polyhedron of $\mathbb{Z}^4$ given by

$$\left\{ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} \in \mathbb{R}^4 \;\middle|\; \begin{pmatrix} 2 & 0 & 1 & -4 \\ -2 & -4 & 1 & 4 \\ 0 & 2 & -1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

Figure 7 gives the associated marked vector addition system together with its state graph.

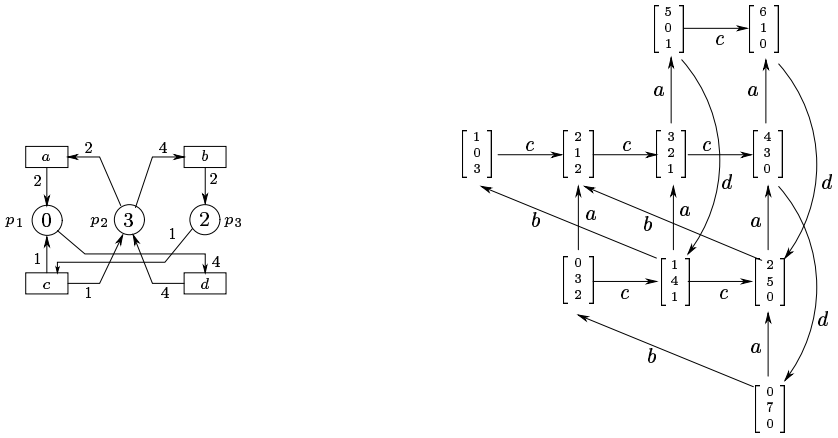


Figure 7: the vector addition system associated with the automaton of Fig. 2 and its state graph

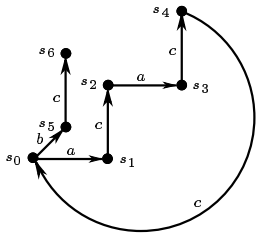


Figure 8: a reversible automaton

Let us now consider the reversible automaton of Fig. 8. The vectors ψ_s associated with the choice of spanning tree obtained by discarding transition $s_4 \stackrel{c}{\to} s_0$ are given in the following table.

	ψ_{s_0}	ψ_{s_1}	ψ_{s_2}	ψ_{s_3}	ψ_{s_4}	ψ_{s_5}	ψ_{s_6}
a	0	1	1	2	2	0	0
b	0	0	0	0	0	1	1
c	0	0	1	1	2	0	1

The fundamental cycle associated with the chord is $2a + 3c$. The Smith normalisation of the relation matrix is

$$\begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix} = R \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

where $R = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 1 \\ 3 & 0 & 1 \end{pmatrix}$ and $R^{-1} = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 3 & 0 & -2 \end{pmatrix}$. The factor of the free abelian group $\mathbb{Z}^E \cong \mathbb{Z}^3$ by the first homology group of A has no torsion coefficient, its Betti number is 2. The canonical projection is given by the matrix Λ consisting of the last two rows of matrix R^{-1}:

$$\Lambda = \begin{pmatrix} 0 & 1 & 0 \\ 3 & 0 & -2 \end{pmatrix}$$

We introduce two symbols e and f associated with the dimensions of the quotient space, then matrix Λ gives a change of variables from the old alphabet $\{a; b; c; d\}$ to the new one $\{e; f\}$.

Λ	λ_a	λ_b	λ_c
e	0	1	0
f	3	0	-2

Similarly the states s are represented as $\lambda_s = \Lambda\psi_s$.

	λ_{s_0}	λ_{s_1}	λ_{s_2}	λ_{s_3}	λ_{s_4}	λ_{s_5}	λ_{s_6}
e	0	0	0	0	0	1	1
f	0	3	1	4	2	0	-2

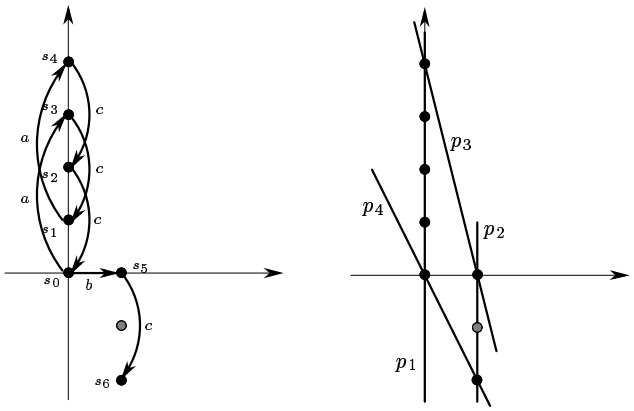


Figure 9: embedding of the automaton of Fig. 8 in $\mathbb{Z}^2$

Every state is represented by a distinct vector and thus λ gives an embedding, shown on the left of Fig. 9, of the automaton in the Cayley graph $C(\mathbb{Z}^2, \{\lambda_e | e \in E\})$. We readily verify that λ is a full embedding as it happens that $\lambda_{s'} = \lambda_s + \lambda_e$ only if $s \xrightarrow{e} s'$. The convex closure of the image of this embedding is a polytope of $\mathbb{Z}^2$ which contains an integral element that is not in the image of the embedding (the grey state in Fig. 9). However this element is not of the form $\lambda_s + \lambda_e$ or $\lambda_s - \lambda_e$ and therefore the automaton of Fig. 8 is isomorphic to the state graph of a vector addition system. For computing such a vector addition system we represent the polytope by the system

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; \begin{pmatrix} 1 & 0 \\ -1 & 0 \\ -4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 4 \\ 0 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

whose inverse image by λ is a polyhedron of $\mathbb{Z}^3$ given by

$$\left\{ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{R}^3 \;\middle|\; \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \\ -3 & -4 & 2 \\ 3 & 2 & -2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 4 \\ 0 \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

Figure 10 gives the associated marked vector addition system together with its state graph.

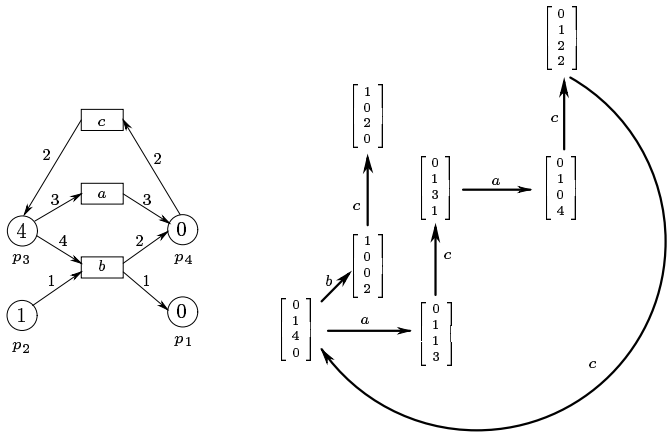


Figure 10: the vector addition system associated with the automaton of Fig. 8 and its state graph

4.5 On the Complexity of the Algorithm

In order to conclude let us give some hints on the complexity of the algorithm. The two costy parts of the algorithm are the computation of the Smith normal form of the relation matrix of the canonical group and the computation of the convex hull of the representation of the state space.

Kannan and Bachem [16] give a polynomial time algorithm for the computation of the Smith normal form of an integer matrix. They indeed prove that both the number of involved algebraic operations and the number of binary digits of all the intermediate numbers are bounded by polynomials in the length of the input data encoded in binary. Another solution is proposed by Rayward-Smith in [22]. Chou and Collins [5] and then Iliopoulos [15] improve the result of Kannan and Bachem by giving an $O(s^5 M(s^2))$ elementary operation algorithm for computing the Smith normal form of an integer matrix where $M(n)$ denotes an upper bound on the number of elementary operations required for the multiplication of two integers of length n bits, and where the size s of an $m \times n$ matrix A is the number $m + n + log\|A\|$ with $\|A\| = max_{i,j}\{|a_{i,j}|\}$.

Computing the convex hull of a finite set of points in an euclidean space is one of the most fundamental problem of computational geometry [7, 8]. There exist algorithms running in time $O(n \log n)$ in dimension 2 or 3. General algorithms construct the convex hull of a set of n points in $\mathbb{Z}^d$ in $O(n \log n +$

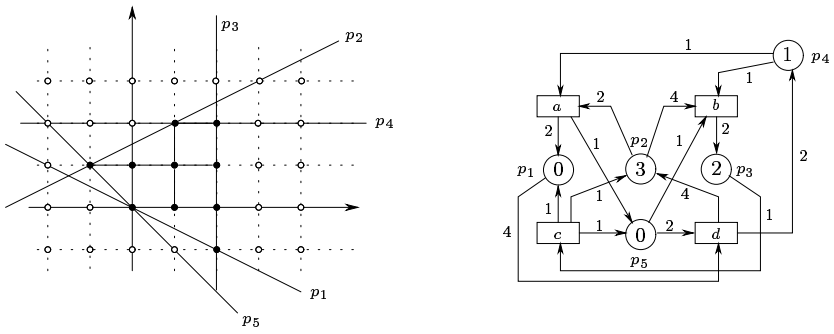


Figure 11: a convex hull for the representation of the state space of the automaton of Fig. 6 with a non minimal number of facets leading to a vector addition system with two redundant places as compared to the vector addition system indicated in Fig. 7

$n^{\lfloor (d+1)/2 \rfloor})$ in time and $O(n^{\lfloor d/2 \rfloor})$ in space. Since d corresponds to the size of the alphabet minus the dimension of the space of cycles, we see that this worst case complexity is exponential in the size of the automaton. However the points in the representation of the state space of a commutative automaton are not randomly distributed: they are "almost" all the integral points of a polyhedron, and the convex hull may be computed from its extremal points only. A comparison of the number n of integral points of a d dimensional polyhedron with $m^{\lfloor (d+1)/2 \rfloor}$ where m is the number of its extremal points may give a better hint to the complexity of our algorithm. In the same spirit, Seidel [24] and Swart [28] give the complexity of the convex hull construction in term of the output of the algorithm, namely the number of facets that it computes. Seidel gives an algorithm which has running time $O(n^2 + F \log n)$ where F is the number of facets produced by the algorithm. We know that only a polynomial number of places need to be synthetized when solving the synthesis problem for vector addition systems [1]: there exists a convex hull with a number of facets $F \leq n \times ((n-1) \times p)$ where n is the number of states and p the number of events of the automaton when this automaton is isomorphic to the state graph of a vector addition system. However as shown in Fig. 11 the construction of the convex hull of the representation of the state space may lead to a polyhedron with a non minimal number of

facets; and this result gives no indication on the number of facets that may be produced for an arbitrary automaton. Nevertheless it suggests that we can hope than on average the number of facets be polynomially bounded by the size of the automaton. In that respect we recall that the algorithm that we proposed in [1] is based on Khachiyan's ellispsoid method [23] which in pratice is replaced by the, theoretically inefficient, simplex method. Actually, even though the simplex method is not a polynomial time method it has a better average complexity than the ellipsoid method.

The tool SYNET [3] implements the algorithm of [1] and provides a computer assisted solution to the distribution of protocols. When the automaton decribing a protocol fails to be isomorphic to the state graph of a vector addition system informations are provided in order to assist the designer to modify the specification of the protocol. In that respect, the algorithm described in this paper may give further informations. In particular the canonical representation of a commutative automaton may give useful information for the distribution of the automaton even if it fails to be isomorphic to the state graph of a vector addition system.

References

[1] BADOUEL, E., BERNARDINELLO, L. and DARONDEAU, PH., *Polynomial algorithms for the synthesis of bounded nets*, Proceedings Caap 95, Lecture Notes in Computer Science 915 (1995) 647–679.

[2] BERNARDINELLO, L., DE MICHELIS, G., PETRUNI, K., and VIGNA, S., *On the Synchronic Structure of Transition Systems*, in J. Desel (Ed.), Structures in Concurrency Theory (STRICT), May 1995, Springer (1996) 11–31.

[3] CAILLAUD, B., SYNET : *un outil de synthèse de réseaux de Petri bornés, applications* Irisa Research Report no 1101 (1997).

[4] CHAND, D.R., and KAPUR, S.S., *An algorithm for convex polytopes.* Journal of the Association for Computing Machinery, vol. 17, No 1 (1970) 78–86.

[5] CHOU, T.J., and COLLINS, G.E., *Algorithms for the solution of systems of linear Diophantine equations*, SIAM Journal of Computing, 11 (1982) 687–708.

[6] DESEL, J., REISIG, W., *The Synthesis Problem of Petri Nets.* Acta Informatica vol. 33 (1996) 297–315.

[7] EDELSBRUNNER, H., *Algorithms in Combinatorial Geometry.* EATCS Monographs in Theoretical Computer Science vol. 10, Springer, Heidelberg (1987).

[8] EDELSBRUNNER, H., *Geometric Algorithms.* In P.M. Gruber and J.M. Wills (Eds.) Handbook of Convex Geometry vol. A, North-Holland (1993) 699–735.

[9] EHRENFEUCHT, A., and ROZENBERG, G., *Partial 2-structures ;* Part I : *Basic Notions and the Representation Problem*, Acta Informatica, vol. 27 (1990) 315–342.

[10] EHRENFEUCHT, A., and ROZENBERG, G., *Partial 2-structures ;* Part II :*State Spaces of Concurrent Systems*, Acta Informatica, vol. 27 (1990) 343–368.

[11] GROSS, J.L., and TUCKER, T.W., *Topological Graph Theory*, Wiley-Interscience, New York (1987).

[12] HERWIG, B., *Extending partial isomorphisms on finite structures*, Combinatorica 15 (1995) 365–371.

[13] HERWIG, B., and LASCAR, D., *Extending partial automorphism and the profinite topology on the free groups.* Draft (1997).

[14] HRUSHOVSKI, E. *Extending partial isomorphisms of graphs*, Combinatorica 12 (1992) 204–218.

[15] ILIOPOULOS, C.S., *Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix.* SIAM Journal on Computing, Vol. 18, No 4 (1989) 658–669.

[16] KANNAN, R., and BACHEM, A., *Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix.* SIAM Journal on Computing, Vol. 8, No 4 (1979) 499–507.

[17] KARP, R.M., and MILLER, R.E., *Parallel program schemata.* Journal of Computer and System Sciences vol. 3 (1969) 147–195.

[18] LYNDON, R.C., and SCHUPP, P.E., *Combinatorial Group Theory.* Ergebnisse Vol. 89, Springer (1977).

[19] MAGNUS, W., KARRASS, A., and SOLITAR, D., *Combinatorial Group Theory.* Wiley, New York (1966).

[20] MARCUS, M., and MINC, H., *A Survey of Matrix Theory and Matrix Inequalities.* Dover Publications, New York (1992).

[21] PETRICH, M., *Inverse Semigroups*, Wiley, New York (1984).

[22] RAYWARD-SMITH, V.J., *On computing the Smith normal form of an integer matrix.* ACM Transaction on Mathematical Software, Vol. 5. No 4 (1979) 451–456.

[23] SCHRIJVER, A., *Theory of Linear and Integer Programming.* John Wiley (1986).

[24] SEIDEL, R., *Constructing Higher-Dimensional Convex Hulls at Logarithmic Cost per Face.* Proceedings Annual ACM Symposium on Theory of Computing 18 (1986) 404–413.

[25] SILVA, M., and COLOM, J.M., *On the Computation of Structural Synchronic Invariants in P/T nets.* In "Advances in Petri Nets 1988", G. Rozenberg (Ed.), volume 340 of Springer Verlag Lecture Notes in Computer Science (1988) 386–417.

[26] STALLINGS, J.R., *Topology of Finite Graphs.* Inventiones Mathematicae. 71 (1983) 551–565.

[27] STILLWELL, J., *Classical Topology and Combinatorial Group Theory*, Springer Verlag, New York (1980).

[28] SWART, G., *Finding the Convex Hull Facet by Facet.* Journal of Algorithm 6 (1985) 17–48.

Appendix

In this appendix we first relate Galois coverings of automata with the free realizations of groups. On this basis, we suggest a definition of Galois covering for reversible transition systems (which are not necessarily connected) in terms of quotients associated with free actions of groups. We then can state a result which illustrates the problem that we encounter in order to establish that state graphs of vector addition systems are torsion-free. Namely we have two groups which are natural candidates for representing a commutative automaton whose Parikh unfolding is a connected component of a polyhedral graph with set of vertices $P = \{x \in \mathbb{Z}^n | \mu \cdot x + b \geq 0\}$. The first one is its canonical group $\mathcal{C}(A) = \mathbb{Z}^n / H_1(A)$ with associated representation computed by our algorithm. The second one is the factor $\mathbb{Z}^n / ker(\mu)$ which corresponds to the usual definition of the marking graph of the vector addition system associated with P. We have $H_1(A) \subseteq ker(\mu)$ leading to a surjective morphism between the two representing groups, This map does not identify elements which are in the images of the representations but may identifies some other elements.

Conjecture 22 states that if P is the convex hull of the commutative image of the automaton, then this two representations coincide, i.e. $H_1(A) = ker(\mu)$.

Coverings and Groups Acting on Graphs

A *representation* of a group G by a reversible automaton $A = (E, S, T, s_0)$, also called *realization*, is a group morphism $\varphi : G \to \mathbf{Aut}(A)$ where $\mathbf{Aut}(A)$ is the group of the automorphisms of A, i.e. the group consisting of those bijections $f : S \to S$ such that $\forall s, s' \in S$, $\forall e \in E$ $s \xrightarrow{e} s' \Leftrightarrow f(s) \xrightarrow{e} f(s')$. φ is also termed an *action* of G on A and we let $g \cdot s$ denote $\varphi(g)(s)$. The representation is termed *free* if the identity is the only element of G having a fixed point: $\exists s \in S \quad g \cdot s = s \Rightarrow g = 1$. If G acts on A, the quotient of A by the action of G is the reversible automaton $A/G = (E, S/G, T/G, Gs_0)$ whose states are G-orbits, $S/G = \{Gs \mid s \in S\}$, and whose transitions are given by $T/G = \{(Gs, e, Gs') \mid (s, e, s') \in T\}$. The canonical map $q : A \to A/G$ that takes a state to its orbit $q(s) = Gs$ is a morphism of automata.

Let $f : \tilde{A} \to A$ be a Galois covering with Galois group G between reversible automata, i.e. $\tilde{A} \cong A^\alpha$ for some regular voltage assignment in G for A, then G acts freely on $\tilde{A}$ by $g \cdot (s, h) = (s, gh)$ and $\tilde{A}/G \cong A$. Conversely if a group G has a free action on a reversible automaton A, then the map $q : A \to A/G$ is a Galois covering with Galois group G. Indeed, let us choose one state s_ω in each orbit (where $s_\omega = s_0$ if ω is the orbit of the initial state s_0); since G acts transitively and freely on each orbit, a state $s \in S$ can univocally be encoded by the pair (ω, g) where ω is its orbit and $g \in G$ the unique element of the group such that $g.s_\omega = s$. With that representation the action of G on A writes down $g'.(\omega, g) = (\omega, g'g)$ and the canonical projection $p(\omega, g) = \omega$. Let $\omega \xrightarrow{e} \omega'$ be a transition in T/G, then there exists $g, g' \in G$ such that $g \cdot s_\omega \xrightarrow{e} g' \cdot s_{\omega'}$, and thus $s_\omega \xrightarrow{e} g^{-1}g' \cdot s_{\omega'}$. If we let this element $\alpha_t = g^{-1}g'$ be assigned to the transition $t = \omega \xrightarrow{e} \omega'$ we deduce $(\omega, g) \xrightarrow{e} (\omega', g')$ in T if and only if $\omega \xrightarrow{e} \omega'$ in T/G and $g' = g\alpha_t$. Thus A is isomorphic to the derived automaton A^α and is therefore a Galois covering of A/G.

Thus free realizations of groups correspond to Galois coverings. Do we have a class of group realizations corresponding to the whole class of coverings? In fact not because if the canonical map $q : A \to A/G$ associated with the action of a group G on a reversible automaton A is a covering then it is a Galois

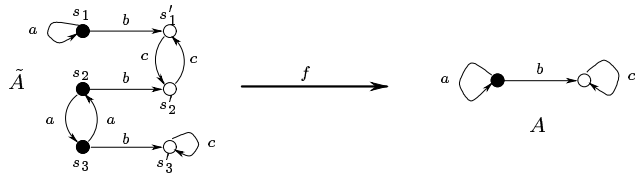
covering. Actually p is a covering if and only any two distinct transitions sharing the same source or the same target belong to distinct orbits. We can assume without loss of generality that the identity is the only element of G that fixes every state of S, because the set of such elements form a normal subgroup K of G, and the factor group $G' = G/K$ acts on A with $A/G \cong A/G'$. Assume p is a covering and suppose that $g \in G$ has a fixed point: $g \cdot s = s$, let s' be some state connected to s by a transition, e.g. $s \xrightarrow{e} s'$, then $s = g \cdot s \xrightarrow{e} g \cdot s'$ and thus $g \cdot s' = s'$ by determinacy of A, since A is connected g fixes every state of S and thus is the identity. G acts freely on A and therefore p is a Galois covering.

The above definitions for realization of a group, quotient of an automaton by an action of a group and derived automaton associated with a regular voltage assignment extend naturally to reversible transition systems. It is then natural to define a Galois covering of a reversible transition system as follows.

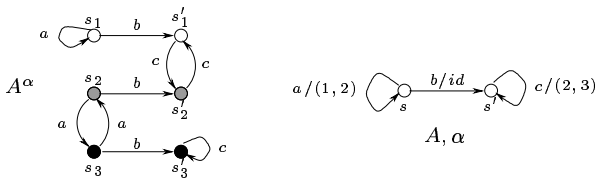
Definition 27 *A covering $f : \tilde{\mathbf{T}} \to \mathbf{T}$ of reversible transition systems is termed a Galois covering with Galois group G if G acts freely on $\tilde{\mathbf{T}}$ and there exists an isomorphism $\varphi : \tilde{\mathbf{T}}/G \to \mathbf{T}$ such that $\varphi \circ p = f$ (where $p : \tilde{\mathbf{T}} \to \tilde{\mathbf{T}}/G$ is the canonical projection).*

Let $f : \tilde{\mathbf{T}} \to \mathbf{T}$ be a Galois covering of Galois group G, then $\tilde{\mathbf{T}} \cong \mathbf{T}^\alpha$ for some voltage assignement α (with f identified with the projection p^α). Let $s \in S$ be some state of $\mathbf{T}$, then the group $\pi_1(\tilde{\mathbf{T}}, \tilde{s})$ does not depend upon the choice of $\tilde{s} \in f^{-1}(s)$ and is a normal subgroup of $\pi_1(\mathbf{T}, s)$, namely it is the kernel of the group morphism $\alpha : \pi_1(\mathbf{T}, s) \to G$ derived from the map α. Thus $\pi_1(\mathbf{T}, s)/\pi_1(\tilde{\mathbf{T}}, \tilde{s})$ can be viewed as a subgroup of G whose index gives the number of connected components of its inverse image $f^{-1}(\mathbf{T}, s)$.

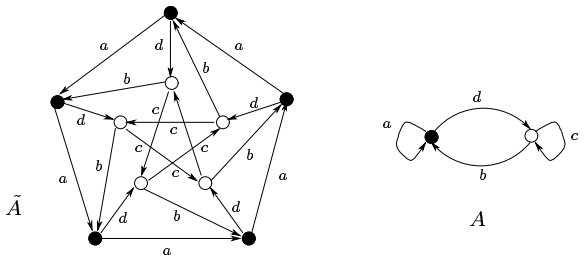
Here is an example of a covering which is not a Galois covering since for instance the transitions $s_1 \xrightarrow{a} s_1$ and $s_2 \xrightarrow{a} s_3$ are conjugate chains whose common image the transition $s \xrightarrow{a} s$ and the former is a cycle while the latter is not.



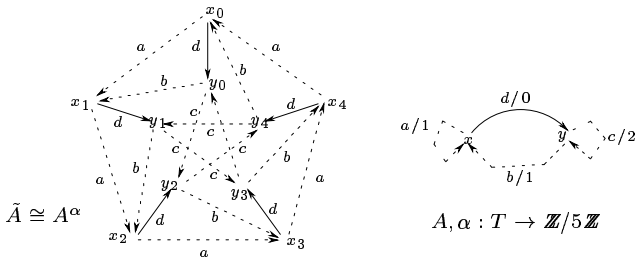
Let $U = \{s \xrightarrow{b} s'\}$ the spanning tree of A, the lifts of the spanning tree U are the trees U_1, U_2 and U_3 whose nodes are colored respectively in white, grey and black, and whose union spans $\tilde{A}$. The automaton $\tilde{A}$ is isomorphic to A^α where α is the voltage assignment taking each transition of A to the permutation of the set $\{1;2;3\}$ such that the fiber of $t = x \xrightarrow{e} y$ consists of the transitions $x_i \xrightarrow{e} y_{\alpha_t(i)}$ where x_i stands for the element of U_i projecting to x.



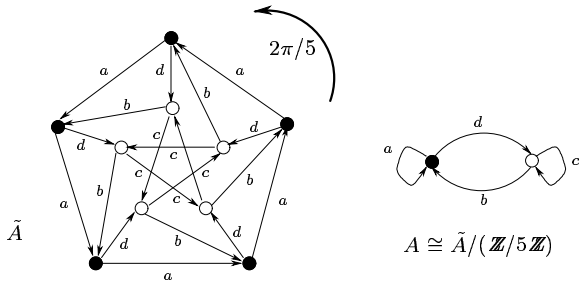
On the contrary the following is a Galois covering:



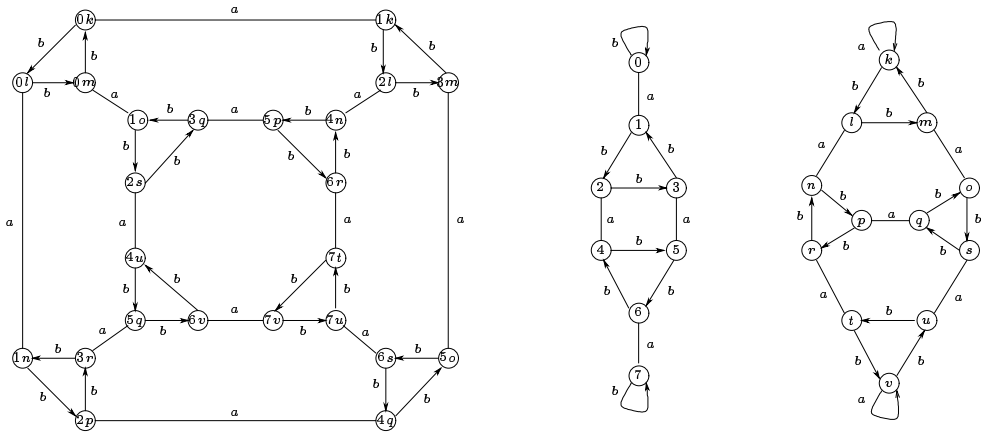
$\pi_1(A)$ is the group generated by a, db, and dcd^{-1}, $\pi_1(\tilde{A})$ is the group generated by a^5, c^5, $ab^{-1}d^{-1}$ and $dcd^{-1}a^{-2}$. The Galois group is $\pi_1(A)/\pi_1(\tilde{A}) = \mathbf{gp}(\{a\}, a^5) = \mathbb{Z}/5\mathbb{Z}$ because $db = a$ and $dcd^{-1} = a^2$ modulo $\pi_1(\tilde{A})$. If we choose the d labelled transition as covering tree, the chords represented in dashed lines are associated to the following elements of $\pi_1(A)$: a, da, and dcd^{-1} whose images in $\pi_1(A)/\pi_1(\tilde{A}) = \mathbf{gp}(\{a\}, a^5)$ are respectively a, a, and a^2 i.e. 1,1, and 2 in $\mathbb{Z}/5\mathbb{Z}$. Thus $\tilde{A}$ is isomorphic to A^α where α is the regular voltage assignment $\alpha : T \to \mathbb{Z}/5\mathbb{Z}$ indicated below.



$\mathbb{Z}/5\mathbb{Z}$ acts freely on $\tilde{A}$, the action of its generator 1 (associated with word $a \in F(E)$) is the rotation of $2\pi/5$. There is two orbits corresponding respectively to the black and white states, and $A \cong \tilde{A}/(\mathbb{Z}/5\mathbb{Z})$.



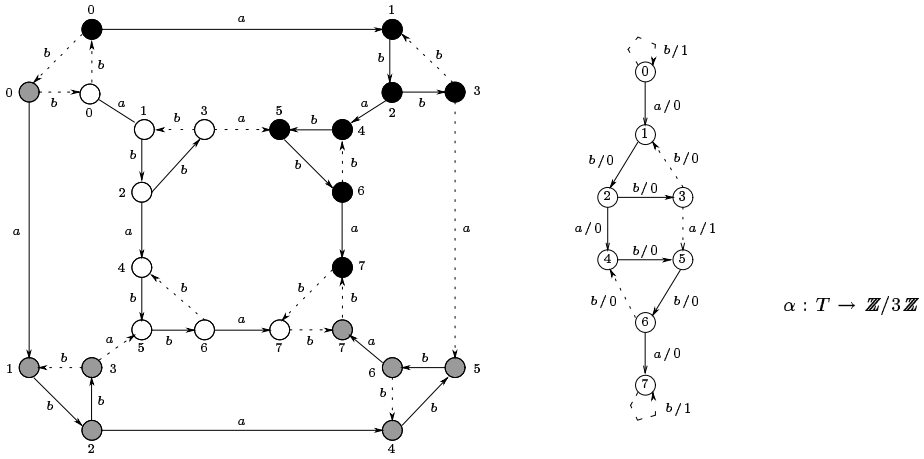
If E is a set of generators of a group G and H and K two subgroups of G with $H \subseteq K$, then the map $f : S(G,H,E) \to S(G,K,E) \ : Hg \mapsto Kg$ is a covering, and it is a Galois covering if and only if H is a normal subgroup of K (because $\pi_1(S(G,H,E)) = H$). In particular since $C(G,E) = S(G,1,E)$ the map $f : C(G,E) \to S(G,H,E) \ : g \mapsto Hg$ is a Galois covering for any subgroup H of G. For instance if $G = \mathbf{gp}(\{a;b\}; a^2, b^3, (ab)^4)$, $E = \{a;b\}$ and H is respectively the subgroup of G generated by a and by b then the resulting quotients are Galois coverings of respective degree 3 and 2.



$C(G,\{a;b\})$ where $G = \mathbf{gp}(\{a;b\}; a^3, b^2, (ab)^4)$ $S(G,<b>,\{a;b\})$ $S(G,<a>,\{a;b\})$

Below is a particular choice of a spanning tree U for $A = S(G,<a>,\{a;b\})$ (the corresponding chords are represented in dashed lines). The fiber of state

0 form the upper left triangle in $\tilde{A} = C(G, \{a; b\})$ and the lifts of the spanning tree U are the trees U_1, U_2 and U_3 whose nodes are colored respectively in black, grey and white and whose union spans $\tilde{A}$. The Galois group is $< b >= \mathbf{gp}(\{b\}, b^3) \cong \mathbb{Z}/3\mathbb{Z}$. The automaton $\tilde{A}$ is isomorphic to A^α where $\alpha : T \to \mathbb{Z}/3\mathbb{Z}$ is the regular voltage assignment indicated in the figure (since a is of order 2 one has $\alpha(s' \xrightarrow{a} s) = -\alpha(s \xrightarrow{a} s')$, we thus have omitted half of the transitions labelled a).



Observe finally that the Schreier graphs $S(G, H, E)$ coincide with the connected coverings of the bouquet B_E, the subclass of the Cayley graphs corresponding to the Galois coverings. The bouquet B_E is the automaton with just one state s_0 and one transition $s_0 \xrightarrow{e} s_0$ for each $e \in E$. Actually $B_E \cong S(G, G, E)$ and thus the canonical map $S(G, H, E) \to B_E \cong S(G, G, E)$ is a covering and is a Galois covering if and only if H is a normal subgroup of G and then $S(G, H, E) \cong C(G/H, E)$ is a Cayley graph. Conversely a connected covering of the bouquet B_E is of the form B_E^{α, x_0} for some voltage assignment α taking each event $e \in E$ to some permutation of a set X, i.e. it is a permutation automaton on the alphabet E, hence isomorphic to the Schreier graph $S(G, H, E)$ where G is the group generated by the permutations α_e and $H = G_{x_0}$ is the stabiliser of x_0. A connected Galois covering of the bouquet B_E is of the form B_E^α for some regular voltage assignment $\alpha : E \to G$ and thus isomorphic to the Cayley graph $C(G, E)$. From this discussion it follows the result (already

mentioned) according to which a Schreier graph $S(G, H, E)$ is isomorphic to a Cayley graph if *and only if* H is a normal subgroup of G.

The Conjecture Revisited

Proposition 28 *Let $\tilde{\mathbf{T}}$ be the polyhedral transition system associated with set of vertices $P = \{x \in \mathbb{Z}^n \mid \mu \cdot x + b \geq 0\}$ where $\mu \in \mathbb{Z}^{m,n}$ and $b \in \mathbb{N}^m$, and $\mathbf{T}$ be the transition system with set of states $S = \{y \in \mathbb{N}^m \mid y = Ax + b\}$ and transition relation given by $y \xrightarrow{e_i} y' \Leftrightarrow y' = y + \mu \cdot e_i$. The affine function $f(x) = \mu \cdot x + b$ is a Galois covering from $\tilde{\mathbf{T}}$ to $\mathbf{T}$ with Galois group $ker(\mu) = \{u \in \mathbb{Z}^n \mid \mu \cdot u = 0\}$. The first homolgy group of some connected component of $\mathbf{T}$ is a subgroup of $ker(\mu)$ whose index corresponds to the number of connected components in its inverse image.*

Proof: $ker(\mu)$ acts freely on $\tilde{\mathbf{T}}$ by $u \bullet x = x + u$, let $q : \tilde{\mathbf{T}} \to \tilde{\mathbf{T}}/ker(\mu)$ be the canonical projection.There exists an isomorphism $\varphi : \tilde{\mathbf{T}}/ker(\mu) \to \mathbf{T}$ such that $\varphi \circ q = f$. Indeed $ker(\mu)x = ker(\mu)y$ if and only if $x - y \in ker(\mu)$ if and only if $f(x) = f(y)$ from which it follows that the map φ sending the coset $ker(\mu)x$ to the vector $\mu \cdot x + b$ (i.e. such that $\varphi \circ q = f$) is well defined and one to one. Now φ is onto because f is onto and is a morphism of transition systems because f and q are both coverings.

Let $\mathbf{A} = (\mathbf{T}, s_0)$ be a reversible automaton associated with the connected component of s_0 in $\mathbf{T}$. For each $\tilde{s}_0 \in f^{-1}(s_0)$ the restriction of f is a Galois covering from $\tilde{\mathbf{A}} = (\tilde{\mathbf{T}}, \tilde{s}_0)$ to $\mathbf{A}$ with Galois group $\pi_1(\mathbf{A})/\pi_1(\tilde{\mathbf{A}}) = \psi(\pi_1(\mathbf{A}))$ the first homology group of $\mathbf{A}$ which is therefore a subgroup of $ker(\mu)$ whose index corresponds to the number of connected components of $f^{-1}(\mathbf{A})$. ∎

The following is then a restatement of Conjecture. 22.

Conjecture 29 *If P is the convex hull of the connected component of the origin in $\tilde{\mathbf{T}}$ then $H_1(\mathbf{A}) = ker(\mu)$.*

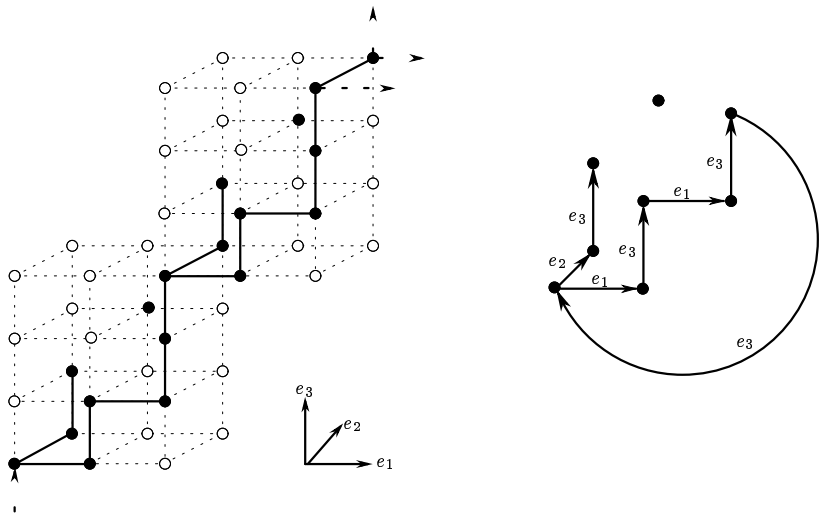


Figure 12: the $\mathbb{Z}$-transition system shown on the left is associated with the polyhedron presented by the inequations $0 \leq x_2 \leq 1$, $3x_1 + 2x_2 - 2x_3 \geq 0$, and $-3x_1 - 4x_2 + 2x_3 + 4 \geq 0$. Its kernel K is the group generated by $v = 2e_1 + 3e_3$ (it is the set of vectors $u = x_1e_1 + x_2e_2 + x_3e_3$ such that $x_2 = 0$ and $3x_1 - 2x_3 = 0$). The quotient has two connected components. The first homology group of the former is K hence its inverse image is connected. The latter is an isolated point its first homology group is therefore trivial and its inverse image consists of infinitely many isolated points

Unit´e de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unit´e de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unit´e de recherche INRIA Rhône-Alpes, 655, avenue de l'Europe, 38330 MONTBONNOT ST MARTIN
Unit´e de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unit´e de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
http://www.inria.fr
ISSN 0249-6399