Finite Semigroups of Cellular Automata

Alonso Castillo-Ramirez

Joint work with Maximilien Gadouleau

Durham University
School of Engineering and Computing Sciences

alonso.castillo-ramirez@durham.ac.uk

November 2015

1. Cellular Automata and Groups

Notation

- Let A be **any set**. We call the elements of A "states".
- Let G be **any group** (i.e. a set equipped with an associative binary operation, an identity and an inverse for each element).
- Let $L_g : G \to G$ be the **left multiplication map** by $g \in G$ (i.e. $L_g(h) := gh$ for any $h \in G$).
- A map $x : G \to A$ is called a **configuration** over G and A.
- Denote by $A^G := \{x : G \to A\}$ the set of **all configurations** over G and A.

Cellular Automata (CA)

The following definition of **cellular automaton** appears in *Cellular Automata and Groups* by T. Ceccherini-Silberstein and M. Coornaert (Springer, 2010).

Definition

Let G be a group and A a set. A **cellular automaton** over G and A is a **transformation** $\tau : A^G \to A^G$ such that there is a finite subset $S \subseteq G$ and a local map $\tau_e : A^S \to A$ satisfying

$$\tau(x)(g) = \tau_e((x \circ L_g)|_S),$$

for all $x \in A^G$, $g \in G$.

Cellular Automata (CA)

- In the **classical setting**, CA are studied over $G = \mathbb{Z}^d$, where $d \in \mathbb{N}$ is called the **dimension**, and A is a finite set.
- For example, John Conway's **Game of Life** is a 2-dimensional cellular automaton over $G = \mathbb{Z}^2$ and $A = \{0, 1\}$.
- The Game of Life is known to be **Turing complete** (i.e. it is capable of simulate any Turing machine).
- Consider the set of all CA over G and A:

$$\mathrm{CA}(G; A) := \left\{ \tau : A^G \to A^G \mid \tau \text{ is a cellular automaton} \right\}.$$

Basic Properties

- The set $\mathrm{CA}(G; A)$ is a **semigroup** (i.e. it is closed under composition of maps).
- Every $\tau \in \mathrm{CA}(G; A)$ is
  1. G-**equivariant**: $\tau(x \circ L_g) = \tau(x) \circ L_g$, $\forall x \in A^G, g \in G$.
  2. **Continuous** in the *prodiscrete* topology of A^G (i.e. the product of the discrete topology of A).
- Equivariance and continuity characterise CA when A is a finite set (**Curtis-Hedlund theorem**).
- If $\tau \in \mathrm{CA}(G; A)$ is bijective, then $\tau^{-1} \in \mathrm{CA}(G; A)$.

Connections to Amenable Groups

Let E be a set. A map $\mu : \mathcal{P}(E) \to [0,1]$ is a **finitely additive probability measure** if:

(i) $\mu(E) = 1$.

(ii) $\mu(B \cup C) = \mu(B) + \mu(C)$ for all $B, C \subseteq E$ with $B \cap C = \emptyset$.

Definition (von Neumann '29)

A group G is **amenable** if there is a finitely additive probability measure $\mu : \mathcal{P}(G) \to [0,1]$ that is **left invariant** (i.e. $\forall g \in G$, $B \subseteq G$, we have $\mu(B) = \mu(gB)$).

Finite, abelian and solvable groups are all amenable. However, any group containing the free group F_2 is not amenable.

Connections to Amenable Groups

- **Almost equal**: $x \approx y$, for $x, y \in A^G$, if the set $\{g \in G : x(g) \neq y(g)\}$ is finite.
- **Pre-injective**: $\tau \in \mathrm{CA}(G; A)$ is pre-injective if $\tau|_C$ is injective for any equivalence class $C \in A^G / \approx$.

Theorem (Ceccherini-Silberstein, Machì, Scarabotti '99)

Let G be an amenable group and A a finite set. A cellular automation $\tau \in \mathrm{CA}(G; A)$ is surjective iff it is pre-injective.

Theorem (Bartholdi '10)

A group G is amenable iff, for every finite A, every surjective $\tau \in \mathrm{CA}(G; A)$ is pre-injective.

Other Algebraic Results

- **Surjunctive groups**: G is *surjunctive* if for every finite A, every injective $\tau \in \mathrm{CA}(G; A)$ is surjective. Is every group surjunctive? (Open question).
- **Linear cellular automata**: if V is a vector space, $\mathrm{LCA}(G; V) := \mathrm{CA}(G; V) \cap \mathrm{End}(V)$.
- **Locally finite group**: G is *locally finite* if every finitely generated subgroup is finite.

Theorem (Ceccherini-Silberstein, Coornaert '09)

A group G is locally finite iff, for every finite-dimensional V, every surjective $\tau \in \mathrm{LCA}(G; V)$ is injective.

3. Cellular Automata and Semigroups

The Semigroup $\mathrm{CA}(G; A)$

- When G and A are finite, say $|G| = n$ and $|A| = q$, then $\mathrm{CA}(G; A)$ is a **finite semigroup** of size q^{q^n}.
- In this setting, we may ask some **new questions** that are typical in finite semigroup theory.
- The **rank** of a finite semigroup S, denoted by $\mathrm{Rank}(S)$, is the cardinality of a smallest generating set of S:

$$\mathrm{Rank}(S) := \min\{|H| : H \subseteq S \text{ and } \langle H \rangle = S\}.$$

- **Problem**: Determine $\mathrm{Rank}(\mathrm{CA}(G; A))$ for any G, A finite.

Ranks of Semigroups of Transformations

Let X be a finite set with $|X| = m$.

- $\mathrm{Rank}(\mathrm{Tran}(X)) = \mathrm{Rank}(\mathrm{Sym}(X)) + 1 = 3$.
- $\mathrm{Rank}(\mathrm{Sing}(X)) = \frac{1}{2}m(m-1)$ (Gomes-Howie '87).
- $\mathrm{Rank}\left(\{f \in \mathrm{Tran}(X) : |f(X)| \leq r\}\right) = S(m, r)$, the Stirling number of the second kind (Howie-McFadden '90).
- $\mathrm{Rank}(\mathrm{Tran}(X, \mathcal{O})) = 4$, where $\mathcal{O}$ is a uniform partition of X (Araújo-Schneider '09).
- $\mathrm{Rank}(\mathrm{Tran}(X, \mathcal{O}))$ is known, where $\mathcal{O}$ is an arbitrary partition of X (Araújo-Bents-Mitchell-Schneider '15).

Cellular Automata over Cyclic Groups

Let $G = \mathbb{Z}_n$ be the **cyclic group** of order $n \geq 2$ and A is a finite set of size $q \geq 2$.

Lemma

Let $\sigma : A^n \to A^n$ be the transformation

$$\sigma(x_1, x_2, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

Then,

$$\mathrm{CA}(\mathbb{Z}_n; A) = C_{\mathrm{Tran}(A^n)}(\sigma) := \{\tau \in \mathrm{Tran}(A^n) : \tau\sigma = \sigma\tau\}$$

Corollary

$\mathrm{CA}(\mathbb{Z}_n; A) \leq \mathrm{Tran}(A^n, \mathcal{O})$, *where $\mathcal{O}$ is the set of orbits of σ.*

Cellular Automata over Cyclic Groups

Let $\mathcal{O}$ be the set of orbits of $\sigma : A^n \to A^n$, as defined before.

- For every $P \in \mathcal{O}$, $|P|$ divides n.
- For every $\tau \in \mathrm{CA}(\mathbb{Z}_n; A)$ and $P \in \mathcal{O}$, we have $\tau(P) \in \mathcal{O}$ and $|\tau(P)|$ divides $|P|$.
- The number of orbits in $\mathcal{O}$ of size $d \mid n$ is given by **Moreau's necklace-counting function**:

$$\alpha(d, q) = \frac{1}{d} \sum_{b|d} \mu\left(\frac{d}{b}\right) q^b,$$

where μ is the classic Möbius function.

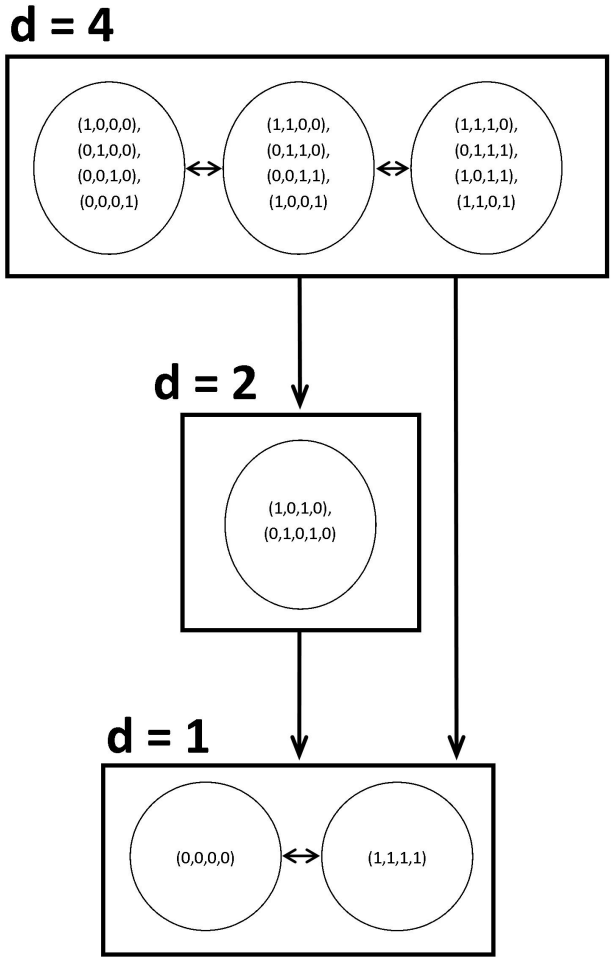
Relative Rank and Invertible CA

- **Relative rank**: The relative rank of $U \subseteq S$ is $\mathrm{Rank}(S : U) = \min\{|V| : V \subseteq S \text{ and } \langle U, V\rangle = S\}$.
- **Invertible CA**: $\mathrm{ICA}(G; A) := \mathrm{CA}(G; A) \cap \mathrm{Sym}(A^G)$.
- $\mathrm{Rank}(\mathrm{CA}(G; A)) = \mathrm{Rank}(\mathrm{CA}(G; A) : \mathrm{ICA}(G; A)) + \mathrm{Rank}(\mathrm{ICA}(G; A))$.
- If $d_1, d_2, \ldots, d_\ell$ are the non-one divisors of n, then:

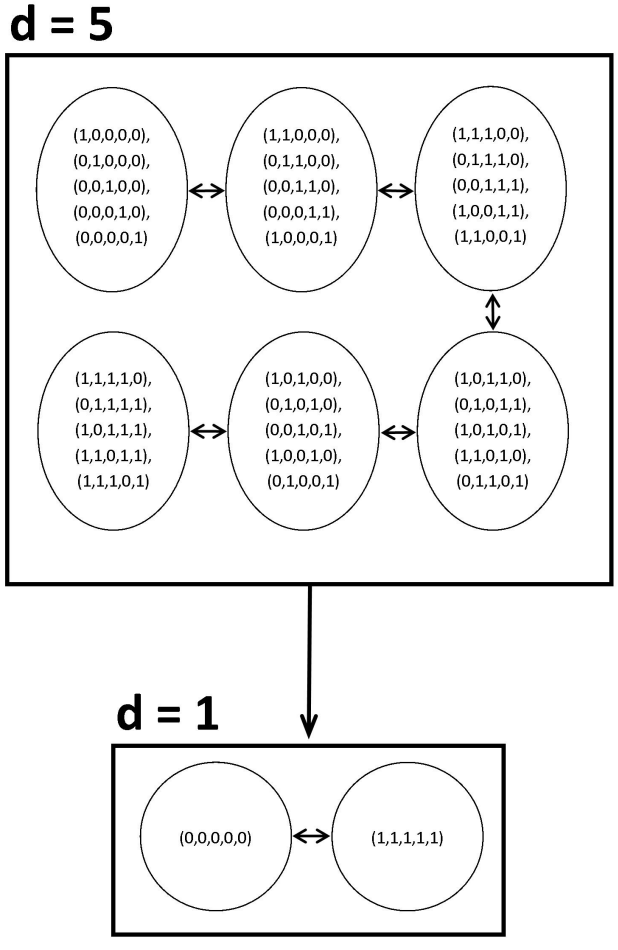
$$\mathrm{ICA}(\mathbb{Z}_n; A) \cong (\mathbb{Z}_{d_1} \wr \mathrm{Sym}_{\alpha_1}) \times \cdots \times (\mathbb{Z}_{d_\ell} \wr \mathrm{Sym}_{\alpha_\ell}) \times \mathrm{Sym}_q,$$

where $\alpha_i := \alpha(d_i, q)$.

Examples

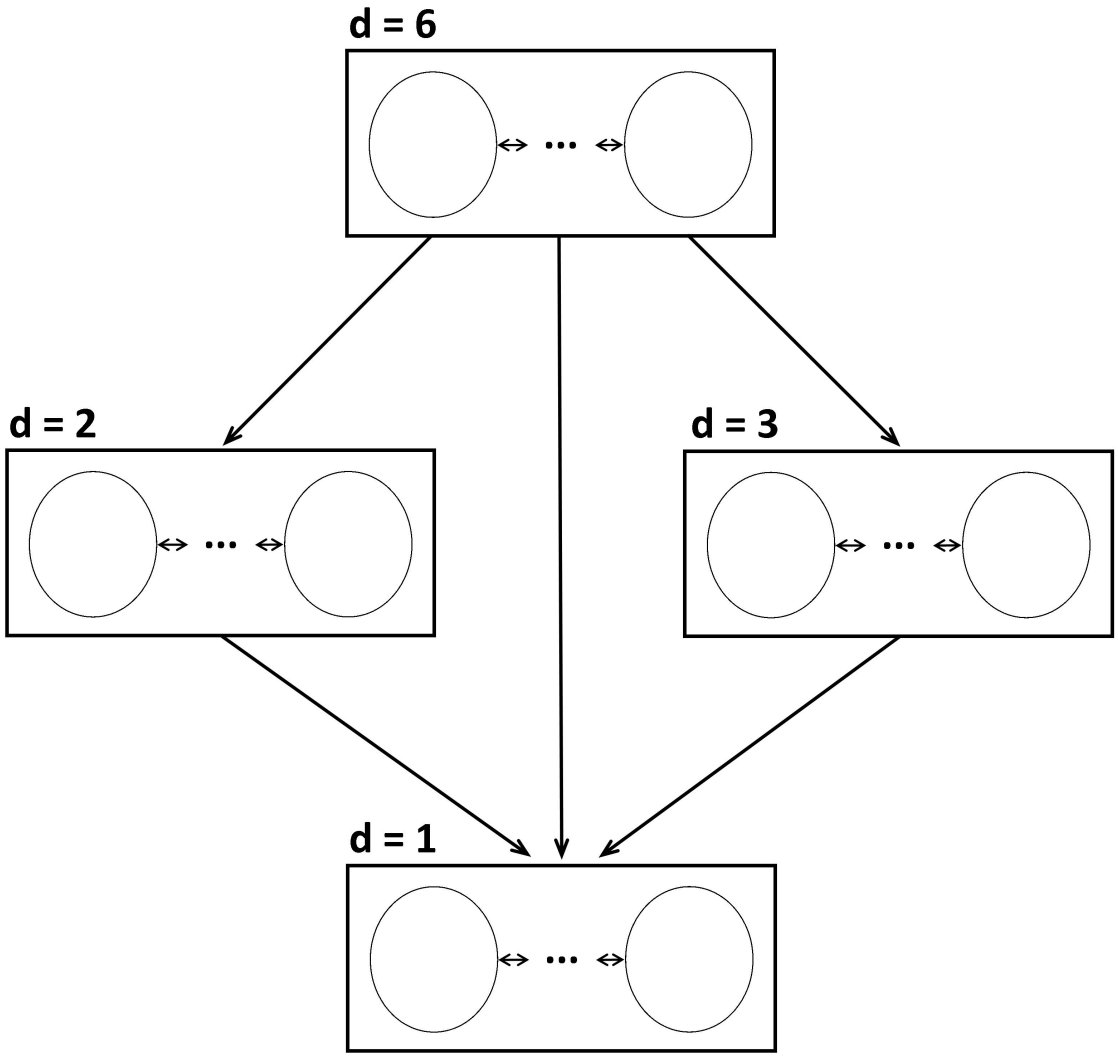


(a) Case $n = 4$, $q = 2$



(b) Case $n = 5$, $q = 2$

Examples: Case $n = 6$, $q \geq 2$



Main Result 1

Theorem (CR, Gadouleau '15+)

Let $k \geq 1$ be an integer, p an odd prime, and A a finite set of size $q \geq 2$. Then:

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_p; A)) = 5;$$

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_{2^k}; A)) = \begin{cases} 4, & \text{if } (k,q) = (1,2); \\ \frac{1}{2}(k+1)(k+4) + k, & \text{otherwise;} \end{cases}$$

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_{2^k p}; A)) = \frac{3}{2}(k+1)(k+4).$$

Main Result 2

For an integer $n \geq 2$, let

- $d(n)$ be the number of **divisors** of n (including 1 and n),
- $d_+(n)$ be the number of **even divisors** of n,
- $E(n)$ be the number of edges in the **divisibility graph** of n.

Theorem (CR, Gadouleau '15+)

Let A be a finite set of size $q \geq 2$ and $n \geq 2$. Then:

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_n; A)) = d(n) + d_+(n) + E(n) + \epsilon(n, q),$$

where $0 \leq \epsilon(n, q) \leq \max\{0, d(n) - d_+(n) - 2\}$.

Remarks on the Proof

- In general, $\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_n; A) : \mathrm{ICA}(\mathbb{Z}_n; A)) = E(n)$.
- The **main obstacle** to generalise our results is to determine $\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_n; A))$.
- When $n = p$ is a prime, **representation theoretic** results help to calculate this rank.
- Lemma. The only non-zero Sym_α-invariant submodules of $(\mathbb{Z}_p)^\alpha$ are

$$U_1 := \{(a, \ldots, a) : a \in \mathbb{Z}_p\},$$
$$U_2 := \{(a_1, \ldots, a_\alpha) \in (\mathbb{Z}_p)^\alpha : \textstyle\sum_{i=1}^{\alpha} a_i = 0\}.$$

Open Problems and Questions

1. For any $d_i, \alpha_i, q \geq 2$, determine the rank of

$$(\mathbb{Z}_{d_1} \wr \mathrm{Sym}_{\alpha_1}) \times \cdots \times (\mathbb{Z}_{d_\ell} \wr \mathrm{Sym}_{\alpha_\ell)}) \times \mathrm{Sym}_q.$$

2. For any $n, d \geq 2$, determine $\mathrm{Rank}(\mathrm{CA}((\mathbb{Z}_n)^d; A))$.

3. For any **finite abelian** group G, determine $\mathrm{Rank}(\mathrm{CA}(G; A))$.

4. For any finite group G and any **finite field** $\mathbb{F}$, determine $\mathrm{Rank}(\mathrm{LCA}(G; \mathbb{F}^d))$.

5. What other **semigroup theoretic properties** can be investigated in $\mathrm{CA}(G; A)$?

Thanks for listening!

A. Castillo-Ramirez and M. Gadouleau,
Ranks of finite semigroups of one-dimensional cellular automata,
arXiv:1510.00197.