International Conference on Semigroups and Automata 2016

Celebrating the 60th birthday of Jorge Almeida and Garcinda Gomes

University of Lisbon

Ranks of Finite Semigroups of Cellular Automata

Alonso Castillo-Ramirez

Joint work with Maximilien Gadouleau

Durham University

Notation

- Let A be **any set** and let G be **any group**.
- Right multiplication map: for $g \in G$, define $R_g : G \to G$ by $(h)R_g := hg$.
- 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.

Definition of Cellular Automata

Definition (von Neumann, Ceccherini-Silberstein, Coornaert, et al)

Let G be a group and A a set. A **cellular automaton** (CA) over G and A is a **transformation**

$$\tau : A^G \to A^G$$

such that:

($\star$) There is a **finite subset** $S \subseteq G$ and a **local map** $\mu : A^S \to A$ satisfying

$$(g)(x)\tau = ((R_g \circ x)|_S)\,\mu, \quad \forall g \in G, x \in A^G.$$

Example: Rule 110

- Let $G = \mathbb{Z}$, and $A = \{0, 1\}$.
- Let $S = \{-1, 0, 1\} \subseteq G$ and define $\mu : A^S \to A$ by

$x \in A^S$	111	110	101	100	011	010	001	000
$(x)\mu$	0	1	1	0	1	1	1	0

- The CA $\tau : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ defined by S and μ is called **Rule 110**.
- E.g., $(\dots 0001000 \dots)\tau = \dots 0011000 \dots$.
- It is known that Rule 110 is **Turing complete** (Cook '04).

Classical Results

- Another example: John Conway's **Game of Life** is a CA over $G = \mathbb{Z}^2$ and $A = \{0, 1\}$.
- **Classical setting**: $G = \mathbb{Z}^d$, $d \in \mathbb{N}$, and A is finite.
- Classical lines of research on CA include:
  1. Universality of CA (e.g. Game of Life and Rule 110 are Turing complete).
  2. Characterisation of surjective and injective CA (e.g. Garden of Eden theorems).
  3. Dynamical behaviour (e.g. orbits, fixed points).
  4. Linear CA over vector spaces or abelian groups.

Classical Results: Curtis-Hedlund Theorem

The group G **acts** on the configuration space as follows: for any $g \in G$, $x \in A^G$, define the map $x \cdot g : G \to A$ by

$$(h)(x \cdot g) = (hg^{-1})x, \quad \forall h \in G.$$

Theorem (Curtis-Hedlund)

Let G be a group and A a **finite** *set. A transformation $\tau : A^G \to A^G$ is a cellular automaton if and only if*

1. *τ is G-***equivariant** *(i.e. commutes with the action of G on A^G); and,*
2. *τ is* **continuous** *in the prodiscrete topology of A^G.*

Semigroups of Cellular Automata

- Consider the set of all CA over G and A:

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

- Consider the set of all invertible CA over G and A:

$$\mathrm{ICA}(G;A) := \left\{ \tau \in \mathrm{CA}(G;A) \cap \mathrm{Sym}(A^G) \mid \tau^{-1} \in \mathrm{CA}(G;A) \right\}$$

- Equipped with the composition of transformations,
  1. $\mathrm{CA}(G;A)$ is a **monoid**, and
  2. $\mathrm{ICA}(G;A)$ is its **group of units**.

Finite Semigroups of Cellular Automata

- **Idea:** Let G and A be both finite, and study the finite semigroup $\mathrm{CA}(G;A)$.
- If $|G| = n$ and $|A| = q$, then $|\mathrm{CA}(G;A)| = q^{q^n}$.
- The **rank** of a finite semigroup S is

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

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

Ranks of Semigroups of Transformations

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

- $\mathrm{Rank}(\mathrm{Tran}(X)) = \mathrm{Rank}(\mathrm{Sym}(X)) + 1 = 3$.
- $\mathrm{Rank}(\mathrm{Sing}(X)) = \binom{m}{2}$ (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-Bentz-Mitchell-Schneider '15).

Cellular Automata over Cyclic Groups $\mathbb{Z}_n$

Lemma

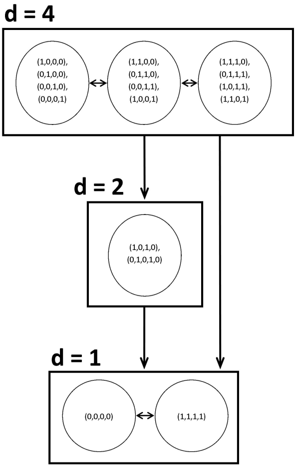
Let $\sigma : A^n \to A^n$ be defined by $(x_1, \dots, x_n)\sigma = (x_n, x_1, \dots, x_{n-1})$. Then,

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

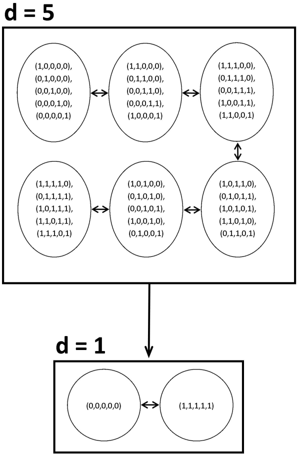
Let $\mathcal{O}$ be the set of $\mathbb{Z}_n$-orbits on A^n.

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

Examples

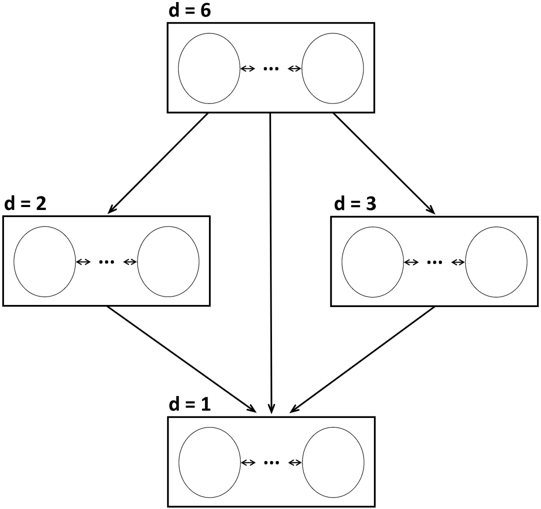


(a) Case $n = 4$, $q = 2$



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

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



Relative Rank

The **relative rank** of $U \subseteq S$ is

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

Lemma

(i) $\mathrm{Rank}(\mathrm{CA}) = \mathrm{Rank}(\mathrm{CA} : \mathrm{ICA}) + \mathrm{Rank}(\mathrm{ICA})$.

(ii) *If $E(n)$ is the number of edges in the* **divisibility graph** *of n,*

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_n; A) : \mathrm{ICA}(\mathbb{Z}_n; A)) = \begin{cases} E(n) - 1 & q = 2, n \in 2\mathbb{Z}; \\ E(n) & \textit{otherwise.} \end{cases}$$

Invertible Cellular Automata

Lemma

If $d_1, d_2, \dots, d_\ell$ are the non-one divisors of n, then:

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

Representation theory helps to calculate $\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_n; A))$ when $n = p$ is prime (Araújo-Schneider '09).

Lemma

The only proper nonzero Sym_α-invariant submodules of $(\mathbb{Z}_p)^\alpha$ are:

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

Main Result 1

Theorem (CR, Gadouleau '16)

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

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

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_{2^k}; A)) = \begin{cases} \frac{1}{2}k(k+7), & \text{if } q = 2; \\ \frac{1}{2}k(k+7) + 2, & \text{if } q \geq 3; \end{cases}$$

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_{2^k p}; A)) = \begin{cases} \frac{1}{2}k(3k+17) + 3, & \text{if } q = 2; \\ \frac{1}{2}k(3k+17) + 5, & \text{if } q \geq 3. \end{cases}$$

Main Result 2

- $d(n)$ is the number of **divisors** of n (including 1 and n),
- $d_+(n)$ is the number of **even divisors** of n,
- $S(n) := d(n) + d_+(n) + E(n)$.

Theorem (CR, Gadouleau '16)

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

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_n; A)) = \begin{cases} S(n) - 2 + \epsilon_{n,2}, & (q = 2) \wedge (n \in 2\mathbb{Z}); \\ S(n) + \epsilon_{n,q}, & \text{otherwise;} \end{cases}$$

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

Thanks for listening!

A. Castillo-Ramirez and M. Gadouleau,
Ranks of finite semigroups of one-dimensional cellular automata,
Semigroup Forum (Online First, 2016).