Additive Cellular Automata over $\mathbb{Z}_p$ and the Bottom of (CA,$\leq$)

Jacques Mazoyer and Ivan Rapaport

LIP-École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
email: {Jacques.Mazoyer,Ivan.Rapaport}@ens-lyon.fr

Abstract. In a previous work we began to study the question of "how to compare" cellular automata (CA). In that context it was introduced a preorder (CA,$\leq$) admitting a global minimum and it was shown that all the CA satisfying very simple dynamical properties as nilpotency or periodicity are located "on the bottom of (CA,$\leq$)". Here we prove that also the (algebraically amenable) additive CA over $\mathbb{Z}_p$ are located on the bottom of (CA,$\leq$). This result encourages our conjecture that says that the "distance" from the minimum could represent a measure of "complexity" on CA. We also prove that the additive CA over $\mathbb{Z}_p$ with p prime are pairwise incomparable. This fact improves our understanding of (CA,$\leq$) because it means that the minimum, even in the canonical order compatible with $\leq$, has infinite outdegree.

1 Introduction

One-dimensional cellular automata with radius 1, or simply CA, are infinite arrays of finite-state machines called cells and indexed by $\mathbb{Z}$. These identical cells evolve synchronously at discrete time steps following a local rule by which the state of a cell is determined as a function of its own state together with the states of its two neighbors. These devices, despite their simplicity, may exhibit very complex behavior.

In order to "understand" these CA one should find some criteria capable of structuring them into natural classes or hierarchies. In this direction, the classification of S. Wolfram [11], though heuristical and coarse, corresponds to the best-known attempt. Wolfram, by "observing" the long-term behavior of "arbitrary" periodic configurations, distinguishes four CA classes. Some efforts have been made in order to formalize this classification [6] or, typically by dynamical systems arguments, to introduce new classification schemes [5, 4]. Unfortunately, this last approach yields to some paradoxes: the shift CA, for instance, appears to be chaotic.

CA may also be seen as computational devices. In fact, it is easy to exhibit a CA that simulates any Turing machine [7]. In other words, the CA model is Turing-universal. The question whether the CA model is intrinsic-universal or, in other words, whether there exists a CA capable of simulating any other, remained open for some years. Notice that the CA can not be simulated by a Turing machine because the latter have a unique head which obviously will never visit the whole tape. J. Albert and K. Čulik II exhibited in [1] an intrinsic-universal CA. The "intrinsic-reducibility" notion induces a preorder on the set of CA. Unfortunetly, the study of this preorder structure is very difficult: it is based on the evolution of all the possible configurations (which are uncountable) and it does not take explicitly into account the CA transition tables. In addition, the "simulation" notion is so broad that a pair of CA with extremely different dynamics could appear to be "equivalent".

Another approach is to consider CA as algebraic objects. In this context, with the purpose of endowing the set of CA with an order relation, it would be sufficient to say that A is a subautomaton of B if the transition table of A is contained (after a suitable relabeling of the states) in the transition table of B. This notion is extremely restrictive. In fact, if A is a subautomaton of B then the space-time diagrams of A are "cell by cell equivalent" to the corresponding space-time diagrams of B (space-time diagrams are representations of a CA from a particular initial configuration in $\mathbb{Z}^2$). In other words, A and B may not be associated by the subautomaton relation even with their respective space-time diagrams being identical after suitable "changes of scale".

It seems therefore very natural to try to replace the subautomaton relation by a new one which could take into account potential changes of scale. This can be done by defining the powers of a CA. More precisely, let us denote by X^i the CA that generates the i-scaled space-time diagram of X and which is simply obtained by grouping i cells (or states) into blocks and by considering as transitions the interactions of neighbor blocks. Let us also note $A \leq B$ when some power of A is a subautomaton of some power of B or, equivalently, when the space-time diagrams of A are "block by block equivalent" to the corresponding space-time diagrams of B.

In [9] it was shown that (CA,$\leq$) is a preorder with no maximum. It was also proved that (CA,$\leq$) admits a global minimum and that all the CA satisfying very simple dynamical properties (nilpotents, periodics, shift-like) are located "on the bottom of (CA,$\leq$)". In addition, the fact that an algorithmically non-trivial "synchronization CA" was separated from the minimum by an infinite chain led us to conjecture that the "distance" from the minimum could represent a measure of "complexity" on CA.

In this paper we give more "evidence" supporting the intuitive expectation that says that the "simplest" CA should be located on the bottom of (CA,$\leq$) or, more precisely, that the "simplest" CA should be located immediately above the global minimum. By following an algebraic criterion of simplicity we decide to study the class of additive CA over $\mathbb{Z}_p$. In fact, these CA have been extensively studied because of their amenability to algebraic analysis [8, 2]. We prove that, for p prime, the additive CA over $\mathbb{Z}_p$ are located on the bottom of (CA,$\leq$). We also show that the additive CA over $\mathbb{Z}_p$ with p prime are pairwise incomparable. Therefore, if we note by CA* the set of CA modulo the canonical equivalence relation induced by $\leq$, then the minimum of the order (CA*,$\leq$) has infinite outdegree. Until now, we had no examples of unbounded outdegrees in (CA*,$\leq$).

2 Preliminaries

In this section we formally introduce the preorder (CA,$\leq$) and we recall some already known results. First, a CA is defined by a couple (Q, δ) where Q is a finite set of states and $\delta : Q^3 \to Q$ is a transition function. We say that (Q_1, δ_1) is a subautomaton of (Q_2, δ_2), and we note $(Q_1, \delta_1) \subseteq (Q_2, \delta_2)$, if there exists an injection $\varphi : Q_1 \to Q_2$ such that for all $x, y, z \in Q_1$:

$$\varphi(\delta_1(x, y, z)) = \delta_2(\varphi(x), \varphi(y), \varphi(z)).$$

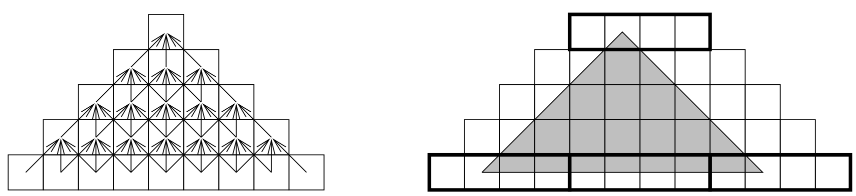
When the function φ is a bijection we say that (Q_1, δ_1) and (Q_2, δ_2) are isomorphic and we note $(Q_1, \delta_1) \cong (Q_2, \delta_2)$.

Let $I\!N^* = I\!N - \{0\}$. For any CA (Q, δ) the evolution of a finite block of states looks like a light-cone (see Figure 1-i). This basic fact inspires the notion of the n-block evolution function $\delta^n : Q^{2n+1} \to Q$, which is recursively defined for all $n \in I\!N^*$ as follows:

$$\delta^1(w_{-1}, w_0, w_1) = \delta(w_{-1}, w_0, w_1),$$
$$\delta^n(w_{-n} \cdots, w_0, \cdots, w_n) = \delta^{n-1}(\delta(w_{-n}, w_{-n+1}, w_{-n+2}) \cdots \delta(w_{n-2}, w_{n-1}, w_n)).$$

By grouping several states into blocks and by letting interact triplets of blocks as schematically appears in Figure 1-ii, we generate CA with (exponentially) more states. Formally, the n-power of a CA (Q, δ) is the CA $(Q, \delta)^n = (Q^n, \delta^n_{\mathcal{G}})$, where $\overrightarrow{q} \in Q^n$ is denoted by $(q_1, \cdots, q_n)$ and for all $\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z} \in Q^n$:

$$(\delta^n_{\mathcal{G}}(\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z}))_i = \delta^n(x_i, \cdots, x_n, y_1, \cdots, y_i, \cdots, y_n, z_1, \cdots, z_i).$$



(i) (ii)

Fig. 1. (i) Dependencies diagram representing a block of states evolution as a light-cone. (ii) Interaction of three blocks.

We relate two CA by $\leq$ when some power of the first is a subautomaton of some power of the second. More precisely, for (Q_1, δ_1) and (Q_2, δ_2):

$$(Q_1, \delta_1) \leq (Q_2, \delta_2) \Longleftrightarrow \exists n, m \in I\!N^* : (Q_1, \delta_1)^n \subseteq (Q_2, \delta_2)^m.$$

In [9] it was shown that (CA,$\leq$) is a preorder. In addition, it was proved that (CA,$\leq$) admits a global minimum corresponding to the (set of isomorphic)

CA having a single state. This fact allows us to define the "bottom of (CA,$\leq$)". More precisely, a CA is said to belong to the bottom of (CA,$\leq$) if there is no other CA located strictly between the minimum and itself. In other words, (Q^*, δ^*) belongs to the bottom of (CA,$\leq$) if for any other non-singleton CA (Q, δ), $(Q, \delta) \leq (Q^*, \delta^*) \implies (Q^*, \delta^*) \leq (Q, \delta)$. Finally, the following lemma is going to be used later:

Lemma 1. *If $(Q, \delta) \leq (\tilde{Q}, \tilde{\delta})$ then there exist $i_0, j_0 \in I\!N^*$ and $\overrightarrow{q_0} \in Q^{i_0}$ such that $(Q, \delta)^{i_0} \subseteq (\tilde{Q}, \tilde{\delta})^{j_0}$ and $\delta_{\mathcal{G}}^{i_0}(\overrightarrow{q_0}, \overrightarrow{q_0}, \overrightarrow{q_0}) = \overrightarrow{q_0}$.*

Proof. Let $(Q, \delta) \leq (\tilde{Q}, \tilde{\delta})$. By definition, there exist $i, j \in I\!N^*$ such that $(Q, \delta)^i \subseteq (\tilde{Q}, \tilde{\delta})^j$. By the finiteness of Q there exist $q \in Q$ and $k \in I\!N^*$ such that $\delta^k(q \cdots q) = q$. Considering the fact that $(Q, \delta)^{ik} \subseteq (\tilde{Q}, \tilde{\delta})^{jk}$ [9], the lemma is concluded for $i_0 = ik, j_0 = jk$ and $\overrightarrow{q_0} = (q \cdots q)$. □

3 Permutive CA

The notion of permutive CA has been extensively used (see for instance [10]). A given CA (Q, δ) is said to be right permutive if for all $a, b \in Q$ the function $\delta(a, b, \cdot) : Q \to Q$ is bijective. A CA (Q, δ) is said to be left permutive if for all $a, b \in Q$ the function $\delta(\cdot, a, b) : Q \to Q$ is bijective. A CA (Q, δ) is said to be permutive if it is right and left permutive.

Here we prove that all the subautomata and all the powers of a given permutive CA are permutive.

Lemma 2. *Let (Q_2, δ_2) be a permutive CA. If (Q_1, δ_1) is such that $(Q_1, \delta_1) \subseteq (Q_2, \delta_2)$ then (Q_1, δ_1) is also permutive.*

Proof. Direct. □

Lemma 3. *Let (Q, δ) be a CA and let $n \in I\!N^*$. (Q, δ) is permutive if and only if $(Q, \delta)^n$ is permutive.*

Proof. We prove the equivalence for the right permutivity. For the left permutivity the proof is identical. Let us therefore assume (Q, δ) to be right permutive. It is easy to prove by induction that for all $m \in I\!N^*$, for all $\overrightarrow{a} \in Q^{2m}$, and for all $x, y \in Q$: $\delta^m(\overrightarrow{a} x) = \delta^m(\overrightarrow{a} y) \Rightarrow x = y$. Let $\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{x}, \overrightarrow{y} \in Q^n$. If $\overrightarrow{x} \neq \overrightarrow{y}$ then there is an index $i \in \{1, \cdots, n\}$ such that $i = \min\{j \in \{1, \cdots, n\} : x_j \neq y_j\}$. It follows that $\delta^n(a_i \cdots a_n b_1 \cdots b_n x_1 \cdots x_i) \neq \delta^n(a_i \cdots a_n b_1 \cdots b_n x_1 \cdots y_i)$, and therefore $(\delta_{\mathcal{G}}^n(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{x}))_i \neq (\delta_{\mathcal{G}}^n(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{y}))_i$.

Let us assume now that $(Q, \delta)^n$ is right permutive (notice that the non-trivial case is when $n > 1$). Let $a, b, x, y \in Q$. If $\delta(a, b, x) = \delta(a, b, y)$ then:

$$\delta_{\mathcal{G}}^n(a \cdots a, a \cdots a, \underbrace{a \cdots a}_{n-2} bx) = \delta_{\mathcal{G}}^n(a \cdots a, a \cdots a, \underbrace{a \cdots a}_{n-2} by),$$

and therefore $(\underbrace{a \cdots a}_{n-2} bx) = (\underbrace{a \cdots a}_{n-2} by)$, which implies that $x = y$. □

4 Additive Cellular Automata Over $\mathbb{Z}_p$

This section is the core of the present work. Here we prove that, for p prime, the additive CA over $\mathbb{Z}_p$ are pairwise incomparable (Corollary 9) and that they are all located on the bottom of (CA,$\leq$) (Corollary 12).

Let us start by denoting, for each $p \in IN^*, p > 1$, the additive abelian group of integers modulo p by $(\mathbb{Z}_p, +)$. For each $n \in IN^*$ we denote the canonical product group by $(\mathbb{Z}_p^n, +)$. More precisely, for all $(x_1, \cdots, x_n), (y_1, \cdots, y_n)$:

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + z_n).$$

Stated for arbitrary groups of finite order, the following proposition appears in any introductory textbook of Algebra (see for instance [3]).

Proposition 4. *Let $p, n \in IN^*, p > 1$, and let $\mathcal{X} \subseteq \mathbb{Z}_p^n$ be a nonempty set. If $(\mathcal{X}, +)$ is such that for all $\overrightarrow{x}, \overrightarrow{y} \in \mathcal{X} : \overrightarrow{x} + \overrightarrow{y} \in \mathcal{X}$, then $(\mathcal{X}, +)$ is a subgroup of $(\mathbb{Z}_p^n, +)$ and $|\mathcal{X}| \mid p^n$. Moreover, if p is prime then:*

$$\mathcal{X} = \prod_{k=1}^{n} \mathcal{X}_k, \ \text{with } \mathcal{X}_k = \mathbb{Z}_p \text{ or } \mathcal{X}_k = \{0\} \text{ for all } k \in \{1, \cdots, n\}.$$

To the abelian group $(\mathbb{Z}_p, +)$ we associate in the canonical way the CA $(\mathbb{Z}_p, \oplus)$ such that for all $x, y, z \in \mathbb{Z}_p : \oplus(x, y, z) = x + y + z$. Similarly, to the product group $(\mathbb{Z}_p^n, +)$ we associate the CA $(\mathbb{Z}_p^n, \oplus)$ in such a way that for all $\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z} \in \mathbb{Z}_p^n : \oplus(\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z}) = \overrightarrow{x} + \overrightarrow{y} + \overrightarrow{z}$. Finally, the n-power of the CA $(\mathbb{Z}_p, \oplus)$ corresponds, by definition, to $(\mathbb{Z}_p, \oplus)^n = (\mathbb{Z}_p^n, \oplus_{\mathcal{G}}^n)$.

Remark. Notice that in $\mathbb{Z}_p^n$ the operations $\oplus$ and $\oplus_{\mathcal{G}}^n$ are not the same. For instance, if we consider the set $\mathbb{Z}_3^4$ (see Figure 2):

$$\oplus((2, 2, 1, 2), (1, 1, 0, 2), (0, 1, 2, 1)) = (0, 1, 0, 2) \text{ and}$$
$$\oplus_{\mathcal{G}}^4((2, 2, 1, 2), (1, 1, 0, 2), (0, 1, 2, 1)) = (2, 1, 1, 1).$$

				2	1	1	1				
			1	2	2	0	2	2			
		2	1	1	0	1	2	2	1		
	2	2	1	1	2	0	2	0	0	1	
2	2	1	2	1	1	0	2	0	1	2	1

Fig. 2. $\oplus_{\mathcal{G}}^4((2, 2, 1, 2), (1, 1, 0, 2), (0, 1, 2, 1)) = (2, 1, 1, 1)$.

Lemma 5. *For all $p, n \in IN^*, p > 1$, the CA $(\mathbb{Z}_p, \oplus)^n$ is permutive.*

Proof. By Lemma 3 together with the permutivity of $(\mathbb{Z}_p, \oplus)$. $\square$

The following (and easy to prove) "superposition principle" [8] reflects why additive CA are so amenable to algebraic analysis.

Proposition 6 The superposition principle. *Let $p, n \in I\!N^*, p > 1$. For all $\overrightarrow{x_1}, \overrightarrow{x_2}, \overrightarrow{y_1}, \overrightarrow{y_2}, \overrightarrow{z_1}, \overrightarrow{z_2} \in \mathbb{Z}_p^n$ it holds the following:*

$$\oplus_{\mathcal{G}}^n(\overrightarrow{x_1} + \overrightarrow{x_2}, \overrightarrow{y_1} + \overrightarrow{y_2}, \overrightarrow{z_1} + \overrightarrow{z_2}) = \oplus_{\mathcal{G}}^n(\overrightarrow{x_1}, \overrightarrow{y_1}, \overrightarrow{z_1}) + \oplus_{\mathcal{G}}^n(\overrightarrow{x_2}, \overrightarrow{y_2}, \overrightarrow{z_2}).$$

Proposition 7. *Let $p, n \in I\!N^*, p > 1$, and let $\mathcal{X} \subseteq \mathbb{Z}_p^n$ with $\overrightarrow{0} = (0, \cdots, 0) \in \mathcal{X}$. It holds that if $(\mathcal{X}, \oplus_{\mathcal{G}}^n) \subseteq (\mathbb{Z}_p^n, \oplus_{\mathcal{G}}^n)$ then $(\mathcal{X}, +)$ is a subgroup of $(\mathbb{Z}_p^n, +)$.*

Proof. Let $(\mathcal{X}, \oplus_{\mathcal{G}}^n) \subseteq (\mathbb{Z}_p^n, \oplus_{\mathcal{G}}^n)$ and let $\overrightarrow{x_0}, \overrightarrow{y_0} \in \mathcal{X}$. Considering Lemma 2 together with Lemma 5, it follows that $(\mathcal{X}, \oplus_{\mathcal{G}}^n)$ is permutive and therefore there exists $\overrightarrow{\alpha_0} \in \mathcal{X}$ such that $\oplus_{\mathcal{G}}^n(\overrightarrow{\alpha_0}, \overrightarrow{x_0}, \overrightarrow{x_0}) = \overrightarrow{0}$. By the superposition principle:

$$\begin{aligned} \oplus_{\mathcal{G}}^n(\overrightarrow{\alpha_0}, \overrightarrow{x_0}, \overrightarrow{x_0} + \overrightarrow{y_0}) &= \oplus_{\mathcal{G}}^n(\overrightarrow{\alpha_0}, \overrightarrow{x_0}, \overrightarrow{x_0}) + \oplus_{\mathcal{G}}^n(\overrightarrow{0}, \overrightarrow{0}, \overrightarrow{y_0}) \\ &= \oplus_{\mathcal{G}}^n(\overrightarrow{0}, \overrightarrow{0}, \overrightarrow{y_0}) = \overrightarrow{y_*} \in \mathcal{X}. \end{aligned}$$

On the other hand, again by permutivity of $(\mathcal{X}, \oplus_{\mathcal{G}}^n)$, there exists $\overrightarrow{x_*} \in \mathcal{X}$ such that $\oplus_{\mathcal{G}}^n(\overrightarrow{\alpha_0}, \overrightarrow{x_0}, \overrightarrow{x_*}) = \overrightarrow{y_*}$. Finally, now by permutivity of $(\mathbb{Z}_p^n, \oplus_{\mathcal{G}}^n)$, $\overrightarrow{x_*} = (\overrightarrow{x_0} + \overrightarrow{y_0}) \in \mathcal{X}$. $\square$

Proposition 8. *Let (Q, δ) be a CA and let $p \in I\!N^*, p > 1$. If $(Q, \delta) \leq (\mathbb{Z}_p, \oplus)$ then there exist $i, j \in I\!N^*$ and an injection $\psi : Q^i \to \mathbb{Z}_p^j$ such that:*

$$(Q, \delta)^i \cong (\psi(Q^i), \oplus_{\mathcal{G}}^j) \subseteq (\mathbb{Z}_p^j, \oplus_{\mathcal{G}}^j),$$

with $(\psi(Q^i), +)$ being a subgroup of $(\mathbb{Z}_p^j, +)$.

Proof. Let us suppose that $(Q, \delta) \leq (\mathbb{Z}_p, \oplus)$. By definition, there exist $i, j \in I\!N^*$ such that $(Q, \delta)^i \subseteq (\mathbb{Z}_p, \oplus)^j$ by some injection φ. Moreover, by Lemma 1, we can assume that there exists $\overrightarrow{q_0} \in Q^i$ such that $\delta_{\mathcal{G}}^i(\overrightarrow{q_0}, \overrightarrow{q_0}, \overrightarrow{q_0}) = \overrightarrow{q_0}$ and therefore $\oplus_{\mathcal{G}}^j(\varphi(\overrightarrow{q_0}), \varphi(\overrightarrow{q_0}), \varphi(\overrightarrow{q_0})) = \varphi(\overrightarrow{q_0})$. Let us define the injection $\psi : Q^i \to \mathbb{Z}_p^j$ in such a way that, for all $\overrightarrow{q} \in Q^i : \psi(\overrightarrow{q}) = \varphi(\overrightarrow{q}) - \varphi(\overrightarrow{q_0})$. Let us denote $\mathcal{X} = \psi(Q^i)$. Notice that $\overrightarrow{0} = (0, \cdots, 0) \in \mathcal{X}$ because $\overrightarrow{0} = \varphi(\overrightarrow{q_0}) - \varphi(\overrightarrow{q_0})$.

In order to prove that $(Q, \delta)^i \cong (\mathcal{X}, \oplus_{\mathcal{G}}^j) \subseteq (\mathbb{Z}_p^j, \oplus_{\mathcal{G}}^j)$ it suffices to prove that $(\varphi(Q^i), \oplus_{\mathcal{G}}^j) \cong (\mathcal{X}, \oplus_{\mathcal{G}}^j)$ because $(Q, \delta)^i \cong (\varphi(Q^i), \oplus_{\mathcal{G}}^j)$. Let $\eta : \varphi(Q^i) \to \mathcal{X}$ be such that $\eta(\overrightarrow{x}) = \overrightarrow{x} - \varphi(\overrightarrow{q_0})$. The function η is obviously a bijection and, in addition, for all $\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z} \in \varphi(Q^i)$:

$$\begin{aligned} \eta(\oplus_{\mathcal{G}}^j(\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z})) &= \oplus_{\mathcal{G}}^j(\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z}) - \oplus_{\mathcal{G}}^j(\varphi(\overrightarrow{q_0}), \varphi(\overrightarrow{q_0}), \varphi(\overrightarrow{q_0})) \\ &= \oplus_{\mathcal{G}}^j(\eta(\overrightarrow{x}), \eta(\overrightarrow{y}), \eta(\overrightarrow{z})). \end{aligned}$$

From Proposition 7, it follows that $(\psi(Q^i), +)$ is a subgroup of $(\mathbb{Z}_p^j, +)$. $\square$

Remark. The process of searching additive CA $(\mathbb{Z}_p, \oplus)$ located on the bottom of (CA,$\leq$) may be restricted to p prime because if $a, b \in I\!N^*$ are such that $a|b$ then $(\mathbb{Z}_a, \oplus) \leq (\mathbb{Z}_b, \oplus)$. In fact, it suffices to notice that $(\mathbb{Z}_a, \oplus) \subseteq (\mathbb{Z}_b, \oplus)$ by the injection $\varphi : \mathbb{Z}_a \to \mathbb{Z}_b$ which assigns to each $x \in \mathbb{Z}_a$ the value $\varphi(x) = \frac{bx}{a} \in \mathbb{Z}_b$.

Corollary 9. *Let $p, q > 1$ be prime numbers. If $p \neq q$ then $(\mathbb{Z}_p, \oplus) \not\leq (\mathbb{Z}_q, \oplus)$.*

Proof. Let us suppose that $(\mathbb{Z}_p, \oplus) \leq (\mathbb{Z}_q, \oplus)$. Then, by Proposition 8, there exist $i, j \in I\!N^*$ and an injection $\psi : \mathbb{Z}_p^i \to \mathbb{Z}_q^j$ such that $(\psi(\mathbb{Z}_p^i), +)$ is a subgroup of $(\mathbb{Z}_q^j, +)$. By Proposition 4, $p^i | q^j$. This is a contradiction. □

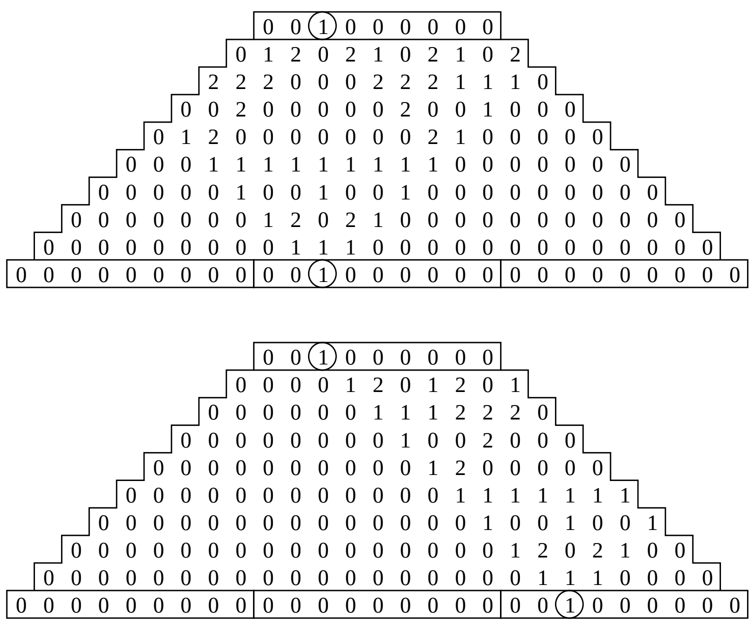


Fig. 3. $\oplus_{\mathcal{G}}^{3^2}(\overrightarrow{0}, \overrightarrow{e_3}, \overrightarrow{0}) = \oplus_{\mathcal{G}}^{3^2}(\overrightarrow{0}, \overrightarrow{0}, \overrightarrow{e_3}) = \overrightarrow{e_3}$.

Proposition 10. *For all $\alpha \in I\!N^*$ and $p > 1$ prime it holds that:*

$$(\mathbb{Z}_p^{p^\alpha}, \oplus) \cong (\mathbb{Z}_p, \oplus)^{p^\alpha}.$$

On the other hand, for every $\mathcal{X} \subseteq \mathbb{Z}_p^{p^\alpha}$ such that $|\mathcal{X}| > 1$ and $(\mathcal{X}, \oplus_{\mathcal{G}}^{p^\alpha}) \subseteq (\mathbb{Z}_p^{p^\alpha}, \oplus_{\mathcal{G}}^{p^\alpha})$ with $(\mathcal{X}, +)$ being a subgroup of $(\mathbb{Z}_p^{p^\alpha}, +)$, it holds that $(\mathbb{Z}_p, \oplus) \subseteq (\mathcal{X}, \oplus_{\mathcal{G}}^{p^\alpha})$.

Proof. By using the well-known dipolynomial representation of additive CA that appears in [8], together with the fact that a dipolynomial over $\mathbb{Z}_p$ of the form $\sum x^i$ satisfies that $(\sum x^i)^{p^\alpha} = \sum x^{ip^\alpha}$, it can be proved that (see Figure 3): $\oplus_{\mathcal{G}}^{p^\alpha}(\overrightarrow{e_k}, \overrightarrow{0}, \overrightarrow{0}) = \oplus_{\mathcal{G}}^{p^\alpha}(\overrightarrow{0}, \overrightarrow{e_k}, \overrightarrow{0}) = \oplus_{\mathcal{G}}^{p^\alpha}(\overrightarrow{0}, \overrightarrow{0}, \overrightarrow{e_k}) = \overrightarrow{e_k}$, with $\overrightarrow{e_k} = (\underbrace{0, \cdots, 0, 1}_{k \in \{1, \cdots, p^\alpha\}}, 0, \cdots, 0) \in \mathbb{Z}_p^{p^\alpha}$ and $\overrightarrow{0} = (0, \cdots, 0)$.

The previous result, together with the superposition principle, allows us to conclude, as it appears in the example of Figure 4, that $(\mathbb{Z}_p^{p^\alpha}, \oplus) \cong (\mathbb{Z}_p, \oplus)^{p^\alpha}$. Finally, let $\mathcal{X} \subseteq \mathbb{Z}_p^{p^\alpha}$ be such that $|\mathcal{X}| > 1$ and $(\mathcal{X}, \oplus_{\mathcal{G}}^{p^\alpha}) \subseteq (\mathbb{Z}_p^{p^\alpha}, \oplus_{\mathcal{G}}^{p^\alpha})$ with $(\mathcal{X}, +)$ being a subgroup of $(\mathbb{Z}_p^{p^\alpha}, +)$. By considering Proposition 4 we conclude the existence of an index $k_0 \in \{1, \cdots, p^\alpha\}$ such that $\mathcal{X}_{k_0} = \mathbb{Z}_p$. It follows that $(\mathbb{Z}_p, \oplus) \subseteq (\mathcal{X}, \oplus_{\mathcal{G}}^{p^\alpha})$ by the injection $\varphi : \mathbb{Z}_p \to \mathcal{X}$ that assigns, to each $x \in \mathbb{Z}_p$, the image $\varphi(x) = (\underbrace{0, \cdots, 0, x}_{k_0}, \cdots, 0)$. □

									1	2	1	0	2	0	1	2	1									
								1	1	2	2	0	1	1	1	2	2	0								
							1	1	2	1	2	2	2	0	2	2	1	2	0							
						1	2	1	1	0	0	2	0	0	0	2	0	2	0	1						
					1	1	2	2	0	2	1	0	1	2	0	1	1	1	0	2	2					
				1	1	2	1	2	2	2	1	1	1	2	2	2	0	2	2	2	1	2				
			1	2	1	1	0	0	2	0	0	1	0	0	2	0	0	0	2	0	0	1	1			
		1	2	1	2	1	1	1	1	0	2	1	1	1	1	0	2	1	0	1	2	0	2	2		
	1	0	0	2	2	1	1	2	1	1	1	0	0	1	0	0	0	2	2	2	0	0	0	2	0	
2	0	2	1	0	1	1	2	1	2	1	1	2	0	1	0	2	1	0	1	1	0	2	1	0	1	2

Fig. 4. $(\mathbb{Z}_3^{3^2}, \oplus) \cong (\mathbb{Z}_3, \oplus)^{3^2}$.

Proposition 11. *Let $n \in \mathbb{N}^*$ and let $p > 1$ be prime. If $\mathcal{X} \subseteq \mathbb{Z}_p^n$ is such that $|\mathcal{X}| > 1$ and $(\mathcal{X}, \oplus_{\mathcal{G}}^n) \subseteq (\mathbb{Z}_p^n, \oplus_{\mathcal{G}}^n)$ with $(\mathcal{X}, +)$ being a subgroup of $(\mathbb{Z}_p^n, +)$, then there exists $m \in \mathbb{N}^*$ satisfying $(\mathbb{Z}_p^m, \oplus_{\mathcal{G}}^m) \subseteq (\mathcal{X}, \oplus_{\mathcal{G}}^n)$.*

Proof. Let us consider the decomposition $n = \lambda p^\alpha$ with $\alpha \in \mathbb{N}$ and $\lambda \in \mathbb{N}^*$ such that $p \not| \lambda$. Let us assume first that $\lambda = 1$. If $\alpha = 0$ then, considering that $(\mathcal{X}, +)$ is a subgroup of $(\mathbb{Z}_p, +)$ together with the fact that $|\mathcal{X}| > 1$, it can be concluded by Proposition 4 that $\mathcal{X} = \mathbb{Z}_p$ and therefore $(\mathcal{X}, \oplus) \cong (\mathbb{Z}_p, \oplus)$. On the other hand, if $\alpha > 0$ then, by considering Proposition 10, we conclude that $(\mathbb{Z}_p, \oplus) \subseteq (\mathcal{X}, \oplus_{\mathcal{G}}^{p^\alpha})$. Let us assume now that $\lambda > 1$. By Proposition 4:

$$\mathcal{X} = \prod_{k=1}^{\lambda p^\alpha} \mathcal{X}_k, \text{ with } \mathcal{X}_k = \mathbb{Z}_p \text{ or } \mathcal{X}_k = \{0\} \text{ for all } k \in \{1, \cdots, \lambda p^\alpha\}.$$

Let us suppose that there exist $k_1, k_2 \in \{1, \cdots, \lambda p^\alpha\}$ with $k_2 - k_1 = p^\alpha$ such that $\mathcal{X}_{k_1} = \{0\}$ and $\mathcal{X}_{k_2} = \mathbb{Z}_p$. Let $\overrightarrow{e_{k_2}} = (\underbrace{0, \cdots, 0, 1}_{k_2}, 0, \cdots, 0)$. It follows, as it is schematically shown in Figure 5, that $(\oplus_{\mathcal{G}}^{\lambda p^\alpha}(\overrightarrow{e_{k_2}}, \overrightarrow{0}, \overrightarrow{0}))_{k_1} = \lambda \bmod p \neq 0$, and then $(\oplus_{\mathcal{G}}^{\lambda p^\alpha}(\overrightarrow{e_{k_2}}, \overrightarrow{0}, \overrightarrow{0}))_{k_1} \notin \mathcal{X}_{k_1}$, which is a contradiction. We can therefore assume that $\mathcal{X}$ is such that for any pair of indexes $k_1, k_2 \in \{1, \cdots, \lambda p^\alpha\}$ satisfying that $k_2 - k_1 = p^\alpha$ it holds that $\mathcal{X}_{k_1} = \mathcal{X}_{k_2}$. Let $k \in \{1, \cdots, p^\alpha\}$ be such that $\mathcal{X}_k = \mathbb{Z}_p$. This k does exist because $|\mathcal{X}| > 1$. It follows, as it is shown in the example of Figure 6, that $(\mathbb{Z}_p, \oplus)^\lambda \subseteq (\mathcal{X}, \oplus_{\mathcal{G}}^{\lambda p^\alpha})$. In fact, it suffices to consider the injection $\varphi : \mathbb{Z}_p^\lambda \to \mathcal{X}$ such that for all $\overrightarrow{x} = (x_1, \cdots, x_\lambda) \in \mathbb{Z}_p^\lambda$ and for all $i \in \{1, \cdots, \lambda p^\alpha\}$:

$$(\varphi(\overrightarrow{x}))_i = \begin{cases} (\overrightarrow{x})_{\frac{i-k}{p^\alpha}+1} & \text{if } i = k \bmod p^\alpha \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

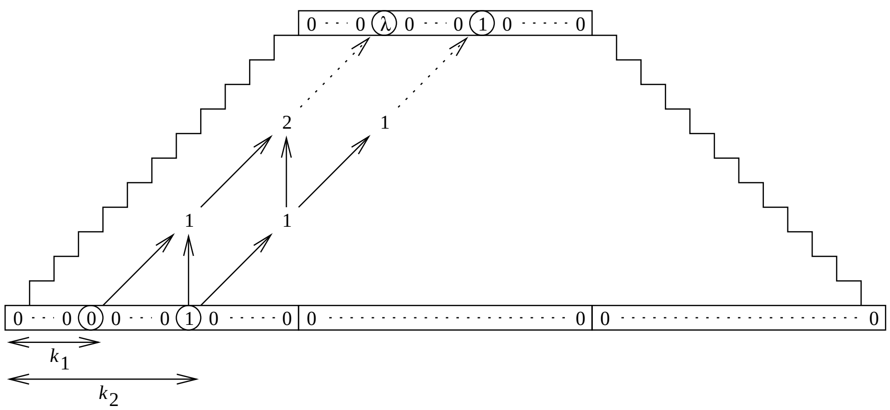


Fig. 5. $(\oplus_{\mathcal{G}}^{n}(\overrightarrow{e_{k_2}}, \overrightarrow{0}, \overrightarrow{0}))_{k_1} = \lambda \bmod p$.

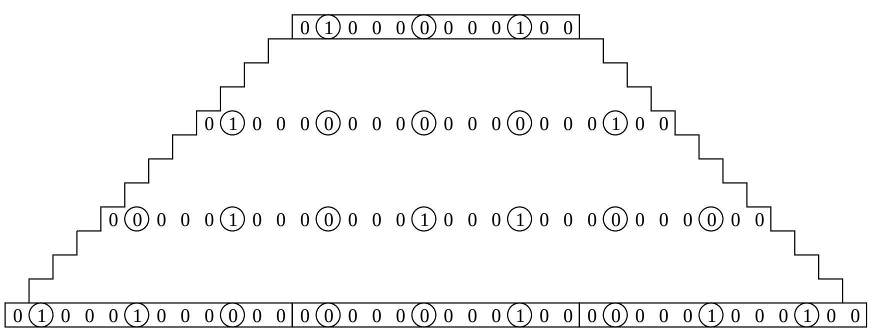


Fig. 6. $(\mathbb{Z}_2, \oplus)^3 \subseteq (\mathcal{X}, \oplus_{\mathcal{G}}^{3\times 2^2})$ with the index $k = 2 \in \{1, \cdots, 2^2\}$.

Corollary 12. *Let (Q, δ) be a CA with $|Q| > 1$ and let $p > 1$ be prime. It holds that if $(Q, \delta) \leq (\mathbb{Z}_p, \oplus)$ then $(\mathbb{Z}_p, \oplus) \leq (Q, \delta)$.*

Proof. Let us suppose that $(Q, \delta) \leq (\mathbb{Z}_p, \oplus)$. From Proposition 8 there exist $i, j \in \mathbb{N}^*$ and an injection $\psi : Q^i \to \mathbb{Z}_p^j$ such that $(Q, \delta)^i \cong (\psi(Q^i), \oplus_{\mathcal{G}}^j) \subseteq (\mathbb{Z}_p^j, \oplus_{\mathcal{G}}^j)$, with $(\psi(Q^i), +)$ being a subgroup of $(\mathbb{Z}_p^j, +)$. Then, by Proposition 11, there exists $m \in \mathbb{N}^*$ such that $(\mathbb{Z}_p, \oplus)^m \subseteq (\psi(Q^i), \oplus_{\mathcal{G}}^j) \cong (Q, \delta)^i$. □

Remark. If we denote by $\sim$ the canonical equivalence relation induced by $\leq$, then the minimum of the canonical order (CA/$\sim$,$\leq$) has infinite outdegree.

5 Concluding Remarks

We have shown that, according to (CA,$\leq$), all the additive CA over $\mathbb{Z}_p$ with p prime have the same "complexity": they are all incomparable and located immediately above the minimum. Moreover, for finding the position of any additive CA in (CA,$\leq$) one should follow simple number divisibility considerations. Nevertheless, one question remains open: given $x, y, i, j \in \mathbb{N}^*$ with $x^i | y^j$, is it true or false that $(\mathbb{Z}_x, \oplus) \leq (\mathbb{Z}_y, \oplus)$?

References

1. J. Albert and K. Čulik II. A simple universal cellular automaton and its one-way and totalistic version. *Complex Systems*, 1:1–16, 1987.
2. J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, and G. Skordev. Linear cellular automata, finite automata and Pascal's triangle. *Discrete Applied Mathematics*, 66:1–22, 1996.
3. G. Birkhoff and S. Mac Lane. *A survey of modern algebra*, chapter VI. MacMillan, New York, 1953. (Theorem 15, Theorem 18).
4. F. Blanchard, A.Maass, and P.Kurka. Topological and measure-theoretic properties of one-dimensional cellular automata. *Physica D*, 103:86–99, 1997.
5. G. Braga, G. Cattaneo, P. Flocchini, and C. Quaranta Vogliotti. Pattern growth in elementary cellular automata. *Theoretical Computer Science*, 45:1–26, 1995.
6. K. Čulik II and S. Yu. Undecidability of CA classification schemes. *Complex Systems*, 2:177–190, 1988.
7. A.R. Smith III. Simple computation-universal cellular spaces. *Journal ACM*, 18:339–353, 1971.
8. O. Martin, O. Odlyzko, and S. Wolfram. Algebraic properties of cellular automata. *Communications in Mathematical Physics*, 93:219–258, 1984.
9. J. Mazoyer and I. Rapaport. Inducing an order on cellular automata by a grouping operation. In *STACS'98*, volume 1373 of *Lecture Notes in Computer Science*, pages 116–127, 1998.
10. C. Moore. Predicting nonlinear cellular automata quickly by decomposing them into linear ones. *Physica D*, 111:27–41, 1998.
11. S. Wolfram. Universality and complexity in cellular automata. *Physica D*, 10:1–35, 1984.

This article was processed using the LaTeX macro package with LLNCS style