The group of reversible Turing machines and the torsion problem for $\mathrm{Aut}(A^{\mathbb{Z}})$ and related topological fullgroups

Sebastián Barbieri

From a joint work with Jarkko Kari and Ville Salo
LIP, ENS de Lyon – CNRS – INRIA – UCBL – Université de Lyon

CMM, universidad de Chile
December, 2016

Motivation

Given a fullshift $(\mathcal{A}^{\mathbb{Z}}, \sigma)$ recall that its automorphism group is given by

$$\mathrm{Aut}(\mathcal{A}^{\mathbb{Z}}) = \{\phi : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}} \text{ homeomorpism}, [\sigma, \phi] = \mathrm{id}\}$$

Motivation

Given a fullshift $(\mathcal{A}^{\mathbb{Z}}, \sigma)$ recall that its automorphism group is given by

$$\mathrm{Aut}(\mathcal{A}^{\mathbb{Z}}) = \{\phi : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}} \text{ homeomorpism}, [\sigma, \phi] = \mathrm{id}\}$$

It is still unknown whether $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \cong \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$, but we know that

$$\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$$

$$\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$$

Motivation

A simple example with that property :

$$G_1 = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z} \text{ and } G_2 = \mathbb{Z}/2\mathbb{Z} \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z}$$

Motivation

A simple example with that property :

$$G_1 = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z} \text{ and } G_2 = \mathbb{Z}/2\mathbb{Z} \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z}$$

$$G_1 \hookrightarrow G_2 : (a_1, a_2, \cdots) \to (0, a_1, a_2, \cdots)$$

Motivation

A simple example with that property :

$$G_1 = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z} \text{ and } G_2 = \mathbb{Z}/2\mathbb{Z} \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z}$$

$$G_1 \hookrightarrow G_2 : (a_1, a_2, \cdots) \to (0, a_1, a_2, \cdots)$$

$$G_2 \hookrightarrow G_1 : (a_1, a_2, \cdots) \to (2a_1, a_2, \cdots)$$

Motivation

A simple example with that property :

$$G_1 = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z} \text{ and } G_2 = \mathbb{Z}/2\mathbb{Z} \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/4\mathbb{Z}$$

$$G_1 \hookrightarrow G_2 : (a_1, a_2, \cdots) \to (0, a_1, a_2, \cdots)$$

$$G_2 \hookrightarrow G_1 : (a_1, a_2, \cdots) \to (2a_1, a_2, \cdots)$$

However, they are not isomorphic : Each element of G_1 which has order 2 has square roots, while $(1, 0, 0, 0, \cdots)$ has none in G_2.
Moral : we should try to understand torsion and roots in $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$

Talk highlights

Definition (Torsion problem)

Let $G = \langle S \mid R \rangle$ be a finitely generated group. The torsion problem of G is the language $\mathtt{TP}(G)$ where

$$\mathtt{TP}(G) = \{w \in S^* \mid \exists n \in \mathbb{N} \text{ such that } w^n =_G 1\}$$

Talk highlights

Definition (Torsion problem)

Let $G = \langle S \mid R \rangle$ be a finitely generated group. The torsion problem of G is the language $\mathtt{TP}(G)$ where

$$\mathtt{TP}(G) = \{w \in S^* \mid \exists n \in \mathbb{N} \text{ such that } w^n =_G 1\}$$

Theorem (B, Kari, Salo)

For any finite alphabet $|A| \geq 2$, $\mathrm{Aut}(A^{\mathbb{Z}})$ *contains a finitely generated subgroup with undecidable torsion problem*

Talk highlights

Definition (Torsion problem)

Let $G = \langle S \mid R \rangle$ be a finitely generated group. The torsion problem of G is the language $\mathtt{TP}(G)$ where

$$\mathtt{TP}(G) = \{w \in S^* \mid \exists n \in \mathbb{N} \text{ such that } w^n =_G 1\}$$

Theorem (B, Kari, Salo)

For any finite alphabet $|A| \geq 2$, $\mathrm{Aut}(A^{\mathbb{Z}})$ contains a finitely generated subgroup with undecidable torsion problem

Theorem (B, Kari, Salo)

Let $(A^{\mathbb{Z}^d}, \sigma)$ be a full shift and $|A| \geq 2$. The topological fullgroup $[[\sigma]]$ contains a finitely generated subgroup with undecidable torsion problem if and only if $d \geq 2$.

Background

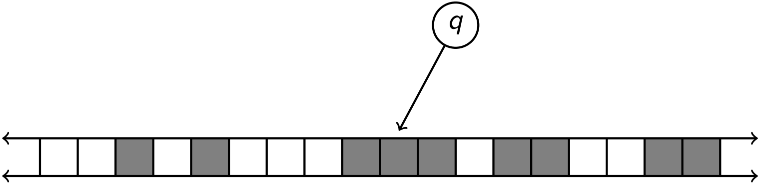
Recall that a Turing machine is defined by a rule :

$$\delta_T : \Sigma \times Q \to \Sigma \times Q \times \{-1, 0, 1\}$$

Background

Recall that a Turing machine is defined by a rule :

$$\delta_T : \Sigma \times Q \to \Sigma \times Q \times \{-1, 0, 1\}$$

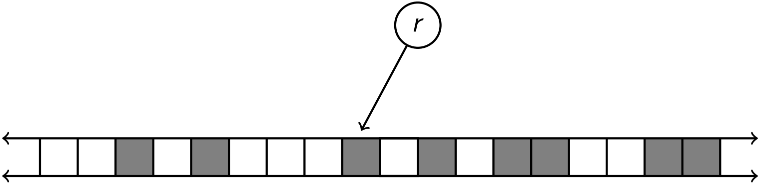


$$\delta_T(\blacksquare, q) = (\square, r, -1)$$

Background

Recall that a Turing machine is defined by a rule :

$$\delta_T : \Sigma \times Q \to \Sigma \times Q \times \{-1, 0, 1\}$$

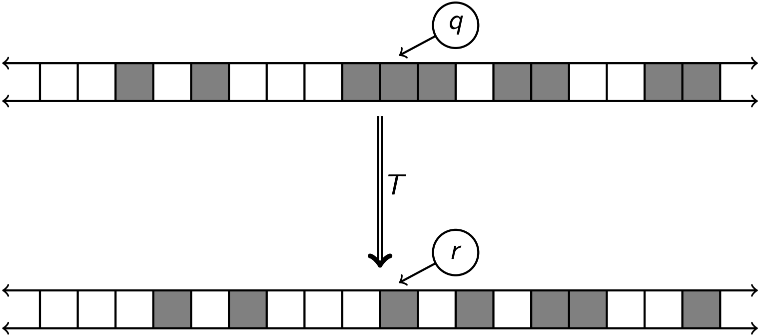


$$\delta_T(\blacksquare, q) = (\square, r, -1)$$

Background

This defines a natural action

$$T : \Sigma^{\mathbb{Z}} \times Q \to \Sigma^{\mathbb{Z}} \times Q$$



This defines a natural action

$$T : \Sigma^{\mathbb{Z}} \times Q \to \Sigma^{\mathbb{Z}} \times Q$$

Such that if $(x, q) \in \Sigma^{\mathbb{Z}} \times Q$ and $\delta_T(x_0, q) = (a, r, d)$ then :

$$T(x, q) = (\sigma_{-d}(\tilde{x}), q')$$

where $\sigma : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ is the shift action given by $\sigma_d(x)_z = x_{z-d}$, $\tilde{x}_0 = a$ and $\tilde{x}|_{\mathbb{Z}\setminus\{0\}} = x|_{\mathbb{Z}\setminus\{0\}}$.

Motivation

- The composition of two actions $T \circ T'$ is not necessarily an action generated by a Turing machine.
- if the action T is a bijection then the inverse it not necessarily an action generated by a Turing machine.

Motivation

- The composition of two actions $T \circ T'$ is not necessarily an action generated by a Turing machine.
- if the action T is a bijection then the inverse it not necessarily an action generated by a Turing machine.

As in cellular automata, the class of CA with radius bounded by some $k \in \mathbb{N}$ is not closed under composition or inverses.

Definition

Let's get rid of these constrains. Given F, F' finite subsets of a group G, consider instead of δ_T a function :

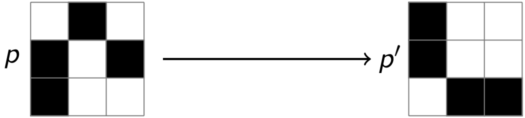
$$f_T : \Sigma^F \times Q \to \Sigma^{F'} \times Q \times G,$$

Definition

Let's get rid of these constrains. Given F, F' finite subsets of a group G, consider instead of δ_T a function :

$$f_T : \Sigma^F \times Q \to \Sigma^{F'} \times Q \times G,$$

Let $F = F' = \{0, 1, 2\}^2$, then $f_T(p, q) = (p', q', \vec{d})$ means :

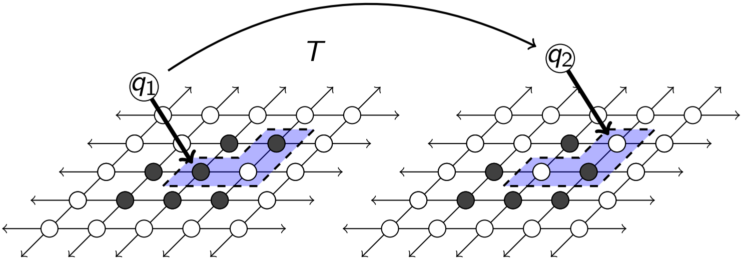
- 

- Turn state q into state q'
- Move head by $\vec{d}$.

Moving head model

f_T defines naturally an action

$$T \curvearrowright \Sigma^G \times Q \times \mathbb{Z}^d$$

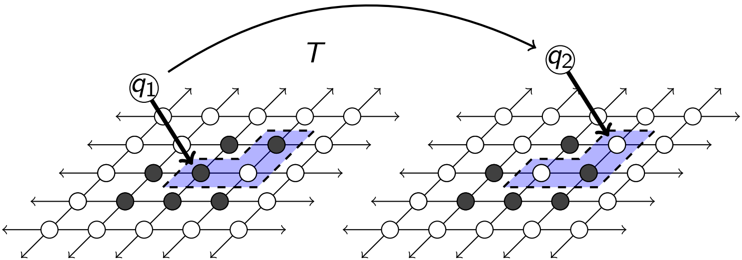


$f(\bullet\overset{\bullet}{\circ}, q_1) = (\circ\overset{\circ}{\bullet}, q_2, (1,1))$ $\quad$ $F = \{(0,0),(1,0),(1,1)\}$

Moving head model

f_T defines naturally an action

$$T \curvearrowright \Sigma^G \times Q \times \mathbb{Z}^d$$



$f(\bullet\overset{\bullet}{\circ}, q_1) = (\circ\overset{\circ}{\bullet}, q_2, (1,1))$ $\quad$ $F = \{(0,0),(1,0),(1,1)\}$

Let $|\Sigma| = n$ and $|Q| = k$.
$(\mathrm{TM}(G,n,k), \circ)$ is the monoid of all such T with the composition operation ; $(\mathrm{RTM}(G,n,k), \circ)$ is the group of all such T which are bijective .

Moving head model : As cellular automata

Let $Q = \{1, \ldots, k\}$ and $\Sigma = \{0, \ldots, n-1\}$.

$$\Sigma^G = \{x : G \to \Sigma\}$$

$$X_k = \{x \in \{0, 1, \ldots, k\}^G \mid 0 \notin \{x_g, x_h\} \implies g = h\}$$

Let $X_{n,k} = \Sigma^G \times X_k$ and $Y = \Sigma^G \times \{0^G\}$. Then :

Moving head model : As cellular automata

Let $Q = \{1, \ldots, k\}$ and $\Sigma = \{0, \ldots, n-1\}$.

$$\Sigma^G = \{x : G \to \Sigma\}$$

$$X_k = \{x \in \{0, 1, \ldots, k\}^G \mid 0 \notin \{x_g, x_h\} \implies g = h\}$$

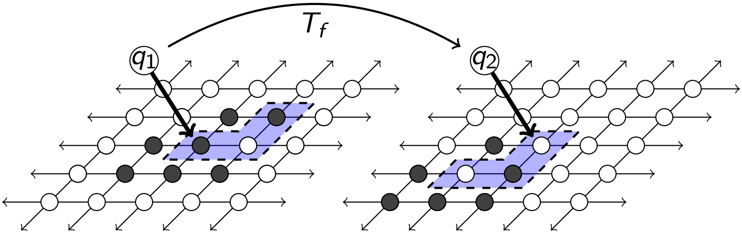
Let $X_{n,k} = \Sigma^G \times X_k$ and $Y = \Sigma^G \times \{0^G\}$. Then :

$$\mathrm{TM}(G, n, k) = \{\phi \in \mathrm{End}(X_{n,k}) \mid \phi|_Y = \mathrm{id}, \phi^{-1}(Y) = Y\}$$
$$\mathrm{RTM}(G, n, k) = \{\phi \in \mathrm{Aut}(X_{n,k}) \mid \phi|_Y = \mathrm{id}\}$$

Moving tape model

f_T defines naturally an action

$$T \curvearrowright \Sigma^G \times Q$$

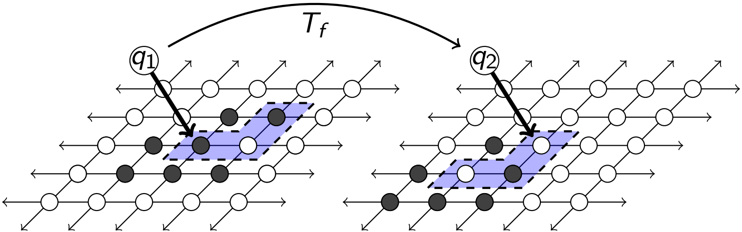


$f(\bullet\overset{\bullet}{\circ}, q_1) = (\circ\overset{\circ}{\bullet}, q_2, (1,1))$ $\quad F = \{(0,0),(1,0),(1,1)\}$

Moving tape model

f_T defines naturally an action

$$T \curvearrowright \Sigma^G \times Q$$



$f(\bullet\overset{\bullet}{\circ}, q_1) = (\circ\overset{\circ}{\bullet}, q_2, (1,1))$ $\quad F = \{(0,0), (1,0), (1,1)\}$

Let $|\Sigma| = n$ and $|Q| = k$.
$(\mathrm{TM}_{\mathrm{fix}}(G,n,k), \circ)$ is the monoid of all such T with the composition operation ; $(\mathrm{RTM}_{\mathrm{fix}}(G,n,k), \circ)$ is the group of all such T which are bijective .

Moving tape model : dynamical definition

Let $x, y \in \Sigma^G$. x and y are *asymptotic*, and write $x \sim y$, if they differ in finitely many coordinates. We write $x \sim_F y$ if $x_g = y_g$ for all $g \notin F$, F a finite subset of G.

Moving tape model : dynamical definition

Let $x, y \in \Sigma^G$. x and y are *asymptotic*, and write $x \sim y$, if they differ in finitely many coordinates. We write $x \sim_F y$ if $x_g = y_g$ for all $g \notin F$, F a finite subset of G.

Let $T : \Sigma^G \times Q \to \Sigma^G \times Q$ be a function.

Dynamical definition

T is a moving tape Turing machine $\iff$ T is continuous, and for a continuous function $s : \Sigma^G \times Q \to G$ and $F \subset G$ we have $T(x, q)_1 \sim_F \sigma_{s(x,q)}(x)$ for all $(x, q) \in \Sigma^G \times Q$.

Moving tape model : dynamical definition

Let $x, y \in \Sigma^G$. x and y are *asymptotic*, and write $x \sim y$, if they differ in finitely many coordinates. We write $x \sim_F y$ if $x_g = y_g$ for all $g \notin F$, F a finite subset of G.

Let $T : \Sigma^G \times Q \to \Sigma^G \times Q$ be a function.

Dynamical definition

T is a moving tape Turing machine $\iff$ T is continuous, and for a continuous function $s : \Sigma^G \times Q \to G$ and $F \subset G$ we have $T(x, q)_1 \sim_F \sigma_{s(x,q)}(x)$ for all $(x, q) \in \Sigma^G \times Q$.

$s : \Sigma^G \times Q \to G$ is the shift indicator function

Equivalence of the models

$\mathrm{RTM}_{\mathrm{fix}}(G, 1, k) \cong S_k$ and $G \hookrightarrow \mathrm{RTM}(G, 1, k)$.

Equivalence of the models

$\mathrm{RTM}_{\mathrm{fix}}(G, 1, k) \cong S_k$ and $G \hookrightarrow \mathrm{RTM}(G, 1, k)$.

Proposition

If $n \geq 2$ then :

$$\mathrm{TM}_{\mathrm{fix}}(G, n, k) \cong \mathrm{TM}(G, n, k)$$
$$\mathrm{RTM}_{\mathrm{fix}}(G, n, k) \cong \mathrm{RTM}(G, n, k).$$

Properties of RTM

Proposition

Let $T \in \mathrm{TM}_{\mathrm{fix}}(G, n, k)$. Then the following are equivalent :

1. T is injective.
2. T is surjective.
3. $T \in \mathrm{RTM}_{\mathrm{fix}}(G, n, k)$.
4. T preserves the uniform measure ($\mu(T^{-1}(A)) = \mu(A)$ for all Borel sets A).
5. $\mu(T(A)) = \mu(A)$ for all Borel sets A.

Properties of RTM

Proposition

If $n \geq 2$ $\mathrm{RTM}(\mathbb{Z}, n, k)$ is not finitely generated.

Properties of RTM

Proposition

If $n \geq 2$ $\mathrm{RTM}(\mathbb{Z}, n, k)$ is not finitely generated.

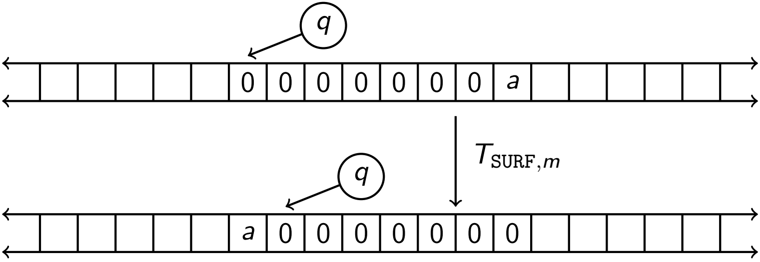
Proof : We find an epimorphism from RTM to a non-finitely generated group.
Let $T \in \mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}, n, k)$, therefore, it has a shift indicator $s : \Sigma^{\mathbb{Z}} \times Q \to \mathbb{Z}$. Define

$$\alpha(T) := \mathrm{E}_{\mu}(s) = \int_{\Sigma^{\mathbb{Z}} \times Q} s(x, q) d\mu,$$

One can check that $\alpha(T_1 \circ T_2) = \alpha(T_1) + \alpha(T_2)$.
Therefore $\alpha : \mathrm{RTM}(\mathbb{Z}, n, k) \to \mathbb{Q}$ is an homomorphism

Properties of RTM

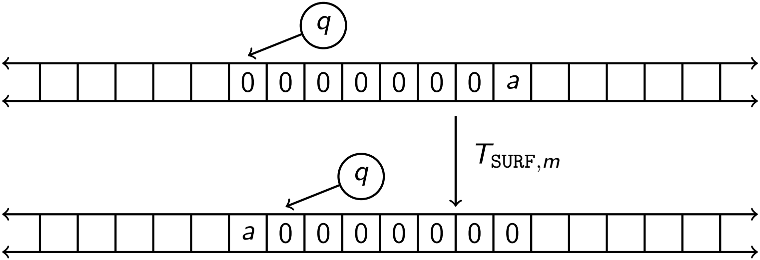
Now consider the machine $T_{\mathrm{SURF},m}$ where for all $a \in \Sigma$ and $q \in Q$:



$f(0^m a, q) = (a0^m, q, 1)$. Otherwise $f(u, q) = (u, q, 0)$.

Properties of RTM

Now consider the machine $T_{\texttt{SURF},m}$ where for all $a \in \Sigma$ and $q \in Q$:

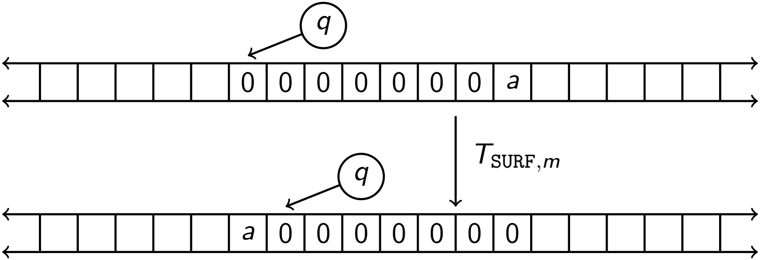


$f(0^m a, q) = (a0^m, q, 1)$. Otherwise $f(u, q) = (u, q, 0)$.

$T_{\texttt{SURF},m} \in \mathrm{RTM}(\mathbb{Z}, n, k)$ and $\alpha(T_{\texttt{SURF},m}) = 1/n^m$

Properties of RTM

Now consider the machine $T_{\mathtt{SURF},m}$ where for all $a \in \Sigma$ and $q \in Q$:



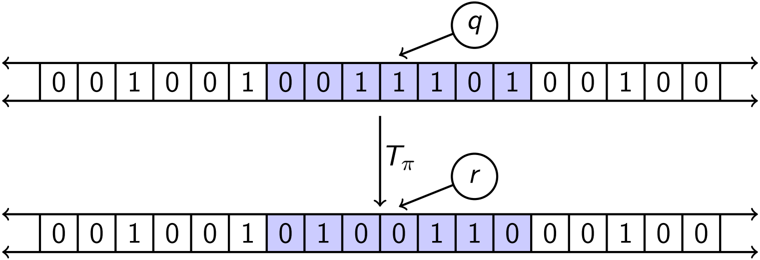
$$f(0^m a, q) = (a0^m, q, 1). \text{ Otherwise } f(u, q) = (u, q, 0).$$

$T_{\mathtt{SURF},m} \in \mathrm{RTM}(\mathbb{Z}, n, k)$ and $\alpha(T_{\mathtt{SURF},m}) = 1/n^m$

$\langle (1/n^m)_{m \in \mathbb{N}} \rangle \subset \alpha(\mathrm{RTM}(\mathbb{Z}, n, k))$ which is thus a non-finitely generated subgroup of $\mathbb{Q}$.

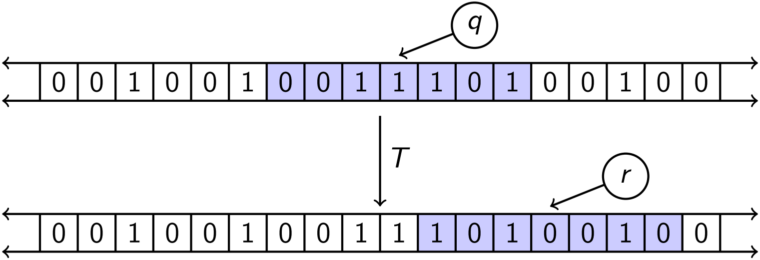
Interesting subgroups of RTM

▷ $\mathrm{LP}(G, n, k) \longrightarrow$ Local permutations.



Interesting subgroups of RTM

- $\triangleright$ $\mathrm{LP}(G, n, k) \longrightarrow$ Local permutations.
- $\triangleright$ $\mathrm{RFA}(G, n, k) \longrightarrow$ Reversible finite-state automata.



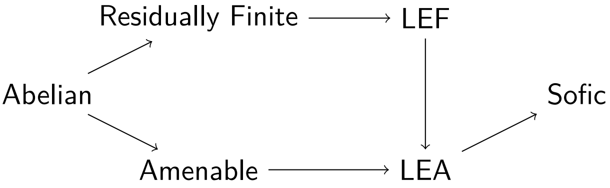
Interesting subgroups of RTM

- $\triangleright$ $\mathrm{LP}(G, n, k) \longrightarrow$ Local permutations.
- $\triangleright$ $\mathrm{RFA}(G, n, k) \longrightarrow$ Reversible finite-state automata.
- $\triangleright$ $\mathrm{OB}(G, n, k) \longrightarrow$ Oblivous machines $\langle \mathrm{LP}, \mathrm{Shift} \rangle$.

Interesting subgroups of RTM

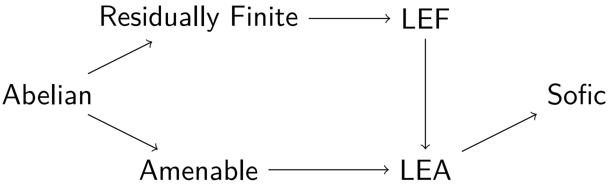
- $\triangleright$ $\mathrm{LP}(G, n, k) \longrightarrow$ Local permutations.
- $\triangleright$ $\mathrm{RFA}(G, n, k) \longrightarrow$ Reversible finite-state automata.
- $\triangleright$ $\mathrm{OB}(G, n, k) \longrightarrow$ Oblivous machines $\langle \mathrm{LP}, \mathrm{Shift} \rangle$.
- $\triangleright$ $\mathrm{EL}(G, n, k) \longrightarrow$ Elementary machines $\langle \mathrm{LP}, \mathrm{RFA} \rangle$.

Small group theory roadmap



- Res. finite groups are those where every non-identity element can be mapped to a non-identity element by a homomorphism to a finite group
- Amenable groups admit left invariant finitely additive measures.
- LEF and LEA stand for locally embeddable into (finite/amenable) groups.
- Sofic groups are generalizations of LEF and LEA.

Small group theory roadmap



Theorem

$\forall n \geq 2, \mathrm{RTM}(\mathbb{Z}^d, n, k)$ is LEF but neither amenable nor residually finite.

Some properties : $\mathrm{LP}(G, n, k)$

For $n \geq 2$, we have $S_\infty \hookrightarrow \mathrm{LP}(G, n, k)$.

Some properties : $\mathrm{LP}(G, n, k)$

For $n \geq 2$, we have $S_\infty \hookrightarrow \mathrm{LP}(G, n, k)$.

This means that RTM is not residually finite, and that it contains all finite groups.

Some properties : $\mathrm{LP}(G, n, k)$

For $n \geq 2$, we have $S_\infty \hookrightarrow \mathrm{LP}(G, n, k)$.

This means that RTM is not residually finite, and that it contains all finite groups.

$\mathrm{LP}(G, n, k)$ is locally finite.

Some properties : $\mathrm{LP}(G, n, k)$

For $n \geq 2$, we have $S_\infty \hookrightarrow \mathrm{LP}(G, n, k)$.

This means that RTM is not residually finite, and that it contains all finite groups.

$\mathrm{LP}(G, n, k)$ is locally finite.

In particular, for $n \geq 2$ $\mathrm{LP}(G, n, k)$ is amenable and not finitely generated.

Some properties : $\mathrm{OB}(\mathbb{Z}^d, n, k)$

Now let's add the shift. Recall that $\mathrm{OB}(G, n, k) = \langle \mathrm{LP}, \mathrm{Shift} \rangle$.

Some properties : $\mathrm{OB}(\mathbb{Z}^d, n, k)$

Now let's add the shift. Recall that $\mathrm{OB}(G, n, k) = \langle \mathrm{LP}, \mathrm{Shift} \rangle$.

$$\mathrm{OB}(G, n, k) \text{ is amenable } \iff G \text{ is amenable.}$$

Some properties : $\mathrm{OB}(\mathbb{Z}^d, n, k)$

Now let's add the shift. Recall that $\mathrm{OB}(G, n, k) = \langle \mathrm{LP}, \mathrm{Shift} \rangle$.

$$\mathrm{OB}(G, n, k) \text{ is amenable } \iff G \text{ is amenable.}$$

Proof : Use the short exact sequence

$$1 \longrightarrow \mathrm{LP}(G, n, k) \longrightarrow \mathrm{OB}(G, n, k) \longrightarrow G \longrightarrow 1.$$

Some properties : $\mathrm{RFA}(\mathbb{Z}^d, n, k)$

Recall that $\mathrm{RFA}(G, n, k)$ is the subgroup of machines which do not modify the tape. Note that if $[[\sigma]]$ is the fullgroup of (Σ^G, σ) then $[[\sigma]] \cong \mathrm{RFA}(G, n, 1)$.

Theorem

For $n \geq 2$, countable and not locally finite G we have that

$$\underbrace{\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}}_{m \text{ times}} \hookrightarrow \mathrm{RFA}(G, n, k)$$

Some properties : $\mathrm{RFA}(\mathbb{Z}^d, n, k)$

Recall that $\mathrm{RFA}(G, n, k)$ is the subgroup of machines which do not modify the tape. Note that if $[[\sigma]]$ is the fullgroup of (Σ^G, σ) then $[[\sigma]] \cong \mathrm{RFA}(G, n, 1)$.

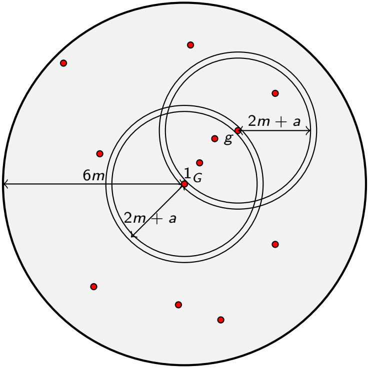
Theorem

For $n \geq 2$, countable and not locally finite G we have that

$$\underbrace{\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}}_{m \text{ times}} \hookrightarrow \mathrm{RFA}(G, n, k)$$

Proof : Blackboard.

Some properties : $\mathrm{RFA}(\mathbb{Z}^d, n, k)$



Some properties : $\mathrm{RFA}(\mathbb{Z}^d, n, k)$

Theorem

For $n \geq 2$, countable and not locally finite G we have that

$$\underbrace{\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}}_{m \text{ times}} \hookrightarrow \mathrm{RFA}(G, n, k)$$

In particular, this means that RFA and RTM are not amenable in this case.

Some properties : $\mathrm{RFA}(\mathbb{Z}^d, n, k)$

Theorem

For $n \geq 2$, countable and not locally finite G we have that

$$\underbrace{\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}}_{m \text{ times}} \hookrightarrow \mathrm{RFA}(G, n, k)$$

In particular, this means that RFA and RTM are not amenable in this case.

Theorem

For $n \geq 2$, infinite and residually finite G we have that $\mathrm{RFA}(G, n, k)$ is residually finite but not finitely generated.

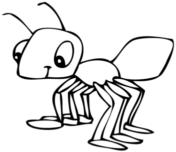
Some properties : $\mathsf{EL}(\mathbb{Z}^d, n, k)$ and $\mathrm{RTM}(\mathbb{Z}^d, n, k)$

$\mathsf{EL}(\mathbb{Z}^d, n, k) = \langle \mathrm{LP}(\mathbb{Z}^d, n, k), \mathrm{RFA}(\mathbb{Z}^d, n, k) \rangle$ is the subgroup of elementary Turing machines.

Some properties : $\mathsf{EL}(\mathbb{Z}^d, n, k)$ and $\mathrm{RTM}(\mathbb{Z}^d, n, k)$

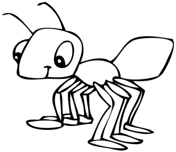
$\mathsf{EL}(\mathbb{Z}^d, n, k) = \langle \mathrm{LP}(\mathbb{Z}^d, n, k), \mathrm{RFA}(\mathbb{Z}^d, n, k) \rangle$ is the subgroup of elementary Turing machines.

Example : Langton's ant $\in \mathsf{EL}(\mathbb{Z}^2, 2, 4)$.



Some properties : $\mathrm{EL}(\mathbb{Z}^d, n, k)$ and $\mathrm{RTM}(\mathbb{Z}^d, n, k)$

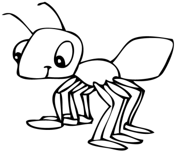
$\mathrm{EL}(\mathbb{Z}^d, n, k) = \langle \mathrm{LP}(\mathbb{Z}^d, n, k), \mathrm{RFA}(\mathbb{Z}^d, n, k) \rangle$ is the subgroup of elementary Turing machines.
Example : Langton's ant $\in \mathrm{EL}(\mathbb{Z}^2, 2, 4)$.



Question : Is $\mathrm{EL}(\mathbb{Z}^d, n, k) = \mathrm{RTM}(\mathbb{Z}^d, n, k)$?

Some properties : $\mathrm{EL}(\mathbb{Z}^d, n, k)$ and $\mathrm{RTM}(\mathbb{Z}^d, n, k)$

$\mathrm{EL}(\mathbb{Z}^d, n, k) = \langle \mathrm{LP}(\mathbb{Z}^d, n, k), \mathrm{RFA}(\mathbb{Z}^d, n, k) \rangle$ is the subgroup of elementary Turing machines.
Example : Langton's ant $\in \mathrm{EL}(\mathbb{Z}^2, 2, 4)$.



Question : Is $\mathrm{EL}(\mathbb{Z}^d, n, k) = \mathrm{RTM}(\mathbb{Z}^d, n, k)$?

For $n \geq 2$, $\alpha(\mathrm{EL}(\mathbb{Z}^d, n, k)) = \alpha(\mathrm{RFA}(\mathbb{Z}^d, n, k))$ has bounded denominator. In particular $\mathrm{EL} \subsetneq \mathrm{RTM}$.

Computability properties

Given a finite rules : f, f' :

- It is decidable (in any model) whether $T_f = T_{f'}$.
- We can effectively calculate a rule for $T_f \circ T_{f'}$.
- It is decidable whether T_f is reversible.
- If it is, we can effectively compute a rule for T_f^{-1}.

Computability properties

Given a finite rules : f, f' :

- It is decidable (in any model) whether $T_f = T_{f'}$.
- We can effectively calculate a rule for $T_f \circ T_{f'}$.
- It is decidable whether T_f is reversible.
- If it is, we can effectively compute a rule for T_f^{-1}.

$\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is a recursively presented group with decidable word problem.

Computability properties

Given a finite rules : f, f' :

- It is decidable (in any model) whether $T_f = T_{f'}$.
- We can effectively calculate a rule for $T_f \circ T_{f'}$.
- It is decidable whether T_f is reversible.
- If it is, we can effectively compute a rule for T_f^{-1}.

$\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is a recursively presented group with decidable word problem.

What can we say about the torsion ($\exists n$ such that $T^n = 1$) problem ?

Back to the target : $TP(\mathrm{Aut}(A^{\mathbb{Z}}))$ is undecidable.

We want to prove that the torsion problem is undecidable for a f.g. subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$. The sketch is as follows :

1. The torsion problem for reversible classical Turing machines is undecidable [Kari, Ollinger 2008].

Back to the target : $TP(\mathrm{Aut}(A^{\mathbb{Z}}))$ is undecidable.

We want to prove that the torsion problem is undecidable for a f.g. subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$. The sketch is as follows :

1. The torsion problem for reversible classical Turing machines is undecidable [Kari, Ollinger 2008].
2. Classical Turing machines embed into $\mathrm{EL}(\mathbb{Z}, n, k)$.

Back to the target : $TP(\mathrm{Aut}(A^{\mathbb{Z}}))$ is undecidable.

We want to prove that the torsion problem is undecidable for a f.g. subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$. The sketch is as follows :

1. The torsion problem for reversible classical Turing machines is undecidable [Kari, Ollinger 2008].
2. Classical Turing machines embed into $\mathrm{EL}(\mathbb{Z}, n, k)$.
3. $\mathrm{EL}(\mathbb{Z}, n, k)$ is finitely generated.

Back to the target : $TP(\mathrm{Aut}(A^{\mathbb{Z}}))$ is undecidable.

We want to prove that the torsion problem is undecidable for a f.g. subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$. The sketch is as follows :

1. The torsion problem for reversible classical Turing machines is undecidable [Kari, Ollinger 2008].
2. Classical Turing machines embed into $\mathrm{EL}(\mathbb{Z}, n, k)$.
3. $\mathrm{EL}(\mathbb{Z}, n, k)$ is finitely generated.
4. There exists a "torsion preserving function" from $\mathrm{EL}(\mathbb{Z}, n, k)$ to $\mathrm{Aut}(A^{\mathbb{Z}})$

$$\text{Classical} \hookrightarrow \text{EL}'' \hookrightarrow \text{''}\mathrm{Aut}(A^{\mathbb{Z}})$$

$\mathrm{OB}(\mathbb{Z}^d, n, k)$ is finitely generated.

This proof is inspired both on the existence of strongly universal reversible gates for permutations of Σ^m and the Juschenko Monod proof for the fullgroup of minimal actions.
A controlled swap is a transposition (s, t) where s, t have Hamming distance 1 in $Q \times \Sigma^m$.

Theorem

The group generated by the applications of controlled swaps of $Q \times \Sigma^4$ at arbitrary positions generates $Sym(Q \times \Sigma^m)$ if $|\Sigma|$ is odd and $Alt(Q \times \Sigma^m)$ if it's even.
Corollary : $[Sym(Q \times \Sigma^m)]_{m+1} \subset \langle [Sym(Q \times \Sigma^4)]_{m+1} \rangle$.

$\mathrm{OB}(\mathbb{Z}^d, n, k)$ is finitely generated.

Using this result, a generating set can be constructed :

- $A_1 =$ Shifts T_{e_i} for $\{e_i\}_{i \leq d}$ a base of $\mathbb{Z}^d$.
- $A_2 =$All $T_\pi \in \mathrm{LP}(\mathbb{Z}^d, n, k)$ of fixed support $E \subset \mathbb{Z}^d$ of size 4.
- $A_3 =$ The swaps of symbols in positions $(\vec{0}, e_i)$.

$\mathrm{EL}(\mathbb{Z}, n, k)$ is finitely generated.

$$\mathrm{EL}(\mathbb{Z}, n, k) = \langle LP(\mathbb{Z}, n, k), \mathrm{RFA}(\mathbb{Z}, n, k) \rangle = \langle \mathrm{OB}(\mathbb{Z}, n, k), \mathrm{RFA}(\mathbb{Z}, n, k) \rangle$$

$\mathrm{EL}(\mathbb{Z}, n, k)$ is finitely generated.

$$\mathrm{EL}(\mathbb{Z}, n, k) = \langle LP(\mathbb{Z}, n, k), \mathrm{RFA}(\mathbb{Z}, n, k)\rangle = \langle \mathrm{OB}(\mathbb{Z}, n, k), \mathrm{RFA}(\mathbb{Z}, n, k)\rangle$$

We can show that $\mathrm{RFA}(\mathbb{Z}, n, k)$ is generated by orbitwise shifts and controlled position swaps.

1. f is orbitwise shift is $\forall x \in X\ \exists k \in \mathbb{Z}$ such that $f(\sigma^n(x)) = \sigma^{n+k}(x)$.
2. f is controlled position swap if for some $u, v \in \Sigma^*$, $f(xu.avy) = xua.vy$ and $f(xua.vy) = xu.avy$.

$\mathrm{EL}(\mathbb{Z}, n, k)$ is finitely generated.

$$\mathrm{EL}(\mathbb{Z}, n, k) = \langle LP(\mathbb{Z}, n, k), \mathrm{RFA}(\mathbb{Z}, n, k)\rangle = \langle \mathrm{OB}(\mathbb{Z}, n, k), \mathrm{RFA}(\mathbb{Z}, n, k)\rangle$$

We can show that $\mathrm{RFA}(\mathbb{Z}, n, k)$ is generated by orbitwise shifts and controlled position swaps.

1. f is orbitwise shift is $\forall x \in X\ \exists k \in \mathbb{Z}$ such that $f(\sigma^n(x)) = \sigma^{n+k}(x)$.
2. f is controlled position swap if for some $u, v \in \Sigma^*$, $f(xu.avy) = xua.vy$ and $f(xua.vy) = xu.avy$.

In the fullshift, orbitwise shifts are precisely the shifts. So we only need to implement controlled position swaps [technical].

Definition

Let G and H be groups. We say a function $\phi : G \to H$ is a blurphism if the following holds : If $F \subset G^*$ is finite, then the group $\langle w \mid w \in F \rangle \leq G$ is infinite if and only if the group $\langle \phi(w_1)\phi(w_2) \cdots \phi(w_{|w|}) \mid w \in F \rangle$ is infinite.

From $\mathrm{EL}(\mathbb{Z}, n, k)$ to $\mathrm{Aut}(A^{\mathbb{Z}})$

Definition

Let G and H be groups. We say a function $\phi : G \to H$ is a blurphism if the following holds : If $F \subset G^*$ is finite, then the group $\langle w \mid w \in F \rangle \leq G$ is infinite if and only if the group $\langle \phi(w_1)\phi(w_2) \cdots \phi(w_{|w|}) \mid w \in F \rangle$ is infinite.

Lemma

If G has a finitely generated subgroup G' with generating set B with undecidable torsion problem and there is a computable blurphism $\phi : G \to H$, then the subgroup H' of H generated by $\phi(b)$ where $b \in B$ has undecidable torsion problem.

From $\mathrm{EL}(\mathbb{Z}, n, k)$ to $\mathrm{Aut}(A^{\mathbb{Z}})$

Definition

Let G and H be groups. We say a function $\phi : G \to H$ is a blurphism if the following holds : If $F \subset G^*$ is finite, then the group $\langle w \mid w \in F \rangle \leq G$ is infinite if and only if the group $\langle \phi(w_1)\phi(w_2)\cdots\phi(w_{|w|}) \mid w \in F \rangle$ is infinite.

Lemma

If G has a finitely generated subgroup G' with generating set B with undecidable torsion problem and there is a computable blurphism $\phi : G \to H$, then the subgroup H' of H generated by $\phi(b)$ where $b \in B$ has undecidable torsion problem.

A better name than blurphism is needed, any ideas ?

Construction of the blurphism

- Let $A = \{\Sigma^2 \times (\{\leftarrow, \rightarrow\} \cup (Q \times \{\uparrow, \downarrow\}))\}$.

Construction of the blurphism

- Let $A = \{\Sigma^2 \times (\{\leftarrow, \rightarrow\} \cup (Q \times \{\uparrow, \downarrow\}))\}$.
- Parse the third layer into zones $(\leftarrow^* \, (q, a) \rightarrow^* \mid \leftarrow^* \rightarrow^*)^*$.

Construction of the blurphism

- Let $A = \{\Sigma^2 \times (\{\leftarrow, \rightarrow\} \cup (Q \times \{\uparrow, \downarrow\}))\}$.
- Parse the third layer into zones $(\leftarrow^* (q, a) \rightarrow^* \mid \leftarrow^* \rightarrow^*)^*$.
- Define ϕ to act as a conveyor belt [Blackboard]

Construction of the blurphism

- Let $A = \{\Sigma^2 \times (\{\leftarrow, \rightarrow\} \cup (Q \times \{\uparrow, \downarrow\}))\}$.
- Parse the third layer into zones $(\leftarrow^* (q, a) \rightarrow^* \mid \leftarrow^* \rightarrow^*)^*$.
- Define ϕ to act as a conveyor belt [Blackboard]
- ϕ is a computable blurphism.

Construction of the blurphism

- Let $A = \{\Sigma^2 \times (\{\leftarrow, \rightarrow\} \cup (Q \times \{\uparrow, \downarrow\}))\}$.
- Parse the third layer into zones $(\leftarrow^* (q, a) \rightarrow^* \mid \leftarrow^* \rightarrow^*)^*$.
- Define ϕ to act as a conveyor belt [Blackboard]
- ϕ is a computable blurphism.

Therefore $\phi(\mathrm{EL}(\mathbb{Z}, n, k))$ is a finitely generated subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ with undecidable torsion problem. As $\mathrm{Aut}(A^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ the same is valid for any automorphism group of a fullshift.

The torsion problem for RFA

$\mathrm{RFA}(\mathbb{Z}, n, k)$ has decidable torsion problem.

Proof : As $\mathbb{Z}$ is two-ended, any non-torsion machine must shift to the left or right in at least a periodic configuration.

The torsion problem for RFA

$\mathrm{RFA}(\mathbb{Z}, n, k)$ has decidable torsion problem.

Proof : As $\mathbb{Z}$ is two-ended, any non-torsion machine must shift to the left or right in at least a periodic configuration.

Theorem

$\mathrm{RFA}(\mathbb{Z}^d, n, k)$ has a finitely generated subgroup with undecidable torsion problem for $d, n \geq 2$.

The torsion problem for RFA

$\mathrm{RFA}(\mathbb{Z}, n, k)$ has decidable torsion problem.

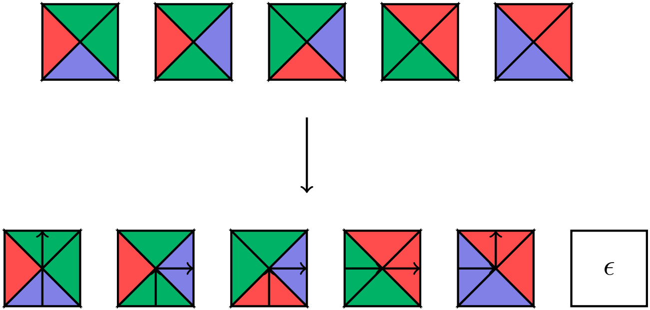
Proof : As $\mathbb{Z}$ is two-ended, any non-torsion machine must shift to the left or right in at least a periodic configuration.

Theorem

$\mathrm{RFA}(\mathbb{Z}^d, n, k)$ has a finitely generated subgroup with undecidable torsion problem for $d, n \geq 2$.

Proof : Reduction to the snake tiling problem, which reduces to the domino problem for $\mathbb{Z}^d$.

The snake problem



Can we tile the plane in a way which produces a bi-infinite path ?

The snake problem

Theorem (Kari)

The snake tiling problem is undecidable.

The proof uses a plane filling curve generated by a substitution.

The snake problem

Theorem (Kari)

The snake tiling problem is undecidable.

The proof uses a plane filling curve generated by a substitution.

For every instance of the snake tiling problem, one can construct $T \in \mathrm{RFA}$ which walks the path of the snake, and turns back if it encounters a problem.

The torsion problem for RFA : Cheating version

We'll first do it by cheating : Arbitrary alphabet τ as an instance of the snake tiling problem and at least two states L, R.

- Let t be the tile at $(0, 0)$. If $t = \epsilon$, do nothing.
- Otherwise :
  - If the state is L. Check the tile in the direction $\texttt{left}(t)$. If it matches correctly with t move the head to that position, otherwise switch the state to R.
  - If the state is R. Check the tile in the direction $\texttt{right}(t)$. If it matches correctly with t move the head to that position, otherwise switch the state to L

The torsion problem for RFA : The real deal

We are going to code everything in a binary alphabet and use no states.

1	1	1	1	1	1	1
1	0	0	0	0	0	1
1	0	b_1	b_2	b_3	0	1
1	0	r_1	r_2	b_4	0	1
1	0	l_1	l_2	b_5	0	1
1	0	0	0	0	0	1
1	1	1	1	1	1	1

The torsion problem for RFA : The real deal

Consider the group spanned by the following machines :

1. $\{T_{\vec{v}}\}_{v \in D}$ that walks in the direction $\vec{v} \in D$ independently of the configuration.
2. $T_{\mathtt{walk}}$ that walks along the direction codified by l_1, l_2 or r_1, r_2 depending on the direction bit.
3. $\{g_c\}_{c \in C}$ that flips the direction bit if the current pattern is $c \in C$,
4. $\{h_c\}_{c \in C}$ that flips the auxiliary bit if the current pattern is $c \in C$,
5. $\{g_{+,c}\}_{c \in C}$ that adds the auxiliary bit to the direction bit if the current pattern is $c \in C$, and
6. $\{h_{+,c}\}_{c \in C}$ that adds the direction bit to the auxiliary bit if the current pattern is $c \in C$,

The torsion problem for RFA : The real deal

The previous group spans the machines g_p and h_p for patterns p composed of fragments of c in compatible positions.

The torsion problem for RFA : The real deal

The previous group spans the machines g_p and h_p for patterns p composed of fragments of c in compatible positions.

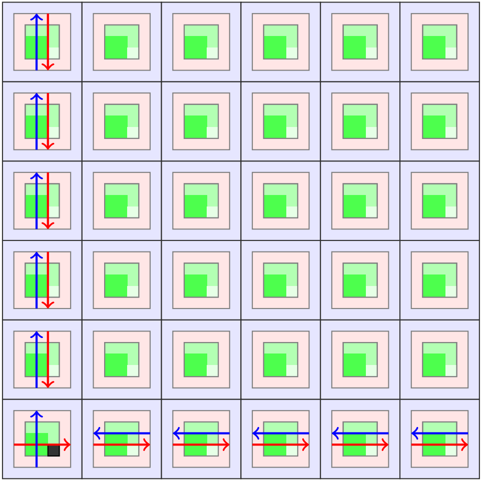
$$g_{p^*} = (T_{-7\vec{v}} \circ g_{+,c} \circ T_{7\vec{v}} \circ h_{p^*_{F\setminus\{\vec{v}\}}})^2.$$

$$h_{p^*} = (T_{-7\vec{v}} \circ h_{+,c} \circ T_{7\vec{v}} \circ g_{p^*_{F\setminus\{\vec{v}\}}})^2.$$

Finally, we use these machines to code the first ones.

The torsion problem for RFA : The real deal

$$\mathcal{M}(t) =$$



The torsion problem for RFA : The real deal

$$T^* = (T_{\texttt{walk}})^M \circ \prod_{p^* \in \mathcal{M}} g_{p^*} \circ \prod_{c \in C} g_c$$

Acts as the first machine, but using these coded macrotiles.

The torsion problem for RFA : The real deal

$$T^* = (T_{\texttt{walk}})^M \circ \prod_{p^* \in \mathcal{M}} g_{p^*} \circ \prod_{c \in C} g_c$$

Acts as the first machine, but using these coded macrotiles.

Corollary

Let $d \geq 2$ and σ be the shift action of $\mathbb{Z}^d$ over a full shift $\mathcal{A}^{\mathbb{Z}^d}$ where $|\mathcal{A}| \geq 2$. Then the full group $[[\sigma]]$ contains a finitely generated subgroup with undecidable torsion problem.

Thank you for your attention !