Physics Letters A 377 (2013) 276–285

Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Symmetry analysis of cellular automata

V. García-Morales *

Institute for Advanced Study – Technische Universität München, Lichtenbergstr. 2a, D-85748 Garching, Germany

ARTICLE INFO

Article history:
Received 19 September 2012
Received in revised form 26 November 2012
Accepted 27 November 2012
Available online 29 November 2012
Communicated by C.R. Doering

Keywords:
Computation theory
Mathematical results
Complexity
Dynamics

ABSTRACT

By means of $\mathcal{B}$-calculus [V. García-Morales, Phys. Lett. A 376 (2012) 2645] a universal map for deterministic cellular automata (CAs) has been derived. The latter is shown here to be invariant upon certain transformations (global complementation, reflection and shift). When constructing CA rules in terms of rules of lower range a new symmetry, "invariance under construction" is uncovered. Modular arithmetic is also reformulated within $\mathcal{B}$-calculus and a new symmetry of certain totalistic CA rules, which calculate the Pascal simplices modulo an integer number p, is then also uncovered.

1. Introduction

Complexity arises in nature already when simple dynamical systems involving a finite number of states are considered [1–3]. Cellular automata (CAs) constitute examples of such paradigmatic models of complexity [1–6] and allow complex natural systems made of large numbers of identical parts to be described [4–9]. The dynamics of CAs takes place in a discrete lattice of sites, with a finite set of possible values each. Inputs and outputs of a CA rule are thus integers on the interval $[0, p-1]$ with p being a non-negative integer, the CA rule being thus an endomorphism within this set of integers. The site values evolve synchronously in discrete time steps according to identical rules, being determined by the previous values on the sites of their neighborhood [1–3]. The range ρ of the neighborhood is given as $\rho = l + r + 1$, where l and r denote the number of sites to the left and to the right of the cell that is updated after each time step, respectively. Thus there are $p^\rho = p^{l+r+1}$ different configurations that the symbols can have within the neighborhood and, therefore there are $\Gamma = p^{p^{l+r+1}}$ CA rules for given values of p, l and r. For example, when only two possible site values ($p = 2$) and first neighbors ($l = r = 1$) are considered there are a total of $\Gamma = 256$ rules. Not all these Γ rules exhibit behavior that is qualitatively different from each other. Some of these rules are related by elementary symmetry transformations so that, if the behavior of certain rules is known, the one of their class-equivalent relatives is automatically known as well. Within the 256 rules above described only 88 are independent upon global complementation (i.e. exchanging the site values) or reflection (i.e. exchanging left and right directions) [1,4,10].

In this Letter, use is made of a recently derived universal map for CA [3] to systematically investigate symmetry relationships between CA rules in a general manner (i.e. for arbitrary number of symbols and range). The universal map is found to be invariant not only under global complementation and reflection but also under shift (Galilean invariance), a symmetry that is uncovered here. These invariances allow classification of CA rules into equivalence classes. Within each equivalence class, a specific symmetry is broken when specific CA rules are considered but the dynamical behavior of all class members is automatically known, when just the dynamical behavior of one CA belonging to them is known. When applied to the 256 rules, only 85 are found to be independent in this sense (Galilean invariance reduces the total of 88 independent Wolfram rules even further). A theorem is then proven on how CA rules are constructed in terms of rules of lower range and a new symmetry of CAs called "invariance under construction" is uncovered. Modular arithmetic is also reformulated within $\mathcal{B}$-calculus allowing the time-reversal symmetry to be discussed in a systematic manner. A new symmetry of certain totalistic 1D CA rules, which calculate the Pascal simplices modulo an integer number p is then also uncovered. We first review the essentials of $\mathcal{B}$-calculus and the universal map for CA to be explored in subsequent sections.

2. $\mathcal{B}$-calculus and universal map for 1D cellular automata (CAs)

Dynamical systems governed by rules evolve as follows: the state of the dynamical system is given as *input* to the dynamical

* Tel.: +49 89 289 10595.
E-mail address: vmorales@ph.tum.de.

0375-9601/$ – see front matter
http://dx.doi.org/10.1016/j.physleta.2012.11.052

rule. This *input* is compared with the specification of all possible inputs (henceforth called *configurations*) given in a table, and the rule returns *output*. Each *input* is separated from the other one in the table by a distance *tolerance*. The most simple rule is now considered, i.e. one containing just only one configuration with one non-zero output. When *input* coincides with *configuration* within a certain *tolerance*, the rule returns *output*. Otherwise, the result is zero. This simple rule can be written formally as

$$\mathit{output} \times \mathcal{B}(\mathit{configuration} - \mathit{input}, \mathit{tolerance}) \tag{1}$$

where $\mathcal{B}(x, \epsilon)$ is the boxcar function,

$$\mathcal{B}(x, \epsilon) = \frac{1}{2}\left(\frac{x+\epsilon}{|x+\epsilon|} - \frac{x-\epsilon}{|x-\epsilon|}\right) \tag{2}$$

which returns one when $|\mathit{configuration} - \mathit{input}| < \mathit{tolerance}$ and zero otherwise. $\mathcal{B}$-calculus concerns all kinds of mathematical structures that can be constructed through addition and multiplication of simple structures of the form of Eq. (1). When one has a rule with several different configurations indexed by n so that to $\mathit{configuration}_n$ corresponds an output_n, the rule is completely given by summing over all elementary structures describing the action of the rule on each separate $\mathit{configuration}_n$ as given in Eq. (1). The *output* of the rule is then

$$\mathit{output} = \sum_{n \in \mathit{table}} \mathit{output}_n \times \mathcal{B}(\mathit{configuration}_n - \mathit{input}, \mathit{tolerance}) \tag{3}$$

The *tolerance* is related to the distance separating two adjacent configurations on the table and is defined as

$$\mathit{tolerance} = \frac{\mathit{configuration}_{n+1} - \mathit{configuration}_n}{2} \tag{4}$$

and so, if each $\mathit{configuration}_n$ is given by a non-negative integer number, $\mathit{tolerance} = 1/2$. If each configuration is instead given by a rational number separated a distance $1/d$ from the next, then $\mathit{tolerance} = 1/(2d)$.

Eq. (3) can now be applied to provide a theory for CA as follows in [3]. Let us consider a 1D ring containing a total number of N_s sites. An input is given as initial condition in the form of a vector $\mathbf{x}_0 = (x_0^1, \ldots, x_0^{N_s})$. Each of the x_0^i is an integer in the range 0 through $p-1$ where superindex i specifies the position of the site on the 1D ring. At each t the vector $\mathbf{x}_t = (x_t^1, \ldots, x_t^{N_s})$ specifies the state of the CA. Periodic boundary conditions are considered so that $x_t^{N_s+1} = x_t^1$ and $x_t^0 = x_t^{N_s}$. Let x_{t+1}^i be taken to denote the value of site i at time step $t+1$. Formally, its dependence on the values at the previous time step is given through the mapping $x_{t+1}^i = \phi(x_t^{i-r}, x_t^{i-r+1}, \ldots, x_t^i, \ldots, x_t^{i+l-1}, x_t^{i+l})$ or, equivalently $x_{t+1}^i = {}^lR_p^r(x_t^i)$, where $\phi(\cdots) \equiv {}^lR_p^r$ is the function of the site values which specifies the rule. Here r and l denote the number of cells to the right and to the left of site i respectively. Each $\mathit{configuration}_n$ in the table is then given by the integer number n which runs between 0 and $p^{r+l+1}-1$ (then $\mathit{tolerance} = 1/2$). They compare to the dynamical configuration reached by site i and its r and l first neighbors at time t and given by $\sum_{k=-r}^{l} p^{k+r} x_t^{i+k}$. The latter is the *input* of the rule. The outputs a_n for each configuration n are also integers $\in [0, p-1]$. An integer number R can then be given in base 10 to fully specify the rule ${}^lR_p^r$ as $R = \sum_{n=0}^{p^{r+l+1}-1} a_n p^n$. With all these correspondences the following expression is obtained from Eq. (3), see [3]

$$x_{t+1}^i = \sum_{n=0}^{p^{r+l+1}-1} a_n \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \tag{5}$$

Eq. (5) describes *all first-order-in-time deterministic CA rules in* 1D with no freely adjustable parameters: the p^{r+l+1} coefficients a_n directly specify the dynamical rule. For example, for Wolfram's rule ${}^1110_2^1$ $(a_0, a_1, \ldots, a_7) = (0, 1, 1, 1, 0, 1, 1, 0)$ (see Fig. 2 in [3], where all above notation is clarified).

3. Invariances of the universal CA map

Since each site on the ring satisfies Eq. (5), the whole set of equations is globally invariant upon translation modulo N_s. Eq. (5) is also invariant under reordering of the integers in $[0, p-1]$ (global complementation), reflection and shift (Galilean invariance) as discussed in the following. These invariances allow to classify all CA rules into equivalence classes reducing enormously the number of rules to a few representative ones. They are introduced in the following as theorems.

Theorem 1 *(Invariance under global complementation). The universal CA map, Eq.* (5) *remains invariant after the following set of transformations*

$$x_t^{i+k} \to p - 1 - x_t^{i+k} \tag{6}$$

$$x_{t+1}^i \to p - 1 - x_{t+1}^i \tag{7}$$

$$p - 1 - a_{p^{l+r+1}-1-n} \to a_n \tag{8}$$

Proof. Introduce the two former transformations, Eqs. (6) and (7), in Eq. (5)

$$\begin{aligned} p - 1 - x_{t+1}^i &= \sum_{n=0}^{p^{l+r+1}-1} a_n \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r}\left(p - 1 - x_t^{i+k}\right), \frac{1}{2}\right) \\ &= \sum_{n=0}^{p^{l+r+1}-1} a_n \mathcal{B}\left(n - \left(p^{l+r+1} - 1\right) + \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \end{aligned} \tag{9}$$

Now, by solving for x_{t+1}^i, by defining $n' = p^{l+r+1} - 1 - n$, by introducing the latter transformation, Eq. (8), and by using that $\mathcal{B}(x, \epsilon) = \mathcal{B}(-x, \epsilon)$ we obtain

$$\begin{aligned} x_{t+1}^i &= \sum_{n'=0}^{p^{l+r+1}-1} [p - 1 - a_{p^{l+r+1}-1-n'}] \mathcal{B}\left(-n' + \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \\ &= \sum_{n'=0}^{p^{l+r+1}-1} a_{n'} \mathcal{B}\left(n' - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \end{aligned}$$

which proves the theorem. □

When one considers specific rules, described by the universal maps above, they usually *break* this symmetry as shown in the following example.

Example. Rule ${}^0453_3^1$ (see Fig. 1, top left) with three symbols '0', '1' and '2' has range $\rho = r + l + 1 = 2$ (and hence $p^\rho = 3^2 = 9$) and coefficients $(a_0, a_1, \ldots, a_8) = (0, 1, 2, 1, 2, 1, 0, 0, 0)$ (i.e. the number 453 in base 3 in inverse order) in Eq. (5). The neighborhood contains only the cell that is updated in the next time step and the first neighboring site to the right. The rule that operates with the symbols 2, 1, 0 in the same way as rule ${}^0453_3^1$ does with symbols 0, 1, 2, respectively, can now be derived. Each coefficient b_n ($n \in [0, 8]$) in such rule is obtained from Eq. (8) as $b_n = p - 1 - a_{p^{l+r+1}-1-n}$, so that $(b_0, b_1, \ldots, b_8) = (2 - a_8, 2 - a_7, \ldots, 2 - a_0) =$

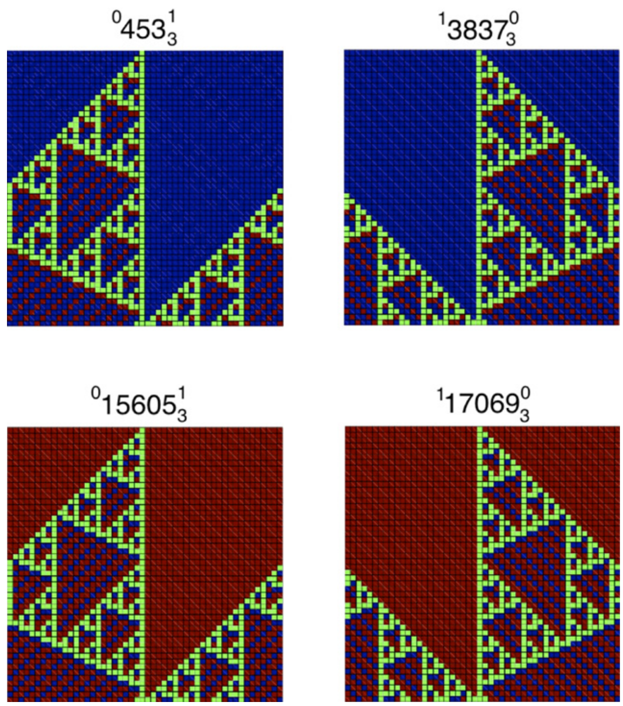

Fig. 1. Spatiotemporal evolution of rules $^{0}453^{1}_{3}$, $^{0}15605^{1}_{3}$, $^{1}3837^{0}_{3}$ and $^{1}17069^{0}_{3}$. Rules on the top are related to the ones at the bottom through global complementation. Rules on the left are related to the ones on the right through reflection. (For interpretation of the references to color in this figure, the reader is referred to the web version of this Letter.)

$(2, 2, 2, 1, 0, 1, 0, 1, 2)$, which corresponds to rule $^{0}15605^{1}_{3}$ (see Fig. 1, bottom left). The colors corresponding to symbols with values 0 (blue) and 2 (red) are exchanged in both figures, while sites with value 1 (green) remain unchanged. Rules $^{0}453^{1}_{3}$ and $^{0}15605^{1}_{3}$ belong then to the same equivalence class under global complementation.

Theorem 2 *(Invariance under reflection). The universal CA map, Eq.* (5) *remains invariant after the following set of transformations*

$$p^{k+r}x_t^{i+k} \to p^{l-k}x_t^{i+k}, \qquad k \in [-r, l] \tag{10}$$

$$n \equiv p^{k+r}x^{i+k} \to n' \equiv p^{l-k}x^{i+k}, \qquad k \in [-r, l] \tag{11}$$

$$a_{n-\sum_{k=-r}^{l}(p^{k+r}-p^{l-k})x^{i+k}} \to a_n \tag{12}$$

Proof. This theorem can be directly proved by making the corresponding transformations in Eq. (5). Introduce the two former transformations, Eqs. (10) and (11), in Eq. (5)

$$\begin{aligned} x_{t+1}^i &= \sum_{n'=0}^{p^{l+r+1}-1} a_{n'}\mathcal{B}\left(n' - \sum_{k=-r}^{l} p^{l-k}x_t^{i+k}, \frac{1}{2}\right) \\ &= \sum_{n=0}^{p^{l+r+1}-1} a_{n-\sum_{k=-r}^{l}(p^{k+r}-p^{l-k})x^{i+k}} \\ &\quad \times \mathcal{B}\left(\sum_{k=-r}^{l} p^{l-k}\left(x^{i+k} - x_t^{i+k}\right), \frac{1}{2}\right) \end{aligned}$$

whence, by using that

$$\mathcal{B}\left(\sum_{k=-r}^{l} p^{l-k}\left(x^{i+k} - x_t^{i+k}\right), \frac{1}{2}\right) = \mathcal{B}\left(\sum_{k=-r}^{l} p^{k+r}\left(x^{i+k} - x_t^{i+k}\right), \frac{1}{2}\right)$$

and introducing now Eq. (12), we obtain

$$\begin{aligned} x_{t+1}^i &= \sum_{n=0}^{p^{l+r+1}-1} a_{n-\sum_{k=-r}^{l}(p^{k+r}-p^{l-k})x^{i+k}}\mathcal{B} \\ &\quad \times \left(\sum_{k=-r}^{l} p^{k+r}\left(x^{i+k} - x_t^{i+k}\right), \frac{1}{2}\right) \\ &= \sum_{n=0}^{p^{l+r+1}-1} a_n\mathcal{B}\left(n - \sum_{k=-r}^{l} p^{l-k}x_t^{i+k}, \frac{1}{2}\right) \end{aligned}$$

which is the result that we wanted to prove. □

Invariance under reflection and under change of colors can be followed after the other in either direction since both commute. In Fig. 1 it is shown how rules $^{0}453^{1}_{3}$ and $^{0}15605^{1}_{3}$ are related through reflection to rules $^{1}3837^{0}_{3}$ and $^{1}17069^{0}_{3}$ respectively.

Example. The above theorems can be cursorily checked with the specific case of Wolfram $^{1}110^{1}_{2}$ rule for which $p^{l+r+1} - 1 = 7$, $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (0, 1, 1, 1, 0, 1, 1, 0)$. Therefore, global complementation (from Theorem 1) gives $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7) = (1-a_7, 1-a_6, 1-a_5, 1-a_4, 1-a_3, 1-a_2, 1-a_1, 1-a_0) = (1, 0, 0, 1, 0, 0, 0, 1)$, which corresponds to rule $^{1}137^{1}_{2}$. Under reflection one obtains, from Theorem 2 $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7) = (a_0, a_4, a_2, a_6, a_1, a_5, a_3, a_7) = (0, 0, 1, 1, 1, 1, 1, 0)$ which corresponds to rule $^{1}124^{1}_{2}$. Finally, global complementation after reflection gives: $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7) = (1-a_7, 1-a_3, 1-a_5, 1-a_1, 1-a_6, 1-a_2, 1-a_4, 1-a_0) = (1, 0, 0, 0, 0, 0, 1, 1)$ which corresponds to rule $^{1}193^{1}_{2}$.

Remark. When applied to the specific case of Wolfram's 256 rules $^{1}R^{1}_{2}$ global complementation and reflection symmetries, as described by Theorems 1 and 2, allow the number of independent rules under study to be reduced to just 88. This result was obtained by means of other methods [1,4,10]. As shown after the following two theorems, however, *there are further symmetries that allow this number to be further reduced to just* 85.

Theorem 3 *(Invariance under shift – Galilean invariance). The universal CA map, Eq.* (5) *remains invariant after the following set of transformations*

$$l \to l \mp 1 \tag{13}$$

$$r \to r \pm 1 \tag{14}$$

$$x_{t+1}^i \to x_{t+1}^{i\mp1} \tag{15}$$

Proof. By making the transformations implied by Eqs. (13) to (15) in Eq. (5)

$$\begin{aligned} x_{t+1}^{i\mp1} &= \sum_{n=0}^{p^{l+r+1}-1} a_n\mathcal{B}\left(n - \sum_{k'=-r\mp1}^{l\mp1} p^{k'+r\pm1}x_t^{i+k'}, \frac{1}{2}\right) \\ &= \sum_{n=0}^{p^{l+r+1}-1} a_n\mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r}x_t^{i\mp1+k}, \frac{1}{2}\right) \end{aligned} \tag{16}$$

where the change of the dummy variable $k' \to k \mp 1$ has been made. The latter expression is, of course, equivalent to

$$x_{t+1}^{i\mp1} = {}^{l}R^{r}_{p}\left(x_t^{i\mp1}\right) \tag{17}$$

Making the change $i \to i \pm 1$ (since global translation invariance holds) the invariance under shift is proved. □

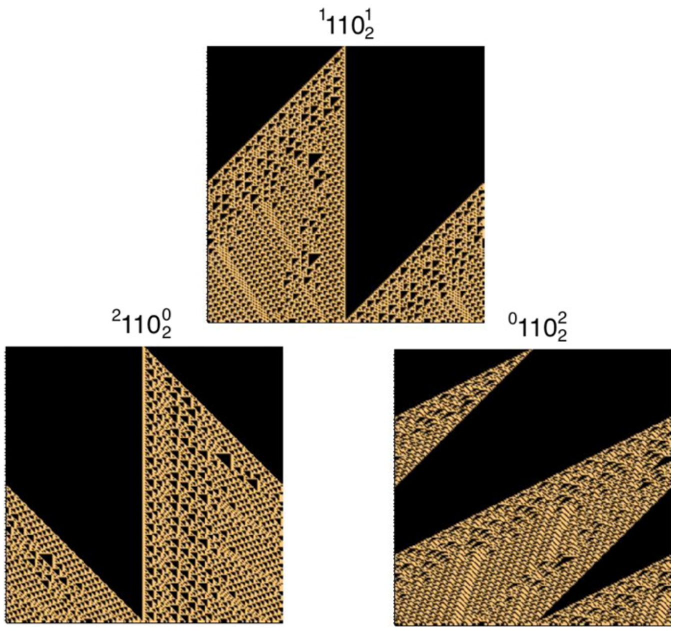

Fig. 2. Spatiotemporal evolution of rules $^{1}110_2^1$, $^{2}110_2^0$ and $^{0}110_2^2$. All three rules are related by a shift transformation and belong to the same equivalence class under shift.

The invariance under shift of the universal CA map implies the existence of classes of rules related by a breaking of this symmetry which contain, at most, ρ elements. The rules on these classes share the same code R but the neighborhoods contain different numbers of sites to the left and to the right (although the range ρ is the same). These rules satisfy the following identities

$$^{l}R_p^r\left(x_t^i\right) = {}^{l-1}R_p^{r+1}\left(x_t^{i-1}\right) \tag{18}$$

$$^{l}R_p^r\left(x_t^i\right) = {}^{l+1}R_p^{r-1}\left(x_t^{i+1}\right) \tag{19}$$

The rules are equivalent in a sense that, when known the dynamical behavior of one of them, the behavior of the others is predictable in terms of the latter just by applying a global spatial shift of the dynamical state on the ring.

Example. Rules $^{1}110_2^1$, $^{2}110_2^0$ and $^{0}110_2^2$ (see Fig. 2) are related by a shift transformation and belong to the same equivalence class under shift: once known the dynamical behavior of rule $^{1}110_2^1$, the ones of rules $^{2}110_2^0$ and $^{0}110_2^2$ are equivalent by globally shifting the dynamical state on the ring one site to the right or to the left, respectively.

Rules related by shifting transformations correspond to the same dynamical behaviors as seen by observers moving with different (constant) velocities to either side of the ring. For a given rule $^{l}R_p^r$, the shifted rules $^{l\pm v}R_p^{r\mp v}$ correspond to the same dynamics as followed by an observer moving on the ring at a constant velocity $\pm v$ (where the positive sign corresponds to motion to the left). This is the principle of Galilean invariance for cellular automata rules.

In Table 1 the above theorems are applied to rules with range $\rho = l + r + 1 = 2$ and $p = 2$. The total number of rules are 32 (i.e. 16 rules $^{0}R_2^1$ and 16 rules $^{1}R_2^0$). These rules can all be solved for the orbit by means of the induction method [3]. By using the symmetry transformations above, only 7 rules are indeed found to be independent: the dynamical behavior of the remaining 25 rules can be automatically known in terms of these seven rules, that characterize the seven equivalence classes under global complementation, reflection and shift.

The following theorem can be used to understand how a given CA rule is constructed in terms of CA rules of lower range and, as it is shown elsewhere [11], it is crucial to understand the origin of complexity in CA behavior. The theorem is referred to in the following as "constructor's theorem" and leads to uncover the invariance under construction of CA rules (and the concept of equivalence classes under construction), which is presented as a corollary.

Theorem 4 *(Constructor's theorem). Let us consider a set of p different CA rules $^{l}A_{m}{}_p^r$ with $m \in [0, p-1]$ and code $A_m = \sum_{n=0}^{p^{l+r+1}-1} a_n^{(m)} p^n$, each obeying Eq. (5), i.e.*

$$x_{t+1}^i = {}^{l}A_{m}{}_p^r\left(x_t^i\right) = \sum_{n=0}^{p^{r+l+1}-1} a_n^{(m)} \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \tag{20}$$

Then, a rule of higher range $^{l+1}R_p^r$ can be "constructed from the left" as

$$^{l+1}R_p^r\left(x_t^i\right) = \sum_{k=0}^{p-1} \mathcal{B}\left(x_t^{i+l+1} - m, \frac{1}{2}\right) {}^{l}A_{m}{}_p^r\left(x_t^i\right) \tag{21}$$

with $R = \sum_{n=0}^{p^{l+r+1}-1} \sum_{m=0}^{p-1} a_n^{(m)} p^{n+mp^{l+r+1}}$. A rule of higher range $^{l}R_p^{r+1}$ can then be also "constructed from the right" as

$$^{l}R_p^{r+1}\left(x_t^i\right) = \sum_{k=0}^{p-1} \mathcal{B}\left(x_t^{i-r-1} - m, \frac{1}{2}\right) {}^{l}A_{m}{}_p^r\left(x_t^i\right) \tag{22}$$

with $R = \sum_{n=0}^{p^{l+r+1}-1} \sum_{m=0}^{p-1} a_n^{(m)} p^{np+m}$.

Proof. By using Eqs. (20) and (21)

$$\begin{aligned}
x_{t+1}^i &= \sum_{n=0}^{p^{l+r+1}-1} \sum_{m=0}^{p-1} a_n^{(m)} \mathcal{B}\left(x_t^{i+l+1} - m, \frac{1}{2}\right) \\
&\quad \times \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \\
&= \sum_{n=0}^{p^{l+r+1}-1} \sum_{x^{i+l+1}=0}^{p-1} c_{n,x^{i+l+1}} \mathcal{B}\left(x_t^{i+l+1} - x^{i+l+1}, \frac{1}{2}\right) \\
&\quad \times \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \\
&= \sum_{n=0}^{p^{l+r+1}-1} \sum_{x^{i+l+1}=0}^{p-1} c_{n,x^{i+l+1}} \mathcal{B}\left(p^{l+r+1}\left(x_t^{i+l+1} - x^{i+l+1}\right), \frac{1}{2}\right) \\
&\quad \times \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right)
\end{aligned}$$

where $\mathcal{B}(ax, \epsilon) = \mathcal{B}(x, \epsilon)$ (for $0 < \epsilon \leqslant 1/2$ and $a > 0$ and $x \geqslant 0$ integers) has been used, and

$$c_{n,x^{i+l+1}} \equiv a_n^{(m)} \mathcal{B}\left(x^{i+l+1} - m, \frac{1}{2}\right) = \begin{cases} 0, & m \neq x^{i+l+1} \\ a_n^{(m)}, & m = x^{i+l+1} \end{cases}$$

has been introduced. By using now that $\mathcal{B}(x, \epsilon)\mathcal{B}(y, \epsilon) = \mathcal{B}(ax + by, \epsilon)$ (for any natural numbers a, b such that the non-negative integers x and y satisfy $|ax| \neq |by|$ when either x or y is non-zero and $0 < \epsilon \leqslant 1/2$)

$$x_{t+1}^i = \sum_{n'=0}^{p^{l+r+2}-1} c_{n'} \mathcal{B}\left(n' - \sum_{k=-r}^{l+1} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \tag{23}$$

Table 1
The 7 independent rules from the total of 32 rules with $p=2$ and range $\rho=2$ (${}^0R_2^1$ and ${}^1R_2^0$) and their class-equivalent rules upon global complementation (GC), reflection (R), global complementation following reflection (GCR), shift (S), shift following global complementation (SGC), shift following reflection (SR) and shift following global complementation following reflection (SGCR).

Rule	(a_0,a_1,a_2,a_3)	GC	R	GCR	S	SGC	SR	SGCR
${}^0 0_2^1$	(0, 0, 0, 0)	${}^0 15_2^1$	${}^1 0_2^0$	${}^1 15_2^0$	${}^1 0_2^0$	${}^1 15_2^0$	${}^0 0_2^1$	${}^0 15_2^1$
${}^0 1_2^1$	(1, 0, 0, 0)	${}^0 7_2^1$	${}^1 1_2^0$	${}^1 7_2^0$	${}^1 1_2^0$	${}^1 7_2^0$	${}^0 1_2^1$	${}^0 7_2^1$
${}^0 2_2^1$	(0, 1, 0, 0)	${}^0 11_2^1$	${}^1 4_2^0$	${}^1 13_2^0$	${}^1 2_2^0$	${}^1 11_2^0$	${}^0 4_2^1$	${}^0 13_2^1$
${}^0 3_2^1$	(1, 1, 0, 0)	${}^0 3_2^1$	${}^1 5_2^0$	${}^1 5_2^0$	${}^1 3_2^0$	${}^1 3_2^0$	${}^0 5_2^1$	${}^0 5_2^1$
${}^0 6_2^1$	(0, 1, 1, 0)	${}^0 9_2^1$	${}^1 6_2^0$	${}^1 9_2^0$	${}^1 6_2^0$	${}^1 9_2^0$	${}^0 6_2^1$	${}^0 9_2^1$
${}^0 8_2^1$	(0, 0, 0, 1)	${}^0 14_2^1$	${}^1 8_2^0$	${}^1 14_2^0$	${}^1 8_2^0$	${}^1 14_2^0$	${}^0 8_2^1$	${}^0 14_2^1$
${}^0 10_2^1$	(0, 1, 0, 1)	${}^0 10_2^1$	${}^1 12_2^0$	${}^1 12_2^0$	${}^1 10_2^0$	${}^1 10_2^0$	${}^0 12_2^1$	${}^0 12_2^1$

where $n'=\sum_{k=-r}^{l+1} p^{k+r}x^{i+k}=n+p^{l+r+1}x^{i+l+1}$ and $c_{n'}=a^{(m)}_{n'-mp^{l+r+1}}$. The new rule, Eq. (23) has then the code $R=\sum_{n'=0}^{p^{l+r+2}-1} c_{n'}p^{n'}=\sum_{n=0}^{p^{l+r+1}-1}\sum_{m=0}^{p-1} a_n^{(m)} p^{n+mp^{l+r+1}}$.

The proof of the statement on the construction from the right proceeds in a similar manner. By using Eqs. (20) and (22)

$$\begin{aligned}
x_{t+1}^i &= \sum_{n=0}^{p^{l+r+1}-1}\sum_{m=0}^{p-1} a_n^{(m)}\mathcal{B}\left(x_t^{i-r-1}-m,\frac{1}{2}\right) \\
&\quad\times\mathcal{B}\left(n-\sum_{k=-r}^{l}p^{k+r}x_t^{i+k},\frac{1}{2}\right) \\
&= \sum_{n=0}^{p^{l+r+1}-1}\sum_{x^{i-r-1}=0}^{p-1} c_{n,x^{i-r-1}}\mathcal{B}\left(x_t^{i-r-1}-x^{i-r-1},\frac{1}{2}\right) \\
&\quad\times\mathcal{B}\left(n-\sum_{k=-r}^{l}p^{k+r}x_t^{i+k},\frac{1}{2}\right) \\
&= \sum_{n=0}^{p^{l+r+1}-1}\sum_{x^{i-r-1}=0}^{p-1} c_{n,x^{i-r-1}}\mathcal{B}\left(x_t^{i-r-1}-x^{i-r-1},\frac{1}{2}\right) \\
&\quad\times\mathcal{B}\left(np-\sum_{k=-r}^{l}p^{k+r+1}x_t^{i+k},\frac{1}{2}\right)
\end{aligned}$$

where $\mathcal{B}(ax,\epsilon)=\mathcal{B}(x,\epsilon)$ (for $0<\epsilon\leqslant 1/2$ and $a>0$ and $x\geqslant 0$ integers) has been again used, and

$$c_{n,x^{i-r-1}}\equiv a_n^{(m)}\mathcal{B}\left(x^{i-r-1}-m,\frac{1}{2}\right)=\begin{cases}0, & m\neq x^{i-r-1}\\ a_n^{(m)}, & m=x^{i-r-1}\end{cases}$$

has been introduced. By using now again that $\mathcal{B}(x,\epsilon)\mathcal{B}(y,\epsilon)=\mathcal{B}(ax+by,\epsilon)$ (for any natural numbers a, b such that the non-negative integers x and y satisfy $|ax|\neq|by|$ when either x or y is non-zero and $0<\epsilon\leqslant 1/2$)

$$x_{t+1}^i=\sum_{n'=0}^{p^{l+r+2}-1} c_{n'}\mathcal{B}\left(n'-\sum_{k=-r-1}^{l}p^{k+r+1}x_t^{i+k},\frac{1}{2}\right) \tag{24}$$

where $n'=\sum_{k=-r-1}^{l}p^{k+r+1}x^{i+k}=np+x^{i-r-1}$ and $c_{n'}=a^{(m)}_{(n'-m)/p}$. The new rule, Eq. (24) has then the code $R=\sum_{n'=0}^{p^{l+r+2}-1}c_{n'}p^{n'}=\sum_{n=0}^{p^{l+r+1}-1}\sum_{m=0}^{p-1}a_n^{(m)}p^{np+m}$ and the result is proved. □

Example. Theorem 4 can be straightforwardly applied to any rule. For example Wolfram rule ${}^1 30_2^1$ is known to be a random number generator. It has vector $(a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)=(0,1,1,1,1,0,0,0)$. To obtain the construction from the left, separate $(0,1,1,1,1,0,0,0)$ into $p=2$ consecutive blocks. Rules with vectors $(0,1,1,1)$ and $(1,0,0,0)$ are obtained, which correspond, respectively, to rules ${}^0 14_2^1$ and ${}^0 1_2^1$. To construct the same rule from the right, separate the odd entries and the even entries of $(0,1,1,1,1,0,0,0)$. Rules $(0,1,1,0)$ and $(1,1,0,0)$ which correspond to rules ${}^1 6_2^0$ and ${}^1 3_2^0$ are, hence, obtained.

Corollary *(Construction invariance). Let us consider a CA rule ${}^lA_p^r$ with code $A=\sum_{n=0}^{p^{l+r+1}-1}a_np^n$. Then rules ${}^{l+1}B_p^r$ and ${}^lC_p^{r+1}$ with codes $B=\sum_{n=0}^{p^{l+r+1}-1}\sum_{m=0}^{p-1}a_np^{n+mp^{l+r+1}}$ and $C=\sum_{n=0}^{p^{l+r+1}-1}\sum_{m=0}^{p-1}a_np^{np+m}$, respectively, have the same dynamical behavior and are called equivalent under construction.*

Proof. Rules ${}^{l+1}B_p^r$ and ${}^lC_p^{r+1}$ are constructed from the left and from the right using rule ${}^lA_p^r$ as the only constructing rule (i.e. $\forall m$) in the constructor theorem. This means that the new site added to the left (or to the right) is irrelevant and, independently of its value, the output is entirely governed by the rule of lower range ${}^lA_p^r$. This can be straightforwardly seen from Eq. (21) (and, analogously, for the construction from the right) since,

$$\begin{aligned}
{}^{l+1}B_p^r\left(x_t^i\right) &= \sum_{m=0}^{p-1}\mathcal{B}\left(x_t^{i+l+1}-m,\frac{1}{2}\right){}^lA_p^r\left(x_t^i\right) \\
&= {}^lA_p^r\left(x_t^i\right)\sum_{m=0}^{p-1}\mathcal{B}\left(x_t^{i+l+1}-m,\frac{1}{2}\right)={}^lA_p^r\left(x_t^i\right)
\end{aligned}$$

since x_t^{i+l+1} is equal to one integer within $[0,p-1]$ and the sum over m checks for all integers in this interval and, hence, $\sum_{m=0}^{p-1}\mathcal{B}(x_t^{i+l+1}-m,\frac{1}{2})=1$. Proving equivalence under construction of rule ${}^lC_p^{r+1}$ is similar. □

Example.

- All rules ${}^l0_p^r$ are equivalent under construction to rule ${}^0 0_p^0$.
- All rules ${}^lA_p^r$ with $A=p^{p^{l+r+1}}-1$ are equivalent under construction to rule ${}^0B_p^0$, with $B=p^p-1$.
- Wolfram's rules ${}^1 102_2^1$ and ${}^1 60_2^1$ are equivalent under construction to rule ${}^0 6_2^1$. □

Since constructing equivalent rules of higher range is now straightforward from the above corollary specially from the left (one concatenates the vector of the rule after itself $p-1$ times to form a vector p times larger in size as the original one), we introduce the following definition for future reference.

Definition 1 *(Copying rules).* The rule ${}^lA_p^r$ is said to be *copied* to a higher range if it is used as the only rule in constructing ${}^{l+1}R_2^r$

Table 2
The 85 independent rules out of the 256 Wolfram's rules ${}^{1}R_2^1$.

${}^{1}0_2^1$	${}^{1}1_2^1$	${}^{1}2_2^1$	${}^{1}3_2^1$	${}^{1}4_2^1$	${}^{1}5_2^1$	${}^{1}6_2^1$	${}^{1}7_2^1$	${}^{1}8_2^1$	${}^{1}9_2^1$	${}^{1}10_2^1$
${}^{1}11_2^1$	${}^{1}12_2^1$	${}^{1}13_2^1$	${}^{1}14_2^1$	${}^{1}15_2^1$	${}^{1}18_2^1$	${}^{1}19_2^1$	${}^{1}22_2^1$	${}^{1}23_2^1$	${}^{1}24_2^1$	${}^{1}25_2^1$
${}^{1}26_2^1$	${}^{1}27_2^1$	${}^{1}28_2^1$	${}^{1}29_2^1$	${}^{1}30_2^1$	${}^{1}32_2^1$	${}^{1}33_2^1$	${}^{1}35_2^1$	${}^{1}36_2^1$	${}^{1}37_2^1$	${}^{1}38_2^1$
${}^{1}40_2^1$	${}^{1}41_2^1$	${}^{1}42_2^1$	${}^{1}43_2^1$	${}^{1}44_2^1$	${}^{1}45_2^1$	${}^{1}46_2^1$	${}^{1}50_2^1$	${}^{1}54_2^1$	${}^{1}56_2^1$	${}^{1}57_2^1$
${}^{1}58_2^1$	${}^{1}60_2^1$	${}^{1}62_2^1$	${}^{1}72_2^1$	${}^{1}73_2^1$	${}^{1}74_2^1$	${}^{1}76_2^1$	${}^{1}77_2^1$	${}^{1}78_2^1$	${}^{1}90_2^1$	${}^{1}94_2^1$
${}^{1}104_2^1$	${}^{1}105_2^1$	${}^{1}106_2^1$	${}^{1}108_2^1$	${}^{1}110_2^1$	${}^{1}122_2^1$	${}^{1}126_2^1$	${}^{1}128_2^1$	${}^{1}130_2^1$	${}^{1}132_2^1$	${}^{1}134_2^1$
${}^{1}136_2^1$	${}^{1}138_2^1$	${}^{1}140_2^1$	${}^{1}142_2^1$	${}^{1}146_2^1$	${}^{1}150_2^1$	${}^{1}152_2^1$	${}^{1}154_2^1$	${}^{1}156_2^1$	${}^{1}160_2^1$	${}^{1}162_2^1$
${}^{1}164_2^1$	${}^{1}168_2^1$	${}^{1}170_2^1$	${}^{1}172_2^1$	${}^{1}178_2^1$	${}^{1}184_2^1$	${}^{1}200_2^1$	${}^{1}232_2^1$			

from the left, i.e. if ${}^{l}(A_m)_p^r = {}^{l}A_2^r$ $\forall m$ in Eq. (21) to produce a rule equivalent under construction.

Example. To copy rule ${}^{0}6_2^1$ to a higher range $\rho = 3$ its vector $(a_0, a_1, a_2, a_3) = (0, 1, 1, 0)$ is concatenated to itself, adding the same sequence of zeroes and ones after it, i.e. $(0, 1, 1, 0, 0, 1, 1, 0)$. The latter corresponds to rule ${}^{1}102_2^1$ which is the copy of ${}^{0}6_2^1$ to range $\rho = 3$. This is consistent with the construction from the left of rule ${}^{1}102_2^1$ as established in Theorem 4. Both rules belong to the same class under construction and display identical dynamical behavior.

Example. To copy rule ${}^{0}25_3^0$ to a higher range $\rho = 2$ its vector $(a_0, a_1, a_2) = (1, 2, 2)$ is concatenated after itself two times (since $p = 3$), i.e. $(1, 2, 2, 1, 2, 2, 1, 2, 2)$. The latter corresponds to rule ${}^{1}18925_3^0$ which is, therefore, equivalent under construction to rule ${}^{0}25_3^0$.

Remark. When Wolfram's rules ${}^{1}R_2^1$ are considered, the shift transformation combined with invariance under construction allows the 88 equivalence classes (under global complementation and reflection) to be reduced to only 85. Rules ${}^{1}34_2^1$, ${}^{1}51_2^1$ and ${}^{1}170_2^1$ are equivalent under construction from the left to rules ${}^{0}2_2^1$, ${}^{0}3_2^1$ and ${}^{0}10_2^1$, which are related through shift to rules ${}^{1}2_2^0$, ${}^{1}3_2^0$ and ${}^{1}10_2^0$. The latter allow, in turn, to construct the equivalent rules ${}^{1}12_2^1$, ${}^{1}15_2^1$ and ${}^{1}204_2^1$ from the right. This means that rules ${}^{1}12_2^1$, ${}^{1}15_2^1$ and ${}^{1}204_2^1$ are related through shift to rules ${}^{1}34_2^1$, ${}^{1}51_2^1$ and ${}^{1}170_2^1$. This means that, out of these 6 rules, only 3 are independent, and these can be chosen to be ${}^{1}12_2^1$, ${}^{1}15_2^1$ and ${}^{1}170_2^1$. Table 2 lists all 85 independent Wolfram' rules obtained from global complementation, reflection, shift and all possible combinations of these operations.

4. Modular algebra, time-reversal symmetry and symmetry upon addition modulo *p*

Modular algebra can be formulated within the $\mathcal{B}$-calculus introduced in [3] and briefly sketched in Section 2. Such algebra proves very useful to gain insight in CA dynamics. It leads to the uncovering of new symmetries, under addition modulo p and under time-reversal, whose crucial interest lies in the relationship that they suggest between local and global behavior on one hand and short-time and long-time behavior on the other. In Definition 2 the modular sum (p-sum) and subtraction (p-subtraction) are introduced and a series of theorems exposing the above mentioned symmetries are proved.

Definition 2 *(Modular sum and subtraction).* Within $\mathcal{B}$-calculus, the following operations for integer numbers a and $b \in [0, p-1]$ can be defined:

(i) *p-sum*: $a +_p b = \sum_{q=0}^{1} \sum_{r=0}^{p-1} r\mathcal{B}(a + b - (qp + r), \frac{1}{2})$;
(ii) *p-subtraction*: $a -_p b = \sum_{q=0}^{1} \sum_{r=0}^{p-1} r\mathcal{B}(a - b - (r - qp), \frac{1}{2})$.

Theorem 5. *The following relations hold*:

(i) *commutativity*: $a +_p b = b +_p a$;
(ii) *if* $a +_p b = c$ *then* $a = c -_p b$ *and* $b = c -_p a$ *also hold*;
(iii) *let* $\mathcal{R}_p(\sum_{i=0}^{n-1} a_i) \equiv a_0 +_p \cdots +_p a_{n-1}$ *(modular sum of n integers* $\in [0, p-1]$*) then* $\mathcal{R}_p(\sum_{i=0}^{n-1} a_i) = \sum_{q=0}^{n-1} \sum_{r=0}^{p-1} r\mathcal{B}(\sum_{i=0}^{n-1} a_i - (qp + r), \frac{1}{2})$;
(iv) *associativity*: $a +_p (b +_p c) = (a +_p b) +_p c$.

Proof. (i) can be proved easily since

$$a +_p b = \sum_{q=0}^{1} \sum_{r=0}^{p-1} r\mathcal{B}\left(a + b - (qp + r), \frac{1}{2}\right)$$
$$= \sum_{q=0}^{1} \sum_{r=0}^{p-1} r\mathcal{B}\left(b + a - (qp + r), \frac{1}{2}\right) = b +_p a$$

The proof of (ii) proceeds by observing that

$$c = a +_p b = \sum_{q=0}^{1} \sum_{r=0}^{p-1} r\mathcal{B}\left(a + b - (qp + r), \frac{1}{2}\right)$$
$$= \sum_{q=0}^{1} \sum_{r=0}^{p-1} (a + b - qp)\mathcal{B}\left(a + b - (qp + r), \frac{1}{2}\right)$$
$$= a + b - \sum_{q=0}^{1} \sum_{r=0}^{p-1} qp\mathcal{B}\left(a + b - (qp + r), \frac{1}{2}\right)$$

where to get the next-to-last equality it has been used that $\mathcal{B}(a + b - (qp + r), \frac{1}{2}) = 1$ for the only values of q and r which satisfy $a + b = r + pq$ and zero otherwise. Since q and r always exist and are unique, the fact that $\sum_{q=0}^{1} \sum_{r=0}^{p-1} \mathcal{B}(a + b - (qp + r), \frac{1}{2}) = 1$ has been also used to get the last equality. Then

$$a = c - b + \sum_{q=0}^{1} \sum_{r=0}^{p-1} qp\mathcal{B}\left(a + b - (qp + r), \frac{1}{2}\right)$$
$$= \sum_{q=0}^{1} \sum_{r=0}^{p-1} (c - b + qp)\mathcal{B}\left(a + b - (qp + r), \frac{1}{2}\right)$$
$$= \sum_{q=0}^{1} \sum_{r'=0}^{p-1} r'\mathcal{B}\left(r' - c + b - qp, \frac{1}{2}\right)$$
$$= \sum_{q=0}^{1} \sum_{r'=0}^{p-1} r'\mathcal{B}\left(c - b - (r' - qp), \frac{1}{2}\right) = c -_p b$$

where the dummy index $r' \equiv c - b + qp = a + c - r$ has been introduced. Similarly, one has $b = c -_p a$.

Induction can be now used to prove (iii). The result is valid for $n = 2$ since, then, it reduces to the definition of the p-sum in Definition 2(i). Let the result be assumed valid for n integers. For $n+1$ integers $\in [0, p-1]$ we, then, have

$$\begin{aligned}\mathcal{R}_p\left(\sum_{i=0}^{n} a_i\right) &= \mathcal{R}_p\left(\sum_{i=0}^{n-1} a_i\right) +_p a_n \\ &= \sum_{\tilde q=0}^{1}\sum_{\tilde r=0}^{p-1} \tilde r \mathcal{B}\left(a_n + \sum_{q=0}^{n-1}\sum_{r=0}^{p-1} r \right. \\ &\quad \left. \times \mathcal{B}\left(\sum_{i=0}^{n-1} a_i - (qp+r), \frac{1}{2}\right) - (\tilde q p + \tilde r), \frac{1}{2}\right) \\ &= \sum_{\tilde q=0}^{1}\sum_{\tilde r=0}^{p-1} \tilde r \mathcal{B}\left(-\tilde r + \sum_{i=0}^{n} a_i - p\sum_{q=0}^{n-1}\sum_{r=0}^{p-1}(q+\tilde q)\right. \\ &\quad \left. \times \mathcal{B}\left(\sum_{i=0}^{n-1} a_i - (qp+r), \frac{1}{2}\right), \frac{1}{2}\right) \\ &= \sum_{q'=0}^{n}\sum_{r'=0}^{p-1} r' \mathcal{B}\left(\sum_{i=0}^{n} a_i - (q'p + r'), \frac{1}{2}\right)\end{aligned}$$

where we have defined $r' \equiv \tilde r$ and

$$q' \equiv \sum_{q=0}^{n-1}\sum_{r=0}^{p-1}(q+\tilde q)\mathcal{B}\left(\sum_{i=0}^{n-1} a_i - (qp+r), \frac{1}{2}\right)$$

which is an integer $\in [0, n]$, since $\tilde q$ can be either 0 or 1. The above proves (iii). Then (iv) is a consequence of (iii) and the associativity of the conventional sum of integers. □

We are now able to prove the following theorem which, in fact, is inspired in previous work by Fredkin on reversible logic (see [6] and references therein).

Theorem 6 *(Time-reversal invariance). For any CA rule ${}^l R_p^r(x_t^i)$ described by Eq. (5), the rule ${}^l R_p^r(x_t^i) -_p x_{t-1}^i$ and denoted $rev[{}^l R_p^r(x_t^i)]$ is time-reversal invariant, i.e. invariant upon the transformation $t+1 \leftrightarrow t-1$.*

Proof. We have

$$x_{t+1}^i = {}^l R_p^r\left(x_t^i\right) -_p x_{t-1}^i \tag{25}$$

And, by introducing the time-reversal transformation $t+1 \leftrightarrow t-1$

$$x_{t-1}^i = {}^l R_p^r\left(x_t^i\right) -_p x_{t+1}^i$$

but now, by using results (i) and (ii) from Theorem 5 we obtain

$$x_{t-1}^i +_p x_{t+1}^i = {}^l R_p^r\left(x_t^i\right) \quad \rightarrow \quad x_{t+1}^i = {}^l R_p^r\left(x_t^i\right) -_p x_{t-1}^i$$

which proves the invariance under time-reversal. □

By using Eqs. (5) and (ii) from Definition 2, Eq. (25) can be alternatively written as

$$x_{t+1}^i = \sum_{n=0}^{p^{r+l+1}-1}\left(a_n -_p x_{t-1}^i\right)\mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \tag{26}$$

$$\begin{aligned} &= \sum_{n=0}^{p^{r+l+1}-1}\sum_{q=0}^{1}\sum_{r=0}^{p-1} r\mathcal{B}\left(a_n - x_{t-1}^i - (r - qp), \frac{1}{2}\right) \\ &\quad \times \mathcal{B}\left(n - \sum_{k=-r}^{l} p^{k+r} x_t^{i+k}, \frac{1}{2}\right) \end{aligned} \tag{27}$$

For $p = 2$, Eq. (26) can be written as

$$x_{t+1}^i = \sum_{n=0}^{2^{r+l+1}-1}\left|a_n - x_{t-1}^i\right|\mathcal{B}\left(n - \sum_{k=-r}^{l} 2^{k+r} x_t^{i+k}, \frac{1}{2}\right) \tag{28}$$

A correction is here to be made: Eq. (38) in [3] is only valid for $p = 2$ as it was written there. In the general case, it is Eq. (26) (or, alternatively, Eq. (27)) the correct universal map for any reversible automata with arbitrary number of symbols p. It is to be noted that two initial conditions at times $t = 0$ and $t = 1$ are needed to evolve the reversible CA rule. In Fig. 3 the spatiotemporal evolution of the reversible rule $rev[{}^1 215_3^1]$ in the forward direction in time (left), obtained from Eq. (26) and starting from a single seed with value 1 at $t = 0$ and $t = 1$, is shown. The backward direction in time (right) is followed by introducing the last and the next-to-the-last states reached by the CA in the forward direction, at $t = 0$ and $t = 1$ respectively. The reversibility of the CA rule is clear, since the original state is again reached following exactly the same chain of dynamical states as in the forward direction but now to the past: for any forward trajectory there exists one and only one backward trajectory as well.

Remark. Theorem 6 is quite general for all cellular automata first-order-in-time and the rule ${}^l R_p^r(x_t^i)$ in Eq. (25) can indeed be two- or three-dimensional and of arbitrary topology, by using the universal maps for higher-dimensional CAs given in [3] (note that Eq. (26) is obtained for 1D CAs).

For totalistic cellular automata, a subset of the total possibilities described by Eq. (5), the following map was also derived [3]

$$x_{t+1}^i = \sum_{s=0}^{\rho(p-1)} \sigma_s \mathcal{B}\left(s - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right) \tag{29}$$

where $\rho = l + r + 1$ and again each σ_s is an integer value between 0 and $p-1$ like the inputs and the output of the rule, which is now labelled as ${}^l RT_p^r$, with $R = \sum_{s=0}^{\rho(p-1)} \sigma_s p^s$.

Eq. (29) is a particular case of Eq. (5) since the output at a later time depends only on the sum of the values over the sites in the neighborhood and not on their relative position (therefore, such totalistic rules are invariant under reflection). Starting from a totalistic rule with vector $(\sigma_0, \sigma_1, \ldots, \sigma_{\rho(p-1)})$ described by Eq. (29) the vector specifying the normal rule as described by Eq. (5) $(a_0, a_1, \ldots, a_{p^{l+r+1}-1})$ can be calculated from the following system of equations (for all possible integer values of $k \in [-r, l]$ and $x^{i+k} \in [0, p-1]$) [3]

$$n = \sum_{k=-r}^{l} p^{k+r} x^{i+k}, \qquad s = \sum_{k=-r}^{l} x^{i+k}, \qquad a_n = \sigma_s \tag{30}$$

As discussed above, R specifies in Eq. (5) the vector $(a_0, a_1, \ldots, a_{p^{l+r+1}-1})$, since it provides the decimal representation of the base p number $a_{p^{l+r+1}-1} \ldots a_1 a_0$. However, in the case of totalistic rules, the number R specifies the vector $(\sigma_0, \sigma_1, \ldots, \sigma_{\rho(p-1)})$, since it coincides with the decimal representation of the base p number $\sigma_{\rho(p-1)} \ldots \sigma_1 \sigma_0$ [3].

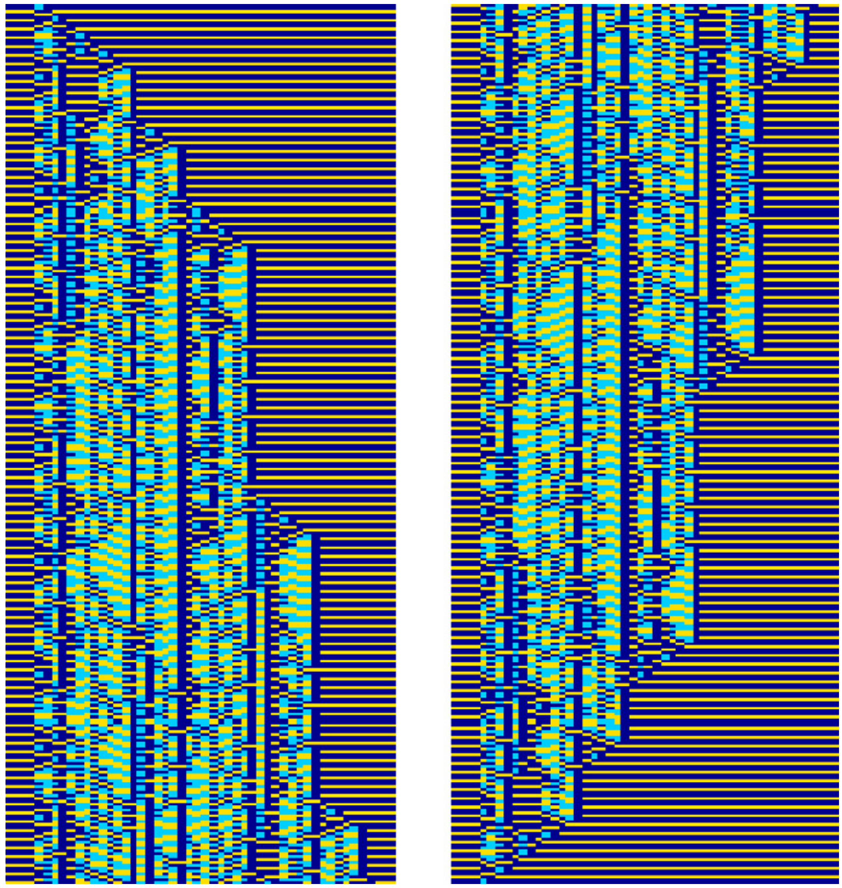

Fig. 3. Spatiotemporal evolution of the reversible rule $rev[^1 215^1_3]$ in the forward (left) and the backward (right) directions in time, obtained from Eq. (26).

Theorem 7 *(Invariance upon addition modulo p). The totalistic universal CA map, Eq. (29) remains invariant after the following set of transformations*

$$\sum_{k=-r}^{l} x_t^{i+k} \to \sum_{k=-r}^{l} x_t^{i+k} + mp \tag{31}$$

$$s - mp \to s' \tag{32}$$

$$\sigma_{s'+mp} \to \sigma_{s'} \tag{33}$$

where m is any integer $\in [0, \rho(p-1)]$.

Proof. Introducing the three transformations, Eqs. (31) to (33), each one after the other in Eq. (29) we have

$$x_{t+1}^i = \sum_{s=mp}^{\rho(p-1)+mp} \sigma_s \mathcal{B}\left(s - \sum_{k=-r}^{l} x_t^{i+k} - mp, \frac{1}{2}\right)$$
$$= \sum_{s'=0}^{\rho(p-1)} \sigma_{s'+mp} \mathcal{B}\left(s' - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right)$$
$$= \sum_{s'=0}^{\rho(p-1)} \sigma_{s'} \mathcal{B}\left(s' - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right)$$

which proves the result. □

Most rules break this symmetry. The only exceptions are, of course, the ones that satisfy $\sigma_s = \sigma_{s+mp}$, $\forall m$ so that $s + mp \in [0, \rho(p-1)]$. And specially interesting within these are those which put every symbol $[0, p-1]$ into play during the time evolution. Because of their importance, and for reference, these rules invariant upon addition modulo p can be called *Pascal rules*: these rules, as observed below, reproduce after a bijective application all Pascal simplices modulo p. When $\rho = 2$, the Pascal simplex coincides with the Pascal triangle. When $\rho > 2$ the Pascal simplex is related to the multinomial expansion modulo p. Pascal rules are a subset of the so-called additive cellular automata, for which an algebraic theory was formulated [12].

Definition 3 *(Pascal rules).* A totalistic rule ${}^l RT_p^r$ is called Pascal rule if it satisfies the following property

$$\sigma_{s+mp} = \sigma_s = s \tag{34}$$

where m is an integer so that $s + mp \in [0, \rho(p-1)]$. These rules perform the addition modulo p of all site values contained in the neighborhood.

Theorem 8 *(Pascal rules perform the addition modulo p). A Pascal rule* ${}^l RT_p^r$ *performs the addition modulo p of all site values contained in the neighborhood, i.e. it has the form*

$$x_{t+1}^i = \sum_{m=0}^{\rho} \sum_{s=0}^{p-1} s\mathcal{B}\left(s + mp - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right)$$
$$= \mathcal{R}_p\left(\sum_{k=-r}^{l} x_t^{i+k}\right) \tag{35}$$

where $\mathcal{R}_p(x)$ *is the remainder upon division of an integer number x by p.*

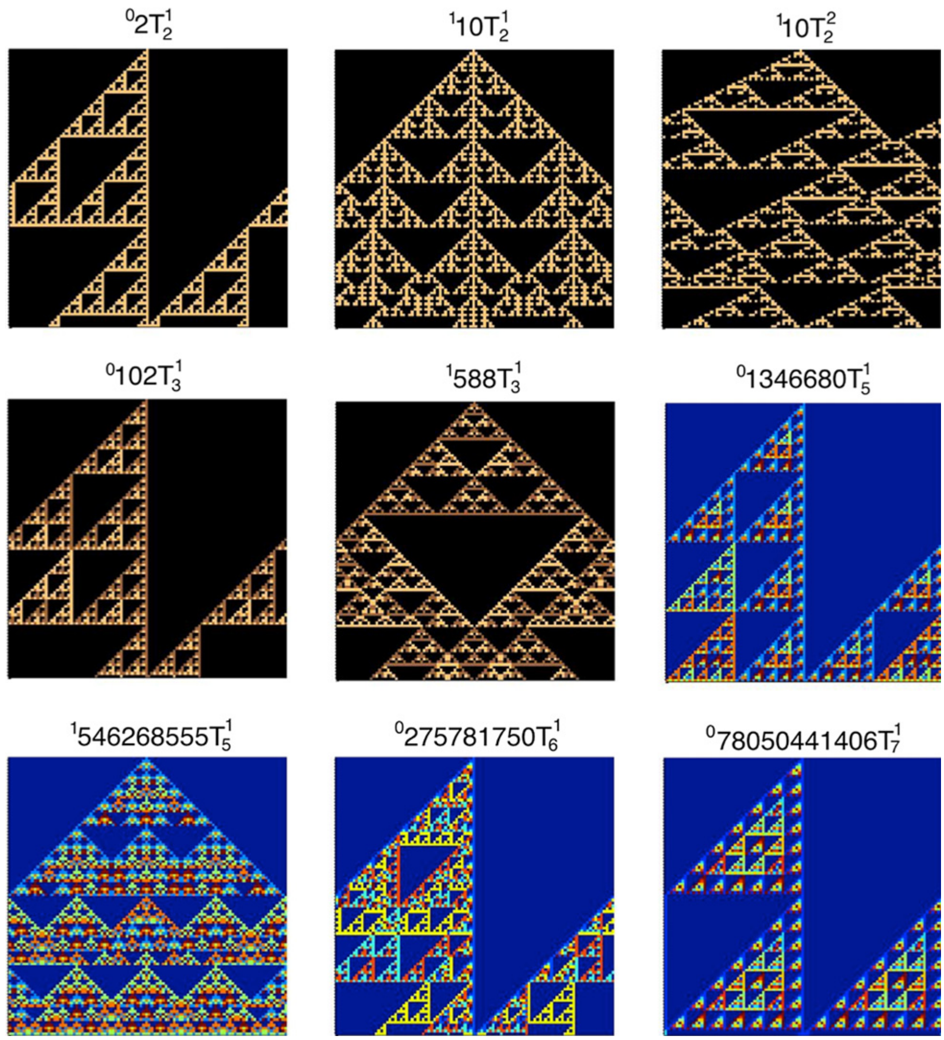

Fig. 4. Spatiotemporal evolution of some Pascal rules with totalistic codes indicated in the figure. The number of different colors in the figures coincides with p. Regular, nested structures arise in every case.

Proof. The first of the equalities in Eq. (35) is obtained from the totalistic universal map Eq. (29) by using the definition of the Pascal rule above,

$$\begin{aligned} x_{t+1}^i &= \sum_{s=0}^{\rho(p-1)} \sigma_s \mathcal{B}\left(s - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right) \\ &= \sum_{s+mp=0}^{\rho(p-1)} \sigma_{s+mp} \mathcal{B}\left(s + mp - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right) \\ &= \sum_{m=0}^{\rho} \sum_{s=0}^{p-1} s \mathcal{B}\left(s + mp - \sum_{k=-r}^{l} x_t^{i+k}, \frac{1}{2}\right) \end{aligned} \quad (36)$$

The second equality is then proved since it coincides with result (iii) of Theorem 5, with $\rho = n - 1$. □

The structure of these rules is pretty simple. They have vectors $(\sigma_0, \ldots, \sigma_{\rho p})$ with the structure (S, S, S'), where S is a chain of integers $0, 1, 2, \ldots, (p-1)$ repeated until the ρp positions characterizing the rule are filled. S' is the chain S truncated when position $\rho(p-1)$ is reached.

Examples.

- ${}^0 2T_2^1$ with $(\sigma_0, \sigma_1, \sigma_2) = (0, 1, 0)$, i.e. $x_{t+1}^i = \mathcal{R}_2(\sum_{k=-1}^{0} x_t^{i+k})$.
- ${}^1 10T_2^1$ with $(\sigma_0, \sigma_1, \sigma_2, \sigma_3) = (0, 1, 0, 1)$, i.e. $x_{t+1}^i = \mathcal{R}_2(\sum_{k=-1}^{1} x_t^{i+k})$.
- ${}^1 10T_2^2$ with $(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4) = (0, 1, 0, 1, 0)$, i.e. $x_{t+1}^i = \mathcal{R}_2(\sum_{k=-1}^{2} x_t^{i+k})$.
- ${}^0 102T_3^1$ with $(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4) = (0, 1, 2, 0, 1)$, i.e. $x_{t+1}^i = \mathcal{R}_3(\sum_{k=-1}^{0} x_t^{i+k})$.
- ${}^1 588T_3^1$ with $(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6) = (0, 1, 2, 0, 1, 2, 0)$, i.e. $x_{t+1}^i = \mathcal{R}_3(\sum_{k=-1}^{1} x_t^{i+k})$.
- ${}^0 1346680T_5^1$ with $(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8) = (0, 1, 2, 3, 4, 0, 1, 2, 3)$, i.e. $x_{t+1}^i = \mathcal{R}_5(\sum_{k=-1}^{0} x_t^{i+k})$.
- ${}^1 546268555T_5^1$ with $(\sigma_0, \sigma_1, \ldots, \sigma_{11}, \sigma_{12}) = (0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, 2)$, i.e. $x_{t+1}^i = \mathcal{R}_5(\sum_{k=-1}^{1} x_t^{i+k})$.
- ${}^0 275781750T_6^1$ with $(\sigma_0, \sigma_1, \ldots, \sigma_9, \sigma_{10}) = (0, 1, 2, 3, 4, 5, 0, 1, 2, 3, 4)$, i.e. $x_{t+1}^i = \mathcal{R}_6(\sum_{k=-1}^{0} x_t^{i+k})$.
- ${}^0 78050441406T_7^1$ with $(\sigma_0, \sigma_1, \ldots, \sigma_{11}, \sigma_{12}) = (0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5)$, i.e. $x_{t+1}^i = \mathcal{R}_7(\sum_{k=-1}^{0} x_t^{i+k})$.

The spatiotemporal evolution of all above Pascal rules is shown in Fig. 4. In Fig. 5 a detail of the first time steps of the evolution of

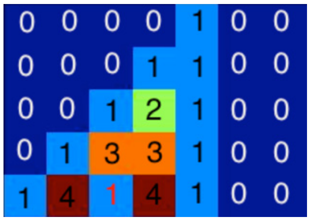

Fig. 5. Detail of the former stages of the spatiotemporal evolution from a single seed of the Pascal rule with totalistic code ${}^{0}13466 80T_5^1$. The Pascal structure modulo 5 is clearly recognized. The '1' colored red at the bottom of the figure corresponds to the value 6 in the Pascal triangle, which happens to be equal to 1 modulo 5. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this Letter.)

rule ${}^{0}1346680T_5^1$ is shown making apparent how it, indeed, calculates the Pascal triangle modulo 5.

5. Conclusions

In this Letter, the universal CA map recently derived [3] has been shown to be invariant after certain transformations that allow to classify CA rules into different equivalent classes. Some specific rules are also invariant upon these transformations and are, therefore, symmetrical upon them. Some others break symmetries, but since the universal map is invariant, the existence of equivalence classes with a number of members (i.e. cardinal) higher than 1 then follows. Besides the well-known global complementation and reflection, this Letter has uncovered important new symmetries in CA behavior: shift/Galilean invariance and invariance under construction. When applied to the Wolfram 256 elementary CA rules, it has been shown here how the number of independent rules can indeed be reduced to just 85. All these symmetries can be handled in a systematic way for every conceivable CA. Within $\mathcal{B}$-calculus, it has also been shown how modular arithmetic can be formulated, and the invariance under time-reversal of universal CA maps (which depend on the previous time step through the modular subtraction) has also been established. A new invariance (under addition modulo p) and systematic way of constructing certain totalistic 1D CA rules with this symmetry, which calculate the Pascal simplices modulo an integer number p, has then also been uncovered.

Although certain symmetries of CA evolution might also be well exposed through more traditional methods, the power and generality of the universal CA map Eq. (5) to uncover new symmetries and establish equivalence classes of CA behavior has been made apparent. To prove the general statements made on construction invariance – and how equivalent rules under construction can be found – Eq. (5) is crucial, since it directly addresses any 1D CA rule. Theorem 4, called "constructor's theorem" and its corollary are the main new results of this manuscript. Together with Theorems 7 and 8 (on Pascal rules and invariance upon addition modulo p), they can be used to establish the origin of complexity in 1D cellular automata [11]: *a weak symmetry breaking of the invariance upon addition modulo p of a Pascal rule after copying it to a higher range* (*see Definition 1*) *yields the most complex CA rules*. This will be discussed in detail elsewhere (see also [11]).

Acknowledgements

Thanks to Katharina Krischer and Jose Manuel García Sanchis for fruitful conversations. Financial support from the Technische Universität München – Institute for Advanced Study, funded by the German Excellence Initiative, is also gratefully acknowledged.

References

[1] S. Wolfram, A New Kind of Science, Wolfram Media Inc., Champaign, IL, 2002.
[2] A. Ilachinski, Cellular Automata: A Discrete Universe, World Scientific, Singapore, 2001.
[3] V. García-Morales, Phys. Lett. A 376 (2012) 2645.
[4] S. Wolfram, Cellular Automata and Complexity: Collected Papers, Addison–Wesley, Reading, MA, 1994.
[5] Physica (Amsterdam) D issues No. 10 and No. 45 are devoted to CA.
[6] E. Fredkin, Physica D 45 (1990) 254.
[7] S. Wolfram, Nature 311 (1984) 419.
[8] S. Wolfram, Rev. Mod. Phys. 55 (1983) 601.
[9] S. Wolfram, Physica D 10 (1984) 1.
[10] L.O. Chua, A Nonlinear Dynamics Perspective of Wolfram's New Kind of Science, vols. I–IV, World Scientific, Singapore, 2006–2011.
[11] See V. Garcia-Morales, arXiv:1203.3939.
[12] O. Martin, A.M. Odlyzko, S. Wolfram, Comm. Math. Phys. 93 (1984) 219.